Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Section 6.2: Weak Laser Pulses through Free Space

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: Richard Hughes, Jane Nordholt 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 and Figures

List of Acronyms and Abbreviations

APT	acquisition, pointing, and tracking
DoS	denial of service
FSO	free-space optical
GAO	General Accounting Office
GEO	geosynchronous-Earth orbit
GPS	global-positioning system
LEO	low-Earth orbit
QCrypt	quantum cryptography
QIS	quantum information science
QKD	quantum key distribution
TEP	Technology Experts Panel
TT&C	tracking, telemetry, and control

6.2 Weak Laser Pulses through Free-Space Approaches to QKD

Table 6.2-1.
Groups Pursuing Weak Laser Pulses through Free Space Implementations of QKD

Research Leaders	Research Location	Research Focus
Edwards, P.	Univ. Canberra	Ground to satellite
Gilbert, G.	MITRE	Theory
Hughes, R.	LANL	Ground to satellite
Kurtsiefer, C.	Univ. Singapore	Line of sight
Lowans, B.	Qinetiq	Small system
Rarity, J.	Univ. Bristol	Ground to satellite
Williams, C.	NIST Gaithersberg	High speed QKD
Weinfurter, H.	Univ. Munich	Line of sight
Zeilinger, A.	Univ. Vienna	Line of sight

1. Brief description and background for weak laser pulses through free space approaches to QKD

At first sight, quantum key distribution (QKD) through the atmosphere (“free space”)[1] might appear to be a very much more challenging problem than QKD with weak laser pulses in optical fiber: the transmitter and receiver must reliably acquire, point, and track each other to establish and maintain the quantum channel; single-photon level signals must be reliably transmitted through the turbulent atmosphere and detected in the presence of background radiance, which is a strong error source even at night. Fortunately, the free-space optical (FSO) and laser communications communities have effectively solved the acquisition, pointing, and tracking (APT) problems even for moving platforms, the atmosphere is known to be essentially nonbirefringent at optical wavelengths[2] and possesses several good transmission windows that coincide with the high detection efficiency, low-noise regime of commercial off-the-shelf single-photon detectors. Furthermore, at optical wavelengths Faraday rotation in the ionosphere is of negligible consequence for QKD (in contrast to conventional radio communications) in a ground-to-satellite context. Background rejection is also readily dealt with once it is appreciated that even daylight radiance corresponds to a photon occupation number per mode of the electromagnetic field that is very much less than one. The background can then be reduced to a very manageable level using a readily achievable combination of spectral, spatial, and temporal filtering. The synchronization requirements are especially important but can be addressed with commercial off-the-shelf technology.

In weak-laser-pulse approaches “single photon” signals are approximated by light pulses with Poisson photon-number distributions characterized by small values of μ, the mean number of photons/pulse, just as in optical-fiber QKD with weak laser pulses, although wavelengths in the 750–850 nm range are strongly preferred for efficient atmospheric propagation and detection. The probability of pulses containing multiple photons relative to single-photon pulses (~ $\mu/2$ for small μ) must be kept small to limit the efficacy of beamsplitting and other attacks that exploit multiple-photon signals and loss in the quantum channel. Typically values of $\mu \sim 0.1$–0.5 are used in experimental systems.

Free-space QKD may be well-suited for ground-to-ground applications over campus or metro-area distances in conjunction with free-space optical communications. Another potential application of particular interest is for secure satellite-to-ground communications, to allow on-orbit re-key for secure satellite tracking, telemetry, and control (TT&C) and data dissemination [3]. These aspects of satellite communications were pointed out as deserving of additional attention in a 2002 General Accounting Office (GAO) report [4]. A QKD-capable satellite also opens up the possibility of using it to distribute cryptographic keys between any ground stations that it can contact [5]. The feasibility of satellite QKD has been further discussed in References 6 and 7.

The first, proof-of-principle demonstration of QKD (performed in 1991) was in free-space over a ~ 30 cm laboratory distance [8], and the essential feasibility of quantum communications through the atmosphere was experimentally demonstrated that same year [9]. Then, in 1996, one of the early fiber QKD experiments at the Applied Physics Laboratory was adapted to show the feasibility of short distance (~ 70 m) QKD through the air [10] over a folded path. The results of a demonstration over a 205-m indoor folded path using a synchronization method that would open the way to both long-distances and satellite QKD were published in 1998 [11]. Today, free-space QKD has been demonstrated over distances up to 10 km in daylight [12] and 23 km at night [13], while recent work has begun to explore the feasibility of increasing the speed of QKD over short distances (< 1 km) at night [14].

2. Attributes for weak laser pulse systems through free space

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: **M**

   Weak-laser-pulse QKD implementations have inspired considerable analysis of the eavesdropping opportunities associated with the (typically small) fraction of signals that contain more than one photon and lossy quantum channels.

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

   Multikilometer ground-to-ground demonstrations of free-space QKD have been performed and several groups have published detailed modeling to show that low-Earth orbit (LEO) satellite-to-ground QKD would be feasible even in daylight, with typical ranges of ~ 1,000 km. Similar modeling has established the feasibility of even geosynchronous-Earth orbit (GEO) to ground QKD at night.

3. Relative speed potential: **H**

   Present-day free-space QKD is not as limited in rate by detector technology as optical-fiber QKD, owing to the commercial availability of high-efficiency detectors capable of operating at rates up to 10 MHz.

4. Relative maturity: **M**

   Weak-laser-pulse free-space QKD is a relatively mature technology for QKD; it can be implemented with today's technology, and several prototypes are now operational.

5. Relative robustness: **M**

   With effective background rejection and beacon-aided pointing and tracking, free-space QKD is remarkably robust: useful key rates over multikilometer transmission distances have been demonstrated, even in full daylight.

3. Development-status metrics

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

One of the most significant strengths of this approach is that it can already be performed at rates useful for key transfer using commercial off-the-shelf components. Secondly, integration and co-existence with FSO communications is likely to be considerably less challenging than for QKD in optical fibers, owing to the underlying point-to-point link nature of this communications environment. Third, in many respects free-space QKD most closely approximates the idealizations of theoretical QKD security analyses of any of the approaches. Finally, *known* secure-communications needs could, indeed, be the “killer apps” for free-space QKD.

5. Unknowns/weaknesses

The unknowns in this approach are primarily in the area of availability of service under diverse atmospheric and weather conditions. These are issues that can be explored with further experimentation and modeling. Another unknown, as with any approach to QKD, is the extent to which it is resistant to denial-of-service (DoS) attacks, although the strong background-rejection methodology required to implement free-space QKD already provides greater resistance to DoS than with some other approaches.

6. Five-year goals

- Exploration of free-space QKD beyond ground-to-ground links, such as air-to-ground
- Integration with optical-fiber QKD systems to form a hybrid QKD network.

7. Ten-year goals

- Source pulse rates of at least 1 GHz, which will require substantial detector improvement
- Continuous key generation with > 100,000 bits•sec^{-1} secret key rates.

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

All necessary components to implement a working version of this approach exist, and several operational systems exist.

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

Weak-pulse QKD in free-space would benefit from improvements in detector technology, including higher bias rates, higher detector efficiency, lower dark-count probability, and reduced timing jitter. One can envision a weak-pulse system that runs at gigahertz rates, if suitable detectors existed. Optimistically, single-photon sources efficiently coupled to free-space launch optics could potentially improve both the rate and security of this implementation.

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

Developments in weak-laser-pulse free-space QKD will pave the way for follow-on "second-wave" QKD implementations using single-photon and entangled light sources.

11. Role of theory/security-proof status for weak laser pulses through free space QKD

Although the theory of weak laser-pulse QKD is relatively mature, further theoretical work is still required in two areas:

- detailed analysis of the vulnerabilities incurred by multiple-photon pulses and
- the degree of protection possible with QKD systems built from real (imperfect) equipment.

Novel protocols, such as a new sifting procedure invented by the Geneva group, may also obviate the security issues caused by multiple-photon pulses; these should be carefully investigated.

References

[1] For a review, see:
Nordholt, J.E. and R.J. Hughes, "A new face for cryptography," Los Alamos Science **27**, 68–85 (2002) [available at URL: http://lib-www.lanl.gov/cgi-bin/getfile?00783355.pdf].

[2] Saleh, A.A., "An investigation of laser wave depolarization due to atmospheric transmission," *IEEE Journal of Quantum Electronics* **3**, 540–543 (1967).

[3] Hughes, R.J. *et al.*, "Secure communications with low-orbit spacecraft using quantum cryptography"; U.S. Patent 5,966,224, filed May 20, 1997, issued October 12, 1999;
Hughes, R.J. and J.E. Nordholt, "Quantum cryptography takes to the air," *Physics World* **12**, 31–35 (May 1999).

[4] "Critical infrastructure protection: commercial satellite security should be more fully addressed," General Accounting office report GAO-02-781 (2002).

[5] Hughes, R.J., W.T. Buttler, P.G. Kwiat, S.K. Lamoreuax, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, "Quantum cryptography for secure satellite communications," in *Proceedings of the IEEE Aerospace Conference 2000*, (IEEE, Piscataway, NJ, 2000) **1803** Vol. 1, pp. 191–200.

[6] Nordholt, J.E. *et al.*, "Present and future free-space quantum key distribution," in *Free-Space Laser Communication Technologies XIV (Proceedings of SPIE Volume: 4635)*, G. Stephen Mecherle, Ed., (SPIE, Bellingham, WA, 2002) Vol. 4635, pp. 116–126.

[7] Rarity, J.G., P.R. Tapster, P.M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics* **4**, 82.1–82.9 (2002).

[8] Bennett, C.H., *et al.*, "Experimental quantum cryptography," *Journal of Cryptology* **5**, 3 (1992).

[9] Seward, S.F. *et al.*, "Daylight demonstration of a low-light-level communication system using correlated photon pairs," *Quantum Optics: Journal of the European Optical Society Part B* **3**, 201 (1991).

[10] Franson, J. and B. Jacobs, "Quantum cryptography in free-space," *Optics Letters* **21**, 1854–1856 (1996).

[11] Buttler, W.T., R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, "Free space quantum key distribution," *Physical Review A* **57**, 2379–2382 (1998).

[12] Hughes, R.J., J.E. Nordholt, D. Derkacs, and C.G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics* **4**, 43.1–43.14 (2002).

[13] Kurtsiefer, C., P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, "A step towards global key distribution," *Nature* **419**, 450 (2002).

[14] Bienfang, J., A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," *Optics Express* **12**, 2011–2016 (2004).