Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Section 6.3: Single-Photon Light Sources

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
Draft 1.0

ARDA

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

Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Sae Woo Nam

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 and Figures

List of Acronyms and Abbreviations

NVC	nitrogen vacancy-center
PNS	photon-number splitting (attack)
QCrypt	quantum cryptography
QIS	quantum information science
QKD	quantum key distribution
TEP	Technology Experts Panel
WCP	weak coherent pulse

6.3 Single Photon Light Source Approaches to QKD

Table 6.3-1.
Groups Pursuing Single-Photon Light Source Implementations of QKD

Research Leader(s)	Research Location	Research Focus
Yamamoto, Y. & Vuckovic, J.	Stanford Univ., USA	experiment
Grangier, P.	Institut d'Optique, CNRS, France	experiment
Kwiat, P.	Univ. Illinois, Urbana-Champaign, USA	experiment
Rarity, J.	Univ. Bristol, UK	experiment
Migdall, A. & Williams, C.	NIST, USA	experiment
Shields, A.	UK	experiment

1. Brief description and background for single-photon light source approaches to QKD

Most implementations of quantum key distribution (QKD) rely on photon sources that are approximations to a single-photon source. The generation of two or more photons in a pulse used in a quantum link poses an opportunity for information to be obtained by an eavesdropper. Much work has been done in generating single photons on demand as a photon source for QKD. Various methods of single-photon generation "on demand" are being explored using controlled excitations of single molecules [1], nitrogen vacancy-centers (NVCs) in diamond [2,3], semiconductor quantum-wells [4,5], semiconductor quantum dots [6,7], and spontaneous parametric down-conversion [8]. See the components section for more details.

2. Attributes for single-photon source 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 using single-photon sources is similar to other QKD implementations. The principal advantage is that a true single-photon source with the second-order correlation, $g^{(2)} = 0$ is that the system is intrinsically secure from the photon-number splitting (PNS) attack, because any given pulse never has more than one photon present. As long as $g^{(2)} > 0$, additional privacy amplification is required to remove the extra information obtainable by an eavesdropper looking at multiple-photon pulses. Although the limiting case $g^{(2)} = 0$ is ideal and will never be achieved in practice, one can nevertheless do much better than simply using attenuated laser pulses for which $g^{(2)} = 1$. For the purposes of this section we apply the term "single-photon source" to any source with $g^{(2)} < 0.1$. At this point in time, the lowest reported value is $g^{(2)} < 0.05$ [9].

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

   In principle, for a given bit rate, QKD with single-photon sources can achieve longer distances for key transmission than QKD with weak coherent pulses (WCPs). (The reason is that, although a WCP can be attenuated to arbitrarily reduce the multiple-photon probability, this comes at the cost of producing an ever-greater fraction of "empty" pulses. However, the protocol requires that Bob look at each pulse, and therefore, the contribution of noise in Bob's detectors increases as the fraction of empty pulses.) The maximum range demonstrated to date using a single-photon source has been 50 m in free space [10]. At the present time, the distance has been limited by a combination of source-coupling inefficiency and detector dark-count rates. To obtain longer distances in free space and fiber, development of single-photon sources at more optimum wavelengths and linewidths is needed.

3. Relative speed potential: **M**

   The speed is limited by the optical pumping process (repetition frequency and intrinsic generation efficiency) and the optical-coupling efficiency. Speeds of 1–10 GHz are not unrealistic, though current QKD experiments have rates much less than 1–10 GHz.

4. Relative maturity: **L**

   Proof-of-principle experiments have been done with quantum-dot sources and nitrogen-vacancy sources [10,11]. The single-photon sources are still an active area of research. Commercial optical components are not optimized for the wavelengths of existing research-grade sources. Furthermore, no sources are available commercially at the present time.

5. Relative robustness: **M**

   Like other point-to-point protocols, the availability is immediately compromised by any form of eavesdropping.

3. Development-status metrics

To date, two groups have used a single-photon source in a QKD link which includes sifting, error-correction, and privacy amplification. Both systems were free-space demonstrations over short distances, 1 m [10] and 50 m [11]. Attenuators were used in the 1-m experiment to demonstrate the effect of further channel losses (potentially longer distances).

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 use of a single-photon source can significantly improve the security from the PNS attack. Other potential practical advantages even with nonideal single-photon sources are, for instance, a possible reduction in classical communication overhead because the number of multiple-photon pulses is significantly less than in a WCP system.

5. Unknowns/weaknesses

Two primary weaknesses exist at the present time. The first is source efficiency, which is related to the ability to efficiently outcouple the optical mode. At present, sources are being driven with 5–100 MHz pump frequencies, but yield single photons at rate of 100 kHz. One method to improve the efficiency is to use optical cavities to enhance outcoupling into particular modes. This has already been initially demonstrated with one of the sources [10]. The use of a cavity must be carefully designed so that the time window for the photon emission is not significantly lengthened, thereby reducing the ability to use timing to discriminate against background.

A second weakness are the wavelengths and linewidths available from the single-photon sources. At present, the wavelengths are best suited for free-space demonstrations. Also, the linewidths from some implementations are many nanometers [3]. This severely restricts the ability to use narrow-band spectral filters to reduce the contribution of background light, probably rendering these sources unsuitable for practical QKD applications.

6. Five-year goals

- Demonstration of single-photon source QKD on kilometer-length scales

7. Ten-year goals

- Demonstration of single-photon source QKD on 100-km-length scales at MHz rates
- Satellite QKD with single-photon sources

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

Improvements in source efficiency, wavelength, and linewidth.

For sources based on parametric downconversion, the development of bright, diode-pumped sources, at appropriate wavelengths and also the development of low-loss optical switches.

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.

The development of low-cost adaptive optics might significantly improve the coupling from source to transmission channel. For quantum dot implementations, the development of low cost cryogenic techniques will be important for practical implementations.

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 single-photon source QKD

Theoretical proofs of security are in place. Further study is needed to optimize practical implementation details in sifting, error correction, and privacy amplification to take advantage of imperfect nonclassical light emission.

References

[1] Lounis, B. and W.E. Moerner, "Single photons on demand from a single molecule at room temperature," *Nature* **407**, 491–493 (2000).

[2] Beveratos, A., S. Kühn, R. Brouri, T. Gacoin, J.-P. Poizat, and P. Grangier "Room temperature stable single-photon source," *European Physical Journal D* **18**, 191–196 (2002).

[3] Kurtsiefer, C., S. Mayer, P. Zarda, and H. Weinfurter, "Stable solid-state source of single photons," *Physical Review Letters* **85**, 290–293 (2000).

[4] Imamoglu, A. and Y. Yamamoto, "Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions," *Physical Review Letters* **72**, 210–213 (1994).

[5] Kim, J., O. Benson, H. Kan, and Y. Yamamoto, "A single-photon turnstile device," *Nature* **397**, 500–503 (1999).

[6] Moreau, E., I. Robert, J.M. Gérard, I. Abram, L. Manin, and V. Thierry-Mieg "Single-mode solid-state single photon source based on isolated quantum dots in pillar microcavities," *Applied Physics Letters* **79**, 2865–2867 (2001).

[7] Ward, M.B., Z. Yuan, R.M. Stevenson, B.E. Kardynal, C.J. Lobo, K. Cooper, D.A. Ritchie, and A.J. Shields "Single photon emitting diode," *Free-Space Laser Communication and Laser Imaging II: Proceedings of the SPIE - The International Society for Optical Engineering* **4821**, 466–473 (2002).

[8] Migdall, A.L., D.A. Branning, S. Castelletto, and M. Ware, "Single photon source with individualized single photon certifications," *Free-Space Laser Communication and Laser Imaging II: Proceedings of the SPIE - The International Society for Optical Engineering* **4821**, 455–465 (2002).

[9] Santori, C., D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "Indistinguishable photons from a single-photon device," *Nature* **419**, 594–597 (2002).

[10] Beveratos, A., R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier "Single photon quantum cryptography," *Physical Review Letters* **89**, 187901 (2002).

[11] Waks, E., K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto "Secure communication: Quantum cryptography with a photon turnstile," *Nature* **420**, 762 (2002).