Summary of Implementation Schemes for Quantum Key Distribution and Quantum Cryptography

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Section 6.1: Weak Laser Pulses over Fiber

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: Don Bethune and Chip Elliott

Editing and compositing: Todd Heinrichs

Table of Contents

List of Tables and Figures

List of Acronyms and Abbreviations

APD	avalanche photodiode
QIS	quantum information science
QKD	quantum key distribution
SPD	single-photon detector
TEP	Technology Experts Panel

6.1 Weak Laser Pulses over Optical Fiber Approaches to QKD

In this approach, highly attenuated light pulses generated by conventional diode lasers are transmitted over conventional single-mode optical fiber [1]. Either polarization or phase encoding of quantum information can been used for fiber-based quantum key distribution (QKD) systems, by splitting each pulse into two amplitude packets with orthogonal or parallel polarizations, respectively. The relative phase of these packets is used to encode information. Such systems can operate over short distances with light wavelengths near 800 nm, or over much longer distances at the telecom wavelength ranges near 1300 or 1550 nm. Solid-state avalanche photodiodes (APDs) are used as single-photon detectors (SPDs). Fiber attenuation and typical detector dark-count probabilities lead to a maximum range of ~100 km for this approach. These approaches can be usefully subdivided into two classes: "one-way" schemes, or "round-trip" (sometimes known as "plug-and-play") schemes.

A. Weak Laser Pulses over Fiber ("One-Way")

This section provides detailed information about full QKD systems employing weak laser pulses through telecommunications fiber for so-called "one way" systems (i.e., those in which a modulated weak pulse propagates directly from Alice to Bob). It includes information about the research teams working in this area, current state of the art, strengths and weaknesses of this approach, and five- and ten-year goals for such systems.

Table 6.1-1.
Groups Pursuing Weak Laser Pulses over Fiber "One-Way" Implementations of QKD

Research Leader(s)	Research Location	Research Focus
	Elsag-Bailey (Italy)	Software protocols
Elliott, C.	BBN, Boston	Metropolitan QKD network, protocols
J. Franson, J.	JHU/APL, Maryland	Fiber and free space systems
Goedgebuer, J.-P.	University of Franche-Comté	Differential phase modulation
Hasegawa, T.	Mitsubishi Electric	Complete QKD system
Hjelme, D.	Norwegian University of Science and Technology	Complete QKD system
Hughes, R.J.	LANL	Complete QKD system
Shields, A.	Toshiba UK	Complete QKD sys, single photon source, long distance
Townsend, P.D.	University College, Cork (Eire)	Metropolitan QKD networks
Zeng, H.	East China Normal University	Sagnac interferometer for phase encoding

1. Brief description and background for "One-Way" weak laser pulse systems through fiber

QKD systems based on transmitting highly attenuated light pulses generated by conventional diode lasers over optical fiber exploit currently available telecommunications technology to

allow present-day implementation of quantum cryptography over existing optical fiber networks. Key generation over distances on the order of tens of kilometers is already practical, and distances up to about 100 km seem feasible. This range is suitable for metro-area scale QKD.

These systems approximate "single-photon" pulses by weak coherent pulses (e.g., from attenuated telecommunications lasers), with Poisson photon-number distributions characterized by μ, the mean number of photons/pulse. The frequency of pulses that contain multiple photons relative to single-photon pulses (~ $\mu/2$, for small μ) must be kept small to limit the efficacy of beamsplitter attacks. Typically values $\mu \sim 0.1$–0.5 are used in practical systems.

Due to their relative simplicity, low cost, and immediate applicability, such systems have been the focus of numerous prototype-development efforts. For short ranges (< 10 km), fiber-based systems have used wavelengths near 800 nm, allowing them to take advantage of available highly efficient silicon-based APD detectors. But, starting with the pioneering work of P. Townsend and colleagues [2], greater transmission distances require use of the telecommunications wavelengths near 1300 and 1550 nm, because at these wavelengths the dispersion and attenuation of optical fiber, respectively, are minimized. InGaAs-InP -based APD detectors are typically used for light at these wavelengths.

Either phase or polarization encoding of quantum information can been used for fiber-based QKD systems, but polarization-encoded "one-way" fiber systems are difficult to make practical, due to the unpredictable polarization scrambling imposed by installed telecommunications fiber. Phase-encoded fiber systems require continuous active control of Mach-Zehnder interferometer arm lengths. Such systems have been demonstrated in prototype QKD implementations, with phase-drift errors easily low enough for practical systems; a transmission distance of 122 km has been recently reported [3]. Some preliminary research has also been carried out on networking with one-way fiber QKD [4,5].

2. Attributes for "One-Way" weak laser pulse systems through fiber

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**
2. Relative transmission distance potential: **M**
3. Relative speed potential: **H**
4. Relative maturity: **M**

   This is a relatively mature QKD technology, which can be implemented with today's technology. Several prototypes are now operational; some groups have performed demonstrations through *in situ* telecommunications fiber.

5. Relative robustness: **M**

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-way" QKD systems exploit currently available telecommunications technology to allow present-day implementation of quantum cryptography over existing optical-fiber networks. Key generation over distances on the order of tens of kilometers has been repeatedly demonstrated, and distances up to about 100 km seem feasible. This range is suitable for metro-area scale QKD. A first generation of commercial hardware implementing this approach is now available.

"One-way" QKD systems have the potential to run at very high rates. One can readily envision a transmitter that prepares 10 billion pulses per second, rather than today's 5 million, for a 2,000-fold speedup in QKD delivery rates. However, these systems will not be feasible until very fast detectors at telecommunications wavelengths, with good quantum efficiency and low dark count, become available.

Finally, "one way" designs can migrate quite easily from weak laser pulses to single-photon sources when workable sources become available.

5. Unknowns/weaknesses

This approach has been heavily investigated and most aspects of the technology are well understood. Questions remain concerning integration with the telecom network, detector availability and optimization, and maximum feasible distance and key generation rates. Security issues are still being investigated, and to date there are few actual experimentally implemented attacks.

Even though distances up to about 100 km seem feasible, the extension of this method to longer ranges is problematic. Work on exotic ultralow attenuation fibers is being carried out (notably at MIT), but even if successfully developed, cost and limited installation would likely restrict long-distance key generation over such fiber to a few highly critical applications. It is also possible that successful development of quantum repeaters could help address the range limitation.

At present, there are no good detectors for QKD at telecommunications frequencies (1300 or 1550 nm). Existing InGaAs detectors have not been optimized for such weak signals, and suffer from poor quantum efficiency, high dark count, and/or serious after-pulsing issues. Detectors are a very serious issue for all approaches to QKD through telecommunications fiber.

6. Five-year goals

- Generally agreed theory of eavesdropping attacks and defenses in realistic systems
- Integration into telecommunications links and QKD networks
- Implementation over existing telecommunications networks on a point-to-point basis, with continuous key generation with >10,000 bits•sec^{-1} secret key rates
- Full protocol implementation including authentication and protection against eavesdropping
- Community-wide agreement on catalog of eavesdropping attacks and analysis

7. Ten-year goals

- Source pulse rates of at least 1 GHz (requires much better detectors)
- Implementation over multiuser networks with any-to-any connectivity with metro-scale areas
- Continuous key generation with > 100,000 bits•sec^{-1} distilled key rates
- Integration with free-space systems to form a hybrid QKD network
- Implementation of quantum-repeaters to extend distance to intercity distances (500 km)

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

QKD based on weak laser pulses has been demonstrated in several operational systems, but considerable work will be required in order to achieve the five- and ten-year goals. Chief among them are continued advances in understanding security for realistic systems, breakthroughs in SPD technology, and experimentation with networked versions of weak-laser-pulse QKD.

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

Weak-pulse-over-fiber QKD would most benefit from improvements in detector technology (higher bias rates, higher detector efficiency, lower dark-count probability, reduced after-pulse probability). One can envision a weak-pulse fiber system that run at gigahertz rates, if workable detectors existed. Optimistically, quantum repeaters would allow range extensions, and single-photon sources efficiently coupled to fiber could potentially improve both the rate and security of this implementation.

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

In principle, wide application of this approach in metropolitan-sized areas is possible.

11. Role of theory/security-proof status for “One-Way” weak laser pulse systems through fiber

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 protocol invented by the Geneva group, may also obviate the security issues caused by multiple-photon pulses; these should be carefully investigated.

B. Weak Laser Pulses over Fiber ("Plug-and-Play")

This section provides detailed information about another type of full QKD system employing weak laser pulses through telecommunications fiber that uses the so-called "plug and play" [6,1] or "autocompensating" design [7]. It includes information about the research teams working in this area, current state of the art, strengths and weaknesses of this approach, and five- and ten-year goals for such systems. In such systems, Bob sends a relatively strong, orthogonally-polarized pair of light pulses to Alice, who modulates their relative phase, attenuates them to "single-photon-level" amplitude, and retroreflects them back to Bob using a Faraday mirror. The relative phase of the amplitude pulses carries the quantum information to Bob. He extracts the phase information by combining the pulses interferometrically and determining which path the combined pulse follows using a pair of SPDs.

Table 6.1-2.
Groups Pursuing Weak Laser Pulses over Fiber "Plug and Play" Implementations of QKD

Research Leader(s)	Research Location	Research Focus
Bethune, D. & Risk, W.	IBM Almaden	Complete QKD system
Hjelme, D.	Norwegian University of Science and Technology	Practical attacks/defenses for "plug and play" systems
Nakamura, K.	NEC Japan	Complete QKD system
Nielsen, M. *et al.*	U. of Aarhus (Denmark)	Complete QKD system
Ribordy, G.	ID Quantique (U. of Geneva)	Commercial "plug and play" system
Trifonov, A.	Magiq	Commercial "plug and play" system
Yoshizawa, A.	National Institute of Advanced Industrial Science and Technology (AIST), Japan	Complete QKD system
Karlsson, A.	KTH, Sweden [8]	Long-wavelength demonstration system

1. Brief description and background for "Plug and Play" weak laser pulse systems through fiber

QKD systems based on transmitting highly attenuated light pulses generated by conventional diode lasers over optical fiber exploit currently available telecommunications technology to allow present-day implementation of quantum cryptography over existing optical-fiber networks. Key generation over distances on the order of tens of kilometers is already practical, and distances up to about 100 km seem feasible. This range is suitable for metro-area scale QKD.

Polarization scrambling due to uncontrolled refractive index tensor changes in the fiber poses a difficulty for polarization-based fiber systems. Two approaches to overcoming this problem have been developed. The first is to actively measure the optical transformation due to the fiber and optically compensate to correct for this transformation as the fiber state changes. This can be done in a closed-loop feedback arrangement as demonstrated by Franson *et al.* [9,10,11].

The second approach is to use a round-trip system, referred to as either "plug-and-play" or "autocompensating" in the literature. Such systems send the light on a round trip through the fiber, at relatively high intensity on the outbound leg but attenuated to the single-photon level for the return trip. A Faraday mirror at the fiber end is used to reflect the light with a 90° polarization rotation. This has the effect that the total optical phase a light pulse accumulates over the course of a round trip through the fiber and back does not depend on the polarization state in which it is launched. This permits the relative phase of two orthogonally polarized amplitude packets to be used as a fiber-state invariant coding variable. Transmission distances of up to 67 km have been reported [12].

Both of the recently introduced commercial fiber-based QKD systems use this round-trip arrangement due to the inherent stability and high contrast readout attainable with such automatically compensated interferometers. [13]

The relative security of "one-way" vs. "round-trip" systems is a topic that is still actively being studied, but the security of the latter certainly requires taking additional precautions such as Alice monitoring the frequency, amplitude, timing, and total average power of the pulses arriving at her station.

An important question is how readily QKD protocols can be adapted to existing fiber-optic networks. This has bearing on numerous choices ranging from what quantum channel wavelength to use to whether round-trip or one-way architectures are more suitable. Early work on this question was carried out Townsend *et al.* at British Telecom. Additional work to address these questions is being carried out under the DARPA-QuIST program [14] by collaborations including groups at BBN Corporation, Boston University, Harvard University, Telcordia Technologies, and Los Alamos National Laboratory.

2. Attributes for "Plug and Play" weak laser pulse systems through fiber

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**
2. Relative transmission distance potential: **M**
3. Relative speed potential: **H**
4. Relative maturity: **M**

   This is the most mature technology for QKD; commercial systems are being advertised for dark fiber applications.

5. Relative robustness: **M**

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

QKD systems based on transmitting highly attenuated light pulses generated by conventional diode lasers over optical fiber exploit currently available telecommunications technology to allow present-day implementation of quantum cryptography over existing optical-fiber networks. Key generation over distances on the order of tens of kilometers is already practical, and distances up to about 100 km seem feasible. This range is suitable for metro-area scale QKD. First commercial hardware implementing this approach is now available.

Plug and play systems are based on the invariance of the round trip optical phase to polarization state that results from the use of a Faraday mirror, first noted by M. Martinelli. This invariance is very robust: the interferometric contrast can be very high (>99%) independent of optical-pulse duration, shape and bandwidth, and fiber and component dispersion, because the interfering components trace identical optical paths in opposite directions. These systems also have the virtue of relative simplicity, with a fairly low parts count and no need for active control loops.

Because of the asymmetry of plug and play systems, one of the two stations (e.g., Alice) may be significantly less expensive than the other. This works well with QKD network designs in which a single, more-expensive resource is placed at the center of a star topology, and the replicated less-expensive stations are placed at "customer" sites.

5. Unknowns/weaknesses

This approach is a heavily investigated approach and most aspects of the technology are well understood. Questions remain concerning integration with the telecommunications network, detector availability and optimization, maximum feasible distance, and key-generation rates. Security issues are still being investigated, and to date there have been few actual experimentally implemented attacks.

While many of these issues are common to both "plug and play" and "one-way" systems, the question of the security of "plug and play" systems needs additional work, even to allow specification of the required hardware (e.g., what optical filters, detectors, and discriminators are required by Alice and/or Bob to defeat probe attacks?). A recent paper that begins to address some of these questions is Reference [15].

Extension of this method to ranges of 100 km or greater is problematic. Work on exotic ultralow attenuation fibers is being carried out (notably at MIT), but even if successfully developed, cost and limited installation would likely restrict long-distance key generation over such fiber to a few highly critical applications.

Because plug and play systems put the source and detectors in a single entity (Bob), care must be taken that the bright outgoing pulses do not overwhelm detection of faint incoming pulses. To this end, it may be necessary to time-division-multiplex the fiber channel (e.g., send a train of bright pulses, and then cease transmitting bright pulses so the incoming reflections may be detected). In this approach, throughput will suffer due to duty factor reduction.

By their very nature, plug and play systems are not readily adaptable to employ single-photon sources when they become available. Their potential use with quantum repeaters, for increased distance, has not been investigated.

At present, there are no good detectors for QKD at telecommunications frequencies (1300 or 1550 nm). Existing InGaAs detectors have not been optimized for such weak signals, and suffer from poor quantum efficiency, high dark count, and/or serious after-pulsing issues. Detectors are a very serious issue for all QKD through telecommunications fiber.

6. Five-year goals

- Generally agreed theory of eavesdropping attacks and defenses in realistic "plug and play" systems
- Integration into telecommunications links and QKD networks
- Implementation over existing telecommunications networks on a point-to-point basis, with continuous key generation with >10,000 bits•sec^{-1} distilled key rates
- Full protocol implementation including authentication and protection against eavesdropping.

7. Ten-year goals:

- Source pulse rates of at least 1 GHz (requires much better detectors)
- Implementation over multiuser networks with any-to-any connectivity with metro-scale areas.
- Continuous key generation with >100,000 bits•sec^{-1} distilled key rates
- Integration with free-space systems to form hybrid QKD network
- Implementation of quantum-repeaters to extend distance to intercity distances (500 km).

8. Necessary achievements

Plug-and-play QKD based on weak laser pulses has been demonstrated in several operational systems, but considerable work will be required in order to achieve the five- and ten-year goals. Chief among them are continued advances in understanding security for realistic systems, breakthroughs in SPD technology, and experimentation with networked versions of weak-laser-pulse QKD.

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

Weak-pulse-over-fiber QKD would most benefit from improvements in detector technology (higher bias rates, higher detector efficiency, lower dark-count probability, reduced after-pulse probability). One can envision a weak-pulse fiber system that run at gigahertz rates, if workable detectors existed.

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

In principle, wide application of this approach for point-to-point links in metropolitan-sized areas is possible. Further analysis of how these systems could be integrated with networks is needed.

11. Role of theory/security-proof status for "Plug and Play" weak laser pulse systems through fiber

Although theory of 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 plug and play systems built from real (imperfect) equipment.

Security in "plug and play" systems is, in practice, different from those of "one-way" systems, and these differences require careful investigation. In "one way" systems, neither station is attached to the fiber by a fiber channel that is necessarily bidirectional; in "plug and play" systems, both are. Thus, it appears that Eve has significantly greater opportunities for active probing of Alice and Bob in "plug and play" systems.

C. References for Weak Laser Pulses over Fiber

[1] For a review, see:
N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–196 (2002).

[2] Townsend, P.D., J.G. Rarity, and P.R. Tapster, "Single photon interference in 10 km long optical fibre interferometer," *IEEE Electronics Letters* **29**, 634–635 (1993);
Townsend, P.D., "Secure key distribution system based on quantum cryptography," *IEEE Electronics Letters* **30**, 809–811 (1994).

[3] Gobby C., Z.L. Yuan, and A.J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters* **84**, 3762–3764 (2004).

[4] Townsend, P.D., "Quantum cryptography on multi-user optical fiber networks," *Nature* **385**, 47–49 (1997);
Townsend, P.D., "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *IEEE Electronics Letters* **33**, 188–190 (1997).

[5] Toliver, P., R.J. Runser, T.E. Chapuran, J.L. Jackel, T.C. Banwell, M.S. Goodman, R.J. Hughes, C.G. Peterson, D. Derkacs, J.E. Nordholt, L. Mercer, S. McNown, A. Goldman, and J. Blake, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photonics Technology Letters* **15**, 1669–1671 (2003).

[6] Muller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug & play systems for quantum cryptography," *Applied Physics Letters* **70**, 793–795 (1997).

[7] Bethune, D. and W. Risk, "An auto-compensating fiber-optic quantum cryptography system based on polarization splitting of light," *IEEE Journal of Quantum Electronics* **36**, 340–347 (2000).

[8] Bourennane, M., D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, and J.P. Ciscar, "Experimental long wavelength quantum cryptography: From single-photon transmission to key extraction protocols," *Journal of Modern Optics* **47**(2-3), 563–579 (2000); Bourennane, M., F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, "Experiments on long wavelength (1550 nm) "plug and play" quantum cryptography systems," *Optics Express* **4**(10), 383–387 (1999).

[9] Franson, J.D. and B.C. Jacobs, "Operational system for quantum cryptography," *IEEE Electronics Letters* **31**, 232–234 (1995).

[10] Franson, J.D., "Quantum cryptography," *Optics and Photonics News* **6**, 30–33 (1995).

[11] Franson, J.D., "Recent developments in quantum optics," *Johns Hopkins APL Technical Digest* **16**, 324–332 (1995).

[12] D. Stucki, D., N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New *Journal of Physics* **4**, 41.1–41.8 (2002).

[13] MagiQ of Somerville, MA, USA (http://www.magiqtech.com/), and Id Quantique SA; Rue Cingria, 10; 1205 Genève, Switzerland (http://www.idquantique.com).

[14] http://www.darpa.mil/ipto/programs/quist/.

[15] Vakhitov, A., V. Makarov, and D.R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics* **48**, 2023–2038 (2001).