Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Section 6.4: Entangled Photon Pairs

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

ARDA

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

Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Paul Kwiat and John Rarity

Editing and compositing: Todd Heinrichs

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

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

Table of Contents

List of Tables, Figures, and Equations

List of Acronyms and Abbreviations

BER	bit error rate
QCrypt	quantum cryptography
QIS	quantum information science
QKD	quantum key distribution
TEP	Technology Experts Panel

6.4 Entangled Photon Pair Approaches to QKD

Table 6.4-1.
Groups Pursuing Entangled-Photon Implementations of QKD

Research Leader(s)	Research Location	Research Focus
Gisin, N.	Univ. Geneva	Experiment
Karlsson, A.	KTH Stockholm	Experiment
Kwiat, P.	Univ. Illinois, Urbana-Champaign	Experiment
Rarity, J.	Univ. Bristol	Experiment
Sergienko, A.	Boston Univ	Experiment
Weinfurter, H.	MPQ/LMU Munich	Experiment
Zeilinger, A.	Univ. Vienna	Experiment

1. Brief Description and Background for entangled-photon approaches to QKD

Entanglement is the nonlocal quantum-mechanical correlation that can exist between two quantum systems that have interacted at some point. It is now well established that pairs of photons can be produced in various sorts of entangled states, including polarization entangled [1], time-frequency entangled [2], and momentum entangled [3]. The strong correlation implied in the entangled state can be used to exchange keys [4]. A schematic of the method is shown in Figure 6.4-1 below.

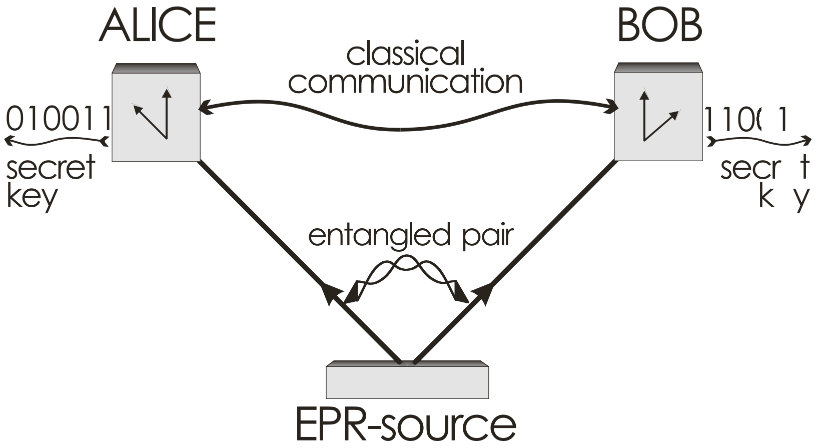

Figure 6.4-1. Schematic entangled-pair key-exchange system. Alice and Bob measure the arriving photons in one of two nonorthogonal bases (e.g., horizontal-vertical and diagonal polarization). Keeping only those coincident detections measured in the same basis they are able to establish identical keys, after the usual classical error-correction and privacy-amplification procedures are applied.

A source of entangled-photon pairs is configured to send one photon to Alice and one photon to Bob.[†] Alice and Bob's detectors are both configured to measure randomly in one of two measurement bases. Alice and Bob then record the bit value, measurement basis, and exact time for each detection. Arrival times are used to establish coincident detections. Due to entanglement, when measurement bases coincide, the bits are near 100% correlated and can be used to form a secret key. Eavesdropping will cause errors as the entangled state will be measured in one basis and the ensuing state collapse leads to imperfect correlations in the other basis.

2. Attributes for entangled-photon 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: **H**

   The security of systems that rely on entanglement has been discussed in References [4,5,6]. Although it was originally believed that there were no actual benefit to using entangled states [7], it is now realized that there are some key advantages over the faint pulse systems:

   (a) There is no encoding of a random number to form the basis of the key, as the randomness comes from the entangled state, e.g.,

   $$|\psi\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right) \qquad \text{(Equation 6.4-1)}$$

   which is in a superposition of two possible 100% correlated states ($|1\rangle = |V\rangle$, $|0\rangle = |H\rangle$ in a polarization system).

   (b) The entanglement allows for "automatic source checking" [8]. In systems in which the various qubit states are produced by several different lasers (or even single-photon generators), information about the state of the qubit can be leaked to other degrees of freedom (thus allowing an eavesdropper to detect the qubit state without inducing any errors). This is prevented if entangled photons are used—any leakage of information to other degrees of freedom of the photon automatically shows up as an increased bit error rate (BER). (Note: leakage of information via some classical means, e.g., detector afterpulsing [9], is *not* eliminated using entanglement.) The security of the key exchange is also not compromised even if the source itself is in the hands of an eavesdropper.

[†] In fact, depending on the relative placement and control of the source, there are two distinct, but related modes of operation. In the asymmetric mode (also sometimes referred to as the "entanglement-assisted" protocol, Alice (acting as the primary sender) essentially owns the source. She immediately detects one photon and sends the other to Bob. In this scenario, the photon traveling to Bob is in a definite (but random) state of polarization. In the balanced, or symmetric, scenario the source is between Alice and Bob, and in general not necessarily controlled by either one. Nevertheless, because the quantum correlations (or lack thereof) will necessarily reveal any source imperfections, the security and quality of the source is readily verifiable by Alice and Bob. The balanced scenario might apply, for instance, when Alice and Bob are both located at ground stations and the source is located on a satellite. In principle, there is no difference between the symmetric and asymmetric models. One is always free to label the source as belonging to Alice or Bob or both or neither.

In practice, the asymmetric scheme is probably slightly easier to maintain, as quantum and classical communications need only be synchronized between two independent parties (Alice and Bob) and not three (Alice, Bob, and Source).

(c) It is, in principle, possible to store the photons in some "quantum memory" until the key is required. *The key does not exist until the photons are measured.* As a corollary, this means that one can, in principle, generate a key even when no quantum channel is available (as long as it was previously available and the quantum bits can be stored). Also, as long as no eavesdropper was present at the time of entanglement distribution, the protocol is secure, even if the measurements are not made—and the secret key not created—until some later time when there *is* an eavesdropper.

2. Relative transmission distance potential: **H**

   The maximum range to date is tens of kilometers in fiber; in free space, only table-top demonstrations have been carried out, though very recently entangled photons were distributed (without key exchange) over ~1 km in free space [10]. In principle the range of secure communication is high because the background-induced coincidence rate (leading to errors) can be extremely low [11]. Lumped loss tolerance up to 50 dB is expected, based on a 1 ns gate and 1000 counts•sec^{-1} (this implies a background rate of only 1 millicoincidence•sec^{-1}; however, detector noise will increase this.) The availability of "quantum repeaters" would also increase the usable distance [12].

3. Relative speed potential: **M**

   Pair-photon generation rates limit systems at the moment. Highest rates are 4×10^5 to 1.3×10^6 coincidences per second [13,14] measured in the laboratory, significantly lower in fibers.

4. Relative maturity: **M**

   Medium maturity as proof-of-principle experiments have been done [15,16,17] but full development is still to come.

5. Relative robustness: **M**

   As with all point-to-point schemes, availability is immediately compromised by any form of eavesdropping. Note, however, that if entangled quantum bits have been previously distributed and stored, a key can be generated at a time even when no transmission of single photons is possible. As long as there was no eavesdropper present at the time of entanglement distribution, the protocol is secure, even if the measurements are not made—and the secret key not created—until some later time when there *is* an eavesdropper.

3. Development-status metrics

Fiber-based experiments have demonstrated key exchange using interferometry [15] and polarization[†] [16] (however, it is unlikely that long fiber systems using polarization encoding will be used in practical systems, due to random polarization transformations induced by the fiber). Free-space table-top experiments have demonstrated Ekert protocol and six-state protocol [17].

[†] While it is unlikely that long fiber systems using polarization encoding will be used in practical systems, due to random polarization transformations induced by the fiber, it actually might not be overly difficult to actively compensate for the unwanted transformations; using polarization could then obviate the need for stabilized fiber interferometers; in any event, it seems that some form of active stabilization is needed.

Free-space experiments to 1 km have recently been performed [10] (but still without key exchange).

Preliminary experiments on quantum repeaters and entanglement swapping have been reported [18], though the bit rates are still very low (typically << 1 per second), and the resulting final entangled states are not of exceedingly high quality (maximum fidelity ~ 93%, corresponding to BERs of 7%). Preliminary experiment on quantum memory has been reported, but with storage times of less than 100 ns [19]; preliminary storage of nonentangled photons indicates 1–10 µs should be achievable [20].

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

The security advantages in Section 2 are the special strengths: the key does not exist until after the detection process (so that it could be generated long after the quantum channel is available to distribute the entanglement—if long-term quantum memories can be realized), information leakage to other degrees of freedom is automatically revealed, and in principle the source can even be in the hands of an eavesdropper. This last is of particular significance when one considers a network, where one does not want to have to "trust" each node.

5. Unknowns/weaknesses

The main limitation to the entangled-state quantum cryptography, at present, is the source brightness. Typical sources generate less than 1×10^{6} pair photons•sec^{-1}, and to date the highest *detected* pair rates range 4×10^{5} to 1.3×10^{6} coincidences•sec^{-1} [13–14].

For fiber-based schemes the efficiency of coupling pair photons into single modes needs to be optimized—typical coupling to single modes is less than 20% [21]. For free-space schemes, single spatial mode operation is probably not required, as turbulence will introduce extra modes regardless.

6. Five-year goals

- 10^{6} coincidences•sec^{-1} source (detected in laboratory)
- Free-space systems operating out to 10 km (per arm)
- 10^{5} coincidence•sec^{-1} into a single mode
- Prototype systems for fiber communications to 50 km
- Quantum memory with high fidelity storage
- Quantum repeater with bit rate exceeding 10 qubits•sec^{-1}

7. Ten-year goals

- Quantum memory for up to 1 second storage
- Satellite source generating keys at ground level
- Prototype systems for fiber communications to > 100 km

- Quantum repeater with bit rate exceeding 1000 qubits•sec^{-1}

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

High-brightness and high-efficiency compact sources (see, for instance, Reference [22]) are needed. These should emit into only a few spatial modes (or a single mode, for fiber systems). Also, in order to enable spectra filtering as a means to reduce background, it is desirable that the brightness into reduced bandwidths (~ 1 nm FWHM) be increased.

It is also desirable to have an "on-demand" source of entangled photons, as this would further reduce noise from empty pulses. Some of the advantages of entanglement outlined in Section 2, Security, are only achievable if one has quantum memory devices, which ideally would store unmeasured quantum bits indefinitely. Finally, in order to achieve distances longer than 100 km in optical fibers, quantum repeaters [12] will have to be efficiently realized. One proposal for achieving this is by coupling the polarization of (narrow-bandwidth) entangled down-conversion photons into an atomic system [23].

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

For fiber implementations, the development of improved detectors at communications wavelengths is necessary. Improved crystals and particularly waveguide and fiber sources of photon pairs are needed. Improved mode-matching between pair source and single-mode fibers is needed; inexpensive adaptive optics would be very helpful.

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

High-brightness sources will feed into other quantum-communications schemes (entanglement swapping, quantum teleportation, dense coding) and into quantum information in general (linear optical gates, efficient heralded single-photon sources etc).

11. Role of theory/security-proof status for entangled-photon QKD

Theoretical proofs of security are in place [5,6]. Further study is needed on the use of entanglement in systems with multiple degrees of freedom or continuous variables, and multipartite protocols (i.e., connecting more than two parties).

References

[1] Kwiat, P.G., K. Mattle, H. Weinfurter, and A. Zeilinger, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letters* **75**, 4337–4341 (1995);
Kwiat, P.G., E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, "Ultrabright source of polarization-entangled photons," *Physical Review A* **60**, R773–R776 (1999).

[2] Brendel, J., E. Mohler, and W. Martienssen, *Europhysics Letters* **20**, 575 (1993;
Kwiat, P.G., A.M.!Steinberg, and R.Y.!Chiao, "High-visibility interference in a Bell-inequality experiment for energy and time," Physical Review A 47, R2472–R2475 (1993);

Strekalov, D.V., T.B. Pittman, A.V. Sergienko, and Y.H. Shih, “Postselection-free energy-time entanglement,” *Physical Review A* **54**, R1–R4 (1996).

[3] Rarity, J.G. and P.R. Tapster, “Experimental violation of Bell's inequality based on phase and momentum,” *Physical Review Letters* **64**, 2495–2498 (1990).

[4] Ekert, A.K., “Quantum cryptography based on Bell's theorem,” *Physical Review Letters* **67**, 661–663 (1991);
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)

[5] Lo, H.-K. and H.F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science* **283,** 2050–2056 (1999);
Lo, H.-K., “Proof of unconditional security of six-state quantum key distribution scheme,” *Quant. Inform. Comput.* **1**(2), 81–94 (2001).

[6] Lutkenhaus, N., “Security against individual attacks for realistic quantum key distribution,” *Physical Review A* **61**, 052304 (2000).

[7] Bennett, C.H., G. Brassard, and D. Mermin, “Quantum cryptography without Bell's theorem,” *Physical Review Letters* **68**, 557–559 (1992).

[8] Mayers, D. and A. Yao, “Quantum cryptography with imperfect apparatus,” *Proceedings of the 39th Annual Symposium on the Foundations of Computer Science (FOCS98)*, K. Kelly, Ed., (IEEE, Los Alamitos, California, USA, 1998), Catalog #: 98CB36280 pp. 503–509 [quant-ph/9809039].

[9] Kurtsiefer, C., P. Zarda, S. Mayer, and H. Weinfurter, “The breakdown flash of silicon avalanche photodiodes—back door for eavesdropper attacks?,” *Journal of Modern Optics* **48**, 2039–2047 (2001).

[10] Aspelmeyer, M., H.R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, “Long-distance free-space distribution of quantum entanglement,” *Science* **301**, 621–623 (2003).

[11] Waks, E., A. Zeevi, and Y. Yamamoto, “Security of quantum key distribution with entangled photons against individual attacks,” *Physical Review A* **65**, 052310 (2002).

[12] Briegel, H.-J., W. Dür, J.I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication,” *Physical Review Letters* **81,** 5932–5935 (1998).

[13] Kurtseifer, C., M. Oberparleiter, and H. Weinfurter, “High-efficiency entangled photon pair collection in type-II parametric fluorescence,” *Physical Review A* **64**, 023802 (2001).

[14] Kwiat, P.G., private communication (2003).

[15] Tittel, W.J., H. Brendel, H. Zbinden and N. Gisin, “Quantum cryptography using entangled photons in energy-time Bell states,” *Physical Review Letters* **84**, 4737–4740 (2000);
Ribordy, G., J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, “Long-distance entanglement-based quantum key distribution,” *Physical Review A* **63**, 012309 (2001).

[16] Jennewein, T., C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Physical Review Letters* **84**, 4729–4732 (2000).

[17] Naik, D.S., C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, "Entangled state quantum cryptography: Eavesdropping on the Ekert protocol," *Physical Review Letters* **84**, 4733–4736 (2000);
Enzer, D.G., P.G. Hadley, R.J. Hughes, C.G. Peterson, and P.G. Kwiat, "Entangled-photon six-state quantum cryptography," *New Journal of Physics* **4**, 45.1–45.8 (2002).

[18] Jennewein, T., G. Weihs, J.-W. Pan, and A. Zeilinger, "Experimental nonlocality proof of quantum teleportation and entanglement swapping," *Physical Review Letters* **88**, 017903 (2002);
Pan, J.W., S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, "Experimental entanglement purification of arbitrary unknown states," *Nature* **423**, 417–422 (2003);
Zhao, Z., T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan, "Experimental realization of entanglement concentration and a quantum repeater," *Physical Review Letters* **90**, 207901 (2003).

[19] Pittman, T.B. and J.D. Franson, "Cyclical quantum memory for photonic qubits," *Physical Review A* **66**, 062302 (2002).

[20] Kwiat, P.G., J. Altepeter, J. Barreiro, D.A. Branning, E.R. Jeffrey, N. Peters, and A.P. VanDevender, "Optical technologies for quantum information science," in *Quantum Communications and Quantum Imaging*, R.E. Meyers and Y. Shih, Eds., (SPIE, Bellingham, Washington, USA, 2004), *Proceedings of SPIE* Vol. 5161, pp. 87–101.

[21] Banaszek, K., A.B. U'Ren, and I.A. Walmsley, "Generation of correlated photons in controlled spatial modes by downconversion in nonlinear waveguides," *Optics Letters* **26**, 1367–1369 (2001);
Sanaka, K., K. Kawahara, and T. Kuga, "New high-efficiency source of photon pairs for engineering quantum entanglement," *Physical Review Letters* **86**, 5620–5623 (2001).

[22] Tanzilli S., H. De Riedmatten, H. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D.B. Ostrowsky, N. Gisin, "Highly efficient photon-pair source using periodically poled lithium niobate waveguide," *Electronics Letters* **37**, 26–28 (2001);
Kuklewicz, C.E., M. Fiorentino, G. Messin, F.N.C. Wong, and J.H. Shapiro, "High-flux source of polarization-entangled photons from a periodically poled $KTiOPO_4$ parametric down-converter," *Physical Review A* **69**, 013807 (2004);
Oberparleiter, M. and H. Weinfurter, "Cavity-enhanced generation of polarization-entangled photon pairs," *Optics Communications* **183**, 133–137 (2000).

[23] Shapiro, J., "Architectures for long-distance quantum teleportation," *New Journal of Physics* **4**, 47.1–47.18 (2002).