LA-UR-04-1777

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 to 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

This document is available electronically at: http://qist.lanl.gov

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.

Table of Contents

List of Acronyms and Abbreviations

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

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 isomporphism 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 algoritms.

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 □, arbitrarily long quantum computations can be faithfully carried out. Currently the best schemes for fault-tolerant QC give a value of □ between 10^{-3} and 10^{-4} [9,10]. On the other hand, the only limit we know on □ 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 □ 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 = 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 □ = 10^{-6}, arbitrarily long quantum computations may be carried out. The error model here is that each each gate is subject to decoherence independently with probability □. 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 = 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 = 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 incomparible 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 multibody 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 μm. 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 multibody 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. Pulin *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 $\square_i$ perfectly. This kind of channel is now known as a "cq" channel [100], in which a classical instruction, *i*, indicates that the quantum state $\square_i$ 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 = 1. For N = 1 the optimization is quite easy, and an explicit form (the Holevo □ 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, □, 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" □ 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 ρs 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 Tr (W ρ) 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 QCRYPT, 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" QCRYPT 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 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≥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 know 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 $t < n/4$ 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 ofdissipative 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 Unspeakable 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] Wooters, 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. Crepeau, 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*].

[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/ln/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*].

[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*].

[147] Buhrman, H., R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Physical Review Letters* **87**(16), 167902 (2001) [*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*, Gonis 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).