

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Report of the Quantum Information Science and Technology Experts Panel

“... it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds sway.”

Richard P. Feynman (1985)

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Technology Experts Panel (TEP) Membership:

Chair: Dr. Richard Hughes – Los Alamos National Laboratory

Deputy Chair: Dr. Gary Doolen – Los Alamos National Laboratory

Prof. David Awschalom – University of California: Santa Barbara

Prof. Carlton Caves – University of New Mexico

Prof. Michael Chapman – Georgia Tech

Prof. Robert Clark – University of New South Wales

Prof. David Cory – Massachusetts Institute of Technology

Dr. David DiVincenzo – IBM: Thomas J. Watson Research Center

Prof. Artur Ekert – Cambridge University

Prof. P. Chris Hammel – Ohio State University

Prof. Paul Kwiat – University of Illinois: Urbana-Champaign

Prof. Seth Lloyd – Massachusetts Institute of Technology

Prof. Gerard Milburn – University of Queensland

Prof. Terry Orlando – Massachusetts Institute of Technology

Prof. Duncan Steel – University of Michigan

Prof. Umesh Vazirani – University of California: Berkeley

Prof. K. Birgitta Whaley – University of California: Berkeley

Dr. David Wineland – National Institute of Standards and Technology: Boulder

Produced for the Advanced Research and Development Activity (ARDA)

Document coordinator: Richard Hughes

Editing & compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

QUANTUM COMPUTATION ROADMAP VERSION 2.0 RELEASE NOTES	v
EXECUTIVE SUMMARY	1
1.0 BACKGROUND: QUANTUM COMPUTATION	1
2.0 INTRODUCTION: PURPOSE AND METHODOLOGY OF THE ROADMAP.....	2
3.0 QUANTUM COMPUTATION ROADMAP 2007 AND 2012 HIGH-LEVEL GOALS	4
4.0 QUANTUM COMPUTATION ROADMAP MID-LEVEL VIEW.....	5
5.0 QUANTUM COMPUTATION ROADMAP DETAILED-LEVEL VIEW	10
6.0 DETAILED QUANTUM COMPUTATION SUMMARIES.....	11
7.0 QUANTUM COMPUTATION ROADMAP SUMMARY: THE WAY FORWARD ...	11
APPENDIX: A LIST OF ACRONYMS AND ABBREVIATIONS	A-1
APPENDIX: A GLOSSARY OF TERMS.....	A-2
APPENDIX: B REFERENCES FOR THE QC ROADMAP	B-1

List of Tables

Table 4.0-1 The Mid-Level Quantum Computation Roadmap: Promise Criteria.....	7
Table 6.0-1 Detailed Summaries of Quantum Computation Approaches.....	11

List of Acronyms and Abbreviations

(**Note:** Definitions of acronyms and technical terms for the whole roadmap are contained in Appendix A.)

ARDA	Advanced Research and Development Activity	QC	quantum computation/computing
ARO	Army Research Office	QCPR	Quantum Computing Program Review
CMOS	complementary metal oxide semiconductor	QED	quantum electrodynamics
DFS	decoherence-free subspace	QIP	quantum information processing
GHZ	Greenberger, Horne, and Zeilinger	QIS	quantum information science
KLM	Knill, Laflamme, and Milburn	QIST	quantum information science and technology
NMR	nuclear magnetic resonance	rf	radio frequency
NRO	National Reconnaissance Office	RSFQ	rapid single flux quantum
NSA	National Security Agency	SET	single electron transistor
		TEP	technology experts panel

QUANTUM COMPUTATION ROADMAP VERSION 2.0 RELEASE NOTES

April 2004

The quantum computation (QC) roadmap was released in Version 1.0 form in December 2002 as a living document. This new, Version 2.0, release, while retaining the majority of the Version 1.0 content, provides an opportunity to

- incorporate advances in the field that have occurred during the intervening 14 months;
- make minor modifications to the roadmap structure to better capture the challenges involved in transitioning from a single qubit to two;
- add major sections on topics that could not be covered in Version 1.0; and
- reflect on the purpose, impact, and scope of the roadmap, as well as its future role.

Some of the most significant changes in this Version 2.0 of the QC roadmap have been to incorporate the major advances that have occurred since the release of Version 1.0. These include

- realization of probabilistic controlled-NOT quantum logic gates in linear optics,
- the controlled-NOT quantum logic gates demonstrated in two-ion traps,
- the achievement of near single-shot sensitivity for single electron spins in quantum dots, and
- the excellent coherence times observed in Josephson qubits

which, together with the other multiple advances noted in the roadmap, are indicative of the continued healthy rate of development of this challenging field toward the roadmap desired goals.

In meetings of the roadmap experts panel members at the August 2003 Quantum Computing Program Review in Nashville, Tennessee, it was decided to increase the number of “two qubit” development status metrics in the mid-level roadmap view to more accurately reflect the distinct, challenging scientific steps encountered within each QC approach in moving from one qubit to two. It was also decided to relegate coverage of the DiVincenzo “promise criteria” and development status metrics for “unique qubits” from the mid-level view roadmap tables to the appropriate summary section. With these changes and additions, Version 2.0 of the QC roadmap provides a more precise and up-to-date account of the status of the field and its rate of development toward the roadmap 2007 desired goal, as of March 2004.

Perhaps the most unsatisfactory aspect of Version 1.0 of the QC roadmap was that with its almost exclusive focus on experimental implementations, only a limited coverage of the important role of theory in reaching the roadmap desired goals was possible. One of the major additions in Version 2.0 is the expansion of the theory summary section to adequately represent the pivotal roles of theory, with sections on: quantum algorithms and quantum computational complexity, quantum information theory, quantum computer architectures, and the theory of decoherence. A second major addition in Version 2.0 is a full summary section on cavity-QED approaches to QC. Another significant change in Version 2.0 is in the coverage of solid-state

QC, where the summary section has been streamlined, and in the roadmap's mid-level view the great diversity of SSQC approaches has been captured into just two categories: "charge or excitonic qubits" and "spin qubits." With these major additions and changes, Version 2.0 of the QC roadmap provides a significantly more comprehensive view of the entire field and the role of each element in working toward the roadmap high-level desired goals.

With the benefit of just over one year of experience with the impact of and community response to the first version of the QC roadmap, this Version 2.0 release provides an opportunity to reflect on its structure, scope, and future role. One of the most useful features of the roadmap is that by proposing specific desired development targets and an associated timeline it has focused attention and inspired debate, which are essential for effectively moving forward. The roadmap experts panel members have received considerable input regarding the roadmap's chosen desired high-level goals; the majority of comments characterize these goals as falling into the "ambitious yet attainable" category. Nevertheless, in the light of the recent progress noted in this roadmap update, it is worth asking whether an even more aggressive time line could be envisioned leading to a significantly more advanced development destination for QC (beyond the roadmap's desired quantum computation testbed era) within the 2012 time horizon. This question can be best considered by comparing the QC roadmap with generally accepted principles of science and technology roadmaps [1,2]. The research degree of difficulty involved in reaching the 2007 desired high-level goal is unquestionably very high, but the risk associated with the fundamental scientific challenges involved is mitigated by pursuing the multiple paths described in the roadmap. Achieving the high-level goals along one or more of these paths will require a sustained and coordinated effort; the uncertainties remain too high today to pick out a more focused development path. An attempt to do so at this time could potentially divert resources away from ultimately more promising research directions. This would increase the risk that QC could fail to reach the quantum computational testbed era by 2012, beyond the considerable but acceptable levels of the path defined in this roadmap. However, this issue should be reassessed once the field moves closer to the 2007 desired goal. The roadmap experts panel members believe that the QC roadmap's desired high-level goals and timeline, while remaining consistent with accepted norms of risk within advanced, fundamental science and technology research programs, are sufficiently challenging to effectively stimulate progress. They intend to revisit these important issues in future updates.

- [1] Kostoff R.N. and R.R. Schaller, "Science and technology roadmaps," *IEEE Transactions on Engineering Management* **48**, 132–143 (2001).
- [2] Mankins, J.C., "Approaches to strategic research and technology (R&T) analysis and road mapping," *Acta Astronautica* **51**, 3–21 (2002).

EXECUTIVE SUMMARY

Quantum computation (QC) holds out tremendous promise for efficiently solving some of the most difficult problems in computational science, such as integer factorization, discrete logarithms, and quantum simulation and modeling that are intractable on any present or future conventional computer. New concepts for QC implementations, algorithms, and advances in the theoretical understanding of the physics requirements for QC appear almost weekly in the scientific literature. This rapidly evolving field is one of the most active research areas of modern science, attracting substantial funding that supports research groups at internationally leading academic institutions, national laboratories, and major industrial-research centers. Well-organized programs are underway in the United States, the European Union and its member nations, Australia, and in other major industrial nations. Start-up quantum-information companies are already in operation. A diverse range of experimental approaches from a variety of scientific disciplines are pursuing different routes to meet the fundamental quantum-mechanical challenges involved. Yet experimental achievements in QC, although of unprecedented complexity in basic quantum physics, are only at the proof-of-principle stage in terms of their abilities to perform QC tasks. It will be necessary to develop significantly more complex quantum-information processing (QIP) capabilities before quantum computer-science issues can begin to be experimentally studied. To realize this potential will require the engineering and control of quantum-mechanical systems on a scale far beyond anything yet achieved in any physics laboratory. This required control runs counter to the tendency of the essential quantum properties of quantum systems to degrade with time (“decoherence”). Yet, it is known that it should be possible to reach the “quantum computer-science test-bed regime”—if challenging requirements for the precision of elementary quantum operations and physical scalability can be met. Although a considerable gap exists between these requirements and any of the experimental implementations today, this gap continues to close.

To facilitate the progress of QC research towards the quantum computer-science era, a two-day “Quantum Information Science and Technology Experts Panel Meeting” (membership is listed on the inside cover of this document) was held in La Jolla, California, USA, in late January 2002 with the objective of formulating a QC roadmap. The panel’s members decided that a desired future objective for QC should be

- to develop by 2012 a suite of viable emerging-QC technologies of sufficient complexity to function as quantum computer-science test-beds in which architectural and algorithmic issues can be explored.

The panel’s members emphasize that although this is a desired outcome, not a prediction, they believe that it is attainable if the momentum in this field is maintained with focus on this objective. The intent of this roadmap is to set a path leading to the desired QC test-bed era by 2012 by providing some direction for the field with specific five- and ten-year technical goals. While remaining within the “basic science” regime, the five-year (2007) goal would project QC far enough in terms of the precision of elementary quantum operations and correction of quantum errors that the potential for further scalability could be reliably assessed. The ten-year (2012) goal would extend QC into the “architectural/algorithmic” regime, involving a quantum system of such complexity that it is beyond the capability of classical computers to simulate. These high-level goals are ambitious but attainable as a collective effort with cooperative interactions between different experimental approaches and theory.

Within these overall goals, different scientific approaches to QC will play a variety of roles: it is expected that one or more approaches will emerge that will actually attain these goals. Other approaches may not—but will instead play other vitally important roles, such as offering better scalability potential in the post-2012 era or exploring different ways to implement quantum logic, that will be essential to the desired development of the field as a whole. It was the unanimous opinion of the Technology Experts Panel (TEP) that it is too soon to attempt to identify a smaller number of potential “winners;” the ultimate technology may not have even been invented yet. Considerable evolution of and hybridization between approaches has already taken place and should be expected to continue in the future, with existing approaches being superseded by even more promising ones.

A second function of the roadmap is to allow informed decisions about future directions to be made by tracking progress and elucidating interrelationships between approaches, which will assist researchers to develop synergistic solutions to obstacles within any one approach. To this end, the roadmap presents a “mid-level view” that segments the field into the different scientific approaches and provides a simple graphical representation using a common set of criteria and metrics to capture the promise and characterize progress towards the high-level goals within each approach. A “detailed-level view” incorporates summaries of the state-of-play within each approach, provides a timeline for likely progress, and attempts to capture its role in the overall development of the field. A summary provides some recommendations for moving toward the desired goals. The panel members developed the first version of the QC roadmap from the La Jolla meeting and five follow-up meetings held in conjunction with the annual ARO/ARDA/NSA/NRO Quantum Computing Program Review (QCPR) in Nashville, Tennessee, USA, in August 2002. The present (version 2.0) update was developed out of a further four meetings at the August 2003 QCPR; the roadmap will continue to be updated annually.

The quantum computer-science test-bed destination that we envision in this roadmap will open up fascinating, powerful new computational capabilities: for evaluating quantum-algorithm performance; allowing quantum simulations to be performed; and for investigating alternative architectures, such as networked quantum subprocessors. The journey to this destination will lead to many new scientific and technological developments with potential societal and economic benefits. Quantum systems of unprecedented complexity will be created and controlled, potentially leading to greater fundamental understanding of how classical physics emerges from a quantum world, which is as perplexing and as important a question today as it was when quantum mechanics was invented. We can foresee that these QC capabilities will lead into an era of “quantum machines” such as atomic clocks with increased precision with benefits to navigation, and “quantum enhanced” sensors. Quantum light sources will be developed that will be enabling technologies for other applications such as secure communications, and single-atom doping techniques will be developed that will open up important applications in the semiconductor industry. We anticipate that there will be considerable synergy with nanotechnology and spintronics. The journey ahead will be challenging but it is one that will lead to unprecedented advances in both fundamental scientific understanding and practical new technologies.

1.0 BACKGROUND: QUANTUM COMPUTATION

The representation of information by classical physical quantities such as the voltage levels in a microprocessor is familiar to everyone. But quantum information science (QIS) has been developed to describe binary information in the form of two-state quantum systems, such as: two distinct polarization states of a photon; two energy levels of an atomic electron; or the two spin directions of an electron or atomic nucleus in a magnetic field. A single bit of information in this form has come to be known as a “qubit.” With two or more qubits, it becomes possible to consider quantum logical-“gate” operations in which a controlled interaction between qubits produces a (coherent) change in the state of one qubit that is contingent upon the state of another. These gate operations are the building blocks of a quantum computer. (See Appendix A for a glossary of quantum computation [QC] terms.) In principle, a quantum computer is a very much more powerful device than any existing or future classical computer because the superposition principle allows an extraordinarily large number of computations to be performed simultaneously. For certain problems, such as integer factorization and the discrete-logarithm problem, which are believed to be intractable on any present-day or future conventional computer, this “quantum parallelism” would permit their efficient solution. These are important problems as they form the foundation of nearly all publicly used encryption techniques. Another example of great potential impact, as first described by Feynman, is quantum modeling and simulation (e.g., for designing future nanoscale electronic components)—exact calculations of such systems can only be performed using a quantum computer. This simulation capability has the potential for discovering new phenomenology in mesoscopic/nanoscale physics, which in turn could lead to new devices and technologies. (It is not known if quantum computers will offer computational advantages over conventional computers for general-purpose computation.) To realize this potential will require the engineering and control of quantum-mechanical systems on a scale far beyond anything yet achieved in any physics laboratory. Many approaches to QC from diverse branches of science are being pursued. Needless to say, these present-day QC technologies are some orders of magnitude away in both numbers of qubits and numbers of quantum logic operations that can be performed from the sizes that would be required for solving interesting problems. A few experimental approaches are now capable of performing small numbers of quantum operations on small numbers of qubits, with realistic assessments of the challenges for scale-up, while the bulk of the field is at the single-qubit stage with optimistic ideas for producing large-scale systems. There are both fundamental and technical challenges to bridging this gap.

A serious obstacle to practical QC is the propensity for qubit superpositions of 0 and 1 to “decohere” into either 0 or 1. (This phenomenon of decoherence is invoked to explain why macroscopic objects are not observed in quantum superposition states.) However, theoretical breakthroughs have been made in generalizing conventional error-correction concepts to correct decoherence in a quantum computer. A single logical bit would be encoded as the state of several physical qubits and quantum logic operations used to correct decoherence errors. These quantum error-correction ideas have been shown to allow robust, or fault-tolerant QC with the encoded logical qubits, at the expense of introducing considerable overhead in the numbers of physical qubits and elementary quantum logic operations on them. (For example, one logical qubit may be encoded as a state of five physical qubits in one scheme, although the number of physical qubits constituting a logical qubit could well be different for different physical QC

implementations.) It has been established, under certain assumptions, that if a threshold precision per gate operation could be achieved, quantum error correction would allow a quantum computer to compute indefinitely.

An essential ingredient of quantum error-correction techniques and QC in general, is the capability to create entangled states of multiple qubits on demand. In these peculiarly quantum-mechanical states the joint properties of several qubits are uniquely defined, even though the individual qubits have no definite state. The strength of the correlations between qubits in entangled states is the most prominent feature distinguishing quantum physics from the familiar world of classical physics. The unusual properties of these states, which do not readily exist in nature, underlie the potential new capabilities of QC and other quantum technologies. Although present-day QC experiments are making rapid progress, demonstrations of on-demand entanglement are few and the precision of gate operations is quite far from the fault-tolerant thresholds. However, experimental capabilities will progress and the fault-tolerant requirements are likely to be relaxed once the underlying assumptions are adapted to specific approaches. The overall purpose of this roadmap is to help achieve these thresholds and to facilitate the progress of QC research towards the quantum computer-science era.

2.0 INTRODUCTION: PURPOSE AND METHODOLOGY OF THE ROADMAP

This roadmap has been formulated and written by the members of a Technology Experts Panel (TEP or the “panel”), whose membership of internationally recognized researchers (see list on inside cover) in quantum information science and technology (QIST) held a kick-off meeting in La Jolla, California, USA, in late January 2002 to develop the underlying roadmap methodology. The TEP held a further five meetings in conjunction with the annual ARO/ARDA/NSA/NRO Quantum Computation Program Review (QCPR) meeting in Nashville, Tennessee, USA, in August 2002. The sheer diversity and rate of evolution of this field, which are two of its significant strengths, made this a particularly challenging exercise. To accommodate the rapid rate of new developments in this field, the roadmap will be a living document that will be updated annually, and at other times on an *ad hoc* basis if merited by significant developments. Certain topics will be revisited in future versions of the roadmap and additional ones added; it is expected that there will be significant changes in both content and structure. At the La Jolla meeting, TEP members decided that the overall purpose of the roadmap should be to set as a desired future objective for QC

- to develop by 2012 a suite of viable emerging-QC technologies of sufficient complexity to function as quantum computer-science test-beds in which architectural and algorithmic issues can be explored.

The roadmap is intended to function in several ways to aid this development. It has a prescriptive role by identifying what scientific, technology, skills, organizational, investment, and infrastructure developments will be necessary to achieve the desired goal, while providing options for how to get there. It also performs a descriptive function by capturing the status and likely progress of the field while elucidating the role that each aspect of the field is expected to play toward achieving the desired goal. The roadmap can identify gaps and opportunities, and places where strategic investments would be beneficial. It will provide a framework for coordinating research activities and a venue for experts to provide advice. The roadmap will therefore

allow informed decisions about future directions to be made, while tracking progress, and elucidating interrelationships between approaches to assist researchers to develop synergistic solutions to obstacles within any one approach. The roadmap is intended to be an aid to researchers and to those managing or observing the field.

Underlying the overall objective for the QC roadmap, the panel members decided on a four-level structure with a division into “high level goals,” “mid-level descriptions,” “detailed level summaries,” and a summary that includes the panel’s recommendations for optimizing the way forward.

The panel members decided on specific ambitious, but attainable five- and ten-year high level technical goals for QC. These technical goals set a path for the field to follow that will lead to the desired QC test-bed era in 2012.

The mid-level roadmap view captures the breadth of approaches to QC on the international scale and uses a graphical format to describe in general terms how the different research approaches are progressing towards these technical goals relative to common sets of criteria and metrics. The panel decided to first segment the field into a few broad categories, with multiple projects grouped together in each category according to their underlying similarities. The panel decided that two types of measures were necessary to adequately represent the status of each category: a set of criteria characterizes the “promise” of a class of approaches as a candidate QC technology; whereas a set of metrics captures the “status” of the approach in terms of technical advances along the way to achieving the high-level goals.

The “detailed summaries” provide more information on the essential concept of each approach, the breadth of projects involved, the advantages and challenges of the class of approaches, and a timeline for likely progress according to a common format. These summaries, written by subgroups of the panel members after soliciting input from their respective scientific communities, are intended to provide a brief, readable account that represents the status and potential of the entire approach from a world-wide perspective. The panel has endeavored to provide a complete, balanced, and inclusive picture of each research approach, but with the caveat that it is expected that additional content will need to be added to each summary in future versions of the roadmap, after further input from the scientific community. The panel members decided that it was not appropriate for the roadmap to attempt to describe the relative status of different individual projects within each approach.

The panel members found it especially challenging to adequately represent the status and role of theory in the roadmap. Clearly, theory has been pivotal in the development of QC to its present state, providing often unanticipated advances that have stimulated experimental investigations. At the same time, it is difficult to schedule or define meaningful “metrics” for such future breakthroughs. For Version 1.0 of the roadmap the panel decided that the primary focus would be on experimental approaches to QC and limited the description of theory to its historical role. In the present Version 2.0 release all sections have been updated to reflect advances in the 14 months since release of Version 1.0. In addition new sections on cavity-QED approaches to QC and a full theory section, with coverage of decoherence theory, quantum information theory, quantum algorithms and QC complexity, and quantum computer architectures, have been added. In addition, each detailed summary for the different experimental areas provides an overview of the specific areas in which additional theory work is needed.

3.0 QUANTUM COMPUTATION ROADMAP 2007 AND 2012 HIGH-LEVEL GOALS

Although QC is a basic-science endeavor today, it is realistic to predict that within a decade fault-tolerant QC could be achieved on a small scale. The overall objective of the roadmap can be accomplished by facilitating the development of QC to reach a point from which scalability into the fault-tolerant regime can be reliably inferred. It is essential to appreciate that “scalability” has two aspects: the ability to create registers of sufficiently many physical qubits to support logical encoding *and* the ability to perform qubit operations within the fault-tolerant precision thresholds. The desired 2007 and 2012 high-level goals of the roadmap for QC are therefore,

- by the year 2007, to
 - encode a single qubit into the state of a logical qubit formed from several physical qubits,
 - perform repetitive error correction of the logical qubit, and
 - transfer the state of the logical qubit into the state of another set of physical qubits with high fidelity, and
- by the year 2012, to
 - implement a concatenated quantum error-correcting code.

Meeting these goals will require both experimental and theoretical advances. While remaining within the basic-science regime, the 2007 high-level goal requires the achievement of four ingredients that are necessary for fault-tolerant scalability:

- creating deterministic, on-demand quantum entanglement;
- encoding quantum information into a logical qubit;
- extending the lifetime of quantum information; and
- communicating quantum information coherently from one part of a quantum computer to another.

This is a challenging 2007 goal—requiring something on the order of ten physical qubits and multiple logic operations between them, yet it is within reach of some present-day QC approaches and new approaches that may emerge from synergistic interactions between present approaches.

The 2012 high-level goal, which requires on the order of 50 physical qubits,

- exercises multiple logical qubits through the full range of operations required for fault-tolerant QC in order to perform a simple instance of a relevant quantum algorithm, and
- approaches a natural experimental QC benchmark: the limits of full-scale simulation of a quantum computer by a conventional computer.

The 2012 goal would be within reach of approaches that attain the 2007 goal. It would extend QC into the quantum computer test-bed regime, in which architectural and algorithmic issues could be explored experimentally. Quantum computers of this size would also open up the possibilities of quantum simulation as originally envisioned by Feynman. New ways of using the computational capabilities of these small quantum computers could be explored, such as

distributed QC and classically networked arrays (“type II” quantum computers), which recent work suggests may be advantageous for partial differential equation simulations, even though in contrast to other potential QC applications no exponential or polynomial speed-up would be possible.

Within these overall goals, different scientific approaches will play a variety of roles; it is expected that one or more approaches will emerge that will actually attain these goals, while others will not, but will instead play vitally important supporting roles (by exploring different ways to implement quantum logic, for instance) that will be essential to the desired development of the field as a whole. It was the unanimous opinion of the TEP that it is too soon to attempt to identify a smaller number of potential “winners;” the ultimate technology may not have even been invented yet. Considerable evolution of and hybridization between the various approaches has already taken place and should be expected to continue in the future, with some existing approaches being superseded by even more promising ones.

4.0 QUANTUM COMPUTATION ROADMAP MID-LEVEL VIEW

The mid-level roadmap view is intended to describe in general terms how the entire field of QC is progressing towards the high-level goals and provides a simple graphical tool to characterize the promise and development status according to common sets of criteria and metrics, respectively. The requirements for quantum computer hardware capable of achieving the high-level goals are simply stated but are very demanding in practice.

1. A quantum register of multiple qubits must be prepared in an addressable form and isolated from environmental influences, which cause the delicate quantum states to decohere.
2. Although weakly coupled to the outside world, the qubits must nevertheless be strongly coupled together to perform logic-gate operations.
3. There must be a readout method to determine the state of each qubit at the end of the computation.

Many different routes from diverse fields of science to realizing these requirements are being pursued. Consequently, in order to adequately represent progress, the TEP decided to segment the field into several broad classes, based on their underlying experimental physics subfields. These subfields are

- nuclear magnetic resonance (NMR) quantum computation,
- ion trap quantum computation,
- neutral atom quantum computation,
- cavity quantum electro-dynamic (QED) computation
- optical quantum computation,
- solid state (spin-based and quantum-dot-based) quantum computation,
- superconducting quantum computation, and
- “unique” qubits (e.g., electrons on liquid helium, spectral hole burning, etc.) quantum computation.
- the theory subfield, including quantum information theory, architectures, and decoherence challenges.

Each of the different experimental approaches has its own particular strengths as a candidate QC technology. For example, atomic, optical, and NMR approaches build on well-developed experimental capabilities to create and control the quantum properties necessary for QC, whereas the solid-state and superconducting approaches can draw on existing large investments in fabrication technologies and materials studies. However, the different approaches are at different stages of development. Insights from the more developed approaches can be usefully incorporated into other, less advanced approaches, which may hold out greater potential for leading to larger-scale quantum computers. The panel decided that to adequately represent this diversity required a set of criteria for the ‘promise’ of each approach, and a set of metrics for its ‘status’ (state of progress towards the high-level goals).

To represent the promise of each approach the panel decided to adopt the “DiVincenzo criteria.” Necessary conditions for any viable QC technology can be simply stated as:

1. a scalable physical system of well-characterized qubits;
2. the ability to initialize the state of the qubits to a simple fiducial state;
3. long (relative) decoherence times, much longer than the gate-operation time;
4. a universal set of quantum gates; and
5. a qubit-specific measurement capability.

Two additional criteria, which are necessary conditions for quantum computer networkability are

6. the ability to interconvert stationary and flying qubits and
7. the ability to faithfully transmit flying qubits between specified locations.

The physical properties, such as decoherence rates of the two-level quantum systems (qubits) used to represent quantum information must be well understood. The physical resource requirements must scale linearly in the number of qubits, not exponentially, if the approach is to be a candidate for a large-scale QC technology. It must be possible to initialize a register of qubits to some state from which QC can be performed. The time to perform a quantum logic operation must be much smaller than the time-scales over which the system’s quantum information decoheres. There must be a procedure identified for implementing at least one set of universal quantum logic operations. In order to read out the result of a quantum computation there must be a mechanism for measuring the final state of individual qubits in a quantum register. The two networking criteria are necessary if it is desired to transfer quantum information from one location to another, (e.g., between different registers or between different processors in a distributed computing situation).

Many different QC architectures are possible within the DiVincenzo framework. For example, architectures based on “clocked” or “ballistic” quantum logic implementations are being pursued. Some approaches are intrinsically limited to quantum logic gates between nearest-neighbor qubits, which would allow parallel operations within a QC, whereas other approaches are capable of performing logic gates between widely-separated qubits but are limited to serial operations.

To visually represent the DiVincenzo “promise criteria” of each QC approach, the panel decided to use a simple three-color scheme as shown below (Table 4.0-1).

Table 4.0-1
The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Approach	The DiVincenzo Criteria							
	Quantum Computation						QC Networkability	
	#1	#2	#3	#4	#5		#6	#7
NMR								
Trapped Ion								
Neutral Atom								
Cavity QED								
Optical								
Solid State								
Superconducting								
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							

Legend: = a potentially viable approach has achieved sufficient proof of principle
 = a potentially viable approach has been proposed, but there has not been sufficient proof of principle
 = no viable approach is known

- The column numbers correspond to the following QC criteria:
- #1. A scalable physical system with well-characterized qubits.
 - #2. The ability to initialize the state of the qubits to a simple fiducial state.
 - #3. Long (relative) decoherence times, much longer than the gate-operation time.
 - #4. A universal set of quantum gates.
 - #5. A qubit-specific measurement capability.
 - #6. The ability to interconvert stationary and flying qubits.
 - #7. The ability to faithfully transmit flying qubits between specified locations.

The values assigned to these criteria constitute a snapshot in time of the panel’s opinions on the potential of each approach as a candidate QC technology. Future developments within an approach will lead to these values being updated.

To represent the present status of each approach the panel developed a set of metrics that represent relevant steps on the way to the 2007- and 2012-year goals. The panel decided to use a similar color coding to indicate the status of each approach (Table 4.0-2). The “development status metrics”, which have been augmented somewhat for this version 2.0, are given on the page facing Table 4.0-2.

The development status metrics 1 through 4 correspond to steps on the way to achieving the high-level goals for 2007, while development status metrics 5 through 7 correspond to steps leading up to the high-level goal for 2012. For each QC approach the TEP members have assigned a status code for each of these metrics. These codes will be updated in future versions of the roadmap to reflect significant developments within each approach.

Table 4.0-2
The Mid-Level QC Roadmap—Development Status Metrics

QC Approach	1	1.1	2	2.1	2.2	2.3	3	3.1	3.2	3.3	3.4	3.5	3.6	4	4.1	4.2	4.3	4.4
NMR																		
Trapped Ion																		
Neutral Atom																		
Cavity QED																		
Optical																		
Solid State:																		
Charged or excitonic qubits																		
Spin qubits																		
Superconducting																		
QC Approach	4	4.5	5	5.1	5.2	6	6.1	6.2	6.3	7	7.1	7.2	7.3	7.4	7.5			
NMR																		
Trapped Ion																		
Neutral Atom																		
Cavity QED																		
Optical																		
Solid State:																		
Charged or excitonic qubits																		
Spin qubits																		
Superconducting																		

Legend: = sufficient experimental demonstration
 = preliminary experimental demonstration, but further experimental work is required
 = no experimental demonstration and = a change in the development status between Versions 1.0 and 2.0

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states.
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit.
 - 2.2 Demonstrate decoherence times much longer than the Rabi oscillation period.
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere.
3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations.
 - 3.2 Produce and characterize the Bell entangled states.
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times.
 - 3.4 Demonstrate quantum state and process tomography for two qubits.
 - 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS).
 - 3.6 Demonstrate a two-qubit quantum algorithm.
4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, and Zeilinger (GHZ) entangled state of three physical qubits.
 - 4.2 Produce maximally-entangled states of four or more physical qubits.
 - 4.3 Quantum state and process tomography.
 - 4.4 Demonstrate DFSs.
- 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations etc.) between physical qubits.
- 4.6 Demonstrate quantum error-correcting codes.
- 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza).
- 4.8 Demonstrate quantum logic operations with fault-tolerant precision.
5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction.
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit.
6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations.
 - 6.2 Produce two-logical-qubit Bell states.
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations.
7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits.
 - 7.2 Produce maximally-entangled states of four or more logical qubits.
 - 7.3 Demonstrate the transfer of quantum information between logical qubits.
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits.
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits.

When interpreting this mid-level graphical part of the roadmap, it is important to appreciate that both the “promise criteria” and “development status metrics” need to be considered. For example, the “promise criterion” for NMR QC (in the liquid state) indicates that it does not have good scalability potential, but the “development status” metric shows that multiple steps have already been achieved in this approach. Although not likely in its current form to be a candidate for a large-scale QC technology, the opportunity to learn how to perform QIP tasks within this approach is of tremendous value to the field in general. Conversely, some approaches are much less far along in their development status metrics, but an inspection of their promise criteria reveals that they offer significantly greater potential for achieving a large-scale QC technology. Intermediate between these two extremes a few approaches have the essential ingredients for QC under sufficient control that they have started to make the first steps towards developing a scalable architecture. The detailed-level view of the roadmap provides the means to more fully understand these subtleties of interpretation.

5.0 QUANTUM COMPUTATION ROADMAP DETAILED-LEVEL VIEW

The purpose of the detailed-level roadmap summaries is to provide a short description of each of the experimental approaches, along with explanations of the graphical representation of the metrics in the mid-level view and descriptions of the likely developments over the next decade. A common set of points is addressed in each summary:

- who is working on this approach,
- the location and the size of the group,
- a brief description of the essential idea of the approach and how far it is developed,
- a summary of how this approach meets the DiVincenzo criteria and their status,
- a list of what has been accomplished, when it was accomplished, and by whom, for the development status metrics 1–7,
- the “special strengths” of this approach,
- the unknowns and weaknesses of this approach,
- the 5-year goals for this approach,
- the 10-year goals for this approach,
- the necessary achievements to make the 5- and 10-year goals for the approach possible,
- scientific “trophy” that could be produced (these are defined to be breakthrough-quality results)
- what developments in other areas of QIST or other areas of science will be useful or necessary in this approach,
- how will developments within this approach have benefits to others areas of QIST or other areas of science in general,
- the role of theory in this approach, and
- a timeline that shows the necessary achievements and makes connection to the mid-level development status metrics.

Note: The TEP decided that assessments of individual projects within an approach would not be made a part of the roadmap because this is a program-management function.

In addition to the theory component of the detailed-level summary for each approach, there is a separate summary for fundamental theory. This summary provides historical background on significant theory contributions to the development of QC and also spells out general areas of theoretical work that will be needed on the way to achieving the 2007 and 2012-year high-level goals.

6.0 DETAILED QUANTUM COMPUTATION SUMMARIES

The summaries of the different research approaches to QC are listed in the table below (Table 6.0-1). Each of the summaries listed below is linked to a file on this web site (click on the summary title below to view / download that document).

Table 6.0-1
Detailed Summaries of Quantum Computation Approaches

Quantum Computation Approach Summary	Compiled by
6.1 Nuclear magnetic resonance approaches to quantum-information processing and quantum computing	David Cory
6.2 Ion trap approaches to quantum-information processing and quantum computing	David Wineland
6.3 Neutral atom approaches to quantum-information processing and quantum computing	Carlton Caves
6.4 Cavity QED approaches to quantum-information processing and quantum computing	Michael Chapman
6.5 Optical approaches to quantum-information processing and quantum computing	Paul Kwiat and Gerard Milburn
6.6 Solid state approaches to quantum-information processing and quantum computing	David Awschalom, Robert Clark, David DiVincenzo, P. Chris Hammel, Duncan Steel and, Birgitta Whaley
6.7 Superconducting approaches to quantum-information processing and quantum computing	Terry Orlando
6.8 "Unique" qubit approaches to quantum-information processing and quantum computing	P. Chris Hammel and Seth Lloyd
6.9 Theory component of the quantum computing roadmap	David DiVincenzo, Gary Doolen, Seth Lloyd, Umesh Vazirani, Brigitta Whaley

7.0 QUANTUM COMPUTATION ROADMAP SUMMARY: THE WAY FORWARD

"For a successful technology, reality must take precedence over public relations, for Nature cannot be fooled."
—Richard P. Feynman (1986)

When taking on a basic scientific challenge of the complexity and magnitude of QC, diversity of approaches, persistence, and patience are essential. Major strengths of QC research are the breadth of concepts being pursued, the high level of experimental and theoretical innovations, and the quality of the researchers involved. The rate of progress and level of achievements are

very encouraging, but breakthroughs in basic science cannot be expected to happen to a schedule. Nevertheless, the desired 2012 QC destination and the high-level goals that are set out in this roadmap, although ambitious, are within reach if experimenters and theorists work together, appropriate strategic basic research is pursued, and relevant technological developments from closely related fields, such as nanotechnology and spintronics, are incorporated. In developing this document the TEP members have noted several areas where additional attention, effort, or resources would be advantageous.

- The emphasis of the quantum computing roadmap out to 2007 is on the experimental development of error-corrected logical qubits. Without this critical building block, plans for further scale-up would be premature; they would not have a firm foundation. Nevertheless, it is important to begin investigations aimed at evaluating key factors associated with scaled architectures at an exploratory design level, for the various implementation approaches. Such pathway studies, carried out in parallel with the qubit demonstration programs, will require expertise outside of the quantum information science framework. By examining the feasibility of the qubit schemes from a systems perspective, this exercise would define sensible metrics for scale-up, and initiate a closing of the gap between conventional computer systems protocols and quantum information science requirements. It would also encourage a dialogue between quantum information scientists and engineers that will become increasingly important as the field moves toward the logical qubit milestones.
- As one looks to the future development of QC one should anticipate the need for an increasing industrial involvement as the first steps into the realm of scalability are made. For example, much could be learned by trying to develop a few qubit “quantum subprocessor” that incorporates the quantum ingredients and the classical control and readout in a single device. But this will involve a level of applied-science expertise and capability that is unlikely to be found in a university environment. University-industry partnerships would offer an effective route forward. The first steps in this direction are already taking place (e.g., the Australian Centre for Quantum Computing Technology) and the panel recommends that further interactions of this type need to be encouraged and facilitated.
- While the intrinsic scalability of qubits is a central issue, it is also important to think in parallel about the more conventional scalability of experimental infrastructure and techniques required to control and readout the qubits, in order to meet the roadmap timeline. At present, single and few-qubit implementations often involve a substantial array of complex, expensive, and highly specialized equipment items. The step-up from few-qubit experiments to the 2007 high-level goal of encoding quantum information into a logical qubit formed by several physical qubits and the demonstration of fault-tolerant control via repetitive error correction goes beyond replicating qubit cells and will place stringent demands on the overall experimental configuration. In the case of all-electronic solid-state qubits for example, the development of a fast (classical) control chip interfaced to a qubit chip is being pursued to address this issue (where it is instructive to consider the electronics and procedures required to operate a single rf-SET readout element). The control chip in this case may well involve a mix of technologies operating at different temperature levels, such as RSFQ and rf-CMOS, requiring collaboration across traditional boundaries. The drive towards fault-tolerant logical qubit operations separately raises many engineering, as opposed to

physics, issues and the early involvement of industry will be important. These issues will be brought into sharp focus by the 2012 objectives requiring some 50 physical qubits.

- Another area in which the TEP members foresee a future need for increased industrial involvement is in the general area of “supporting technology.” Efforts have already been made to ensure that certain critical capabilities are available to researchers in the superconducting QC community, and analogous needs in other areas of QC research should be anticipated. Examples of relevant areas include: materials and device fabrication, electro-optics, and single-photon detectors. The panel intends to amplify on the role of industry in future versions of this roadmap.
- Theory is an area in which the panel believes that some refocusing or expansion of effort would benefit the development of QC towards the roadmap objectives. Continued research efforts on high-quality, fundamental QC theory remain essential, but additional emphasis on theory and modeling that is directed at specific experimental QC approaches is required if this field is to move forward effectively. For example, further study of the fault-tolerant requirements in the context of the physics of specific approaches to QC is necessary. Closer involvement of theorists with their experimental colleagues is encouraged.
- The panel also recommends that additional effort be directed at QC architectural issues. For example, what architectures are suitable for a scalable system, and how may the most demanding requirements for scalable QC be traded-off against each other? Also, quantum logic units need to be integrated with data storage, data transmission, and schedulers, some or all of which can benefit from quantum implementation.
- Additional efforts within the mathematics and theoretical computer-science communities to better define the classes of problems that are amenable to speed-up on a QC should be encouraged, as should the more mundane but very important analysis of how abstract quantum algorithms can be mapped onto physical implementations of QC.
- The desired developments set out in this roadmap cannot happen without an adequate number of highly skilled and trained people to carry them out. The panel notes that graduate-student demand for research opportunities in QC is outstripping resources in many university departments. The panel believes that additional measures should be adopted to ensure that an adequate number of the best physics, mathematics, and computer-science graduate students can find opportunities to enter this field, and to provide a career path for these future researchers. Additional graduate-student fellowships and postdoctoral positions are essential, especially in experimental areas, and there is a need for additional faculty appointments, and the associated start-up investments, in quantum information science.

The quantum computer-science test-bed destination that we envision in this roadmap will open up fascinating, powerful new computational capabilities: for evaluating quantum algorithm performance, allowing quantum simulations to be performed, and for investigating alternative architectures, such as networked quantum subprocessors. The journey to this destination will lead to many new scientific and technological developments with myriad potential societal and economic benefits. A quantum computer provides the capability to create arbitrary quantum states of its qubits and so could be used as a tool for fundamental science and as an ingredient of quantum technologies that will open up new capabilities utilizing the uniquely quantum-

mechanical property of entanglement. It will be possible to create and control quantum systems of unprecedented complexity, potentially leading to greater fundamental understanding of how classical physics emerges from a quantum world, which is as perplexing and as important a question today as it was when quantum mechanics was invented. The development of small-scale QC capabilities will lead into an era of “quantum machines” such as atomic clocks with increased precision with benefits to navigation, and “quantum enhanced” sensors. Quantum light sources will be developed that will be enabling technologies for other applications such as secure communications, and single-atom doping techniques will be developed that will open up important capabilities in the semiconductor industry. The journey ahead will be challenging but it is one that will lead to unprecedented advances in both fundamental scientific understanding and practical new technologies.

Nuclear Magnetic Resonance Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.1

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not to be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: David Cory

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0	Groups Pursuing This Approach	1
2.0	Background and Perspective	1
3.0	Summary of NMR QC: The DiVincenzo Criteria	2
4.0	What Has Been Accomplished	4
4.1	Highlights of the accomplishments of the NMR approach.....	4
4.2	A long-term view	5
5.0	Considerations	7
6.0	Timeline	10
7.0	Glossary	10
8.0	References	11

List of Tables and Figures

Table 1-1	Nuclear Magnetic Resonance QC Research.....	1
Figure 6-1.	Nuclear magnetic resonance QC developmental timeline.....	10

List of Acronyms and Abbreviations

DFS	decoherence-free subspace	QIP	quantum information processing
GHZ	Greenberger, Horne, and Zeilinger	QIS	quantum information science
Hz	hertz	QFT	quantum Fourier transform
kHz	kilohertz	rf	radio frequency
NMR	nuclear magnetic resonance	TEP	Technology Experts Panel
QC	quantum computation/computing		

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Nuclear Magnetic Resonance (NMR) detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Nuclear Magnetic Resonance QC Research

Research Leader(s)	Research Location
Cory & Havel	MIT Nuclear Engineering
Gershenfeld & Chuang	MIT Media Lab
Glaser	Munich
Jones	Oxford
Kim	Korea
Kumar	Bangalore, India
Knill	Los Alamos
Laflamme	Waterloo
Zeng	China

2.0 Background and Perspective

More than 50 years ago Bloch, Purcell, and coworkers demonstrated the coherent control and detection of nuclear spins via NMR. Shortly thereafter, pulse techniques were developed (e.g., by Ramsey, Torrey, Hahn, and Waugh) to extend coherent control to multispin systems, and to permit the measurement of decoherence and dissipation rates. Since then, NMR technologies have advanced to permit applications ranging from medical imaging, materials science, molecular structure determination, and reaction kinetics (see the texts by Abragam [1], Slichter [2] and Ernst [3] for example).

The NMR approach to quantum information processing (QIP) capitalizes on the successes of this well-proven technology, in order to engineer a processor that fulfills the five requirements for a quantum computer as outlined by David DiVincenzo. Electron and nuclear spins turn out to be nearly ideal qubits which can be manipulated through well-developed radio-frequency (rf) irradiation. The natural interactions (chemical screening, dipolar, indirect, and hyperfine) provide the quantum communication links between these qubits and have been well characterized. The amplitude of noise and imperfections are small and understood enough to realize proof-of-principle demonstrations of this technology for applications to quantum information science (QIS).

By now, many algorithms and other benchmarks have been implemented on liquid-state NMR QIPs, bringing theoretical ideas into the laboratory and enabling the quantitative evaluation of lacks in precision and imperfections of methods for achieving quantum control. In addition, manufacturers have begun work on improving commercially available spectrometers so as to facilitate these and future implementations of QIP.

While liquid-state NMR is expected to remain the most convenient experimental testbed for theoretical QIP advances for some time to come, its limitations (low polarization, limited numbers of resolvable qubits) have been thoroughly documented [4,5,6,7,8]. Its success has, however, also suggested several complementary new routes toward scalable devices, and contributed greatly to the drawing of this roadmap. Most of the new routes lead immediately into the realm of solid-state magnetic resonance, bringing NMR into closer contact with many of the other approaches to QIP now being pursued.

In solid-state NMR, the manipulation of large numbers of spins has already been amply demonstrated [9,10], e.g., by creating correlated states involving 100 or more spins, and with sufficiently precise control to follow their dynamics. This has enabled the first quantitative studies of decoherence as a function of the Hamming weight of the coherence. Solid-state NMR further permits the engineering of larger QIP devices [11] than is possible in the liquid state, because

1. polarizations of order unity have been achieved,
2. the interactions are stronger and hence two-qubit gates are faster,
3. the decoherence times are much longer, and
4. it is possible to implement resettable registers.

In the longer term, investigations will be undertaken to achieve single-spin detection, using force detection, algorithmic amplification and / or optical hyperfine interactions. By integrating the control learned in the liquid state with the polarization and longer decoherence times of the solid state, along with the detection efficiency provided by optics, a firm foundation on which to design engineered, spin-based, and scalable QIP devices can be built. It is anticipated that this experience will be combined with the engineering developments of the spintronic and solid-state proposals, as well as the knowledge on pure-state dynamics from optics and ion traps to provide a complete solution to building a quantum computer. Preliminary proposals for scalable implementations based on solid-state NMR have been suggested and are starting to be explored experimentally [12,13].

3.0 Summary of NMR QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits  (overall)
 - 1.1 Chemically distinct nuclear spins in liquid state; chemically, spatially, or crystallographically distinct nuclear spins in the solid state.  (internal spin-dependent Hamiltonian is very well known)
 - 1.2 Scalability: liquid state is limited by chemistry and by low polarization. 
 - 1.3 Solid-state approaches based on spatially distributed spin ensembles as qubits have been proposed to be scalable. In the solid-state polarization near one is achievable via dynamic nuclear polarization. 
2. The ability to initialize the state of the qubits to a simple fiducial state 
 - 2.1 Pseudopure states in liquids
 - 2.2 Dynamic nuclear polarization in solids
 - 2.3 Optical nuclear polarization in solids
3. Long (relative) decoherence times, much longer than the gate-operation time 
 - 3.1 Liquid state: $T_1 \gg 1 \text{ sec}$, $T_2 \approx 1 \text{ sec}$, $J \approx 10\text{--}200 \text{ Hz}$;
 - 3.1.1 For spin-1/2 nuclei, noise generators and their approximate spectral distributions are known.
 - 3.2 Solid state: $T_1 \gg 1 \text{ min}$, $T_2 \gg 1 \text{ sec}$, $J \approx 100 \text{ Hz--}20 \text{ kHz}$;
 - 3.2.1 T_1 is typically limited by unpaired electrons in lattice defects
 - 3.2.2 T_2 is limited by all spin inhomogeneities (after refocussing of dephasing via dipolar couplings to like spins).
 - 3.3 The following means of controlling decoherence have been investigated:
 - 3.3.1 Quantum error correction;
 - 3.3.2 Decoherence-free subspaces (DFSs);
 - 3.3.3 Noiseless subsystems; and
 - 3.3.4 Geometric phase.
 - 3.4 Full-relaxation superoperators have been measured in a few cases.
4. A universal set of quantum gates 
 - 4.1 Single-qubit rotations depend on differences in chemical shifts.
 - 4.2 Multiple-qubit rotations rely on the bilinear coupling of spins (scalar or dipolar).
 - 4.3 Strongly modulated control sequences for up to four qubits have achieved experimental single-qubit gate fidelities $F > 0.98$.
 - 4.4 Full superoperator of complex control sequences have been measured in a few cases (including QFT [quantum Fourier transform] on three qubits).
 - 4.5 There are proposals for achieving fast gates through control of the hyperfine interaction modulated via optical cycling transitions (preliminary results have been obtained).
 - 4.6 Two encoded qubits have been created and controlled (for a simple collective noise model).

5. A qubit-specific measurement capability 
 - 5.1 Ensemble weak measurement, normally requiring $>10^{14}$ spins at room temperatures.
 - 5.2 Ensemble measurement permits controlled decoherence to attenuate off diagonal terms in a preferred basis.
 - 5.3 Optically detected NMR has demonstrated the detection of the presence of single spins and there are proposals for detecting the state of single spins (none yet realized).

Presently there are no schemes for using NMR as part of a communication protocol.

6. The ability to interconvert stationary and flying qubits: **none** 
7. The ability to faithfully transmit flying qubits between specified locations: **none** 

4.0 What Has Been Accomplished

The accomplishments described in this section will be presented as a direct listing of the major highlights and against the benchmarking outline used in the other roadmap documents.

4.1 Highlights of the accomplishments of the NMR approach

1. Precise coherent and decoherent control
 - 1.1 Geometric phase gates
 - 1.2 Strongly modulating pulses
 - 1.3 Gradient-diffusion-induced decoherence
 - 1.4 Precise control methods in the presence of incoherent interactions
2. Control of decoherence
 - 2.1 DFSs
 - 2.2 Noiseless subsystems
 - 2.3 Quantum error correction (independent errors)
 - 2.4 Quantum error correction (correlated errors)
 - 2.5 Active control (decoupling)
 - 2.6 Concatenation of quantum error correction and active control
 - 2.7 Quantum simulation with decoherence
3. Benchmarking
 - 3.1 Entanglement dynamics (Bell; Greenberger, Horne, & Zeilinger [GHZ]; and extensions to seven qubits)
 - 3.2 Quantum teleportation and entanglement transfer
 - 3.3 Quantum eraser and disentanglement eraser
 - 3.4 Quantum simulation (harmonic oscillator/ driven harmonic oscillator)
 - 3.5 QFT and baker's map
 - 3.6 State, process, and decoherence tomography

4. Algorithms
 - 4.1 Deutsch-Joza
 - 4.2 Grover's algorithm
 - 4.3 Shor's algorithm and quantum counting
 - 4.4 Approximate quantum cloning
 - 4.5 Hogg's algorithm
 - 4.6 Teleportation

4.2 A long-term view

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit

- 1.1 Demonstrate preparation and readout of both qubit states. 
 - 1.1.1 Observation of both states, predates QIP (see Abragam [1]).
 - 1.1.2 Pseudo-pure state preparation.
 - gradient-based spatial average [14] ($F \sim 0.99$ in reference [15])
 - temporal average [16] (no fidelities given in this paper)
 - effective [17], aka logically labeled [18] ($F \sim 0.95$), aka conditional
 - conditional spatial average [19,20] ($F \sim 0.95$)

2. Single-qubit operations

- 2.1 Demonstrate Rabi flops of a qubit. 
 - predates QIP (see Abragam [1])
- 2.2 Demonstrate decoherence times much longer than Rabi oscillation period. 
 - predates QIP (see Abragam [1])
- 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 
 - predates QIP (see Ernst [3])
- 2.4 Demonstrate precise qubit selective rotations. 
 - strong modulation methods [21] ($F > 0.98$ for one-qubit gates)
 - selective transition methods [22] (numbers given in this paper imply $F > 0.85$)
- 2.5 Demonstrate control robust to variations in the system Hamiltonian. 
 - composite pulses [23,24] (no fidelities given in these papers)
 - strong modulation [25] (one-qubit: $F > 0.995$; two-qubit $F > 0.986$)
- 2.6 Demonstrate control based on geometric phase [26] ($F \sim 0.98$). 

3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - early example showing spinor behavior [27] (no fidelities given)
 - C-NOT and swap gates [28,29,30] (no fidelities given in these papers)
 - conditional Berry's phase [26] (other numbers in this paper imply $F \sim 0.98$)
 - 3.2 Produce and characterize Bell states. 
 - pseudo-pure to Bell state [31 & papers in #3.4 below] (no fidelities given in [31])
Note: *While the pseudo-pure to Bell operation has high fidelity, the final state remains highly mixed.*
 - electron/nuclear spin Bell state [32] ($F \sim 0.99$)
 - in the solid state there is potential for creating nearly pure Bell states
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
 - predates QIP (see references [2,3])
 - use of dipolar couplings in a liquid crystal phase to increase gate speed [33]
 - 3.4 Two-qubit examples of algorithms. 
 - quantum counting [34] (no fidelities given)
 - Deutsch-Josza [35,36] (no fidelities given), [37] ($F \sim 0.99$)
 - Grover [38] (no fidelities given)
 - Hogg [39] (other numbers in this paper imply $F \sim 0.95$)
 - 3.5 Demonstration of 1 logical qubit DFS [40] ($F > 0.93$). 
 - 3.6 Demonstration of quantum error detection [41] (detailed error analysis but no clear overall fidelity given). 
4. Operations on 3–10 physical qubits
 - 4.1 Produce a GHZ-state of three physical qubits. 
 - pseudo-pure GHZ state [42,43] ($F \cong 0.95$); note this F only tracks the deviation part of the density mat—the system remains highly mixed
 - 4.2 Produce maximally entangled states of four and more physical qubits. 
 - 7-spin cat state [44] ($F \cong 0.73$); note this F only tracks the deviation part of the density matrix—the system remains highly mixed
 - 4.3 Quantum state and process tomography. 
 - state tomography [most papers cited herein] (errors estimated at 2%–5%)
 - quantum process tomography [45,46] (no rigorous error analysis available)
 - 4.4 Demonstrate decoherence-free subspace/system. 
 - one logical qubit subsystem for collective isotropic noise from three physical qubits [47] ($F \cong 0.70$ for encoding, application of noise, & decoding)
 - 4.5 Demonstrate the transfer of quantum information (e.g. teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 

- teleportation [48] ($F \sim 0.50$)
 - entanglement swap [49] ($F \approx 0.90$)
 - quantum erasers [50] ($F \sim 0.90$), [51] ($F \sim 0.75$)
- 4.6 Demonstrate quantum error correcting codes. 
- three-qubit code [52] ($F \sim 0.80$), [53] ($F \sim 0.98$), [15] ($F \approx 0.99$)
 - five-qubit code [54] ($F \approx 0.75$)
- 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) on three or more qubits. 
- quantum Fourier transform [55] ($F \approx 0.80$ w/o swap, 0.52 with)
 - Shor's algorithm [56] (no fidelities reported)
 - quantum baker's map [57] ($F \approx 0.76$ forward, 0.56 forward & back)
 - adiabatic quantum optimization algorithm [58] (fidelity not applicable)
- 4.8 Demonstrate quantum logic operations with fault-tolerant precision 
5. Operations on one logical qubit
- 5.1 Create a single logical qubit and "keep it alive" using repetitive error correction. 
- 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
6. Operations on two logical qubits
- 6.1 Implement two-logical-qubit operations [59]. 
- 6.2 Produce two-logical-qubit Bell states. 
- 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
- 6.4 Demonstrate simple quantum algorithms with two logical qubits. 
7. Operations on 3–10 logical qubits
- 7.1 Produce a GHZ-state of three logical qubits. 
- 7.2 Produce maximally entangled states of four and more logical qubits. 
- 7.3 Demonstrate the transfer of quantum information between logical qubits. 
- 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with 3 or more logical qubits. 
- 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

1. Strengths
- 1.1 Very well characterized experimental system with proven ability to achieve arbitrary unitary dynamics in Hilbert spaces of at least seven qubits.
 - 1.2 Stable and precise instrumentation, most of which is commercially available.
 - 1.3 Convenient means of implementing a wide variety of decoherence models.
 - 1.4 Solid-state implementations have demonstrated coherent control over larger Hilbert spaces (of order 100 spins), but so far without a convenient mapping to qubits.

2. Unknowns, weaknesses
 - 2.1 Unknowns
 - 2.1.1 Spectral densities of noise generators (liquid state); ultimate causes of decoherence (solid state).
 - 2.1.2 Limitations on the number of qubits tied to frequency addressing of qubits based on the internal Hamiltonian.
 - 2.1.3 Single-spin detection.
 - 2.2 Weaknesses
 - 2.2.1 Use of the internal Hamiltonian (chemistry) to define qubits is not scalable (presumed limits are about 10 qubits in liquids and somewhat larger in the solid state).
 - 2.2.2 Clock speed, when using the internal Hamiltonian for gates, is extremely slow (< 1 kHz in liquid state and somewhat larger in solids).
 - 2.2.3 Liquid-state polarization is very low ($\sim 10^{-5}$), meaning all states are highly mixed and thus do not have unique microscopic interpretation.
 - 2.2.4 In the solid state, polarization > 0.9 has been achieved, which is sufficient for Schumacher compression—if sufficient control is available.
 - 2.2.5 Single-spin detection and/or control has not been achieved (at least $\sim 10^6$ nuclear spins are needed).
 - 2.2.6 There are a variety of single-spin proposals for the solid state, although this is an old problem that has been attacked for many years. I am not aware of any proposals for detecting single spins in the liquid state.
3. Goals 2002–2007
 - 3.1 Process tomography for gates, algorithms, and decoherence.
 - 3.2 Metrics for control, especially in large Hilbert spaces.
 - 3.3 Approach fault-tolerant threshold for single-gate errors.
 - 3.4 Demonstrate fault-tolerant gates on encoded qubits and decoherence-free subsystems.
 - 3.5 Obtain high polarization in the solid state for a system that can be conveniently mapped to qubits.
 - 3.6 Perform simple computations and prove attainment of quantum entanglement at high polarizations in the solid state.
 - 3.7 Combine quantum error correction with subsystem encoding.
 - 3.8 Explore quantum error-correction codes to second order.
 - 3.9 Prepare Bell states of two logical qubits.
4. Goals 2007–2012
 - 4.1 Transfer knowledge and experience for the liquid-state control techniques to solid-state and further improve the precision.
 - 4.2 Achieve single-nuclear-spin detection, measurement, and control (or know why it cannot be achieved).

- 4.3 Implement and control >10 qubits in the solid state.
- 4.4 Create a GHZ state of three logical qubits.
- 4.5 Quantify the fidelity of entanglement transfer between logical qubits.
- 4.7 Develop optical means of coherently controlling the hyperfine interaction.
- 4.8 Explore spintronics (i.e., interfaces to electronic degrees of freedom).
5. Necessary achievements
 - 5.1 Learn to spatially address single spins (cf. 4.2), or
 - 5.2 Learn to create coherences among polarized spin ensembles.
6. Trophies
 - 6.1 Shor's algorithm [56]
 - 6.2 Bell's inequality violation in a true pure state
7. Connections to other technologies
 - 7.1 Methods and metrics of control developed for NMR will transfer to many other technologies.
 - 7.2 Understanding decoherence and the control of decoherence is fundamental to the entire field of QIP.
8. Subsidiary developments
 - 8.1
9. Role of theory
 - 9.1 Allows simulation of experiments on small systems (Hamiltonians are known with high precision).
 - 9.2 Complex theoretical models may be needed to describe real decoherence mechanisms.
 - 9.3 Achieving and benchmarking control in Hilbert spaces too large to simulate classically; it will require new theoretical techniques.
 - 9.4 Methods of control (trajectory planning, holonomic control, error correction, and decoherence-free subsystems) require sophisticated mathematics.
 - 9.5 New concepts are needed to understand complex dynamics.

6.0 Timeline



Figure 6-1. Nuclear magnetic resonance QC developmental timeline

7.0 Glossary

Correlation

Cosine of the angle between two states.

Fidelity

Magnitude of the projection of one state on another.

Physical qubit

A system that has observables that behave as the Pauli matrices.

Logical qubit

A combination of physical qubits that is more robust against a specific set of noise generators.

8.0 References

- [1] Abragam A., *The Principles of Nuclear Magnetism* (Clarendon Press, Oxford, 1961).
- [2] Slichter C.P., *Principles of Magnetic Resonance* (Springer-Verlag, New York, 1980).
- [3] Ernst, R.R., G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1987).
- [4] Cory, D.G., A.F. Fahmy and T.F. Havel, "Ensemble quantum computing by NMR spectroscopy," *Proceedings of the National Academy of Science (USA)* **94**, 1634–1639 (1997).
- [5] Warren, W.S., "The Usefulness of NMR Quantum Computing," *Science* **277**, 1688–1690 (1997); see also response by N. Gershenfeld & I.L. Chuang, *ibid*, p. 1688.
- [6] Braunstein, S.L., C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, "Separability of very noisy mixed states and implications for NMR quantum computing," *Physical Review Letters* **83**, 1054–1057 (1999).
- [7] Havel, T.F., S.S. Somaroo, C.-H. Tseng, and D.G. Cory, "Principles and demonstrations of quantum information processing by NMR spectroscopy," *Applicable Algebra in Engineering, Communication, and Computing* **10**, 339–374 (2000).
- [8] Laflamme, R., D.G. Cory, C. Negrevergne, and L. Viola, "NMR quantum information processing and entanglement," *Quantum Information and Computation* **2**, 166–176 (2002).
- [9] Warren, W.S., D.P. Weitekamp, and A. Pines, "Theory of selective excitation of multiple-quantum transitions," *Journal of Chemical Physics* **73**, 2084–2099 (1980).
- [10] Ramanathan, C., H. Cho, P. Cappellaro, G.S. Boutis, and D.G. Cory, "Encoding multiple quantum coherences in non-commuting bases," *Chemical Physics Letters* **369**, 311–317 (2003).
- [11] Cory, D.G., R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemarian, Y.S. Weinstein, and Z.H. Zurek, "NMR based quantum information processing: Achievements and prospects," *Fortschritte der Physik [Progress of Physics]* **48**, 875–907 (2000).
- [12] Abe, E., K.M. Itoh, T.D. Ladd, J.R. Goldman, F. Yamaguchi, and Y. Yamamoto, "Solid-state silicon NMR quantum computer," *Journal of Superconductivity: Incorporating Novel Magnetism* **16**, 175–178 (2003).
- [13] Suter, D. and K. Lim, "Scalable architecture for spin-based quantum computers with a single type of gate," *Physical Review A* **65**, 052309 (2002).
- [14] Cory, D.G., M.D. Price, and T.F. Havel, "Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing," *Physica D* **120**, 82–101 (1998).

- [15] Boulant, N., M.A. Pravia, E.M. Fortunato, T.F. Havel, and D.G. Cory, "Experimental concatenation of quantum error correction with decoupling," *Quantum Information Processing* **1**, 135–144 (2002).
- [16] Knill, E., I.L. Chuang, and R. Laflamme, "Effective pure states for bulk quantum computation," *Physical Review A* **57**, 3348–3363 (1998).
- [17] Gershenfeld, N. and I.L. Chuang, "Bulk spin-resonance quantum computation," *Science* **275**, 350–356 (1997).
- [18] Vandersypen, L.M.K., C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "Realization of logically labeled effective pure states for bulk quantum computation," *Physical Review Letters* **83**, 3085–3088 (1999).
- [19] Sharf, Y., T.F. Havel, and D.G. Cory, "Spatially encoded pseudopure states for NMR quantum-information processing," *Physical Review A* **62**, 052314 (2000).
- [20] Mahesh, T.S. and A. Kumar, "Ensemble quantum-information processing by NMR: Spatially averaged logical labeling technique for creating pseudopure states," *Physical Review A* **64**, 012307 (2001).
- [21] Fortunato, E.M., M.A. Pravia, N. Boulant, G. Teklemariam, T.F. Havel, and D.G. Cory, "Design of strongly modulating pulses to implement precise effective Hamiltonians for quantum information processing," *Journal of Chemical Physics* **116**, 7599–7606 (2002).
- [22] Das, R., T.S. Mahesh, and A. Kumar, "Implementation of conditional phase-shift gate for quantum information processing by NMR, using transition-selective pulses," *Journal of Magnetic Resonance* **159**, 46–54 (2002).
- [23] Levitt, M.H., "Composite pulses," *Progress in NMR Spectroscopy* **18**, 61–122 (1986).
- [24] Cummins, H.K., G. Llewellyn, and J.A. Jones, "Tackling systematic errors in quantum logic gates with composite rotations," *Physical Review A* **67**, 042308 (2003).
- [25] Pravia, M.A., N. Boulant, J. Emerson, A. Farid, E.M. Fortunato, T.F. Havel, R. Martinez, and D.G. Cory, "Robust control of quantum information," *Journal of Chemical Physics* **119**, 9993–10001 (2003).
- [26] Jones, J.A., V. Vedral, A. Ekert, and G. Castagnoli, "Geometric quantum computation using nuclear magnetic resonance," *Nature* **403**, 869–871 (2000).
- [27] Stoff, M.E., A.J. Vega, and R.W. Vaughan, "Explicit demonstration of spinor character for a spin-1/2 nucleus via NMR interferometry," *Physical Review A* **16**, 1521–1524 (1977).
- [28] Price, M.D., S.S. Somaroo, C.H. Tseng, J.C. Gore, A.F. Fahmy, T.F. Havel, and D.G. Cory, "Construction and implementation of NMR quantum logic gates for two spin systems," *Journal of Magnetic Resonance* **140**, 371–378 (1999).

- [29] Linden, N., H. Barjat, R. Kupic, and R. Freeman, "How to exchange information between two coupled nuclear spins: the universal SWAP operation," *Chemical Physics Letters* **307**, 198–204 (1999).
- [30] Madi, Z.L., R. Brüschweiler, and R.R. Ernst, "One- and two-dimensional ensemble quantum computing in spin Liouville space," *Journal of Chemical Physics* **109**, 10603–10611 (1998).
- [31] Pravia, M.A., E.M. Fortunato, Y. Weinstein, M.D. Price, G. Teklemariam, R.J. Nelson, Y. Sharf, S.S. Somaroo, C.-H. Tseng, T.F. Havel, and D.G. Cory, "Observations of quantum dynamics by solution-state NMR spectroscopy," *Concepts in Magnetic Resonance* **11**, 225–238 (1999).
- [32] Mehring, M., J. Mende, and W. Scherer, "Entanglement between an electron and a nuclear spin $1/2$," *Physical Review Letters* **90**, 153001 (2003).
- [33] Yannoni, C.S., M.H. Sherwood, D.C. Miller, I.L. Chuang, L.M.K. Vandersypen, and M.G. Kubanic, "Nuclear magnetic resonance quantum computing using liquid crystal solvents," *Applied Physics Letters* **75**, 3563–3565 (1999).
- [34] Jones, J.A. and M. Mosca, "Approximate quantum counting on an NMR ensemble quantum computer," *Physical Review Letters*, **83**, 1050–1053 (1999).
- [35] Jones, J.A. and M. Mosca, "Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer," *Journal of Chemical Physics* **109**, 1648–1653 (1998).
- [36] K. Dorai, Arvind, and A. Kumar, "Implementation of a Deutsch-like quantum algorithm utilizing entanglement at the two-qubit level on an NMR quantum-information processor," *Physical Review A* **63**, 034101 (2001).
- [37] Chuang, I.L., L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd, "Experimental realization of a quantum algorithm," *Nature* **393**, 143–146 (1998).
- [38] Jones, J.A., M. Mosca, and R.H. Hansen, "Implementation of a quantum search algorithm on a quantum computer," *Nature* **393**, 344–346 (1998).
- [39] Zhu, X.W., X.M. Fang, M. Feng, F. Du, K.L. Gao, and X. Mao, "Experimental realization of a highly structured search algorithm," *Physica D* **156**, 179–185 (2001).
- [40] Fortunato, E.M., L. Viola, J. Hodges, G. Teklemariam, and D.G. Cory, "Implementation of universal control on a decoherence-free qubit," *New Journal of Physics* **4**, 5.1–5.20 (2002).
- [41] Leung, D., L.M.K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I.L. Chuang, "Experimental realization of a two-bit phase damping quantum code," *Physical Review A* **60**, 1924–1943 (1999).
- [42] Laflamme, R., E. Knill, W.H. Zurek, P. Catasti, and S.V.S. Mariappan, "NMR Greenberger-Horne-Zeilinger states," *The Royal Society Philosophical Transactions: Mathematical, Physical, and Engineering Sciences* **356**, 1941–1948 (1998).

- [43] Nelson, R.J., D.G. Cory, and S. Lloyd, "Experimental demonstration of Greenberger-Horne-Zeilinger correlations using nuclear magnetic resonance," *Physical Review A* **61**, 022106 (2000).
- [44] Knill, E., R. Laflamme, R. Martinez, and C.-H. Tseng, "An algorithmic benchmark for quantum information processing," *Nature* **404**, 368–370 (2000).
- [45] Childs, A.M., I.L. Chuang, and D.W. Leung, "Realization of quantum process tomography in NMR," *Physical Review A* **64**, 012314 (2001).
- [46] Boulant, N., T.F. Havel, M.A. Pravia, and D.G. Cory, "Robust method for estimating the Lindblad operators of a dissipative quantum process from measurements of the density operator at multiple time points," *Physical Review A* **67**, 042322 (2003).
- [47] Viola, L., E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, and D.G. Cory, "Experimental realization of noiseless subsystems for quantum information processing," *Science* **293**, 2059–2063 (2001).
- [48] Nielsen, M.A., E. Knill, and R. Laflamme, "Complete quantum teleportation using nuclear magnetic resonance," *Nature* **396**, 52–55 (1998).
- [49] Boulant, N., K. Edmonds, J. Yang, M.A. Pravia, and D.G. Cory, "Experimental demonstration of an entanglement swapping operation and improved control in NMR quantum-information processing," *Physical Review A* **68**, 032305 (2003).
- [50] Teklemariam, G., E.M. Fortunato, M.A. Pravia, T.F. Havel, and D.G. Cory, "NMR analog of the quantum disentanglement eraser," *Physical Review Letters* **86**, 5845–5849 (2001).
- [51] Teklemariam, G., E.M. Fortunato, M.A. Pravia, Y. Sharf, T.F. Havel, D.G. Cory, A. Bhattacharyya, and J. Hou, "Quantum erasers and probing classifications of entanglement via nuclear magnetic resonance," *Physical Review A* **66**, 012309 (2002).
- [52] Cory, D.G., M. Price, W. Maas, E. Knill, R. Laflamme, W.H. Zurek, T.F. Havel, and S.S. Somaroo, "Experimental quantum error correction," *Physical Review Letters* **81**, 2152–2155 (1998).
- [53] Sharf, Y., D.G. Cory, S.S. Somaroo, T.F. Havel, E. Knill, R. Laflamme and W.H. Zurek, "A study of quantum error correction by geometric algebra and liquid-state NMR spectroscopy," *Molecular Physics* **98**, 1347–1363 (2000).
- [54] Knill, E., R. Laflamme, R. Martinez, and C. Negreverne, "Benchmarking quantum computers: The five-qubit error correcting code," *Physical Review Letters* **86**, 5811–5814 (2001).
- [55] Weinstein, Y.S., M.A. Pravia, E.M. Fortunato, S. Lloyd, and D.G. Cory, "Implementation of the Quantum Fourier Transform," *Physical Review Letters* **86**, 1889–1891 (2001).

- [56] Vandersypen, L.M.K., M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature* **414**, 883–887 (2001).
- [57] Weinstein, Y.S., S. Lloyd, J. Emerson, and D.G. Cory, "Experimental implementation of the quantum Baker's map," *Physical Review Letters* **89**, 157902 (2002).
- [58] Steffen, M., W. van Dam, T. Hogg, G. Breyta, and I.L. Chuang, "Experimental implementation of an adiabatic quantum optimization algorithm," *Physical Review Letters* **90**, 067903 (2003).
- [59] Ollerenshaw, J.E., D.A. Lidar, and L.E. Kay, "Magnetic resonance realization of decoherence-free quantum computation," *Physical Review Letters* **91**, 217904 (2003).

Ion Trap Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.2

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: David Wineland

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0 Groups Pursuing This Approach	1
2.0 Background and Perspective	1
3.0 Summary of Trapped-Ion QC: The DiVincenzo Criteria	2
4.0 What Has Been Accomplished	5
5.0 Considerations	7
6.0 Timeline	11
7.0 Glossary	12
8.0 References	12

List of Tables and Figures

Table 1-1 Approaches to Ion Trap QC Research	1
Figure 6-1. Ion trap QC developmental timeline	12

List of Acronyms and Abbreviations

C-NOT	controlled-NOT (gate)	QIP	quantum information processing
DAC	digital to analog converter	rf	radio frequency
DFS	decoherence-free subspace	SPD	single-photon detector
GHZ	Greenberger, Horne, and Zeilinger	SPS	single-photon source
MEMS	micro-electro-mechanical systems	TEP	Technology Experts Panel
QC	quantum computation/computing	UV	ultraviolet
QED	quantum electrodynamics		

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Ion Trap detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Approaches to Ion Trap QC Research

Research Leader(s)	Research Location	Research Focus
Berkeland, D.	Los Alamos National Laboratory	Sr ⁺
Blatt, R.	Innsbruck	Ca ⁺
Devoe, R.	Almaden (IBM)	Ba ⁺
Drewsen, M.	Aarhus	Ca ⁺
Gill, P.	National Physical Lab (NPL), Teddington, UK	Sr ⁺
King, B.	McMaster U., Hamilton, Ontario	Mg ⁺
Monroe, C.	U. of Michigan	Cd ⁺
Steane, A.	Oxford	Ca ⁺
Wunderlich, C.	Hamburg	Yb ⁺
Walther, H.	Max-Planck Institute, Garching	Mg ⁺ , In ⁺
Wineland, D.	NIST, Boulder	⁹ Be ⁺ , Mg ⁺

2.0 Background and Perspective

Schemes for ion-trap quantum-information processing (QIP) are derived from the basic ideas put forth by Cirac and Zoller[1]. These schemes satisfy all of the DiVincenzo criteria and most of the criteria have been experimentally demonstrated.

Scalability can be achieved by use of ion-trap arrays that are interconnected with

1. photons[2,3,4,5];
2. a movable “head” ion that transfers information between ions in separate traps[6]; or
3. by moving ions between trap nodes in the array[7,8].

Ion qubits can now be moved between nodes in a multiple-zone trap without decoherence in a time approximately equal to the gate time[9]. Efficient separation of ion qubits for transport to separate nodes will require smaller traps with good electrode surface integrity. This can likely be accomplished with the use of existing micro-electro-mechanical systems (MEMS) or nanofabrication technology. Multiplexing can also be accomplished with optical interconnects; efforts are currently underway at Garching[10] and Innsbruck[11] to develop efficient cavity-quantum electrodynamic (QED) schemes for information transfer between ions and photons.

3.0 Summary of Trapped-Ion QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits 
 - 1.1 “Spin” qubit levels are typically chosen to be (1) two hyperfine or Zeeman sublevels in the electronic ground state of an ion or (2) a ground and excited state of weakly allowed optical transition (e.g., Innsbruck Ca^+ experiment).
 - 1.1.1 *Motional-state quantum bus:* Direct interactions between ion qubits are extremely weak because of the relatively large ($>1 \mu\text{m}$) spacing between ions, which is determined by a balance between the trap potential and Coulomb repulsion between ions. Therefore, quantum information is typically mapped through the motional state to transmit information between qubits [1].
 - 1.2 Scalability
 - 1.2.1 Scaling to large qubit numbers can be achieved by using arrays of interconnected ion traps.
 - 1.2.1.1 *Photon interconnections:* Cavity-QED techniques [2–4] can be employed to transfer quantum superpositions from a qubit in one trap to a second ion in another trap via optical means.
 - 1.2.1.2 *Moving-ion qubits:* Ion qubits can be moved from one trap to another by application of time-varying potentials to “control” electrodes [7] or by employing a moveable “head” ion [6].
2. Ability to initialize the state of the qubits to a simple fiducial state 
 - 2.1 Spin qubits can be prepared in one of the eigenstates with high probability by using standard optical-pumping techniques (since ~ 1950).
 - 2.2 Motional state preparation can be accomplished by laser cooling to the ground state of motion (since ~ 1989).
 - 2.2.1 For certain classes of gates, we require only the Lamb-Dicke limit (motional wave packet extent $\ll \lambda/2$, where λ is the relevant optical wavelength). Therefore, ground-state cooling is not strictly required. In the 2000 Cirac and Zoller proposal [6], ion confinement can be well outside of Lamb-Dicke limit (see #4 below).
 - 2.2.2 Sympathetic cooling, in the context of quantum computation (QC), has been demonstrated.
 - 2.2.2.1 Cooling of like species (Ca^+) [12].
 - 2.2.2.2 Cooling of different isotopes of Cd^+ [13].

2.2.2.3 Cooling of ${}^9\text{Be}^+$ with Mg^+ (and vice-versa) [14].

3. Long (relative) decoherence times, much longer than the gate-operation time 
 - 3.1 Spin-state coherence
 - 3.1.1 Spin qubit memory:
 - 3.1.1.1 Qubit decay times (T_1 , T_2) for hyperfine levels can be extremely long (>10 min observed [15]) compared to typical gate times (<10 ns). This requires use of first-order magnetic-field “independent” transitions; that is, use of an ambient magnetic field where the spin qubit energy separation goes through an extremum with respect to magnetic field. Natural decay times of hyperfine transitions is typically >1 year.
 - 3.1.1.2 Weakly allowed optical transitions can have lifetimes of ~ 1 s (e.g., Ca^+), substantially longer than gate times.
 - 3.1.2 Spin qubit coherence during operations:
 - 3.1.2.1 Laser intensity and phase fluctuations and spontaneous emission will cause decoherence and must therefore be suppressed.
 - 3.2 Motional-state coherence
 - 3.2.1 Coherence between motional states is currently limited by heating due to stochastically fluctuating electric fields at the position of the ion. Observed single-quantum excitation times typically lie between 100 ns and 100 ms. This heating has so far exceeded that expected from thermal radiation and appears to be related to electrode surface integrity [9].
4. Universal set of quantum gates 
 - 4.1 Single-bit rotations:
 - 4.1.1 Fidelity of single-bit rotations is not fundamentally limited by internal-state qubit decoherence from spontaneous emission. Certain ions can satisfy fault-tolerant levels (see 5.2.3).
 - 4.2 Cirac and Zoller 2-qubit controlled-NOT (C-NOT) gate (1995 [1]): A selected mode of motion is cooled to the ground state and the ground and first excited state of this mode are used as a “bus-qubit.” The spin qubit state of an ion can be mapped onto the bus qubit with the use of laser beams focused onto that ion. A gate operation can then be performed between the motional qubit and a second selected ion thereby effectively performing a gate between the first and second ion.
 - 4.3 Cirac and Zoller 2-qubit “push” gate (2000, [6]): Information can be transferred and gates implemented between ions located in an array of traps with a movable “head” ion. This scheme has advantages over the 1995 version [1]:
 - a. Ions do not have to be cooled to a definite state or satisfy the Lamb-Dicke criterion. The motional spread of ions need only be negligible compared to their separation.
 - b. All ions are separately localized. Therefore, they need not be separated during a computation (as in references [7] and [9]), and individual spin-qubit addressing is easier.

- c. In principle, gate speeds need not be limited by motional frequencies. Higher-intensity stability is required for this gate.

4.4 Mølmer and Sørensen 2-qubit gate [16] gate:
$$\frac{|I,J\rangle \pm (|I,J\rangle + i|I \oplus 1, J \oplus 1\rangle)}{\sqrt{2}[I,J \pm (0,1)]}$$

A logic gate can be performed using two (different-frequency) excitation fields—neither of which causes a resonant transition but in combination they cause a coherent two-qubit transition. In comparison to the 1995 Cirac and Zoller gate [1], this gate has the technical advantages that

- it is a one step process,
- an auxiliary internal state is not needed
- individual-ion laser addressing is not needed during the gate (both ions are equally illuminated),
- it does not require motional eigenstates if ions are confined to the Lamb-Dicke limit, and
- the same logic gate can be applied in the (phase) decoherence-free subspace (DFS) using the same physical interaction [7,17].

capability 

5.1 State-sensitive laser light scattering can be used to distinguish spin-state qubit levels with nearly unit efficiency (“quantum jump” detection) [18]. Here, one of the qubit levels is driven with light having a polarization such that when it scatters a photon, by radiation selection rules, the ion must decay back in the same qubit level. The other qubit level is detuned from the laser light so that photon scattering is nearly absent. Therefore, if the ion is found in the first level, the photon scattering can be repeated many times so that, even if only a small fraction of the scattered photons are collected and detected, the “bright” state can be seen with very high (>0.9999) probability.

6. The ability to interconvert stationary and flying qubits 

6.1 The basic ideas are laid out in references [2–4]. This overlaps strongly with cavity-QED and the key ideas and experiments are expected to come from that area.

7. The ability to faithfully transmit flying qubits between specified locations 

7.1 In principle, qubits transferred between nodes in a multiplexed trap qualify as flying qubits if the transfer distances are small (<1 μm). This is not relevant for practical quantum communication but can be employed to spread quantum information in a quantum processor as outlined in 1.2.1.2 above.

4.0 What Has Been Accomplished

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states. 
 - 1.1.1 Single trapped ions were first observed in 1980 [19]. The ability to distinguish between two spin states with high efficiency was first demonstrated in 1986 [18,20,21,22].
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.1.1 Rabi flops on ensembles of ions and neutral atoms have been observed for decades. Rabi flops on single ions in the context of QC have been observed since 1996 ($\tau_{\text{hop}} \approx 0.5 \mu\text{s}$).
 - 2.1.2 Selective single-spin qubit operations on chain of ions have been demonstrated [23].
 - 2.2 Demonstrate high-Q of qubit transition. 
 - 2.2.1 The highest observed Q-factor for a microwave transition (suitable for a qubit) is 1.5×10^{13} [15].
 - 2.2.2 The highest observed Q-factor for an optical transition (suitable for a qubit) is 1.6×10^{14} . Rabi flops have been observed with a laser having line width less than 1 Hz. [24]
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere 
 - 2.3.1 "Theta" pulses on Bloch sphere are controlled by controlling duration of Rabi flopping pulse time.
 - 2.3.2 "Phi" pulses can be synthesized from theta pulses with phase shifts inserted between pulses, changing the spatial phase of the ion relative to the laser beams, or in software by shifting phase of oscillator in subsequent operations.
3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - 3.1.1 Coherent Rabi flopping between spin and motional qubits has been demonstrated for hyperfine qubits [25] and optical-state qubits ($\tau_{\text{exchange}} \approx 10 \mu\text{s}$) [26].
 - 3.1.2 A C-NOT gate between motional and spin qubits using Cirac and Zoller scheme [1] was demonstrated in 1995 [27].

- 3.1.3 A two-spin qubit gate proposed by Mølmer and Sørensen was demonstrated in 2000 (gate time $\sim 20 \mu\text{s}$) [28].
- 3.1.4 A simplified C-NOT gate between motional and spin qubits [29] was demonstrated in 2002 [30] (gate time $\sim 20 \mu\text{s}$).
- 3.1.5 Experiments are underway which show coupling of spin qubits to photons at the single-photon level [10,11].
- 3.1.6 Implementing the Deutsch-Jozsa algorithm on an ion-trap quantum computer [31] (new gate demonstrated as part of this).
- 3.1.7 Realization of the Cirac-Zoller controlled-NOT quantum gate [32].
- 3.1.8 A robust, high-fidelity geometric two-ion qubit phase gate was experimentally demonstrated [33].
- 3.1.9 Quantized phase shifts and a dispersive universal quantum gate [34].
- 3.2 Produce and characterize Bell states. 
 - 3.2.1 Violations of Bell's inequalities were established for two entangled ions (same operations as those needed to produce and characterize Bell states) [35].
 - 3.2.2 Fidelity of Bell states produced was 0.71 [36] and 0.97 [33].
 - 3.2.3 Tomography of entangled massive particles using trapped ions [36].
 - 3.2.4 Demonstration of entangled Bell states between atoms and photons [37].
- 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
 - 3.3.1 Qubit memory coherence times can be much longer than gate times but coherence during gate operations limited by spontaneous emission and laser fluctuations (see DiVincenzo criteria, #3.1 above and #s 2.3 and 2.4 of "Considerations" below).
- 3.4 Demonstrate quantum state and process tomography for two qubits. 
 - 3.4.1 The motional quantum state of a trapped atom was experimentally determined [38,39].
 - 3.4.2 Tomography of entangled massive particles demonstrated with ions [36].
- 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS). 
- 3.6 Demonstrate a two-qubit quantum algorithm. 
 - 3.6.1 The entanglement-enhanced rotation angle estimation using trapped ions was experimentally demonstrated [40].
 - 3.6.2 Simulation of nonlinear interferometers [41].
 - 3.6.3 A technique to generate arbitrary quantum superposition states of a harmonically bound spin-1/2 particle was experimentally demonstrated [42].
 - 3.6.4 Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer [31].
- 4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, & Zeilinger (GHZ)-state of three physical qubits. 
 - 4.2 Produce maximally-entangled states of four and more physical qubits. 

- 4.2.1 A four-spin maximally entangled state has been experimentally produced [28].
- 4.3 Quantum state and process tomography. 
- 4.4 Demonstrate DFSs. 
- 4.4.1 (Phase) DFS for logical spin qubit has been demonstrated [28].
- 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations etc.) between physical qubits. 
- 4.6 Demonstrate quantum error-correcting codes. 
- 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
- 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
- 5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
- 6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
- 7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally-entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

- 1. Special strengths
 - 1.1 The long coherence times of spin qubits based on trapped ions imply a robust quantum memory.
 - 1.2 High-efficiency state preparation and detection can be readily implemented (need readout efficiency per qubit $\geq \exp(-1/N)$ for an N-bit processor without error correction or at the level of the noise threshold with error correction).
 - 1.3 Methods to achieve large-scale devices have been outlined.
- 2. Unknowns, weaknesses
 - 2.1 Motional decoherence caused by stochastically fluctuating electric fields must be reduced. The source of the fields is not known but appears to be due to trap electrode surface integrity [9]; efforts are underway to improve the trap electrode surfaces.
 - 2.2 Multiplexing in trap arrays is not yet operational.

- 2.3 Spontaneous emission[43]:
 - 2.3.1 for Raman transitions, we want large fine-structure splitting to avoid decoherence caused by spontaneous emission (e.g., Sr⁺[24 THz], Cd⁺[74 THz], and Hg⁺[274 THz])[44].
 - 2.3.2 for optical qubit transitions, we want upper-state lifetime to be $\geq 1 \mu$ s (e.g., Sr⁺, Ca⁺)
- 2.4 Laser noise
 - 2.4.1 Laser intensity and phase fluctuations can be suppressed efficiently at the site of detection. However, controlling the intensity at the position of the ion qubits is more difficult and needs to be improved.
- 3. Goals: present–2007
 - 3.1 Improve coherence.
 - 3.1.1 Identify and reduce sources of motional heating. If the motional heating can be reduced sufficiently, this will allow the use of smaller traps thereby increasing gate speed and facilitating ion separation in multiplexed trap scheme.
 - 3.1.1.1 Study different electrode surfaces (e.g., Boron-doped silicon, metallic alloys).
 - 3.1.1.2 Implement *in-situ* electrode cleaning (e.g., sputtering).
 - 3.1.2 Implement logic with “field-independent” spin qubit transitions.
 - 3.2 Multiplex ion traps.
 - 3.2.1 Build trap arrays with “Xs” and “Ts” to facilitate arbitrary qubit positioning [7].
 - 3.2.2 Moving ions between traps [7]:
 - 3.2.2.1 We must parcel out ions located in one trap and deliver to multiple selected traps with minimal heating.
 - 3.2.2.2 Ions must be efficiently re-cooled (preferably to the ground state) using sympathetic cooling.
 - 3.2.3 In the scheme to couple traps with photons [2–4], efficient spin-qubit/ photon coupling must be demonstrated.
 - 3.2.4 Generate entanglement between traps using probabilistic means [5].
 - 3.3 Improve laser stability to reach fault-tolerance limits.
 - 3.3.1 For Raman transitions and single photon optical transitions, this implies controlling the intensity and phase at the site of ions, which is a function of laser power and beam position stability.
 - 3.4 Spin-qubit/ photon coupling
 - 3.4.1 Demonstrate a high-efficiency single-photon source (SPS).
 - 3.4.2 Demonstrate coherent transfer of a qubit between a spin and photon state. This may require a miniature optical cavity (under 100 microns) surrounding the ion trap. This implies either special mirror coatings that are low-loss dielectrics

in the ultraviolet (UV) domain and conductive at microwave/ rf frequencies or the operation of ion traps that are smaller than the cavity (see #s 3.1.1 and 2.1 above).

- 3.5 Perform algorithms that avoid post selection and pseudoentanglement [45].
 - 3.5.1 Perform repetitive error correction on a single logical qubit “keeping a logical qubit alive.”
 - 3.5.1.1 A first experiment could be aimed at correcting only phase decoherence or bit-flip errors.
 - 3.5.1.2 A second experiment would be aimed at correcting both phase and bit-flip errors.
 - 3.5.2 Dense coding
 - 3.5.3 Teleportation
 - 3.5.4 Entanglement-enhanced communication (e.g., Steane’s “guess my number” [46])
4. Goals 2007–2012
 - 4.1 Operations on logical qubits
 - 4.1.1 Demonstrate single-bit rotations.
 - 4.1.2 Demonstrate gates between logical qubits.
 - 4.2 Spin-qubit/ photon coupling
 - 4.2.1 Demonstrate high-efficiency of coherent exchange between spin qubits mediated by photons.
 - 4.3 Development of integrated optics.
 - 4.3.1 Direct laser light and collect fluorescence using micro-optics that is integrated with the trap structure.
 - 4.4 Assess feasibility of constructing useful large-scale device
 - 4.4.1 Perform fault-tolerant algorithms on multiple qubits.
 - 4.4.2 From the performance of a multiple-node trap array, give an accurate assessment of scaling to arbitrary size.
5. Necessary achievements
 - 5.1 Goals: present–2007
 - 5.1.1 Generic causes and/or generic cures for reduction of stochastic electric field noise must be found. If the noise is, in fact, related to electrode surface integrity and cleanliness, it may not be necessary to know the exact make up of the contaminants that cause the problem, but we must be able to reliably produce “clean” electrodes.
 - 5.1.2 Ion separation and transfer between trap nodes in multiplexer must be reliably accomplished.
 - 5.1.2.1 It is expected that sympathetic recooling will be required.

- 5.1.2.2 Transfer and recoiling time must be accomplished in on-the-order-of the logic-gate time.
- 5.2 Goals 2007–2012
 - 5.2.1 “The” ion must be identified. For example, spontaneous emission dictates that it won’t be an ion with a small fine-structure splitting such as ${}^9\text{Be}^+$, although ${}^9\text{Be}^+$ can be used for many test experiments and as a possible cooling ion for sympathetic cooling [44].
 - 5.2.2 Single-bit rotation errors must be further reduced. To reach fault tolerant levels, laser intensity and phase must be stabilized further (power stabilization plus laser-beam position stabilization).
 - 5.2.3 Integrated optics. In contrast to table-top experimental-optics setups currently used, micro-optics integrated with the trap structures must be employed. A lead can be taken from current-neutral atom-manipulation experiments [47] where microlenses, etc. are beginning to be employed.
- 6. Trophies
 - 6.1 Repetitive error correction
 - 6.2 Demonstrate teleportation of matter states between separate traps (without post selection).
 - 6.3 Morph a qubit from atomic spin to a traveling photon.
- 7. Connections with other quantum information science technologies
 - 7.1 Motional decoherence caused by stochastic electric field noise may be related to charge/voltage fluctuations in superconducting qubits or surface-state fluctuations. Materials research is needed to reduce this source of decoherence. Low-noise, high-speed DACS will be required in both implementations.
 - 7.2 The construction of smaller traps may require MEMS or related nanofabrication technology.
 - 7.3 Integrated optics will be required for any large-scale processor; this requirement may benefit from any other quantum information technology that employs optics.
 - 7.4 Proposed spin-photon conversion will track advances in cavity-QED and high-finesse optical cavity technology, as optical coating technology gets better and more reliable in the UV and blue region of the spectrum.
- 8. Subsidiary developments
 - 8.1 Quantum measurement
 - 8.1.1 Entanglement methods from a quantum computer can be used to improve quantum-limited signal-to-noise ratio in spectroscopy and atomic clocks [40,48].
 - 8.1.2 Information-swapping techniques can be used for cooling and state detection in spectroscopy and atomic clocks [49].
 - 8.1.3 If the loss in MEMS resonator systems can be reduced, sympathetic laser-cooling techniques may be useful to enable these systems to reach the ground state of mechanical motion [8].

8.2 Noise measurement

- 8.2.1 The ion motion is a very sensitive (tunable) detector of surface electric field fluctuations. This feature, which causes motional decoherence in an ion-trap quantum computer, can perhaps find use in the study of fluctuating fields which affect other quantum-information-processing devices.

9. Role of theory

9.1 Hardware-specific algorithm development

- 9.1.1 Develop algorithms and error-correcting codes tailored to typical sources of decoherence found in ion traps.

9.1.1.1 Incorporate realizable two-bit or multibit gates.

9.1.1.2 Incorporate the parallelism inherent in multiplexed trap arrays.

9.1.1.3 Determine fault-tolerant thresholds for feasible operations.

9.1.1.4 Can gate teleportation be used to increase overall computational speed?

- 9.1.2 Various noise sources could be modeled and their effects on an ion-trap quantum computer estimated.

- 9.2 Develop a theory for the sources of observed decoherence (particularly relating to the electric potential noise observed on trap electrodes.)

9.3 Quantum processing using multi-level logic

- 9.3.1 Electronic ground states of atomic ions (and neutrals) typically have multiple hyperfine Zeeman sublevels in which high coherence could be maintained. Theorists could explore the use of these multilevel systems, as opposed to two-level qubits for QIP.

9.4 Multiqubit (>2) and other gate structures in trapped ions

- 9.4.1 Investigate use of multiple modes of motion to streamline certain logic operations

- 9.4.2 Investigate use of shaped fields (e.g., with an optical lattice) to simultaneously address many ions.

9.5 Coupling of an entangled system to its environment

- 9.5.1 The richness of an open system of even a few qubits offers many theoretical challenges.

- 9.5.2 Investigate optimization of DFS encoding for realistic couplings to the environment.

6.0 Timeline

1. Timeline for 2002–2007

- 1.1 Refer to the Excel timeline chart below and #3 of “Considerations” (above).

2. Timeline for 2007–2012

- 2.1 Refer to the Excel timeline chart below and #4 of “Considerations” (above).

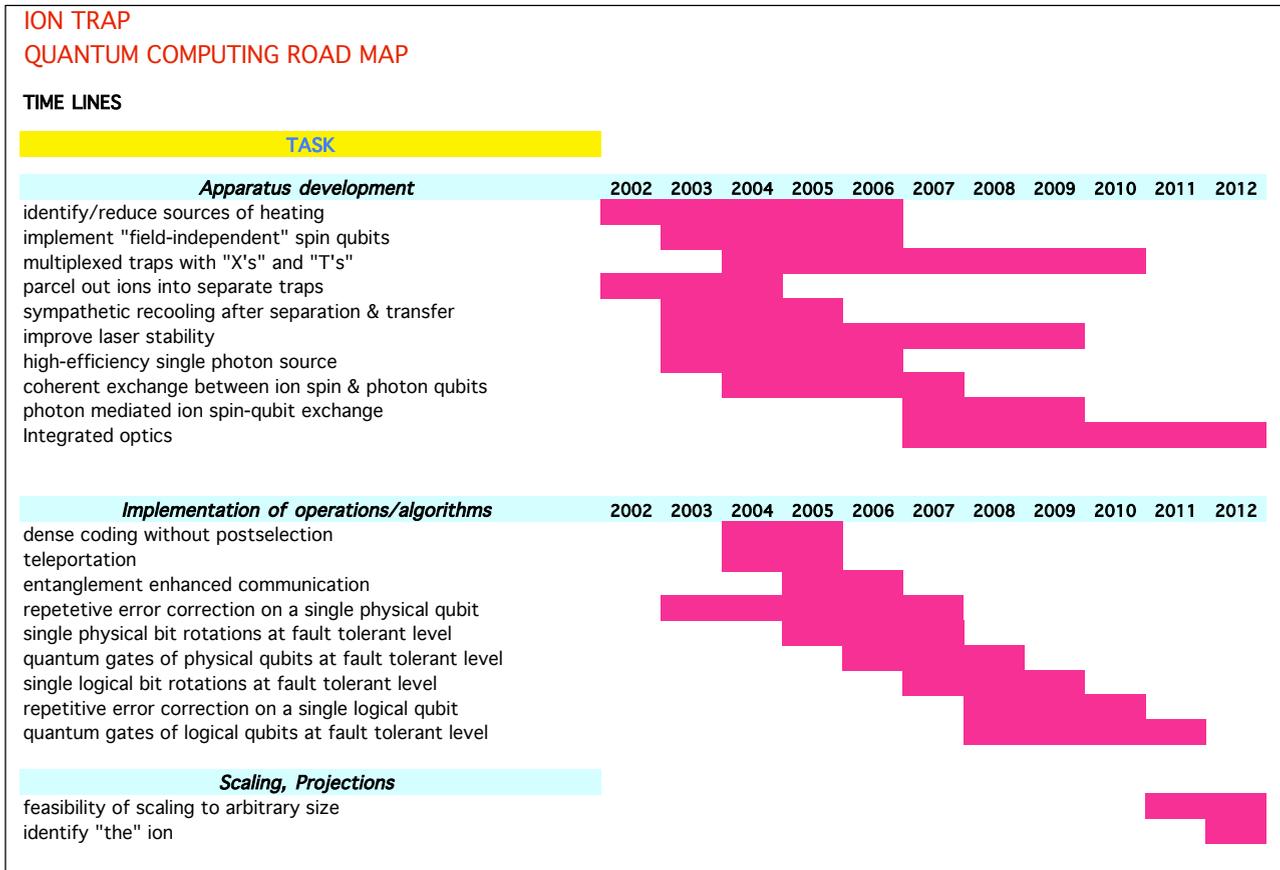


Figure 6-1. Ion trap QC developmental timeline

7.0 Glossary

8.0 References

- [1] Cirac, J.I. and P. Zoller, "Quantum computations with cold trapped ions," *Physical Review Letters* **74**, 4091–4094 (1995).
- [2] Cirac, J.I., P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Physical Review Letters* **78**, 3221–3224 (1997).
- [3] Pellizzari, T., "Quantum networking with optical fibers," *Physical Review Letters* **79**, 5242–5245 (1997).
- [4] DeVoe, R.G., "Elliptical ion traps and trap arrays for quantum computation," *Physical Review A* **58**, 910–914 (1998).
- [5] Duan, L.-M., B.B. Blinov, D.L. Moehring, and C. Monroe, "Scalable trapped ion quantum computation with a probabilistic ion-photon mapping," (5-Jan-04) preprint *quant-ph/0401020*.

- [6] Cirac, J.I. and P. Zoller, "A scalable quantum computer with ions in an array of microtraps," *Nature* **404**, 579–581 (2000).
- [7] Kielpinski, D., C. Monroe, and D.J. Wineland, "Architecture for a large-scale ion-trap quantum computer," *Nature* **417**, 709–711 (2002).
- [8] Wineland, D.J., C. Monroe, W.M. Itano, D. Leibfried, B.E. King, and D.M. Meekhof, "Information issues in coherent quantum-state manipulation of trapped atomic ions," *Journal of Research of the National Institute of Standards and Technology* **103**(3), 259–328 (1998).
- [9] Rowe, M.A., A. Ben-Kish, B. DeMarco, D. Leibfried, V. Meyer, J. Beall, J. Britton, J. Hughes, W.M. Itano, B. Jelenkovi, C. Langer, T. Rosenband, and D.J. Wineland, "Transport of quantum states and separation of ions in a dual RF ion trap," *Quantum Information and Computation* **2**, 257–271 (2002).
- [10] Guthöhrlein, G.R., M. Keller, K. Hayasaka, W. Lange, and H. Walther, "A single ion as a nanoscopic probe of an optical field," *Nature* **414**, 49–51 (2001).
- [11] Eschner, J., Ch. Raab, F. Schmidt-Kaler, and R. Blatt, "Light interference from single atoms and their mirror images," *Nature*, **413**, 495–498 (2001).
- [12] Rohde, H., S.T. Gulde, C.F. Roos, P.A. Barton, D. Leibfried, J. Eschner, F. Schmidt-Kaler and R. Blatt, "Sympathetic ground-state cooling and coherent manipulation with two-ion crystals," *Journal of Optics B: Quantum and Semiclassical Optics* **3**, S34–S41 (2001).
- [13] Blinov, B.B., L. Deslauriers, P. Lee, M.J. Madsen, R. Miller, and C. Monroe, "Sympathetic cooling of trapped Cd^+ isotopes," *Physical Review A* **65**, 040304 (2002).
- [14] Barrett, M.D., B. DeMarco, T. Schätz, V. Meyer, D. Leibfried, J. Britton, J. Chiaverini, W.M. Itano, B. Jelenkovic, J.D. Jost, C. Langer, T. Rosenband, and D.J. Wineland, "Sympathetic cooling of $^9\text{Be}^+$ and $^{24}\text{Mg}^+$ for quantum logic," *Physical Review A* **68**, 042302 (2003).
- [15] Fisk, P.T.H., M.J. Sellars, M.A. Lawn, C. Coles, A.G. Mann, and D.G. Blair, "Very high Q microwave spectroscopy on trapped $^{171}\text{Yb}^+$ ions: Application as a frequency standard," *IEEE Transactions on Instrumentation and Measurement*, **44**, 113–116 (1995).
- [16] Sørensen, A. and K. Mølmer, "Entanglement and quantum computation with ions in thermal motion," *Physical Review A* **62**, 022311 (2000).
- [17] Bacon, D.M., Ph.D. thesis, University of California, Berkeley (2001), Chapter 10.
- [18] Blatt, R. and P. Zoller, "Quantum jumps in atomic systems," *European Journal of Physics* **9**, 250–256 (1988).
- [19] Neuhauser, W., M. Hohenstatt, P.E. Toschek, and H. Dehmelt, "Localized visible Ba^+ mono-ion oscillator," *Physical Review A* **22**, 1137–1140 (1980).
- [20] Nagourney, W., J. Sandberg, and H. Dehmelt, "Shelved optical electron amplifier: Observation of quantum jumps," *Physical Review Letters* **56**, 2797–2799 (1986).

- [21] Sauter, Th., W. Neuhauser, R. Blatt, and P.E. Toschek, "Observation of quantum jumps," *Physical Review Letters* **57**, 1696–1698 (1986).
- [22] Bergquist, J.C., R.G. Hulet, W.M. Itano, and D.J. Wineland, "Observation of quantum jumps in a single atom," *Physical Review Letters* **57**, 1699–1702 (1986).
- [23] Nägerl, H.C., D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, "Laser addressing of individual ions in a linear ion trap," *Physical Review A* **60**, 145–148 (1999).
- [24] Rafac, R.J., B.C. Young, J.A. Beall, W.M. Itano, D.J. Wineland, and J.C. Bergquist, "Sub-dekahertz ultraviolet spectroscopy of $^{199}\text{Hg}^+$," *Physical Review Letters* **85**, 2462–2465 (2000).
- [25] Meekhof, D.M., C. Monroe, B. King, W.M. Itano, and D.J. Wineland, "Generation of nonclassical motional states of a trapped atom," *Physical Review Letters* **76**, 1796–1799 (1996); erratum, **77**, 2346 (1996).
- [26] Roos, Ch., Th. Eigher, H. Rohde, H.C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt-Kaler, and R. Blatt, "Quantum state engineering on an optical transition and decoherence in a Paul trap," *Physical Review Letters* **83**, 4713–4716 (1999).
- [27] Monroe, C., D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, "Demonstration of a fundamental quantum logic gate," *Physical Review Letters* **75**, 4714–4717 (1995).
- [28] Sackett, C.A., D. Kielpinski, B.E. King, C. Langer, V. Meyer, C.J. Myatt, M. Rowe, Q.A. Turchette, W.M. Itano, D.J. Wineland, and C. Monroe, "Experimental entanglement of four particles," *Nature* **404**, 256–259 (2000).
- [29] Monroe, C., D. Leibfried, B.E. King, D.M. Meekhof, W.M. Itano, and D.J. Wineland, "Simplified quantum logic with trapped ions," *Physical Review A* **55**, R2489–2491 (1997).
- [30] DeMarco, B., A. Ben-Kish, D. Leibfried, V. Meyer, M. Rowe, B.M. Jelenkovic, W.M. Itano, J. Britton, C. Langer, T. Rosenband, and D.J. Wineland, "Experimental demonstration of a controlled-NOT wave-packet gate," *Physical Review Letters* **89**, 267901 (2002).
- [31] Gulde, S., M. Riebe, G.P.T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I.L. Chuang, R. Blatt, "Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer." *Nature* **421**, 48–50 (2003). (new gate demonstrated as part of this)
- [32] Schmidt-Kaler, F., H. Häffner, M. Riebe, S. Gulde, G.P.T. Lancaster, T. Deuschle, C. Becher, C.F. Roos, J. Eschner, and R. Blatt, "Realization of the Cirac-Zoller controlled-NOT quantum gate," *Nature* **422**, 408–411 (2003).
- [33] Leibfried, D., B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W.M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D.J. Wineland, "Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate," *Nature* **422**, 412–415 (2003).

- [34] Schmidt-Kaler, F., H. Häffner, S. Gulde, M. Riebe, G. Lancaster, J. Eschner, C. Becher, and R. Blatt, “Quantized phase shifts and a dispersive universal quantum gate,” (29-Jul-03) preprint *quant-ph/0307211*.
- [35] Rowe, M.A., D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, “Experimental violation of a Bell’s inequality with efficient detection,” *Nature*, **409**, 791–794 (2001).
- [36] Roos, C.F., G.P.T. Lancaster, M. Riebe, H. Häffner, W. Haensel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, and R. Blatt, “Tomography of entangled massive particles,” (29-Jul-03) preprint *quant-ph/0307210*.
- [37] Blinov, B.B., D.L. Moehring, L.-M. Duan, and C. Monroe, “Observation of entanglement between a single trapped atom and a single photon,” *Nature* **428**, 153–157 (2004).
- [38] Leibfried, D., D.M. Meekhof, B.E. King, C. Monroe, W.M. Itano, and D.J. Wineland, “Experimental determination of the motional quantum state of a trapped atom,” *Physical Review Letters* **77**, 4281–4284 (1996).
- [39] Leibfried, D., D.M. Meekhof, C. Monroe, B.E. King, W.M. Itano, and D.J. Wineland, “Experimental preparation and measurement of quantum states of motion of a trapped atom,” *Journal of Modern Optics* **44**, 2485–2505 (1997).
- [40] Meyer, V., M.A. Rowe, D. Kielpinski, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, “Experimental demonstration of entanglement-enhanced rotation angle estimation using trapped ions,” *Physical Review Letters* **86**, 5870–5873 (2001).
- [41] Leibfried, D., B. DeMarco, V. Meyer, M. Rowe, A. Ben-Kish, J. Britton, W.M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D.J. Wineland, “Trapped-ion quantum simulator: experimental application to nonlinear interferometers,” *Physical Review Letters* **89**, 247901 (2002).
- [42] Ben-Kish, A., B. DeMarco, V. Meyer, M. Rowe, J. Britton, W.M. Itano, B.M. Jelenkovic, C. Langer, D. Leibfried, T. Rosenband, and D.J. Wineland, “Experimental demonstration of a technique to generate arbitrary quantum superposition states of a harmonically bound spin-1/2 particle,” *Physical Review Letters* **90**, 037902 (2003).
- [43] Plenio, M.B. and P.L. Knight, “Decoherence limits to quantum computation using trapped ions,” *Proceedings of the Royal Society of London, Series A – Mathematical and Physical Sciences*, **453**, 2017–2041 (1997).
- [44] Wineland, D.J., M. Barrett, J. Britton, J. Chiaverini, B. DeMarco, W.M. Itano, B. Jelenkovic, C. Langer, D. Leibfried, V. Meyer, T. Rosenband, and T. Schätz, “Quantum information processing with trapped ions,” *Philosophical Transactions of the Royal Society of London A* **361**, 1349–1361 (2003).
- [45] Steane, A.M. and D.M. Lucas, “Quantum computation with trapped ions, atoms and light,” in *Scalable Quantum Computers*, S.L. Braunstein and H.K. Lo Eds., (Wiley-VCH, Berlin, 2001), pp. 69–88.

- [46] Steane, A.M. and W. van Dam, "Physicists Triumph at 'Guess My Number'," *Physics Today* **53**(2), 35--39 (2000).
- [47] Birkel, G., F.B.J. Buchkremer, R. Dumke, and W. Ertmer, "Atom optics with microfabricated optical elements," *Optics Communications* **191**, 67--81 (2001).
- [48] Bollinger, J.J., W.M. Itano, D.J. Wineland, and D.J. Heinzen, "Optimal frequency measurements with maximally correlated states," *Physical Review A* **54**, R4649--4652 (1996).
- [49] Wineland, D.J., J.C. Bergquist, J.J. Bollinger, R.E. Drullinger, and W.M. Itano, "Quantum computers and atomic clocks," *Proceedings of the 6th Symposium Frequency Standards & Metrology*, P. Gill, Ed., (World Scientific, Singapore, 2002), pp 361--368.

Neutral Atom Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.3

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not to be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Carlton Caves

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0 Groups Pursuing This Approach	1
2.0 Background and Perspective	2
3.0 Summary of Neutral Atom QC: The DiVincenzo Criteria.....	3
4.0 What Has Been Accomplished.....	6
5.0 Considerations	7
6.0 Timeline.....	10
7.0 Glossary	11
8.0 References	12

List of Tables and Figures

Table 1-1 Approaches to Neutral Atom QC Research*.....	1
Figure 6-1. Neutral atom QC developmental timeline.....	11

List of Acronyms and Abbreviations

3-D	three dimensional
BEC	Bose-Einstein condensate
GHZ	Greenberger, Horne, and Zeilinger
kHz	kilohertz
MHz	megahertz
NMR	nuclear magnetic resonance
QC	quantum computation/ computing
QED	quantum electrodynamics
TEP	Technology Experts Panel

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Neutral Atom detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Approaches to Neutral Atom QC Research*

Research Leader(s)	Research Location	Research Focus
Chapman, M. S.	Georgia Tech, Atlanta	magnetic and optical trapping/cavity QED
Cirac, J. I.	Max-Planck-Institute, Garching	Theory
Cote, R.	U. of Connecticut, Storrs	Theory
Deutsch, I. H.	U. of New Mexico	Theory
Ertmer, W. & Birkl, G.	U. of Hannover	optical trapping with micro-optics
Gould, P.	U. of Connecticut, Storrs	optical trapping of Rydberg atoms
Grangier, P.	Institute d'Optique, Orsay	single-atom trapping
Haensch, T. W. & Bloch, I.	Max-Planck-Institute, Garching	BEC/optical trapping
Haroche, S.	Ecole Normale, Paris	cavity QED
Jessen, P. S.	U. of Arizona, Tucson	optical lattices
Kimble, H. J. & Mabuchi, H.	Caltech	cavity QED
Lukin, M.	Harvard, Massachusetts	Theory
Meschede, D.	U. of Bonn	single-atom trapping
Mølmer, K.	U. of Aarhus	Theory
Phillips, W. D. & Rolston, S. L.	NIST Gaithersburg, Maryland	optical lattices
Reichel, J.	U. of Mainz	magnetic microtraps
Saffman, M. & Walker, T. G.	U. of Wisconsin, Madison	optical trapping of Rydberg atoms
Schmiedmayer, J.	U. of Heidelberg	magnetic microtraps
Stamper-Kurn, D.	UC Berkeley, California	magnetic microtraps/cavity QED
Walther, H. & Rempe, G.	Max-Planck-Institute, Garching	cavity QED
Weiss, P.	Penn State, State College	optical lattice/Rydberg atoms
Williams, C. J.	NIST Gaithersburg, Maryland	Theory
You, L.	Georgia Tech, Atlanta	Theory
Zoller, P. & Briegel, H. J.	U. of Innsbruck	Theory

* Including neutral atoms trapped in optical lattices and/or magnetic guides and microtraps.

2.0 Background and Perspective

A system of trapped neutral atoms is a natural candidate for implementing scalable QC [1,2] given the

- simple quantum-level structure of atoms,
- isolation of neutrals from the environment, and
- present ability to trap and act on a very large ensemble of identical atoms.

In much the same way as the groundbreaking work on QC in ion traps [3], such a system builds on years of expertise in coherent spectroscopy developed by the atomic/optical community for application in precision measurements, most notably in atomic clocks. One might argue that a quantum computer is nothing more than a multiatom atomic clock, with controlled interactions between the constituent atoms. More recent advances in laser cooling and trapping technology open the door to unprecedented levels of coherence and control [4], as made evident [5] through the production of Bose-Einstein condensates (BECs) and Fermi degenerate gases.

The architecture of such a computer will depend strongly on the specific trapping techniques and the method for coupling atoms. Two basic interactions can be used to trap neutral atoms: fields interacting with the atom's induced electric dipole moment or with its permanent magnetic dipole moment. The best-studied trapping technology is the optical lattice [6], in which electric dipole-force potential wells are produced by the standing waves of intersecting laser beams. This virtual crystal can be dynamically controlled through the parameters of the trapping lasers or other external fields. Optical dipole forces can also be used to trap atoms in other configurations, such as through engineered micro-optics [7,8,9] and particular configurations of time-varying fields [10]. Magnetic trapping, especially in microtraps [11,12], though less mature, has also been demonstrated.

Trapped atoms can be cooled to the motional ground state of the potential wells, and the internal atomic states can be prepared in a desired initial state using standard techniques of laser spectroscopy. The motional and internal states provide a number of choices of levels for defining qubits. The trap itself and additional fields make available a variety of "handles" for coherent control of the motional and internal states. That the atoms are neutral means that they are relatively poorly coupled to the environment, thus reducing decoherence. By the same token, however, the atoms interact only weakly with one another. Proposals for two-qubit gates rely on

1. moving pairs of atoms into close proximity to increase their coupling (coherent transport of atoms in an optical lattice has been demonstrated [13],
2. turning on briefly much stronger electric-dipole or other interactions, or
3. both of these.

These techniques pose an inherent risk of opening up additional decoherence channels during gate operation.

To implement a neutral-atom quantum computer, the logical encoding for qubits, the method for performing logical operations, and the read-out strategy must all be addressed as a whole, with the design contingent on the specific atom to be used and the trapping technology. For example, parallel operations are natural in the lattice geometry, but because the atoms in a filled

optical lattice are spaced less than a trap-laser wavelength apart, there are difficult questions about how to address individual atoms. Various approaches might be used to overcome this difficulty. As another example, magnetic traps restrict the possible states available for logical encoding, but offer possible advantages for integrating with solid-state devices. Whichever approach proves superior, the highest priority for any experiment is to implement controlled high-fidelity quantum logic operations. This might be achieved in a geometry that does not provide the clearest route to a scalable quantum computer (e.g., ensemble operation without individual addressing), but nonetheless provide the proof-of-principle necessary to design such a scalable system.

3.0 Summary of Neutral Atom QC: The DiVincenzo Criteria

Recognizing that optical lattices are the most mature such technology, this section concentrates on optical lattices, while drawing attention in places to the potential of other trapping techniques.

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits 
 - 1.1 Optical lattices can be loaded with many atoms from a laser-cooled sample or from a BEC.
 - 1.1.1 Approximately a million atoms have been loaded into an optical trap from a laser-cooled sample [14]. Loading of one atom per well in a three-dimensional (3-D) lattice has been achieved by using the transition to a Mott insulator [15]. Designer lattices in which the depth of the wells varies spatially provide the potential for loading more complex configurations. A notable feature for scalability is that the character and properties of the lattice and the trapped atoms don't change in any essential way when going from a smaller to a larger lattice.
 - 1.1.2 A potential problem exists in addressing individual atoms, which are separated by less than a wavelength of the trapping lasers. Possible solutions include the following:
 - 1.1.2.1 Designer lattices with wells separated by more than a wavelength [16].
 - 1.1.2.2 Trapping in a long-wavelength lattice. Resolution of individual Rb atoms has been demonstrated in a CO₂ lattice [17,18] and in a magnetic-trap storage ring [19].
 - 1.1.2.3 Controlled partial loading of the lattice, so that only a well defined subset of the potential wells is occupied [16].

- 1.1.2.4 Use of gradient fields to distinguish atoms in different wells and thus provide individual addressing.
- 1.1.2.5 Use of other trapping techniques for neutral atoms, which provide tighter confinement and/or greater separation. Individual addressing has been achieved with neutrals trapped in optical micro-traps [17], where the atoms are separated by many wavelengths.
- 1.2 The many motional and internal atomic states provide a number of choices for defining qubits.
 - 1.2.1 Internal-state qubits are formed from the ground hyperfine states, which are well characterized by atomic spectroscopy and atomic-clock technology.
 - 1.2.2 Motional qubits are formed from the well characterized quantized levels in the trapping potential.
 - 1.2.3 The many atomic levels other than those chosen to define qubits pose a problem for quantum control because of the potential for leakage outside the qubit state space. The additional levels might be used to advantage, however, as intermediate states in conditional logic operations or in quantum logic involving more than two levels (qudits, instead of qubits).
- 2. The ability to initialize the state of the qubits to a simple fiducial state 
 - 2.1 Internal-state qubits can be prepared reliably in a standard initial state using optical-pumping techniques in use since the 1950s. These techniques can achieve populations in the desired state >0.9999 .
 - 2.2 Motional qubits can be cooled to the motional ground state using techniques of laser cooling and Raman sideband cooling [14,20,21,22,23]. Ground-state populations greater than 95% have been achieved [14].
 - 2.3 Loading of a lattice from a precooled BEC through use of the superfluid–Mott-insulator phase transition has the potential to prepare both internal and motional states reliably.
- 3. Long (relative) decoherence times, much longer than the gate operation time 
 - 3.1 Memory decoherence.
 - 3.1.1 For internal-state qubits (hyperfine states), coherence times are known to be long (μs , ms ~ many minutes), but have not yet been measured and are expected to be highly system specific.
 - 3.1.2 Motional qubits are expected to have a long coherence time because of neutrals' weak coupling to the environment, but the time has not yet been measured.
 - 3.1.3 The fundamental decoherence mechanism for both kinds of qubits in an optical trap is photon scattering. Technical decoherence mechanisms, such as stray magnetic fields, trapping-field fluctuations, and inelastic collisions with background gas, are likely to play a role. Long-term trapping times in an optical lattice are unknown.

- 3.2 Decoherence during gate operations is likely to be a greater problem than memory decoherence. Additional decoherence channels are opened up during gate operations, especially in two-qubit gates, as a consequence of the strong couplings introduced to perform the gate. Issues that need to be addressed experimentally and theoretically for gate-operation decoherence include
- laser-beam intensity stability,
 - pulse timing stability,
 - spontaneous emission during gates that populate levels outside the qubit state space,
 - molecular chemistry during gates that rely on close atomic encounters,
 - unwanted entanglement between internal and motional degrees of freedom, and
 - transitions out of the qubit state space during gate operation.

Fundamental decoherence mechanisms giving decoherence times $\sim 1 \mu\text{s}$, when combined with gate times of $0.1 \mu\text{s}$ to $100 \mu\text{s}$ (determined by lattice trapping frequencies), give a decoherence time/gate time ratio of $10:10^4$. Experiments are needed to get a handle on what is possible.

4. A universal set of quantum gates 
- Single-qubit rotations on atomic systems have been carried out in nuclear magnetic resonance (NMR) and laser spectroscopy since the 1940s.
 - No two-qubit gates have as yet been implemented. Proposals for two-qubit gates are listed below. The speed of gates that involve moving atoms (all except #4.2.1.2 in the following list) is limited by the trap frequency, which lies in the range $10 \text{ kHz} - 10 \text{ MHz}$. Coherent transport of atoms in an optical lattice has been demonstrated [13].
 - Gates based on electric-dipole interactions between pairs of atoms.
 - Optically induced conditional electric-dipole interaction between pairs of atoms brought into close proximity [24,25,26].
 - Electric-dipole interaction via conditional excitation to a Rydberg state [27]. Because this gate does not involve moving atoms, its speed can be set by the strength of the electric-dipole interaction. This gate is potentially insensitive to motional heating. Collective versions of this gate have also been proposed [28].
 - Gates based on ground-state elastic collisions.
 - Cold collisions between atoms conditioned on internal states [29,30].
 - Cold collisions between atoms conditioned on motional-state tunneling [31].
 - Gates based on magnetic dipole interactions between pairs of atoms brought into close proximity [32].
 - Parallel operations for both single-qubit and two-qubit gates are the natural method of operation in optical lattices.

5. A qubit-specific measurement capability 
 - 5.1 The “quantum-jump” method of detection via cycling transitions is a standard technique in atomic physics.
6. The ability to interconvert stationary and flying qubits 
 - 6.1 Cavity-QED (quantum electrodynamics) techniques can be used to convert between atomic-state qubits and photons, although it is not clear whether this capability would be useful in neutral-atom QC.
7. The ability to faithfully transmit flying qubits between specified locations 
 - 7.1 Standard optical techniques can be used to transmit photons from one location to another.

4.0 What Has Been Accomplished

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states. 
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.2 Demonstrate decoherence times much longer than Rabi oscillation period. 
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 
3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - 3.2 Produce and characterize Bell states. 
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
 - 3.4 Demonstrate quantum state and process tomography for two qubits. 
 - 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS). 
 - 3.6 Demonstrate a two-qubit quantum algorithm. 
4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, & Zeilinger (GHZ)-state of three physical qubits. 
 - 4.2 Produce maximally-entangled states of four and more physical qubits. 
 - 4.3 Quantum state and process tomography. 

Tomography of the quantum states of the large angular-momentum hyperfine spaces of Cs atoms trapped in an optical lattice has been demonstrated by Klose [33].

- 4.4 Demonstrate decoherence-free subspaces. 
- 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
- 4.6 Demonstrate quantum error correcting codes. 
- 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
- 4.9 Demonstrate quantum logic operations with fault-tolerant precision. 
- 5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
- 6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
- 7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

- 1. Special strengths
 - 1.1. Neutral atoms have a simple well-characterized energy-level structure.
 - 1.2. Neutral atoms start with the obvious advantage of being uncharged, which gives a substantial advantage in terms of weak coupling to the environment and consequent low decoherence for both internal and motional states.
 - 1.3. Laser-cooling and laser-spectroscopy techniques make available high-fidelity initial-state preparation.
 - 1.4. Standard “quantum jump” detection techniques provide efficient readout.
 - 1.5. The lattice geometry makes it easy to perform massively parallel operations.
 - 1.6. There are straightforward paths to scalability—*provided* individual addressing can be achieved or rendered unnecessary by new models for QC.
 - 1.7. Neutral atoms are relatively clean systems for theoretical analysis, particularly compared to condensed systems. Well-developed, often first-principles theoretical understanding and techniques can be used to analyze state preparation, quantum control, and decoherence in neutral-atom systems.

2. Unknowns, weaknesses
 - 2.1. The interactions required for two-qubit gates are less straightforward than, say, for ions. Though theoretical estimates of decoherence times and achievable gate fidelities are encouraging, these need to be demonstrated and measured in experiments.
 - 2.2. Whether individual addressing can be achieved and the extent to which it is necessary is a major open question.
 - 2.3. Error-correction protocols and fault-tolerant computation suitable for the lattice geometry have not yet been designed, although the lattice geometry seems natural for robust “topological” codes.
 - 2.4. Long-term trapping times are unknown.
 - 2.5. To achieve quantum-information-processing goals in this, as in other approaches to quantum computing, generally requires a period of basic research and technology development in the laboratory. Though it is difficult to predict the outcome of such technology development, it must be supported as an essential part of the process of achieving the more glamorous information-processing goals.
3. Goals 2002–2007
 - 3.1. Demonstrate full (arbitrary) two-qubit state manipulation.
 - 3.2. Characterize relevant decoherence mechanisms, especially those that become important during gate operations.
 - 3.3. Demonstrate individual addressing in a trapping environment suitable for quantum information processing or a scheme that circumvents the need for individual addressing.
 - 3.4. Assemble ingredients for simple error correction, say, for spontaneous emission.
4. Goals 2007–2012
 - 4.1. Demonstrate full error correction for several logical qubits.
 - 4.2. Provide a clear path to a scalable system.
5. Necessary achievements
 - 5.1. Demonstrate controlled loading of optical lattice.
 - 5.2. Demonstrate one or more of the proposed two-qubit gates with high enough fidelity to warrant further development.
 - 5.2. Demonstrate one or more of the schemes for individual addressing in a trapping environment suitable for quantum information processing or an alternative scheme that circumvents or reduces the need for individual addressing.
6. Trophies
 - 6.1. Entanglement between motional and internal atomic degrees of freedom in neutral-atom systems.
 - 6.2. Entanglement among two or more qubits as a consequence of one or more two-qubit gate operations.

- 6.3. Continuous measurement of feedback control of atomic dynamics.
 - 6.4. Controlled loading of lattices with complex, well-defined configurations of atoms.
 - 6.5. Demonstration of error-correction protocol for correction of spontaneous-emission errors.
 - 6.6. Demonstration of quantum teleportation in an optical lattice.
 - 6.6. Loading of an optical lattice from a BEC.
 - 6.7. Individual addressing of atoms in an optical lattice for purposes of quantum information processing.
7. Connections with other quantum information science technologies
 - 7.1. Trapping in optical lattices can be married with magnetic microtraps, to take advantage of tighter confinement and thus potentially stronger interactions between atoms, and with cavity QED technology, to take advantage of coupling to photons (flying qubits).
 - 7.2. BECs provide a method for loading traps and might also provide additional possibilities for quantum control.
8. Subsidiary developments
 - 8.1. Trapped neutral atoms provide an avenue to improved signal-to-noise in atomic spectroscopy, with applications to atomic clocks.
 - 8.2. QC techniques can be applied to cooling, state preparation, state manipulation, and detection of the atoms in atomic clocks.
 - 8.3. Developments in quantum control of trapped neutral atoms for QC can be used to control collisions of neutral atoms for study of chemical reactions and of molecular physics.
 - 8.4. Developments in quantum control of trapped neutral atoms can be used to study new states of matters, such as BECs and Mott insulators.
9. Role of theory
 - 9.1. Design and analyze additional two-qubit gates for neutral atoms.
 - 9.2. Study atomic/molecular interactions between neutrals for application to analysis of quantum gates.
 - 9.3. Develop and analyze control tools (e.g., feedback and adaptive measurements, for trapped neutrals).
 - 9.4. Model and characterize decoherence and noise, including effects of molecular chemistry in close collisions.
 - 9.5. Develop error-correction and fault-tolerant protocols suited to optical-lattice geometry.
 - 9.6. Explore QC paradigms suited to massively parallel operations available in lattice geometry (e.g., cellular automata) thereby circumventing the need for individual addressing.

- 9.7. Develop algorithms tailored to the particular sources of decoherence found in neutral-atom traps.
- 9.8. Develop quantum-computing architectures appropriate to neutral atoms.

6.0 Timeline

Each section of the timeline (5-year and 10-year) is broken out by period, with tasks for each period. *Critical-path, necessary achievements* are indicated by italics.

1. Timeline for 2002–2007
 - 1.1 Period 1: 2002–2004
 - 1.1.1 3-D lattice cooled to the motional ground state
 - 1.1.2 Preparation of internal states
 - 1.1.3 Arbitrary single-qubit control
 - 1.1.4 *Proof-of-principle two-qubit gates*
 - 1.1.5 Projective measurements on ensemble of lattice atoms
 - 1.1.6 Ensemble process tomography
 - 1.2 Period 2: 2005–2007
 - 1.2.1 *Controlled loading of lattice*
 - 1.2.2 High-fidelity two-qubit gates
 - 1.2.3 *Full (arbitrary) two-qubit control*
 - 1.2.4 *Individual addressing or alternative*
 - 1.2.5 *Measurements of individual atoms*
 - 1.2.6 Continuous measurement and feedback
 - 1.2.7 Individual-atom process tomography
2. Timeline for 2007–2012
 - 2.1 Period 1: 2008–2009
 - 2.1.1 Encoding logical qubit
 - 2.1.2 Using ancilla to diagnose errors
 - 2.1.3 *Simple error-correction protocol*
 - 2.1.4 Additional cooling beyond initialization
 - 2.1.5 Refreshing ancilla
 - 2.2 Period 2: 2010–2012
 - 2.2.1 Full error correction for several logical qubits
 - 2.2.2 Begin full-system integration

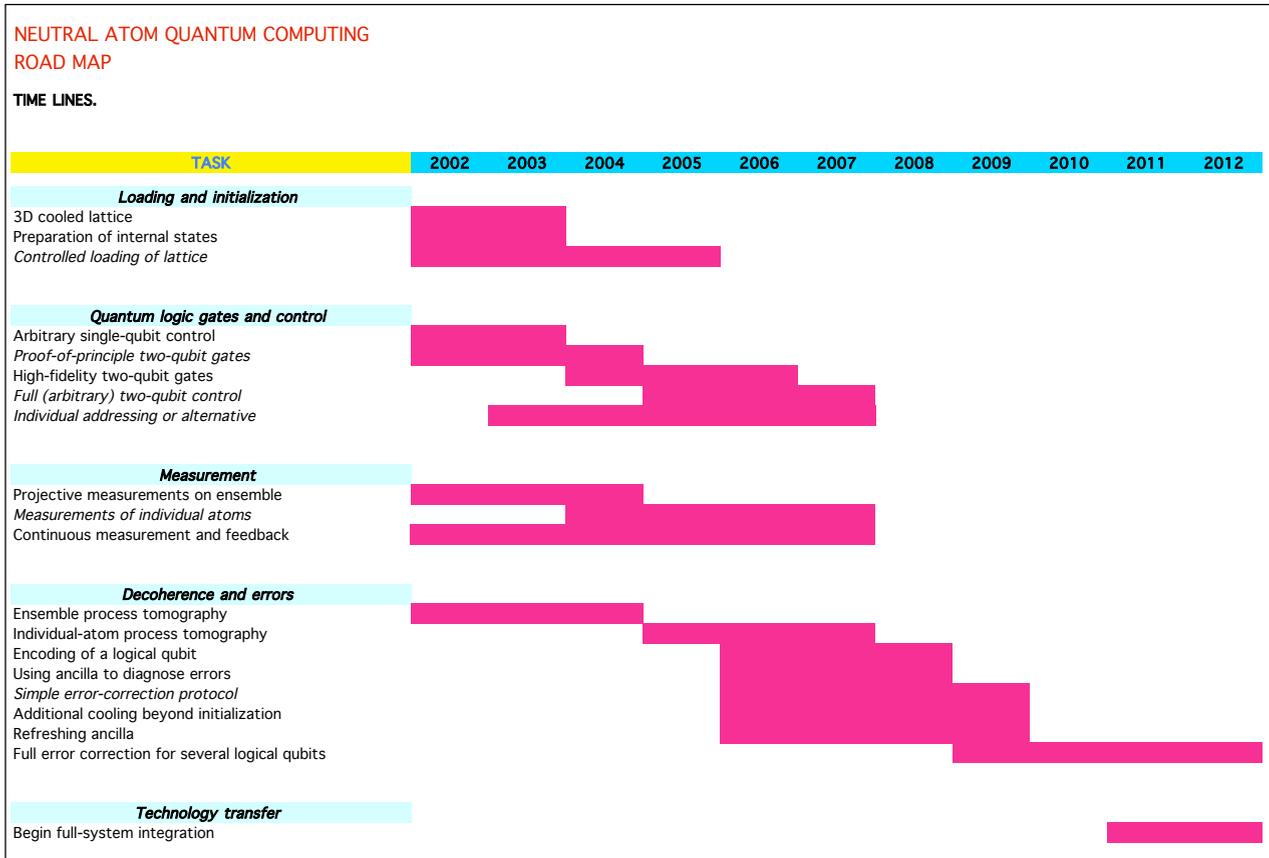


Figure 6-1. Neutral atom QC developmental timeline

7.0 Glossary

Bose-Einstein condensate

A state of a tenuous, very low-temperature gas in which all the atoms occupy the same motional quantum state; typically all the atoms are essentially at rest.

cavity quantum electrodynamics (QED)

Individual atoms interacting with the strong electromagnetic field inside a small optical-frequency cavity.

magnetic microtrap

A configuration of magnetic fields in which atoms can be trapped in the regions of strongest field strength via the interaction of the atomic magnetic-dipole moments with the magnetic field.

optical dipole force

When an atom is exposed to light, the electric field of the light induces an optical-frequency electric-dipole moment in the atom, and then the electric field exerts a DC optical dipole force on the induced dipole.

optical lattice

A pattern of standing light waves created by the interference of intersecting laser beams; neutral atoms can be trapped in the standing-wave pattern by optical dipole forces.

optical microtrap

A configuration of tightly focused light beams; atoms can be trapped by optical dipole forces in the regions of greatest light intensity.

qudit

A quantum system where more than two Hilbert-space dimensions are used for quantum information processing, as opposed to the two dimensions used in a qubit.

Rydberg atom

An atom with one valence electron that has been excited to a high-lying (Rydberg) energy level.

8.0 References

- [1] Deutsch, I.H., G.K. Brennen, and P.S. Jessen, "Quantum computing with neutral atoms in an optical lattice," *Fortschritte der Physik [Progress of Physics]* **48**, 925–943 (2000).
- [2] Briegel, H.J., T. Calarco, D. Jaksch, J.I. Cirac, and P. Zoller, "Quantum computing with neutral atoms," *Journal of Modern Optics* **47**, 415–451 (2000).
- [3] Monroe, C., "Quantum information processing with atoms and photons," *Nature* **416**, 238–246 (2002).
- [4] Chu, S., "Cold atoms and quantum control," *Nature* **416**, 206–210 (2002).
- [5] Anglin, J.R. and W. Ketterle, "Bose-Einstein condensation of atomic gases," *Nature* **416**, 211–218 (2002).
- [6] Jessen, P.S. and I.H. Deutsch, "Optical lattices," in *Advances in Atomic, Molecular, and Optical Physics*, Vol. 37, B. Bederson and H. Walther, Eds., (Academic, San Diego, 1996), pp. 95–138.
- [7] Birkl, G., F.B.J. Buchkremer, R. Dumke, and W. Ertmer, "Atom optics with microfabricated optical elements," *Optics Communications* **191**, 67–81 (2001).
- [8] Buchkremer, F.B.J., R. Dumke, M. Volk, T. Muther, G. Birkl, and W. Ertmer, "Quantum information processing with microfabricated optical elements," *Laser Physics* **12**, 736–741 (2002).
- [9] K. Eckert, J. Mompert, X.X. Yi, J. Schliemann, D. Bruss, G. Birkl, and M. Lewenstein, "Quantum computing in optical microtraps based on the motional states of neutral atoms," *Physical Review A* **66**, 042317 (2002).
- [10] Milner, V., J.L. Hanssen, W.C. Campbell, and M.G. Raizen, "Optical billiards for atoms," *Physical Review Letters* **86**, 1514–1517 (2001).

- [11] Folman, R., P. Krueger, D. Cassettari, B. Hessmo, T. Maier, and J. Schmiedmayer, "Controlling cold atoms using nanofabricated surfaces: Atom chips," *Physical Review Letters* **84**, 4749–4752 (2000).
- [12] Reichel, J., W. Haenschel, P. Hommelhoff, and T.W. Haensch, "Applications of integrated magnetic microtraps," *Applied Physics B – Lasers and Optics* **72**, 81–89 (2001).
- [13] Mandel, O., M. Greiner, A. Widera, T. Rom, T.W. Haensch, and I. Bloch, "Coherent transport of neutral atoms in spin-dependent optical lattice potentials," *Physical Review Letters* **91**, 010407 (2003).
- [14] Hamann, S.E., D.L. Haycock, G. Klose, P.H. Pax, I.H. Deutsch, and P.S. Jessen, "Resolved-sideband Raman cooling to the ground state of an optical lattice," *Physical Review Letters* **80**, 4149–4152 (1998).
- [15] Greiner, M., O. Mandel, T. Esslinger, T.W. Haensch, and I. Bloch, "Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms," *Nature* **415**, 39–44 (2002).
- [16] Peil, S., J.V. Porto, B. Laburthe-Tolra, J.M. Obrecht, B.E. King, M. Subbotin, S.I. Rolston, and W.D. Phillips, "Patterned loading of a Bose-Einstein condensate into an optical lattice," *Physical Review A* **67**, 051603(R) (2003).
- [17] Scheunemann, R., F.S. Cataliotti, T.W. Haensch, and M. Weitz, "Resolving and addressing atoms in individual sites of a CO₂-laser optical lattice," *Physical Review A* **62**, 051801(R) (2000).
- [18] Scheunemann, R., F.S. Cataliotti, T.W. Haensch, and M. Weitz, "An optical lattice with single lattice site optical control for quantum engineering," *Journal of Optics B - Quantum and Semiclassical Optics* **2**, 645–650 (2000).
- [19] Sauer, J.A., M.D. Barrett, and M.S. Chapman, "Storage ring for neutral atoms," *Physical Review Letters* **87**, 270401 (2001).
- [20] Dumke, R., M. Volk, T. Muether, F.B.J. Buchkremer, G. Birkl, and W. Ertmer "Micro-optical realization of arrays of selectively addressable dipole traps: A scalable configuration for quantum computation with atomic qubits," *Physical Review Letters* **89**, 097903 (2002).
- [21] Perrin, H., A. Kuhn, I. Bouchoule, and C. Salomon, "Sideband cooling of neutral atoms in a far-detuned optical lattice," *Europhysics Letters* **42**, 395–400 (1998).
- [22] Vuletic, V., C. Chin, A.J. Kerman, and S. Chu, "Degenerate Raman sideband cooling of trapped cesium atoms at very high densities," *Physical Review Letters* **81**, 5768–5771 (1998).
- [23] Han, D.J., S. Wolf, S. Oliver, C. McCormick, M.T. Depue, and D.S. Weiss, "3D Raman sideband cooling of cesium atoms at high density," *Physical Review Letters* **85**, 724–727 (2000).

- [24] Brennen, G.K., C.M. Caves, P.S. Jessen, and I.H. Deutsch, “Quantum logic gates in optical lattices,” *Physical Review Letters* **82**, 1060–1063 (1999).
- [25] Brennen, G.K., I.H. Deutsch, and P.S. Jessen, “Entangling dipole-dipole interactions for quantum logic with neutral atoms,” *Physical Review A* **61**, 062309 (2000).
- [26] Brennen, G.K., I.H. Deutsch, and C.J. Williams, “Quantum logic for trapped atoms via molecular hyperfine interactions,” *Physical Review A* **65**, 022313 (2002).
- [27] Jaksch, D., J.I. Cirac, P. Zoller, S.L. Rolston, R. Cote, and M.D. Lukin, “Fast quantum gates for neutral atoms,” *Physical Review Letters* **85**, 2208–2211 (2000). (Rydberg dipole)
- [28] Lukin, M.D., M. Fleischhauer, R. Cote, L.M. Duan, D. Jaksch, J.I. Cirac, and P. Zoller, “Dipole blockade and quantum information processing in mesoscopic atomic ensembles,” *Physical Review Letters* **87**, 037901 (2001).
- [29] Jaksch, D., H.-J. Briegel, J.I. Cirac, C.W. Gardiner, and P. Zoller, “Entanglement of atoms via cold controlled collisions,” *Physical Review Letters* **82**, 1975–1978 (1999).
- [30] Calarco, T., E.A. Hinds, D. Jaksch, J. Schniedmayer, J.I. Cirac, and P. Zoller, “Quantum gates with neutral atoms: controlling collisional interactions in time-dependent traps,” *Physical Review A* **61**, 022304(11) (2000).
- [31] Calarco, T., E.A. Hinds, D. Jaksch, J. Schniedmayer, J.I. Cirac, and P. Zoller, “Quantum gates with neutral atoms: controlling collisional interactions in time-dependent traps,” *Physical Review A* **61**, 022304(11) (2000).
- [32] You, L. and M.S. Chapman, “Quantum entanglement using trapped atomic spins,” *Physical Review A* **62**, 152302 (2000).
- [33] Klose, G., G. Smith, and P.S. Jessen, “Measuring the quantum state of a large angular momentum,” *Physical Review Letters* **86**, 4721–4724 (2001).

Other relevant citations:

Burnett, K., P.S. Julienne, P.D. Leff, E. Tiesinga, and C.J. Williams, “Quantum encounters of the cold kind,” *Nature* **416**, 225–232 (2002).

Deutsch, I.H. and P.S. Jessen, “Quantum-state control in optical lattices,” *Physical Review A* **57**, 1972–1986 (1998).

Friebel, S., C. D’Andrea, J. Walz, M. Weitz, and T.W. Haensch, “CO₂-laser optical lattice with cold rubidium atoms,” *Physical Review A* **57**, R20–R23 (1998).

Greiner, M., O. Mandel, T.W. Haensch, and I. Bloch, “Collapse and revival of the matter wave field of a Bose-Einstein condensate,” *Nature* **419**, 51–54 (2002).

Haycock, D.L., P.M. Alsing, I.H. Deutsch, J. Grondalski, and P.S. Jessen, “Mesoscopic quantum coherence in an optical lattice,” *Physical Review Letters* **85**, 3365–3368 (2000).

Hinds, E.A., M.G. Boshier, and I.G. Hughes, “Magnetic waveguide for trapping cold atoms in two dimensions,” *Physical Review Letters* **80**, 645–649 (1998).

Jaksch, D., C. Bruder, J.I. Cirac, C.W. Gardiner, and P. Zoller, "Cold bosonic atoms in optical lattices," *Physical Review Letters* **81**, 3108–3111 (1998).

Jaksch, D., V. Venturi, J.I. Cirac, C.J. Williams, and P. Zoller, "Creation of a molecular condensate by dynamically melting a Mott insulator," *Physical Review Letters* **89**, 040402 (2002).

Protsenko, I.E., G. Reymond, N. Schlosser, and P. Grangier, "Operation of a quantum phase gate using neutral atoms in microscopic dipole traps," *Physical Review A* **65**, 052301 (2002).

Raithel, G., W.D. Phillips, and S.L. Rolston, "Collapse and revivals of wave packets in optical lattices," *Physical Review Letters* **81**, 3615–3618 (1998).

Rolston, S.L. and W.D. Phillips, "Nonlinear and quantum atom optics," *Nature* **416**, 219–224 (2002).

Schlosser, N., G. Reymond, I. Protsenko, and P. Grangier, "Sub-Poissonian loading of single atoms in a microscopic dipole trap," *Nature* **411**, 1024–1027 (2001).

Sørensen, A. and K. Mølmer, "Spin-spin interaction and spin squeezing in an optical lattice," *Physical Review Letters* **83**, 2274–2277 (1999).

Cavity QED Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.4

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Michael Chapman

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0	Groups Pursuing This Approach	1
2.0	Background and Perspective	1
2.1	Importance to Quantum Information Processing	1
2.2	Types of systems	2
3.0	Summary of Cavity QED QC: The DiVincenzo Criteria.....	2
4.0	What Has Been Accomplished.....	5
5.0	Considerations	6
6.0	Timeline.....	9
7.0	Glossary	9
8.0	References	9

List of Tables and Figures

List of Acronyms and Abbreviations

DFS	decoherence-free subspace
GHZ	Greenberger, Horne, and Zeilinger
LIGO	Laser Interferometer Gravitational Wave Observatory
QC	quantum computation/ computing
QED	quantum electrodynamics
QIP	quantum information processing
rf	radio frequency
TEP	Technology Experts Panel

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Cavity QED (quantum electrodynamics) detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Approaches to Cavity QED QC Research

Research Leader(s)	Research Location	Research Focus
Blatt, R.	U. of Innsbruck	Ca ⁺
Chapman, M.	Georgia Tech	Rb, Ba ⁺
Esslinger, T.	ETH, Zurich	Rb
Feld, M.	MIT	Ba
Haroche, S.	Ecole Normale Supérieure, Paris	Rb (Rydberg)
Kimble, J.	Caltech	Cs
Kuga, T.	U. of Tokyo	Rb
Mabuchi, H.	Caltech	Cs
Meschede, D.	U. of Bonn	Cs
Orozco, L.	U. Maryland	Rb
Rempe, G.	Max-Planck Institute, Garching	Rb
Stamper-Kurn, D.	UC Berkeley	Rb
Walther, H.	Max-Planck Institute, Garching	Ca ⁺

2.0 Background and Perspective

In the context of quantum information ‘cavity QED’ refers to the coherent interaction of a material qubit (such as a trapped atom or semiconductor dot system) with the quantized (usually single photon) field of a high-finesse optical or microwave resonator. To achieve coherent dynamics with just a single photon and atom, a small, extremely low-loss build-up cavity is used to enhance the electric field per photon such that the coherent Rabi frequency of the atom-field interaction is faster than the spontaneous emission rate of the atom or the decay rate of the field in the cavity—this is known as the strong coupling regime. While this is very challenging, this limit has been achieved in ~10 labs over the past 15 years or so in both the microwave and optical domains (see [1,2,3,4,5] for recent overviews).

2.1 Importance to Quantum Information Processing

Applications of cavity QED systems to quantum information processing (QIP) derive mostly from the ability to coherently intra-convert quantum states between material qubits and photon qubits. Using this basic primitive, many two-qubit gate protocols have been developed for

creating atom-photon, atom-atom, or photon-photon entanglements [6,7,8,9,10,11], and proof-of-principle experiments have been performed for some of these ideas [12,13]. Scalable architectures have also been suggested using these gates. More uniquely, cavity QED systems are featured in many ideas relating to distributed quantum information processing and communication [14,15,16,17,18,19,20,21,22,23] and provide a leading candidate for robust, controllable single and multiple photon sources [24,25,26,27,28,29,30]. Additionally, the system provides an attractive method for single atom detection [31,32,33,34,35].

2.2 Types of systems

Rydberg atoms in microwave cavities: the strong coupling limit has been achieved in microwave cavity QED experiments employing highly excited (Rydberg) states of neutral atoms. Some of the cleanest entanglement experiments performed to-date have been in these systems. The major obstacle to this implementation is scaling: microwave cavity QED experiments use atomic beams intersecting the cavity to deliver atoms and hence atomic delivery to the cavity is stochastic.

Neutral atoms in optical cavities: the strong coupling regime is also well-established in the neutral atom work with optical cavities. The principle obstacles to be overcome relate to incorporating a scalable trapping geometry using optical and/or magnetic trapping potentials, while still preserving the strong coupling regime. A key element to this challenge is controlling the atomic motion and atom localization so that the coupling is sufficiently well defined.

Trapped ion cavity QED: recently there has been experimental work incorporating linear ion traps with optical cavities [36,37]. Achieving the strong coupling regime is the major outstanding challenge facing this approach. This requires shrinking the cavity size, without adversely affecting the fields confining the ion.

Other systems: there are several related systems that are actively pursued by different groups. These are listed here, but are not included in this section of the roadmap

- Semiconductor quantum dots systems,
- Solid state ion vacancy systems,
- Superconducting junctions + cavity systems, and
- Neutral atom ensemble (many atom) based cavity QED system.

3.0 Summary of Cavity QED QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits 
 - 1.1 Spin qubits: long-lived hyperfine states suitable for storing quantum information are available both for neutral atom systems and for trapped ion system. The challenges associated with implementing these qubits are largely the same as for the trapped ion and neutral atom approaches reviewed in other sections of the roadmap and the reader is referred to these sections for further discussion. Some of the distinguishing features and unique challenges are highlighted below.
 - 1.1.1 Trapped atoms in cavities: a principle challenge to developing this system is to be able to trap individual atoms/ions and arrays of atoms/ions inside the cavity. This has recently been accomplished for single neutral atoms in cavities in the strong coupling regime [38,39,40,41,42,43], and for trapped ions in the weak coupling regime [36,37]. Single atoms have been distinguishably trapped and translated in one-dimensional arrays (atom conveyors) without cavities [44,45], and single and many atoms have been delivered inside of cavities with similar conveyors [35]. Long-range dipole-dipole forces between distant intracavity atoms (but not in a controlled manner) have been observed in [46].
 - 1.1.2 Photon qubits: cavity QED systems offer photonic or 'flying' qubits as excitations of the cavity mode, or as single photon pulses escaping from through the cavity mirrors. Cavity QED systems can also provide nonlinear photon-photon interactions in the cavity for fields at the single photon level [12]. While optical photons leaking out of the cavity can be readily transported with fibers and can be directly detected efficiently, similarly capabilities are not available in the microwave regime.
 - 1.2 Motional qubits: motional qubits are also available for trapped ion cavity systems. For neutral atom systems, motional qubits are also available in principle, but experimental work is needed to assess their potential. The reader is referred to ion trapping and neutral atom sections of the roadmap for further discussion.
 - 1.3 Scalability: the scalability of cavity QED system faces similar challenges to the trapped ion and neutral atom approaches, with the additional constraint that the qubit trapping system and geometry has to be compatible with the small mode volume of the optical resonator. Translating arrays of atoms or ions can be used to enhance scaling, but at a potential cost in the speed of the system. This is a nontrivial constraint that will possibly limit individual cavity QED systems to smaller numbers than their free-space counterparts. Experiments are on-going to address this challenge [35]. Importantly, the cavity QED system lends itself to a distributed QC architecture, whereby relatively small QC nodes will be interconnected with quantum communication channels (optical fibers).
2. Ability to initialize the state of the qubits to a simple fiducial state 
 - 2.1 Spin qubits: hyperfine states are readily initialized using standard optical pumping techniques widely used in atomic physics
 - 2.2 Motional qubits: motional states of trapped ions and neutral atoms have been initialized by cooling to the ground-state of the trapping potential, however, not yet in cavity QED experiments

- 2.3 Photon qubits: for optical cavities, initialization to the ground state ('vacuum') is trivial—the thermal occupation of an optical cavity is negligible at room temperature.
3. Long (relative) decoherence times, much longer than the gate-operation times 
 - 3.1 Spin coherence
 - 3.1.1 Spin qubit memory: the spin coherence of trapped ions is very long (many minutes) for magnetically insensitive transitions. For neutral atoms, the coherence will be somewhat less due to differential stark shifts from the optical trapping fields [47]
 - 3.1.2 Spin qubit coherence during operations: this relates to the achievement of the strong coupling requirement in cavity QED. This is/ can be satisfied by a factor of 2–50 depending on the details of the cavity dimension and atomic transition.
 - 3.2 Photon qubit coherence during operation: this also relates directly to the strong coupling condition. This has been satisfied by factors ranging from 2–50 in recent experiments.
 - 3.3 Motional coherence: motional decoherence caused by trap fluctuation or environmental noise should be negligible on the time-scale of the gate operation. Motional decoherence caused by the gate operation itself needs to be further addressed theoretically [48,49,50] and evaluated experimentally.
4. Universal set of quantum gates 
 - 4.1 Single-bit rotations: these can be accomplished with excellent fidelity. These operations are not limited by qubit decoherence, but rather by external noise, noise in the driving field and differential stark shifts (in the case of neutral atom optical traps) [45,47]
 - 4.2 Photon-photon phase gates: several gates have been proposed, and there has been a proof-of-principle demonstration using weak coherent states [12]
 - 4.3 Atom-atom gates: several gates have been proposed [6–8,10,11] and there has been a demonstration experiment in the microwave domain [13]. Gate 'success' rates exceeding 90% are possible based on parameters in current experiments—employing high-efficiency photon detection to measure cavity decay can yield effective fidelities exceeding 99% [6,8,11]. Success rates are very dependent on the cavity geometry and mirror quality—the compromise between the small cavities for strong coupling and allowing for sufficient space for incorporating qubit arrays is a critical aspect of these systems.
 - 4.4 Atom-photon gates: many of the photon-photon and atom-atom gates can be adapted to atom-photon entanglements
5. A qubit-specific measurement capability 
 - 5.1 Both individual neutral atoms [45] and trapped ions have been detected in state-sensitive means.
 - 5.2 Cavity QED itself provides an excellent single atom detector that could be employed in other neutral atom-based systems [31–35]

6. The ability to interconvert stationary and flying qubits 
 - 6.1 This is one of the strongest potential applications of cavity QED. The coherent dynamics of the atom—photon interaction has been one of the cornerstones of the field of quantum optics for the last 40 years.
7. The ability to faithfully transmit flying qubits between specified locations 
 - 7.1 Photonic (optical) qubits are readily transported between sites using fibers.

4.0 What Has Been Accomplished

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states 
 - 1.1.1 This has been accomplished for both trapped ion and neutral atom systems, although not in an experimental set-up with a cavity. In microwave cavity QED systems, single qubit preparation and readout has been accomplished for atoms transiting the cavity.
 - 1.1.2 Single photon ‘guns’ have been created in atom-cavity systems in both the optical [29,30] and microwave domains [27,28].
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit 
 - 2.1.1 Rabi flops are readily observed for single trapped ions (see Ion Trap section of Roadmap), and more recently, single trapped neutral atoms [45]
 - 2.2 Demonstrate high-Q of qubit transition 
 - 2.2.1 Extremely high Q’s have been observed in hyperfine transitions, and qubit coherence on the order of seconds to minutes is realistically achieved with proper control of external fields.
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere 
3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operation 
 - 3.1.1 In optical cavity QED, a quantum phase gate has been realized for weak coherent optical fields [12]. A quantum phase gate has also been realized in the microwave domain [13,51]. Both of these experiments utilized atomic beams to provide the atoms.

- 3.2 Produce and characterize Bell states 
 - 3.2.1 Atom-field Bell states have been produced and measured in a microwave cavity system[52]
- 3.3 Demonstrate decoherence times much longer than two-qubit gate times 
- 3.4 Demonstrate quantum state and process tomography for two qubits.
- 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS).
- 3.6 Demonstrate a two-qubit quantum algorithm
- 4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, and Zeilinger (GHZ) entangled state of three physical qubits. 
 - 4.1.1 GHZ states have been prepared in a microwave cavity QED system[53]
 - 4.2 Produce maximally entangled states of four and more physical qubits. 
 - 4.3 Quantum state and process tomography. 
 - 4.4 Demonstrate DFSs. 
 - 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations etc.) between physical qubits. 
 - 4.6 Demonstrate quantum error-correcting codes. 
 - 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
 - 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
- 5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
- 6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
- 7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally-entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

- 1. Special strengths
 - 1.1 Ability to interconvert material and photonic qubits

- 1.2 Source of deterministic single photons and entangled photons
 - 1.3 Cavity QED systems provide viable platforms for distributed quantum computing implementations for both neutral atom and trapped ions
 - 1.4 Well understood systems from a theoretical standpoint. The cavity QED system has been an important paradigm of quantum optics
2. Unknowns, weaknesses
 - 2.1 Ultimate performance of systems is dependent on advances in mirror coating and polishing technologies. Current mirror reflectivities, while adequate to achieve the strong coupling limit, are still ~ 100 times lower than the theoretical limit imposed by Rayleigh scattering in the coating. Additionally, smaller mirror curvature would provide for large coherent coupling rates.
 - 2.2 The role of the atomic motional degree of freedom in the cavity gate operation and subsequent evolution needs to be better understood both experimentally and theoretically, see e.g. [48–50, 54].
 - 2.3 Other emerging cavity technologies such as whispering gallery mode cavities [55,56] and photonic band gap cavities [57] may provide for stronger coupling and better performance.
 - 2.4 Strategies for control of Rydberg atom localization and control in microwave cavity QED systems need to be developed. It is possible that advances in technology from Rydberg direct atom-atom coupling approaches (discussed in the neutral atom section of the roadmap) could be adapted for the cavity QED system
3. Goals 2002–2007
 - 3.1 Demonstrate high quality single photon generator
 - 3.2 Achieve deterministic entanglement between atoms/ions and photons in optical cavity QED
 - 3.3 Achieve deterministic entanglement between two atoms or ions using the cavity field
4. Goals 2007–2012
 - 4.1 Demonstrate high quality entangled photon pair generator
 - 4.2 Distribute entanglement between two cavity QED based systems
 - 4.3 Demonstrate scalability of system
5. Necessary achievements
 - 5.1 Demonstrate qubit array storage in neutral cavity QED system
 - 5.2 Achieve strong coupling limit in ion trap cavity QED systems
 - 5.3 Further develop mirror technology to increase mirror reflectivity and reduce the mode volume by reducing the mirror curvature
6. Trophies
 - 6.1 Demonstration of a deterministic single photon gun
 - 6.2 Demonstration of atom-field entanglement in an optical cavity QED system
 - 6.3 Demonstration of atom-atom entanglement in an optical cavity QED system

- 6.4 Demonstration of a deterministic entangled photon source
- 6.5 Demonstration of entanglement distribution between two cavity systems
- 7. Connections with other quantum information science technologies
 - 7.1 Cavity QED is a universal paradigm for intra-converting material-based and photonic-based quantum information
 - 7.2 Cavity QED systems are some of the cleanest, best-understood 'open' quantum systems to be studied. The lessons learned in cavity QED systems will be widely applicable across different QI implementations
- 8. Subsidiary developments
 - 8.1 Improvements in cavity technology will lead to more accurate optical clocks and positively impact a host of precision measurements in both fundamental and applied physics (e.g. LIGO, precision spectroscopy, inertial sensing).
 - 8.2 Development of high quality optical polishing and coating technologies that will benefit many laser based industrial applications.
 - 8.3 Improved atomic control can be used to improve atomic clock technologies
- 9. Role of theory
 - 9.1 The cavity QED system is one of the foundations of quantum optics. Theoretical research in this field has been prodigious and the general methods and formalisms developed are applicable to many physical implementations of QIP systems.
 - 9.2 Investigate different 2-qubit gate protocols
 - 9.3 Develop error-correcting protocols adapted to the decoherence mechanisms specific to the cavity QED system
 - 9.4 Explore distributed QC architectures employing photonic quantum communication
 - 9.5 Develop and analyze algorithms and architectures specifically tailored to cavity QED systems

6.0 Timeline

1. Timeline for 2002–2007
 - 1.1 Refer to the Excel timeline chart below and #3 of “Considerations” (above).
2. Timeline for 2007–2012
 - 2.1 Refer to the Excel timeline chart below and #4 of “Considerations” (above).

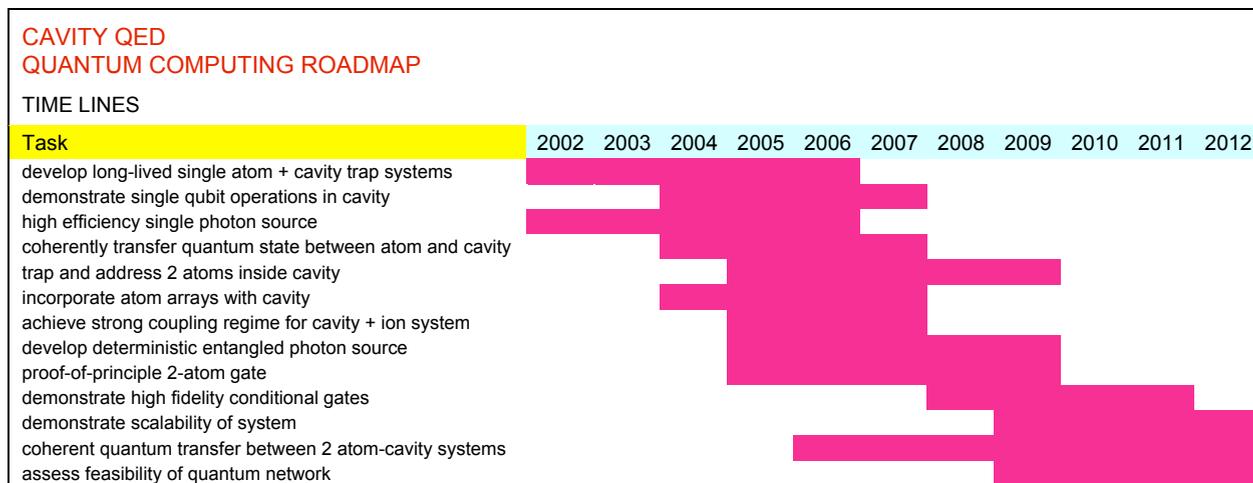


Figure 6-1. Cavity QED QC developmental timeline

7.0 Glossary

8.0 References

- [1] *Cavity Quantum Electrodynamics*, P. Berman, Ed. (Academic Press, Boston, MA, 1994).
- [2] Mabuchi, H. and A.C. Doherty, “Cavity quantum electrodynamics: Coherence in context,” *Science* **298**, 1372–1377 (2002).
- [3] Raimond, J.M., M. Brune, and S. Haroche, “Colloquium: Manipulating quantum entanglement with atoms and photons in a cavity,” *Reviews of Modern Physics* **73**, 565–582 (2001).
- [4] Walther, H., “Generation of photon number states on demand,” *Fortschritte Der Physik (Progress of Physics)* **51**, 521–530 (2003).
- [5] Walther, H., “Generation and detection of Fock-states of the radiation field,” *Zeitschrift Fur Naturforschung Section A (Journal of Physical Sciences-A)* **56**, 117–123 (2001).
- [6] Pellizzari, T., S.A. Gardiner, J.I. Cirac, and P. Zoller, “Decoherence, continuous observation, and quantum computing: A cavity QED model,” *Physical Review Letters* **75**, 3788–3791 (1995).

- [7] van Enk, S.J., J.I. Cirac, and P. Zoller, "Purifying two-bit quantum gates and joint measurements in cavity QED," *Physical Review Letters* **79**, 5178–5181 (1997).
- [8] Pachos, J. and H. Walther, "Quantum computation with trapped ions in an optical cavity," *Physical Review Letters* **89**, 187903 (2002).
- [9] Duan, L.M., A. Kuzmich, and H.J. Kimble, "Cavity QED and quantum-information processing with "hot" trapped atoms," *Physical Review A* **67**, 032305 (2003).
- [10] Yi, X.X., X.H. Su, and L. You, "Conditional quantum phase gate between two 3-state atoms," *Physical Review Letters* **90**, 097902 (2003).
- [11] You, L., X.X. Yi, and X.H. Su, "Quantum logic between atoms inside a high-Q optical cavity," *Physical Review A* **67**, 032308 (2003).
- [12] Turchette, Q.A., C.J. Hood, W. Lange, H. Mabuchi, and H.J. Kimble, "Measurement of Conditional Phase-Shifts for Quantum Logic," *Physical Review Letters* **75**, 4710–4713 (1995).
- [13] Rauschenbeutel, A., G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.M. Raimond, and S. Haroche, "Coherent operation of a tunable quantum phase gate in cavity QED," *Physical Review Letters* **83**, 5166–5169 (1999).
- [14] Cirac, J.I., P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Physical Review Letters* **78**, 3221–3224 (1997).
- [15] van Enk, S.J., J.I. Cirac, P. Zoller, H.J. Kimble and H. Mabuchi, "Quantum state transfer in a quantum network: a quantum-optical implementation," *Journal of Modern Optics* **44**, 1727–1736 (1997).
- [16] van Enk, S.J., J.I. Cirac, and P. Zoller, "Ideal quantum communication over noisy channels: A quantum optical implementation," *Physical Review Letters* **78**, 4293–4296 (1997).
- [17] Briegel, H.J., W. Dür, J.I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters* **81**, 5932–5935 (1998).
- [18] Briegel, H.J., W. Dür, S.J. van Enk, J.I. Cirac, and P. Zoller, "Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel," *Philosophical Transactions of the Royal Society of London Series A-Mathematical, Physical, and Engineering Sciences* **356**, 1841–1851 (1998).
- [19] Cirac, J.I., S.J. van Enk, P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum communication in a quantum network," *Physica Scripta* **T76**, 223–232 (1998).
- [20] van Enk, S.J., J.I. Cirac, and P. Zoller, "Photonic channels for quantum communication," *Science* **279**, 205–208 (1998).
- [21] Briegel, H.J., J.I. Cirac, W. Dür, S.J. van Enk, H.J. Kimble, H. Mabuchi, and P. Zoller, "Physical implementations for quantum communication in quantum networks," *Quantum Computing and Quantum Communications* **1509**, 373–382 (1999).

- [22] Gheri, K.M., P. Torma, and P. Zoller, "Quantum state engineering with photonic qubits," *Acta Physica Slovaca* **49**, 523–532 (1999).
- [23] van Enk, S.J., H.J. Kimble, J.I. Cirac, and P. Zoller, "Quantum communication with dark photons," *Physical Review A* **59**, 2659–2664 (1999).
- [24] Kuhn, A., M. Hennrich, T. Bundo, and G. Rempe, "Controlled generation of single photons from a strongly coupled atom-cavity system," *Applied Physics B* **69**, 373–377 (1999).
- [25] Law, C.K. and H.J. Kimble, "Deterministic generation of a bit-stream of single-photon pulses," *Journal of Modern Optics* **44**, 2067–2074 (1997).
- [26] Lange, W. and H.J. Kimble, "Dynamic generation of maximally entangled photon multiplets by adiabatic passage," *Physical Review A* **61**, 063817 (2000).
- [27] Varcoe, B.T.H., S. Brattke, M. Weidinger, and H. Walther, "Preparing pure photon number states of the radiation field," *Nature* **403**, 743–746 (2000).
- [28] Bertet, P., S. Osnaghi, P. Milman, A. Auffeves, P. Maioli, M. Brune, J.M. Raimond, and S. Haroche, "Generating and probing a two-photon Fock state with a single atom in a cavity," *Physical Review Letters* **88**, 143601 (2002).
- [29] Kuhn, A., M. Hennrich, and G. Rempe, "Deterministic single-photon source for distributed quantum networking," *Physical Review Letters* **89**, 067901 (2002).
- [30] McKeever, J., A. Boca, A.D. Boozer, R. Miller, J.R. Buck, A. Kuzmich, and H.J. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity," *Science* **303**, 1992–1994 (2004).
- [31] Mabuchi, H., Q.A. Turchette, M.S. Chapman, and H.J. Kimble, "Real-time detection of individual atoms falling through a high-finesse optical cavity," *Optics Letters* **21**, 1393–1395 (1996).
- [32] Hood, C.J., M.S. Chapman, T.W. Lynn, and H.J. Kimble, "Real-time cavity QED with single atoms," *Physical Review Letters* **80**, 4157–4160 (1998).
- [33] Munstermann, P., T. Fischer, P.W.H. Pinkse, and G. Rempe, "Single slow atoms from an atomic fountain observed in a high-finesse optical cavity," *Optics Communications* **159**, 63–67 (1999).
- [34] Shimizu, Y., N. Shiokawa, N. Yamamoto, M. Kozuma, T. Kuga, L. Deng, and E.W. Hagley, "Control of light pulse propagation with only a few cold atoms in a high-finesse microcavity," *Physical Review Letters* **89**, 233001 (2002).
- [35] Sauer, J.A., K.M. Fortier, M.S. Chang, C.D. Hamley, and M.S. Chapman, "Cavity QED with optically transported atoms," (4-Sep-03) preprint *quant-ph/0309052*.
- [36] Guthohrlein, G.R., M. Keller, K. Hayasaka, W. Lange, and H. Walther, "A single ion as a nanoscopic probe of an optical field," *Nature* **414**, 49–51 (2001).

- [37] Mundt, A.B., A. Kreuter, C. Becher, D. Leibfried, J. Eschner, F. Schmidt-Kaler, and R. Blatt, "Coupling a single atomic quantum bit to a high finesse optical cavity," *Physical Review Letters* **89**, 103001 (2002).
- [38] Ye, J., D.W. Vernooy, and H.J. Kimble, "Trapping of single atoms in cavity QED," *Physical Review Letters* **83**, 4987–4990 (1999).
- [39] Hood, C.J., T.W. Lynn, A.C. Doherty, D.W. Vernooy, J. Ye, and H.J. Kimble, "Single atoms bound in orbit by single photons," *Laser Physics* **11**, 1190–1192 (2001).
- [40] Pinkse, P.W.H., T. Fischer, P. Maunz, and G. Rempe, "Trapping an atom with single photons," *Nature* **404**, 365–368 (2000).
- [41] Fischer, T., P. Maunz, P.W.H. Pinkse, T. Puppe, and G. Rempe, "Feedback on the motion of a single atom in an optical cavity," *Physical Review Letters* **88**, 163002 (2002).
- [42] McKeever, J., A. Boca, A.D. Boozer, J.R. Buck, and H.J. Kimble, "Experimental realization of a one-atom laser in the regime of strong coupling," *Nature* **425**, 268–271 (2003).
- [43] McKeever, J., J.R. Buck, A.D. Boozer, A. Kuzmich, H.-C. Nägerl, D.M. Stamper-Kurn, and H.J. Kimble, "State-insensitive cooling and trapping of single atoms in an optical cavity," *Physical Review Letters* **90**, 133602 (2003).
- [44] Schrader, D., S. Kuhr, W. Alt, M. Müller, V. Gomer, and D. Meschede, "An optical conveyor belt for single neutral atoms," *Applied Physics B-Lasers and Optics* **73**, 819–824 (2001).
- [45] Kuhr, S., W. Alt, D. Schrader, I. Dotsenko, Y. Miroshnychenko, W. Rosenfeld, M. Khudaverdyan, V. Gomer, A. Rauschenbeutel, and D. Meschede, "Coherence properties and quantum state transportation in an optical conveyor belt," *Physical Review Letters* **91**, 213002 (2003).
- [46] Münstermann, P., T. Fischer, P. Maunz, P.W.H. Pinkse, and G. Rempe, "Observation of cavity-mediated long-range light forces between strongly coupled atoms," *Physical Review Letters* **84**, 4068–4071 (2000).
- [47] Kaplan, A., M.F. Andersen, and N. Davidson, "Suppression of inhomogeneous broadening in rf spectroscopy of optically trapped atoms," *Physical Review A* **66**, 045401 (2002).
- [48] Vernooy, D.W. and H.J. Kimble, "Well-dressed states for wave-packet dynamics in cavity QED," *Physical Review A* **56**, 4287–4295 (1997).
- [49] Doherty, A.C., A.S. Parkins, S.M. Tan, and D.F. Walls, "Effects of motion in cavity QED," *Journal of Optics B-Quantum and Semiclassical Optics* **1**, 475–482 (1999).
- [50] You, L., "Motional effects of trapped atomic or ionic qubits," *Physical Review A* **64**, 012302 (2001).

- [51] Rauschenbeutel, A., P. Bertet, S. Osnaghi, G. Nogues, M. Brune, J.M. Raimond, and S. Haroche, "Controlled entanglement of two field modes in a cavity quantum electrodynamics experiment," *Physical Review A* **64**, 050301 (2001).
- [52] Hagley, E., X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond, and S. Haroche, "Generation of Einstein-Podolsky-Rosen pairs of atoms," *Physical Review Letters* **79**, 1–5 (1997).
- [53] Rauschenbeutel, A., G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.-M. Raimond, and S. Haroche, "Step-by-step engineered multiparticle entanglement," *Science* **288**, 2024–2028 (2000).
- [54] Münstermann, P., T. Fischer, P. Maunz, P.W.H. Pinkse, and G. Rempe, "Dynamics of single-atom motion observed in a high-finesse cavity," *Physical Review Letters* **82**, 3791–3794 (1999).
- [55] Ilchenko, V.S., P.S. Volikov, V.L. Velichansky, F. Treussart, V. Lefèvre-Seguin, J.-M. Raimond, and S. Haroche, "Strain-tunable high-Q optical microsphere resonator," *Optics Communications* **145**, 86–90 (1998).
- [56] Buck, J.R. and H.J. Kimble, "Optimal sizes of dielectric microspheres for cavity QED with strong coupling," *Physical Review A* **67**, 033806 (2003).
- [57] Vuckovic, J., M. Lonar, H. Mabuchi, and A. Scherer, "Design of photonic crystal microcavities for cavity QED," *Physical Review E* **65**, 016608 (2002).

Optical Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.5

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Paul Kwiat and Gerard Milburn

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0 Groups Pursuing This Approach	1
2.0 Background and Perspective	1
3.0 Summary of Optical QC: The DiVincenzo Criteria	3
4.0 What Has Been Accomplished	5
5.0 Considerations	8
6.0 Timeline	11
7.0 Glossary	14
8.0 References	15

List of Tables and Figures

Table 1-1 Optical QC Research	1
Figure 6-1. Optical QC developmental timeline	14

List of Acronyms and Abbreviations

C-NOT	controlled-not (gate)	QIP	quantum information processing
DFS	decoherence-free subspace	QED	quantum electrodynamics
GHZ	Greenberger, Horne, and Zeilinger	SPD	single-photon detector
HOM	Hong, Ou, and Mandel	SPS	single-photon source
KLM	Knill, Laflamme, and Milburn	SPDC	spontaneous parametric down conversion
LOQC	linear-optics quantum computing	TEP	Technology Experts Panel
QC	quantum computation/computing		

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Optical detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Optical QC Research

Research Leader(s)	Research Location
Bouwmeester, D.	U. of California, Santa Barbara, USA
DeMartini, F.	Rome U., Italy
Dowling, J.	JPL, California, USA
Franson, J. D.	John Hopkins, Maryland, USA
Gisin, N.	U. of Geneva, Switzerland
Howell, J. C.	U. of Rochester, New York, USA
Imamoglu, A.	U. of California, Santa Barbara, USA
Kwiat, P. G.	U. of Illinois, Urbana-Champaign, USA
Milburn, G. J. and Ralph, T. C.	U. of Queensland, Australia
Nakamura, J.	NEC, Tsukuba, Japan
Rarity, J.	U. of Bristol, UK
Sergienko, A. V.	Boston U., Massachusetts, USA
Shih, Y. H.	UMBC, Maryland, USA
Steinberg, A.	U. of Toronto, Canada
Takeuchi, S.	Hokkaido U., Japan
Walmsley, I.	U. of Oxford, UK
Weinfurter, H.	U. of Munich, Germany
White, A. G.	U. of Queensland, Brisbane Australia
Yamamoto, Y.	Stanford U., California, USA
Zeilinger, A.	U. of Vienna, Austria
A European collaboration (RAMBOQ)*	John Rarity (coordinator), U. of Bristol

* This collaboration has been funded in the current round of the FET QIPC scheme of the European Commission.

2.0 Background and Perspective

Optical implementations of qubits have played an important role for quantum information science. In addition to their successful application for experimentally realizing quantum cryptography [1], photonic qubits have been among the first physical systems to enable the realization of multiparticle entanglement [2,3,4,5,6], quantum-state [7,8] and quantum-process tomography [9,10,11,12,13,14], teleportation [15,16,17,18,19,20], decoherence-free subspaces (DFSs) [21,22], and even simple quantum algorithms [23,24,25,26,27,28]. Photons have an intrinsic

lack of decoherence, as well as an extreme precision with which they may be controlled using standard off-the-shelf components. For these reasons, optical qubits have played, and will continue to play, an important role in investigating foundations of quantum information processing (QIP), and fundamentals of QC in systems with small numbers of qubits. Photonic qubits for QC are particularly attractive because they could interface immediately to various quantum-communication applications (e.g., distributed QC).

Due to the extremely small photon-photon coupling available in existing materials, it was at one point believed that optical qubits could never be used for scalable QC. However, recent advances with slow light [29,30,31] and “stopped” light [32,33] indicate that these limitations may be overcome [34]. In addition, interesting results have appeared, which indicate that light which is initially prepared in a nonclassical “squeezed” state may enable additional gains for QIP (so called “continuous variable” encoding) [35,36]. Finally, it is now understood that the process of photo detection itself can lead to effective photon-photon nonlinearities [37]. For example, it has been shown in the Knill, Laflamme, and Milburn (KLM) scheme [38] that deterministic single-photon sources (SPSs) and high-efficiency single-photon detectors (SPDs) may be used to realize scalable QC with only linear optical elements. Below, we concentrate on this scheme as an example of optical QC. However, it should be emphasized that other approaches are also being followed, and may be critical for the overall progress toward scalable QC, even if these other approaches do not themselves realize it. For example, hybrid schemes involving qubits, qudits, and continuous variables, as can be realized in optical systems, have interesting and important properties—some of them display “hyper-entanglement” (simultaneous entanglement in multiple degrees of freedom), which may facilitate certain tasks in quantum information processing [39,40], such as purification and quantum error correction. Similarly, optical systems can be used to explicitly study decoherence in a controlled manner and to implement proposals for avoiding the negative effects of decoherence (e.g., DFSs). It is a feature of optically encoded qubits that decoherence can be controllably introduced by artificially coupling the qubit to other degrees of freedom [21]. This feature allows optically based systems to simulate other qubit realizations in a very clean, controllable way.

Linear optics quantum computing (LOQC) is a scheme for QIP using linear optics, SPSs, and SPDs [38]. A number of authors have suggested simplifications and modifications of the original scheme [41,42,43,44]. We take a broader view of optical QC that may also include nonlinear elements as a crucial component, provided those nonlinear elements are readily available or under development (e.g., entangled state via spontaneous parametric down conversion [SPDC], quantum memories, etc.). A number of simple experiments have been done to test the most elementary components of the scheme [45,46,47,48,49]. All of these use SPDC sources which require that experiments be done in a post-selective manner using multicoincidence detection. Further progress in the KLM scheme will require on-demand SPSs and very efficient discriminating SPDs. One of the main challenges in an LOQC approach may be the generation of the required entangled ancilla states. This becomes especially difficult if the detector efficiency is low (less than 99%). Hence, development of entanglement sources could play a key role in achieving LOQC. In addition, other alternative schemes (not based on single-photon states) have been proposed [36,50].

3.0 Summary of Optical QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits 
 - 1.1 Qubits in the KLM scheme are represented by single-photon occupation of one mode of a pair of optical modes (dual rail logic). The two modes can be polarization modes. Other schemes using the state of a single mode are possible (e.g., coherent-state encoding represents different logical states with different coherent amplitudes in a single mode and single-mode photon number state codes also exist).
2. The ability to initialize the state of the qubits to a simple fiducial state 
 - 2.1 Initialization of the qubits requires fast, reliable, periodic (on-demand) SPSs. Each pulse must contain one and only one photon. It must be possible to demonstrate nonclassical interference (e.g., a Hong, Ou, and Mandel [HOM] interferometer [51]) between two single-photon pulses.
3. Long (relative) decoherence times, much longer than the gate-operation time 
 - 3.1 Single-qubit gate times are determined by the time it takes light to pass through an optical element, typically less than a picosecond. Two-qubit gate times depend on the time taken to implement a teleportation protocol. Some of these gates have been demonstrated in a post-selected mode, or conditional mode, but gates “on-demand” have not yet been demonstrated. Typically, these gates would operate on the order of nanoseconds. At optical frequencies, the effective temperature of the electromagnetic environment is zero ($kT \ll \hbar\omega$). However, although the coupling of the qubits to the thermal environment is weak, photons are easily lost to the system. Imperfect optical elements (e.g., beam splitters, waveplates, and phase shifters) are possible sources of decoherence, and these effects have yet to be completely determined. Imperfect mode matching, which is formally equivalent to photon loss, is a more serious problem. Sources of decoherence or error are:
 - interferometric stability,
 - mode matching (both spatial and temporal),
 - photon loss, and
 - detector accuracy and efficiency.

The error probability per gate can be estimated by examining the extent to which current interferometers can be stabilized and mode matched. With current technology this is approximately 0.1% for one-photon interference and 1% for two-photon interference. The photon loss per gate can be made less than 0.001. Preliminary

calculations indicate that source and detector inefficiencies have a similar effect on the net gate fidelity [52]. These will need to be better than 99% for a fault-tolerant implementation, which is beyond the reach of current devices.

If gates are realized in terms of optical-fiber couplers or planar-integrated optical devices, mode-matching stability will be better than free-space devices; however, losses in the devices and at interfaces may be more of an issue and will still need to be minimized.

4. A universal set of quantum gates

4.1 Single-qubit operations are performed by linear elements such as beam splitters, polarization rotators, and phase shifters. Two-qubit interactions are induced conditionally by measurement of photon number in LOQC. However, teleportation gates will require very fast electro-optic control systems or photon storage. Solutions in this area will have direct relevance to current problems in conventional photonic switching technologies for optical communication systems.

4.2 Methods for generating prior entanglement are available with current technology, though not for producing entanglement on demand. Prior entanglement is useful for implementing particular error-correction codes, and may also be a method to substantially reduce gate complexity. In the long term, integrated optical devices and elementary interferometer modules will need to be developed to replace currently bulky elements. For example, a planar optical waveguide could be used to replace the four-port beam splitters used in the KLM scheme. Such devices could be made highly compact using photonic band-gap techniques and integration with SPSs.

5. A qubit-specific measurement capability

5.1 Fault-tolerant implementation of LOQC requires high efficiency (greater than 99%), discriminating, single-photon devices. While such devices have never been demonstrated, much progress has been made toward their realization [53,54,55,56]. It may be necessary to investigate novel photodetectors based on cavity quantum electrodynamics (QED) and atomic systems; feasible proposals have recently appeared [57,58].

6. The ability to interconvert stationary and flying qubits

6.1 Optical schemes can interface to solid-state systems via electro-optic devices such as exciton quantum dots. No detailed scheme has been demonstrated that uses such an interface. Some theoretical work has been done on interconverting electronic quantum information to optical entanglement [59,60]. Optical schemes can also interface to atomic schemes, either in high-finesse cavities [61,62] or using “slow-light” schemes in atomic vapor [34].

7. The ability to faithfully transmit flying qubits between specified locations

7.1 For free-space propagation of photons, this requirement is relatively straightforward to accomplish. However, it is necessary to have well-defined mode structure so that good mode matching can be achieved at beam splitters. In optical fibers, photon loss must be accounted for over distances of more than a few meters; experimentally demonstrated

quantum key-distribution protocols give confidence that this is not a serious problem. Implementations that exploit propagation in a photonic band-gap waveguides are possible—but have not yet been demonstrated.

4.0 What Has Been Accomplished

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit

1.1 Demonstrate preparation and readout of both qubit states.

- 1.1.1 These requirements have been accomplished to some extent using conditional single-photon states from SPDC and post-selection [7,63,64,65]. Precision state tomography has been demonstrated [8]. The first electrically driven single-photon sources (SPSs) were based on a Coulomb blockade effect in a p-n junction [66]. More recently, promising results from single quantum dots have been reported [67,68,69,70]; however, the lowest achieved error (probability of something other than one photon) is still $\sim 60\%$. Single nitrogen vacancies in diamond have demonstrated photon antibunching, but the output collection efficiency (less than 5%) and large spectral bandwidth (~ 100 nm) make these unlikely candidates for LOQC [71,72]. Finally, some work has been reported using single atoms in a high-finesse cavity (as in the cavity QED QC schemes); at present the outcoupling efficiency is again only $\sim 8\%$ [73,74].
- 1.1.2 SPDs with efficiencies of 88% (and predicted to be as high as 95%) have been demonstrated. These detectors have some ability to distinguish incident photon number [53–55]. Superconducting detectors with excellent resolving characteristics have been reported, but their detection efficiency is still low (20%); increases to 80% have been predicted [75].
- 1.1.3 Suggestions for greater than 99%-efficient detectors with photon-number resolving capability have been proposed, based on coupling to atomic systems [53–56]. Similar schemes for photon quantum memories have been discussed [76]. A simple proof-of-principle optical storage cavity has been demonstrated, reporting storage times of ~ 50 ns to 1 microsecond [48,49]; technical improvements may increase this to 10s or even 100s of microseconds.

2. Single-qubit operations

2.1 Demonstrate Rabi flops of a qubit.

- 2.1.1 Single-photon gates only require a beam splitter with a variable-reflectivity amplitude. For polarization-based dual-rail encoding, single-qubit rotations are easily implemented [77] and performed routinely. A simple feed-forward control

has been demonstrated using SPDC [46], as well as a basic quantum memory (photon storage) [48,49].

- 2.1.2 It would be more difficult to perform a single Rabi flop on a logical qubit encoded in two or more physical qubits in this scheme, although it would depend on how the code was implemented.

2.2 Demonstrate decoherence times much longer than Rabi oscillation.

- 2.2.1 For a single-qubit gate based on a beam splitter, a huge number of ‘Rabi flops’ (single-qubit rotations) could be performed before dephasing or photon loss become a problem. Similarly, a polarization qubit can be transformed with essentially no decoherence.

2.3 Demonstrate control of both degrees of freedom on the Bloch sphere.

- 2.3.1 In both interferometric schemes, and also polarization qubit schemes, arbitrary transformations of qubits have been demonstrated. Recently, single-qubit, entanglement-assisted, and ancilla-assisted quantum process tomography [9,10] have been demonstrated [11–14].

3. Two-qubit operations

3.1 Implement coherent two-qubit quantum logic operations.

- 3.1.1 A nonuniversal two-qubit gate based on SPDC and post selection has been partially achieved [45,47]. In addition, various simple quantum algorithms have been implemented using linear optical systems [23–28,78]. However, much work needs to be done before this is accomplished in a way suitable for scaling. Further progress awaits good SPSs and SPDs. Recently, independently generated single photons (from a quantum dot) were made to demonstrate two-photon HOM interference [79], and independent photons from down-conversion were observed to violate a Bell’s inequality [80].

3.2 Produce and characterize Bell states.

- 3.2.1 This has already been achieved using SPDC and linear optics [2–8]; however, the methods are based on post selection. A major challenge is to use LOQC methods to generate and characterize Bell states on demand without post selection. This requires SPSs or entanglement-on-demand sources.

3.3 Demonstrate decoherence times much longer than two-qubit gate times.

- 3.3.1 A typical two-qubit gate may be characterized by the time for photons to propagate through their interferometric gates (less than 1 ns); the time they need to be stored while waiting for a photodetection event (about 50 ns, when all circuitry is accounted for); and the time they will need to be stored while waiting for the next single-photon pulse (still hundreds of nanoseconds). These sorts of storage times are routinely achieved in high-finesse optical cavities.

- 3.4 Demonstrate quantum state and process tomography for two qubits. 
 - 3.4.1 State tomography for one and two qubits, and process tomography for single-qubit processes has been demonstrated [7,8,11–14,81].
- 3.5 Demonstrate a two-qubit DFS. 
 - 3.5.1 The optical demonstration of DFSs has been achieved for two qubits [21,22,82].
- 3.6 Demonstrate a two-qubit quantum algorithm. 
 - 3.6.1 Several simple quantum algorithms have been implemented using optical qubits: Deutsch-Josza [24,25], Grover [23,26], quantum Baker's map [27,28]. While these systems are not scalable, they allow one to investigate the fundamentals of quantum algorithms, and may also allow one to investigate the incorporation of various decoherence-avoidance/correction techniques.
- 4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, & Zeilinger (GHZ) state of three physical qubits. 
 - 4.1.1 This production has already been achieved using SPDC and post selection with linear optics [83]. A major challenge is to generate and characterize GHZ states on demand using LOQC methods and SPSs.
 - 4.2 Produce maximally entangled states of four or more physical qubits. 
 - 4.3 Quantum state and process tomography. 
 - 4.4 Demonstrate DFSs. 
 - 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
 - 4.5.1 This has been partially achieved using post selection and in the continuous variable system [15–20], but not yet in the LOQC scheme, although the protocols for doing so are well understood.
 - 4.6 Demonstrate quantum error-correcting codes. 
 - 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
 - 4.7.1 The Deutsch-Jozsa algorithm has been implemented with 3 qubits [24,25]. Also, Grover's search algorithm has been implemented with ~10 qubits [26].
 - 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
- 5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit (DFS work). 
 - 5.2.1 Same as in Section 3.5, above [82].

6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ state of three logical qubits. 
 - 7.2 Produce maximally entangled states of four or more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. This has been achieved for two qubits encoded in a decoherence-free subspace [82]. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

1. Special strengths
 - 1.1 Well understood physics.
 - 1.2 Very precise single-qubit operations.
 - 1.3 Very low intrinsic decoherence.
 - 1.4 Much off-the-shelf technology is available.
 - 1.5 Directly compatible with quantum communication and scale-up path may be available using planar integrated optics or photonic band-gap technology.
2. Unknowns, weaknesses
 - 2.1 Unknowns
 - 2.1.1 We need a realistic assessment of the resource requirements for a nontrivial implementation (e.g., a five-qubit error correction [or CS5]).
 - 2.1.2 We need a realistic statement of what is possible with (nearly) existing technology.
 - 2.1.3 We should understand the equivalent nonlinearity for a given detection efficiency.
 - 2.1.4 We need to develop the design rules for scaling up an integrated device.
 - 2.1.5 The possible advantages of employing “special” quantum states (e.g., hyperentangled states simultaneously entangled in multiple degrees of freedom, bound entangled states, or maximally entangled mixed states).
 - 2.1 Weaknesses
 - 2.2.1 A reliable, periodic SPS has not been demonstrated.

- 2.2.2 Discriminating SPDs with demonstrated efficiency $>99\%$ have not been demonstrated.
 - 2.2.3 It is difficult to mode-match and stabilize very many, multiply nested, interferometers.
 - 2.2.4 The scheme requires photon detection and fast electro-optic feed-forward control of optical switches on a time scale of nanoseconds. It may become possible to reduce the bandwidth using photon storage.
3. Goals 2002–2007
- 3.1 Development of discriminating SPDs with efficiencies greater than 95% .
 - 3.2 Development of periodic SPSs and entangled multiphoton sources with an error probability per pulse of less than 10% .
 - 3.3 Demonstration of a $1\text{--}10\ \mu\text{s}$ optical quantum memory (to coincide with likely SPS rates).
 - 3.4 Demonstration of a controlled-NOT (C-NOT) gate that is *not* in the coincidence basis (no post selection) using SPSs.
 - 3.5 Demonstration of a Bell state on demand, with Bell inequality violation demonstrated *not* in the coincidence basis.
 - 3.6 Demonstration of a GHZ state on demand with verification *not* in the coincidence basis.
 - 3.7 Demonstration of a simple error-correction code gate (e.g., loss-detection code, measurement-error code for teleportation gates etc.).
 - 3.8 Demonstration of a compound gate (e.g., a Toffoli gate).
 - 3.9 Implementation of a three or four physical qubit (e.g., six or eight mode, three or four photon) processor for a ‘test-bed’ algorithm (e.g., Deutsch-Jozsa or general error-correction code).
 - 3.10 Demonstration of a quantum memory compatible with LOQC operation.
 - 3.11 Demonstration of a coherent state-based scheme for a single C-NOT gate.
4. Goals 2007–2012
- 4.1 Development of discriminating SPDs with efficiencies greater than 99% .
 - 4.2 Development of periodic SPSs and entangled multiphoton sources, with error probability, per pulse, less than 1% .
 - 4.3 Development of an integrated optical device for a ten logical qubit (e.g., 20 modes, 10 photons) algorithm, incorporating a SPS and a discriminating SPD.
 - 4.4 Demonstration of a 10-qubit factoring algorithm with error correction.
 - 4.5 Development of hybrid electro-optic quantum processors that use both solid-state and linear optics for processing.
5. Necessary achievements
- 5.1 Develop periodic SPSs with error probabilities less than 1% .
 - 5.2 Develop discriminating SPDs with efficiencies greater than 99% .

- 5.3 Demonstration of a C-NOT gate that is *not* based on post selection (i.e., not in the coincidence basis).
 - 5.4 Demonstration of a loss-detection code implementation.
 - 5.5 Demonstration of measurement error-detection code.
 - 5.6 Demonstration of state and process tomography for more than one qubit.
 - 5.7 Demonstration of simple gate operations within an integrated device (optical-fiber or photonic-band-gap device).
6. Trophies
 - 6.1 SPS with 50% probability of success; 90%; 95%; 99%; the mode quality of the source can be verified (e.g., by demonstrating HOM interference with greater than 95% contrast).
 - 6.2 Generate all Bell states via LOQC on demand with fidelity greater than 90% and demonstrate a noncoincidence Bell violation.
 - 6.3 Implement quantum process tomography on more than one qubit.
 - 6.4 High-fidelity (greater than 99%), low-loss (less than 10%; 5%; 1%) optical quantum memory.
 - 6.5 Discriminating SPDs with demonstrated efficiency greater than 90% and a sufficiently low dark-count rate; greater than 99%.
 - 6.6 Loss-detection code or compound-gate implementation.
 - 6.7 Teleportation protocol with greater than 67% efficiency without post selection.
 - 6.8 Teleportation protocol with error-correction code without post selection.
 - 6.9 C-NOT (or some other two-qubit gate) without post selection.
 - 6.10 Generate a maximally entangled N-photon state without post selection.
 - 6.11 Demonstrate process tomography for two-qubit states; three qubits; four qubits.
 - 6.12 Demonstrate a few-qubit quantum memory.
 - 6.13 Demonstrate a fiber-based few-qubit device.
(Note: requires appropriate SPS and discriminating SPD.)
 - 6.14 Demonstrate an integrated few-qubit device.
 - 6.15 Demonstrate a coherent cat-state code.
 7. Connections with other quantum information science technologies
 - 7.1 The scheme is close to quantum communication schemes, and the KLM scheme in particular relies on optical quantum teleportation. Because the information already resides in optical modes, an all-optical QC realization might not need to convert the qubits in order to link them to an optical quantum communication scheme. If the quantum communication link relies on telecommunication fibers, it is likely that the wavelength of the qubits will either need to be 1550 nm, or will need to be shifted to 1550 nm to reduce propagation loss. It should also be stressed that optical qubits may be an optimal way to shuffle information from one part of a quantum processor to another even if these main processors are not themselves optically realized. For the case of distributed QC over substantial distances (which promises increased capacity for

certain problems), optical qubits are by far the most likely candidate to connect the individual nodes; high-fidelity, high-efficiency wavelength converters will most likely be needed to match the optimal processing wavelength to the optimal transmission wavelength.

8. Subsidiary developments

- 8.1 The realization of ultrafast, low-loss electro-optic technologies has direct benefit to future electro-optic quantum communication schemes. Also, reliable quantum memories are a required element of quantum repeater chains, which extend the usable distance for quantum communications (e.g., cryptography and teleportation).
- 8.2 The development of brighter, tunable, more robust optical sources of entanglement has a positive impact on quantum communication, and also on (quantum) metrology. It is known that particular quantum states can allow better timing and/or spatial resolution in measurements.

9. Role of theory

- 9.1 More theoretical work needs to be done to assess the physical resource requirements for realistic devices (i.e., including photon loss and other sources of imperfect operation).
- 9.2 The search for other quantum optical schemes that are simpler to implement should be encouraged. New theoretical tools for the systematic discovery of multi mode conditional gates need to be developed. Only limited work has been done in this area [84].
- 9.3 More theoretical work needs to be done on developing optimal fault-tolerant gate implementations.
- 9.4 The concept of conditional nonunitary gates needs to be explored in contexts outside of quantum optics whenever good measurements are available. Even if suitable two-particle interactions are available for implementing two-qubit gates, some saving in resources might be made using conditional gates [85] or measurement-induced gates.
- 9.5 Scalable devices based on integrated optics and photonic-band-gap devices will require a considerable amount of classical optical modeling.
- 9.6 The benefits of employing novel quantum states—hyperentangled states, bound entangled states, etc.—need to be evaluated, as these may reduce the gate complexity or error-correcting code resources.

6.0 Timeline

In a five-year period, we require the demonstration of a few-qubit device. There is some ambiguity as to what would constitute a few-qubit device (particularly when one includes continuous-variable QC). More theoretical work needs to be done to specify a nontrivial, achievable, test algorithm for a three-qubit linear optics implementation that would be a useful technical challenge.

For example, we might propose a *three-qubit device* that can generate any of the eight possible orthogonal entangled states of either GHZ or W class [86], with high fidelity. Another possible

test implementation would require an implementation of a three-qubit error-correction code. A three-qubit device would require three photons in six modes in the original code scheme of KLM, plus a number of ancilla modes and ancilla photons. The precise number of ancillas required would depend on the particular implementation and the desired ideal probability of success.

We need to devise a way to quantify the requirements. For example we might ask that the eight orthogonal GHZ or W entangled states are generated with a sufficiently high fidelity, when the algorithm is considered to have worked, (we do not specify the success probability for the ideal implementation) to enable a quantum-communication task to demonstrate a nonclassical correlation without post selection.

To implement the KLM-type scheme, progress is dependent on the availability of SPSs, discriminating SPDs, and optical quantum memories. While such sources are under development, it is difficult to give a firm timeline until such sources are routinely available. However, many proof-of-principle experiments can be done with bright SPDC sources. We will assume that preliminary SPS devices are available by 2004. We also predict that many early implementations may move to fiber-based schemes as a possible entry path to a long-term integrated large-scale device. If low-loss, photonic, band-gap-based technology becomes available, this may be a likely candidate over fiber—if it is shown to be more stable and robust. As they can reduce the gate complexity, entangled-photon sources should continue to be developed. Finally, work is needed to understand the possible benefits of using hybrid sources (qubit + continuous variable, or simultaneous entanglement in multiple degrees of freedom).

1. Timeline for 2002–2007

1.1 SPS and SPD development

- 1.1.1 Development of a prototype SPS with error probability, per pulse, of less than 50% (where error is either zero or more than one photon per pulse).
- 1.1.2 Continued development of multiple, bright SPDC sources, including hyperentangled sources.
- 1.1.3 Development of robust SPSs, with error probability, per pulse, less than 10%.
- 1.1.4 Development of photon-entanglement on-demand source, with error probability, per pulse, less than 10%.
- 1.1.5 Development of novel discriminating SPDs with high efficiency (e.g., quantum memories run as photon detectors, cavity-QED schemes).
- 1.1.6 Incorporation of a SPS into a quantum interferometer (HOM)—greater than 95% contrast should be achieved.
- 1.1.7 Development of high-fidelity (greater than 99%), high-efficiency (greater than 90%) wavelength shifters, if needed to match optimized sources and detectors.

1.2 Measurement and control

- 1.2.1 Optimization of prototype detectors for high efficiency.
- 1.2.2 Sustained development of other novel SPD schemes with high efficiency.

- 1.2.3 Development of fast electro-optic, feed-forward delay lines for quantum memory and other control circuits for optical teleportation without post selection.
- 1.2.4 Development of automated multiqubit, quantum state and process tomography systems.
- 1.3 Basic LOQC
 - 1.3.1 Theory: realistically assess resource overheads for a three-qubit (six-mode) linear optical quantum processor for a test-bed task such as generating a CS code teleportation resource (see KLM), or a GHZ or W state (not in coincidence basis) including required reliability of the SPS and detector efficiency.
 - 1.3.2 Theory: develop experimentally relevant schemes (tomography or another scheme) for determining multimode entanglement of photon-number states.
 - 1.3.3 Theory: determine benefit of using hybrid sources (qubit + continuous variable), or simultaneous multiparameter entanglement.
 - 1.3.4 Demonstration device using SPDC sources (e.g., C-NOT in coincidence basis) using fiber-based interferometers.
 - 1.3.5 Implementation of teleportation with loss-detection code (e.g., see KLM article, Figure 4) using SPDC.
 - 1.3.6 Implementation of the nondeterministic C-NOT_{1/4} teleportation gate in the coincidence basis, using a single very bright SPDC source or two or more multiplexed SPDC sources (requires eight modes and four photons).
 - 1.3.7 Implementation, using SPSs, of a C-NOT gate *not* in the coincidence basis to generate arbitrary Bell states on demand and demonstrate a noncoincidence Bell violation.
 - 1.3.8 Implementation of a three- or four-qubit (six- or eight-mode, three- or four-photon) processor for a 'test-bed' algorithm (to be determined).
 - 1.3.9 Demonstration of a quantum memory compatible with LOQC operation.
2. Timeline for 2007–2012
 - 2.1 Develop discriminating SPDs with efficiencies greater than 99%.
 - 2.2 Develop periodic SPDs and entangled multiphoton sources, with error probability, per pulse, less than 1%; demonstration of full entanglement swapping.
 - 2.3 Development of 99%-efficient quantum memory.
 - 2.4 Develop an integrated optical device for a 10-qubit (20 modes, 10 photons) algorithm, incorporating a SPS and a discriminating SPD as integral components.
 - 2.5 Develop hybrid electro-optic quantum processors that use both solid-state and linear optics for processing.

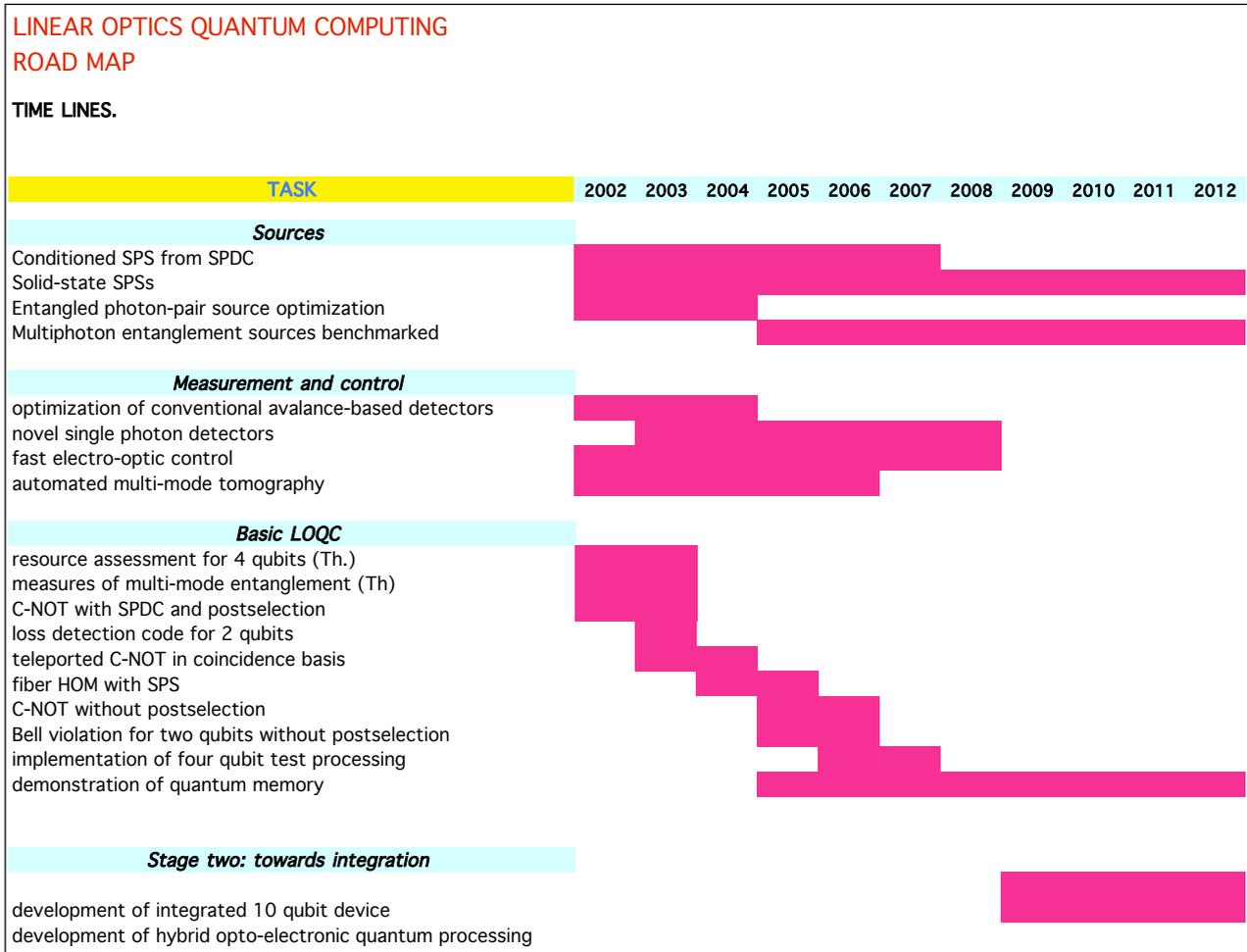


Figure 6-1. Optical QC developmental timeline

7.0 Glossary

Single-photon source (SPS)

A transform-limited pulsed optical field with one and only one photon per pulse. The pulses must exhibit first-order coherence (i.e., must exhibit self interference) and must enable two-photon interference (e.g., HOM interferometer [51]) using a delay line.

Discriminating single-photon detector (SPD)

A photon counter that detects one or more photons with high efficiency and can robustly discriminate between 0, 1, 2, or more photons.

Spontaneous parametric down conversion (SPDC)

The current method of choice for producing pairs of correlated photons. A high-frequency photon is split into two lower-frequency daughter photons via a nonlinear optical crystal. In addition to being able to directly create polarization-entangled pairs, several groups are pursuing it as a means to realizing a SPS.

Linear optics

Any optical device that is described by a Hamiltonian which is at most quadratic in the field amplitudes. Such devices include phase-shift components, mirrors, beam splitters, and polarizers. The class may be extended to include devices that make use of the second-order susceptibility in which one of the fields is classical (e.g., parametric down conversion with a classical pump field). As the Hamiltonian for a linear optical device is, at most, quadratic in the field amplitudes, the resulting Heisenberg equations of motion are linear in the field amplitudes.

HOM interferometer

A quantum interferometer, first implemented by Hong, Ou, and Mandel [51], in which single photons enter each of the two input ports of a 50:50 beam splitter. The probability for coincidence counts at the two output ports is zero when temporal and spatial mode-matching is perfect. This is the required test of a SPS intended for LOQC. Also, the HOM interferometer is useful for polarization Bell-state analysis, as required (e.g., in quantum dense coding and teleportation).

GHZ (Greenberger, Horne, and Zeilinger) and W states.

There are two classes of entangled states for a three-qubit system in the sense that a state in one class cannot be transformed into a state in the other class by local operations and classical communication (LOCC) [86]. There are two orthogonal GHZ states (with the form $|000\rangle \pm |111\rangle$) and six orthogonal W states (with the form $|010\rangle \pm |100\rangle$). The GHZ states are pure states specified by the correlation "all qubits have the same value." The W states are specified by the correlation "any two qubits are correlated."

Quantum state and quantum process tomography

In quantum state tomography, a number of measurements are made on an ensemble of identically prepared quantum systems. If the Hilbert space is of finite dimension, then a finite number of measurements suffices to allow one to reconstruct the quantum state of the particles [8]. Quantum process tomography uses similar techniques to characterize a quantum process, e.g., a unitary transformation, decoherence, etc. [9,10]. This means the effect on any possible input state to the process may be predicted.

8.0 References

- [1] Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–195 (2002).
- [2] Ou, Z.Y. and L. Mandel, "Violation of Bell's inequality and classical probability in a two-photon correlation experiment," *Physical Review Letters* **61**, 50–53 (1988).
- [3] Shih, Y.H. and C.O. Alley, "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion," *Physical Review Letters* **61**, 2921–2924 (1988).
- [4] Kwiat, P.G., K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y.H. Shih, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letters* **75**, 4337–4341 (1995).

- [5] Strekalov, D.V., T.B. Pittman, A.V. Sergienko, Y.H. Shih, and P.G. Kwiat, "Post selection-free energy-time entanglement," *Physical Review A* **54**, R1–R4 (1996).
- [6] Kwiat, P.G., E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, "Ultrabright source of polarization-entangled photons," *Physical Review A* **60**, R773–R776 (1999).
- [7] White, A.G., D.F.V. James, P.H. Eberhard, and P.G. Kwiat, "Non-maximally entangled states: Production, characterization, and utilization," *Physical Review Letters* **83**, 3103–3107 (1999).
- [8] James, D.F.V., P.G. Kwiat, W.J. Munro, and A.G. White, "Measurement of qubits," *Physical Review A* **64**, 052312 (2001).
- [9] Chuang, I.L. and M.A. Nielsen, "Prescription for experimental determination of the dynamics of a quantum black box," *Journal of Modern Optics* **44**, 2455–2467 (1997).
- [10] Poyatos, J.F., J.I. Cirac and P. Zoller, "Complete characterization of a quantum process: the two-bit quantum gate," *Physical Review Letters* **78**, 390–393 (1997).
- [11] Mazzei, A., M. Ricci, F. De Martini, and G.M. D'Ariano, "Pauli tomography: Complete characterization of a single qubit device," *Fortschritte de Physik* **51**, 342 (2003).
- [12] Altepeter, J.B., D. Branning, E. Jeffrey, T.C. Wei, P.G. Kwiat R.T. Thew, J.L. O'Brien, M.A. Nielsen, and A.G. White, "Ancilla-assisted quantum process tomography," *Physical Review Letters* **90**, 193601 (2003).
- [13] Edamatsu, K., *private communication* (2003).
- [14] Mitchell, M.W., C.W. Ellenor, S. Schneider, and A.M. Steinberg, "Diagnosis, prescription and prognosis of a Bell-state filter by quantum process tomography," *Physical Review Letters* **91**, 120402 (2003).
- [15] Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature* **390**, 575–579 (1997).
- [16] Pan, J.-W., D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Physical Review Letters* **80** 3891–3894 (1998).
- [17] Pan, J.-W., M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, "Experimental demonstration of four-photon entanglement and high-fidelity teleportation," *Physical Review Letters* **86**, 4435–4438 (2001).
- [18] Boschi, D., S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **80**, 1121–1125 (1998).
- [19] Furusawa, A., J. Sorensen, S.L. Braunstein, C. Fuchs, H.J. Kimble, and E.S. Polzik, "Unconditional quantum teleportation," *Science* **282**, 706–709 (1998).

- [20] Kim, Y.-H., S.P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," *Physical Review Letters* **86**, 1370–1373 (2001).
- [21] Kwiat, P.G., A.J. Berglund, J.B. Altepeter, and A.G. White, "Experimental verification of decoherence-free subspaces," *Science* **290**, 498–501 (2000).
- [22] Altepeter, J.B., P.G. Hadley, S.M. Wendelken, A.J. Berglund, and P.G. Kwiat, "Experimental investigation of a two-qubit decoherence-free subspace," (to appear in *Physical Review Letters* 2004).
- [23] Kwiat, P.G., J.R. Mitchell, P.D.D. Schwindt, and A.G. White, "Grover's search algorithm: An optical approach," *Journal of Modern Optics* **47**, 257–266 (2000).
- [24] Takeuchi, S., "Analysis of errors in linear-optics quantum computation," *Physical Review A* **61**, 052302 (2000).
- [25] Takeuchi, S., "Experimental demonstration of a three-qubit quantum computation algorithm using a single photon and linear optics," *Physical Review A* **62**, 032301 (2000).
- [26] Bhattacharya, N., H.B. van Linden van den Heuvell, and R.J.C. Spreeuw, "Implementation of quantum search algorithm using classical Fourier optics," *Physical Review Letters* **88**, 137901 (2002).
- [27] Howell, J.C., J.A. Yeazell, and D. Ventura, "Optically simulating a quantum associative memory," *Physical Review A* **62**, 042303 (2000).
- [28] Howell, J.C. and J.A. Yeazell, "Linear optics simulations of the quantum baker's map," *Physical Review A* **61**, 012304 (2000).
- [29] Hau, L.V., S.E. Harris, Z. Dutton, and C.H. Behroozi, "Light speed reduction to 17 metres per second in an ultracold atomic gas," *Nature (London)* **397**, 594–598 (1999).
- [30] Kash, M.M., V.A. Sautenkov, A.S. Zibrov, L. Hollberg, G.R. Welch, M.D. Lukin, Y. Rostovtsev, E.S. Fry, and M.O. Scully, "Ultraslow group velocity and enhanced nonlinear optical effects in a coherently driven hot atomic gas," *Physical Review Letters* **82**, 5229–5232 (1999).
- [31] Budker, D., D.F. Kimball, S.M. Rochester, and V.V. Yashchuk, "Nonlinear magneto-optics and reduced group velocity of light in atomic vapor with slow ground state relaxation," *Physical Review Letters* **83**, 1767–1770 (1999).
- [32] Liu, C., Z. Dutton, C.H. Behroozi and L.V. Hau, "Observation of coherent optical information storage in an atomic medium using halted light pulses," *Nature* **409**, 490–493 (2001).
- [33] Phillips, D.F., A. Fleischhauer, A. Mair, R.L. Walsworth, and M.D. Lukin, "Storage of light in atomic vapor," *Physical Review Letters* **86**, 783–786 (2001).
- [34] Lukin, M.D. and A. Imamoglu, "Nonlinear optics and quantum entanglement of ultraslow single photons," *Physical Review Letters* **84**, 1419–1422 (2000).

- [35] Lloyd, S. and S.L. Braunstein, "Quantum computation over continuous variables," *Physical Review Letters* **82**, 1784–1787 (1999).
- [36] Gottesman, D., A. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator" *Physical Review A* **64**, 012310 (2001).
- [37] Bartlett, S.D., B.C. Sanders, S.L. Braunstein, and K. Nemoto, "Efficient classical simulation of continuous variable quantum information processes," *Physical Review Letters* **88**, 097904 (2002).
- [38] Knill, E., R. Laflamme and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature* **409**, 46–52 (2001).
- [39] Kwiat, P.G., "Hyper-entangled states," *Journal of Modern Optics* **44**, 2173–2184 (1997).
- [40] Atature, M., G. Di Giuseppe, M.D. Shaw, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, "Multi-parameter entanglement in femtosecond parametric down-conversion," *Physical Review A* **65**, 023808 (2002).
- [41] Pittman, T.B., B.C. Jacobs, and J.D. Franson, "Probabilistic quantum logic operations using polarizing beam splitters," *Physical Review A* **64**, 062311 (2001).
- [42] Knill, E., "Quantum gates using linear optics and post selection," *Physical Review A* **66**, 052306 (2002).
- [43] Hofmann, H.F. and S. Takeuchi, "Quantum phase gate for photonic qubits using only beam splitters and post-selection," *Physical Review A* **66**, 024308 (2002).
- [44] Ralph, T.C., A.G. White, and G.J. Milburn "Simple scheme for efficient linear optics quantum gates," *Physical Review A* **65**, 012314 (2002).
- [45] Pittman, T.B., B.C. Jacobs and J.D. Franson, "Demonstration of non-deterministic quantum logic operations using linear optical elements," *Physical Review Letters* **88**, 257902 (2002).
- [46] Pittman, T.B., B.C. Jacobs and J.D. Franson, "Demonstration of feed forward control for linear optics quantum computation," *Physical Review A* **66**, 052305 (2002).
- [47] O'Brien, J.L., G.J. Pryde, A.G. White, T.C. Ralph, and D. Branning, "Demonstration of an all-optical quantum controlled-NOT gate," *Nature* **426**, 264 (2003).
- [48] Pittman, T.B. and J.D. Franson, "Cyclical quantum memory for photonic qubits," *Physical Review A* **66**, 062302 (2002).
- [49] Kwiat, P.G., J. Altepeter, J. Barreiro, D. Branning, E.R. Jeffrey, N. Peters, and A.P. van Devender, "Optical technologies for quantum information science," *Proceedings of SPIE International Society of Optical Engineering* **5161**, 87–100 (2004).
- [50] Ralph, T.C., A. Gilchrist, G.J. Milburn, W.J. Munro, and S. Glancy, "Quantum computation with optical coherent states," *Physical Review A* **68**, 042319 (2003).

- [51] Hong, C.K., Z.Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Physical Review Letters* **59**, 2044–2046 (1987).
- [52] Lund, A.P., T.B. Bell, and T.C. Ralph, "Comparison of linear optics quantum-computation control-sign gates with ancilla inefficiency and an improvement to functionality under these conditions," *Physical Review A* **68**, 022313 (2003).
- [53] Kwiat, P.G., A.M. Steinberg, R.Y. Chiao, P. Eberhard and M. Petroff, "High efficiency single-photon detectors," *Physical Review A* **48**, R867–R870 (1993).
- [54] Kim, J., S. Takeuchi, Y. Yamamoto, and H.H. Hogue, "Multiphoton detection using visible light photon counter," *Applied Physics Letters* **74**, 902–904 (1999).
- [55] Takeuchi, S., J. Kim, Y. Yamamoto, and H.H. Hogue, "Development of a high-quantum-efficiency single-photon counting system," *Applied Physics Letters* **74**, 1063–1065 (1999).
- [56] Waks, E., K. Inoue, E. Diamanti, and Y. Yamamoto, "High efficiency photon number detection for quantum information processing," (10-Aug-03) preprint *quant-ph/0308054*.
- [57] Imamoglu, A., "High efficiency photon counting using stored light," *Physical Review Letters* **89**, 163602 (2002).
- [58] James, D.F.V. and P.G. Kwiat, "Atomic vapor-based high efficiency optical detectors with photon number resolution," *Physical Review Letters* **89**, 183601 (2002).
- [59] Vrijen, R. and E. Yablonovitch, "A spin-coherent semiconductor photodetector for quantum communication," *Physica E: Low-dimensional Systems and Nanostructure* **10**, 569–575 (2001).
- [60] Kosaka, H., A.A. Kiselev, F.A. Baron, K.-W. Kim, and E. Yablonovitch, "Electron g-factor engineering in III–IV semiconductors for quantum communication," *Electronics Letters* **37**, 464 (2001).
- [61] van Enk, S.J., H.J. Kimble, J.I. Cirac, and P. Zoller, "Quantum communication with dark photons," *Physical Review A* **59**, 2659–2664 (1999).
- [62] Duan, L.-M., J.I. Cirac, P. Zoller, and E.S. Polzik, "Quantum communication between atomic ensembles using coherent light," *Physical Review Letters* **85**, 5643–5646 (2000).
- [63] Hong, C.K. and L. Mandel, "Experimental realization of a localized one-photon state," *Physical Review Letters* **56**, 58–60 (1986).
- [64] Migdall, A.L., D. Branning, S. Castelletto, and M. Ware, "Tailoring single and multiphoton probabilities of a single photon on-demand," *Physical Review A* **66**, 053805 (2002).
- [65] Pittman, T.B., B.C. Jacobs, and J.D. Franson, "Single photons on pseudo-demand from stored parametric down-conversion," *Physical Review A* **66**, 042303 (2002).
- [66] Kim, J., O. Benson, H. Kan, and Y. Yamamoto, "A single-photon turnstile device," *Nature* **397**, 500–503 (1999).

- [67] Michler, P., A. Kiraz, C. Becher, W.V. Schoenfeld, P.M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, "A quantum dot single-photon turnstile device," *Science* **290**, 2282–2285 (2000).
- [68] Santori, C, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "Triggered single photons from a quantum dot," *Physical Review Letters* **86**, 1502–1505 (2001).
- [69] Yuan, Z., B.E. Kardynal, R.M. Stevenson, A.J. Shields, C.J. Lobo, K. Cooper, N.S. Beattie, D.A. Ritchie, and M. Pepper, "Electrically driven single-photon source," *Science* **295**, 102–105 (2002).
- [70] Vuckovic, J., D. Fattal, C. Santori, G.S. Solomon, and Y. Yamamoto, "Enhanced single-photon emission from a quantum dot in a micropost microcavity," *Applied Physics Letters* **82**, 35963598 (2003).
- [71] Kurtsiefer, C., S. Mayer, P. Zarda, and H. Weinfurter, "A stable solid-state source of single photons," *Physical Review Letters* **85**, 290–293 (2000).
- [72] Brouri, R., A. Beveratos, J.-P. Poizat, and P. Grangier, "Photon antibunching in the fluorescence of individual colored centers," *Optics Letters* **25**, 1294–1296 (2000).
- [73] Kuhn, A., M. Hennrich, and G. Rempe, "Deterministic single-photon source for distributed quantum networking," *Physical Review Letters* **89**, 067901 (2002).
- [74] McKeever, J., A. Boca, A.D. Boozer, R. Miller, J.R. Buck, A. Kuzmich, and H.J. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity" *Science Express Reports* (online 26 February 2004).
- [75] Martinis, J., *private communication* (2002).
- [76] Kozhekin, A.E., K. Mølmer, and E. Polzik, "Quantum memory for light," *Physical Review A* **62**, 033809 (2000).
- [77] Cerf, N.J., C. Adami, and P.G. Kwiat, "Optical simulation of quantum logic," *Physical Review A* **57**, R1477–R1480 (1998).
- [78] Hofmann, H.F. and S. Takeuchi, "Realization of quantum operations on photonic qubits by linear optics and post-selection," *Proceedings of The Sixth Quantum Information Technology Symposium* May 27th–28th, Kyoto, Japan (2002); also (13-May-02) preprint *quant-ph/0204045*.
- [79] Santori, C., D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "Indistinguishable photons from a single-photon device," *Nature* **419**, 594–597 (2002).
- [80] Pittman, T.B. and J.D. Franson, "Violation of Bell's inequality with photons from independent sources" *Physical Review Letters* **90**, 240401 (2003).
- [81] De Martini, F., A. Mazzei, M. Ricci, G.M. D'Ariano, "Exploiting quantum parallelism of entanglement for a complete experimental quantum characterization of a single qubit device," *Physical Review A* **67**, 062307 (2003).

- [82] Mohseni, M., J.S. Lundeen, K.J. Resch, A.M. Steinberg, "Experimental application of decoherence-free subspaces in a quantum-computing algorithm" *Physical Review Letters* **91**, 187903 (2003).
- [83] Bouwmeester, D., J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon Greenberger-Horne-Zeilinger entanglement," *Physical Review Letters* **82**, 1345–1349 (1999).
- [84] Lapaire, G.G., P. Kok, J.P. Dowling, and J.E. Sipe, *Physical Review A* **68**, 042314 (2003).
- [85] Raussendorf, R. and H.J. Briegel, "A one-way quantum computer," *Physical Review Letters* **86**, 5188–5191 (2001).
- [86] Dur, W., G. Vidal, and J.I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Physical Review A* **62**, 062314 (2000).

Solid State Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.6

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not to be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: David Awschalom, Robert Clark, David DiVincenzo, P. Chris Hammel,
Duncan Steel and K. Birgitta Whaley

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0	Groups Pursuing This Approach	1
2.0	Background and Perspectives	2
2.1	Nuclear spin of P donors in Si	3
2.2	Electron spin in GaAs QDs.....	3
3.0	Summary of Solid-State QC: The DiVincenzo Criteria	4
4.0	What Has Been Accomplished.....	9
4.1	All of the above bode well for solid-state approaches.....	9
4.2	A long-term view	10
4.3	Metrics and Milestones: Gated Qubits	10
4.4	Metrics and Milestones: Optically Measured QD Qubits.....	11
4.5	Metrics and Milestones: Doped or “Spin” QD Qubits.....	12
5.0	Considerations	14
6.0	Timeline.....	18
7.0	Glossary	19
8.0	References	19

List of Tables and Figures

Table 1-1	Approaches to Solid State QC Research.....	1
Figure 6-1.	Solid state QC developmental timeline	18

List of Acronyms and Abbreviations

2-D	two dimensional	NMR	nuclear magnetic resonance
2-DEG	two-dimensional electron gas	NV	nitrogen vacancy
C-NOT	controlled-NOT (gate)	QC	quantum computation/computing
CPB	Cooper pair box	QD	quantum dot
CV	carbon vacancy	QED	quantum electrodynamics
CW	continuous wave	qNOT	quantum-NOT (gate)
ESR	electron-spin resonance	rf	radio frequency
FET	field-effect transistors	SAW	surface-acoustic wave
GHz	gigahertz	SET	single-electron tunneling
GHZ	Greenberger, Horne, and Zeilinger	SPD	single-photon detector
kHz	kilohertz	SPS	single-photon source
MHz	megahertz	SQUID	superconducting quantum interference device
mK	millikelvin	STM	scanning-tunneling microscopy
MRFM	magnetic resonance force microscope	T	Tesla
		TEP	Technology Experts Panel

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Solid State detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input we can improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Approaches to Solid State QC Research

Research Leader(s)	Research Location	Research Focus
Awschalom, D.	UC-Santa Barbara	GaAs spin systems, excitonic systems
Barrett, S.	Yale	ESR in semiconductor devices
Clark, R.	U. of New South Wales	P in Si
Das Sarma, S.	Maryland	theory
Doolen, G.	LANL	theory
Ensslin, K.	ETH	GaAs quantum dots (QDs)/rings
Gammon, D.	NRL	single exciton spectroscopy
Hammel, P. C.	Ohio State U.	magnetic force spin readout
Hawley, M.	LANL	P in Si
Kane, B.	Maryland	P in Si
Kastner, M.	MIT	GaAs QDs (spin decoherence)
Kotthaus, J.	Munich	GaAs QDs
Kouwenhoven, L.	TU Delft	GaAs QDs
Levy, J.	Pitt	Si/Ge QDs
Loss, D.	U. of Basel	theory
Marcus, C.	Harvard	GaAs wires and dots, Carbon nanotubes
Nakamura, Y.	NEC	Cooper pair box (CPB)
Pepper, M.	Cambridge	surface-acoustic wave (SAW) channeled electrons, Na in Si
Raymer, M.	U. of Oregon	QDs in microcavities
Rossi, F.	Torino, Italy	theory
Roukes, M.	Caltech	high frequency and quantum cantilevers
Sachrajda, A.	NRC Ottawa	GaAs QDs, edge states
Schenkel, T.	LBNL	P in Si
Schoelkopf, R.	Yale	rf single-electron tunneling (SET) device and CPB
Schwab, K.	NSA	quantum cantilevers and CPB
Sham, L. J.	UC-Santa Barbara	theory
Steel, D.	U. of Michigan	excitons & trions in QDs
Tarucha, S.	Tokyo	GaAs QDs
Tucker, J.	U. of Illinois at Urbana-Champaign	P in Si

Table 1-1
Approaches to Solid State QC Research

Research Leader(s)	Research Location	Research Focus
	U. of Wisconsin consortium	Si/Ge QDs
Webb, R.	Maryland	GaAs QDs
Whaley, B.	UC-Berkeley	theory
Yablonovich, E.	UC-Los Angeles	P in Si

2.0 Background and Perspectives

The work of recent years, starting in the mid 1990s, has uncovered a very large number of possible solid-state systems in which quantum computing might be achieved, reflecting the huge variety of quantum phenomena that are known in condensed matter physics. Given the current state of discussions and progress on these proposals, it is the judgment of the TEP that the most important existing progress in the laboratory, and the clearest prospects for continuing mid-term progress, is provided by localized “spin” or “charge” qubits, which will be described here in detail. We do not exclude the possibility that further progress on various of the other proposals, including electrons on liquid helium, quantum Hall edge states, carbon tubes and balls, semiconductor nanowires, or others might make them worthy of detailed assessment at a later date.

Many of the variations on the spin and charge approaches discussed here rely on the fact that in many solid state systems, the spin states of localized electrons or of nuclei, form well-defined, highly coherent two-level systems that are useable as qubits. The quantum-gate implementations typically rely on the most natural physical interaction between spins, the exchange interaction. It is envisioned that a highly miniaturizable, all-electronic or optoelectronic qubit is conceivable in this area. Localized spins are available via confinement to QDs or impurity atoms, by entrainment by SAW techniques, and by other methods. While the necessary device-fabrication techniques for QDs are available down to single-electron spins, this is not the case yet for impurity atoms. QDs are a versatile system for qubits; other schemes, including excitonic qubits with optical addressing and coupling, have been devised as well as optically driven spin based QDs using a charged exciton as an optically induced transient high-speed gate. Quantum mechanical systems, using nanocantilevers, can also play a role in coupling and reading out solid-state qubits.

In a system using optically driven quantum-dot excitons, charge refers to the fact that the state of the qubit is determined by the state of excitation of an electron-hole pair in a semiconductor QD. In this case, the qubit becomes the optical Bloch vector where a $|0\rangle$ corresponds to the optical Bloch vector pointing down $|\downarrow\rangle$ and the dot is unexcited. Excitation of the dot leading to formation of the exciton now puts the qubit value at $|\uparrow\rangle$ and the optical Bloch vector pointing up $|\uparrow\rangle$. The decoherence time in this system is then limited by the optical dipole, which determines the radiative recombination rate. Measurements have shown there are generally no other dephasing mechanisms. The clock-speed is limited by the reciprocal pulsewidth that would excite higher lying states of the dot. This leads to a limiting figure of merit probably near or

somewhat in excess of 10^3 . QDs are produced either epitaxially or by chemical synthesis. Two-qubit non-scalable devices can be demonstrated in single QDs using orthogonally polarized excitonic transitions. The interactions between the two qubits essential to creating entanglement are produced by higher-order Coulomb coupling leading to bi-exciton formation. Scalable systems have been envisioned where nearby QDs interact via dipole-dipole coupling, wave-function overlap, or radiation coupling via an optical cavity. The relatively fast decoherence, determined by radiative lifetime, is often seen as a limiting liability in these systems. However, these systems represent the prototypical optical excitation needed to enable optical manipulation of single-electron spins for spin-based qubit. Interestingly, the exciton QD is a charged-based system where the dot is neutral. In most cases of interest, the spin-based qubit in a QD is charged. The optical excitation path uses the same path as in the exciton system, but a second photon is needed to complete the rotation of the spin.

The basic ideas that are being pursued in this area were laid out by Loss and DiVincenzo (QDs) [1], and were adapted to impurity spins by Kane [2], and extended to optically driven spin-based systems by Rossi and Zoller [3] and Sham *et al.* [4]. Two specific examples in solid-state systems are impurity spins and spins in QDs [1].

2.1 Nuclear spin of P donors in Si

The nuclear spin ($I = 1/2$) of ^{31}P is a natural two-level system embedded in a spin-free substrate of ^{28}Si ($I = 0$). The nuclear spins of ^{31}P donors are separated by approximately 20 nm and there is a hyperfine interaction between donor electron spin and nuclear spin (qubit). Interaction between qubits is mediated through the donor-electron exchange interaction. The spins are maintained at millikelvin (mK) temperatures in an external magnetic field of several Tesla, perpendicular to the plane of the substrate. Nanoscale surface A and J gates control the hyperfine and exchange interactions at qubit sites. Two distinct states have been observed in ensemble nuclear magnetic resonance (NMR) experiments, but not in single-spin systems. Radio frequency (rf) coils can be used to apply π -pulses (or surface control gates can be pulsed in the presence of a continuous wave [CW] rf field B_a), demonstrated in ensemble-spin systems but not single-spin systems. Rabi oscillations are yet to be demonstrated for single spins. The system scales essentially linearly with respect to resources (gates, donors, etc).

2.2 Electron spin in GaAs QDs

The spin of a single electron confined in a QD provides a natural qubit which can be manipulated either electronically or optically. The QD can be defined by 50-nm-wide electrostatic gates on top of a AlGaAs/GaAs two-dimensional electron gas (2-DEG), or by three-dimensional (3-D) confinement in a patterned semiconductor heterostructure, with a center-to-center distance between dots of about 200 nm . It is currently possible to isolate a single electron in each of two such QDs. In equilibrium at 300 mK and 5 Tesla (T), the electrons will be in the ground state spin-up with $>99\%$ probability. An essential idea of the proposal is an all-electrical control of spin via electrical gates, i.e., to make use of a "spin-to-charge conversion" based on the Pauli principle obeyed by electrons. The spin of the electron is used as storage of quantum information, while the charge and Coulomb interaction of the electron allows for fast gate operations and readout. In addition, if the magnetic field is oriented perpendicular to the

substrate, the leads provide a reservoir of spin-polarized electrons, which can serve as a reference for qubit readout. Pulsed microwave fields on resonance with the spins give single-qubit rotations, and electrostatic control of the exchange interaction between spins in neighboring dots permits two-qubit gates. Both types of quantum gates still need to be demonstrated. The resources (gates etc.) scale linearly with the number of qubits.

An all-optical approach allows us to exploit the advances in ultrafast laser technology, potentially integrated on-chip without the use of metallic gates and electrical coupling. QDs can be defined by 3-D confinement in a patterned semiconductor heterostructure, with a center-to-center distance between dots of about 200 nm. QDs can be doped with a single electron and operated at 4K at magnetic fields of order 7–10 T. Quantum logic-gate operations involving spins of single electrons confined in QDs occur through the exchange interaction of spin to nearby QDs through the spin-spin interaction. The gate interaction is controlled by an ultrafast solid-state laser which transiently excite electron-hole pairs (excitons or trions) that mediate the spin-spin interaction.

3.0 Summary of Solid-State QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits (gated or optically driven spins). 

In the solid state, a number of candidate qubits may be characterized by the following groupings:

- spins in confined structures such as
 - laterally or vertically coupled lithographic QDs,
 - spins confined in a two-dimensional (2-D) system,
 - doped colloidal QDs,
 - high-spin magnetic nanoparticles,
 - nuclear-spin lattices or ensembles,
 - nuclear-spin heterolayers, and
 - single-electron-doped self-assembled or patterned QDs or single electrons in SAW channels;
- *impurity spins* such as
 - shallow donors in Si, SiGe, or GaAs;
 - paramagnetic ions in C_{60} ;

- paramagnetic ions in carbon nanotubes; and
- nitrogen vacancy (NV) diamond centers or rare-earth color centers;
- *charged or excitonic systems* (the numbers indicate an quantum-dot-exciton-based qubit system is scalable based on any of the three coupling schemes using adjacent QDs; the single-quantum-dot system is not significantly scalable beyond two qubits) such as
 - electron position in double quantum wells,
 - helicity of excitons trapped at a III-V heterostructure interface,
 - electrons in quantum wires, and
 - localized Cooper pairs in quantum wires; and
- *mechanical systems* such as the phonon states of high Q nanocantilevers.

For each candidate qubit, characterization involves the demonstration of coherent oscillations, between the two states, whether accurate π -pulses can be applied and if the qubit system is scaleable.

2. The ability to initialize the state of the qubits to a simple fiducial state (gated or optically driven spins). 

The important measures of the success of initialization include how well the qubits can be initialized, how quickly they can be reset, how long the initialization takes, and what has been demonstrated to date.

- *Spin systems*:
 - electron spins require cryogenic temperatures (<4K) and
 - nuclear spins require special techniques (such as the Overhauser effect), dynamic nuclear polarization or optical pumping, or techniques for manipulating individual spins using electric fields or magnetic-field gradients. A promising approach currently under study is the use of optical pulse shaping for state initialization.
- *Charge systems* require the use of external voltages applied to gates to control the electron position.
- *Excitonic systems* require laser excitation of specific helicity.
 - This system is easily initialized. It relaxes to the $|0\rangle$ state within 50 ps to 1 ns, depending on the dot structure. It may be driven to the $|1\rangle$ state with an optical π -pulse.
- *Mechanical systems* require the cooling of cantilevers to reduce the degrees of freedom. Pumping techniques have been proposed.

3. Long (relative) decoherence times, much longer than the gate-operation time (gated or optically driven spins). 

For each proposal, several mechanisms of decoherence exist. In the case of QD excitons, extensive measurements have been performed at the single-dot level and ensemble level that show coherence times ranging from 50 ps to 1 ns, depending on dot size and is due to radiative decay rather than pure dephasing. A few measurements have been performed

for individual qubits to date. However some low-temperature ensemble measurements exist as detailed below. All the times quoted here should be measured against gate times that are hoped to be on the order of 1 ns.

- *Spins in confined structures*: Ensemble measurements for electrons in GaAs, $T_2 \approx 1$ ns (at least).
- *Impurity spins*: Ensemble measurements of electron T_2 for P in Si ~ 1 ns.
- *Charge or excitonic systems*: Electron spatial coherence times (~ 1 ns in GaAs QDs) generically less than spin coherence time. Exciton coherence times typically 10s of ps to ns but can be greatly lengthened by electron-hole separation.
 - The minimum switching time is determined by energy spacing to adjacent states, which at present is believed to be around 1 ps or perhaps somewhat smaller. More studies are needed to know these numbers more accurately.
- *Mechanical systems*: No available data.

4. A universal set of quantum gates (gated or optically driven spins).

Solid-state implementations use a variety of techniques to perform arbitrary rotations of single qubits together with two-qubit coupling to perform all universal gate operations. Techniques used for single-qubit operations include:

- *spins in confined structures QDs*:
 - Heisenberg operations alone,
 - local magnetic fields,
 - ESR rotation of spins,
 - Rabi driven trion (optical Raman) transitions (with/without cavities/photonic bandgap),
 - magnetic-field gradients with rf pulses,
 - displacement of electron wave function into high-g regions,
 - Rashba and spin-orbit modulation using gate modulation of electric fields, and
 - ac Stark effects [5];
- *impurity spins*:
 - Stark, Knight, Zeeman, or Lande-g-factor shifted electron and nuclear resonances using surface gates;
 - local magnetic fields and rf fields; and
 - optical resonance techniques including laser excited Raman transitions; and
- *charged or excitonic systems* (the universal gates in this system is comprised of controlled-NOTs and single-qubit rotations or other possible gates, such as phase gates):
 - Stark shifts are controlled by optical fields,
 - resonant microwave or optical fields,
 - Raman excitation, and

- gateable or fixed dipole-dipole interaction.

4.1 Two-qubit operations

Physical implementations of two-qubit operations are more uniform across the different systems, and are generally performed via the Heisenberg-exchange interaction (RKKY for optically driven doped QDs) or dipole-dipole coupling for some cases of nuclear spins. Electrostatic control of a barrier between two qubits manipulates the exchange coupling. Cavity quantum electrodynamics (QED) or optical-dipole coupling is also being explored for systems such as carbon vacancy (CV)-diamond.

5. A qubit-specific measurement capability (gated  or optically driven  spins).

To operate a quantum computer, it is necessary to be able to read out the state of a specific qubit with high accuracy (high probability). In some sense, qubit (single spin) measurements have been accomplished already quite some time ago; the Moerner and Orrit groups in 1993, independently, measured single spins using optical techniques. But for the solid-state qubits under consideration, workable techniques are not yet in place; a number of different strategies are being pursued to achieve this goal:

- *Spins in confined structures:* A number of techniques have been proposed for readout:
 - Conceptually, the simplest approach is to perform direct readout of the spin using a spin-filter such as a magnetic semiconductor.
 - An elegant suggestion (Loss-DiVincenzo) is to convert the spin information to charge information through a spin-dependent tunnelling process, and then detect the resultant spin-dependent charge transfer using highly sensitive electrometers such as submicron field-effect transistors (FETs), quantum point contacts, or SETs.
 - Optically driven resonance fluorescence (analogous to optically cycling in ion traps) and cavity-enhanced (QED) absorption are promising techniques for dots with optical transitions available.
 - A further promising suggestion is to read out the spin on the dot via a transport current (spin-polarized) passing through the QD. Due to Pauli blocking, the current is typically 10–1000 times larger for spin up than it is for spin down [6].
 - Mechanical methods of detecting the spin/charge state of the qubit have also been proposed, based on magnetic resonance force microscope (MRFM) techniques would be applicable independent of optical or transport properties.
 - Nanomagnetometers such as nano-SQUIDs (superconducting quantum interference devices) have also been suggested, as well as solid-state Stern-Gerlach devices.
 - Near-field optical readout has also been proposed, using luminescence or Faraday rotation. Progress toward this goal was reported in *Science* by Guest *et al.* [7].

- *Impurity spins*: The readout techniques for this architecture are essentially the same as for spins in confined structures:
 - For nuclear-spin devices the information stored on nuclear spins can be transferred to the associated donor-electron spin through the hyperfine interaction. The electron spins can then be detected through the methods outlined above.
- *Charged or excitonic systems*: In these systems readout is either optical or electrostatic:
 - Optical techniques include luminescence readout and ensemble optical readout.
 - Electrostatic techniques include SET readout and for the specific case of e/He, state-selective tunnelling of electrons from the liquid He surface.
 - More work is needed in this area, but it is envisioned that optically driven qubits must be within a few hundred angstroms of each other in order to have adequate coupling. This is well below the far-field spatial-resolution limit. One architecture that has been proposed uses an array of near-field optical-fiber probes to address specific qubits. An alternative approach is to use coherent control techniques to manipulate and read out specific bits. Another approach to readout is to use electrical methods. Optical-readout proposals are limited at present except for the generally accepted approach of signal averaging.
- *Mechanical systems* such as the phonon states of high-Q nanocantilevers.
 - Proposed approaches to detection of the cantilever's displacement include SET detection of electrostatic interaction or heterodyne optical measurements.

6. The ability to interconvert stationary and flying qubits.

This would allow different parts of the quantum computer to be connected at will, and act as a bus. This requires movement of the individual qubits throughout the device. Interesting progress toward to this end has come from another scientific area called coherent optical control [8].

- *Spins in confined structures and impurity spins*: Flying qubits are possible for some of these architectures and could consist of mobile electrons guided through the host material by surface gates or channels in the material or photons confined to optical waveguides.
- *Charged/excitonic systems*: There has been relatively little work in this area. Optical-cavity coupling and fiber-optical interconnects have been mentioned, but this area remains open for further investigation.
- *Mechanical systems*: No flying qubits are envisioned for these systems.

7. The ability to faithfully transmit flying qubits between specified locations.

The ability to convert qubits stored at specific points in the computer into flying qubits will be advantageous for scale-up and error correction. The question, then, is how to transfer the information stored on a fixed qubit to a flying qubit:

- *Spins in confined structures and impurity spins*: As mentioned above, flying qubits have not been extensively investigated for these systems. Conversion between fixed and mobile qubits could involve exchange interaction between electrons bound at a donor

site and free electrons, electrons tunnelling into quantum wires, or coupling to photons via microcavities with single-photon sources (SPSs) and detectors (SPDs). Indeed, in the case of optically driven qubits, the fact that spins in GaAs QDs are optically active with the application of a magnetic field can be exploited for the transfer of the spin qubit to a flying photonic qubit, using cavity-QED techniques to achieve the needed high fidelity.

- *Charged/excitonic systems:* As indicated in item 6, relatively little effort has been given to this problem.
- *Mechanical systems:* No ideas for flying qubits have been considered at this time.

4.0 What Has Been Accomplished

At present, only a few of the metrics below have been partially achieved within the solid-state arena. As examples, single-qubit action, in an ensemble setting, is well documented in recent Awschalom work and earlier spin-resonance work. Steel and coworkers have evidence for entanglement of electron-hole states in a single QD as well as Rabi oscillations corresponding to qubit rotations. However, the plan of the coming years' effort is taking shape, and a reasonable view can be given of how these metrics will be approached.

At present, the solid-state community, and much of the quantum-information community, is correctly focused on Rabi flops and relatively simple quantum logic operations. While this is important, it is likely that several technologies will have sufficient coherence for QC. It is important to realize however that the decisive issues for assessing the promise of a technology for a scaleable QC will come after coherence has been demonstrated. It will then be necessary to learn how to control quantum information flow between devices. It is clear that some technologies will have significant advantages over others. For example, nearest-neighbor-only coupling will have disadvantages compared to schemes where quantum information can be communicated over long distances. Two- (or three-) dimensional arrangements of quantum logic devices will be superior to approaches in which devices are arranged linearly.

The solid-state approaches should show their strengths when the following considerations start to become important:

- fast qubits will be better than slow qubits,
- parallel is better than serial, and
- small qubits will be better than big qubits.

All of these points seem obvious, but precisely the opposite conditions apply for doing early easy experiments. Slow qubits are easier to control with precision than fast ones. Big qubits are easier to fabricate than small ones. (Note that 'easier' here is relative, as there are no easy experiments in quantum information science and technology.)

4.1 All of the above bode well for solid-state approaches

With regard to solid-state implementations, systems in which, for example, electrons convey information will be advantageously fast due to the small electron mass. Similarly, whilst approaches centered on electrons in solids require the 'hard' fabrication of architectures such as

quantum-dot and single-donor-atom arrays on the nanometer or atomic scale, they avoid many obstacles to scaling such as cross talk between electromagnetic fields of macroscopic circuits which are more easily fabricated with conventional technology.

The specific case of spin qubits is a good example, as this particular solid-state implementation has features that make it extremely well positioned to overcome the obstacles to scaling and it has properties favorable for all of the criteria mentioned above. The dominant spin interactions are local and can be very fast. Spins on electrons can be transported rapidly. Because the dominant interaction between them falls off exponentially with distance, large amounts of quantum information can be transported with minimal amounts of unwanted interaction. Parallel operations and 2-D architectures are realizable in principle.

4.2 A long-term view

Whilst experiments on solid-state qubits are difficult, and particularly hard for spin, it is important to emphasize that the 'easy' qubits are not necessarily the best qubits for a large-scale quantum computer and that 'difficult' nanostructured qubits in solids have highly favorable properties necessary for large-scale quantum computer architectures, despite the tremendous challenges facing this research.

4.3 Metrics and Milestones: Gated Qubits

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states. 
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.2 Demonstrate decoherence times much longer than Rabi oscillation period. 
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 
3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - 3.2 Produce and characterize Bell states. 
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, & Zeilinger (GHZ)-state of three physical qubits. 

- 4.2 Produce maximally entangled states of four and more physical qubits. 
- 4.3 Quantum state and process tomography. 
- 4.4 Demonstrate decoherence-free subspaces. 
- 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
- 4.6 Demonstrate quantum error-correcting codes. 
- 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
- 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
- 5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
- 6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
- 7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

4.4 Metrics and Milestones: Optically Measured QD Qubits

- 1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states. 
- 2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.2 Demonstrate decoherence times much longer than Rabi oscillation period. 
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 
- 3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - 3.2 Produce and characterize Bell states. 
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
 - 3.4 Demonstrate quantum state and process tomography for two qubits. 

- 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS). 
- 3.6 Demonstrate a two-qubit quantum algorithm. 
- 4. Operations on 3–10 physical qubits
 - 4.1 Produce a GHZ-state of three physical qubits. 
 - 4.2 Produce maximally entangled states of four and more physical qubits. 
 - 4.3 Quantum state and process tomography. 
 - 4.4 Demonstrate decoherence-free subspaces. 
 - 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
 - 4.6 Demonstrate quantum error-correcting codes. 
 - 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
 - 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
- 5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
- 6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
- 7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

4.5 Metrics and Milestones: Doped or “Spin” QD Qubits

- 1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states. 
- 2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.2 Demonstrate decoherence times much longer than Rabi oscillation period. 

- 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 
3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - 3.2 Produce and characterize Bell states. 
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
4. Operations on 3–10 physical qubits
 - 4.1 Produce a GHZ-state of three physical qubits. 
 - 4.2 Produce maximally entangled states of four and more physical qubits. 
 - 4.3 Quantum state and process tomography. 
 - 4.4 Demonstrate decoherence-free subspaces. 
 - 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
 - 4.6 Demonstrate quantum error-correcting codes. 
 - 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
 - 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

1. Special strengths
 - 1.1 Semiconductor systems (GaAs, Si, SiGe,) offer inherent scalability. Established and new semiconductor patterning processes allow for the construction of submicron 2-D arrays of qubits.
 - 1.2 Semiconductor systems have compatibility with existing microelectronics industry and have high potential for development of integrated on-chip devices.
 - 1.3 Spin qubits in semiconductors are well-defined “native” qubits (two-level systems).
 - 1.4 Spin qubits in semiconductors (single donor or QDs) can be decoupled from charge fluctuations, leading to long decoherence times (from s to ms) compared with practical gate operation times (from ps to ns).
 - 1.5 Charge qubits in semiconductors (e.g., \uparrow electron position in double quantum wells) offer potential for extremely fast qubit (ps) operations. Single-charge detection has been demonstrated with SETs.
 - 1.6 There is the potential for coupling to flying qubits (e.g., \uparrow in QDs attached to quantum wires, see reference [9]).
2. Unknowns, weaknesses
 - 2.1 Background impurity levels and disorder in semiconductor systems may lead to difficulties in device reproducibility. These issues are common with sub-100-nm devices in conventional microprocessors.
 - 2.2 For spin qubits—single-spin readout has not been demonstrated and will be challenging. Best technique still to be determined from electrical (SET); optical; or mechanical (MRFM).
 - 2.3 For spin qubits—actual decoherence times for stationary *single* electron/nuclear spins not yet measured. Measurements will require single-spin readout. Further theoretical calculations are also needed.
 - 2.4 For spin qubits in Si—the exchange interaction is predicted to oscillate as a function of donor separation, which may place stringent requirements on nanofabrication accuracy.
 - 2.5 For charge qubits—decoherence likely to be dominated by voltage fluctuations on control gates and may be fast. Experiments on GaAs dots indicate dephasing times on the order of ns.
 - 2.6 Most semiconductor-based schemes are based on linear qubit arrays. The extension to 2-D arrays will require via-gate techniques on the sub-100-nm scale, which is challenging.
 - 2.7 A number of solid-state schemes are still at the conceptual phase. Detailed fabrication strategies still to be developed.
3. Goals 2002–2007
 - 3.1 Readout
 - 3.1.1 *Spin qubits*: single-spin measurement demonstrated as a general capability

- 3.1.1.1 Spin-selective charge displacement/tunneling transport induced by electric or electromagnetic fields followed rf-SET readout or cavity-QED readout.
- 3.1.1.2 Direct magnetic measurement of single spin by force detection with an MRFM employing high Q nanocantilevers; this approach should be distinguished from optical or transport approaches in that it is a general approach whose applicability is independent of optical or transport properties of the material or the presence of gates.
- 3.1.1.3 Advanced development of other possible readout schemes:
 - solid-state Stern-Gerlach device,
 - near-field optical readout—luminescence, Faraday rotation,
 - ESR-STM detection of Larmor precession in STM tunneling current, and
 - optical-readout via spin coupling to singly addressable sites (e.g., NV center in diamond).
- 3.1.2 *Charge, Excitonic, and Mechanical systems:* measurement capability in place
 - SET readout,
 - luminescence readout,
 - ensemble optical readout, and
 - heterodyne optical measurement of cantilever displacements.
- 3.2 Qubits and quantum gates
 - 3.2.1 *Spins in confined structures:*
 - few-qubit entanglement in Loss-DiVincenzo scheme has been demonstrated,
 - good scientific understanding of sources of decoherence and precision issues,
 - reliable fabrication process and materials issues addresses,
 - plan for scaling to 10+ entangled qubits, and
 - convergence with impurity schemes.
 - 3.2.1.1 Possible:
 - demonstrate reliable quantum gates in a few-qubit array.
 - 3.2.2 *Impurity spins:*
 - few-device version of Kane scheme has been largely realized,
 - strong but not perfect quantum measurements have been demonstrated,
 - reliable fabrication process and materials issues have been addressed, and
 - we have a plan for scaling to 10+ entangled qubits.
 - 3.2.2.1 Possible:

- develop hybrid conventional—quantum processor architectures in Si for few-qubit arrays, including some convergence with on-chip, ultra-fast superconducting circuitry, or HEMT GaAs circuitry (for compatibility with high magnetic fields).
- demonstrate a functioning linear array of dopant qubits in Si structure, with reliable measurements achieved.

3.2.3 Charge/Excitonic Systems:

- controllable entanglement of charge qubits and of excitons demonstrated and
- potential of extremely fast qubit operations evaluated.

3.2.3.1 Possible:

- simple device with several qubits demonstrated and
- potential of coupling to flying qubits demonstrated.

4. Goals 2007–2012

- 4.1 Resolve all major physics and materials-science issues.
- 4.2 Develop fast control and readout schemes.
- 4.3 Develop process tomography for gates, algorithms, and decoherence.
- 4.4 Demonstrate fault-tolerant gates and decoherence-free subspaces.
- 4.5 Demonstrate 10 or more entangled qubits.
- 4.6 Plan for scaling to 100 or more entangled qubits.
- 4.7 Converge on best type of solid-state qubit.
- 4.8 Demonstrate coupling to flying qubits.
- 4.9 Achieve advances in reducing required precision for a reliable quantum computer.

Possible:

- 4.10 Develop a small-scale hybrid conventional/quantum processor for commercial applications.

5. Necessary achievements

- 5.1 Solve materials-fabrication issues in several schemes for electron-spin confinement.
- 5.2 Achieve good control of the reproducibility of these structures; suppress $1/f$ noise.
- 5.3 Develop precision high-speed instrumentation, perhaps involving on-chip electronics, for the all-electrical control of qubits.
- 5.4 Demonstrate a high-efficiency spin readout compatible with the qubit gate devices.

6. Trophies

- 6.1 *Demonstration of efficient generally applicable single qubit readout of spin state.* For example, for spin systems, the ability to detect a single electron or nuclear spin is a major physical challenge and would be a significant achievement in its own right. A

- readout technology independent of specific material or device properties will have broad impact as a tool for quantum device applications.
- 6.2 *Fabrication of devices with precise arrays of addressable qubits:* (e.g., creation of periodic dopant arrays in semiconductors with atomic precision; fabrication of large arrays of quantum wires for SAW channels).
 - 6.3 Demonstration and characterization of single-qubit operations.
 - 6.4 Creation and manipulation of entanglement between many subsystems.
 - 6.5 Identification and demonstration of flying-qubit schemes.
 - 6.6 Identification and demonstration of efficient error-correcting codes for qubits with nearest-neighbour interactions only.
 - 6.7 QC with standard electronic control or all optical control.
7. Connections with other quantum information science technologies
 - 7.1 NMR pulse-shaping techniques should be adapted to achieve precision control.
 - 7.2 The potential for optical control and readout must stay on the table.
 - 7.3 Continuing interaction with materials science and magnetism is necessary.
 - 7.4 Strong links to research in classical spin-based electronics should be exploited.
 8. Subsidiary developments
 - 8.1 Nanofabrication challenges for semiconductor systems (particularly Si) are common to many of those for next generation of ultra large scale integration (ULSI) microprocessor chips, leading to synergies with developments in existing industry. Such challenges include precision donor placement, relevant to both a quantum computer and sub-100-nm transistors.
 - 8.2 Solid-state QC systems require advanced bottom-up assembly approaches which are relevant to the broad new range of nanotechnology-based industries, such as those utilizing scanned-probe single-atom manipulation, carbon nanotube and C_{60} structures, and self-assembly of devices.
 - 8.3 Many of the device capabilities needed for semiconductor-based QC have potential applications in the microelectronics industry, such as ultrafast (GHz) gating techniques and SET development.
 - 8.4 Demonstrated optoelectronic semiconductor devices (lasers/photodetectors) offer hope for integration between on-chip quantum processing and fiber-based quantum communication.
 - 8.5 Exciton-based QC systems have potential spin-offs in development of new optoelectronic systems.
 - 8.6 Electronics exploiting quantum devices will have important impact on information-processing applications other than computing.
 9. Role of theory
 - 9.1 *For spin qubits:* Measurement of decoherence times will require single-spin readout. Considerable further theoretical calculations are needed; this includes decoherence

by the lattice (phonons), decoherence due to voltage fluctuations on control gates and readout devices, and decoherence by impurity spins and charges. Many of these calculations are currently underway.

- 9.2 Calculation of decoherence induced by measurement back-action processes (SETs, MRFM, etc).
- 9.3 *For spin qubits:* Calculation of qubit coupling strengths for Si-, SiGe-, and GaAs-based schemes using real Bloch wave functions.
- 9.4 *For spin qubits:* We will need development of both general and specific strategies for achieving very accurate unitary control, including pulse shaping (for both optical and electrical pulses), refocusing, and unwinding of undesired evolutions.
- 9.5 Development of detailed measurement schemes (SET-, optical-, conductivity-based) to determine degree of entanglement.
- 9.6 Development of error-correction codes for specific architectures.
- 9.7 *For excitonic systems:* Determination of optical pulse shaping and understanding of exciton line widths.
- 9.8 *For mechanical systems:* Understanding of cantilever damping mechanisms.

6.0 Timeline

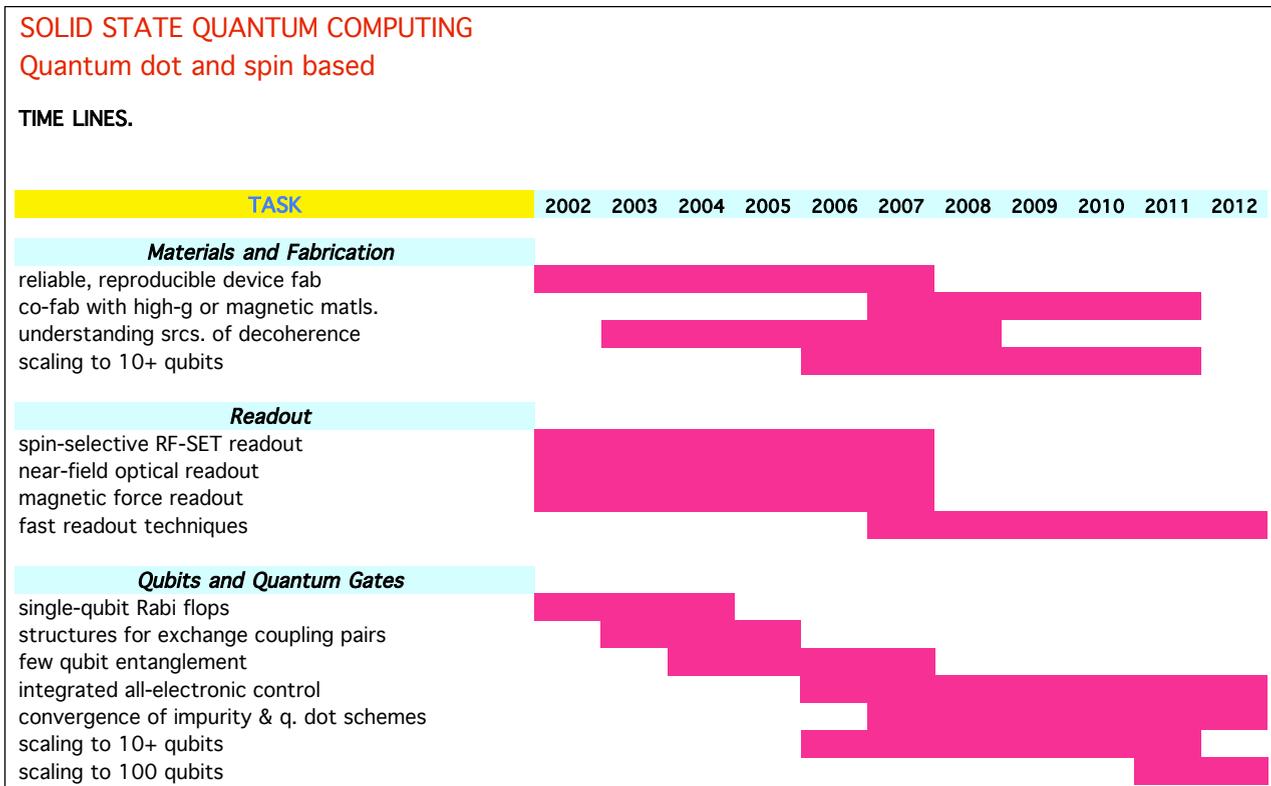


Figure 6-1. Solid state QC developmental timeline

1. Timeline for 2002–2007
 - 1.1 *Materials and Fabrication*: In the early years, the basic precise, reproducible fabrication of a number of important qubit structures will be done. As these devices are produced, a basic understanding of the origins and nature of decoherence in these structures will be obtained.
 - 1.2 *Readout*: Techniques for measuring single spins must be mastered in the early years. As time goes on, it should be learned how to make these measurements faster. Ultimately transduction to electrical signals will be important, but in the short term direct optical or mechanical readout will also be important.
 - 1.3 *Qubits and Quantum Gates*: Present progress on achieving single-spin Rabi flopping will continue. Within a couple of years realistic structures for exchange-coupling two spins should be built. Subsequent to that, few-qubit entanglement should be demonstrated.
2. Timeline for 2007–2012
 - 1.1 *Materials and Fabrication*: Hybrid structures should begin to emerge in which elements of spintronic, magnetic, and semiconducting structures are put together for optimized functionality. Feasible scalability to the 10 or more qubit level should be moving ahead.
 - 1.2 *Readout*: Methods of very fast, reliable, and fully parallel measurement should be achieved.
 - 1.3 *Qubits and Quantum Gates*: Integrated, all-electronic control of quantum gating should be achieved. Optimization of the impurity-based and QD-based qubits schemes, incorporating elements of both, should be achieved. Some simple problems involving 10 qubits should be attacked, and plans for scaling to larger systems should be in place.

7.0 Glossary

Quantum dot.

A confining structure for electrons, which can be designed to stably hold a small number of electrons.

Exchange coupling.

Basic physical interaction between the spins of electrons whose wave functions overlap, arising from the Pauli exclusion principle.

8.0 References

- [1] Loss, D. and D.P. DiVincenzo, "Quantum computation with quantum dots," *Physical Review A* **57**, 120–126 (1998).
- [2] Kane, B.E., "A silicon-based nuclear spin quantum computer," *Nature* **393**, 133–137 (1998).

- [3] Pazy, E., E. Biolatti, T. Calarco, I. D'Amico, P. Zanardi, F. Rossi, and P. Zoller "Spin-based optical quantum gates via Pauli blocking in semiconductor quantum dots," (19-Sep-2001) preprint *cond-mat/0109337*.
- [4] Piermarocchi, C., P. Chen, L.J. Sham, and D.G. Steel, "Optical RKKY interaction between charged semiconductor quantum dots," *Physical Review Letters* 89, 167402 (2002).
- [5] Gupta, J.A., R. Knobel, N. Samarth, and D.D. Awschalom, "Ultrafast manipulation of electron spin coherence," *Science* 292, 2458–2461 (2001).
- [6] Recher, P., E.V. Sukhorukov, and D. Loss, "Quantum dot as spin filter and spin memory," *Physical Review Letters* 85, 1962–1965 (2000).
- [7] Guest, J.R., T.H. Stievater, G. Chen, E.A. Tabak, B.G. Orr, D.G. Steel, D. Gammon, and D.S. Katzer, "Near-field coherent spectroscopy and microscopy of a quantum dot system," *Science* 293, 2224–2227 (2001).
- [8] Stevens, M.J., A.L. Smirl, R.D.R. Bhat, J.E. Sipe, and H.M. van Driel, "Coherent control of an optically injected ballistic spin-polarized current in bulk GaAs," *Journal of Applied Physics* 91, 4382–4386 (2002).
- [9] Kane, B.E., "Silicon-based quantum computation," *Progress of Physics* 48, 1023–1041 (2000).

Superconducting Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.7

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Terry Orlando

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0 Groups Pursuing This Approach	1
2.0 Background and Perspective	2
3.0 Summary of Superconducting QC: The DiVincenzo Criteria.....	3
4.0 What Has Been Accomplished.....	4
5.0 Considerations	6
6.0 Timeline.....	9
7.0 Glossary	9
8.0 References	9

List of Tables and Figures

Table 1-1 Approaches to Superconducting QC Research.....	1
Figure 6-1. Superconducting QC developmental timeline.....	9

List of Acronyms and Abbreviations

dc	direct current	rf	radio frequency
GHz	gigahertz	SET	single-electron transistor
GHZ	Greenberger, Horne, and Zeilinger	SFQ	single flux quantum
mK	millikelvin	SPD	single-photon detector
NMR	nuclear magnetic resonance	SQUID	superconducting quantum interference device
QC	quantum computing/computation	TEP	Technology Experts Panel

1.0 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Superconducting detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 1-1
Approaches to Superconducting QC Research

Research Leader(s)	Research Location	Research Focus
Averin & Likharev	StonyBrook	theory of superconducting qubits
Berggren	MIT	flux-based qubits
Bruder	Basel	theory of superconducting qubits
Buisson	Grenoble	charge-based qubits
Choi	Korea	theory of superconducting qubits
Clarke	Berkeley	flux-based qubits
Cosmelli	Rome	flux-based qubits
Delsing	Chalmers	charge-based qubits
Devoret	Yale	charge-based qubits
Echternach	JPL	charge-based qubits
Esteve	Saclay	charge-based qubits
Falci	Catania	theory of superconducting qubits
Fazio	Pisa	theory of superconducting qubits
Feldman/Bocko	Rochester	flux-based qubits
Han	Kansas	flux-based qubits AND single-junction phase-based qubits
Koch	IBM	flux-based qubits
Kouwenhoven	Delft	charge-based qubits
Ladizinsky	TRW	flux-based qubits
Levitov	MIT	theory of superconducting qubits
Likharev	StonyBrook	charge-based qubits
Lloyd	MIT	theory of superconducting qubits
Lukens, Likharev, & Semenov	StonyBrook	flux-based qubits
Manheimer	LPS	charge-based qubits
Martinis	UCSB	single-junction phase-based qubits
Mooij	Delft	flux-based qubits
Nakamura	NEC	charge-based qubits

**Table 1-1
Approaches to Superconducting QC Research**

Research Leader(s)	Research Location	Research Focus
Nori	Michigan and Riken	theory of superconducting qubits
Oliver, Gouker	Lincoln Lab	flux-based qubits
Orlando	MIT	flux-based qubits
Schoelkopf	Yale	charge-based qubits
Schön, Shnirman, & Makhlin	Karlsruhe	theory of superconducting qubits
Silvestrini	Naples	flux-based qubits
Simmonds	NIST	phase-based qubits
Tanaka	NTT	flux-based qubits
Ustinov	Erlangen	flux-based qubits
van Harlingen	Illinois	flux-based qubits
Wellstood, Anderson, & Lobb	Maryland	flux-based qubits AND single-junction phase-based qubits
Wilhelm	Munich	theory of superconducting qubits

2.0 Background and Perspective

The qubits are superconducting circuits made with Josephson junctions and operating at millikelvin (mK) temperatures. The information is stored in either the charge on a nanoscale superconducting island, the flux or phase drop in a circulating current, or in the energy levels in a single junction [1]. The interactions are either capacitive for charge-based circuits or inductive for flux- or phase-based circuits. Because these are electrical circuits, other electrical coupling elements are possible, such as tunnel junctions, transformers, single-electron transistors (SETs), etc.

The typical energy-level splitting between the qubit states varies between 1 and 10 GHz.

Clock speeds are estimated to be of the order of a nanosecond (this is the minimum time for a one-qubit rotation). The qubits are prepared in their initial state by cooling the system to their ground state. Then radio frequency (rf) electromagnetic pulses are used to manipulate the qubits to perform quantum operations. The manipulation of the superconducting qubits can be controlled by on-chip, ultrafast superconducting circuitry. For example, simple single-flux-quantum (SFQ) circuitry can operate at speeds up to 700 GHz with small power dissipation. There is a broad diversity of measurement options appropriate to different speeds and measurement bases. Most measurement schemes are based on superconducting quantum interference device (SQUID) magnetometers, SET electrometers, or switching of Josephson junctions.

3.0 Summary of Superconducting QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits 
 - 1.1 The existence of two quantum states has been demonstrated experimentally. 
 - 1.1.1 Charge states [2,3] 
 - 1.1.2 Flux states in rf SQUID [4], persistent-current qubit [5], and an asymmetric direct current (dc) SQUID and fluxon qubits [6] 
 - 1.1.3 Phase states in a single junction [7,8] 
 - 1.2 Rabi oscillations between the two-qubit states 
 - 1.2.1 Single junction [7,8] 
 - 1.2.2 Charge states [2,3] 
 - 1.2.3 Flux-based qubit [9] 
 - 1.3 Ramsey Fringe experiments in hybrid qubits [3] 
 - 1.4 No fundamental physical limits to scaling are currently known (note that few-qubit scaling vs many-qubit scaling will have very different challenges). 
2. The ability to initialize the state of the qubits to a simple fiducial state 
 - 2.1 The system is cooled to place the qubits in their ground states. 
 - 2.1.1 Initial experiments suggest this can be done >90% [8]. 
3. Long (relative) decoherence times, much longer than the gate-operation time 
 - 3.1 Calculations suggest the relaxation times are of the order of milliseconds or greater [1,10]. 
 - 3.2 Experimental measurements show at present a lower bound of about 1–10 μ s for the relaxation time, and 0.1–0.5 μ s for the dephasing time [2,3,7–9,11]. 
 - 3.3 Charge, flux, and critical-current noise are probably a technological and materials-processing problem [2,3,7–9,11]. 
 - 3.4 The nonresonant upper levels: in principle the effects of these levels can be compensated by a pulse sequence which allows the system to act as an effective two-level system [12]. 
 - 3.5 Experiments have demonstrated about a thousand gate operations prior to decoherence [3]. 

4. A universal set of quantum gates 
 - 4.1 Many different schemes have been proposed for a universal set of two-level systems for gates in superconducting qubits. Most schemes are based on an NMR-like approach of using pulses of microwave radiation to perform qubit operations. In addition, nonadiabatic switching has been used to manipulate a single superconducting qubit [1]. 
 - 4.2 Parallel operations are possible in principle. 
5. A qubit-specific measurement capability 
 - 5.1. There is a broad diversity of measurement options appropriate to different speeds and measurement bases. 
 - 5.1.1 RF-sets and SET-electrometers are used for charge states [13]. 
 - 5.1.2 SQUIDs are used to readout flux states, either by measuring its switching current modulation or by measuring its inductance [4,5,14,15,16]. 
 - 5.1.3 In the phase qubit, the switching current is measured [7,8]. 
 - 5.1.4 In hybrid circuits, the qubit and readout can be of different types. However, additional theoretical work is needed to build a testable, phenomenological model to optimize the measurement process [3]. 
6. The ability to interconvert stationary and flying qubits 
 - 6.1 An optical cavity interacting with a flying qubit has been suggested. 
7. The ability to faithfully transmit flying qubits between specified locations 
 - 7.1 A superconducting transmission line has been suggested. 

4.0 What Has Been Accomplished

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states [2,4,5,7,8]. 
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.2 Demonstrate decoherence times much longer than Rabi oscillation period [3,7-9,11]. 
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 

3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations [17]. 
 - 3.2 Produce and characterize Bell states. 
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times [17]. 
 - 3.4 Demonstrate quantum state and process tomography for two qubits. 
 - 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS). 
 - 3.6 Demonstrate a two-qubit quantum algorithm. 
4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, & Zeilinger (GHZ) state of three physical qubits. 
 - 4.2 Produce maximally entangled states of four and more physical qubits. 
 - 4.3 Quantum state and process tomography. 
 - 4.4 Demonstrate decoherence-free subspaces. 
 - 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
 - 4.6 Demonstrate quantum error-correcting codes. 
 - 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
 - 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
7. Operations on 3–logical qubits
 - 7.1 Produce a GHZ state of three logical qubits. 
 - 7.2 Produce maximally entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

5.0 Considerations

1. Special strengths
 - 1.1 The use of superconductors ensures an inherently low-dissipation, long-range-phase-coherent technology.
 - 1.2 The technology is a proven one for fabrication, measurement, and control.
 - 1.2.1 The technology requires incremental improvements for progress, but not qualitatively new developments[[18]].
 - 1.2.2 The fabrication technology enables integration of qubits with custom electronics for fast control and readout[[18]].
 - 1.2.3 Established superconducting electronics can be used to engineer the Hamiltonian. The Hamiltonian can also be modified by fabrication and by voltages and currents.
 - 1.2.4 Relatively strong interactions allow for gating and control, with a very fast speed of operation.
 - 1.3 A broad diversity of approaches for qubits has already been demonstrated.
 - 1.4 The preparation of a pure state is easy; it relies only on cooling the qubit to low temperatures.
2. Unknowns, weaknesses
 - 2.1 Sources of noise need to be identified and the mechanisms of relaxation and dephasing need to be quantified. Are there new mechanisms of decoherence that can only be observed in highly entangled systems?
 - 2.2 Quantitative comparisons need to be made on the experiments and theory concerning the effect of the electromagnetic environment on one-qubit operations and dephasing and relaxation times.
 - 2.3 Characterization of the fabrication of qubits and associated circuitry needs to be standardized by developing standards for the quality of junctions; reducing flux, charge, and critical-current noise; and assessing the best material.
 - 2.4 Inherent nonuniformity of the qubits from fabrication inaccuracies needs to be assessed theoretically and experimentally.
 - 2.5 Broad diversity of approaches for qubits, control, and measurement possibilities will require an assessment of these types.
3. Goals 2002–2007
 - 3.1 The physical limitations of single and coupled physical qubits will be understood and controlled.
 - 3.1.1 Major sources of decoherence in superconducting systems will be identified and quantified.
 - 3.1.2 The effect of the electromagnetic environment will be controlled.
 - 3.1.3 Phenomenological theories of measurement and control.

- 3.2 Three-to-five entangled qubits will be demonstrated and controlled in various types of qubits.
 - 3.2.1 Two-qubit gates and simple algorithms will be demonstrated.
 - 3.2.2 On-chip superconducting electronics will be used for the manipulation of a single qubit for some approaches.
- 3.3 A plan will be developed for scaling to 10 physical qubits.
- 3.4 An assessment will be made of the alternative types of qubits and fabrication schemes.
 - 3.4.1 Some narrowing of diversity of superconducting qubits will be done.
 - 3.4.2 Reliable fabrication processes and the associated materials issues will be identified.
4. Goals 2007–2012
 - 4.1 Encode a single-qubit state into a logical qubit formed from several qubits.
 - 4.1.1 Demonstrate ten or more entangled qubits.
 - 4.2 Perform repetitive error correction of a logical qubit.
 - 4.2.1 Develop fast control and readout schemes with superconducting electronics.
 - 4.2.2 Reduce noise due to fluctuations of the charge, flux noise, and critical current.
 - 4.3 Plan to be developed for scaling to 100 or more entangled qubits.
 - 4.4 Assess the best types of superconducting qubits.
5. Necessary achievements
 - 5.1 No clear roadblocks exist at this time.
6. Trophies
 - 6.1 A superconducting qubit which is robust during its operation to fluctuations due to charge, flux, and critical current.
 - 6.2 Experimental confirmation of theory to predict decoherence in superconducting circuits.
 - 6.3 Coupling of two superconducting qubits.
 - 6.4 Fast control and manipulations of a qubit with on-chip superconducting electronics.
 - 6.5 Fabrication process capable of producing qubits with long coherence times and integration of SFQ electronics.
 - 6.6 Theory to assess and to overcome the effects of the inherent fabrication differences in qubits.
 - 6.7 Development of fault-tolerant schemes for superconducting qubits.
 - 6.8 Development of interfaces between disparate quantum technologies (e.g., microwaves and superconducting qubits) for flying qubit.
 - 6.9 Novel uses of superconducting qubits.

7. Connections with other quantum information science technologies
 - 7.1 Improved instrumentation and sensors operating at the quantum limit that use entanglement and squeezing.
 - 7.2 Experimental tests of quantum mechanics on a macroscopic scale.
 - 7.3 Superconducting devices are being used as single photon detectors (SPDs) for quantum key distribution [19].
8. Subsidiary developments
 - 8.1 Improved instrumentation and sensors operating at the quantum limit that use entanglement and squeezing will be developed.
 - 8.2 Experimental tests of quantum mechanics on a macroscopic scale will be possible with some types of superconducting qubits.
9. Role of theory
 - 9.1 Develop a detailed theory of the sources of decoherence.
 - 9.2 Formulate a theory for scaling, including threshold theorems for particular architectures.
 - 9.3 Develop fault-tolerant schemes which use the unique properties of superconductor.
 - 9.4 Design novel architectures to exploit better algorithm implementation.
 - 9.5 Design novel uses of superconducting qubits for quantum-limited instrumentation.
 - 9.6 Make a more generic the connection between classical dissipation and quantum decoherence.
 - 9.7 Develop methods of determining degree of entanglement and benchmark the fidelity of operations of multiqubit systems
 - 9.8 Optimize error correction for realistic noise sources.
 - 9.9 Develop of interfaces between disparate quantum technologies (e.g., microwaves and superconducting qubits).

6.0 Timeline

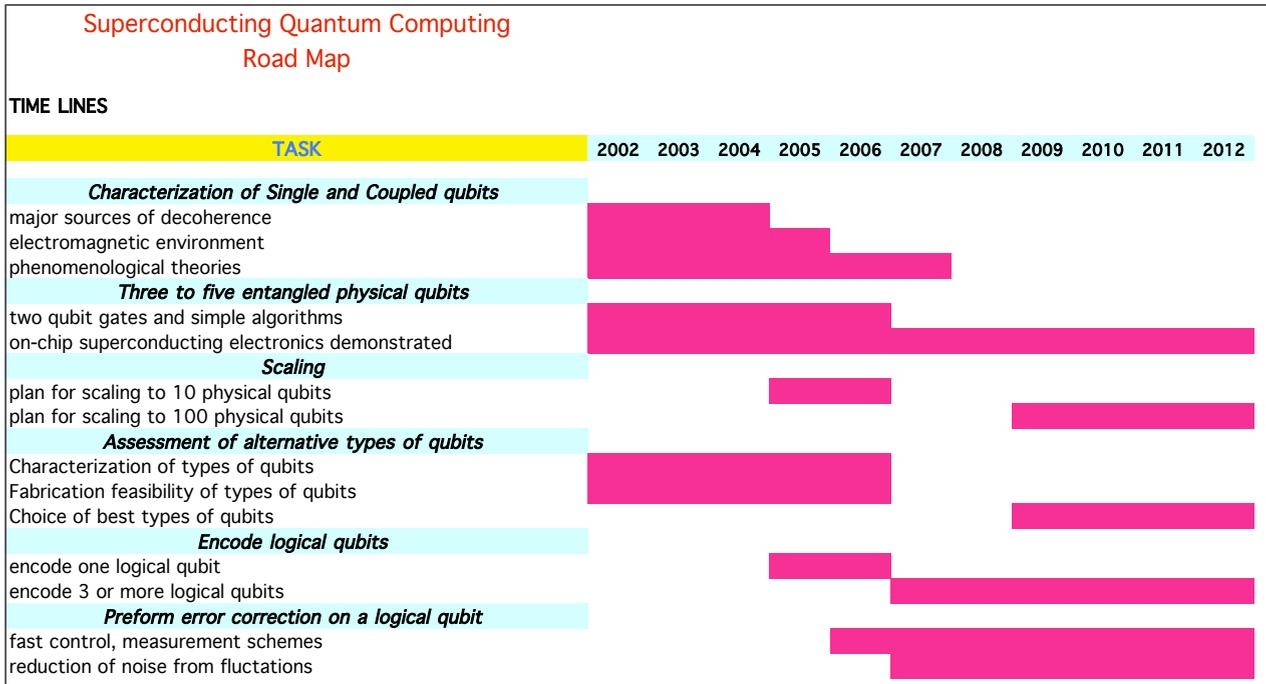


Figure 6-1. Superconducting QC developmental timeline.

7.0 Glossary

8.0 References

Note: The following references mostly detail the experimental progress, and are only a partial list of results. Much of the theory and earlier work is reviewed in Reference 1.

- [1] Maklin, Y., G. Schön, and A. Shnirman, "Quantum-state engineering with Josephson-junction devices," *Reviews of Modern Physics* **73**, 357–400 (2001).
- [2] Nakamura, Y., Y.A. Pashkin, and J.S. Tsai, "Coherent control of macroscopic quantum states in a single-Cooper-pair box," *Nature* **398**, 786–788 (1999).
- [3] Vion, D., A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, and M.H. Devoret "Manipulating the quantum state of an electrical circuit," *Science* **296**; 886–889 (2002).
- [4] Friedman, J.R., V. Patel, W. Chen, S.K. Tolpygo, and J.E. Lukens, "Quantum superposition of distinct macroscopic states," *Nature* **406**, 43–46, (2000).

- [5] van der Wal, C.H., A.C.J. ter Haar, F.K. Wilhelm, R.N. Schouten, C.J.P.M. Harmans, T.P. Orlando, S. Lloyd, and J.E. Mooij, "Quantum superposition of macroscopic persistent-current states," *Science* **290**, 773–777 (2000).
- [6] Koch, R., *et al.*, (not published).
- [7] Yu, Y., S. Han, X. Chu, S.-I. Chu, and Z. Wang, "Coherent temporal oscillations of macroscopic quantum states in a Josephson junction," *Science* **296**, 889–892 (2002).
- [8] Martinis, J.M., S.-W. Nam, J. Aumentado, and C. Urbina, "Rabi oscillations in a large Josephson-junction qubit," *Physical Review Letters* **89**, 117901 (2002).
- [9] ter Haar, A., J.E. Mooij, *et al.*, (not published).

Probable reference (consistent with words in the citing text):

Title:Decoherence of flux qubits coupled to electronic circuits Author:Wilhelm, FK ; Storez, MJ ; van der Wal, CH ; Harmans, CJPM ; Mooij, JE Institution:Univ Munich, Sekt Phys, D-80333 Munich, Germany Journal:ADVANCES IN SOLID STATE PHYSICS; 2003; v.43, p.763-778 Conference:Spring Meeting of the Argeitskreis-Festorperphysik of the Deutsche-Physikalische-Gesellschaft; March 24-28, 2003; DRESDEN, GERMANY

- [10] Tian, L., L. Levitov, C.H. van der Wal, J.E. Mooij, T.P. Orlando, S. Lloyd, C.J.P.M. Harmans, and J.J. Mazo, "Decoherence of the superconducting persistent current qubit," in *Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics*, I.O. Kulik and R. Ellialogulu, Eds. (Kluwer Academic Publishers, Dordrecht, Netherlands, 2000) Part VII, #28.
- [11] Nakamura, Y., Y.A. Pashkin, and J.S. Tsai, "Rabi oscillations in a Josephson-junction charge two-level system," *Physical Review Letters* **87**, 246601 (2001).
- [12] Tian, L. and S. Lloyd, "Resonant cancellation of off-resonant effects in a multilevel qubit," *Physical Review A* **62**, 050301 (2000).
- [13] Aassime, A., G. Johansson, G. Wendin, R.J. Schoelkopf, and P. Delsing, "Radio-frequency single-electron transistor as readout device for qubits: Charge sensitivity and backaction," *Physical Review Letters* **86**, 3376–3379 (2001).
- [14] Bocko, M.F., A.M. Herr, and M.F. Feldman, "Prospects for quantum coherent computation using superconducting electronics," *IEEE Transactions on Applied Superconductivity* **7**, 3638–3641 (1997).
- [15] Carelli, P., M.G. Castellano, F. Chiarello, C. Cosmelli, R. Leoni, and G. Torrioli, "SQUID systems for macroscopic quantum coherence and quantum computing," *IEEE Transactions on Applied Superconductivity* **11**, 210–214 (2001).
- [16] Granata, C., V. Corato, L. Longobardi, M. Russo, B. Ruggiero, and P. Silvestrini, "Josephson device for quantum experiments," *Applied Physics Letters* **80**, 2952–2954 (2002).

- [17] Yamamoto, T., Y.A. Pashkin, O. Astafiev, Y. Nakamura, and J.S. Tsai, "Demonstration of conditional gate operation using superconducting charge qubits," *Nature* **425**, 941–944 (2003).
- [18] Berggren, K., D. Nakada, T.P. Orlando, E. Macedo, R. Slattery, and T. Weir, "An integrated superconductive device technology for qubit control," *Proceedings of the International Conference on Experimental Methods in Quantum Computation*, (Rinton Press, 2001) pp. 121–126.
- [19] Verevkin, A., J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G.N. Gol'tsman, and A. Semenov, "Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range," *Applied Physics Letters* **80**, 4687–4689 (2002).

“Unique” Qubits Approaches to Quantum Information Processing and Quantum Computing

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.8

Disclaimer:

The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not be taken to indicate in any way an official position of U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Seth Lloyd and P. Chris Hammel

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0 Introduction	1
2.0 Electrons on Helium Films Approaches to Quantum Information Processing and Quantum Computing	3
2.1 Groups Pursuing This Approach.....	3
2.2 Background and Perspective.....	3
2.3 Summary of Electrons on Helium QC: The DiVincenzo Criteria.....	4
2.4 What Has Been Accomplished	5
2.5 Considerations.....	6
3.0 Spectral Hole Burning Approaches to Quantum Information Processing and Quantum Computing.....	7
3.1 Summary of Spectral Hole Burning QC: The DiVincenzo Criteria	7
3.2 References	9

List of Tables and Figures

Table 2.1-1 Approaches to Electrons on Helium Films QC Research	3
---	---

List of Acronyms and Abbreviations

C-NOT	controlled-NOT (gate)	QDs	quantum dots
DFS	decoherence-free subspace	QED	quantum electrodynamics
GHz	gigahertz	QIP	quantum information processing
GHZ	Greenberger, Horne, and Zeilinger	rf	radio frequency
MEMS	micro-electro-mechanical systems	SHB	spectral hole burning
mK	milliKelvin	SPD	single-photon detector
NMR	nuclear magnetic resonance	SPS	single-photon source
NV	nitrogen-vacancy	TEP	Technology Experts Panel
QC	quantum computation/computing	UV	ultraviolet

1.0 Introduction

In addition to the relatively well-established methods for performing quantum information processing (QIP) and quantum computing (QC) described in detail earlier in this document, there exist potentially fruitful approaches to QIP based on a variety of quantum technologies.

Virtually any quantum system that is addressable, controllable, and coherent has the potential to perform QC. The situation is reminiscent of the early days of digital computing, when switches and circuits were constructed from a variety of technologies, including electromechanical relays, vacuum tubes, and even from purely mechanical and hydraulic components in environments where electrical systems were inappropriate. Even today, when virtually all computers are based on integrated circuits, memory technologies exhibit considerable diversity. There are a variety of types of integrated circuits for memory, as well as magnetic memories (hard disks) and optical memories (CDs). Perhaps as a result of the diversity of different memory technologies, the Moore's law rate of increase of density of memory circuits has followed a more rapid pace than that of processing circuits. Similarly, we anticipate that a variety of different QIP technologies may be used for different purposes as the field matures further.

This section lists several such approaches to QIP. There exist tens of such "unique" approaches: not all will be described here. Rather, this section will concentrate on approaches that have current, funded research programs: these approaches have been thoroughly researched and found worth further investigation. It is anticipated that in the future more unique approaches will arise; these will be evaluated as they arrive. In addition, the ongoing research will serve to show which of these various approaches are the most promising. Summaries of existing efforts follow; which include general discussions of the state of the art for input-output, coherent computation, and decoherence. For two of these approaches, electronics on helium QC and spectral hole burning QC, short additional write-ups are included in the following sections.

QIP using Nanotubes and Nanowires.

Carbon nanotubes and silicon nanowires represent a well-developed nanotechnology. Such systems are known to exhibit significant degrees of quantum coherence for electron transport. Nanotubes can be used to create arrays of quantum dots (QDs) whose coupling can be turned on and off using silicon nanowires. Such systems share virtues and deficiencies with lithographed QD systems and potentially possess additional features, such as an enhanced degree of regularity of the dots due to the chemical synthesis of the nanotubes. Experimental efforts exist: further research is being performed on input-output, coherent control, and the properties of decoherence of electron spin in nanotube systems.

Quantum Logic Using Electrons on the Surface of Liquid Helium.

Electrons on the surface of liquid helium represent a clean system for registering and processing quantum information. The electrons effectively float above the surface of the helium, and their states can be manipulated by microwaves and by circuits embedded in the silicon substrate below the helium film. Experiments have been performed exhibiting single-electron detection, and are underway to exhibit coherent control of electrons on helium by the application of

microwaves. Further investigations are taking place into the properties of decoherence and into the performance of quantum logic operations in such systems.

Molecular Spin Arrays

Chemical techniques can be used to produce self-assembled arrays of molecules containing electron spins. Such systems represent natural candidates for quantum computers with a cellular-automaton architecture. Experiments on such systems are in the initial phase. Issues of decoherence, input-output, and coherent control are understood to some degree in theory; more theoretical and experimental investigations are underway.

Quantum Hall Effect QC

Quantum-Hall-effect systems are well-studied experimentally and represent good potential systems in which to perform QIP. Quantum information can be stored on highly coherent, long-lived nuclear spins, then transferred to electron spins and excitons for information transmission and readout. Coherence times have been measured in such systems and are favorable for QC. Detailed studies of input-output characteristics, decoherence, and quantum logic operations are underway.

QC using Nonabelian Anyons

Topological methods for QC have attracted considerable interest because of their intrinsically fault-tolerant properties. In such methods, quantum information is stored on nonabelian anyons, and quantum logic operations are performed by 'braiding' the anyons around each other in a two-dimensional plane. Nonabelian anyons are relatively exotic systems, which could potentially be constructed using arrays of quantum logic gates (e.g., superconducting quantum logic circuits) or implemented using the higher order fractional quantum Hall effect. Preliminary theoretical investigations of both types of approaches indicate their feasibility. Experiments are forthcoming.

QC using the Fractional Quantum Hall Effect

QC can also be performed in a topological fashion using abelian anyons, such as the usual fractional quantum Hall quasiparticles. Abelian anyons share some, though not all, of the fault-tolerance of the nonabelian anyons discussed above, and have the advantage that they have been investigated and manipulated experimentally. Theoretical and experimental investigations are currently underway to determine levels of decoherence for quantum Hall quasiparticles, and to perform simple quantum logic operations.

Electro-Mechanical Systems for QIP

Nanofabricated mechanical resonators exhibit high Qs and quantum coherence. Such mechanical devices represent natural structures on which to perform QIP. They can be coupled to electronic systems for measurement and control purposes. They can be interfaced, in principle, with superconducting quantum computers. Initial theoretical and experimental

investigations on quantum control and decoherence for such systems have been performed; more extensive investigations are in progress.

QC using Spectral Hole Burning

Spectral hole burning is a well-established technique for addressing optically active atoms in solids. It allows for a potentially high density of quantum bits by using both spatial and frequency addressing techniques. A variety of models for quantum computing using spectral hole burning have been investigated, using optical cavities and/or dipolar coupling between spectral holes. Experimental investigations of the controllability and coherence properties of spectral holes have been performed and indicate a level of controllability comparable to normal quantum optical approaches to QC, with reduced coherence due to the solid-state nature of spectral hole systems. Current experimental investigations are aimed towards elucidating the coherence structure of spectral holes and towards coupling spectral holes to perform quantum logic operations.

2.0 Electrons on Helium Films Approaches to Quantum Information Processing and Quantum Computing

2.1 Groups Pursuing This Approach

Note: This document constitutes the most recent draft of the Electrons on Helium Films detailed summary in the process of developing a roadmap for achieving QC. Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

Table 2.1-1
Approaches to Electrons on Helium Films QC Research

Research Leader(s)	Research Location
Goodkind, J.	UC-San Diego
Dahm, A.	Case Western Reserve
Dykman, M.	Michigan State U.
Platzman, P.	Bell Labs
Lea, M.	Royal Holloway
Mukharsky, Y.	Saclay
Kono, K.	Riken, Japan

2.2 Background and Perspective

Electrons on a helium surface are attracted to the surface by the helium dielectric image potential and occupy "hydrogenic" states associated with motion normal to the helium surface

with a Rydberg energy of $\sim 8\text{K}$. A Pauli exclusion force prevents electrons from entering the liquid. Electrons are localized laterally by a microelectrode (post) located under each electron. The posts are separated by a distance $d \sim 1\ \mu\text{m}$ and are covered with an $\sim 1\text{-}\mu\text{m}$ -thick helium film. The states for lateral motion are harmonic oscillator states in the post potential with an energy separation of $\sim 1\text{K}$. The ground and excited states in the hydrogenic potential are identified with the $|0\rangle$ and $|1\rangle$ components of a qubit.

2.3 Summary of Electrons on Helium QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
- b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
- c)  = no viable approach is known.

1. A scalable physical system with well-characterized qubits 

Electrons on a helium surface are attracted to the surface by the helium dielectric image potential and occupy "hydrogenic" states associated with motion normal to the helium surface with a Rydberg energy of $\sim 8\text{K}$. A Pauli exclusion force prevents electrons from entering the liquid. Electrons are localized laterally by a microelectrode (post) located under each electron. The posts are separated by a distance $d \sim 1\ \mu\text{m}$ and are covered with an $\sim 1\text{-}\mu\text{m}$ -thick helium film. The states for lateral motion are harmonic oscillator states in the post potential with an energy separation of $\sim 1\text{K}$. The ground and excited states in the hydrogenic potential are identified with the $|0\rangle$ and $|1\rangle$ components of a qubit. In principle, this system is scalable to an arbitrary number of qubits.
2. Ability to initialize the state of the qubits to a simple fiducial state 

Once placed on the helium surface, the electrons relax to the ground state in a time scale of $\sim 1\ \mu\text{s}$. The energy separation of the excited state is controlled by a Stark field applied to the posts and is of order $100\ \text{gigahertz (GHz)}$, so at the operating temperature of $10\ \text{milliKelvins (mK)}$ ($\sim 0.2\ \text{GHz}$) all of the qubits are easily and reliably initialized into their ground states.
3. Long (relative) decoherence times, much longer than the gate-operation time 

Phonon emission into the liquid dominates the decay of the excited state with a lifetime of $\sim 100\ \mu\text{s}$ (T_1). Coupling is via phonon modulation of the surface level and image potential. The dephasing time (T_2) is estimated to be $\sim 100\ \mu\text{s}$ due to Nyquist noise on the electrodes, so decoherence/gate time ratios are $\sim 10^5$.

4. Universal set of quantum gates 

The operation begins with all qubits in the $|0\rangle$ state. Single-qubit operations are performed by Stark shifting qubits into resonance with an radio frequency (rf) field applied for a prescribed length of time. An expansion gives a dipolar interaction term between qubits $\mu \frac{e^2(z_2 - z_1)^2}{d^3}$. The computer will be operated at a temperature of 10mK. Quantum gates are implemented by bringing neighboring qubits into resonance alone (SWAP) or in conjunction with an rf field (C-NOT—controlled-NOT). The time required for a SWAP operation depends on the spacing between electrons (i.e., posts), and is ~ 1 ns for a 0.5 μ m spacing between.
5. A qubit-specific measurement capability 

A simultaneous readout of all qubits will be accomplished by applying a moderate extracting field such that electrons in the $|1\rangle$ state will tunnel from the surface. Subsequently, a large extracting field will be applied sequentially to each post such that electrons in the $|0\rangle$ state will tunnel into the vacuum. Electrons detected (not detected) by the bolometer detector will register a $|0\rangle$ ($|1\rangle$) for that post.
6. The ability to interconvert stationary and flying qubits 
7. The ability to faithfully transmit flying qubits between specified locations 

2.4 What Has Been Accomplished

Note: For the status of the metrics of QC described in this section, the symbols used have the following meanings:

- a)  = sufficient experimental demonstration;
- b)  = preliminary experimental demonstration, but further experimental work is required; and
- c)  = no experimental demonstration.

1. Creation of a qubit
 - 1.1 Demonstrate preparation and readout of both qubit states. 

The system consists of two parallel plates that form the upper and lower surfaces of an expanded waveguide. The microelectrodes are incorporated in the lower plate that is covered with a helium film. A tungsten superconducting transition-edge bolometer able to detect 10 eV electrons in the read-out process and a tunnel-diode electron source for loading electrons onto the posts have been fabricated and are located above a small opening in the upper plate.
2. Single-qubit operations
 - 2.1 Demonstrate Rabi flops of a qubit. 
 - 2.2 Demonstrate high-Q of qubit transition. 
 - 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere. 

3. Two-qubit operations
 - 3.1 Implement coherent two-qubit quantum logic operations. 
 - 3.2 Produce and characterize Bell states. 
 - 3.3 Demonstrate decoherence times much longer than two-qubit gate times. 
4. Operations on 3–10 physical qubits
 - 4.1 Produce a Greenberger, Horne, & Zeilinger (GHZ)-state of three physical qubits. 
 - 4.2 Produce maximally entangled states of four and more physical qubits. 
 - 4.3 Quantum state and process tomography. 
 - 4.4 Demonstrate DFSs. 
 - 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations, etc.) between physical qubits. 
 - 4.6 Demonstrate quantum error correcting codes. 
 - 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza). 
 - 4.8 Demonstrate quantum logic operations with fault-tolerant precision. 
5. Operations on one logical qubit
 - 5.1 Create a single logical qubit and "keep it alive" using repetitive error correction. 
 - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit. 
6. Operations on two logical qubits
 - 6.1 Implement two-logical-qubit operations. 
 - 6.2 Produce two-logical-qubit Bell states. 
 - 6.3 Demonstrate fault-tolerant two-logical-qubit operations. 
7. Operations on 3–10 logical qubits
 - 7.1 Produce a GHZ-state of three logical qubits. 
 - 7.2 Produce maximally-entangled states of four and more logical qubits. 
 - 7.3 Demonstrate the transfer of quantum information between logical qubits. 
 - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits. 
 - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits. 

2.5 Considerations

1. Special strengths
 - 1.1 The physics is well-understood and has been experimentally explored.
 - 1.2 The system naturally presents long decoherence times due to intrinsic cleanliness of helium films.
 - 1.3 The qubit separation of $\sim 1 \mu\text{m}$ is lithographically well within reach.

- 1.4 The range of interaction energy between qubits in the presence of a ground plane is $\mu \bar{e}^2 / r^3$, a short range interaction that improves controllability of qubit interactions.
2. Unknowns, weaknesses
3. Five-year goals
 - 3.1 Within the next year, we expect to localize electrons above posts and detect electrons that tunnel from the surface in an extracting field, and perform single and two-qubit operations.
 - 3.2 Explore materials other than helium, such as neon, which have larger excited-state separations allowing use of lasers to couple to qubits.

3.0 Spectral Hole Burning Approaches to Quantum Information Processing and Quantum Computing

Note: This document constitutes the most recent draft of the Spectral Hole Burning detailed summary in the process of developing a roadmap for achieving QC. Please submit any revisions to this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input can we improve this roadmap as a guidance tool for the continued development of QC research.

3.1 Summary of Spectral Hole Burning QC: The DiVincenzo Criteria

Note: For the five DiVincenzo QC criteria and the two DiVincenzo QC networkability criteria (numbers six and seven in this section), the symbols used have the following meanings:

- a)  = a potentially viable approach has achieved sufficient proof of principle;
 - b)  = a potentially viable approach has been proposed, but there has not been sufficient proof of principle; and
 - c)  = no viable approach is known.
1. A scalable physical system with well-characterized qubits 

To illustrate the basic mechanism behind the spectral-hole-burning (SHB) approach to quantum computing, consider a small volume of a medium such as nitrogen-vacancy (NV) color centers in diamond [1]. A laser beam incident on this volume can interact with all the centers in this volume. However, each center has a transition frequency that is slightly different from that of the others, a feature known as inhomogeneous broadening. This implies that individual centers can be addressed distinctively by tuning the laser, if the system is prepared so that only a single center is present in each spectral band. This enables single-qubit operations [1,2]. In order to perform two qubit operations, such as the C-NOT, it is necessary to couple two centers that are spectrally adjacent [1]. One mechanism for such a coupling is the dipole-dipole interaction [3]. However, because the spectral neighbors are not necessarily close to each other spatially, it is necessary to enhance this interaction artificially. This can be achieved by embedding the centers in a high-Q optical cavity. The number of qubits that can be realized this way in a single

diffraction-limited spot can be as high as 10^5 for realistic parameters, making this scheme a good candidate for **scalable QC**. Many spots on a single crystal, each containing a quantum computer, can also be used for the so-called type II quantum computing for efficient simulation of lattice gas dynamics [4,5]. Furthermore, this approach is readily suited for coupling the individual quantum computers via optical means [6].

The qubit in this process is a spin transition that is excited by a Raman interaction. In order to realize distinct qubits, we must have at most one atom per spectral channel. As discussed in detail in reference 1, this can be achieved in NV-diamond by making use of a storage level where all but one atom from each channel can be transferred to for a long time (hours). As such, this system can be claimed to have a **well characterized qubit**.

2. Ability to initialize the state of the qubits to a simple fiducial state 

This criterion pertains to the ability to prepare the quantum bits in a pure (0 or 1) state. At the onset, there are two metastable states in NV-Diamond [7] that are both occupied, with the normalized population difference determined by the exponent of the negative of the ratio of Δ and the product of the temperature and the Boltzmann constant. For the case of nuclear magnetic resonance (NMR) at room temperature, this implies that the number of spins that are in a pure state is very small. For other systems such as phosphorous in QDs, this problem requires that the quantum computer be operated at temperatures in the mK regime. In our model, near-perfect alignment can be produced at much higher temperatures (at least up to 15K, accessible by compressor-based closed-cycle cryostats), via a process known as the two-photon induced coherent population trapping, or the dark resonance [1,2].
3. Long (relative) decoherence times, much longer than the gate-operation time 

This criterion requires that the time needed to perform a single operation should be much less than the dephasing time of the qubits. In NV-diamond, the dephasing time is about 0.1 ms, while the time for a single operation can be as low as 100 ns. The number of operations that can be performed before dephasing can thus be as high as 10^3 . The dephasing time can be reduced further by

 - a. using samples that are free from ^{13}C and
 - b. using techniques of dynamic noise suppression developed in the context of NMR quantum computing [8].
4. Universal set of quantum gates 

We have identified in explicit detail two different methods for realizing a C-NOT operation between two nearest-neighbor qubits in NV-diamond. The first method [3], applicable to high-density of color centers, uses the direct optical dipole-dipole coupling between two qubits that are very close to each other spatially and can be turned into spectral neighbors via applying a magnetic field. This method is somewhat limited in the number of bits that can be coupled. The second method [1], applicable to low-density of color centers, uses a high-finesse optical cavity, resonant with a transition common to both bits, in order to enhance the optical dipole-dipole coupling. The number of qubits that can be realized this way can be as high as 10^5 .

5. A qubit-specific measurement capability 

In the model of reference 1, the two laser photons used to excite the qubit can be encoded (in the form of the amplitude and phase of the beat between the two frequencies) with the quantum information during the input process. The information then can be transferred to a distinct qubit occupying the matching spectral channel. The reversal of this process enables the retrieval of the quantum information from distinct qubits.
6. The ability to interconvert stationary and flying qubits 

The SHB model inherently satisfies this criterion, because the quantum bit can be copied in to the state of a cavity photon, which in turn can transmit the bit to another system upon exiting the cavity. This converts a stationary qubit in to a flying one. The reverse process enables the conversion of a flying qubit in to a stationary qubit.
7. The ability to faithfully transmit flying qubits between specified locations 

Once the flying qubit exits in the cavity at one location, it can then be transmitted to the other location via free-space or via an optical fiber, and then coupled to the cavity at the other location for conversion into a stationary qubit, in a manner analogous to reference 8.

3.2 References

- [1] Shahriar, M.S., P.R. Hemmer, S. Lloyd, P.S. Bhatia, and A.E. Craig, "Solid-state quantum computing using spectral holes," *Physical Review A* **66**, 032301 (2002).
- [2] Hemmer, P.R., A.V. Turukhin, M.S. Shahriar, and J.A. Musser, "Raman excited spin coherence in NV-diamond," *Optics Letters* **26**, 361–363 (2001).
- [3] Lukin, M.D. and P.R. Hemmer, "Quantum entanglement via optical control of atom-atom interactions," *Physical Review Letters* **84**, 2818–2821 (2000).
- [4] Yepez, J., "Lattice-gas quantum computation," *International Journal of Modern Physics C* **9**, 1587–1596 (1998);
- [5] Yepez, J., "Quantum computation of fluid dynamics," Quantum Computing and Quantum Communications, First NASA International Conference (QCQC'98), Palm Springs, California, USA, February 17–20, 1998, published in *Lecture Notes in Computer Science* **1509**, 34–60 (1999)
- [6] Turukhin, A.V., V.S. Sudarshanam, M.S. Shahriar, J.A. Musser, B.S. Ham, and P.R. Hemmer, "Observation of ultraslow and stored light pulses in a solid," *Physical Review Letters* **88**, 023602 (2002).
- [7] Redman, D.A., S.W. Brown, and S.C. Rand, "Origin of persistent hole burning of N-V centers in diamond," *Journal of the Optical Society of America B* **9**, 768 (1992).
- [8] Viola, L., S. Lloyd, and E. Knill, "Universal control of decoupled quantum systems," *Physical Review Letters* **83**, 4888–4891 (1999).

Theory Component of the Quantum Information Processing and Quantum Computing Roadmap

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.9

Disclaimer:

The opinions expressed in this document are those of the Technology Experts' Panel members and are subject to change. They should not be taken to indicate in any way an official position of the U.S. Government sponsors of this research.

April 2, 2004
Version 2.0



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Seth Lloyd, David DiVincenzo, Umesh Vazirani, Gary Doolen and
Birgitta Whaley

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

1.0	Introduction	1
2.0	Fundamental Theoretical Challenges	1
2.1	Quantum Algorithms	2
2.2	Quantum Complexity Theory	3
2.3	Fault-Tolerant Quantum Computing	3
2.4	Simulation of Quantum Systems	3
3.0	Quantum Computation Historical Review	3
3.1	A Short Summary of Significant Breakthroughs in Quantum Information Theory	3
3.2	Current Developments and Directions	7
4.0	Quantum Information Theory	12
4.1	Capacities	13
4.2	Entanglement and Correlations	15
4.3	Cryptographic Primitives	19
5.0	Quantum-Computer Architectures	22
5.1	Initial Conceptual Development	23
5.2	Testing the Components	24
5.3	Assembling the Components into a Working Device	24
5.4	Scaling up the Architecture	25
5.5	“Type-II” Quantum Computing	25
6.0	Decoherence Roadblocks for Quantum Information Processing	26
6.1	Theoretical Terminology	26
6.2	Studies of Decoherence and Ways to Overcome It	27
6.3	Physical Sources of Decoherence	28
6.4	Decoherence Analyses	31
7.0	Glossary	33
8.0	References	33

List of Acronyms and Abbreviations

1-D	one dimensional	POVM	positive operator value measurement
2-D	two dimensional	PPT	positive under partial transposition
3-D	three dimensional	PSPACE	problem solvable with polynomial memory
BQNP	bounded quantum analogue of NP	QC	quantum computation/computing
BQP	bounded quantum polynomial	QCPR	Quantum Computing Program Review
DFS	decoherence-free subspace	QCRYPT	quantum cryptography
EPR	Einstein, Podolsky, Rosen	QIP	quantum information processing/processor
HSP	hidden subgroup problem	QIT	quantum information theory
IP	interaction proof	QSAT	quantum analog of satisfiable problem
LOCC	local operations and classical communication	QSPIR	quantum k-server symmetrically private information-retrieval (system)
MA	Merlin-Arthur (problems)	SPIR	symmetrically private information-retrieval (system)
NMR	nuclear magnetic resonance	SZK	statistical zero knowledge
NP	nondeterministic polynomial (time)	TEP	Technology Experts Panel
P	polynomial (time)		
PIR	private-information-retrieval (system)		

1.0 Introduction

Note: This document constitutes the most recent draft of the Theoretical Approaches detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any comments or suggestions on this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input we can improve this roadmap as a guidance tool for the continued development of QC research.

This section of the Quantum Computing Roadmap is the initial effort of the TEP to summarize the theoretical aspects of QC and quantum information theory (QIT). Section 2 gives an overview of the role of theory in constructing quantum computers. Section 3.1 presents a historical survey of some of the key theoretical developments in QC. Section 3.2 gives a more detailed landscape of the important theoretical challenges in QC, and highlights some grand challenges. Section 4 surveys the current and prospective future development of QIT, including capacities, entanglement and correlations, and cryptographic primitives. Section 5 discusses the four stages of the development of QC architectures that must be accomplished at least once for each viable QC technology: initial conceptual development; testing components; assembling the components into a working device; and scaling up the architecture. Section 6 gives an overview of the role of decoherence in QC and ways to overcome decoherence. This section includes an extensive list of the sources of decoherence in each type of quantum computer. The Theory Component of the Quantum Computing Roadmap concludes with a list of references cited.

2.0 Fundamental Theoretical Challenges

Quantum computing as a field has its roots very firmly planted in major theoretical developments in the 1980s and 1990s. The early musings of Feynman on how efficiently quantum mechanics could be simulated on a computer, Deutsch's definition of quantum Turing machines and quantum circuits, Deutsch and Jozsa's algorithm, and the study of quantum complexity theory by Bernstein and Vazirani showing that quantum Turing machines violate the modified Church-Turing thesis—all led up to Shor's remarkable polynomial (P) time quantum algorithms for factoring and discrete logarithm. These algorithms provided the killer applications that brought QC in the limelight. However, before any serious effort by experimentalists to realize quantum computers, another seemingly insurmountable hurdle had to be overcome by theoreticians. Quantum states are fragile and subject to decoherence that is continuous rather than discrete. This and the no-cloning theorem seemed to rule out the application of error-correction techniques. The invention of quantum error-correcting codes by Calderbank, Shor, and Steane overturned conventional wisdom in quantum mechanics and paved the way for fault-tolerant QC and the threshold result that was independently obtained by Aharonov and Ben-Or; Knill, LaFlamme, and Zurek; and Gottesman and Preskill. Theoretical work has played a similarly central role in quantum cryptography (QCRYPT), where the protocol for quantum key-distribution (QKD) due to Bennett and Brassard from 1984 provided the major moving force for the field.

For the last decade, QC has brought about a remarkable collaboration between theoreticians and experimentalists often through joint workshops and conferences. This collaboration has

resulted in the elucidation of viable designs for quantum computers. The establishment by DiVincenzo, and Barenco, *et al.* of elementary universal families of one and two-qubit quantum gates for QC did much to simplify the quantum circuit model that the physical design needed to implement. Theorists, notably Lloyd, Cirac and Zoller, and DiVincenzo proposed the first potentially viable designs for quantum computers using ion traps and electromagnetic-resonance techniques. The first prototypes of quantum computers were built by experimentalists, notably Wineland, Kimble, Cory, and Chuang—working closely with the theorists.

As the technological program of experimentally realizing quantum computers advances towards its goals, what is the future role of theory in QC? We outline below some of the grand-challenge theoretical problems where progress is essential to both the success of the experimental efforts as well as the impact of QC. (These are elaborated upon in Section 3.2). In addition, as the experimental effort accelerates, the collaboration between theory and experiment outlined above must continue to grow and evolve.

2.1 Quantum Algorithms

The search for new quantum algorithms is one of the biggest challenges in quantum computation today. Although factoring and discrete logarithms provide the killer applications for quantum computation today, once we have quantum computers, cryptography will no longer rely on these problems—therefore greatly reducing the practical value of these algorithms. The exploration of quantum algorithms is therefore of fundamental importance. In the years since Shor's algorithms, the framework of the hidden subgroup problem (HSP) has been developed, and the holy grail of quantum algorithms has been clearly identified as the HSP for non-abelian groups. Two especially important cases are the dihedral group, which corresponds to the shortest lattice vector problem, and the symmetric group, which corresponds to graph isomorphism and graph automorphism, are important in their own right. The two most promising avenues are to extend the Fourier sampling approach used by Shor, and a novel approach based on adiabatic evolution as proposed by Farhi, *et al.* [1] and elaborated by Aharonov, *et al.* [2,3]

Another interesting area is the use of quantum random walks to give polynomial speedups for basic problems such as element distinctness [4], and their potential for providing exponential speedups [5].

The future ability of quantum computers might be a decade or two away, their future ability to break public-key cryptography has important implications for the encryption of highly sensitive information today. For these applications, we must already design new public-key cryptosystems and one-way functions that are immune to quantum cryptanalysis. The existence of such one-way functions in an abstract setting follows from the paper of Bennett *et al.* [6] on exponential black-box lower bounds for inverting a random permutation. Finding concrete implementations of quantum one-way functions will require a better understanding of the scope of quantum algorithms.

2.2 Quantum Complexity Theory

Understanding the class BQP (bounded quantum polynomial), of problems that can be solved in polynomial time on a quantum computer, is the fundamental question in quantum complexity theory. Two very basic questions are the relationship between BQP and NP (nondeterministic polynomial) and between BQP and PH (the polynomial hierarchy). Although the early oracle results of Bennett *et al.* [6] provided evidence that BQP is not in NP, we must interpret these results carefully, especially in view of results from [7,8]. Given the enormous payoff if NP were in BQP, this possibility remains worth exploring. Pessimists might try to prove that if BQP subset NP then some very unlikely complexity theoretic consequence (such as the collapse of the polynomial hierarchy) would follow.

2.3 Fault-Tolerant Quantum Computing

The threshold result in fault-tolerant QC says that provided the decoherence rate is below a threshold ϵ , arbitrarily long quantum computations can be faithfully carried out. Currently the best schemes for fault-tolerant QC give a value of ϵ between 10^{-3} and 10^{-4} [9,10]. On the other hand, the only limit we know on ϵ is that it is less than $1/2$ [11]. Narrowing this gap, and improving the achievable threshold is an essential goal for the realization of scalable, practical QC. Eventually we would like to show that ϵ is of the order of $1/100$. Equally important is the challenge of reducing the overheads in the number of qubits and the processing time incurred in making a procedure fault-tolerant. Finally, it is important to revisit the model for fault-tolerant computation, in view of more detailed decoherence models from experimental efforts, as well as issues such as the relative delays for gate operations versus measurements.

2.4 Simulation of Quantum Systems

Quantum simulation is currently one of the most important applications of quantum computers. Kitaev's phase estimation method [12] provides an exponential speedup when applied to the problem of estimating eigenvalues of an operator [13], a problem of great importance in many areas of physical sciences. Grover's algorithm yields quadratic speedups when it is applied to a variety of continuous problems such as multivariate integration and path integration [14]. A very recent result by Vidal [15] shows how to classically simulate 1-D spin chains with logarithmically bounded entanglement length (the entanglement between a contiguous block of L spins and the rest of the spin chain; that is, the von-Neumann entropy of the density matrix of the block of L spins) in polynomial time on a classical computer. Extending this classical simulation to two and three dimensions could potentially have great impact, because they would be applicable to a greater range of systems.

3.0 Quantum Computation Historical Review

3.1 A Short Summary of Significant Breakthroughs in Quantum Information Theory

Information theory is rooted in physics, which places limitations on how information may be processed and manipulated for computation and for communication. Before the 1980s this

meant classical physics, but since that time there has been a conscious paradigm shift to the examination of benefits that may derive from basing a theory of information upon the laws of quantum physics. At least two important precursors to this paradigm shift had critical influence. The first was the demonstration of nonlocal correlations between different parts of a quantum system, correlations that possess no classical counterpart, by Bell in the early 1960s [16,17]. The second important precursor to the new field of QIT was provided by the work of Landauer and Bennett on the thermodynamic cost of computation [18,19]. Bennett's 1973 proof that reversible classical computation is possible [19] was the key idea in Benioff's positive response in 1980 to negative prognoses of fundamental limitations of computation provided by physics [20,21].

In a key paradigm shift, Feynman pointed out in 1992 that simulating quantum physics on a classical computer appeared to incur an exponential slowdown [22], thus paving the way for QC. Deutch took a major step further in 1985, with the introduction of quantum circuits and universal gate sets, providing the critical leap from the restrictions of Boolean logic underlying classical computation to non-Boolean unitary operations [23]. With this critical step, the concept of QC was formalized. In 1993, Bernstein and Vazirani [24] built upon an algorithm of Deutsch and Jozsa [25], to show that quantum computers provide a superpolynomial advantage over probabilistic computers, thus showing that quantum computers violate the modified Church-Turing thesis. These algorithms as well as Simon's 1994 algorithm [26] benefited from the features of quantum superposition and entanglement, with the roots of the latter clearly identifiable with the nonclassical correlations observed by Bell in the early 1960s. This slow growth in exploration of algorithmic advantages derived from quantum circuits for computation virtually exploded in 1994 with the discovery by Shor of the polynomial time quantum algorithms for integer factorization and discrete logarithm problems [27], followed by the discovery of the quadratic speed-up quantum search algorithm by Grover in 1996 [28]. Both of these theoretical results galvanized the experimental community into active consideration of possible implementations of quantum logic. Experimental interest was further stimulated by another significant result of Calderbank, Shor, and Steane namely that error correction codes could be constructed to protect quantum states just as for classical states [29,30,31]. This demonstration of quantum error correction in 1995 was subsequently incorporated into a scheme by Kitaev [32], Shor [33], Aharonov and Ben-Or [34], Knill, LaFlamme, and Zurek [35], and Gottesman and Preskill [36,37] to provide error thresholds on individual operations that show when computation can continue successfully in the presence of decoherence and errors ("fault tolerant" computation). This result put the implementation of QC on a similar footing with classical computation using unreliable gates, and significantly altered the consciousness of the physics community with regard to experimental implementation.

Quantum complexity theory systematically studies the class of problems that can be solved efficiently using quantum resources such as entanglement. Bernstein and Vazirani's 1993 work showed that relative to an oracle the complexity class BQP, of problems that can be solved in polynomial time on a quantum computer, is not contained in MA (Merlin-Arthur), the probabilistic generalization of NP [24]. Thus even in the unlikely event that $P \equiv NP$, quantum computers could still provide a speed-up over classical computers. The **limits** of quantum computers were explored by Bennett, Bernstein, Brassard, and Vazirani [6], who showed that QC cannot speed up search by more than a quadratic factor. This showed that Grover's

algorithm is optimal and that, relative to a random oracle, quantum computers cannot solve NP-complete problems. They also showed a similar lower bound for inverting a random permutation by a quantum computer, thus opening up the possibility of quantum one-way functions. Recently, Aaronson showed a similar lower bound for the collision problem [38], thus showing that there is no generic quantum attack against collision intractable hash functions. Kitaev has studied the class BQNP, the quantum analogue of NP, and showed that QSAT (quantum analog of satisfiable problem), the quantum analogue of the satisfiability problem, is complete for this class—thus proving that $BQNP = PSPACE$ [32]. Watrous considered the power of quantum communication in the context of interactive proofs, and showed that the class IP (interaction proof) of problems which have interactive proofs with polynomially many rounds of communication can be simulated with only three rounds of quantum communication [39]. In the first demonstration of the power of quantum communication, Burhman, Cleve, and Wigderson showed how two parties could decide set disjointness by communicating only square root of n quantum bits, quadratically fewer than the number required classically [40]. Ambainis, Schulman, Vazirani, and Wigderson showed that for the problem of sampling disjoint subsets, quantum communication yields an exponential advantage over any protocol that communicates only classical bits [41]. Raz [42] gave a complete problem (a relation) for quantum communication complexity and showed that it had an exponential advantage over any classical protocol. Recently, Bar-jossef, Jayram, Kerenidis, [43] showed that one-way quantum protocols are also exponentially more succinct than classical protocols.

Similar paradigm-changing advances have occurred in the theory of data transmission and communication as a result of theoretical breakthroughs in QIT. In fact the oldest branch of QIT concerns the use of quantum channels to transmit classical information, with work of Holevo dating from 1973 [44]. Since then, many significant results for the use of quantum channels to transmit both classical and quantum information have been established. It is useful to realize that these, in many cases very practical, results are derived notwithstanding the two famous results concerning inaccessibility of quantum states, namely the impossibility of distinguishing distinct quantum states (Holevo) [44] and of copying (or “cloning”) an unknown quantum state (Wooters & Zurek) [45]. Notable amongst these quantum-information theoretic results with implications for practical use in quantum communication are quantum data compression, quantum superdense coding, and teleportation. Together with quantum error correction, quantum data compression provides a quantum analog for the two most important techniques of classical information theory. The developments of quantum superdense coding in 1992 (Bennett & Wiesner) [46] and quantum transmission by teleportation (Bennett & coworkers) [47] in 1993, have no classical analogue and are thus very surprising when viewed from a classical paradigm. Teleportation allows states to be transmitted faithfully from one spatial location to the other, while superdense coding allows the classical information to be transmitted with a smaller number of resources (quantum bits) via a quantum channel. A related property of quantum channels is superadditivity, namely that the amount of classical information transmitted may be increased by use of parallel channels [48,49]. Similar to the development of theoretical techniques to deal with noise in QC mentioned above, a significant theoretical effort has also focused on the issues arising from communication with noisy channels. Several results have emerged here, but a number of open questions still remain and this is a very active area of theoretical work. Important results arrived at in recent years include a bound on the capacity of a noisy quantum channel for transmission of classical information (Holevo-Schumacher-

Westmoreland theorem [50,51,52], and the development of protocols for distillation (or “purification”) of entanglement [53,54,55].

A related area in which QIT has made remarkable advances in the last 20 years is QCRYPT. This field provides one of the most successful practical applications of quantum information to date, with the procedures for secure quantum key distribution (QKD). First developed by Bennett and Brassard in 1984 [56], several protocols now exist to make a provably secure quantum key for distribution over a public channel. These schemes rely on the uncertainty of distinguishing quantum states, with the security of the key also guaranteed as a result of the ability to detect any eavesdropping measurement by an observed increase in error rate of communication between the two parties. The remarkable security properties of QKD are a direct result of the properties of quantum information, and hence of the underlying principles of quantum physics.

These advances have demonstrated the usefulness, in many cases unexpected, of treating quantum states as information. They have also validated the field of QIT, providing a critical stimulus to experimental investigation and in some cases literally opening the path to realization of quantum processing of information for communication or computation. In fact, several of the most nonclassical or counterintuitive of the theoretical predictions have been the first to receive experimental verification (e.g., teleportation, superdense coding, and QKD). Looking back on these developments over the last 20 years, it is reasonable to expect that further investigation into the fundamentals of quantum information will continue to provide new and useful insights into issues with very practical implications. We can identify several outstanding open questions in QIT today, whose solution would impact the field as a whole. These include complete analysis of channel capacities for quantum information transmitted via quantum channels and quantification of entanglement measures for many-particle systems. Another, relatively new direction in QIT focuses on the use of measurements as an enabling tool for quantum information processing (QIP), rather than merely as a final step or source of decoherence. Measurement provides our limited access to the exponential resources intrinsic to quantum states, and recent work has shown that this access can itself be manipulated to control the processing, including some schemes to perform entire computations using only measurements in massively entangled states.

The exploration of new quantum algorithms has achieved some success over the last couple of years, following a lull of about six years after Shor’s algorithm. These include Hallgren’s 2002 quantum algorithm for Pell’s equation [57] (one of the oldest problems in number theory), which breaks the Buchman-Williams cryptosystem. The framework for quantum algorithms has also been extended beyond the HSPs. van Dam, Hallgren, and Ip’s 2000 quantum algorithm for shifted multiplicative characters [58,59] breaks homomorphic cryptosystems, and the same techniques were recently extended by van Dam and Seroussi (2002) to a quantum algorithm for estimating Gauss sums [60]. The framework of adiabatic quantum algorithms introduced by Farhi, Goldman, Goldstone, and Sipser 2000 [1], and explored by van Dam, Mosca, and Vazirani 2001 [7] and by Aharonov, *et al.* [2,3] provides a novel paradigm for designing quantum algorithms.

3.2 Current Developments and Directions

This section gives more extensive and detailed descriptions of the theoretical challenges in quantum computation, and places them in the context of current developments in the field.

3.2.1 Quantum algorithms

The search for new quantum algorithms is undoubtedly one of the most important challenges in QC today. Following Shor's [27] discovery of quantum algorithms for factoring and discrete log in 1994 and Grover's [28] quantum search algorithm in 1995, there was a period of over five years with no substantially new quantum algorithms. During this period, the mathematical structure of Shor's algorithm was clarified via the formalism of the HSP—polynomial-time quantum algorithms were known for every finitely generated abelian group. Over the last couple of years, we are starting to see some progress towards the discovery of new algorithms. In 2002, Hallgren [57] gave polynomial-time quantum algorithms for Pell's equation and the class group problem, thus breaking the Buchmann-Williams cryptosystem. This extended the framework to nonfinitely generated abelian groups. The two most important open questions in quantum algorithms are graph isomorphism and the (gap) shortest-lattice vector problem. The first of these corresponds to the HSP in the symmetric group, and Regev [61] showed that the second can be reduced to the HSP in the dihedral group. The dihedral group is a particularly simple nonabelian group, because it has a cyclic subgroup of index two. The standard quantum algorithm for abelian HSP can be generalized in a natural way to nonabelian groups. It was shown by Grigni, Schulman, Vazirani, and Vazirani [62] that for sufficiently nonabelian groups the standard algorithm yields only an exponentially small amount of information about the hidden subgroup. On the other hand, Ettinger, Hoyer, and Knill [63] showed that the quantum query complexity of the problem is polynomial. This suggests that novel algorithmic ideas are necessary to tackle the nonabelian HSP. Recently Kuperberg [64] gave a $O(2^{-n})$ algorithm for the dihedral HSP. The algorithm was an interesting modification of the standard algorithm. Other computational problems that are potential targets for quantum algorithms are the nonsolvable group membership, the McElise cryptosystem, and the learning AC0 circuits.

A different approach to designing quantum optimization algorithms via adiabatic evolution was proposed by Farhi, *et al.* [65]. Initial efforts in this direction concentrated on the question about whether adiabatic optimization could solve NP-complete problems such as variants on SAT in polynomial time. Surprisingly, query lower bounds do not rule out this possibility [7]. However, van Dam and Vazirani [66] and more recently Reichardt [67] gave classes of SAT instances for which the spectral gap is exponentially small. Nevertheless, Farhi, *et al.* [68] showed that adiabatic quantum optimization algorithms can tunnel through local optima and give an exponential speedup over local search. Aharonov and Ta-Shma [2] suggested that rather than optimization problems, adiabatic algorithms might be better suited for quantum-state generation. They also showed that every problem in the complexity class SZK can be reduced to the problem of generating an appropriate quantum state. Aharonov, *et al.* [3] showed that a slightly more general formulation of adiabatic algorithms, when used for quantum-state generation, is in fact universal for QC. Designing quantum algorithms via quantum-state generation is a novel and potentially important direction, because it ties into classical algorithm-design techniques using Markov chains and techniques such as bounds on conductance and

spectral gaps. As a first step, it would be interesting to even give such an algorithm for solved problems such as quadratic residuosity or discrete logarithms.

Quantum random walks have held out the promise, over the last few years, as another interesting approach to the design of quantum algorithms. In the computational context, quantum walks were introduced by Farhi and Goldstone [69] in 1997 in their continuous-time incarnation, and in 1998 by Watrous [70] as discrete-time walks. Aharonov, *et al.* [71] studied such walks and showed that their mixing time is polynomially related to that of the corresponding classical Markov chain. Cleve, *et al.* [4] recently showed that in an oracle setting a quantum-walk-based algorithm gives an exponential speedup over any classical randomized algorithm. This is based on an exponential speedup by quantum walk for the hitting time between two specified vertices in a graph. The promise of quantum walks in the design of algorithms for concrete problems was recently realized by Ambainis [5] by combining it with Grover's search. He gave an optimal algorithm for element distinctness. The approach was further extended by Magniez, Santha, and Szegedy [65] to finding triangles in graphs, and by others to checking matrix multiplication. In each case, the speedup obtained is by a polynomial factor. This approach appears to be very promising. Challenges for the future include applying these new techniques to solve classical computational problems such as matrix multiplication, determinant computations, bipartite matching, or linear programming.

3.2.2 Quantum error-correction and fault-tolerant QC

The discovery of the threshold result in fault-tolerant QC provided the theoretical basis for considering truly scalable physical implementations of QC. The original threshold result showed that as long as the decoherence rate is below $\epsilon \approx 10^{-6}$, arbitrarily long quantum computations may be carried out. The error model here is that each gate is subject to decoherence independently with probability ϵ . More recent improvements by Aharonov and Gottesman [9] put the threshold at 10^{-4} , and Steane [10] shows that under mild assumptions the threshold is 10^{-3} . These improvements make use of quantum teleportation to prepare ancilla states [72] as well as improved use of quantum error-correcting codes. On the flip side, the best upper bound on the threshold was recently established by Razborov [11], who showed that if the threshold is below $1/2$, unless BQP \equiv BQNC. For scalable QC to be practical, it is essential to improve the threshold by at least another order of magnitude.

There is clearly great room for improvement, although this will likely require new techniques. Equally important are the penalty in the number of qubits and total number of gate operations incurred to make a quantum circuit fault-tolerant. These currently scale as 7^k and 343^k respectively for k levels of error correction. Progress in this area will likely require the study of new techniques, including the design of efficiently encodable and decodable quantum error-correcting codes, using expander-graph-based techniques, and list decoding.

Another approach is to search for equivalent quantum models that are resilient to certain types of noise in the physical system under consideration for implementation. An example of this approach is the development of encodings based on recognition of symmetries in the physical interactions underlying the noise sources, referred to as 'decoherence-free subspace' and 'decoherence-free subsystem' encodings [73]. These provide passive error correction, in contrast to the active error-correction approach of standard quantum error correction. Additional

protection can be gained by engineering extra interactions to obtain supercoherent codes which provide thermal suppression of some physical noise sources in addition to complete protection against specific errors [74]. More generally, the approach of topological QC provides a powerful framework to rigorously suppress all effects of noise by encoding into topologically invariant subspaces [75,76]. This passive approach to error correction has led to the emergence of alternative realizations of universal QC, including ‘encoded universality’ [77] (see Section 5) and the topological QC paradigm (see Section 3.2.5).

3.2.3 Quantum complexity theory

Clarifying the limitations of QC is a question of fundamental importance. One important issue is clarifying the relationship between BQP and the classical complexity classes—is NP a subset of BQP? Does BQP lie in the polynomial hierarchy? Progress towards answering the first question was made via the oracle results of Bennett, *et al.*, who showed that relative to a random oracle NP is not a subset of BQP. This may be interpreted as saying that it is unlikely that quantum computers can efficiently solve NP-complete problems, or at least that nonrelativizing techniques are essential to resolving this question. This does not completely rule out the possibility of tackling this question, in light of the results of Arora, *et al.* [8] showing that the principle of local checkability is nonrelativizing, and the demonstration by Mosca, *et al.* that exponential query lower bounds do not apply to queries that examine the number of clauses left unsatisfied by the given truth assignment.

Another important issue is understanding whether the limits on QC provide an opportunity to reconstitute modern cryptography despite Shor’s assault on the two most important one-way functions—factoring and discrete log. Are there one-way functions that cannot be efficiently inverted even by a quantum algorithm? The complexity theoretic basis for an affirmative answer was given by Bennett, *et al.*, by showing that quantum computers require exponential time to invert a random permutation in the query model. More recently, it was shown by Aaronson that quantum computers require exponential time to solve the collision problem in the query model, thus opening the possibility of collision-intractable hash functions that are secure against quantum cryptanalysis.

Interactive-proof systems have had important and unexpected applications in classical complexity theory. Kitaev and Watrous [78,79] proved that quantum interactive-proof systems have interesting properties and are fundamentally different from classical proof systems. They showed that that

1. any polynomial-message quantum interactive proof can be parallelized to three-messages (which does not happen classically unless $AM \equiv PSPACE$), and
2. quantum interactive-proof systems can be simulated in deterministic exponential time.

The first result is interesting because it is unexpected and represents a way of taking advantage of quantum information that seems to be quite different from other applications. The second result represents one of the first applications of semidefinite programming to QC.

In the classical case, the study of interactive-proof systems led to surprising and important applications, in particular with respect to the hardness of approximation problems. Are there interesting applications of quantum interactive-proof systems? For instance, can quantum

interactive-proof systems give us insight into designing new quantum algorithms? Presently, we have no such applications.

The nature of quantum information is such that there is a great potential for zero-knowledge quantum interactive-proof systems. However, it turns out that perplexing mathematical difficulties are also associated with quantum variants of zero-knowledge. Watrous [79] proves some fundamental limitations on one particular type of quantum zero-knowledge, but this is (hopefully) just a beginning. That paper also defines quantum zero-knowledge in a very restrictive setting, but even the first step of giving a cryptographically satisfying general definition of quantum zero-knowledge is a challenging problem.

The simplest variant of the interactive-proof-system model consists of two interacting parties, one prover and one verifier. A more complicated variant of the model allows multiple provers. In the quantum setting, fascinating connections exist between this model and the fundamental notion of a Bell inequality from quantum physics. Kobayashi and Matsumoto [80] studied this model in a very restricted setting where entanglement between the provers is not permitted. However, it seems that entanglement is at the heart of the difficulty in understanding this model in the general case. Two-prover quantum interactive-proof systems could be more powerful, less powerful, or incomparable with classical two-prover interactive proofs—we presently know almost nothing about the power of this model, even in the case where the verifier is classical.

3.2.4 Quantum simulation

Quantum simulation represents, along with Shor's and Grover's algorithms, one of the three main experimental applications of quantum computers. Of the three, quantum simulation is in fact the application of quantum computers that has actually been used to solve problems that are apparently too difficult for classical computers to solve. As larger-scale quantum computers are developed over the next five and ten years, quantum simulation is likely to continue to be the application for which quantum computers can give substantial improvements over classical computation.

Quantum simulation was in fact the first proposed application for which quantum computers might give an exponential enhancement over classical computation. In 1982, Feynman noted that simulating quantum dynamics on a classical computer was apparently intrinsically hard. Merely to write down the state of a quantum system made up of N two-state systems such as spins took up exponential amounts of space in the memory of a classical computer; and determining the dynamical evolution of such a state required the multiplication of exponentially large matrices. Suppose, Feynman continued, that it were possible to construct a "universal quantum simulator", an intrinsically quantum device whose state and dynamical evolution could be programmed to mimic the behavior of the quantum system of interest. Such a device, he concluded, could function as a quantum "analog" computer, capable of reproducing the behavior of any desired quantum system.

Feynman merely noted the potential existence of such universal quantum simulators: he did not supply any prescription for how such a universal quantum analog computer might be realized in practice. In 1996, however, Lloyd, Wiesner, and Zalka showed that conventional "digital"

quantum computers could be programmed to perform universal quantum simulation. Since then, Cory *et al.* have used room-temperature nuclear magnetic resonance (NMR) QIPs to perform coherent quantum simulations of harmonic oscillators [81,82,83] and chaotic quantum dynamics such as the quantum Baker's map [84,85]. Note that for the purpose of quantum simulation, the apparent lack of scalability of a room-temperature NMR QIP does not prevent such a processor from supplying an apparently exponential speed-up over a classical computer: simulating high-temperature quantum systems is still apparently exponentially hard [86].

An example of a large-scale experimental realization of quantum simulation is the use of solid-state NMR QIPs to study the diffusive limit of transport of dipolar coupled spins in dielectric single crystals. The many-body dynamics were studied over times of tens of seconds, corresponding to of order 10^8 times the spin-spin correlation time, and spin transport over a distance of $1\ \mu\text{m}$. One result of these studies was to reveal that the diffusion constant for the two-spin dipolar ordered state is roughly 4 times faster than that of the single-spin, Zeeman ordered state. This speedup was not predicted by theoretical models and has been attributed to constructive interference in the transport of the two-spin state. Today solid-state NMR permits selected many-body problems to be addressed, the field does not yet have sufficient control to enable universal quantum simulation [87,88].

Another potentially interesting source of problems relevant to the sciences are continuous, numerical problems such as integration and Feynman integrals. Because Grover's algorithm gives a quadratic speedup for not just search but also counting, it can be applied to get a quadratic speedup for integration in a natural way [14]. It remains an interesting open question whether some of the more sophisticated quantum walk techniques or other quantum algorithm techniques can be used in this context.

At the other end of the spectrum, QIT has provided novel algorithms for classically simulating quantum systems with limited entanglement. Vidal *et al.* [89] characterized the scaling properties of the ground-state entanglement in several 1-D spin-chain models both near and at the quantum-critical regimes. They showed that the entanglement length scales logarithmically in the number of spins [it scales like $\log(L)$]. Vidal [15] recently gave an efficient classical algorithm for simulating the dynamics of 1-D spin chains that runs in time exponential in the entanglement length. Experimental results suggest that this method may be very effective in simulating a variety of systems. Extension of these results to 2-D and 3-D would be very interesting.

3.2.5 Novel models

What are the primitives necessary to carry out QC? The answer in the quantum circuit model is clear—an implementation of qubits, a universal set of quantum gates, and the ability to measure the output. In recent years, there has been an exploration of novel models for QC that look fundamentally different from the quantum circuit model. One of the first such attempts, the topological QC, provides a different paradigm in which the qubits are no longer identified with specific atomic degrees of freedom but with collective excitations that must then be manipulated. Another approach was motivated by an attempt to prove that linear optics cannot be used to implement scalable quantum computers. In the attempt, Knill, Laflamme, and Milburn [76,90] discovered a technique, using teleportation-based [72] use of ancillas, of

implementing scalable QC using linear optics. In a different direction, Nielsen [91] showed that projective measurements can be used in the place of quantum gates as the fundamental primitive for QC. This was followed by the results of Raussendorf and Briegel [92] showing how to perform QC by preparing certain highly entangled cluster states, followed by a sequence of measurements. Adiabatic QC, first proposed by Farhi, *et al.* [68] and then generalized by Aharonov, *et al.* [2,3] starts with an initial state which is the ground state of a sum of local Hamiltonians, and then gradually transforms to a different sum of local Hamiltonians whose ground state is closely related to the desired output of the QC. Aharonov, *et al.* showed that this model is exactly as powerful as the quantum circuit model, thus providing another potential implementation of QC. The nontrivial spectral gap gives this model some natural fault-tolerant properties.

The role of entanglement in the power of QC is a fundamental theme. Two questions about this issue have arisen in the context of liquid NMR QC. The first question asks about the computational power of a mixed state quantum computer whose state is required to be separable at every time step of the computation. Caves and Schack [93] pointed out that even though at first glance this model appears to be classical (because there is no entanglement), we do not know how to simulate it classically; nor do we know how to perform nontrivial QC with it. Another model, proposed by Knill and Laflamme [94] consists of 1 clean qubit with $n-1$ qubits in the maximally mixed state. Pulini *et al.* [95] give a quantum algorithm in this model to measure the average fidelity decay of a quantum map under perturbation.

4.0 Quantum Information Theory

This section is a survey of the current and prospective future development of QIT. Continuing progress in QIT is crucial to the ultimate success of the laboratory implementation of QC. QIT addresses itself to performing useful processing tasks with noisy resources, and doing so optimally. The laboratory work in quantum information is and will be plagued by noise, and knowing the strategies for dealing with these (e.g., using a well chosen quantum error correcting code) will be very important for making progress. In addition, QIT invents fundamentally new applications for distributed quantum processing. These are in the form of uniquely quantum-mechanical cryptographic primitives such as quantum key distribution, quantum data hiding, and private remote database access.

For the purposes of this write-up, "QIT" should be understood as the information-theoretic analysis of quantum-mechanical systems. Information theory quantifies the correlations between separated systems and the amount by which these correlations can be enhanced using the communications resources at hand. This subject sits at a more abstract level than the analysis of particular information-processing systems; that is, it does not address itself to the particularities of optical or electrical systems, but attempts to give a general framework within which the analysis of any such particular system can be performed. QIT is also distinct from algorithm theory, which seeks efficient procedures for solving mathematical problems; it does interface with it on the point of distributed algorithms, in which procedures using both local computation and communication are employed. The manifold uses of quantum teleportation are a prime example here.

We have chosen to discuss QIT below in terms of three big organizing themes: capacities (i.e., carrying capabilities of different communication resources); entanglement (i.e., quantification of the correlations, quantum and otherwise, between different subsystems); and cryptography (i.e., what do we do with these capacities and correlations when we've got them).

Very close to this subject, but distinct enough that they will not be discussed here, include the studies of communication and sampling complexity in the quantum setting [96], distributed quantum algorithm design, and quantum Kolmogoroff complexity [97,98].

4.1 Capacities

One of the two important quantifications of information theory is the calculation of capacities. Capacities measure the rate at which correlations (e.g., knowledge of a message text, shared randomness, quantum entanglement) grow per use of the given communications resource, in an "asymptotic" setting where arbitrarily many uses of the communication resource are available. More than one type of capacity is definable in the classical setting, and the number of different capacities grows substantially in a quantum setting, because there are more distinct types of channel resources available, as well as more distinct types of correlations.

Historically one can consider Holevo's investigations in the '70s [99] as the starting point of this subject, when he considered the classical capacity of a quantum state; this work remains seminal, in that it established that, in general, a two-level quantum state is not capable of carrying more than one bit of information, despite the large amount of information needed to describe such a quantum state. One can say that it is the evasions of this theorem of Holevo, in the various special circumstances where one qubit can amount to more than one bit of information, that have been one of the important general themes of QIT.

In current language, Holevo's result pertains to the transmission of classical correlations (i.e., a classical message text) from sender to receiver (frequently "Alice" and "Bob" below) using a particular kind of quantum channel, which conveys a certain ensemble of quantum states ρ_i perfectly. This kind of channel is now known as a "cq" channel [100], in which a classical instruction, i , indicates that the quantum state ρ_i should be synthesized, and then conveyed undisturbed to the receiver. This is now considered as a special case of a more general resource, the quantum channel, which is described by some general completely positive trace preserving linear map between a quantum input state and a quantum output state [101]. The general question of the text-carrying capacity of such a general channel has been partly solved, in that there is a formal expression (the Holevo capacity) for this quantity [51,52]. A big open question remains, however, about the evaluation of this expression, which is one of several "additivity" questions that remain open in QIT [102]. The Holevo capacity expression involves an optimization over some number, N , of uses of the quantum channel, where N could be unboundedly large. The capacity is "additive" if the optimal is achieved for $N \geq 1$. For $N \geq 1$ the optimization is quite easy, and an explicit form (the Holevo χ function) is known. But this and other additivity questions remain high on the priority list for solution in this area.

Perhaps the simplest quantum capacity is what has been called "Q" [55], the capacity of a noisy quantum channel to faithfully convey quantum states. Q is important from various points of

view; achieving it requires the use of quantum error-correction codes, and the optimization of Q can and will drive the optimization of these codes. Q also provides a bound on D , an important measure of the entanglement of mixed quantum states, the distillable entanglement [55] (see the next subsection). An entropic expression is now known for Q , the so-called coherent information [103]. It is known *not* to be additive, and its evaluation even for most qubit channels remains open.

Of the multitude of mixed capacities that can be considered, the first one to be studied was the one involving the same task as Q , that is, faithfully conveying quantum states from sender to receiver; but a dual resource was considered, namely a noisy quantum channel plus a classical side channel. It was shown that a forward side channel cannot increase Q , but that a two-way classical channel does, introducing a new capacity, Q_2 , [55] (referring to the case of unlimited two-way use of the side channel). Bounds can be given for Q_2 , and there are known to be quantum channels for which $Q_2 > 0$ but $Q = 0$; but there is no known entropic expression for Q_2 , and there are no obvious strategies for making the present bounds on Q_2 tighter.

The other dual resource capacity that has received a lot of attention is one for which both a channel and shared entanglement are available. The prototypes of these problems are quite famous: if the channel is a noiseless quantum channel, and the task is the conveyance of classical data, then this is the “superdense coding” [46] problem, in which one use of the channel, and the consumption of one entangled EPR (Einstein, Podolsky, Rosen) pair, results in two bits sent. The generalization of this to a noisy quantum channel gives a capacity that has been called C_E [104,105]; useful entropic expressions for C_E have been derived, and it is known to be additive. The dual problem, in which the channel resource is classical, but quantum states are to be transmitted, is teleportation [47]. The fully quantum version of this, in which the channel is quantum and the data to be transmitted is quantum, gives a capacity known as Q_E . For all channels, $Q_E = 1/2 C_E$ [47], showing that added resources can sometimes simplify the quantification of capacities.

Several other tasks that have no analog in the classical world have been considered in recent work. One is “remote state preparation” [106]—given a sender who has complete knowledge of a quantum state, the objective is for the recipient to come into possession of a faithful specimen of that quantum state. If the resources to be used are shared EPR pairs and a classical channel, the scenario resembles teleportation; but unlike in teleportation, the “capacity”, that is, the minimal resources needed to perform the task, are highly non-trivial [107,108]. (More use of the bit channel can reduce the number of EPR pairs needed.) Another uniquely quantum task is the “remote POVM”, in which the sender has a set of quantum states, and the recipient is to obtain a bitstring that represents a fair draw from the output of the POVMs performed on these states. This is to be done using a classical bit channel between sender and receiver, plus preshared randomness. The optimal capacity for this problem is also highly nontrivial, and has introduced new methods for the analysis of a host of other capacity problems [109].

To summarize this work, capacities are defined with respect to the following tasks:

- bit transmission;
- qubit transmission;
- remote state preparation;

- remote POVM;
- private key transmission;
- sharing of entanglement; and
- intersimulation (e.g., simulating a noisy channel by a noiseless one).

Employing the following means:

- classical channel (noisy or noiseless, one-way or two-way);
- quantum channel (noisy or noiseless);
- shared correlations:
 - quantum (noisy or noiseless entanglement) or
 - classical (shared randomness); and
- quantum interaction (i.e., two-body Hamiltonian acting over time t).

Matching all possible tasks with all possible means, and including multiple parties, leads to the observation that the amount of work to be done in this area is practically infinite. It appears that the community will continue to tackle various cases among these infinite possibilities as the interest arises.

4.2 Entanglement and Correlations

Because, from some point of view, entanglement is simply one of the correlation resources available in quantum communication, it would seem that it might not deserve a heading of its own in a survey such as this. But this would be unfair to the unique role that it plays in the quantum setting; it is *the* feature of the quantum world that distinguishes it from the classical world [110,111], saying that for a single pair of systems, a description of each system's state is not sufficient to describe the entire state of the system; it is the property that permits the violation of Bell's inequalities [112]. It is also the feature of quantum systems that makes exponential speedup of computations possible [113]. Thus, entanglement is of special interest, both from the foundational and the practical point of view. And thus, not surprisingly, it has received a large amount of special attention within the quantum-information community, and will doubtless continue to do so.

A great deal of work has been done and continues to be done on the problem of measuring entanglement. For pure states of two parties, there is a single measure that, for most information-theoretic purposes, is satisfactory for quantifying entanglement: the von Neumann entropy of the reduced density matrix [53]. (By "information-theoretic", we mean that, as above, we consider an asymptotic situation in which many copies of the states of interest are available.) For almost any other circumstance, it seems impossible to devise a single measure that will quantify entanglement in physically meaningful ways. The prototype example of this is the mixed state of two parties. If the state is *separable* (can be written as a convex mixture of product projectors), then for almost all purposes the state may be considered to be unentangled [55]; the state has correlations, but for most purposes (some exceptions occur in the next section on cryptography) these correlations behave as in the classical world. So, if a mixed state is inseparable, it is entangled. But how entangled is it? Here is a list of some of the measures that have been described:

- Distillable entanglement (D) [55]. This measure is an answer to the question: how good is my entangled mixed state for doing quantum teleportation? Thus, it has an operational significance in quantum capacities. The distillable entanglement is also the number of EPR singlets that can be obtained from a set of copies of the given mixed state, assuming that the parties can do only “local” operations, where “locality” includes the possibility of classical communication. This was the first setting in which the class of quantum operations denoted by “local quantum operations and classical communication” (usually LOCC [local operations and classical communication]) was introduced—although in some sense it was already implicit in discussions of Bell inequalities. This class of operationally local quantum dynamics has now been considered in many other contexts.

The effort to calculate D explicitly has been difficult. It turns out to have none of the convexity or additivity properties that one would desire for an information-theoretic measure to apply to D [114]. Also, D is not nonzero for all inseparable states [115]; but this relates to the PPT story discussed below.

- Entanglement of formation (E_F) [55]. This is defined as the minimum average entanglement of a pure state ensemble making up the mixed state. Thus, it is not an operational measure of entanglement, but it is one that is amenable to exact calculation, and it is an upper bound on D . It is nonzero for all inseparable states. When it was constructed it was intended to have an operational meaning of the
- Entanglement cost (E_C) [116], which is the smallest number of EPR pairs needed to create a given number of copies of a mixed state, ρ , by LOCC operations. This may equal the entanglement of formation, but it turns out that this is one of the “additivity” questions that has not been settled, and is equivalent to the additivity conjecture for the Holevo capacity [102].

This by no means exhausts the list of entanglement measures of mixed states:

- Relative entropy of entanglement [117,118]. This measure is based on the idea that entanglement should be measured by “how far” ρ is from the set of unentangled (separable) states. One way of measuring “how far” for quantum states is by their relative entropy. This measure is upper bounded by the entanglement cost, and lower bounded by the distillable entanglement. It is relatively easy to compute. It also has the property that it cannot be increased under “separable” quantum operations [119]. This class is not the same as LOCC, but it does include it. This result is illustrative of a more general principle in the quantification of entanglement: because it is supposed to represent uniquely quantum correlations, it should not be possible to increase it using only classical communication between the parties. This has led to
- Entanglement monotones [120]. This is a kind of metameasure—in that it potentially includes an infinity of specific measures. It simply states that any functional of the quantum state that is nonincreasing under LOCC should be considered a measure of entanglement. It is known that there is a whole continuum of such measures, which (under sensible restrictions) lie between the entanglement cost and the distillable entanglement.
- Negativity [121]. This quantification arises from a different idea about the characterization of entanglement, that arising from the “partial transpose.” Peres [122] noted that if the partial transposition, that is, matrix transposition applied only to the indices of one of the

parties, is performed on the matrix describing a separable mixed state, the result is always another mixed state (i.e., it is another matrix with nonnegative eigenvalues). On the other hand, if it is applied to the density matrix of an EPR pair, the result is a matrix with some negative eigenvalues. The “Peres criterion” for entanglement states that ρ is entangled if its partial transpose is negative. For small Hilbert spaces this is a necessary and sufficient condition for entanglement [123]; but in higher Hilbert space there are entangled ρ s that are positive under partial transpose [115]. Recognizing this flaw, it is still possible to give another quantification of entanglement that is the sum of the negative eigenvalues of the partial transpose. This measure is easy to compute and has been used to develop bounds in some calculations pertaining to entanglement.

So, this relatively innocent exercise of trying to associate a number with a degree of entanglement has led to a very complex discussion that raises questions on various fundamental aspects of quantum theory. First, one can ask, can entanglement be reversibly converted from one form to another? For pure bipartite states the answer is yes [53]; this is related to the fact that there is considered to be only one information-theoretic measure of pure state entanglement. Thus, a large supply of partially entangled mixed states can be converted, by purely local operations, to a smaller supply of EPR pairs (“entanglement concentration”), and converted back again to the same number of partially entangled states (“entanglement distillation”). But for mixed states the answer is the reverse [55,116], thanks to the known gap between the entanglement cost and the distillable entanglement. This is connected with another basic question: why does the partial transpose criterion sometimes fail to detect the entanglement of a state? One answer to this is that states exist for which the entanglement cost is finite but the distillable entanglement is zero, so the irreversibility is complete. States for which this happens are said to have “bound entanglement” [115], meaning that it cannot be freed up by LOCC operations.

A great deal is known about bound-entangled states now, e.g., how to construct instances of such states [115,124,125,126], but there remain many unanswered questions about them. Also, this is related to a final question that is only partially answered: what is a good notion of locality for joint operations involving two parties? It was once thought that the LOCC class captured everything of interest; that is, all LOCC operations resulted in only classical correlations (they do not produce or increase entanglement), and that all operations outside the LOCC class could produce quantum correlations.

This is no longer so clear. We mentioned that in the context of the relative entropy of entanglement, the “right” characterization of local quantum operations is the “separable” class, in which each Krauss operator of a superoperator can be written in a product form. It is somewhat surprising that this class is strictly larger than the LOCC class [119]. Yet, from most points of view, such an operator seems incapable of generating any entanglement.

There is yet a larger class, which is called the “ppt preserving” class [127], which by definition includes all bipartite quantum operations such that if the input state is positive under partial transposition, so is the output. These operations can definitely produce entanglement, but only of the bound variety. (So, for example, it cannot produce the kind of entanglement that would be useful for teleportation). Thus, many entanglement measures of interest are well behaved even within this large class. This class has been very useful because its mathematical

characterization turns out to be much simpler than either the LOCC or the separable class. But it remains unclear whether this class of quantum operations has any real physical significance.

The experimental detection of entanglement has been a subject of more recent theoretical interest. The simplest way to approach this, which requires no new ideas, is that a state can be characterized by quantum tomography; then, if the tomography is sufficiently precise, any of the measures of entanglement discussed above can be calculated for the state. But there are potentially more direct ways in which this determination can be made. Terhal's "entanglement witness" [128] is a Hermitian operator, W , that has the property that its expectation value $\text{Tr}(W\rho)$ is positive for all unentangled states, but is negative for some entangled states. (Unfortunately, it is impossible for it to be negative for all entangled states.) Thus, determination of the expectation value of W by repeated measurement can detect entanglement (a negative answer means entangled), and the value of this expectation value becomes another quantification of entanglement. Nonlinear functionals can also detect entanglement: one can find quantum operators for which the variance is only zero for entangled states, being nonzero for all unentangled states [129]. Finally, there are modifications of tomography such that, with only a subset of the measurements performed for full tomography, it can be determined whether a state is entangled or not [129]. It is expected that future work in this area will connect these means of detecting entanglement more directly with the applications of entanglement in cryptography, communications, and computing.

All of the characterizations of entanglement that we have discussed so far are "information theoretic", i.e., apply to a setting where there is a large supply of identical copies of the state ρ of interest; many of the measures of entanglement we discussed, for instance, involve taking the limit of the number of copies of the state to infinity. But there is another, potentially more practical, area of investigation in which the number of copies of the state is considered to be limited. For example, one can ask, if only one specimen of the bipartite state ρ is held by two parties, is it possible for them to convert this state, by LOCC operations, to a single specimen of the state ρ ? If ρ and ρ are pure, then there is a very beautiful answer to this question involving the statistical concept of majorization [91]. But almost all other problems in this area are open.

Finally, it should be mentioned that the theory of entanglement has a direct bearing on QC itself. The theory of quantum error-correcting codes, and their application to fault-tolerant QC, is from some point of view a theory of the properties of special kinds of entangled states. It is a paradoxical truth that has emerged from quantum information research that sometimes highly entangled states can be more robust against decoherence than apparently more classical unentangled states [37]. This robustness has also had application in areas of QCRYPT (see secret sharing, below). Entanglement can also be used in the implementation of quantum logic gates; teleporting through the right kind of entangled quantum state can result in two-bit gate operations applied to a pair of qubits [130]. Generalizations of this ideas have resulted in the discovery that linear optics is sufficient for QC [90]. Also, it is now known that with the right kind of entanglement (the "cluster state"), QC can be reduced completely to a sequence of local quantum measurements, with all information flows in the computer being classical [92]. There is likely to be considerably more work to be done in this area, to connect these remarkable features of entanglement to other workable approaches to QC in the laboratory.

4.3 Cryptographic Primitives

Broadly defined, cryptography considers distributed information-processing tasks constrained by requirements of privacy, secrecy, and security. Quantum mechanics has offered a new toolkit for the construction (and demolition) of cryptographic tasks, and this remains an extremely active area of research.

In many people's minds, cryptography is defined as the sending of secret messages from one party to another. While cryptography actually encompasses much more than this task alone, the "key distribution" problem is still central to Q_{CRYPT} , and it is the only one for which there is active laboratory work. The theory of secure key distribution using quantum channels has been undergoing a continuing rapid evolution in recent years. The basic idea of using the unclonability and unmeasurability of single unknown quantum states to make secret messages intrinsically unreadable to an eavesdropper (without disturbance) dates back to Wiesner's work in the 1970s [131], and the explicit protocols for doing this style of cryptography were all established more than 10 years ago, independently by Bennett and Brassard [56,132] and by Ekert [133]. This work was enough to stimulate serious experimental work [134], which continues to this day. But the security of these protocols remained unproved in the general setting for many years, although proofs for restricted "Eves" were known some time ago. In addition, there was an early insight that entanglement distillation would be a crucial ingredient in this proof [135,136], although the details were a long time in coming. But the real revolution in this area theoretically was initiated by Mayers in the late '90s [137]. He found a proof that BB84 is absolutely secure for sufficiently low detected bit error rate for quantum transmission. His proof was difficult and was not understood by much of the community for some years; but the revolution was made general by Shor, who, with Preskill [138], redid Mayers proof in much more transparent language.

Shor's starting point was a different proof by Lo and Chau [72] that a different key-distribution protocol involving the distillation of perfect entanglement is secure. This proof was much easier than Mayers' and established that the Ekert [133] style of "quantum Vernam cypher" Q_{CRYPT} was actually valid, but assumed that Alice and Bob have the full power of QC. Shor and Preskill showed that using a particular style of quantum error-correction code in the Lo-Chau purification permitted a reduction of this proof to BB84. Their approach to this proof has been workable enough that more results are now flowing out; one result involves the strengthening of the BB84 by use of two-way classical (insecure) communication; it is now known that this resource permits secure key distribution in a more noisy environment (i.e., a more aggressive eavesdropper). Also, B92 has been proved secure now by an ingenious variant of the Shor reduction [139].

It appears that this activity in security proofs for key distribution still has a long way to go. Very important fundamental and practical questions involving imperfect sources persist. Fundamental questions also remain open about the relation of security to the violation of Bell inequalities. Also, because experiments are underway, there are a host of technical questions (e.g., involving the use of weak coherent sources) that deserve theoretical attention.

As stated above, cryptography is not just secret-message transmission. We give a brief survey here of the other areas of cryptography that have been reconsidered in the light of quantum theory:

- *Bit commitment.* Bit commitment, a primitive for many other forms of cryptography (e.g., secure function evaluation) involves
 1. the choosing of a bit value by Alice,
 2. the commitment by Alice of this bit value to Bob in an unreadable form, and
 3. the unveiling of this bit value to Bob at a later time.

Mayers [140] showed that bit commitment is impossible in the standard quantum model of the world, by showing that Alice can always cheat by using quantum entanglement. Partially secure bit commitment is possible and has been analyzed [141]. An interesting recent development here is to consider the effect of various additional fundamental and practical physical effects on the security of bit commitment. For example, special relativity makes a limited form of secure bit commitment possible. Recent work has focused on the role of selection rules. It is now believed that fundamental selection rules (e.g., charge superselection) do not modify the no-go theorem for bit commitment, although the proof is considerably more technical. Perhaps more interesting is the fact that non-fundamental, technological restrictions (e.g., the inability to change spin angular momentum in the lab) may enable a new kind of conditionally secure bit commitment. Current theoretical work in this area is very active.

- *Remote coin tossing.* As with bit commitment, there are quantum no-go results [142]. However a closely related primitive, weak coin tossing, in which Alice would prefer a “heads” and Bob would prefer a “tails” is sufficient for most of the applications of coin tossing. Ambainis and Kerenidis & Nayak gave protocols for weak coin tossing that beat Kitaev’s bound, thus showing that his no-go theorem does not apply in this case. Whether protocols that achieve arbitrarily small bias exist is an open question.
- *Quantum secret sharing.* Secret sharing is a concept in classical cryptography in which many parties receive “shares” of a secret that are unintelligible to the individual parties, or to small groups, but can be faithfully reconstructed if any “quorum” of these parties is brought together or can communicate among themselves. There are protocols that perform similar functions in which a quantum state is the secret [143]. That is, parties receive shares of a quantum state, whose identity is unintelligible to single parties (*i.e.*, the reduced density matrix is proportional to the identity operator). Classical or quantum communication among a subquorum of parties also is incapable of revealing anything about the identity of the secret.
- *Quantum data hiding.* This is dual to the previous: the idea is that the parties receive “shares” representing ordinary classical data, but the idea is to enforce security in the presence of arbitrary classical communication. Thus, reconstruction of the secret is only possible with quantum communication. The existence of states that perform this task is known [144], and, surprisingly, it is known that they can be separable mixtures (*i.e.*, they need not involve any entanglement) [145]. Also recently, it has been shown that a variant of quantum data hiding can be used in conjunction with quantum secret sharing to strengthen the security of the latter [146].

- *Quantum fingerprinting.* Fingerprinting is a classical technique for associating with each large data set a small bitstring such that the bitstring for each data set is distinct. It has been shown that using quantum techniques, more efficient construction of fingerprints for distributed data sets is possible [147].
- *Secure remote computation.* In this protocol, the premise is that Alice has a computation she wants to do on a quantum computer; she has only a very small computer, but she has a quantum channel connecting her to Bob, who has a large quantum computer. She wants to have a computation performed by Bob, but she does not want him to know the nature of the computation or for him to be able to obtain any information about the answers without her detecting it. A quantum protocol exists that meets all these requirements [148,149].
- *Private quantum channels.* Quantum channels can be made private, i.e., containing only transmissions that are completely unintelligible to an interceptor, with the use of shared classical randomness between sender and receiver. For exact privacy, two bits per sent qubit are necessary and sufficient. For asymptotically perfect privacy, it is now known that one bit per qubit is sufficient [150,151,152,153]. If this shared resource is quantum, then there are scenarios in which the shared resource can be recycled [154] (if a negligible amount of eavesdropping is detected).
- *Quantum digital signatures.* With this scheme, a sender (Alice) can sign a message in such a way that the signature can be validated by a number of different people, and all will agree either that the message came from Alice or that it has been tampered with. To accomplish this task, each recipient of the message must have a copy of Alice's "public key", which is a set of quantum states whose exact identity is known only to Alice. Quantum public keys are more difficult to deal with than classical public keys: for instance, only a limited number of copies can be in circulation, or the scheme becomes insecure. However, in exchange for this price, unconditionally secure digital signatures are claimed. Sending an m -bit message uses up $O(m)$ quantum bits for each recipient of the public key (adapted from [155]).
- *Privacy in remote database access.* Private-information-retrieval (PIR) systems allow a user to extract an item from a database that is replicated over $k \geq 1$ servers, while satisfying various privacy constraints. Quantum k -server symmetrically private information-retrieval (QSPIR) systems have been found that
 - use sublinear communication,
 - do not use shared randomness among the servers, and
 - preserve privacy against honest users and dishonest servers.
 Classically, SPIRs without shared randomness do not exist at all (adapted from [156]).
- *Quantum interactive proofs.* Certain computational problems (e.g., graph nonisomorphism) are defined as requiring the participation of two parties; of interest is the case where one knowledgeable party is trying to prove something to an ignorant but intelligent party. It is known that these "interactive proofs" may require arbitrarily many rounds of communication between the two parties. It is now known that in a quantum settings, just three rounds of quantum communication are sufficient [78].
- *Authentication of quantum messages.* Authentication is a well-studied area of classical cryptography: a sender, S , and a receiver, R , sharing a classical private key want to exchange a classical message with the guarantee that the message has not been modified by any third

party with control of the communication line. Authentication of messages composed of quantum states is possible. Assuming S and R have access to an insecure quantum channel and share a private, classical random key, a noninteractive scheme exists that enables S both to encrypt and to authenticate (with unconditional security) an m qubit message by encoding it into $m + s$ qubits, where the failure probability decreases exponentially in the security parameter, s . The classical private key has $2m + O(s)$ bits. Any scheme to authenticate quantum messages must also encrypt them. (In contrast, one can authenticate a classical message while leaving it publicly readable.) This gives a lower bound of $2m$ key bits for authenticating m qubits, and it shows that digitally signing quantum states is impossible, even with only computational security (adapted from [148,149]).

- *Secure multiparty QC.* Secure multiparty computing, also called “secure function evaluation”, has been extensively studied in classical cryptography. This task can be extended to computation with quantum inputs and circuits. The protocols are information-theoretically secure, i.e., no assumptions are made on the computational power of the adversary. For the weaker task of verifiable quantum secret sharing, there is a protocol that tolerates any $t \leq n/4$ cheating parties (out of n). This is optimal. This tool can perform any multiparty QC as long as the number of dishonest players is $< n/6$ (adapted from [148,149]).

5.0 Quantum-Computer Architectures

Large-scale quantum computers, if they can be built, will be complex quantum systems with many parts, all of which must work together coherently to perform large-scale quantum computations. To construct a large-scale quantum computer, it is not enough to exhibit components (qubits, quantum logic gates, input-output devices, etc.) sufficient for attaining the DiVincenzo criteria, and each of which on its own attains the limits required for fault-tolerant QC. The components of a large-scale quantum computer must be designed to fit together and to work together. That is, a large-scale quantum computer must have an architecture—a unified overall design in which each component plays an integral role. In addition, each of these components must be designed for optimal efficiency. For example, the quantum fourier transform is a fundamental building block in all quantum algorithms, and recent work has shown that we can significantly enhance the performance of this component by implementing quantum circuits for the quantum fourier transform with only logarithmic depth [157,158].

Note that theory, coupled strongly to experiment, is a necessary part of developing a viable quantum-computer architecture. Designing an architecture for a quantum computer is fundamentally a theoretical task: one is creating specifications and solving problems for a device that does not yet exist. Of course, because a viable architecture must marry theoretical concept with experimental reality, the design of such an architecture is a theoretical task at which experimentalists can excel as well as theorists. As will be seen below, in the specification of the stages and development of quantum-computing architectures, designing and building quantum computers is a task that must be performed by experimentalists and theoreticians working together. For example, approach of 'encoded universality', which emerged from theoretical work in decoherence-free subspaces, has potential for simplifying spin based computation in solid state QC since it relies exclusively on tuning the exchange interaction and does not require local magnetic fields [159].

A quantum-computer architecture specifies not only the components of a quantum computer (qubits, quantum logic gates, I/O devices, etc.), but provides protocols and mechanisms for how those components are to work together. Even at the early stages of development of a quantum-computing technology, as in the case of semiconductor quantum computers, considerable effort must be made to design architectures that allow the different pieces of the quantum computer to function together.

Quantum-computer architectures have played a key role in the development of quantum computers. The Cirac-Zoller proposal for ion-trap QC provides an architecture for medium-scale quantum computers with $O(10^1)$ qubits. Cirac and Zoller specified explicit designs for qubits (hyperfine levels of ions), quantum logic gates (optical resonance), quantum “wires” (the use of a shared vibrational mode as a quantum “bus” to transfer information from one qubit to another), as well as readout (fluorescence via cycling transitions). Most important, they showed how all of these different components for a small- to medium-scale quantum computer could, in principle, be put together to perform simple QC coherently. Their proposal was based on quantum technologies that had been pioneered by experimentalists in atomic and optical physics (Wineland, Monroe, Blatt). Because it supplied a well-thought-out design together with explicit proposals for implementing the pieces of that design in an integrated fashion, the Cirac-Zoller proposal was swiftly implemented by Wineland and Monroe. The Cirac-Zoller proposal met with swift success exactly because it specified an architecture for QC.

A detailed quantum-computing architecture is a necessary proof of principle that a particular method for performing QC has a chance of succeeding. The initial work on QC of Benioff, Feynman, and Deutsch, in the 1980s took place in the absence of any specific ideas on how a quantum computer might, in fact, be built. It was not until the explicit demonstration of a universal architecture for QC using electromagnetic resonance [160] that it became clear that quantum computers might actually be built. The techniques for using electromagnetic resonance to perform universal QC subsequently matured in simple NMR QIPs, which were then used to demonstrate the first quantum algorithms.

In short, a well-thought-out architecture is the key to successful quantum-computer design. Given the importance of QC architectures, it should be no surprise that the development of such architectures has played and continues to play a key role in the Quantum Computing Roadmap. We can identify a set of stages in the development of QC architectures. Each stage is associated with advances in the quantum technologies required to realize that architecture. Each stage represents, in essence, a test that a QC architecture must pass if it is to form the basis for constructing a viable quantum computer.

5.1 Initial Conceptual Development

In this stage, the basic concepts for meeting the DiVincenzo criteria for constructing a viable quantum computer are developed. Potential answers are supplied to the questions of how quantum information is to be registered (qubits), how it is to be processed (quantum logic gates), how it is to be moved from one place to another (quantum “wires” and quantum “buses”) how it is to be programmed in and read out (I/O devices). The initial conceptual development can be purely theoretical, but must be fully informed by existing quantum

technologies or quantum technologies under development. Care must be taken to insure that the quantum-computer architecture is integrated (i.e., that the various components of the quantum computer can act coherently and in concert together).

5.2 Testing the Components

In this stage, the different components of the architecture are subjected to experimental tests and to more detailed theoretical investigations to determine whether or not they “meet spec.”

- Qubits are prepared, manipulated, and read out.
- Relaxation and decoherence times are measured.
- Quantum operation and state tomography are performed.

The testing stage for the components of a quantum-computer architecture forms the basis for an extended experimental program. As tests reveal the strengths and weaknesses of a particular approach, the architecture is revised and refined to emphasize those strengths and to minimize the effects of the weaknesses. (An example of such revision and refinement is Wineland’s development of techniques for moving ions coherently from one ion trap to another, to get around the problem of the finite size of ion traps.)

5.3 Assembling the Components into a Working Device

In this stage, the various components of the quantum-computing architecture are assembled to construct a working QIP capable of performing QC. The ability to perform sequences of coherent quantum manipulations and to put them together in a quantum algorithm is a strong test of the viability of a quantum-computing architecture. To date, only a few architectures have succeeded in performing extended sequences of coherent logic manipulations. Room-temperature NMR QIPs, despite their intrinsic lack of scalability, have been strikingly successful at performing demonstrations of quantum algorithms such as the Deutsch-Jozsa algorithm, Grover’s algorithm, and Shor’s algorithm, as well as quantum error correction, decoherence-free subspaces (DFSs), etc. The success of such demonstrations bodes well for the ability of lower-temperature (e.g., optically pumpable) scalable NMR devices to perform larger-scale quantum computations. Similarly, ion-trap quantum computers have been used to exhibit a wide variety of techniques for coherently manipulating quantum information, including the recent performance of a quantum algorithm on an ion-trap quantum computer. The recent demonstration of coherent one- and two-qubit quantum logic operations on superconducting quantum bits suggests that superconducting quantum computers may soon be capable of performing quantum algorithms.

Actually operating a quantum computer with a particular architecture is, of course, the proof in practice that the architecture can indeed function at a particular scale (i.e., number of qubits and number of quantum logic operations).

5.4 Scaling up the Architecture

Once a quantum-computing architecture has been developed, tested, and put into practice, it can then be scaled up to more qubits and to more coherent quantum logic operations. As the architecture is scaled up, stages one, two, and three above must be revisited again and again. Often, the testing of the components and their assembly into a coherently functioning whole will reveal a weakness of the initial conceptual scheme, which must be readdressed at the fundamental conceptual level if the architecture is to be scaled to the next level. (Once again, Wineland's movable ions are an example of the recognition of a weakness and the development of a fundamental quantum technology to correct that weakness. Similarly, the development of methods for performing optical pumping for NMR-based systems addresses and corrects the problem of state preparation for liquid-state NMR.)

Each increase in the number of qubits and the number of coherent operations supplies a strong test of the scalability of a QC architecture. Each doubling of the number of qubits and number of quantum logic operations typically brings with it a host of new quantum technological problems, which must be addressed and solved in detail before the quantum-computing architecture can be brought to the next level.

To optimize and test scalable quantum computers requires theoretical software that can simulate the dynamics of algorithms involving a large number of qubits. Some pioneering work has been done to create perturbation theories and software that enable one to calculate the dynamics of a restricted set of logic involving a large number of qubits [161,162]. These perturbation theories are essential for minimizing the error rates of quantum computers involving more than 30 qubits. Related theoretical progress has been in resolving dynamical issues for single-qubit measurement technologies based on magnetic resonance force microscopy, scanning tunneling microscopy, optical magnetic resonance and resolving dynamical problems for utilizing and measuring charge based qubits using single-electron transistors and other nano-devices based on semiconductor and superconductor materials [163].

In order to meet the five- and ten-year goals of the Quantum Computing Roadmap, all four stages of the development of QC architectures must be accomplished at least once for each viable QC technology. In order to construct a quantum computer with eight or more qubits, a QC architecture must undergo at least three doublings from its initial demonstration of a viable quantum bit. Theory plays a key role in the development of QC architectures. The initial conceptual development of such an architecture is a purely theoretical task. As the architecture is tested, assembled, and scaled up, the development of theoretical concepts and solutions is married ever more closely with the experimental development of specific quantum technologies.

5.5 "Type-II" Quantum Computing

Type-II QC is a particular application of quantum simulation, in which quantum "microprocessors" are connected via classical links. Type-II QC is useful for simulating systems in which coherent quantum behavior is important at small scales. Systems that could potentially benefit from the application of Type-II QC include nanofluids, quantum gases, Bose-Einstein condensates, and plasmas at high temperatures and pressures. Unlike quantum simulation in

general, Type-II QC does not afford an exponential speed-up over classical computation. However, there are specific and important problems for which the exponential power of QC can be brought to bear to simulate using a few tens of qubits an intrinsically quantum piece of a larger system that would require a supercomputer to simulate classically. Such few-qubit quantum microprocessors might then be hooked up using classical communication links to perform mixed quantum/classical simulation of extended quantum systems.

6.0 Decoherence Roadblocks for Quantum Information Processing

6.1 Theoretical Terminology

Quantum information processing relies to a large extent upon the ability to ensure and control unitary evolution of an array of coupled qubits for long periods of time. There are a number of physical effects that act against this coherent evolution. These include interaction of the qubits with a larger environment, unwanted or uncontrolled interactions between qubits, and imperfections in applied unitary transformations. The latter can be either systematic or random, and can also give rise to additional unitary errors. The term “decoherence” referred originally explicitly to errors that arise in the wave function phase, i.e., to decay of off-diagonal terms in the density matrix. This decay of phase is basis-set dependent. It also does not constitute the only source of loss of unitarity. Today, the term decoherence is therefore more generally understood in the field of QIP to refer to all manifestations of loss of unitarity in the qubit state time evolution. It thereby includes

1. explicit loss of coherence,
2. dissipative or energy relaxation effects, as well as
3. leakage out of the qubit state space.

There are many theoretical languages in which decoherence may be framed and usefully understood. Nonunitary evolution of qubit states and density matrices may be generally regarded as resulting from entanglement of the qubit states with those of a larger quantum system whose quantum evolution is of no intrinsic interest, such as the environment or a measuring device [164]. This entanglement with the environment converts pure qubit states into mixed states and results in a loss of information from the qubit system that can be quantified by an associated increase in entropy. The resulting qubit density matrix is referred to as the “reduced density matrix.”

- The density matrix allows analysis of decoherence resulting from physical interactions via formulation and solution of many different levels of master equations that have been developed to study the dynamics of reduced density matrices [165] (and see below). These constitute one set of languages for analysis, systematization, and quantification of decoherence.
- Another type of decoherence language deriving from the reduced density matrix is that of superoperators. So named because they act on the density matrix which is itself an operator, superoperators provide a very useful formalism for general analysis of the evolution of pure states into mixed states. An important distinction between unitary evolution operators and superoperators is that the former always constitute a group while the latter may sometimes

define a dynamical semigroup that lacks an inverse. The language of superoperators is naturally related to that of generalized measurements, allowing useful connections between decoherence and measurements to be established. The operator sum representation provides a compact way to obtain the superoperators that result from any specific Hamiltonian describing the qubit system and its interaction with the environment [166].

- Nonunitary time evolution can also be expressed as the action of quantum noise operations [167]. These are maps that describe the introduction of errors onto qubit states. They are written in a digitized form (error occurs with probability p) analogous to the noise channels employed in classical information theory.

6.2 Studies of Decoherence and Ways to Overcome It

Over 2000 publications have appeared in the last four years discussing decoherence. Theoretical studies of decoherence and its mitigation to date have tended to fall into four broad categories.

1. Physical studies of origin and magnitude of decoherence for specific candidate qubit states in specific physical systems. Such studies generally seek to predict values of the decay times T_1 (energy dissipation or population relaxation) and T_2 (dephasing) for qubit states, starting from specific models of coupling mechanisms and of the spectral distribution of the environment (bath), and assumptions as to Markovian or nonMarkovian dynamics of the environment on the intrinsic time scale of the qubit states. For a recent review of these approaches, see, e.g., [168].
2. Mitigation of decoherence by either encoding to allow subsequent quantum error correction (active error correction), or encoding to eliminate or suppress decoherence (passive error correction). The former includes quantum error-correcting codes that have been developed to correct a wide variety of errors [77,169,]. Construction of fault-tolerant protocols using these codes has been demonstrated. The passive error-correction approach includes use of decoherence-free subspaces and subsystems, and in its most ambitious form is represented by topological QC (below).
3. Work on topological QC which seeks to develop naturally fault-tolerant codes may be viewed as an ambitious alternative paradigm that would provide a powerful set of self-correcting codes immune to many of the usual sources of decoherence if the required Hamiltonians could be physically realized [170].
4. Suppression of decoherence by dynamical decoupling techniques. These employ external pulse fields in a controlled manner that is specifically designed to cancel or minimize errors by averaging them out. These methods are related to coherent averaging methods in pulsed magnetic resonance spectroscopy, and have recently been extended from the original techniques requiring arbitrarily strong, instantaneous control pulses (“bang-bang control”) to realistic bounded-strength Hamiltonians (“Eulerian decoupling”) [171].

Some work has been done on combining several of the above approaches to obtain combined error correction techniques for QC architectures that have the capability of correcting errors deriving from very different physical sources [172]. There are a number of further directions beyond these characterization and mitigation studies that would be valuable to pursue in the next period of research into control of decoherence. These include:

- Relatively few studies have addressed the effect of decoherence on short time qubit dynamics, i.e., within T_2 , and possibly over the time period during which control pulses would be applied. Studies of electron spin decoherence due to hyperfine interactions with nuclear spin are a first step in this direction, analyzing the effect of very short time nonexponential electron spin dynamics. Measures of decoherence times based on the density matrix norm rather than on exponential time scales for decay of matrix elements have been proposed to quantify such short time dynamics [173]. Weakly coupled situations where decoherence can produce nonexponential behavior that can give rise to ‘prompt’ loss of coherence amplitude [174] or, under appropriate conditions, manifest itself solely as a reduction in the norm of an effective system wavefunction [175], may provide a useful new avenue to explore coherent control of intrinsically noisy qubit systems. This is particularly relevant to qubit implementations displaying ‘reduced visibility’ or ‘reduced contrast’ Rabi oscillations [176,177].
- There have also been few studies of decoherence that might arise specifically during gate switching of control fields. Some studies of pulse shaping and of compensation techniques to stabilize control pulses against imperfections have been made [178]. We expect such studies to become routine and to benefit from interaction between theory and experiment.
- Complete simulations of controlled manipulations of coupled qubits with realistic decoherence effects are rare. A few such simulations of small-scale algorithms on coupled qubits have been made [179].
- Despite much theoretical work on fault-tolerant protocols, complete analysis of the error threshold for fault-tolerant QC applicable to a specific set of errors for a given physical implementation is lacking. This represents a highly desirable direction of theoretical and simulation research and would usefully be combined with the algorithmic simulations described above.
- Develop realistic microscopic description of the parameters for quantum noise operators, to enable a unification of microscopic physical studies of decoherence with information theoretic description of noise channels.

6.3 Physical Sources of Decoherence

The following is a summary of physical sources of decoherence that have been identified and/or discussed for the physical implementations listed in Table 4.0-1.

1. NMR
 - 1.1 liquid state
 - 1.1.1 external random fields due primarily to dipoles of spins in other molecules going past the molecule in question
 - 1.1.2 modulation of through-space dipolar interactions between spins in the same molecule through rotational diffusion of the molecule changing the direction of the tensor with respect to the external field
 - 1.1.3 modulation of the chemical shift of a spin through its dependence on the orientation of the molecule with respect to the external field and rotational diffusion

- 1.1.4 quadrupole/electric field gradient coupling modulation (spin $> 1/2$)
- 1.2 solid state
 - 1.2.1 chemical shift/dipole coupling dispersion in inhomogeneous samples
 - 1.2.2 entanglement of spins through dipole coupling with their neighbors
 - 1.2.3 spontaneous phonon emission and Raman spin/phonon interactions (the latter dominates at high temperatures)
 - 1.2.4 spectral diffusion due to other nuclear species and magnetic impurities
- 2. Trapped Ions
 - 2.1 spontaneous emission from ions
 - 2.2 cross talk in ion addressing due to imperfect laser focusing
 - 2.3 mode-mode couplings due to anharmonicities of the trap
 - 2.4 "heating" of ion motion due to stray radiofrequency fields, patch potentials, etc.
 - 2.5 coupling of thermal vibrations into internal ion states
 - 2.6 leakage losses into other atomic levels (i.e., breakdown of the two-level qubit approximation)
 - 2.7 ionization
 - 2.8 inefficiencies in readout
- 3. Neutral Atoms
 - 3.1 photon scattering from trapping laser fields
 - 3.2 photon scattering from Raman laser fields during single qubit transitions
 - 3.3 spontaneous emission from Rydberg states during a Rydberg gate operation (including effects of black-body radiation)
 - 3.4 background gas collision (includes qubit loss and leakage, and also standard qubit errors)
 - 3.5 fluctuating trap potentials
 - 3.6 background magnetic fields
 - 3.7 heating of atoms (i.e., vibrational excitation in the optical lattice potential)
 - 3.8 scattering to atomic states outside the computational basis during collisional gates
- 4. Cavity QED
 - 4.1 motional decoherence from trap fluctuations and environmental noise
 - 4.2 motional decoherence from gate operations, noise in driving fields
 - 4.3 photon qubit decoherence when strong coupling regime not achieved or exited during operations
 - 4.4 differential Stark shifts from optical trapping fields
 - 4.5 spontaneous emission, background gas collisions, photon scattering, and other sources of decoherence for ions and neutral atoms (see items 2 and 3 above)
- 5. Optical
 - 5.1 scattering from the electromagnetic vacuum, leading to possible photon loss:

- 5.1.1 loss at the source (failure of single photon source)
 - 5.1.2 loss in processing/transit
 - 5.1.3 loss in detection
 - 5.2 photon addition (from failure of the source or a detector, mistaking one photon for two photons, e.g., as a result of detector noise)
 - 5.3 failure of a teleportation gate (corresponding to a detected qubit measurement error)
 - 5.4 phase errors deriving from failure to carefully tune interferometers or from timing errors in teleportation protocols
6. Solid State
- 6.1 spin based
 - 6.1.1 spontaneous phonon emission mediated by spin-orbit coupling
 - 6.1.2 dipolar couplings with magnetic impurities and other trapped electrons
 - 6.1.3 hyperfine interaction with nuclear spins, giving rise to
 - 6.1.3.1 direct electron-nuclear spin flip (may or may not include phonon emission)
 - 6.1.3.2 spectral diffusion whereby dipolar coupling induced fluctuation of nuclear spins leads to a fluctuating hyperfine field acting on electron spin
 - 6.1.4 inhomogeneous qubit environments (magnetic fields, impurities, quantum-dot sizes, interface strains, defects, frozen hyperfine fields)
 - 6.1.5 gate errors due to inhomogeneities
 - 6.1.6 current and voltage fluctuations
 - 6.1.7 switching errors due to imperfect gate operations on qubits
 - 6.1.8 measurement process
 - 6.2 charge based
 - 6.2.1 spontaneous photon emission
 - 6.2.2 spontaneous phonon emission
 - 6.2.3 gate voltage fluctuations (due to thermal noise, trapped charges, electromagnetic environment)
 - 6.2.4 electron tunneling and co-tunneling in the dots/donors
7. Superconducting
- 7.1 electromagnetic environment
 - 7.2 phonons
 - 7.3 (hot) quasiparticles
 - 7.4 background charges
 - 7.5 critical current noise
 - 7.6 spurious resonances (and critical current noise)
 - 7.7 gate voltage fluctuations
 - 7.8 nuclear spins

7.9 paramagnetic impurities

6.4 Decoherence Analyses

The following decoherence models and theoretical approaches have been used to analyze decoherence in the above QC implementations.

1. NMR
 - 1.1 liquid state
 - 1.1.1 Hadamard product formalism
 - 1.1.2 Redfield theory and Redfield kite structure of NMR relaxation superoperators
 - 1.1.3 spherical harmonic tensor expansions of dipole-dipole and other interactions, combined with Langevin analysis
 - 1.1.4 stochastic Liouville method
 - 1.1.5 quantum noise channels
 - 1.2 solid state
 - 1.2.1 the method of moments
 - 1.2.2 spin-boson models parameterized by experiment
 - 1.2.3 a wide variety of semiclassical models
2. Trapped Ion
 - 2.1 standard first order perturbation theory
 - 2.2 Weisskopf-Wigner/Markov approximation techniques for spontaneous emission modeling
 - 2.3 quantum Monte Carlo numerical modeling
 - 2.4 analytic non-Markovian stochastic models for some effects (e.g., heating)
3. Neutral Atoms
 - 3.1 wave packet simulations
 - 3.2 stochastic Schroedinger equation (Monte Carlo wave function approach); applicable for large scale simulations
 - 3.3 master equation approach (including Redfield or Lindblad model of dissipative superoperator)
 - 3.5 analysis of heating/decoherence rates due to trap fluctuations and collisions
 - 3.6 analysis of gate leakage due to collisions
4. Cavity QED
 - 4.1 perturbation theory
 - 4.2 Weisskopf-Wigner/Markov approximation techniques for spontaneous emission modeling
 - 4.3 Monte Carlo wavefunction (stochastic trajectory) approach
 - 4.4 master equations
 - 4.5 analysis of heating rates due to trap fluctuations and gas collisions

5. Optical
 - 5.1 gate fidelity calculations in presence of photon loss, modeled by beamsplitter that mixes mode with vacuum state
 - 5.2 quantum error encodings and protocols to correct for photon loss
6. Solid State
 - 6.1 spin-based
 - 6.1.1 master equation in extended Bloch-Redfield description for single spin decoherence
 - 6.1.2 single spin decay due to phonon emission by perturbative and basis set calculations within effective mass theory
 - 6.1.3 many spin decay due to inhomogeneities within tight-binding description
 - 6.1.4 method of moments for dipolar coupling to impurities
 - 6.1.5 spin-bath theory
 - 6.1.6 gate fidelity calculations for effects of inhomogeneities, switching errors, spin-orbit coupling
 - 6.1.7 master equation in Born-Markov limit for analysis of measurement efficiency and n-shot read out
 - 6.1.8 exact solution with Laplace transforms for effect of hyperfine coupling in fully polarized nuclear spin field
 - 6.1.9 perturbative analyses of hyperfine coupling effects for general (partially polarized) nuclear spin field, evidence for non-exponential decay
 - 6.1.10 stochastic noise theory combined with method of moments for analysis of indirect effects of hyperfine coupling via nuclear spectral diffusion
 - 6.2 charge-based
 - 6.2.1 perturbation theory for photon/phonon emission
 - 6.2.2 Bloch-Redfield theory for photon/phonon emission and for electron tunneling/co-tunneling
 - 6.2.3 stochastic noise theory to describe charge noise and gate fluctuations
7. Superconducting
 - 7.1 generalized spin-Boson theory
 - 7.2 spin-bath model
 - 7.3 Fano-Anderson/Dutta-Horne model (for $1/f$ noise)
 - 7.4 mesoscopic transport models (for read-out)
 - 7.5 Bloch-Redfield theory
 - 7.6 real-time path integrals
 - 7.7 diagrammatic Keldysh technique and exact solutions for simplified Hamiltonians
 - 7.8 quantum Monte Carlo
 - 7.9 renormalization group
 - 7.10 Bloch vector diffusion (stochastic differential equation)
 - 7.11 analysis of qubit depolarization in readout

7.0 Glossary

8.0 References

- [1] Farhi, E., J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," (28-Jan-00) preprint *quant-ph/0001106*.
- [2] Aharonov, D. and A. Ta-Shma, "Adiabatic quantum state generation and statistical zero knowledge," (7-Jan-03) preprint *quant-ph/0301023*.
- [3] Aharonov, D., W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, "On the universality of adiabatic quantum computation," manuscript 2003.
- [4] Childs, A.M., R.C. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D.A. Spielman, "Exponential algorithmic speedup by a quantum walk," Proceedings of the 35th ACM Symposium on Theory of Computing (STOC 2003), (ACM Press, New York, NY, USA, 2003), pp. 59–68 [ISBN:1-58113-674-9].
- [5] Ambainis, A. "Quantum walk algorithm for element distinctness," (1-Nov-03) preprint *quant-ph/0311001*.
- [6] Bennett, C.H., E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing* **26**, 1510–1523 (1997).
- [7] van Dam, W., M. Mosca, and U. Vazirani, "How powerful is adiabatic quantum computation?," *Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science (FOCS'01)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2001), pp. 279–287.
- [8] Arora, S., R. Impagliazzo, and U. Vazirani, "The principle of local checkability and relativizing arguments in complexity theory," *Proceedings of the 8th Annual Structure in Complexity Theory Conference*, (IEEE Computer Society Press, 1993) [ISBN 0-8186-4070-7].
- [9] Aharonov, D. and D. Gottesmann, "Improved threshold for fault-tolerant quantum computation," manuscript, 2002.
- [10] Steane, A.M. and B. Ibinson, "Fault-tolerant logical gate networks for CSS codes," (4-Nov-03) preprint *quant-ph/0311014*.
- [11] Razborov, A.A., "An upper bound on the threshold quantum decoherence rate," manuscript.
- [12] Kitaev, A., "Quantum measurements and the abelian stabilizer problem," *Proceedings of the Electronic Colloquium on Computational Complexity (ECCC-1996)*, **3**(3), ECCC Report TR96-003 (1996) [*quant-ph/9511026*].

- [13] Abrams, D.S. and S. Lloyd, "A Quantum algorithm providing exponential speed increase for finding eigenvalues and eigenvectors," *Physical Review Letters* **83**, 5162–5165 (1999) [[quant-ph/9807070](#)].
- [14] Traub, J. and H. Wozniakowski, "Path integration on a quantum computer," *Quantum Information Processing* **1**, 365–388 (2002) [[quant-ph/0109113](#)].
- [15] Vidal, G., "Efficient simulation of one-dimensional quantum many-body systems," (14-Oct-03) preprint [quant-ph/0310089](#).
- [16] Bell, J.S., "On the Einstein-Podolski-Rosen paradox," *Physics* **1**, 195–200 (1964), reprinted in *Speakable and Unsayable in Quantum Mechanics*, (Cambridge University Press, Cambridge, UK, 1987) pp. 14–21
- [17] Bell, J.S., "On the problem of hidden variables in quantum mechanics," *Reviews of Modern Physics* **38**, 447–452 (1966).
- [18] Landauer, R., "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development* **5**(3), 183–191 (1961).
- [19] Bennett, C.H., "Logical reversibility of computation," *IBM Journal of Research and Development* **17**(6), 525–530 (1973).
- [20] Benioff, P., "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *Journal of Statistical Physics* **22**, 563–591 (1980).
- [21] Benioff, P., "Quantum mechanical models of Turing machines that dissipate no energy," *Physical Review Letters* **48**, 1581–1585 (1982).
- [22] Feynman, R.P., "Simulating physics with computers," *International Journal of Theoretical Physics* **21**, 467–488 (1982).
- [23] Deutsch, D., "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **400**(1818), 97–117 (1985).
- [24] Bernstein, E. and U. Vazirani, "Quantum complexity theory," *Proceedings of the of the 25th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1993) pp. 11–20 [ISBN: 0-89791-591-7].
- [25] Deutsch, D. and R. Josza, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **439**, 553–558 (1992).
- [26] Simon, D., "On the power of quantum computation," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS'94)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) pp. 116–123.
- [27] Shor, P.W., "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS'94)*,

- (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) pp.124–134; [revised version at *quant-ph/9508027*].
- [28] Grover, L., “A fast quantum mechanical algorithm for database search,” *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1999) pp.212–219 [ISBN:0-89791-785-5, *quant-ph/9605043*].
- [29] Shor, P.W., “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A* **52**, R2493–R2496 (1995).
- [30] Calderbank, A.R. and P.W. Shor, “Good quantum error-correcting codes exist,” *Physical Review A* **54**, 1098–1105 (1996).
- [31] Steane, A.M., “Error correcting codes in quantum theory,” *Physical Review Letters* **77**, 793–797 (1996).
- [32] Kitaev, A.Y., “Quantum computations: Algorithms and error correction,” *Russian Mathematical Surveys* **52**, 1191–1249 (1997).
- [33] Shor, P.W., “Fault-tolerant quantum computation,” *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science (FOCS’96)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1996) pp.56–67.
- [34] Aharonov, D. and M. Ben-Or, “Fault tolerant quantum computation with constant error,” (14-Nov-96) preprint *quant-ph/9611025*.
- [35] Knill, E., R. Laflamme and W.H. Zurek, “Resilient quantum computation: Error models and thresholds,” *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **454**, 365–384 (1998).
- [36] Gottesmann, D., “Stabilizer codes and quantum error correction,” Ph.D. thesis, California Institute of Technology (1997) (114 pp. electronic version at *quant-ph/9705052*).
- [37] Preskill, J., “Reliable quantum computers,” *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **454**, 385–410 (1998).
- [38] Aaronson, S., “Quantum lower bound for the collision problem,” *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 2002) pp.635–642 [ISBN:1-58113-495-9, *quant-ph/0111102*].
- [39] Watrous, J., “On quantum and classical space-bounded processes with algebraic transition amplitudes,” *Proceedings of the 40th Annual Symposium on the Foundations of Computer Science (FOCS’99)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1999) pp.341–351.
- [40] Buhrman, H., R. Cleve, and A. Wigderson, “Quantum vs. classical communication and computation,” *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1998) pp.63–68 [ISBN:0-89791-962-9].

- [41] Ambainis, A., L.J. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson, "The quantum communication complexity of sampling," *Proceedings of the 39th Annual Symposium on the Foundations of Computer Science (FOCS'98)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1998) pp. 342–351.
- [42] Raz, R., "Exponential separation of quantum and classical communication complexity," *Proceedings of the 31st ACM Symposium on Theory of Computing (STOC 1999)*, (ACM Press, New York, NY, USA, 2001), pp. 358–367.
- [43] Bar-Yossef, Z., T.S. Jayram, and I. Kerenidis. "Exponential separation of quantum and classical one-way communication complexity," (to be presented at the 36th Annual ACM Symposium on Theory of Computing [STOC 2004] Chicago, Illinois, USA, June 13–15, 2004).
- [44] Holevo, A.S., "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems of Information Transmission* **9**(3), 177–183 (1973).
- [45] Wootters, W.K. and W.H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, 802–803 (1982).
- [46] Bennett, C.H. and S.J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters* **69**, 2881–2884 (1992).
- [47] Bennett, C.H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **70**, 1895–1899 (1993).
- [48] Schumacher, B., M. Westmoreland, and W.K. Wootters, "Limitation on the amount of accessible information in a quantum channel," *Physical Review Letters* **76**, 3452–3455 (1997).
- [49] Sasaki, M., K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," *Physical Review A* **58**, 146–158 (1998).
- [50] Holevo, A.S., "On capacity of a quantum communications channel," *Problems of Information Transmission* **15**(4), 247–253 (1979).
- [51] Schumacher, B. and M. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A* **56**, 131–138 (1997).
- [52] Holevo, A.S., "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory* **IT-44**(#1), 269–273 (1998).
- [53] Bennett, C.H., H.J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Physical Review A* **53**, 2046–2052 (1996).
- [54] Bennett, C.H., G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters* **76**, 722–725 (1996).
- [55] Bennett, C.H., D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A* **54**, 3824–3851 (1996).

- [56] Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, (IEEE, New York, 1984) pp 175–179.
- [57] Hallgren, S., "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem," *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 2002) pp. 653–658 [ISBN:1-58113-495-9].
- [58] van Dam, W. and S. Hallgren, "Efficient quantum algorithms for shifted quadratic character problems," (15-Nov-00) preprint *quant-ph/0011067*.
- [59] Ip, L., "Solving shift problems and hidden coset problem using the Fourier transform," (7-May-02) preprint *quant-ph/0205034*.
- [60] van Dam, W. and G. Seroussi, "Efficient quantum algorithms for estimating Gauss sums," (23-Jul-02) preprint *quant-ph/0207131*.
- [61] Regev, O., "Quantum computation and lattice problems," *Proceedings of the 43rd Annual Symposium on the Foundations of Computer Science (FOCS'02)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2002), pp. 520–530.
- [62] Grigni, M., L. Schulman, M. Vazirani, and U. Vazirani, "Quantum mechanical algorithms for the nonabelian hidden subgroup problem," *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC 2001)*, (ACM Press, New York, NY, USA, 2001), pp. 68–74 [ISBN:1-58113-349-9].
- [63] Ettinger, M., P. Hoyer, and E. Knill, "The quantum query complexity of the hidden subgroup problem is polynomial," (12-Jan-04) preprint *quant-ph/0401083*.
- [64] Kuperberg, A., "Subexponential-time quantum algorithm for the dihedral hidden subgroup problem," (14-Feb-03) preprint *quant-ph/0302112*.
- [65] Magniez, F., M. Santha, and M. Szegedy, "Quantum algorithm for detecting triangles," manuscript 2003.
- [66] van Dam, W. and U. Vazirani, "Limits on quantum adiabatic optimization," 5th Workshop on Quantum Information Processing (QIP 2002), IBM T.J. Watson Research Center, Yorktown Heights, New York, USA, January 14–17, 2002.
- [67] Reichardt, B., "The quantum adiabatic optimization algorithm and local minima," (to be presented at the 36th Annual ACM Symposium on Theory of Computing [STOC 2004] Chicago, Illinois, USA, June 13–15, 2004).
- [68] Farhi, E., J. Goldstone, S. Gutman, B. Reichardt, U. Vazirani, "Tunneling in quantum adiabatic optimization," manuscript in preparation 2004.
- [69] Farhi, E. and S. Gutmann, "Quantum mechanical square root speedup in a structured search problem," (18-Nov-97) preprint *quant-ph/9711035*.

- [70] Watrous, J. “Quantum simulations of classical random walks and undirected graph connectivity,” *Journal of Computer and System Sciences*, **62**(2), 376–391, (2001) [A preliminary version appeared in *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pp. 180–187, (1999)].
- [71] Ambainis, A., D. Aharonov, J. Kempe, U.V. Vazirani, “Quantum walks on graphs,” *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC 2001)*, (ACM Press, New York, NY, USA, 2001), pp. 50–59 [ISBN: 1-58113-349-9].
- [72] Lo, H.-K. and H.F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science* **283**, 2050–2056 (1999).
- [73] Lidar D.A., and K.B. Whaley, “Decoherence-free subspaces and subsystems in irreversible quantum dynamics,” in *Springer Lecture Notes in Physics*, F. Benatti and R. Floreanini, Eds., (Springer-Verlag, Berlin, 2003) Vol. 622, pp. 83120 [quant-ph/0301032].
- [74] Bacon, D., K.R. Brown, and K.B. Whaley, “Coherence-preserving quantum bits,” *Physical Review Letters* **87**, 247902 (2001).
- [75] Freedman, M., A. Kitaev, M.J. Larsen, and Z. Wang, “Topological quantum computation,” *Bulletin of the American Mathematical Society* **40**, 31–38 (2003) [quant-ph/0101025].
- [76] Gottesman, D., A.Y. Kitaev, and J. Preskill, “Encoding a qubit in an oscillator,” *Physical Review A* **64**, 012310 (2001).
- [77] Gottesman, D., “An introduction to quantum error correction,” in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, S. Lomonaco, Jr., Ed., (American Mathematical Society, Providence, Rhode Island, 2002), pp. 221–235 [quant-ph/0004072].
- [78] Kitaev, A.Y. and J. Watrous, “Parallelization, amplification, and exponential time simulation of quantum interactive proof systems,” *Proceedings of the 32nd ACM Symposium on Theory of Computing (STOC 2000)*, (ACM Press, New York, NY, USA 2000), pp. 608–617 [ISBN: 1-58113-184-4].
- [79] Watrous, J. “Limits on the power of quantum statistical zero-knowledge,” *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS’02)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2002) pp. 459–468.
- [80] Kobayashi, H. and K. Matsumoto, “Quantum multi-prover interactive proof systems with limited prior entanglement,” *Journal of Computer and System Sciences* **66**(3), 429–450 (2003).
- [81] Somaroo, S., C.H. Tseng, T. Havel, R. Laflamme, and D.G. Cory, “Quantum simulation of a quantum computer,” *Physical Review Letters* **82**, 5381–5384 (1999).
- [82] Tseng, C.H., S.S. Somaroo, Y.S. Sharf, E. Knill, R. Laflamme, T.F. Havel, and D.G. Cory, “Quantum simulation of a three-body interaction Hamiltonian on an NMR quantum computer,” *Physical Review A* **61**, 12302–12308. (2000).

- [83] Viola, L., E.M. Fortunato, S. Lloyd, C.-H. Tseng, and D.G. Cory, "Stochastic resonance and nonlinear response by NMR spectroscopy," *Physical Review Letters* **84**, 5466–5470 (2000).
- [84] Weinstein, Y., S. Lloyd, J.V. Emerson, and D.G. Cory, "Experimental implementation of the quantum Baker's map," *Physical Review Letters* **89**, 157902 (2002).
- [85] Emerson, J., Y.S. Weinstein, S. Lloyd, and D.G. Cory, "Fidelity decay as an efficient indicator of quantum chaos," *Physical Review Letters* **89**, 284102 (2002).
- [86] Teklemariam, G., E.M. Fortunato, M.A. Pravia, T.F. Havel, and D.G. Cory, "Experimental investigations of decoherence on a quantum information processor," *Chaos, Solitons, and Fractals* **16**, 457–465 (2002).
- [87] Zhang, W. and D.G. Cory, "First direct measurement of the spin diffusion rate in a homogenous solid," *Physical Review Letters* **80**, 1324–1327 (1998).
- [88] Boutis, G.S., D. Greenbaum, H. Cho, D.G. Cory, and C. Ramanathan "Spin diffusion of correlated two-spin states in a dielectric crystal," *Physical Review Letters* **92**, 137201 (2004).
- [89] Vidal, G., J.I. Latorre, E. Rico, and A.Y. Kitaev, "Entanglement in quantum critical phenomena," *Physical Review Letters* **90**, 227902 (2003) [[quant-ph/0211074](#)].
- [90] Knill, E., R. Laflamme, and G.J. Milburn, "Efficient linear optics quantum computation," *Nature* **409**, 46–52 (2001).
- [91] Nielsen, M.A., "Conditions for a class of entanglement transformations," *Physical Review Letters* **83**(2), 436–439 (1999).
- [92] Raussendorf, R. and H.J. Briegel, "A one-way quantum computer," *Physical Review Letters* **86**, 5188 (2001).
- [93] Schack, R. and C.M. Caves, "Classical model for bulk-ensemble NMR quantum computation," (30-Apr-99) preprint [quant-ph/9903101](#).
- [94] Knill E. and R. Laflamme "On the power of one bit of quantum information," *Physical Review Letters* **81**, 5672–5675 (1998).
- [95] Poulin, D., R. Blume-Kohout, R. Laflamme, and H. Ollivier, "Exponential speed-up with a single bit of quantum information: Testing the quantum butterfly effect," (6-Oct-03) preprint [quant-ph/0310038](#).
- [96] Brassard, G., "Quantum communication complexity: A survey," *Foundations of Physics* **33**(11), 1593–1616 (2003) [[quant-ph/0101005](#)].
- [97] Vitanyi, P.M.B., "Quantum Kolmogorov complexity based on classical descriptions," *IEEE Transactions on Information Theory* **47**(6), 2464–2479 (2001).
- [98] Gacs, P. "Quantum algorithmic entropy," *Journal of Physics A: Mathematical and General* **34**(35), 6859–6880 (2001).

- [99] Holevo, A.S., “Problems in the mathematical theory of quantum communication channels,” *Reports on Mathematical Physics* **12**(2), 273–278 (1977).
- [100] Devetak, I. and A. Winter, “Distilling common randomness from bipartite quantum states,” *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2003)*, (IEEE, Piscataway, NJ, 2003), p. 403 [ISBN: 0-7803-7728-1].
- [101] Nielsen, M.A. and I.L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, UK, 2000), Sec. 8.2.
- [102] Shor, P.W., “Equivalence of additivity questions in quantum information theory,” (7-May-03) preprint *quant-ph/0305035*.
- [103] Shor, P.W., “Capacities of quantum channels and how to find them,” *Mathematical Programming* **97**(1-2), 311–335 (2003).
- [104] Bennett, C.H., P.W. Shor, J.A. Smolin, and A.V. Thapliyal, “Entanglement-assisted classical capacity of noisy quantum channels,” *Physical Review Letters* **83** 3081 (1999).
- [105] Bennett, C.H., P.W. Shor, J.A. Smolin, and A.V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem,” *IEEE Transactions on Information Theory* **48**, 2637–2655 (2002) [*quant-ph/0106052*].
- [106] Lo, H.-K., “Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity,” *Physical Review A* **62**, 012313 (2000).
- [107] Bennett, C.H., D.P. DiVincenzo, J.A. Smolin, B.M. Terhal, and W.K. Wootters, “Remote state preparation,” *Physical Review Letters* **87**, 077902 (2001) [*quant-ph/0006044*].
- [108] Hayden, P., R. Jozsa, and A. Winter, “Trading quantum for classical resources in quantum data compression,” *Journal of Mathematical Physics* **43**(9), 4404–4444 (2002).
- [109] Winter, A. and S. Massar, “Compression of quantum measurement operations,” *Physical Review A* **64**, 012311 (2001).
- [110] Einstein, A., B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?” *Physical Review* **47**, 777 (1935).
- [111] Schrodinger, E., “Die gegenwartige Situation der Quantenmechanik,” *Naturw* **23**, 807, 823, 844, (1935).
- [112] Bell, J.S. “On the Einstein-Podolsky-Rosen paradox,” *Physics* **1**, 195–200 (1964).
- [113] Jozsa, R. and N. Linden, “On the role of entanglement in quantum computational speed-up,” *Proceedings of the Royal Society of London Series A - Mathematical Physical and Engineering Sciences* **459**(2036), 2011–2032 (2003) [*quant-ph/020114*].
- [114] Shor, P.W., J.A. Smolin, and B.M. Terhal “Nonadditivity of bipartite distillable entanglement follows from conjecture on bound entangled Werner states,” *Physical Review Letters* **86**, 2681–2684 (2001).

- [115] Horodecki, P., “Separability criterion and inseparable mixed states with positive partial transposition,” *Physics Letters A* **232**(5), 333–339 (1997).
- [116] Vidal, G. and J.I. Cirac, “Irreversibility in asymptotic manipulations of entanglement,” *Physical Review Letters* **86**, 5803–5806 (2001).
- [117] Vedral, V., M.B. Plenio, M.A. Rippin, and P.L. Knight, “Quantifying entanglement,” *Physical Review Letters* **78**, 2275–2279 (1997).
- [118] Vedral, V., “The role of relative entropy in quantum information theory,” *Reviews of Modern Physics* **74**, 197 (2002).
- [119] Bennett, C.H., D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, and W.K. Wootters, “Quantum nonlocality without entanglement,” *Physical Review A* **59**, 1070–1091 (1999) [[quant-ph/9804053](#)].
- [120] Vidal, G., “Entanglement monotones,” *Journal of Modern Optics* **47**, 355 (2000).
- [121] Vidal, G. and R. Tarrach, “Robustness of entanglement,” *Physical Review A* **59**(1), 141–155 (1999).
- [122] Peres, A., “Separability criterion for density matrices,” *Physical Review Letters* **77**, 1413 (1996).
- [123] Horodecki, M., P. Horodecki, and R. Horodecki, “Separability of mixed states: Necessary and sufficient conditions,” *Physics Letters A* **223**, 1 (1996).
- [124] Bennett, C.H., D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, “Unextendible product bases and bound entanglement,” *Physical Review Letters* **82**, 5385 (1999) [[quant-ph/9808030](#)].
- [125] DiVincenzo, D.P., T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, “Unextendible product bases, uncompletable product bases, and bound entanglement,” *Communications in Mathematical Physics* **238**, 379–410 (2003) [[quant-ph/9908070](#)].
- [126] Lewenstein, M., B. Krauss, J.I. Cirac, and P. Horodecki, “Optimization of entanglement witnesses,” *Physical Review A* **62**, 052310 (2000).
- [127] Rains, E.M., “Rigorous treatment of distillable entanglement,” *Physical Review A* **60**, 173 (1999).
- [128] Terhal, B.M., “A family of indecomposable positive linear maps based on entangled quantum states,” *Linear Algebra Applications* **323**, 61–73 (2000) [[quant-ph/9810091](#)].
- [129] Ekert, A.K., C.M. Alves, D.K.L. Oi, M. Horodecki, P. Horodecki, and L.C. Kwek, “Direct estimations of linear and non-linear functionals of a quantum state,” *Physical Review Letters* **88**, 217901 (2002).
- [130] Gottesman, D. and I.L. Chuang, “Demonstrating the viability of universal quantum computation using teleportation and single qubit operations,” *Nature* **402**, 390–393 (1999).

- [131] Wiesner, S., “Conjugate coding,” *SIGACT News* **15**, 78–88, (1983).
- [132] Bennett, C.H., “Quantum cryptography using any two nonorthogonal states,” *Physical Review Letters* **68**, 3121–3124 (1992).
- [133] Ekert, A.K., “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters* **67**, 661–663 (1991).
- [134] Ekert, A.K., J.G. Rarity, P.R. Tapster, and G.M. Palma, “Practical quantum cryptography based on two-photon interferometry,” *Physical Review Letters* **69**, 1293–1295 (1992).
- [135] Huttner, B. and A.K. Ekert, “Information gain in quantum eavesdropping,” *Journal of Modern Optics* **41**, 2455–2466 (1994)
- [136] Deutsch, D., A.K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, “Quantum privacy amplification and the security of quantum cryptography over noisy channels,” *Physical Review Letters* **77**, 2818–2821 (1996) [[quant-ph/9604039](http://arxiv.org/abs/quant-ph/9604039)].
- [137] Mayers, D., “Unconditionally secure quantum bit commitment is impossible,” *Physical Review Letters* **78**, 3414–3417 (1997).
- [138] Shor, P.W. and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Physical Review Letters* **85**, 441–444 (2000).
- [139] Tamaki, K., M. Koashi, and N. Imoto, “Unconditionally secure key distribution based on two nonorthogonal states,” *Physical Review Letters* **90**, 167904 (2003).
- [140] Mayers, D., “Unconditionally secure quantum bit commitment is impossible,” *Physical Review Letters* **78**, 3414–3417 (1997).
- [141] Spekkens, R.W. and T. Rudolph, “Degrees of concealment and bindingness in quantum bit commitment protocols,” *Physical Review A* **65**, 012310 (2002).
- [142] Kitaev, A.Y., “Quantum coin tossing,” MSRI lecture, (available at URL: <http://www.msri.org/publications/In/msri/2002/qip/kitaev/1/>).
- [143] Cleve, R., D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” *Physical Review Letters* **83**, 648–651 (1999).
- [144] DiVincenzo, D.P., D.W. Leung, and B.M. Terhal, “Quantum data hiding,” *IEEE Transactions on Information Theory* **48**, 580–598 (2002) [[quant-ph/0103098](http://arxiv.org/abs/quant-ph/0103098)].
- [145] Eggeling, T. and R.F. Werner, “Hiding classical data in multipartite quantum states,” *Physical Review Letters* **89**, 097905 (2002).
- [146] DiVincenzo, D.P., P. Hayden, and B.M. Terhal, “Hiding quantum data,” *Foundations of Physics* **33**, 11, 1629–1647 (2003) [[quant-ph/0207147](http://arxiv.org/abs/quant-ph/0207147)].
- [147] Buhrman, H., R. Cleve, J. Watrous, and R. de Wolf, “Quantum fingerprinting,” *Physical Review Letters* **87**(16), 167902 (2001) [[quant-ph/0102001](http://arxiv.org/abs/quant-ph/0102001)].

- [148] Crepeau, C., D. Gottesman, and A. Smith, "Secure multi-party quantum computing," *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC 2002)*, (ACM Press, New York, NY, USA, 2001), pp. 643–652 [ISBN: 1-58113-495-9] [*quant-ph/0206138*].
- [149] Barnum, H., C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science (FOCS'02)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2002) pp. 449–458 [*quant-ph/0205128*].
- [150] Ambainis, A., M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels," *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2000) pp. 547–553.
- [151] Mosca, M., A. Tapp, and R. de Wolf, "Private quantum channels and the cost of randomizing quantum information," (22-Mar-00) preprint *quant-ph/0003101*.
- [152] Boykin, P.O. and V. Roychowdhury, "Optimal encryption of quantum bits," *Physical Review A* **67**(4), 042317 (2003).
- [153] Hayden, P., D.W. Leung, P.W. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," (13-Nov-03) preprint *quant-ph/0307104*.
- [154] Leung, D.W., "Quantum Vernam cipher," *Quantum Information and Computation*; **2**(1), 14–34 (2002) [*quant-ph/0012077*].
- [155] Gottesman, D. and I. Chuang, "Quantum digital signatures," (8-May-01) preprint *quant-ph/0105032*.
- [156] Kerenidis, I. and R. de Wolf, "Quantum symmetrically-private information retrieval," (10-Jul-03) preprint *quant-ph/0307076*.
- [157] Cleve, R. and J. Watrous, "Fast parallel circuits for the quantum Fourier transform," *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2000) pp. 526–536.
- [158] Hales, L. and S. Hallgren, "An improved quantum Fourier transform algorithm and applications," *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2000) pp. 515–525.
- [159] DiVincenzo, D.P., D. Bacon, J. Kempe, G. Burkard, and K.B. Whaley, "Universal quantum computation with the exchange interaction," *Nature* **408**, 339–342, 2000.
- [160] Lloyd, S., "A potentially realizable quantum computer," *Science* **261**, 1569–1571 (1993).
- [161] Berman, G.P., G.D. Doolen, D.I. Kamenev, and V.I. Tsifrinovich, "Perturbation theory for quantum computation with a large number of qubits," *Physical Review A* **65**, 012321 (2002).

- [162] Berman, G.P., G.D. Doolen, G.V. Lopez, and V.I. Tsifrinovich, "A quantum full adder for a scalable nuclear spin quantum computer," *Computer Physics Communications* **146**(3), 324–330 (2002).
- [163] Berman, G.P., F. Borgonovi, H.S. Goan, S.A. Gurvitz, and V.I. Tsifrinovich, "Single-spin measurement and decoherence in magnetic-resonance force microscopy," *Physical Review B* **67**, 094425 (2003).
- [164] Zurek, W.H., "Decoherence, einselection, and the quantum origins of the classical," *Reviews of Modern Physics* **75**, 715–775 (2003).
- [165] Blum, K., "*Density Matrix Theory and Applications*," 2nd Ed. (Plenum Press, New York, 1996).
- [166] Bohm, A. and K. Kraus, "*States, Effects and Operations: Fundamental Notions of Quantum Theory*," (Springer-Verlag, Berlin, 1983).
- [167] Preskill, J., Lecture notes for Caltech graduate course "Quantum Computation" Physics 219/Computer Science 219 (available at URL: <http://www.theory.caltech.edu/people/preskill/ph229/#lecture>).
- [168] Shirman, A. and G. Schön, "Dephasing and renormalization in quantum two-level systems," in *Proceedings of NATO ARW Workshop on Quantum Noise in Mesoscopic Physics*, Y.V. Nazarov, Ed., (Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002), [ISBN 1-4020-1239-X, *cond-mat/0210023*].
- [169] Steane, A.M. "Quantum Computing and Error Correction," in *Decoherence and Its Implications in Quantum Computation and Information Transfer*, Goni and Turchi, Eds. (IOS Press, Amsterdam, 2001), pp. 284–298 [*quant-ph/0304016*].
- [170] Freedman, M., A. Kitaev, M.J. Larsen, and Z. Wang, "Topological Quantum Computation", *Bulletin of the American Mathematical Society* **40**, 31 (2003) [*quant-ph/0101025*].
- [171] Viola L. and E. Knill, "Robust dynamical decoupling of quantum systems with bounded controls," *Physical Review Letters* **90**, 037901 (2003).
- [172] Byrd M.S. and D.A. Lidar, "Combined error correction techniques for quantum computing architectures," *Journal of Modern Optics* **50**, 1285–1297 (2003).
- [173] Fedichkin, L., A. Fedorov, and V. Privman, "Measures of decoherence," *Proceedings of the 2003 International Society for Optical Engineering (SPIE) Conference on Quantum Information and Computation*, E. Donkor, A.R. Pirich, and H.E. Brandt, Eds., (SPIE, Bellingham Washington, 2003), Vol. 5105, pp. 243–254 [*cond-mat/0303158*].
- [174] Loss, D. and D.P. Divincenzo, "Exact Born approximation for the spin-boson model," (10-Apr-03) preprint *cond-mat/0304118*.
- [175] Fiete, G.A. and E.J. Heller, "Semiclassical theory of coherence and decoherence," *Physical Review A* **68**, 022112 (2003).

- [176] Simmonds, R.W., K.M. Lang, D.A. Hite, D.P. Pappas, and J.M. Martinis, "Decoherence in Josephson qubits from junction resonances," (18-Feb-04) preprint *cond-mat/0402470*.
- [177] Vion, D., A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, and M.H. Devoret, "Manipulating the quantum state of an electrical circuit," *Science* **296**, 886–889 (2002).
- [178] For example: Chen, P.C., C. Piermarocchi, and L.J. Sham, "Control of exciton dynamics in nanodots for quantum operations," *Physical Review Letters* **87**, 067401 (2001).
- [179] For example: Myrgren E. and K.B. Whaley, "Implementing a quantum algorithm with exchange-coupled quantum dots: A feasibility study," *Quantum Information Processing*, **2**(5), 1 (2003) [*quant-ph/0309051*] or Raimond, J.M., M. Brune, and S. Haroche, "Manipulating quantum entanglement with atoms and photons in a cavity," *Reviews of Modern Physics* **73**, 565–582 (2001).

Appendix A

Glossary

A-1 LIST OF ACRONYMS AND ABBREVIATIONS

ARDA	Advanced Research and Development Activity	NV	nitrogen vacancy
1-D	one dimensional	P	polynomial (time)
2-D	two dimensional	PIR	private-information-retrieval (system)
2-DEG	two-dimensional electron gas	POVM	positive operator value measurement
3-D	three dimensional	PPT	positive under partial transposition
ARO	Army Research Office	PSPACE	problem solvable with polynomial memory
BEC	Bose-Einstein condensate	QC	quantum computation/computing
BQNP	bounded quantum analogue of NP	QCPR	Quantum Computing Program Review
BQP	bounded quantum polynomial	QCRYPT	quantum cryptography
CMOS	complementary metal oxide semiconductor	QD	quantum dot
C-NOT	controlled-NOT (gate)	QED	quantum electrodynamics
CPB	Cooper pair box	QFT	quantum Fourier transform
CV	carbon vacancy	QIP	quantum information processing/processor
CW	continuous wave	QIS	quantum information science
DAC	digital to analog converter	QIST	quantum information science and technology
dc	direct current	QIT	quantum information theory
DFS	decoherence-free subspace	qNOT	quantum-NOT (gate)
EPR	Einstein, Podolsky, Rosen	QSAT	quantum analog of satisfiable problem
ESR	electron-spin resonance	QSPIR	quantum k-server symmetrically private information-retrieval (system)
FET	field-effect transistors	rf	radio frequency
GHZ	Greenberger, Horne, and Zeilinger	RSFQ	rapid single flux quantum
GHz	gigahertz	SAW	surface-acoustic wave
HOM	Hong, Ou, and Mandel	SET	single-electron transistor
HSP	hidden subgroup problem	SET	single-electron tunneling
Hz	hertz	SFQ	single flux quantum
IP	interaction proof	SHB	spectral hole burning
kHz	kilohertz	SPD	single-photon detector
KLM	Knill, Laflamme, and Milburn	SPDC	spontaneous parametric down conversion
LOCC	local operations and classical communication	SPIR	symmetrically private information-retrieval (system)
LOQC	linear-optics quantum computing	SPS	single-photon source
MA	Merlin-Arthur (problems)	SQUID	superconducting quantum interference device
MEMS	micro-electro-mechanical systems	STM	scanning-tunneling microscopy
MHz	megahertz	SZK	statistical zero knowledge
mK	milliKelvin	T	Tesla
MRFM	magnetic resonance force microscope	TEP	Technology Experts Panel
NMR	nuclear magnetic resonance	UV	ultraviolet
NP	nondeterministic polynomial (time)		
NRO	National Reconnaissance Office		
NSA	National Security Agency		

A-2 GLOSSARY OF TERMS

Bell inequalities – A set of constraints that certain measurement results must satisfy if the underlying theory is local and realistic; quantum mechanics predicts results that violate these inequalities, thereby disproving local realism.

Bell measurement – A joint measurement on two quantum systems to determine which of the 4 Bell states they are in; to make a completely unambiguous Bell measurement usually requires a strong nonlinear interaction between the systems.

Bell states – For a quantum state with two subsystems (*i.e.*, two qubits), the 4 orthogonal maximally entangled states (*e.g.*, $|00\rangle + |11\rangle$, $|00\rangle - |11\rangle$, $|01\rangle + |10\rangle$ and $|10\rangle - |10\rangle$).

Bose-Einstein condensate – A state of a tenuous, very low-temperature gas in which all the atoms occupy the same motional quantum state; typically all the atoms are essentially at rest.

Cat state – a simultaneous superposition of two different states, usually macroscopic. (This state is classically forbidden.)

cavity quantum electrodynamics – Individual atoms interacting with the strong electromagnetic field inside a small optical-frequency cavity.

coherent control – control which maintains quantum coherence.

computational basis – a set of quantum basis states upon which a computation is done.

correlation – Cosine of the angle between two states.

decoherence – normal loss of quantum coherence (both inherent and due to interactions with the environment).

discriminating single-photon detector – A photon counter that detects one or more photons with high efficiency and can robustly discriminate between 0, 1, 2, or more photons.

entanglement – The property of two or more quantum systems whose total quantum state cannot be written as a product of the states of the individual systems (*c.f.*, separable state); this property introduces nonlocality into quantum theory, and is believed to be an essential ingredient of quantum information processing.

exchange coupling – Basic physical interaction between the spins of electrons whose wave functions overlap, arising from the Pauli exclusion principle.

fault-tolerant quantum computation – a quantum computation that can proceed accurately in spite of errors.

fidelity – The magnitude of the projection of one state on another.

GHZ (Greenberger, Horne, and Zeilinger) and W states – There are two classes of entangled states for a three-qubit system in the sense that a state in one class cannot be transformed into a state in the other class by local operations and classical communication (LOCC). There are two

orthogonal GHZ states (with the form $|000\rangle \pm |111\rangle$) and six orthogonal W states (with the form $|001\rangle \pm |010\rangle \pm |100\rangle$). The GHZ states are pure states specified by the correlation “all qubits have the same value.” The W states are specified by the correlation “any two qubits are correlated.”

holonomic constraint – a type of constraint on a system of particles, expressible in the form, $f(x_1, x_2, x_3, \dots, x_N, t) = 0$.

HOM interferometer – A quantum interferometer, first implemented by Hong, Ou, and Mandel, in which single photons enter each of the two input ports of a 50:50 beam splitter. The probability for coincidence counts at the two output ports is zero when temporal and spatial mode-matching is perfect. This is the required test of a single photon source intended for linear-optics quantum computing. Also, the HOM interferometer is useful for polarization Bell-state analysis, as required (*e.g.*, in quantum dense coding and teleportation).

linear optics – Any optical device that is described by a Hamiltonian which is at most quadratic in the field amplitudes. Such devices include phase-shift components, mirrors, beam splitters, and polarizers. The class may be extended to include devices that make use of the second-order susceptibility in which one of the fields is classical (*e.g.*, parametric down conversion with a classical pump field). As the Hamiltonian for a linear optical device is, at most, quadratic in the field amplitudes, the resulting Heisenberg equations of motion are linear in the field amplitudes.

logical qubit – A combination of physical qubits that is more robust against a specific set of noise generators.

magnetic microtrap – A configuration of magnetic fields in which atoms can be trapped in the regions of strongest field strength via the interaction of the atomic magnetic-dipole moments with the magnetic field.

optical dipole force – When an atom is exposed to light, the electric field of the light induces an optical-frequency electric-dipole moment in the atom, and then the electric field exerts a DC optical dipole force on the induced dipole.

optical lattice – A pattern of standing light waves created by the interference of intersecting laser beams; neutral atoms can be trapped in the standing-wave pattern by optical dipole forces.

optical microtrap – A configuration of tightly focused light beams; atoms can be trapped by optical dipole forces in the regions of greatest light intensity.

physical qubit – A system that has observables that behave as the Pauli matrices.

quantum dot – A confining structure for electrons, which can be designed to stably hold a small number of electrons.

quantum error correcting code – a set of quantum operations which tests for errors and corrects errors that are found.

quantum jump detection – experimental detection of a discrete change in a quantum state.

quantum logic operation – a quantum operation which performs reversible logic (NOT, C-NOT, etc.).

quantum measurement – an experimental procedure for determining some or all of the parameters that specify a quantum state.

quantum parallelism – utilization of quantum superposition to do many operations simultaneously.

quantum state and quantum process tomography – In quantum state tomography, a number of measurements are made on an ensemble of identically prepared quantum systems. If the Hilbert space is of finite dimension, then a finite number of measurements suffices to allow one to reconstruct the quantum state of the particles. Quantum process tomography uses similar techniques to characterize a quantum process (*e.g.*, a unitary transformation, decoherence, etc.). This means the effect on any possible input state to the process may be predicted.

qubit – an abbreviation for “quantum bit”, the basic computation building block of most quantum computer paradigms. In addition to being able to assume the values “0” and “1”, a qubit can also be put into a quantum superposition of 0 and 1 at the same time (*e.g.*, $|0\rangle + |1\rangle$).

Rabi oscillation – a two-state system driven by an electromagnetic wave whose energy equals the energy difference between the two states. (This driven system oscillates periodically between the two states.)

reversible computation – a computation for which the time-reversed sequence can also be realized; (no dissipation occurs)

Rydberg atom – An atom with one valence electron that has been excited to a high-lying (Rydberg) energy level.

scalability – the capability of achieving the same efficiency, almost independent of the number of qubits.

separable state – The description of two or more quantum systems which are not entangled, so that it is possible to write the total state of the joint system as a product of the quantum state of each individual piece

single-photon source – A transform-limited pulsed optical field with one and only one photon per pulse. The pulses must exhibit first-order coherence (*i.e.*, must exhibit self interference) and must enable two-photon interference (*e.g.*, Hong, Ou, and Mandel interferometer) using a delay line.

spontaneous parametric down conversion – The current method of choice for producing pairs of correlated photons. A high-frequency photon is split into two lower-frequency daughter photons via a nonlinear optical crystal. In addition to being able to directly create polarization-entangled pairs, several groups are pursuing it as a means to realizing a single-photon source.

superoperator – general class of quantum operator corresponding to the dynamics of open quantum systems.

superposition – a linear combination of two or more quantum states

teleportation – a quantum communication protocol, whereby an unknown quantum state can be indirectly transmitted from one party to another; the protocol requires sending four classical bits of information, and that the parties share entanglement

Toffoli gate – operator acting on three two-state qubits. Only when the first two qubits are in the down state, does the Toffoli gate flip the third state.

Appendix B

References

B-1 LIST OF REFERENCES FOR THE QUANTUM COMPUTING ROADMAP

- Aaronson, S., "Quantum lower bound for the collision problem," *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 2002) pp. 635–642 [ISBN: 1-58113-495-9, *quant-ph/0111102*].
- Aassime, A., G. Johansson, G. Wendin, R.J. Schoelkopf, and P. Delsing, "Radio-frequency single-electron transistor as readout device for qubits: Charge sensitivity and backaction," *Physical Review Letters* **86**, 3376–3379 (2001).
- Abe, E., K.M. Itoh, T.D. Ladd, J.R. Goldman, F. Yamaguchi, and Y. Yamamoto, "Solid-state silicon NMR quantum computer," *Journal of Superconductivity: Incorporating Novel Magnetism* **16**, 175–178 (2003).
- Abraham A., *The Principles of Nuclear Magnetism* (Clarendon Press, Oxford, 1961).
- Abrams, D.S. and S. Lloyd, "A Quantum algorithm providing exponential speed increase for finding eigenvalues and eigenvectors," *Physical Review Letters* **83**, 5162–5165 (1999) [*quant-ph/9807070*].
- Aharonov, D. and A. Ta-Shma, "Adiabatic quantum state generation and statistical zero knowledge," (7-Jan-03) preprint *quant-ph/0301023*.
- Aharonov, D. and D. Gottesmann, "Improved threshold for fault-tolerant quantum computation," manuscript, 2002.
- Aharonov, D. and M. Ben-Or, "Fault tolerant quantum computation with constant error," (14-Nov-96) preprint *quant-ph/9611025*.
- Aharonov, D., W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, "On the universality of adiabatic quantum computation," manuscript 2003.
- Altepeter, J.B., D. Branning, E. Jeffrey, T.C. Wei, P.G. Kwiat, R.T. Thew, J.L. O'Brien, M.A. Nielsen, and A.G. White, "Ancilla-assisted quantum process tomography," *Physical Review Letters* **90**, 193601 (2003).
- Altepeter, J.B., P.G. Hadley, S.M. Wendelken, A.J. Berglund, and P.G. Kwiat, "Experimental investigation of a two-qubit decoherence-free subspace," (to appear in *Physical Review Letters* 2004).
- Ambainis, A. "Quantum walk algorithm for element distinctness," (1-Nov-03) preprint *quant-ph/0311001*.
- Ambainis, A., D. Aharonov, J. Kempe, U.V. Vazirani, "Quantum walks on graphs," *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC 2001)*, (ACM Press, New York, NY, USA, 2001), pp. 50–59 [ISBN: 1-58113-349-9].
- Ambainis, A., L.J. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson, "The quantum communication complexity of sampling," *Proceedings of the 39th Annual Symposium on the Foundations of Computer Science (FOCS'98)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1998) pp. 342–351.
- Ambainis, A., M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels," *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2000) pp. 547–553.
- Anglin, J.R. and W. Ketterle, "Bose-Einstein condensation of atomic gases," *Nature* **416**, 211–218 (2002).
- Arora, S., R. Impagliazzo, and U. Vazirani, "The principle of local checkability and relativizing arguments in complexity theory," *Proceedings of the 8th Annual Structure in Complexity Theory Conference*, (IEEE Computer Society Press, 1993) [ISBN 0-8186-4070-7].
- Atature, M., G. Di Giuseppe, M.D. Shaw, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, "Multi-parameter entanglement in femtosecond parametric down-conversion," *Physical Review A* **65**, 023808 (2002).

- Bacon, D., K.R. Brown, and K.B. Whaley, "Coherence-preserving quantum bits," *Physical Review Letters* **87**, 247902 (2001).
- Bacon, D.M., Ph.D. thesis, University of California, Berkeley (2001), Chapter 10.
- Barnum, H., C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science (FOCS'02)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2002) pp.449–458 [*quant-ph/0205128*].
- Barrett, M.D., B. DeMarco, T. Schätz, V. Meyer, D. Leibfried, J. Britton, J. Chiaverini, W.M. Itano, B. Jelenkovic, J.D. Jost, C. Langer, T. Rosenband, and D.J. Wineland, "Sympathetic cooling of $^9\text{Be}^+$ and $^{24}\text{Mg}^+$ for quantum logic," *Physical Review A* **68**, 042302 (2003).
- Bartlett, S.D., B.C. Sanders, S.L. Braunstein, and K. Nemoto, "Efficient classical simulation of continuous variable quantum information processes," *Physical Review Letters* **88**, 097904 (2002).
- Bar-Yossef, Z., T.S. Jayram, and I. Kerenidis. "Exponential separation of quantum and classical one-way communication complexity," (to be presented at the 36th Annual ACM Symposium on Theory of Computing [STOC 2004] Chicago, Illinois, USA, June 13–15, 2004).
- Bell, J.S., "On the Einstein-Podolski-Rosen paradox," *Physics* **1**, 195–200 (1964), reprinted in *Speakable and Unsayable in Quantum Mechanics*, (Cambridge University Press, Cambridge, UK, 1987) pp.14–21
- Bell, J.S., "On the problem of hidden variables in quantum mechanics," *Reviews of Modern Physics* **38**, 447–452 (1966).
- Benioff, P., "Quantum mechanical models of Turing machines that dissipate no energy," *Physical Review Letters* **48**, 1581–1585 (1982).
- Benioff, P., "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *Journal of Statistical Physics* **22**, 563–591 (1980).
- Ben-Kish, A., B. DeMarco, V. Meyer, M. Rowe, J. Britton, W.M. Itano, B.M. Jelenkovic, C. Langer, D. Leibfried, T. Rosenband, and D.J. Wineland, "Experimental demonstration of a technique to generate arbitrary quantum superposition states of a harmonically bound spin-1/2 particle," *Physical Review Letters* **90**, 037902 (2003).
- Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, (IEEE, New York, 1984) pp 175–179.
- Bennett, C.H. and S.J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters* **69**, 2881–2884 (1992).
- Bennett, C.H., "Logical reversibility of computation," *IBM Journal of Research and Development* **17**(6), 525–530 (1973).
- Bennett, C.H., "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters* **68**, 3121–3124 (1992).
- Bennett, C.H., D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, and W.K. Wootters, "Quantum nonlocality without entanglement," *Physical Review A* **59**, 1070–1091 (1999) [*quant-ph/9804053*].
- Bennett, C.H., D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A* **54**, 3824–3851 (1996).
- Bennett, C.H., D.P. DiVincenzo, J.A. Smolin, B.M. Terhal, and W.K. Wootters, "Remote state preparation," *Physical Review Letters* **87**, 077902 (2001) [*quant-ph/0006044*].

- Bennett, C.H., D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, "Unextendible product bases and bound entanglement," *Physical Review Letters* **82**, 5385 (1999) [[quant-ph/9808030](#)]
- Bennett, C.H., E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing* **26**, 1510–1523 (1997).
- Bennett, C.H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **70**, 1895–1899 (1993).
- Bennett, C.H., G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters* **76**, 722–725 (1996).
- Bennett, C.H., H.J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Physical Review A* **53**, 2046–2052 (1996).
- Bennett, C.H., P.W. Shor, J.A. Smolin, and A.V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Physical Review Letters* **83** 3081 (1999).
- Bennett, C.H., P.W. Shor, J.A. Smolin, and A.V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Transactions on Information Theory* **48**, 2637–2655 (2002) [[quant-ph/0106052](#)].
- Berggren, K., D. Nakada, T.P. Orlando, E. Macedo, R. Slattery, and T. Weir, "An integrated superconductive device technology for qubit control," *Proceedings of the International Conference on Experimental Methods in Quantum Computation*, (Rinton Press, 2001).
- Bergquist, J.C., R.G. Hulet, W.M. Itano, and D.J. Wineland, "Observation of quantum jumps in a single atom," *Physical Review Letters* **57**, 1699–1702 (1986).
- Berman, G.P., F. Borgonovi, H.S. Goan, S.A. Gurvitz, and V.I. Tsifrinovich, "Single-spin measurement and decoherence in magnetic-resonance force microscopy," *Physical Review B* **67**, 094425 (2003).
- Berman, G.P., G.D. Doolen, D.I. Kamenev, and V.I. Tsifrinovich, "Perturbation theory for quantum computation with a large number of qubits," *Physical Review A* **65**, 012321 (2002).
- Berman, G.P., G.D. Doolen, G.V. Lopez, and V.I. Tsifrinovich, "A quantum full adder for a scalable nuclear spin quantum computer," *Computer Physics Communications* **146**(3), 324–330 (2002).
- Bernstein, E. and U. Vazirani, "Quantum complexity theory," *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1993) pp. 11–20 [ISBN: 0-89791-591-7].
- Bertet, P., S. Osnaghi, P. Milman, A. Auffeves, P. Maioli, M. Brune, J.M. Raimond, and S. Haroche, "Generating and probing a two-photon Fock state with a single atom in a cavity," *Physical Review Letters* **88**, 143601 (2002).
- Bhattacharya, N., H.B. van Linden van den Heuvell, and R.J.C. Spreeuw, "Implementation of quantum search algorithm using classical Fourier optics," *Physical Review Letters* **88**, 137901 (2002).
- Birkel, G., F.B.J. Buchkremer, R. Dumke, and W. Ertmer, "Atom optics with microfabricated optical elements," *Optics Communications* **191**, 67–81 (2001).
- Blatt, R. and P. Zoller, "Quantum jumps in atomic systems," *European Journal of Physics* **9**, 250–256 (1988).
- Blinov, B.B., D.L. Moehring, L.-M. Duan, and C. Monroe, "Observation of entanglement between a single trapped atom and a single photon," *Nature* **428**, 153–157 (2004).

- Blinov, B.B., L. Deslauriers, P. Lee, M.J. Madsen, R. Miller, and C. Monroe, "Sympathetic cooling of trapped Cd⁺ isotopes," *Physical Review A* **65**, 040304 (2002).
- Blum, K., "*Density Matrix Theory and Applications*," 2nd Ed. (Plenum Press, New York, 1996).
- Bocko, M.F., A.M. Herr, and M.F. Feldman, "Prospects for quantum coherent computation using superconducting electronics," *IEEE Transactions on Applied Superconductivity* **7**, 3638–3641 (1997).
- Bohm, A. and K. Kraus, "*States, Effects and Operations: Fundamental Notions of Quantum Theory*," (Springer-Verlag, Berlin, 1983).
- Bollinger, J.J., W.M. Itano, D.J. Wineland, and D.J. Heinzen, "Optimal frequency measurements with maximally correlated states," *Physical Review A* **54**, R4649–4652 (1996).
- Boschi, D., S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **80**, 1121–1125 (1998).
- Boulant, N., K. Edmonds, J. Yang, M.A. Pravia, and D.G. Cory, "Experimental demonstration of an entanglement swapping operation and improved control in NMR quantum-information processing," *Physical Review A* **68**, 032305 (2003).
- Boulant, N., M.A. Pravia, E.M. Fortunato, T.F. Havel, and D.G. Cory, "Experimental concatenation of quantum error correction with decoupling," *Quantum Information Processing* **1**, 135–144 (2002).
- Boulant, N., T.F. Havel, M.A. Pravia, and D.G. Cory, "Robust method for estimating the Lindblad operators of a dissipative quantum process from measurements of the density operator at multiple time points," *Physical Review A* **67**, 042322 (2003).
- Boutis, G.S., D. Greenbaum, H. Cho, D.G. Cory, and C. Ramanathan "Spin diffusion of correlated two-spin states in a dielectric crystal," *Physical Review Letters* **92**, 137201 (2004).
- Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature* **390**, 575–579 (1997).
- Bouwmeester, D., J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon Greenberger-Horne-Zeilinger entanglement," *Physical Review Letters* **82**, 1345–1349 (1999).
- Boykin, P.O. and V. Roychowdhury, "Optimal encryption of quantum bits," *Physical Review A* **67**(4), 042317 (2003).
- Brassard, G., "Quantum communication complexity: A survey," *Foundations of Physics* **33**(11), 1593–1616 (2003) [*quant-ph/0101005*].
- Braunstein, S.L., C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, "Separability of very noisy mixed states and implications for NMR quantum computing," *Physical Review Letters* **83**, 1054–1057 (1999).
- Brennen, G.K., C.M. Caves, P.S. Jessen, and I.H. Deutsch, "Quantum logic gates in optical lattices," *Physical Review Letters* **82**, 1060–1063 (1999).
- Brennen, G.K., I.H. Deutsch, and C.J. Williams, "Quantum logic for trapped atoms via molecular hyperfine interactions," *Physical Review A* **65**, 022313 (2002).
- Brennen, G.K., I.H. Deutsch, and P.S. Jessen, "Entangling dipole-dipole interactions for quantum logic with neutral atoms," *Physical Review A* **61**, 062309 (2000).

- Briegel, H.J., J.I. Cirac, W. Dür, S.J. van Enk, H.J. Kimble, H. Mabuchi, and P. Zoller, "Physical implementations for quantum communication in quantum networks," *Quantum Computing and Quantum Communications* **1509**, 373–382 (1999).
- Briegel, H.J., T. Calarco, D. Jaksch, J.I. Cirac, and P. Zoller, "Quantum computing with neutral atoms," *Journal of Modern Optics* **47**, 415–451 (2000).
- Briegel, H.J., W. Dür, J.I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters* **81**, 5932–5935 (1998).
- Briegel, H.J., W. Dür, S.J. van Enk, J.I. Cirac, and P. Zoller, "Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel," *Philosophical Transactions of the Royal Society of London Series A-Mathematical, Physical, and Engineering Sciences* **356**, 1841–1851 (1998).
- Brouri, R., A. Beveratos, J.-P. Poizat, and P. Grangier, "Photon antibunching in the fluorescence of individual colored centers," *Optics Letters* **25**, 1294–1296 (2000).
- Buchkremer, F.B.J., R. Dumke, M. Volk, T. Muther, G. Birkl, and W. Ertmer, "Quantum information processing with microfabricated optical elements," *Laser Physics* **12**, 736–741 (2002).
- Buck, J.R. and H.J. Kimble, "Optimal sizes of dielectric microspheres for cavity QED with strong coupling," *Physical Review A* **67**, 033806 (2003).
- Budker, D., D.F. Kimball, S.M. Rochester, and V.V. Yashchuk, "Nonlinear magneto-optics and reduced group velocity of light in atomic vapor with slow ground state relaxation," *Physical Review Letters* **83**, 1767–1770 (1999).
- Buhrman, H., R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation," *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1998) pp. 63–68 [ISBN: 0-89791-962-9].
- Buhrman, H., R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Physical Review Letters* **87**(16), 167902 (2001) [*quant-ph/0102001*].
- Burnett, K., P.S. Julienne, P.D. Leff, E. Tiesinga, and C.J. Williams, "Quantum encounters of the cold kind," *Nature* **416**, 225–232 (2002).
- Byrd M.S. and D.A. Lidar, "Combined error correction techniques for quantum computing architectures," *Journal of Modern Optics* **50**, 1285–1297 (2003).
- Calarco, T., E.A. Hinds, D. Jaksch, J. Schniedmayer, J.I. Cirac, and P. Zoller, "Quantum gates with neutral atoms: controlling collisional interactions in time-dependent traps," *Physical Review A* **61**, 022304 (2000).
- Calderbank, A.R. and P.W. Shor, "Good quantum error-correcting codes exist," *Physical Review A* **54**, 1098–1105 (1996).
- Carelli, P., M.G. Castellano, F. Chiarello, C. Cosmelli, R. Leoni, and G. Torrioli, "SQUID systems for macroscopic quantum coherence and quantum computing," *IEEE Transactions on Applied Superconductivity* **11**, 210–214 (2001).
- Cavity Quantum Electrodynamics*, P. Berman, Ed. (Academic Press, Boston, MA, 1994).
- Cerf, N.J., C. Adami, and P.G. Kwiat, "Optical simulation of quantum logic," *Physical Review A* **57**, R1477–R1480 (1998).
- Chen, P.C., C. Piermarocchi, and L.J. Sham, "Control of exciton dynamics in nanodots for quantum operations," *Physical Review Letters* **87**, 067401 (2001).

- Childs, A.M., I.L. Chuang, and D.W. Leung, "Realization of quantum process tomography in NMR," *Physical Review A* **64**, 012314 (2001).
- Childs, A.M., R.C. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D.A. Spielman, "Exponential algorithmic speedup by a quantum walk," Proceedings of the 35th ACM Symposium on Theory of Computing (STOC 2003), (ACM Press, New York, NY, USA, 2003), pp. 59–68 [ISBN: 1-58113-674-9].
- Chu, S., "Cold atoms and quantum control," *Nature* **416**, 206–210 (2002).
- Chuang, I.L. and M.A. Nielsen, "Prescription for experimental determination of the dynamics of a quantum black box," *Journal of Modern Optics* **44**, 2455–2467 (1997).
- Chuang, I.L., L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd, "Experimental realization of a quantum algorithm," *Nature* **393**, 143–146 (1998).
- Cirac, J.I. and P. Zoller, "A scalable quantum computer with ions in an array of microtraps," *Nature* **404**, 579–581 (2000).
- Cirac, J.I. and P. Zoller, "Quantum computations with cold trapped ions," *Physical Review Letters* **74**, 4091–4094 (1995).
- Cirac, J.I., P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Physical Review Letters* **78**, 3221–3224 (1997).
- Cirac, J.I., S.J. van Enk, P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum communication in a quantum network," *Physica Scripta* **T76**, 223–232 (1998).
- Cleve, R. and J. Watrous, "Fast parallel circuits for the quantum Fourier transform," *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2000) pp. 526–536.
- Cleve, R., D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters* **83**, 648–651 (1999).
- Cory, D.G., A.F. Fahmy and T.F. Havel, "Ensemble quantum computing by NMR spectroscopy," *Proceedings of the National Academy of Science (USA)* **94**, 1634–1639 (1997).
- Cory, D.G., M. Price, W. Maas, E. Knill, R. Laflamme, W.H. Zurek, T.F. Havel, and S.S. Somaroo, "Experimental quantum error correction," *Physical Review Letters* **81**, 2152–2155 (1998).
- Cory, D.G., M.D. Price, and T.F. Havel, "Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing," *Physica D* **120**, 82–101 (1998).
- Cory, D.G., R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemarian, Y.S. Weinstein, and Z.H. Zurek, "NMR based quantum information processing: Achievements and prospects," *Fortschritte der Physik [Progress of Physics]* **48**, 875–907 (2000).
- Crepeau, C., D. Gottesman, and A. Smith, "Secure multi-party quantum computing," *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC 2002)*, (ACM Press, New York, NY, USA, 2001), pp. 643–652 [ISBN: 1-58113-495-9] [*quant-ph/0206138*].
- Cummins, H.K., G. Llewellyn, and J.A. Jones, "Tackling systematic errors in quantum logic gates with composite rotations," *Physical Review A* **67**, 042308 (2003).
- Das, R., T.S. Mahesh, and A. Kumar, "Implementation of conditional phase-shift gate for quantum information processing by NMR, using transition-selective pulses," *Journal of Magnetic Resonance* **159**, 46–54 (2002).

- DeMarco, B., A. Ben-Kish, D. Leibfried, V. Meyer, M. Rowe, B.M. Jelenkovic, W.M. Itano, J. Britton, C. Langer, T. Rosenband, and D.J. Wineland, "Experimental demonstration of a controlled-NOT wave-packet gate," *Physical Review Letters* **89**, 267901 (2002).
- DeMartini, F., A. Mazzei, M. Ricci, G.M. D'Ariano, "Exploiting quantum parallelism of entanglement for a complete experimental quantum characterization of a single qubit device," *Physical Review A* **67**, 062307 (2003).
- Deutsch, D. and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **439**, 553–558 (1992).
- Deutsch, D., "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **400**(1818), 97–117 (1985).
- Deutsch, D., A.K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Physical Review Letters* **77**, 2818–2821 (1996) [[quant-ph/9604039](#)].
- Deutsch, I.H. and P.S. Jessen, "Quantum-state control in optical lattices," *Physical Review A* **57**, 1972–1986 (1998).
- Deutsch, I.H., G.K. Brennen, and P.S. Jessen, "Quantum computing with neutral atoms in an optical lattice," *Fortschritte der Physik [Progress of Physics]* **48**, 925–943 (2000).
- Devetak, I. and A. Winter, "Distilling common randomness from bipartite quantum states," *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2003)*, (IEEE, Piscataway, NJ, 2003), p. 403 [ISBN:0-7803-7728-1].
- DeVoe, R.G., "Elliptical ion traps and trap arrays for quantum computation," *Physical Review A* **58**, 910–914 (1998).
- DiVincenzo, D.P., D. Bacon, J. Kempe, G. Burkard, and K.B. Whaley, "Universal quantum computation with the exchange interaction," *Nature* **408**, 339–342, 2000.
- DiVincenzo, D.P., D.W. Leung, and B.M. Terhal, "Quantum data hiding," *IEEE Transactions on Information Theory* **48**, 580–598 (2002) [[quant-ph/0103098](#)].
- DiVincenzo, D.P., P. Hayden, and B.M. Terhal, "Hiding quantum data," *Foundations of Physics* **33**, 11, 1629–1647 (2003) [[quant-ph/0207147](#)].
- DiVincenzo, D.P., T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, "Unextendible product bases, uncompletable product bases, and bound entanglement," *Communications in Mathematical Physics* **238**, 379–410 (2003) [[quant-ph/9908070](#)].
- Doherty, A.C., A.S. Parkins, S.M. Tan, and D.F. Walls, "Effects of motion in cavity QED," *Journal of Optics B-Quantum and Semiclassical Optics* **1**, 475–482 (1999).
- Dorai, K., Arvind, and A. Kumar, "Implementation of a Deutsch-like quantum algorithm utilizing entanglement at the two-qubit level on an NMR quantum-information processor," *Physical Review A* **63**, 034101 (2001).
- Duan, L.-M., A. Kuzmich, and H.J. Kimble, "Cavity QED and quantum-information processing with "hot" trapped atoms," *Physical Review A* **67**, 032305 (2003).
- Duan, L.-M., B.B. Blinov, D.L. Moehring, and C. Monroe, "Scalable trapped ion quantum computation with a probabilistic ion-photon mapping," (5-Jan-04) preprint [quant-ph/0401020](#).

- Duan, L.-M., J.I. Cirac, P. Zoller, and E.S. Polzik, "Quantum communication between atomic ensembles using coherent light," *Physical Review Letters* **85**, 5643–5646 (2000).
- Dumke, R., M. Volk, T. Muether, F.B.J. Buchkremer, G. Birkl, and W. Ertmer "Micro-optical realization of arrays of selectively addressable dipole traps: A scalable configuration for quantum computation with atomic qubits," *Physical Review Letters* **89**, 097903 (2002).
- Dur, W., G. Vidal, and J.I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Physical Review A* **62**, 062314 (2000).
- Eckert, K., J. Mompart, X.X. Yi, J. Schliemann, D. Bruss, G. Birkl, and M. Lewenstein, "Quantum computing in optical microtraps based on the motional states of neutral atoms," *Physical Review A* **66**, 042317 (2002).
- Eggeling, T. and R.F. Werner, "Hiding classical data in multipartite quantum states," *Physical Review Letters* **89**, 097905 (2002).
- Einstein, A., B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review* **47**, 777 (1935).
- Ekert, A.K., "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663 (1991).
- Ekert, A.K., C.M. Alves, D.K.L. Oi, M. Horodecki, P. Horodecki, and L.C. Kwek, "Direct estimations of linear and non-linear functionals of a quantum state," *Physical Review Letters* **88**, 217901 (2002).
- Ekert, A.K., J.G. Rarity, P.R. Tapster, and G.M. Palma, "Practical quantum cryptography based on two-photon interferometry," *Physical Review Letters* **69**, 1293–1295 (1992).
- Emerson, J., Y.S. Weinstein S. Lloyd, and D.G. Cory, "Fidelity decay as an efficient indicator of quantum chaos," *Physical Review Letters* **89**, 284102 (2002).
- Ernst, R.R., G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1987).
- Eschner, J., Ch. Raab, F. Schmidt-Kaler, and R. Blatt, "Light interference from single atoms and their mirror images," *Nature*, **413**, 495–498 (2001).
- Ettinger, M., P. Hoyer, and E. Knill, "The quantum query complexity of the hidden subgroup problem is polynomial," (12-Jan-04) preprint *quant-ph/0401083*.
- Farhi, E. and S. Gutmann, Quantum mechanical square root speedup in a structured search problem," (18-Nov-97) preprint *quant-ph/9711035*.
- Farhi, E., J. Goldstone, S. Gutman, B. Reichardt, U. Vazirani, "Tunneling in quantum adiabatic optimization," manuscript in preparation 2004.
- Farhi, E., J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," (28-Jan-00) preprint *quant-ph/0001106*.
- Fedichkin, L., A. Fedorov, and V. Privman, "Measures of decoherence," *Proceedings of the 2003 International Society for Optical Engineering (SPIE) Conference on Quantum Information and Computation*, E. Donkor, A.R. Pirich, and H.E. Brandt, Eds., (SPIE, Bellingham Washington, 2003), Vol. 5105, pp. 243–254 [*cond-mat/0303158*].
- Feynman, R.P., "Simulating physics with computers," *International Journal of Theoretical Physics* **21**, 467–488 (1982).
- Fiete, G.A. and E.J. Heller, "Semiclassical theory of coherence and decoherence," *Physical Review A* **68**, 022112 (2003).

- Fischer, T., P. Maunz, P.W.H. Pinkse, T. Puppe, and G. Rempe, "Feedback on the motion of a single atom in an optical cavity," *Physical Review Letters* **88**, 163002 (2002).
- Fisk, P.T.H., M.J. Sellars, M.A. Lawn, C. Coles, A.G. Mann, and D.G. Blair, "Very high Q microwave spectroscopy on trapped $^{171}\text{Yb}^+$ ions: Application as a frequency standard," *IEEE Transactions on Instrumentation and Measurement*, **44**, 113–116 (1995).
- Folman, R., P. Krueger, D. Cassettari, B. Hessmo, T. Maier, and J. Schmiedmayer, "Controlling cold atoms using nanofabricated surfaces: Atom chips," *Physical Review Letters* **84**, 4749–4752 (2000).
- Fortunato, E.M., L. Viola, J. Hodges, G. Teklemariam, and D.G. Cory, "Implementation of universal control on a decoherence-free qubit," *New Journal of Physics* **4**, 5.1–5.20 (2002).
- Fortunato, E.M., M.A. Pravia, N. Boulant, G. Teklemariam, T.F. Havel, and D.G. Cory, "Design of strongly modulating pulses to implement precise effective Hamiltonians for quantum information processing," *Journal of Chemical Physics* **116**, 7599–7606 (2002).
- Freedman, M., A. Kitaev, M.J. Larsen, and Z. Wang, "Topological quantum computation," *Bulletin of the American Mathematical Society* **40**, 31–38 (2003) [[quant-ph/0101025](#)].
- Freedman, M., A. Kitaev, M.J. Larsen, and Z. Wang, "Topological Quantum Computation", *Bulletin of the American Mathematical Society* **40**, 31 (2003) [[quant-ph/0101025](#)].
- Friebel, S., C. D'Andrea, J. Walz, M. Weitz, and T.W. Haensch, "CO₂-laser optical lattice with cold rubidium atoms," *Physical Review A* **57**, R20–R23 (1998).
- Friedman, J.R., V. Patel, W. Chen, S.K. Tolpygo, and J.E. Lukens, "Quantum superposition of distinct macroscopic states," *Nature* **406**, 43–46, (2000).
- Furusawa, A., J. Sorensen, S.L. Braunstein, C. Fuchs, H.J. Kimble, and E.S. Polzik, "Unconditional quantum teleportation," *Science* **282**, 706–709 (1998).
- Gacs, P. "Quantum algorithmic entropy," *Journal of Physics A: Mathematical and General* **34**(35), 6859–6880 (2001).
- Gershenfeld, N. and I.L. Chuang, "Bulk spin-resonance quantum computation," *Science* **275**, 350–356 (1997).
- Gheri, K.M., P. Torma, and P. Zoller, "Quantum state engineering with photonic qubits," *Acta Physica Slovaca* **49**, 523–532 (1999).
- Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–195 (2002).
- Gottesman, D. and I. Chuang, "Quantum digital signatures," (8-May-01) preprint [quant-ph/0105032](#).
- Gottesman, D. and I.L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single qubit operations," *Nature* **402**, 390–393 (1999).
- Gottesman, D., "An introduction to quantum error correction," in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, S. Lomonaco, Jr., Ed., (American Mathematical Society, Providence, Rhode Island, 2002), pp.221–235 [[quant-ph/0004072](#)].
- Gottesman, D., A.Y. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator," *Physical Review A* **64**, 012310 (2001).
- Gottesmann, D., "Stabilizer codes and quantum error correction," Ph.D. thesis, California Institute of Technology (1997) (114 pp. electronic version at [quant-ph/9705052](#)).

- Granata, C., V. Corato, L. Longobardi, M. Russo, B. Ruggiero, and P. Silvestrini, "Josephson device for quantum experiments," *Applied Physics Letters* **80**, 2952–2954 (2002).
- Greiner, M., O. Mandel, T. Esslinger, T.W. Haensch, and I. Bloch, "Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms," *Nature* **415**, 39–44 (2002).
- Greiner, M., O. Mandel, T.W. Haensch, and I. Bloch, "Collapse and revival of the matter wave field of a Bose-Einstein condensate," *Nature* **419**, 51–54 (2002).
- Grigni, M., L. Schulman, M. Vazirani, and U. Vazirani, "Quantum mechanical algorithms for the nonabelian hidden subgroup problem," *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC 2001)*, (ACM Press, New York, NY, USA, 2001), pp. 68–74 [ISBN: 1-58113-349-9].
- Grover, L., "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1999) pp. 212–219 [ISBN: 0-89791-785-5, *quant-ph/9605043*].
- Guest, J.R., T.H. Stievater, G. Chen, E.A. Tabak, B.G. Orr, D.G. Steel, D. Gammon, and D.S. Katzer, "Near-field coherent spectroscopy and microscopy of a quantum dot system," *Science* **293**, 2224–2227 (2001).
- Gulde, S., M. Riebe, G.P.T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I.L. Chuang, R. Blatt, "Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer." *Nature* **421**, 48–50 (2003). (new gate demonstrated as part of this)
- Gupta, J.A., R. Knobel, N. Samarth, and D.D. Awschalom, "Ultrafast manipulation of electron spin coherence," *Science* **292**, 2458–2461 (2001).
- Guthohrlein, G.R., M. Keller, K. Hayasaka, W. Lange, and H. Walther, "A single ion as a nanoscopic probe of an optical field," *Nature* **414**, 49–51 (2001).
- Hagley, E., X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond, and S. Haroche, "Generation of Einstein-Podolsky-Rosen pairs of atoms," *Physical Review Letters* **79**, 1–5 (1997).
- Hales, L. and S. Hallgren, "An improved quantum Fourier transform algorithm and applications," *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2000) pp. 515–525.
- Hallgren, S., "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem," *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 2002) pp. 653–658 [ISBN: 1-58113-495-9].
- Hamann, S.E., D.L. Haycock, G. Klose, P.H. Pax, I.H. Deutsch, and P.S. Jessen, "Resolved-sideband Raman cooling to the ground state of an optical lattice," *Physical Review Letters* **80**, 4149–4152 (1998).
- Han, D.J., S. Wolf, S. Oliver, C. McCormick, M.T. Depue, and D.S. Weiss, "3D Raman sideband cooling of cesium atoms at high density," *Physical Review Letters* **85**, 724–727 (2000).
- Hau, L.V., S.E. Harris, Z. Dutton, and C.H. Behroozi, "Light speed reduction to 17 metres per second in an ultracold atomic gas," *Nature (London)* **397**, 594–598 (1999).
- Havel, T.F., S.S. Somaroo, C.-H. Tseng, and D.G. Cory, "Principles and demonstrations of quantum information processing by NMR spectroscopy," *Applicable Algebra in Engineering, Communication, and Computing* **10**, 339–374 (2000).
- Haycock, D.L., P.M. Alsing, I.H. Deutsch, J. Grondalski, and P.S. Jessen, "Mesoscopic quantum coherence in an optical lattice," *Physical Review Letters* **85**, 3365–3368 (2000).
- Hayden, P., D.W. Leung, P.W. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," (13-Nov-03) preprint *quant-ph/0307104*.

- Hayden, P., R. Jozsa, and A. Winter, "Trading quantum for classical resources in quantum data compression," *Journal of Mathematical Physics* **43**(9), 4404–4444 (2002).
- Hemmer, P.R., A.V. Turukhin, M.S. Shahriar, and J.A. Musser, "Raman excited spin coherence in NV-diamond," *Optics Letters* **26**, 361–363 (2001).
- Hinds, E.A., M.G. Boshier, and I.G. Hughes, "Magnetic waveguide for trapping cold atoms in two dimensions," *Physical Review Letters* **80**, 645–649 (1998).
- Hofmann, H.F. and S. Takeuchi, "Quantum phase gate for photonic qubits using only beam splitters and post-selection," *Physical Review A* **66**, 024308 (2002).
- Hofmann, H.F. and S. Takeuchi, "Realization of quantum operations on photonic qubits by linear optics and post-selection," *Proceedings of The Sixth Quantum Information Technology Symposium* May 27th–28th, Kyoto, Japan (2002); also (13-May-02) preprint *quant-ph/0204045*.
- Holevo, A.S., "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems of Information Transmission* **9**(3), 177–183 (1973).
- Holevo, A.S., "On capacity of a quantum communications channel," *Problems of Information Transmission* **15**(4), 247–253 (1979).
- Holevo, A.S., "Problems in the mathematical theory of quantum communication channels," *Reports on Mathematical Physics* **12**(2), 273–278 (1977).
- Holevo, A.S., "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory* **IT-44**(#1), 269–273 (1998).
- Hong, C.K. and L. Mandel, "Experimental realization of a localized one-photon state," *Physical Review Letters* **56**, 58–60 (1986).
- Hong, C.K., Z.Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Physical Review Letters* **59**, 2044–2046 (1987).
- Hood, C.J., M.S. Chapman, T.W. Lynn, and H.J. Kimble, "Real-time cavity QED with single atoms," *Physical Review Letters* **80**, 4157–4160 (1998).
- Hood, C.J., T.W. Lynn, A.C. Doherty, D.W. Vernooy, J. Ye, and H.J. Kimble, "Single atoms bound in orbit by single photons," *Laser Physics* **11**, 1190–1192 (2001).
- Horodecki, M., P. Horodecki, and R. Horodecki, "Separability of mixed states: Necessary and sufficient conditions," *Physics Letters A* **223**, 1 (1996).
- Horodecki, P., "Separability criterion and inseparable mixed states with positive partial transposition," *Physics Letters A* **232**(5), 333–339 (1997).
- Howell, J.C. and J.A. Yeazell, "Linear optics simulations of the quantum baker's map," *Physical Review A* **61**, 012304 (2000).
- Howell, J.C., J.A. Yeazell, and D. Ventura, "Optically simulating a quantum associative memory," *Physical Review A* **62**, 042303 (2000).
- Huttner, B. and A.K. Ekert, "Information gain in quantum eavesdropping," *Journal of Modern Optics* **41**, 2455–2466 (1994).
- Ilchenko, V.S., P.S. Volikov, V.L. Velichansky, F. Treussart, V. Lefèvre-Seguin, J.-M. Raimond, and S. Haroche, "Strain-tunable high-Q optical microsphere resonator," *Optics Communications* **145**, 86–90 (1998).

- Imamoglu, A., "High efficiency photon counting using stored light," *Physical Review Letters* **89**, 163602 (2002).
- Ip, L., "Solving shift problems and hidden coset problem using the Fourier transform," (7-May-02) preprint *quant-ph/0205034*.
- Jaksch, D., C. Bruder, J.I. Cirac, C.W. Gardiner, and P. Zoller, "Cold bosonic atoms in optical lattices," *Physical Review Letters* **81**, 3108–3111 (1998).
- Jaksch, D., H.-J. Briegel, J.I. Cirac, C.W. Gardiner, and P. Zoller, "Entanglement of atoms via cold controlled collisions," *Physical Review Letters* **82**, 1975–1978 (1999).
- Jaksch, D., J.I. Cirac, P. Zoller, S.L. Rolston, R. Cote, and M.D. Lukin, "Fast quantum gates for neutral atoms," *Physical Review Letters* **85**, 2208–2211 (2000). (Rydberg dipole)
- Jaksch, D., V. Venturi, J.I. Cirac, C.J. Williams, and P. Zoller, "Creation of a molecular condensate by dynamically melting a Mott insulator," *Physical Review Letters* **89**, 040402 (2002).
- James, D.F.V. and P.G. Kwiat, "Atomic vapor-based high efficiency optical detectors with photon number resolution," *Physical Review Letters* **89**, 183601 (2002).
- James, D.F.V., P.G. Kwiat, W.J. Munro, and A.G. White, "Measurement of qubits," *Physical Review A* **64**, 052312 (2001).
- Jessen, P.S. and I.H. Deutsch, "Optical lattices," in *Advances in Atomic, Molecular, and Optical Physics*, Vol. 37, B. Bederson and H. Walther, Eds., (Academic, San Diego, 1996), pp. 95–138.
- Jones, J.A. and M. Mosca, "Approximate quantum counting on an NMR ensemble quantum computer," *Physical Review Letters*, **83**, 1050–1053 (1999).
- Jones, J.A. and M. Mosca, "Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer," *Journal of Chemical Physics* **109**, 1648–1653 (1998).
- Jones, J.A., M. Mosca, and R.H. Hansen, "Implementation of a quantum search algorithm on a quantum computer," *Nature* **393**, 344–346 (1998).
- Jones, J.A., V. Vedral, A. Ekert, and G. Castagnoli, "Geometric quantum computation using nuclear magnetic resonance," *Nature* **403**, 869–871 (2000).
- Jozsa, R. and N. Linden, "On the role of entanglement in quantum computational speed-up," *Proceedings of the Royal Society of London Series A - Mathematical Physical and Engineering Sciences* **459**(2036), 2011–2032 (2003) [*quant-ph/020114*].
- Kane, B.E., "Silicon-based quantum computation," *Progress of Physics* **48**, 1023–1041 (2000).
- Kane, B.E., "A silicon-based nuclear spin quantum computer," *Nature* **393**, 133–137 (1998).
- Kaplan, A., M.F. Andersen, and N. Davidson, "Suppression of inhomogeneous broadening in rf spectroscopy of optically trapped atoms," *Physical Review A* **66**, 045401 (2002).
- Kash, M.M., V.A. Sautenkov, A.S. Zibrov, L. Hollberg, G.R. Welch, M.D. Lukin, Y. Rostovtsev, E.S. Fry, and M.O. Scully, "Ultraslow group velocity and enhanced nonlinear optical effects in a coherently driven hot atomic gas," *Physical Review Letters* **82**, 5229–5232 (1999).
- Kerenidis, I. and R. de Wolf, "Quantum symmetrically-private information retrieval," (10-Jul-03) preprint *quant-ph/0307076*.
- Kielpinski, D., C. Monroe, and D.J. Wineland, "Architecture for a large-scale ion-trap quantum computer," *Nature* **417**, 709–711 (2002).

- Kim, J., O. Benson, H. Kan, and Y. Yamamoto, "A single-photon turnstile device," *Nature* **397**, 500–503 (1999).
- Kim, J., S. Takeuchi, Y. Yamamoto, and H.H. Hogue, "Multiphoton detection using visible light photon counter," *Applied Physics Letters* **74**, 902–904 (1999).
- Kim, Y.-H., S.P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," *Physical Review Letters* **86**, 1370–1373 (2001).
- Kitaev, A., "Quantum measurements and the abelian stabilizer problem," *Proceedings of the Electronic Colloquium on Computational Complexity (ECCC-1996)*, **3(3)**, ECCC Report TR96-003 (1996) [quant-ph/9511026].
- Kitaev, A.Y., "Quantum computations: Algorithms and error correction," *Russian Mathematical Surveys* **52**, 1191–1249 (1997).
- Kitaev, A.Y. and J. Watrous, "Parallelization, amplification, and exponential time simulation of quantum interactive proof systems," *Proceedings of the 32nd ACM Symposium on Theory of Computing (STOC 2000)*, (ACM Press, New York, NY, USA 2000), pp. 608–617 [ISBN: 1-58113-184-4].
- Kitaev, A.Y., "Quantum coin tossing," MSRI lecture, (available at URL: <http://www.msri.org/publications/ln/msri/2002/qip/kitaev/1/>).
- Klose, G., G. Smith, and P.S. Jessen, "Measuring the quantum state of a large angular momentum," *Physical Review Letters* **86**, 4721–4724 (2001).
- Knill E. and R. Laflamme "On the power of one bit of quantum information," *Physical Review Letters* **81**, 5672–5675 (1998).
- Knill, E., "Quantum gates using linear optics and post selection," *Physical Review A* **66**, 052306 (2002).
- Knill, E., I.L. Chuang, and R. Laflamme, "Effective pure states for bulk quantum computation," *Physical Review A*. **57**, 3348–3363 (1998).
- Knill, E., R. Laflamme and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature* **409**, 46–52 (2001).
- Knill, E., R. Laflamme and W.H. Zurek, "Resilient quantum computation: Error models and thresholds," *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **454**, 365–384 (1998).
- Knill, E., R. Laflamme, and G.J. Milburn, "Efficient linear optics quantum computation," *Nature* **409**, 46–52 (2001).
- Knill, E., R. Laflamme, R. Martinez, and C. Negreverne, "Benchmarking quantum computers: The five-qubit error correcting code," *Physical Review Letters* **86**, 5811–5814 (2001).
- Knill, E., R. Laflamme, R. Martinez, and C.-H. Tseng, "An algorithmic benchmark for quantum information processing," *Nature* **404**, 368–370 (2000).
- Kobayashi, H. and K. Matsumoto, "Quantum multi-prover interactive proof systems with limited prior entanglement," *Journal of Computer and System Sciences* **66(3)**, 429–450 (2003).
- Kosaka, H., A.A. Kiselev, F.A. Baron, K.-W. Kim, and E. Yablonovitch, "Electron g-factor engineering in III–IV semiconductors for quantum communication," *Electronics Letters* **37**, 464 (2001).
- Kostoff R.N. and R.R. Schaller, "Science and technology roadmaps," *IEEE Transactions on Engineering Management* **48**, 132–143 (2001).
- Kozhokin, A.E., K. Mølmer, and E. Polzik, "Quantum memory for light," *Physical Review A* **62**, 033809 (2000).

- Kuhn, A., M. Hennrich, and G. Rempe, "Deterministic single-photon source for distributed quantum networking," *Physical Review Letters* **89**, 067901 (2002).
- Kuhn, A., M. Hennrich, T. Bondo, and G. Rempe, "Controlled generation of single photons from a strongly coupled atom-cavity system," *Applied Physics B* **69**, 373–377 (1999).
- Kuhr, S., W. Alt, D. Schrader, I. Dotsenko, Y. Miroshnychenko, W. Rosenfeld, M. Khudaverdyan, V. Gomer, A. Rauschenbeutel, and D. Meschede, "Coherence properties and quantum state transportation in an optical conveyor belt," *Physical Review Letters* **91**, 213002 (2003).
- Kuperberg, A., "Subexponential-time quantum algorithm for the dihedral hidden subgroup problem," (14-Feb-03) preprint *quant-ph/0302112*.
- Kurtsiefer, C., S. Mayer, P. Zarda, and H. Weinfurter, "A stable solid-state source of single photons," *Physical Review Letters* **85**, 290–293 (2000).
- Kwiat, P.G., "Hyper-entangled states," *Journal of Modern Optics* **44**, 2173–2184 (1997).
- Kwiat, P.G., A.J. Berglund, J.B. Altepeter, and A.G. White, "Experimental verification of decoherence-free subspaces," *Science* **290**, 498–501 (2000).
- Kwiat, P.G., A.M. Steinberg, R.Y. Chiao, P. Eberhard and M. Petroff, "High efficiency single-photon detectors," *Physical Review A* **48**, R867–R870 (1993).
- Kwiat, P.G., E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, "Ultrabright source of polarization-entangled photons," *Physical Review A* **60**, R773–R776 (1999).
- Kwiat, P.G., J. Altepeter, J. Barreiro, D. Branning, E.R. Jeffrey, N. Peters, and A.P. van Devender, "Optical technologies for quantum information science," *Proceedings of SPIE International Society of Optical Engineering* **5161**, 87–100 (2004).
- Kwiat, P.G., J.R. Mitchell, P.D.D. Schwindt, and A.G. White, "Grover's search algorithm: An optical approach," *Journal of Modern Optics* **47**, 257–266 (2000).
- Kwiat, P.G., K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y.H. Shih, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letters* **75**, 4337–4341 (1995).
- Laflamme, R., D.G. Cory, C. Negrevergne, and L. Viola, "NMR quantum information processing and entanglement," *Quantum Information and Computation* **2**, 166–176 (2002).
- Laflamme, R., E. Knill, W.H. Zurek, P. Catasti, and S.V.S. Mariappan, "NMR Greenberger-Horne-Zeilinger states," *The Royal Society Philosophical Transactions: Mathematical, Physical, and Engineering Sciences* **356**, 1941–1948 (1998).
- Landauer, R., "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development* **5**(3), 183–191 (1961).
- Lange, W. and H.J. Kimble, "Dynamic generation of maximally entangled photon multiplets by adiabatic passage," *Physical Review A* **61**, 063817 (2000).
- Lapaire, G.G., P. Kok, J.P. Dowling, and J.E. Sipe, *Physical Review A* **68**, 042314 (2003).
- Law, C.K. and H.J. Kimble, "Deterministic generation of a bit-stream of single-photon pulses," *Journal of Modern Optics* **44**, 2067–2074 (1997).
- Leibfried, D., B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W.M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D.J. Wineland, "Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate," *Nature* **422**, 412–415 (2003).

- Leibfried, D., B. DeMarco, V. Meyer, M. Rowe, A. Ben-Kish, J. Britton, W.M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D.J. Wineland, "Trapped-ion quantum simulator: experimental application to nonlinear interferometers," *Physical Review Letters* **89**, 247901 (2002).
- Leibfried, D., D.M. Meekhof, B.E. King, C. Monroe, W.M. Itano, and D.J. Wineland, "Experimental determination of the motional quantum state of a trapped atom," *Physical Review Letters* **77**, 4281–4284 (1996).
- Leibfried, D., D.M. Meekhof, C. Monroe, B.E. King, W.M. Itano, and D.J. Wineland, "Experimental preparation and measurement of quantum states of motion of a trapped atom," *Journal of Modern Optics* **44**, 2485–2505 (1997).
- Leung, D., L.M.K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I.L. Chuang, "Experimental realization of a two-bit phase damping quantum code," *Physical Review A* **60**, 1924–1943 (1999).
- Leung, D.W., "Quantum Vernam cipher," *Quantum Information and Computation*; **2**(1), 14–34 (2002) [quant-ph/0012077].
- Levitt, M.H., "Composite pulses," *Progress in NMR Spectroscopy* **18**, 61–122 (1986).
- Lewenstein, M., B. Krauss, J.I. Cirac, and P. Horodecki, "Optimization of entanglement witnesses," *Physical Review A* **62**, 052310 (2000).
- Lidar D.A., and K.B. Whaley, "Decoherence-free subspaces and subsystems in irreversible quantum dynamics," in *Springer Lecture Notes in Physics*, F. Benatti and R. Floreanini, Eds., (Springer-Verlag, Berlin, 2003) Vol. 622, pp. 83120 [quant-ph/0301032].
- Linden, N., H. Barjat, R. Kopic, and R. Freeman, "How to exchange information between two coupled nuclear spins: the universal SWAP operation," *Chemical Physics Letters* **307**, 198–204 (1999).
- Liu, C., Z. Dutton, C.H. Behroozi and L.V. Hau, "Observation of coherent optical information storage in an atomic medium using halted light pulses," *Nature* **409**, 490–493 (2001).
- Lloyd, S. and S.L. Braunstein, "Quantum computation over continuous variables," *Physical Review Letters* **82**, 1784–1787 (1999).
- Lloyd, S., "A potentially realizable quantum computer," *Science* **261**, 1569–1571 (1993).
- Lloyd, S., M.S. Shahriar, J.H. Shapiro, and P.R. Hemmer, "Long distance, unconditional teleportation of atomic states via complete Bell state measurements," *Physical Review Letters* **87**, 167903 (2001).
- Lo, H.-K. and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science* **283**, 2050–2056 (1999).
- Lo, H.-K., "Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity," *Physical Review A* **62**, 012313 (2000).
- Loss, D. and D.P. Divincenzo, "Exact Born approximation for the spin-boson model," (10-Apr-03) preprint cond-mat/0304118.
- Loss, D. and D.P. DiVincenzo, "Quantum computation with quantum dots," *Physical Review A* **57**, 120–126 (1998).
- Lukin, M.D. and A. Imamoglu, "Nonlinear optics and quantum entanglement of ultraslow single photons," *Physical Review Letters* **84**, 1419–1422 (2000).
- Lukin, M.D. and P.R. Hemmer, "Quantum entanglement via optical control of atom-atom interactions," *Physical Review Letters* **84**, 2818–2821 (2000).

- Lukin, M.D., M. Fleischhauer, R. Cote, L.M. Duan, D. Jaksch, J.I. Cirac, and P. Zoller, "Dipole blockade and quantum information processing in mesoscopic atomic ensembles," *Physical Review Letters* **87**, 037901 (2001).
- Lund, A.P., T.B. Bell, and T.C. Ralph, "Comparison of linear optics quantum-computation control-sign gates with ancilla inefficiency and an improvement to functionality under these conditions," *Physical Review A* **68**, 022313 (2003).
- Mabuchi, H. and A.C. Doherty, "Cavity quantum electrodynamics: Coherence in context," *Science* **298**, 1372–1377 (2002).
- Mabuchi, H., Q.A. Turchette, M.S. Chapman, and H.J. Kimble, "Real-time detection of individual atoms falling through a high-finesse optical cavity," *Optics Letters* **21**, 1393–1395 (1996).
- Madi, Z.L., R. Brüscheweiler, and R.R. Ernst, "One- and two-dimensional ensemble quantum computing in spin Liouville space," *Journal of Chemical Physics* **109**, 10603–10611 (1998).
- Magniez, F., M. Santha, and M. Szegedy, "Quantum algorithm for detecting triangles," manuscript 2003.
- Mahesh, T.S. and A. Kumar, "Ensemble quantum-information processing by NMR: Spatially averaged logical labeling technique for creating pseudopure states," *Physical Review A* **64**, 012307 (2001).
- Maklin, Y., G. Schön, and A. Shnirman, "Quantum-state engineering with Josephson-junction devices," *Reviews of Modern Physics* **73**, 357–400 (2001).
- Mandel, O., M. Greiner, A. Widera, T. Rom, T.W. Haensch, and I. Bloch, "Coherent transport of neutral atoms in spin-dependent optical lattice potentials," *Physical Review Letters* **91**, 010407 (2003).
- Mankins, J.C., "Approaches to strategic research and technology (R&T) analysis and road mapping," *Acta Astronautica* **51**, 3–21 (2002).
- Martinis, J.M., S.-W. Nam, J. Aumentado, and C. Urbina, "Rabi oscillations in a large Josephson-junction qubit," *Physical Review Letters* **89**, 117901 (2002).
- Mayers, D., "Unconditionally secure quantum bit commitment is impossible," *Physical Review Letters* **78**, 3414–3417 (1997).
- Mazzei, A., M. Ricci, F. De Martini, and G.M. D'Ariano, "Pauli tomography: Complete characterization of a single qubit device," *Fortschritte de Physik* **51**, 342 (2003).
- McKeever, J., A. Boca, A.D. Boozer, J.R. Buck, and H.J. Kimble, "Experimental realization of a one-atom laser in the regime of strong coupling," *Nature* **425**, 268–271 (2003).
- McKeever, J., A. Boca, A.D. Boozer, R. Miller, J.R. Buck, A. Kuzmich, and H.J. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity," *Science* **303**, 1992–1994 (2004).
- McKeever, J., A. Boca, A.D. Boozer, R. Miller, J.R. Buck, A. Kuzmich, and H.J. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity" *Science Express Reports* (online 26 February 2004).
- McKeever, J., J.R. Buck, A.D. Boozer, A. Kuzmich, H.-C. Nägerl, D.M. Stamper-Kurn, and H.J. Kimble, "State-insensitive cooling and trapping of single atoms in an optical cavity," *Physical Review Letters* **90**, 133602 (2003).
- Meekhof, D.M., C. Monroe, B. King, W.M. Itano, and D.J. Wineland, "Generation of nonclassical motional states of a trapped atom," *Physical Review Letters* **76**, 1796–1799 (1996); erratum, **77**, 2346 (1996).
- Mehring, M., J. Mende, and W. Scherer, "Entanglement between an electron and a nuclear spin 1/2," *Physical Review Letters* **90**, 153001 (2003).

- Meyer, V., M.A. Rowe, D. Kielpinski, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, "Experimental demonstration of entanglement-enhanced rotation angle estimation using trapped ions," *Physical Review Letters* **86**, 5870–5873 (2001).
- Michler, P., A. Kiraz, C. Becher, W.V. Schoenfeld, P.M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, "A quantum dot single-photon turnstile device," *Science* **290**, 2282–2285 (2000).
- Migdall, A.L., D. Branning, S. Castelletto, and M. Ware, "Tailoring single and multiphoton probabilities of a single photon on-demand," *Physical Review A* **66**, 053805 (2002).
- Milner, V., J.L. Hanssen, W.C. Campbell, and M.G. Raizen, "Optical billiards for atoms," *Physical Review Letters* **86**, 1514–1517 (2001).
- Mitchell, M.W., C.W. Ellenor, S. Schneider, and A.M. Steinberg, "Diagnosis, prescription and prognosis of a Bell-state filter by quantum process tomography," *Physical Review Letters* **91**, 120402 (2003).
- Mohseni, M., J.S. Lundeen, K.J. Resch, A.M. Steinberg, "Experimental application of decoherence-free subspaces in a quantum-computing algorithm" *Physical Review Letters* **91**, 187903 (2003).
- Monroe, C., "Quantum information processing with atoms and photons," *Nature* **416**, 238–246 (2002).
- Monroe, C., D. Leibfried, B.E. King, D.M. Meekhof, W.M. Itano, and D.J. Wineland, "Simplified quantum logic with trapped ions," *Physical Review A* **55**, R2489–2491 (1997).
- Monroe, C., D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, "Demonstration of a fundamental quantum logic gate," *Physical Review Letters* **75**, 4714–4717 (1995).
- Mosca, M., A. Tapp, and R. de Wolf, "Private quantum channels and the cost of randomizing quantum information," (22-Mar-00) preprint *quant-ph/0003101*.
- Mundt, A.B., A. Kreuter, C. Becher, D. Leibfried, J. Eschner, F. Schmidt-Kaler, and R. Blatt, "Coupling a single atomic quantum bit to a high finesse optical cavity," *Physical Review Letters* **89**, 103001 (2002).
- Münstermann, P., T. Fischer, P. Maunz, P.W.H. Pinkse, and G. Rempe, "Observation of cavity-mediated long-range light forces between strongly coupled atoms," *Physical Review Letters* **84**, 4068–4071 (2000).
- Münstermann, P., T. Fischer, P. Maunz, P.W.H. Pinkse, and G. Rempe, "Dynamics of single-atom motion observed in a high-finesse cavity," *Physical Review Letters* **82**, 3791–3794 (1999).
- Münstermann, P., T. Fischer, P.W.H. Pinkse, and G. Rempe, "Single slow atoms from an atomic fountain observed in a high-finesse optical cavity," *Optics Communications* **159**, 63–67 (1999).
- Myrgren E. and K.B. Whaley, "Implementing a quantum algorithm with exchange-coupled quantum dots: A feasibility study," *Quantum Information Processing*, **2**(5), 1 (2003) [*quant-ph/0309051*].
- Nägerl, H.C., D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, "Laser addressing of individual ions in a linear ion trap," *Physical Review A* **60**, 145–148 (1999).
- Nagourney, W., J. Sandberg, and H. Dehmelt, "Shelved optical electron amplifier: Observation of quantum jumps," *Physical Review Letters* **56**, 2797–2799 (1986).
- Nakamura, Y., Y.A. Pashkin, and J.S. Tsai, "Coherent control of macroscopic quantum states in a single-Cooper-pair box," *Nature* **398**, 786–788 (1999).
- Nakamura, Y., Y.A. Pashkin, and J.S. Tsai, "Rabi oscillations in a Josephson-junction charge two-level system," *Physical Review Letters* **87**, 246601 (2001).
- Nelson, R.J., D.G. Cory, and S. Lloyd, "Experimental demonstration of Greenberger-Horne-Zeilinger correlations using nuclear magnetic resonance," *Physical Review A* **61**, 022106 (2000).

- Neuhauser, W., M. Hohenstatt, P.E. Toschek, and H. Dehmelt, "Localized visible Ba^+ mono-ion oscillator," *Physical Review A* **22**, 1137–1140 (1980).
- Nielsen, M.A. and I.L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, UK, 2000), Sec. 8.2.
- Nielsen, M.A., "Conditions for a class of entanglement transformations," *Physical Review Letters* **83**(2), 436–439 (1999).
- Nielsen, M.A., E. Knill, and R. Laflamme, "Complete quantum teleportation using nuclear magnetic resonance," *Nature* **396**, 52–55 (1998).
- O'Brien, J.L., G.J. Pryde, A.G. White, T.C. Ralph, and D. Branning, "Demonstration of an all-optical quantum controlled-NOT gate," *Nature* **426**, 264 (2003).
- Ollerenshaw, J.E., D.A. Lidar, and L.E. Kay, "Magnetic resonance realization of decoherence-free quantum computation," *Physical Review Letters* **91**, 217904 (2003).
- Ou, Z.Y. and L. Mandel, "Violation of Bell's inequality and classical probability in a two-photon correlation experiment," *Physical Review Letters* **61**, 50–53 (1988).
- Pachos, J. and H. Walther, "Quantum computation with trapped ions in an optical cavity," *Physical Review Letters* **89**, 187903 (2002).
- Pan, J.-W., D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Physical Review Letters* **80** 3891–3894 (1998).
- Pan, J.-W., M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, "Experimental demonstration of four-photon entanglement and high-fidelity teleportation," *Physical Review Letters* **86**, 4435–4438 (2001).
- Pazy, E., E. Biolatti, T. Calarco, I. D'Amico, P. Zanardi F. Rossi, and P. Zoller "Spin-based optical quantum gates via Pauli blocking in semiconductor quantum dots," (19-Sep-2001) preprint *cond-mat/0109337*.
- Peil, S., J.V. Porto, B. Laburthe-Tolra, J.M. Obrecht, B.E. King, M. Subbotin, S.I. Rolston, and W.D. Phillips, "Patterned loading of a Bose-Einstein condensate into an optical lattice," *Physical Review A* **67**, 051603(R) (2003).
- Pellizzari, T., "Quantum networking with optical fibers," *Physical Review Letters* **79**, 5242–5245 (1997).
- Pellizzari, T., S.A. Gardiner, J.I. Cirac, and P. Zoller, "Decoherence, continuous observation, and quantum computing: A cavity QED model," *Physical Review Letters* **75**, 3788–3791 (1995).
- Peres, A., "Separability criterion for density matrices," *Physical Review Letters* **77**, 1413 (1996).
- Perrin, H., A. Kuhn, I. Bouchoule, and C. Salomon, "Sideband cooling of neutral atoms in a far-detuned optical lattice," *Europhysics Letters* **42**, 395–400 (1998).
- Phillips, D.F., A. Fleischhauer, A. Mair, R.L. Walsworth, and M.D. Lukin, "Storage of light in atomic vapor," *Physical Review Letters* **86**, 783–786 (2001).
- Piermarocchi, C., P. Chen, L.J. Sham, and D.G. Steel, "Optical RKKY interaction between charged semiconductor quantum dots," *Physical Review Letters* **89**, 167402 (2002).
- Pinkse, P.W.H., T. Fischer, P. Maunz, and G. Rempe, "Trapping an atom with single photons," *Nature* **404**, 365–368 (2000).
- Pittman, T.B. and J.D. Franson, "Cyclical quantum memory for photonic qubits," *Physical Review A* **66**, 062302 (2002).

- Pittman, T.B. and J.D. Franson, "Violation of Bell's inequality with photons from independent sources" *Physical Review Letters* **90**, 240401 (2003).
- Pittman, T.B., B.C. Jacobs and J.D. Franson, "Demonstration of feed forward control for linear optics quantum computation," *Physical Review A* **66**, 052305 (2002).
- Pittman, T.B., B.C. Jacobs and J.D. Franson, "Demonstration of non-deterministic quantum logic operations using linear optical elements," *Physical Review Letters* **88**, 257902 (2002).
- Pittman, T.B., B.C. Jacobs, and J.D. Franson, "Probabilistic quantum logic operations using polarizing beam splitters," *Physical Review A* **64**, 062311 (2001).
- Pittman, T.B., B.C. Jacobs, and J.D. Franson, "Single photons on pseudo-demand from stored parametric down-conversion," *Physical Review A* **66**, 042303 (2002).
- Plenio, M.B. and P.L. Knight, "Decoherence limits to quantum computation using trapped ions," *Proceedings of the Royal Society of London, Series A – Mathematical and Physical Sciences*, **453**, 2017–2041 (1997).
- Poulin, D., R. Blume-Kohout, R. Laflamme, and H. Ollivier, "Exponential speed-up with a single bit of quantum information: Testing the quantum butterfly effect," (6-Oct-03) preprint *quant-ph/0310038*.
- Poyatos, J.F., J.I. Cirac and P. Zoller, "Complete characterization of a quantum process: the two-bit quantum gate," *Physical Review Letters* **78**, 390–393 (1997).
- Pravia, M.A., E.M. Fortunato, Y. Weinstein, M.D. Price, G. Teklemariam, R.J. Nelson, Y. Sharf, S.S. Somaroo, C.-H. Tseng, T.F. Havel, and D.G. Cory, "Observations of quantum dynamics by solution-state NMR spectroscopy," *Concepts in Magnetic Resonance* **11**, 225–238 (1999).
- Pravia, M.A., N. Boulant, J. Emerson, A. Farid, E.M. Fortunato, T.F. Havel, R. Martinez, and D.G. Cory, "Robust control of quantum information," *Journal of Chemical Physics* **119**, 9993–10001 (2003).
- Preskill, J., "Reliable quantum computers," *Proceedings of the Royal Society of London: Series A – Mathematical and Physical Sciences A* **454**, 385–410 (1998).
- Preskill, J., Lecture notes for Caltech graduate course "Quantum Computation" Physics 219/ Computer Science 219 (available at URL: <http://www.theory.caltech.edu/people/preskill/ph229/#lecture>).
- Price, M.D., S.S. Somaroo, C.H. Tseng, J.C. Gore, A.F. Fahmy, T.F. Havel, and D.G. Cory, "Construction and implementation of NMR quantum logic gates for two spin systems," *Journal of Magnetic Resonance* **140**, 371–378 (1999).
- Protsenko, I.E., G. Reymond, N. Schlosser, and P. Grangier, "Operation of a quantum phase gate using neutral atoms in microscopic dipole traps," *Physical Review A* **65**, 052301 (2002).
- Rafac, R.J., B.C. Young, J.A. Beall, W.M. Itano, D.J. Wineland, and J.C. Bergquist, "Sub-dekahertz ultraviolet spectroscopy of $^{199}\text{Hg}^+$," *Physical Review Letters* **85**, 2462–2465 (2000).
- Raimond, J.M., M. Brune, and S. Haroche, "Manipulating quantum entanglement with atoms and photons in a cavity," *Reviews of Modern Physics* **73**, 565–582 (2001).
- Rains, E.M., "Rigorous treatment of distillable entanglement," *Physical Review A* **60**, 173 (1999).
- Raithel, G., W.D. Phillips, and S.L. Rolston, "Collapse and revivals of wave packets in optical lattices," *Physical Review Letters* **81**, 3615–3618 (1998).
- Ralph, T.C., A. Gilchrist, G.J. Milburn, W.J. Munro, and S. Glancy, "Quantum computation with optical coherent states," *Physical Review A* **68**, 042319 (2003).

- Ralph, T.C., A.G. White, and G.J. Milburn “Simple scheme for efficient linear optics quantum gates,” *Physical Review A* **65**, 012314 (2002).
- Ramanathan, C., H. Cho, P. Cappellaro, G.S. Boutis, and D.G. Cory, “Encoding multiple quantum coherences in non-commuting bases,” *Chemical Physics Letters* **369**, 311–317 (2003).
- Rauschenbeutel, A., G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.M. Raimond, and S. Haroche, “Coherent operation of a tunable quantum phase gate in cavity QED,” *Physical Review Letters* **83**, 5166–5169 (1999).
- Rauschenbeutel, A., G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.-M. Raimond, and S. Haroche, “Step-by-step engineered multiparticle entanglement,” *Science* **288**, 2024–2028 (2000).
- Rauschenbeutel, A., P. Bertet, S. Osnaghi, G. Nogues, M. Brune, J.M. Raimond, and S. Haroche, “Controlled entanglement of two field modes in a cavity quantum electrodynamics experiment,” *Physical Review A* **64**, 050301 (2001).
- Raussendorf, R. and H.J. Briegel, “A one-way quantum computer,” *Physical Review Letters* **86**, 5188 (2001).
- Raz, R., “Exponential separation of quantum and classical communication complexity,” *Proceedings of the 31st ACM Symposium on Theory of Computing (STOC 1999)*, (ACM Press, New York, NY, USA, 2001), pp. 358–367.
- Razborov, A.A., “An upper bound on the threshold quantum decoherence rate,” manuscript.
- Recher, P., E.V. Sukhorukov, and D. Loss, “Quantum dot as spin filter and spin memory,” *Physical Review Letters* **85**, 1962–1965 (2000).
- Redman, D.A., S.W. Brown, and S.C. Rand, “Origin of persistent hole burning of N-V centers in diamond,” *Journal of the Optical Society of America B* **9**, 768 (1992).
- Regev, O., “Quantum computation and lattice problems,” *Proceedings of the 43rd Annual Symposium on the Foundations of Computer Science (FOCS’02)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2002), pp. 520–530.
- Reichardt, B., “The quantum adiabatic optimization algorithm and local minima,” (to be presented at the 36th Annual ACM Symposium on Theory of Computing [STOC 2004] Chicago, Illinois, USA, June 13–15, 2004).
- Reichel, J., W. Haenschel, P. Hommelhoff, and T.W. Haensch, “Applications of integrated magnetic microtraps,” *Applied Physics B – Lasers and Optics* **72**, 81–89 (2001).
- Rohde, H., S.T. Gulde, C.F. Roos, P.A. Barton, D. Leibfried, J. Eschner, F. Schmidt-Kaler and R. Blatt, “Sympathetic ground-state cooling and coherent manipulation with two-ion crystals,” *Journal of Optics B: Quantum and Semiclassical Optics* **3**, S34–S41 (2001).
- Rolston, S.L. and W.D. Phillips, “Nonlinear and quantum atom optics,” *Nature* **416**, 219–224 (2002).
- Roos, C.F., G.P.T. Lancaster, M. Riebe, H. Häffner, W. Haenschel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, and R. Blatt, “Tomography of entangled massive particles,” (29-Jul-03) preprint *quant-ph/0307210*.
- Roos, Ch., Th. Eigher, H. Rohde, H.C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt-Kaler, and R. Blatt, “Quantum state engineering on an optical transition and decoherence in a Paul trap,” *Physical Review Letters* **83**, 4713–4716 (1999).
- Rowe, M.A., A. Ben-Kish, B. DeMarco, D. Leibfried, V. Meyer, J. Beall, J. Britton, J. Hughes, W.M. Itano, B. Jelenkovi, C. Langer, T. Rosenband, and D.J. Wineland, “Transport of quantum states and separation of ions in a dual RF ion trap,” (to be published in *Quantum Information and Computation*).

- Rowe, M.A., D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, "Experimental violation of a Bell's inequality with efficient detection," *Nature*, **409**, 791–794 (2001).
- Sackett, C.A., D. Kielpinski, B.E. King, C. Langer, V. Meyer, C.J. Myatt, M. Rowe, Q.A. Turchette, W.M. Itano, D.J. Wineland, and C. Monroe, "Experimental entanglement of four particles," *Nature* **404**, 256–259 (2000).
- Santori, C, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "Triggered single photons from a quantum dot," *Physical Review Letters* **86**, 1502–1505 (2001).
- Santori, C., D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "Indistinguishable photons from a single-photon device," *Nature* **419**, 594–597 (2002).
- Sasaki, M., K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," *Physical Review A* **58**, 146–158 (1998).
- Sauer, J.A., K.M. Fortier, M.S. Chang, C.D. Hamley, and M.S. Chapman, "Cavity QED with optically transported atoms," (4-Sep-03) preprint *quant-ph/0309052*.
- Sauer, J.A., M.D. Barrett, and M.S. Chapman, "Storage ring for neutral atoms," *Physical Review Letters* **87**, 270401 (2001).
- Sauter, Th., W. Neuhauser, R. Blatt, and P.E. Toschek, "Observation of quantum jumps," *Physical Review Letters* **57**, 1696–1698 (1986).
- Schack, R. and C.M. Caves, "Classical model for bulk-ensemble NMR quantum computation," (30-Apr-99) preprint *quant-ph/9903101*.
- Scheunemann, R., F.S. Cataliotti, T.W. Haensch, and M. Weitz, "An optical lattice with single lattice site optical control for quantum engineering," *Journal of Optics B – Quantum and Semiclassical Optics* **2**, 645–650 (2000).
- Scheunemann, R., F.S. Cataliotti, T.W. Haensch, and M. Weitz, "Resolving and addressing atoms in individual sites of a CO₂-laser optical lattice," *Physical Review A* **62**, 051801(R) (2000).
- Schlosser, N., G. Reymond, I. Protsenko, and P. Grangier, "Sub-Poissonian loading of single atoms in a microscopic dipole trap," *Nature* **411**, 1024–1027 (2001).
- Schmidt-Kaler, F., H. Häffner, M. Riebe, S. Gulde, G.P.T. Lancaster, T. Deuschle, C. Becher, C.F. Roos, J. Eschner, and R. Blatt, "Realization of the Cirac-Zoller controlled-NOT quantum gate," *Nature* **422**, 408–411 (2003).
- Schmidt-Kaler, F., H. Häffner, S. Gulde, M. Riebe, G. Lancaster, J. Eschner, C. Becher, and R. Blatt, "Quantized phase shifts and a dispersive universal quantum gate," (29-Jul-03) preprint *quant-ph/0307211*.
- Schrader, D., S. Kuhr, W. Alt, M. Müller, V. Gomer, and D. Meschede, "An optical conveyor belt for single neutral atoms," *Applied Physics B – Lasers and Optics* **73**, 819–824 (2001).
- Schrodinger, E., "Die gegenwertige Situation der Quantenmechanik," *Nature* **23**, 807, 823, 844, (1935).
- Schumacher, B. and M. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A* **56**, 131–138 (1997).
- Schumacher, B., M. Westmoreland, and W.K. Wootters, "Limitation on the amount of accessible information in a quantum channel," *Physical Review Letters* **76**, 3452–3455 (1997).
- Shahriar, M.S., P.R. Hemmer, S. Lloyd, P.S. Bhatia, and A.E. Craig, "Solid-state quantum computing using spectral holes," *Physical Review A* **66**, 032301 (2002).

- Sharf, Y., D.G. Cory, S.S. Somaroo, T.F. Havel, E. Knill, R. Laflamme and W.H. Zurek, "A study of quantum error correction by geometric algebra and liquid-state NMR spectroscopy," *Molecular Physics* **98**, 1347–1363 (2000).
- Sharf, Y., T.F. Havel, and D.G. Cory, "Spatially encoded pseudopure states for NMR quantum-information processing," *Physical Review A* **62**, 052314 (2000).
- Shih, Y.H. and C.O. Alley, "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion," *Physical Review Letters* **61**, 2921–2924 (1988).
- Shimizu, Y., N. Shiokawa, N. Yamamoto, M. Kozuma, T. Kuga, L. Deng, and E.W. Hagley, "Control of light pulse propagation with only a few cold atoms in a high-finesse microcavity," *Physical Review Letters* **89**, 233001 (2002).
- Shirman, A. and G. Schön, "Dephasing and renormalization in quantum two-level systems," in *Proceedings of NATO ARW Workshop on Quantum Noise in Mesoscopic Physics*, Y.V. Nazarov, Ed., (Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002), [ISBN 1-4020-1239-X, cond-mat/0210023].
- Shor, P.W. and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters* **85**, 441–444 (2000).
- Shor, P.W., "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS'94)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) pp. 124–134; [revised version at quant-ph/9508027].
- Shor, P.W., "Capacities of quantum channels and how to find them," *Mathematical Programming* **97**(1-2), 311–335 (2003).
- Shor, P.W., "Equivalence of additivity questions in quantum information theory," (7-May-03) preprint quant-ph/0305035.
- Shor, P.W., "Fault-tolerant quantum computation," *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science (FOCS'96)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1996) pp. 56–67.
- Shor, P.W., "Scheme for reducing decoherence in quantum computer memory," *Physical Review A* **52**, R2493–R2496 (1995).
- Shor, P.W., J.A. Smolin, and B.M. Terhal "Nonadditivity of bipartite distillable entanglement follows from conjecture on bound entangled Werner states," *Physical Review Letters* **86**, 2681–2684 (2001).
- Simmonds, R.W., K.M. Lang, D.A. Hite, D.P. Pappas, and J.M. Martinis, "Decoherence in Josephson qubits from junction resonances," (18-Feb-04) preprint cond-mat/0402470.
- Simon, D., "On the power of quantum computation," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS'94)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) pp. 116–123.
- Slichter C.P., *Principles of Magnetic Resonance* (Springer-Verlag, New York, 1980).
- Somaroo, S., C.H. Tseng, T. Havel, R. Laflamme, and D.G. Cory, "Quantum simulation of a quantum computer," *Physical Review Letters* **82**, 5381–5384 (1999).
- Sørensen, A. and K. Mølmer, "Entanglement and quantum computation with ions in thermal motion," *Physical Review A* **62**, 022311 (2000).
- Sørensen, A. and K. Mølmer, "Spin-spin interaction and spin squeezing in an optical lattice," *Physical Review Letters* **83**, 2274–2277 (1999).

- Spekkens, R.W. and T. Rudolph, "Degrees of concealment and bindingness in quantum bit commitment protocols," *Physical Review A* **65**, 012310 (2002).
- Steane, A.M. "Quantum computing and error correction," in *Decoherence and Its Implications in Quantum Computation and Information Transfer*, Goni and Turchi, Eds. (IOS Press, Amsterdam, 2001), pp. 284–298 [quant-ph/0304016].
- Steane, A.M. and B. Brubert, "Fault-tolerant logical gate networks for CSS codes," (4-Nov-03) preprint quant-ph/0311014.
- Steane, A.M. and D.M. Lucas, "Quantum computation with trapped ions, atoms and light," in *Scalable Quantum Computers*, S.L. Braunstein and H.K. Lo Eds., (Wiley-VCH, Berlin, 2001), pp. 69–88.
- Steane, A.M. and W. van Dam, "Physicists triumph at 'Guess my number'," *Physics Today* **53**(2), 35–39 (2000).
- Steane, A.M., "Error correcting codes in quantum theory," *Physical Review Letters* **77**, 793–797 (1996).
- Steffen, M., W. van Dam, T. Hogg, G. Breyta, and I.L. Chuang, "Article title," *Physical Review Letters* **90**, 067903 (2003).
- Stevens, M.J., A.L. Smirl, R.D.R. Bhat, J.E. Sipe, and H.M. van Driel, "Coherent control of an optically injected ballistic spin-polarized current in bulk GaAs," *Journal of Applied Physics* **91**, 4382–4386 (2002).
- Stoff, M.E., A.J. Vega, and R.W. Vaughan, "Explicit demonstration of spinor character for a spin-1/2 nucleus via NMR interferometry," *Physical Review A* **16**, 1521–1524 (1977).
- Strekalov, D.V., T.B. Pittman, A.V. Sergienko, Y.H. Shih, and P.G. Kwiat, "Post selection-free energy-time entanglement," *Physical Review A* **54**, R1–R4 (1996).
- Suter, D. and K. Lim, "Scalable architecture for spin-based quantum computers with a single type of gate," *Physical Review A* **65**, 052309 (2002).
- Takeuchi, S., "Analysis of errors in linear-optics quantum computation," *Physical Review A* **61**, 052302 (2000).
- Takeuchi, S., "Experimental demonstration of a three-qubit quantum computation algorithm using a single photon and linear optics," *Physical Review A* **62**, 032301 (2000).
- Takeuchi, S., J. Kim, Y. Yamamoto, and H.H. Hogue, "Development of a high-quantum-efficiency single-photon counting system," *Applied Physics Letters* **74**, 1063–1065 (1999).
- Tamaki, K., M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Physical Review Letters* **90**, 167904 (2003).
- Teklemariam, G., E.M. Fortunato, M.A. Pravia, T.F. Havel, and D.G. Cory, "Experimental investigations of decoherence on a quantum information processor," *Chaos, Solitons, and Fractals* **16**, 457–465 (2002).
- Teklemariam, G., E.M. Fortunato, M.A. Pravia, T.F. Havel, and D.G. Cory, "NMR analog of the quantum disentanglement eraser," *Physical Review Letters* **86**, 5845–5849 (2001).
- Teklemariam, G., E.M. Fortunato, M.A. Pravia, Y. Sharf, T.F. Havel, D.G. Cory, A. Bhattaharyya, and J. Hou, "Quantum erasers and probing classifications of entanglement via nuclear magnetic resonance," *Physical Review A* **66**, 012309 (2002).
- Terhal, B.M., "A family of indecomposable positive linear maps based on entangled quantum states," *Linear Algebra Applications* **323**, 61–73 (2000) [quant-ph/9810091].
- Tian, L. and S. Lloyd, "Resonant cancellation of off-resonant effects in a multilevel qubit," *Physical Review A* **62**, 050301 (2000).

Tian, L., L. Levitov, C.H. van der Wal, J.E. Mooij, T.P. Orlando, S. Lloyd, C.J.P.M. Harmans, and J.J. Mazo, "Decoherence of the superconducting persistent current qubit," in *Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics*, I.O. Kulik and R. Ellialoglu, Eds. (Kluwer Academic Publishers, Dordrecht, Netherlands, 2000) Part VII, #28.

Traub, J. and H. Wozniakowski, "Path integration on a quantum computer," *Quantum Information Processing* **1**, 365–388 (2002) [[quant-ph/0109113](#)].

Tseng, C.H., S.S. Somaroo, Y.S. Sharf, E. Knill, R. Laflamme, T.F. Havel, and D.G. Cory, "Quantum simulation of a three-body interaction Hamiltonian on an NMR quantum computer," *Physical Review A* **61**, 12302–12308. (2000).

Turchette, Q.A., C.J. Hood, W. Lange, H. Mabuchi, and H.J. Kimble, "Measurement of Conditional Phase-Shifts for Quantum Logic," *Physical Review Letters* **75**, 4710–4713 (1995).

Turukhin, A.V., V.S. Sudarshanam, M.S. Shahriar, J.A. Musser, B.S. Ham, and P.R. Hemmer, "Observation of ultraslow and stored light pulses in a solid," *Physical Review Letters* **88**, 023602 (2002).

van Dam, W. and G. Seroussi, "Efficient quantum algorithms for estimating Gauss sums," (23-Jul-02) preprint [quant-ph/0207131](#).

van Dam, W. and S. Hallgren, "Efficient quantum algorithms for shifted quadratic character problems," (15-Nov-00) preprint [quant-ph/0011067](#).

van Dam, W. and U. Vazirani, "Limits on quantum adiabatic optimization," 5th Workshop on Quantum Information Processing (QIP 2002), IBM T.J. Watson Research Center, Yorktown Heights, New York, USA, January 14–17, 2002.

van Dam, W., M. Mosca, and U. Vazirani, "How powerful is adiabatic quantum computation?" *Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science (FOCS'01)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2001), pp. 279–287.

van der Wal, C.H., A.C.J. ter Haar, F.K. Wilhelm, R.N. Schouten, C.J.P.M. Harmans, T.P. Orlando, S. Lloyd, and J.E. Mooij, "Quantum superposition of macroscopic persistent-current states," *Science* **290**, 773–777 (2000).

van Enk, S.J., H.J. Kimble, J.I. Cirac, and P. Zoller, "Quantum communication with dark photons," *Physical Review A* **59**, 2659–2664 (1999).

van Enk, S.J., J.I. Cirac, P. Zoller, H.J. Kimble and H. Mabuchi, "Quantum state transfer in a quantum network: a quantum-optical implementation," *Journal of Modern Optics* **44**, 1727–1736 (1997).

van Enk, S.J., J.I. Cirac, and P. Zoller, "Ideal quantum communication over noisy channels: A quantum optical implementation," *Physical Review Letters* **78**, 4293–4296 (1997).

van Enk, S.J., J.I. Cirac, and P. Zoller, "Photonic channels for quantum communication," *Science* **279**, 205–208 (1998).

van Enk, S.J., J.I. Cirac, and P. Zoller, "Purifying two-bit quantum gates and joint measurements in cavity QED," *Physical Review Letters* **79**, 5178–5181 (1997).

Vandersypen, L.M.K., C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "Realization of logically labeled effective pure states for bulk quantum computation," *Physical Review Letters* **83**, 3085–3088 (1999).

Vandersypen, L.M.K., M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature* **414**, 883–887 (2001).

- Varcoe, B.T.H., S.Brattke, M.Weidinger, and H.Walther, "Preparing pure photon number states of the radiation field," *Nature* **403**, 743–746 (2000).
- Vedral, V., "The role of relative entropy in quantum information theory," *Reviews of Modern Physics* **74**, 197 (2002).
- Vedral, V., M.B.Plenio, M.A.Rippin, and P.L.Knight, "Quantifying entanglement," *Physical Review Letters* **78**, 2275–2279 (1997).
- Verevkin, A., J.Zhang, R.Sobolewski, A.Lipatov, O.Okunev, G.Chulkova, A.Korneev, K.Smirnov, G.N.Gol'tsman, and A.Semenov, "Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range," *Applied Physics Letters* **80**, 4687–4689 (2002).
- Vernooy, D.W. and H.J.Kimble, "Well-dressed states for wave-packet dynamics in cavity QED," *Physical Review A* **56**, 4287–4295 (1997).
- Vidal, G. and J.I.Cirac, "Irreversibility in asymptotic manipulations of entanglement," *Physical Review Letters* **86**, 5803–5806 (2001).
- Vidal, G. and R.Tarrach, "Robustness of entanglement," *Physical Review A* **59**(1), 141–155 (1999).
- Vidal, G., "Efficient simulation of one-dimensional quantum many-body systems," (14-Oct-03) preprint *quant-ph/0310089*.
- Vidal, G., "Entanglement monotones," *Journal of Modern Optics* **47**, 355 (2000).
- Vidal, G., J.I.Latorre, E.Rico, and A.Y.Kitaev, "Entanglement in quantum critical phenomena," *Physical Review Letters* **90**, 227902 (2003) [*quant-ph/0211074*].
- Viola L. and E.Knill, "Robust dynamical decoupling of quantum systems with bounded controls," *Physical Review Letters* **90**, 037901 (2003).
- Viola, L., E.M.Fortunato, M.A.Pravia, E.Knill, R.Laflamme, and D.G.Cory, "Experimental realization of noiseless subsystems for quantum information processing," *Science* **293**, 2059–2063 (2001).
- Viola, L., E.M.Fortunato, S.Lloyd, C.-H.Tseng, and D.G.Cory, "Stochastic resonance and nonlinear response by NMR spectroscopy," *Physical Review Letters* **84**, 5466–5470 (2000).
- Viola, L., S.Lloyd, and E.Knill, "Universal control of decoupled quantum systems," *Physical Review Letters* **83**, 4888–4891 (1999).
- Vion, D., A.Aassime, A.Cottet, P.Joyez, H.Pothier, C.Urbina, D.Esteve, and M.H.Devoret, "Manipulating the quantum state of an electrical circuit," *Science* **296**, 886–889 (2002).
- Vion, D., A.Aassime, A.Cottet, P.Joyez, H.Pothier, C.Urbina, D.Esteve, and M.H.Devoret "Manipulating the quantum state of an electrical circuit," *Science* **296**; 886–889 (2002).
- Vitanyi, P.M.B., "Quantum Kolmogorov complexity based on classical descriptions," *IEEE Transactions on Information Theory* **47**(6), 2464–2479 (2001).
- Vrijen, R. and E.Yablonoitch, "A spin-coherent semiconductor photodetector for quantum communication," *Physica E: Low-dimensional Systems and Nanostructure* **10**, 569–575 (2001).
- Vuckovic, J., D.Fattal, C.Santori, G.S.Solomon, and Y.Yamamoto, "Enhanced single-photon emission from a quantum dot in a micropost microcavity," *Applied Physics Letters* **82**, 3596–3598 (2003).
- Vuckovic, J., M.Lonar, H.Mabuchi, and A.Scherer, "Design of photonic crystal microcavities for cavity QED," *Physical Review E* **65**, 016608 (2002).

- Vuletic, V., C. Chin, A.J. Kerman, and S. Chu, "Degenerate Raman sideband cooling of trapped cesium atoms at very high densities," *Physical Review Letters* **81**, 5768–5771 (1998).
- Waks, E., K. Inoue, E. Diamanti, and Y. Yamamoto, "High efficiency photon number detection for quantum information processing," (10-Aug-03) preprint *quant-ph/0308054*.
- Walther, H., "Generation and detection of Fock-states of the radiation field," *Zeitschrift Fur Naturforschung Section A (Journal of Physical Sciences – A)* **56**, 117–123 (2001).
- Walther, H., "Generation of photon number states on demand," *Fortschritte Der Physik (Progress of Physics)* **51**, 521–530 (2003).
- Warren, W.S., "The Usefulness of NMR Quantum Computing," *Science* **277**, 1688–1690 (1997); see also response by N. Gershenfeld & I.L. Chuang, *ibid*, p. 1688.
- Warren, W.S., D.P. Weitekamp, and A. Pines, "Theory of selective excitation of multiple-quantum transitions," *Journal of Chemical Physics* **73**, 2084–2099 (1980).
- Watrous, J. "Limits on the power of quantum statistical zero-knowledge," *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS'02)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2002) pp. 459–468.
- Watrous, J. "Quantum simulations of classical random walks and undirected graph connectivity," *Journal of Computer and System Sciences*, **62**(2), 376–391, (2001) [A preliminary version appeared in *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pp. 180–187, (1999)].
- Watrous, J., "On quantum and classical space-bounded processes with algebraic transition amplitudes," *Proceedings of the 40th Annual Symposium on the Foundations of Computer Science (FOCS'99)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1999) pp. 341–351.
- Weinstein, Y., S. Lloyd, J.V. Emerson, and D.G. Cory, "Experimental implementation of the quantum Baker's map," *Physical Review Letters* **89**, 157902 (2002).
- Weinstein, Y.S., M.A. Pravia, E.M. Fortunato, S. Lloyd, and D.G. Cory, "Implementation of the Quantum Fourier Transform," *Physical Review Letters* **86**, 1889–1891 (2001).
- Weinstein, Y.S., S. Lloyd, J. Emerson, and D.G. Cory, "Experimental implementation of the quantum Baker's map," *Physical Review Letters* **89**, 157902 (2002).
- White, A.G., D.F.V. James, P.H. Eberhard, and P.G. Kwiat, "Non-maximally entangled states: Production, characterization, and utilization," *Physical Review Letters* **83**, 3103–3107 (1999).
- Wiesner, S., "Conjugate coding," *SIGACT News* **15**, 78–88, (1983).
- Wineland, D.J., C. Monroe, W.M. Itano, D. Leibfried, B.E. King, and D.M. Meekhof, "Information issues in coherent quantum-state manipulation of trapped atomic ions," *Journal of Research of the National Institute of Standards and Technology* **103**(3), 259–328 (1998).
- Wineland, D.J., J.C. Bergquist, J.J. Bollinger, R.E. Drullinger, and W.M. Itano, "Quantum computers and atomic clocks," *Proceedings of the 6th Symposium Frequency Standards & Metrology*, P. Gill, Ed., (World Scientific, Singapore, 2002), pp 361–368.
- Wineland, D.J., M. Barrett, J. Britton, J. Chiaverini, B. DeMarco, W.M. Itano, B. Jelenkovic, C. Langer, D. Leibfried, V. Meyer, T. Rosenband, and T. Schätz, "Quantum information processing with trapped ions," *Philosophical Transactions of the Royal Society of London A* **361**, 1349–1361 (2003).
- Winter, A. and S. Massar, "Compression of quantum measurement operations," *Physical Review A* **64**, 012311 (2001).

- Wooters, W.K. and W.H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, 802–803 (1982).
- Yamamoto, T., Y.A. Pashkin, O. Astafiev, Y. Nakamura, and J.S. Tsai, "Demonstration of conditional gate operation using superconducting charge qubits," *Nature* **425**, 941–944 (2003).
- Yannoni, C.S., M.H. Sherwood, D.C. Miller, I.L. Chuang, L.M.K. Vandersypen, and M.G. Kubanic, "Nuclear magnetic resonance quantum computing using liquid crystal solvents," *Applied Physics Letters* **75**, 3563–3565 (1999).
- Ye, J., D.W. Vernooy, and H.J. Kimble, "Trapping of single atoms in cavity QED," *Physical Review Letters* **83**, 4987–4990 (1999).
- Yepez, J., "Lattice-gas quantum computation," *International Journal of Modern Physics C* **9**, 1587–1596 (1998);
- Yepez, J., "Quantum computation of fluid dynamics," Quantum Computing and Quantum Communications, First NASA International Conference (QCQC'98), Palm Springs, California, USA, February 17–20, 1998, published in *Lecture Notes in Computer Science* **1509**, 34–60 (1999)
- Yi, X.X., X.H. Su, and L. You, "Conditional quantum phase gate between two 3-state atoms," *Physical Review Letters* **90**, 097902 (2003).
- You, L. and M.S. Chapman, "Quantum entanglement using trapped atomic spins," *Physical Review A* **62**, 152302 (2000).
- You, L., "Motional effects of trapped atomic or ionic qubits," *Physical Review A* **64**, 012302 (2001).
- You, L., X.X. Yi, and X.H. Su, "Quantum logic between atoms inside a high-Q optical cavity," *Physical Review A* **67**, 032308 (2003).
- Yu, Y., S. Han, X. Chu, S.-I. Chu, and Z. Wang, "Coherent temporal oscillations of macroscopic quantum states in a Josephson junction," *Science* **296**, 889–892 (2002).
- Yuan, Z., B.E. Kardynal, R.M. Stevenson, A.J. Shields, C.J. Lobo, K. Cooper, N.S. Beattie, D.A. Ritchie, and M. Pepper, "Electrically driven single-photon source," *Science* **295**, 102–105 (2002).
- Zhang, W. and D.G. Cory, "First direct measurement of the spin diffusion rate in a homogenous solid," *Physical Review Letters* **80**, 1324–1327 (1998).
- Zhu, X.W., X.M. Fang, M. Feng, F. Du, K.L. Gao, and X. Mao, "Experimental realization of a highly structured search algorithm," *Physica D* **156**, 179–185 (2001).
- Zurek, W.H., "Decoherence, einselection, and the quantum origins of the classical," *Reviews of Modern Physics* **75**, 715–775 (2003).

