Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Section 6.5: Continuous Variables

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

July 19, 2004
Version 1.0

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

Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: J.G.Rarity (contributions from P.Grangier, N.Cerf, J.Preskill, C.A.Fuchs)

Editing and compositing: Todd Heinrichs

Table of Contents

List of Tables and Figures

List of Acronyms and Abbreviations

QCrypt quantum cryptography

QIS quantum information science

QKD quantum key distribution

TEP Technology Experts Panel

6.5 Continuous-Variable Approaches to QKD

Table 6.5-1.
Groups Pursuing Continuous-Variable Approaches to QKD

Research Leader(s)	Research Location	Research Focus
P. Grangier	Paris	Experiment
G. Leuchs	Erlangen	Experiment
E. Giacobino	Paris	Experiment
N. Cerf	Brussels	Theory
P. Kumar	Northwestern	
J. Preskill	Caltech	theory

1. Brief description and background for continuous-variable approaches to QKD

In these schemes, the key is encoded in small deviations of the phase, amplitude, or polarization of a bright optical pulse. The encoding can be binary or even continuous, in which case the binary key is produced by subsequent classical data processing. Various schemes have been proposed exploiting

- coherent states [1,2],
- squeezed states [3,4,5,6,7,8,9],
- EPR correlated beams [10,11],or
- other modes [12].

In realizations [1,2], Gaussian distributed information is encoded onto two bases with variance comparable with the shot noise limit. The bases could be one of two quadratures or two polarization bases. The detection apparatus randomly chooses a coding basis in which to measure via homodyne detection. Binary data is extracted from the essentially analogue measurements using a protocol such as the bit-slice reconciliation method [13]. Direct reconciliation [1,2,14] of the data at the receiver with the sent data can be done by sending classical side-information from the transmitter to the receiver to help establish a key. Reverse reconciliation [2,15] involves sending data from the receiver to the transmitter. This allows the transmitter to reduce its key length to match that extracted from the noisy data at the receiver. This latter technique allows coherent states to be used to distribute a key over a quantum channel with arbitrary losses. The security may not be guaranteed against an eavesdropper with ultimate technology, though this point is presently under active scrutiny (see below). Unconditional security proofs already exist for squeezed state versions of the protocol if the squeezing parameter exceeds some threshold [6]. Finally, an alternative possibility for distributing a key over a lossy channel (losses > 3 dB) is to apply a post-selection procedure [9].

Other techniques claim to securely encrypt data using coherent states [12] and a symmetric key. Bitwise encoding uses a basis angle (on a great circle of the Poincare sphere) set by an expanded key. Zero and one bit values are displaced small angles from this basis. This means without the key and thus basis the states cannot be unambiguously discriminated. With M bases the technique uses log (M) key bits to encode each bit (not as good as the one time pad). A key expansion algorithm is thus used to generate the bases. However an apparently efficient attack against this protocol has been proposed very recently [16]

2. Attributes for continuous variable Approaches to QKD

Note: The potential for the attributes for this approach are indicated with the following symbols: "low" (**L**), "medium" (**M**), "high" (**H**), or "no activity" (n/a).

1. Relative theoretical security status: **L**

   As yet, security of coherent-state version has been proven against the restricted class of "individual Gaussian attacks", while security against more general attacks (non-Gaussian collective attacks) is the subject of active research. Unconditional security can be considered to be already proven for some properly designed squeezed-states protocols [6].

2. Relative transmission distance potential: **L**
3. Relative speed potential: **H**

   This is a potentially high-bit-rate technique as the number of bits per pulse can be high, and because the homodyne detection technique only uses standard PIN photodiodes, which are much faster than the avalanche photodiodes (APD) used in photon-counting QKD schemes.

4. Relative maturity: **L**

   This is an emerging field. First laboratory demonstrations have just been performed. As yet, the protocols for extracting the key bits have not been fully optimized.

5. Relative robustness: **L**

   Uses off the shelf components and thus easily constructed.

3. Development Status Metrics

Experimental demonstration of coherent state protocol performed by IOTA (Orsay) and ULB (Brussels) published in 2003 [2]. Laboratory experiments on squeezed state and EPR protocols performed in the Erlangen group [9,11].

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

 = sufficient demonstration

 = preliminary status achieved, but further work is required

 = no experimental demonstration

1. Laboratory or local-area distances (<200 m) implementation environment
   - 1.1 Quantum physics implementation maturity 
   - 1.2 Classical protocol implementation maturity 
   - 1.3 Maturity of components and operational reliability 
   - 1.4 Practical security 
   - 1.5 Key transfer readiness 
   - 1.6 Network readiness 
   - 1.7 Encryptor readiness 

2. Campus distances (<2 km) implementation environment
   - 2.1 Quantum physics implementation maturity 
   - 2.2 Classical protocol implementation maturity 
   - 2.3 Maturity of components and operational reliability 
   - 2.4 Practical security 
   - 2.5 Key transfer readiness 
   - 2.6 Network readiness 
   - 2.7 Encryptor readiness 

3. Metro-area distances (<70 km) implementation environment
   - 3.1 Quantum physics implementation maturity 
   - 3.2 Classical protocol implementation maturity 
   - 3.3 Maturity of components and operational reliability 
   - 3.4 Practical security 
   - 3.5 Key transfer readiness 
   - 3.6 Network readiness 
   - 3.7 Encryptor readiness 

4. Long distances (>70 km) implementation environment
   - 4.1 Quantum physics implementation maturity 
   - 4.2 Classical protocol implementation maturity 
   - 4.3 Maturity of components and operational reliability 
   - 4.4 Practical security 
   - 4.5 Key transfer readiness 
   - 4.6 Network readiness 
   - 4.7 Encryptor readiness 

4. Special strengths

Off-the-shelf components developed for conventional fiber communications can be used. Multiple bits per pulse and simplified detection scheme could lead to high secret bit rates.

5. Unknowns/weaknesses

Security questions when lossy transmission systems are used.

6. Five-year goals

- Multikilometer demonstrations over installed fiber.

7. Ten-year goals

- Full systems capable of 100 km available "off the shelf".

8. Necessary achievements to make five- and ten-year goals possible

Full security proofs for coherent state systems. Improved bit slice and reconciliation protocols to allow extension well beyond 3 dB losses.

9. Developments in other areas that would be useful (connections to other technologies)

For fiber implementations the development of fiber optimized for wavelengths which are currently "easily" generated.

10. How will developments in this approach benefit other areas & follow-on potential

Better photon sources (high efficiency, more wavelength options, and narrow linewidths) will help a variety of optically based quantum information applications such as linear optical quantum computing gates, quantum teleportations, etc.

11. Role of theory/security-proof status for continuous-variable QKD

As yet, unconditional security proofs have been given for squeezed-state protocols. However published security proofs for coherent-state implementations are limited to individual Gaussian attacks. Theoretical work is in progress to extend these proofs to more general attacks but it still needs to be accepted by the community.

References

[1] Grosshans, F. and Ph. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters* **88**, 057902 (2002).

[2] Grosshans, F., G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and Ph. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature* **421**, 238–241 (2003).

[3] Hillery, M., "Quantum cryptography with squeezed states," *Physical Review A* **61**, 022309 (2000).

[4] Ralph, T.C., "Continuous variable quantum cryptography," *Physical Review A* **61**, 010303(R) (2000).

[5] Ralph, T.C., "Security of continuous-variable quantum cryptography," *Physical Review A* **62**, 062306 (2000).

[6] Gottesman, D. and J. Preskill, "Secure quantum key distribution using squeezed states," *Physical Review A* **63**, 022309 (2001).

[7] Cerf, N.J., M. Lévy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A* **63**, 052311 (2001).

[8] Bencheikh, K., Th. Symul, A. Jankovic, and J.A. Levenson, "Quantum key distribution with continuous variables," *Journal of Modern Optics* **48**, 1903–1920 (2001).

[9] Silberhorn, Ch., T.C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography beating the 3 dB loss limit," *Physical Review Letters* **89**, 167901 (2002).

[10] Reid, M.D., "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," *Physical Review A* **62**, 062308 (2000).

[11] Silberhorn, Ch., N. Korolkova, G. Leuchs, "Quantum key distribution with bright entangled beams," *Physical Review Letters* **88**, 167902 (2002).

[12] Barbosa, G.A., E. Corndorf, P. Kumar, and H.P. Yuen, "Secure communication using mesoscopic coherent states," *Physical Review Letters* **90**, 227901 (2003).

[13] Van Assche, G., J. Cardinal, N.J. Cerf, "Reconciliation of a quantum distributed Gaussian key," (to appear in *IEEE Transactions on Information Theory*), [e-print cs.CR/0107030 (24-Dec-02)].

[14] Cerf, N.J., S. Iblisdir, and G. Van Assche, "Cloning and cryptography with quantum continuous variables," *European Physical Journal D* **18**, 211–218 (2002).

[15] Grosshans, F. and Ph. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," *Proceedings of the 6th International Conference on Quantum Communications, Measurement, and Computing (QCMC'02)*, J.H. Shapiro and O. Hirota, Eds. (Rinton Press, Paramus, New Jersey, USA, 2003), [ISBN: 1-58949-030-4, *quant-ph/0204127*].

[16] Lo, H.-K., "Some attacks on quantum-based cryptographic protocols," preprint *quant-ph/0309127* (20-Sep-03).