

# A Quantum Information Science and Technology Roadmap

## Part 2: Quantum Cryptography Report of the Quantum Cryptography Technology Experts Panel

**“When elementary quantum systems...are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media.”**

**Charles H. Bennett and Gilles Brassard (1984)**

Disclaimer:

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

July 19, 2004

**Version 1.0**



## **Technology Experts Panel (TEP) Membership:**

Charles Bennett – IBM: Thomas J. Watson Research Center

Donald Bethune – IBM: Almaden Research Center

Gilles Brassard – University of Montréal

Nicholas Donnangelo – The MITRE Corporation

Artur Ekert – Cambridge University

Chip Elliott – BBN Corporation

James Franson – Johns Hopkins University, Applied Physics Laboratory

Christopher Fuchs – Bell Labs, Lucent Technologies

Matthew Goodman – Telcordia Technologies

*Chair:* Richard Hughes – Los Alamos National Laboratory

Paul Kwiat – University of Illinois at Urbana-Champaign

Alan Migdall – National Institute of Standards & Technology: Gaithersburg

Sae-Woo Nam – National Institute of Standards and Technology: Boulder

Jane Nordholt – Los Alamos National Laboratory

John Preskill – California Institute of Technology

John Rarity – University of Bristol

Produced for the Advanced Research and Development Activity (ARDA)

Document coordinator: Richard Hughes

Editing & 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

<b>EXECUTIVE SUMMARY</b> .....	<b>1</b>
<b>1.0 BACKGROUND: QUANTUM CRYPTOGRAPHY RESEARCH ROADMAP</b> .....	<b>1</b>
<b>2.0 INTRODUCTION: PURPOSE AND METHODOLOGY OF THE ROADMAP</b> .....	<b>2</b>
<b>3.0 HIGH-LEVEL ROADMAP DESIRED GOALS FOR QKD</b> .....	<b>3</b>
<b>4.0 ROADMAP MID-LEVEL VIEW</b> .....	<b>5</b>
<b>5.0 ROADMAP DETAILED-LEVEL VIEW</b> .....	<b>10</b>
<b>6.0 DETAILED SUMMARIES</b> .....	<b>11</b>
<b>7.0 THE PATH FORWARD</b> .....	<b>11</b>
<b>8.0 BRIEF OVERVIEW OF SALIENT FEATURES OF QKD</b> .....	<b>13</b>
<b>9.0 REFERENCES</b> .....	<b>17</b>
<b>APPENDIX A GLOSSARY OF TERMS</b> .....	<b>A-1</b>
<b>APPENDIX B REFERENCES FOR THE QKD ROADMAP</b> .....	<b>B-1</b>

## List of Tables

Table 4.0-1. Attributes of QKD Implementations.....	7
Table 4.0-2. QKD Implementation Development Status Metrics .....	9

## List of Acronyms and Abbreviations

ARDA	Advanced Research and Development Activity
BB84	“Bennett & Brassard 1984”
QCRC	Quantum Cryptography Research Conference
QIST	quantum information science and technology
QKD	quantum key distribution
TEP	technology experts panel



## EXECUTIVE SUMMARY

In our increasingly networked world, both the business and government sectors have ever-more demanding secure communications needs. Conventional information-assurance methods face increasing technological challenges and future threats, including unanticipated advances in mathematics, high-performance computing, and the possibility of large-scale quantum computation. For certain applications with an enduring information-assurance requirement, these concerns are highly relevant, and in these cases, it is essential to provide new secure-communications methodologies that have superior long-term security assurances. Also, new methods that provide improved ease-of-use and convenience will be highly desirable to meet future, increasingly complex network requirements to support dynamical reconfiguration of coalitions of users with multilevel security. Demands for bandwidth will continue to grow and new secure-communications technologies with the necessary speeds must be developed.

In a seminal paper published in 1984, Charles Bennett and Gilles Brassard (“BB84”) proposed [i] that the seemingly unrelated fundamental principles of quantum mechanics and information theory could be harnessed to provide powerful new information-assurance capabilities, capabilities impossible with conventional methods, which would be immune to future computational surprises—and would have other attractive security and ease-of-use attributes. Since then, research activity in this new field of quantum cryptography has undergone a tremendous growth—bringing together experimental and theoretical physicists, theoretical computer scientists, and electrical engineers, particularly in the subfield of quantum key distribution (QKD) [ii]. In 1991, Artur Ekert proposed a distinct route to quantum cryptography—harnessing the uniquely quantum-mechanical phenomenon of “entanglement” [iii]. In that same year, Bennett and colleagues published the results of the first proof-of-principle QKD experiment [iv], while John Rarity and colleagues demonstrated the essential feasibility of single-photon communications through the atmosphere [v]. In 1993, Paul Townsend and colleagues demonstrated the feasibility of quantum communications through conventional optical fiber [vi], and then in a 1995 publication, Bennett and colleagues placed the essential information-theoretic ingredient (“privacy amplification”) on a firm theoretical footing [vii]. Over the past decade, novel quantum cryptographic protocols have been proposed, important security proofs established, and experiments that implement the principles of QKD have been demonstrated in laboratories and universities around the world. Quantum cryptography, together with its sister field of quantum computation, is now one of the most active and healthy research areas of modern science, attracting substantial basic-research investments from funding organizations in many countries, and at the time of this writing, the first commercial products are beginning to appear. Yet today, 20 years since the publication of the BB84 paper, this emerging technology remains largely inaccessible to those outside of its community of researchers, and almost no experimental investigations of protocols beyond QKD have been made. As such, its relevance to the larger community of information-security researchers and its ability to address important information-assurance needs and provide solutions to relevant problems remains underdeveloped.

To facilitate the progress of quantum-cryptography research towards a practical “quantum information-assurance era” in which quantum cryptography becomes more closely integrated with conventional, basic, and applied information-security and communications research, a two-day “quantum cryptography technology experts panel (TEP) meeting” (membership listed

on the inside front cover) was held in Warrenton, Virginia in June 2003, with the objective of developing a research roadmap. The panel's members decided that a desired objective for the field should be:

“to develop by 2014 a suite of practical quantum cryptographic technologies of sufficient maturity, accessibility, and robustness that they can, either as stand-alone systems or when seamlessly integrated with conventional information assurance methods, provide new, secure communications tools, which can be evaluated as value-added ingredients of future secure communications solutions with consistent and demonstrable benefits.”

The panel's members emphasize that although this is a desired outcome, not a prediction, they believe that it is attainable as a collective effort if the momentum in this field is maintained with focus on this objective, with cooperative interactions between different experimental approaches and theory, and through engaging the traditional (basic and applied) information-assurance and communications research communities. The intent of this roadmap is to set a path leading to the desired quantum information-assurance objective by 2014 by providing some direction for the field with specific high-level technical goals. A second function of the roadmap is to enable informed decisions about future directions to be made by tracking progress and elucidating interrelationships between approaches, which will assist researchers to develop synergistic solutions to obstacles within any one approach. The roadmap will be a living document that will be updated annually; it is expected that there will be significant changes in both content and structure. While recognizing the tremendous breadth of activities within quantum cryptography, the TEP members decided to focus predominantly on the topic of QKD for this Version 1.0 of the roadmap. The TEP members intend to extend the scope of the roadmap to non-QKD quantum cryptographic protocols in future versions.

QKD allows two parties (traditionally referred to as Alice and Bob) to produce the shared, secret random bit sequences, which are required for secure communications [viii], through a combination of quantum and conventional communications. The security of this procedure is based on an interplay between incontrovertible, well-tested principles of quantum physics and information theory. Today, QKD can be performed experimentally through dedicated optical fibers (over metro-area distances) and across multikilometer line-of-sight (“free-space”) paths. In addition to stand-alone applications, this suggests that QKD might be integrated at the physical layer with optical communications to provide the cryptographic foundation for secure communications. However, few experimental demonstrations have included all of the ingredients of a full QKD protocol, and their focus has been almost exclusively on closing the gap between the idealized assumptions of “theoretical secrecy” proofs for QKD and the realities of imperfect realizations of fundamental quantum processes. Much can and should continue to be learned from these explorations of theoretical secrecy, which shed considerable light on the foundations of cryptography. But as the technology continues to evolve into more mature physical instantiations, it is apparent that QKD is capable of significantly and positively impacting information-security requirements without insisting on theoretically perfect secrecy from inevitably imperfect physical realizations. It is now time to also consider such “practical secrecy” roles for QKD from a complete information-security and communications systems perspective if this technology is to reach a sufficient maturity to meet future needs. Two distinct practical roles for QKD are possible within future networked optical communications infrastructures:

- “key-transfer-mode QKD”: an enhancement to conventional key-management infrastructures supporting the transfer or generation of keys for symmetric-key cryptography
- “encryptor-mode QKD”: a new, physical layer encryption technology (a “quantum generated Vernam or one-time-pad stream cipher” [ix]).

The roadmap sets out specific, high-level desired three-, six- and ten-year research goals for QKD of increasing scientific, technological, and practical sophistication. These goals will stimulate the necessary basic theoretical and experimental physics research and advances in the enabling component technologies, while engaging the information-assurance and communications research communities, so that systems-level, architectural aspects of QKD-supported secure communications can be characterized and evaluated in a prototype setting. The three-year goal will build on existing “first wave” QKD capabilities to integrate them within networked optical communications testbeds at the physical layer, and with key-management infrastructures. The six-year goal will project “second wave” QKD as a new encryption technology in networked optical-communications environments, using advanced quantum light sources now being developed in physics laboratories. The ten-year goal would extend QKD into the quantum information-assurance regime, in which QKD could become a seamlessly integrated ingredient of a key-management/encryption solution for optical-communications networks, setting the stage for applications of QKD in satellite communications and both metro-area and long-haul optical-fiber networks. These high-level goals are ambitious but attainable as a collective effort with cooperative interactions between different experimental approaches, theory, device developers, and the conventional information-assurance and communications research communities.

To this end, the roadmap presents a “mid-level view” that segments the field into the different scientific approaches and provides a brief narrative to capture the promise and characterize progress towards the high-level goals within each approach. A “detailed-level view” incorporates summaries of the state-of-progress within each approach, provides a timeline for likely progress and attempts to capture its role in the overall development of the field. A summary section provides some recommendations for moving toward the desired goals.

The quantum information-assurance destination that we envision in this roadmap will enable powerful new capabilities for solving future networked, secure-communications needs, offering improved convenience, ease-of-use, and unprecedented long-term security assurances. The journey to this destination will lead to many new scientific and technological developments with intellectual, societal, and economic benefits. Component technologies such as quantum light sources, single-photon detectors, quantum repeaters, and “quantum friendly” network components will be developed that will be enabling technologies for other quantum-cryptographic, quantum communications, and quantum computational applications. We anticipate that there will be considerable synergy with nanotechnology and optical communications and networking. The journey ahead will be challenging, but it is one that will lead to unprecedented advances in both fundamental scientific understanding and practical new technologies. This roadmap will be a living document, updated on an annual basis to reflect progress. The roadmap panel also intends to extend the scope of the roadmap to other aspects of quantum cryptography in future versions.

**References**

- [i] Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
- [ii] For reviews, see:  
N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–196 (2002);  
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>).
- [iii] Ekert, A.K., "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663 (1991).
- [iv] Bennett, C.H. *et al.*, "Experimental quantum cryptography," *Journal of Cryptology* **5**, 3–31 (1992).
- [v] Seward, S.F., P.R. Tapster, J.G. Walker, and J.G. Rarity, "Daylight demonstration of a low-light-level communication system using correlated photon pairs," *Journal of Optics B: Quantum and Semiclassical Optics* **3**, 201–207 (1991).
- [vi] Townsend, P.D., J.G. Rarity, and P.R. Tapster, "Single photon interference in 10 km long optical fibre interferometer," *Electronics Letters* **29**, 634–635 (1993).
- [vii] Bennett, C.H., G. Brassard, C. Crépeau, and U.M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory* **41**, 1915–1923 (1995).
- [viii] For a review, see:  
Menezes, A. *et al.*, *Handbook of Applied Cryptography*, (CRC Press, Boca Raton, Florida, 1997).
- [ix] Vernam, G.S. "Cipher printing telegraph systems," *Transactions of the American Institute of Electrical Engineers* **45**, 295 (1926).



## 1.0 BACKGROUND: QUANTUM CRYPTOGRAPHY RESEARCH ROADMAP

Cryptography, the science of secret communications [1], has a long and distinguished history since at least the time of the ancient Greeks [2], and today is widely used (often unobtrusively) in our everyday lives, as well as in its more traditional venues of military and diplomatic communications. Starting from the seminal work of Shannon in 1949 [3], a formal mathematical foundation for cryptography has been developed from the disciplines of information theory and more recently number theory, which has allowed a deep understanding to be developed for how cryptography can provide the security services required for information assurance [4]

- confidentiality,
- authenticity,
- integrity,
- availability, and
- nonrepudiation.

Implicit in classical approaches is that a single bit of information is ultimately represented by some physical quantity (an ink mark on piece of paper, or a magnetized region on a computer hard drive for instance) that obeys the laws of classical physics. Of particular relevance to cryptography, an adversary could, in principle, copy or passively monitor classical information without altering it, preserving it for future analysis by (potentially) much more sophisticated techniques. However, during the late 1970s and early 1980s several investigators, including Wiesner [5], Feynman, and others, began to investigate (theoretically) the possibility that a bit of information could be encoded into two-level quantum systems, such as the vertical or horizontal polarization states of a single photon to represent a zero or a one, respectively. Through the Heisenberg uncertainty principle and the superposition principle, quantum physics introduces new features to information science: in general such a quantum bit, or qubit for short, can neither be faithfully copied nor monitored, and any attempt to do so will inevitably and irreversibly alter it. These features were suggestive of a possible role for quantum information in cryptography and in a 1984 publication (“BB84”) Charles Bennett and Gilles Brassard proposed [6] that quantum communications could provide information assurance capabilities that would be impossible to achieve according to the principles of classical information theory.

Since the publication of the seminal BB84 paper, research activity in developing the theoretical foundations of both quantum communications and quantum cryptography has undergone a tremendous growth. In 1991, Ekert showed [7] how the uniquely quantum-mechanical property of entanglement could be harnessed to provide even greater levels of quantum security. By the early-to-mid 1990s, methods of experimental quantum physics and quantum technology had advanced sufficiently to allow laboratory study of quantum information, and multiple experiments have since been performed to study one class of quantum cryptographic protocols in particular, collectively known as quantum key distribution (QKD). Through these experiments, new insights into the theoretical capabilities of quantum cryptography have been obtained and this field has become one of the most active and intellectually vigorous of modern science attracting considerable research investments as well as leading researchers in most of the developed countries in the world. Yet, in spite of this remarkable 20-year history, much research

remains to be done in quantum cryptography for it to achieve its potential of providing solutions to practical information assurance requirements:

- The full theoretical potential of the field remains to be defined.
- Considerable gaps exist between the idealized, theoretical quantum information concepts and the realities of experimental quantum capabilities.
- Dedicated links have been used for QKD experiments, leaving almost unaddressed the important issue of co-existence of the delicate quantum signals with conventional communications traffic in a network environment.
- Potential practical uses of quantum cryptography are relatively unexplored owing to the inaccessibility of the technology to the conventional information assurance and communications research communities.
- Protocols for extending QKD beyond point-to-point links have received little attention.
- Almost no experimental studies have been made of protocols beyond QKD.

In parallel with these developments, our increasingly networked world has ever-more-demanding information assurance needs in both the business and government sectors. While conventional methods continue to meet these demands, they face increasing technological challenges, including

- unanticipated advances in mathematics, high-performance computing and the possibility of large-scale quantum computation that threaten the security of today's communications.
- increasingly complex future secure network communications requirements to support dynamical reconfiguration of coalitions of users with multi-level security.
- projections for ever greater secure communications bandwidth requirements

Quantum cryptography has the potential to counter these threats and help to meet these future needs with new tools for the secure communications toolbox, if it can reach a stage of sufficient maturity that its information assurance attributes can be evaluated, compared and contrasted with conventional methodologies. The purpose of this roadmap is to help realize this potential by setting out an agenda in both fundamental and applied research and systems engineering that will help quantum cryptography evolve from its present "physics+ information theory" form to a "quantum information assurance" era over the next decade. This will allow these new tools to be considered alongside and integrated with their conventional counterparts as ingredients of future information assurance solutions.

## **2.0 INTRODUCTION: PURPOSE AND METHODOLOGY OF THE ROADMAP**

This roadmap has been formulated and written by the members of a Technology Experts Panel (TEP), consisting of internationally recognized researchers (see inside front cover page) in quantum information science and technology, who held a kick-off meeting in Warrenton, Virginia in early June 2003 to develop the underlying roadmap methodology. The TEP held a further meeting in conjunction with the annual ARDA Quantum Cryptography Research Conference (QCRC) meeting in Wye River, Maryland in September 2003. At the Warrenton meeting the TEP members decided that the overall purpose of the roadmap should be to set as a desired future objective for quantum-cryptography research

“to develop by 2014 a suite of viable quantum-cryptographic technologies of sufficient maturity, accessibility, and robustness that they can, either as stand-alone systems or when seamlessly integrated with conventional information assurance methods, provide new, secure communications tools, which can be evaluated as ingredients of future secure communications solutions with consistent and demonstrable benefits.”

The roadmap is intended to function in several ways to aid this development. It has a prescriptive role by identifying what scientific, technology, skills, organizational, investment, and infrastructure developments will be necessary to achieve the desired goal, while highlighting options for how to get there. This roadmap also has a descriptive function by capturing the status and likely progress of the field, while elucidating the role that each aspect of the field is expected to play toward achieving the desired goal. The roadmap can identify gaps and opportunities, and places where strategic investments would be beneficial. It will provide a framework for coordinating research activities and a venue for experts to provide advice. The roadmap will therefore allow informed decisions about future directions to be made, while tracking progress, and elucidating interrelationships between approaches to assist researchers to develop synergistic solutions to obstacles within any one approach. The roadmap is intended to be an aid to researchers as well as those managing or observing the field.

Underlying the overall objective for the quantum cryptography roadmap, the panel members decided on a four-level structure with a division into “high level goals”, “mid-level descriptions”, “detailed level summaries” and a final summary that includes the panel’s recommendations for optimizing the way forward. Although this roadmap document is not intended to serve as a scientific review paper of the subject, a brief account of the salient aspects of the field is included for completeness. However, the sheer diversity and rate of evolution of this field, which are two of its significant strengths, made this a particularly challenging exercise. To accommodate the rapid rate of new developments in this field, the roadmap will be a living document that will be updated annually, and at other times on an *ad hoc* basis if merited by significant developments. Certain topics will be revisited in future versions of the roadmap and additional ones added; it is expected that there will be significant changes in both content and structure. While recognizing the tremendous breadth of activities within quantum cryptography, the TEP members decided to focus predominantly on the topic of QKD for this Version 1.0 of the roadmap. The TEP members intend to extend the scope of the roadmap to non-QKD quantum cryptographic protocols in future versions.

### **3.0 HIGH-LEVEL ROADMAP DESIRED GOALS FOR QUANTUM KEY DISTRIBUTION**

QKD allows two parties (traditionally referred to as Alice and Bob) to produce shared, secret random-bit sequences, which are required for secure communications, through a combination of quantum (“single photon”) and conventional communications. The success of the technique is contingent upon robust methodologies for locating the quantum signals out of a very strong background. The security of this procedure is based on an interplay between incontrovertible, well-tested principles of quantum physics and information theory. Today QKD can be performed experimentally through dedicated optical fibers (over metro-area distances) and across multi-kilometer line-of-sight (“free-space”) paths for point-to-point links. This suggests that in

addition to stand-alone applications, QKD might be integrated at the physical layer with optical communications infrastructures to provide the cryptographic foundation for secure communications, but:

- few experimental demonstrations have included all of the ingredients of a full QKD protocol
- ranges, rates and availability have been limited
- predominantly point-to-point connectivity has been considered, with little investigation of network support issues
- there has been little effort to explore how QKD could co-exist with conventional network traffic in either transparent optical fiber networks or free-space optical links
- integration of QKD with conventional cryptographic and secure communications architectures has received scant attention
- practical, systems-level security attributes of and roles for QKD remain largely unexplored.

Following Shannon [3] we may distinguish two concepts of secrecy: “theoretical secrecy” and “practical secrecy.” Theoretical secrecy focuses on what may be rigorously proved regardless of an adversary’s assumed technological capabilities, and sheds much light on the foundations of cryptography. QKD demonstrations have been almost exclusively concerned with closing the gap between the idealized assumptions of theoretical secrecy proofs for QKD and the realities of imperfect realizations of fundamental quantum processes. Much can and should continue to be learned from these explorations of theoretical secrecy, but no real system operated by human beings can ever attain this ultimate goal in practice. “Practical security” is concerned with security against adversaries who have large, but ultimately limited, present-day and future resources. In this context, QKD has attractive features including an intrinsic immunity to the possibility of quantum computational or other future computational surprises that must be faced by conventional public-key cryptography. It is now time to consider practical-secrecy roles for QKD if the security advantages of this technology can evolve to a sufficient maturity to meet future needs. This will require that the theoretical secrecy based QKD protocols be re-examined within a complete information security system perspective. At least two distinct practical roles for QKD are possible within future networked optical communications infrastructures

- “key-transfer-mode QKD”: an enhancement to conventional key management infrastructures supporting the transfer or generation of keys for symmetric key cryptography
- “encryptor-mode QKD”: a new, physical layer encryption technology (a “quantum generated Vernam or one-time-pad stream cipher” [8]).

As currently implemented in the majority of (“first wave”) experiments using highly attenuated laser light sources, QKD is too slow to meet the concept of its originators as an encryptor (stream cipher) in practical settings. Instead, this type of QKD could be used in a hybrid mode to transfer (or generate) the relatively short keys required for practical symmetric key cryptography such as the Advanced Encryption Standard. This type of QKD could therefore be considered as an enhancement to key management infrastructures. However, the first experiments are now beginning to appear suggesting that in other forms QKD might be possible at the rates necessary for use directly as a physical layer (quantum optical, one-time-pad) encryption tech-

nology. Furthermore, advanced quantum light sources now being studied in physics laboratories open up the possibilities of intrinsically quantum-mechanical random-number generation and superior security assurances in “second wave” QKD implementations, which use single-photon, entangled-photon pair or continuous variable sources. Research into quantum repeaters suggests that long-haul optical fiber implementations of QKD might be possible.

The panel members decided on specific ambitious, but attainable, high-level technical goals for QKD as both a key management tool and as a new encryption technology within networked optical communications environments. These technical goals set a path for the field to follow that will lead to the desired quantum information assurance era by 2014. The specific desired high-level goals are

- by 2007: to implement networked, secure communications testbeds over metro-area distances in optical fibers and over free-space optical communications paths using “first wave” QKD-enhanced key management;
- by 2010: to implement networked, secure communications testbeds using (“second wave”) advanced light source QKD encryption, in optical fibers over metro-area distances, and over few-kilometer free-space optical-communications paths
- by 2014: to develop integrated QKD-based key management and encryption to support secure networks from intra-net scale to long-haul optical fiber and satellite optical communications.

The 2007 desired high-level goal sets challenging targets for QKD approaches for networking, transmission distance, integration with conventional key management architectures, and co-existence with conventional communications traffic. While building from present-day “first wave” QKD experimental capabilities, this goal will stimulate the necessary engagement of the communications research and information assurance communities, and require the quantum information community to research the theoretical security aspects of QKD in this new setting. The 2010 desired goal further extends these challenges with the additional requirements for a several-orders-of-magnitude increase in speed. Achieving this goal will require the additional engagement of the fundamental quantum optics research and device fabrication communities. Approaches that attain the 2007 or 2010 desired goals will be well-positioned to strive for the long-haul objectives of the 2014 desired goal. By setting these challenging yet attainable goals the TEP hopes to stimulate the necessary fundamental research, component developments and systems engineering that will be essential for reaching the desired quantum information assurance era. The potential advantages of QKD can then be evaluated and compared with conventional information assurance methods.

#### **4.0 ROADMAP MID-LEVEL VIEW**

The purpose of the roadmap’s mid-level view is to provide an overview of both the potential and the development status of the various approaches to quantum key distribution. In contrast with conventional, algorithmic methods of key transport or cryptography, QKD is a physical layer technology, and as such its performance depends on both the method of implementing the quantum physical aspects as well as the properties and quality of the quantum transmission channel. Present day quantum technologies effectively constrain implementations of QKD to optical wavelengths and the optical fiber and free-space optical (FSO) communications media in

particular. A first level of segmentation is to characterize QKD approaches based on the choice of quantum light source, with: a “first wave” utilizing highly attenuated weak laser pulses containing on average less than one photon per pulse; and a “second-wave” using “single-photon” light sources, or entangled photon pairs, or continuous variable quantum states. Each of these approaches has its own “attributes” that make it appealing in one or more respects. For example, weak laser pulse QKD can be implemented with largely commercial-off-the-shelf (COTS) components, while entangled photon pair-based QKD offers additional theoretical security advantages, and continuous variable QKD may allow for higher speeds. To compare and contrast the relative attributes of the different approaches to QKD, the panel members devised a common set of relevant “attributes” and “scores”, along with a table to display their status in summary form. It is important to note that the characterizations of each approach are collective statements about an entire segment of QKD research - no single embodiment of that approach may realize all of the attributes at the stated levels – and that the scores are relative statements between QKD approaches. Specifically, a “low” score for a QKD approach for one attribute merely indicates that it is less suited in this one respect than some other approach.

The five attributes that the panel has chosen as characteristic of approaches to QKD are

1. **Relative theoretical security status.** The score for this attribute is a reflection of both the depth and breadth of analyses of the theoretical security of an approach, as well as the extent to which implementations approach the assumptions of the analyses. For example, entangled photon pair approaches receive a “high” score because of the intrinsic source self-checking feature, whereas continuous variable approaches receive a “low” score because their theoretical security analyses are less developed.
2. **Relative transmission distance potential.** Because QKD is a physical layer technology its performance (secret bits generated per unit time) is dependent on the quality of the quantum channel. Although quite robust in that error rates on the quantum transmissions in the percent range can be tolerated, the amount of (conventional) error correction required to correct these errors reduces the overall yield of secret bits and ultimately imposes a lower bound on transmission quality. Below this bound no secret bits can be generated even though quantum communications may still be performed. Some approaches are intrinsically more capable of tolerating lower quality quantum channels than others and hence have better transmission distance potential.
3. **Relative speed potential.** The speed (numbers of secret bits generated per second) of a QKD approach is a function of the quality of the quantum channel and the clock rate, but some approaches are intrinsically capable of higher rates than others, owing to lower post-processing overhead for instance. Also some sources are more likely to support higher rates than others.
4. **Relative maturity.** Some approaches to QKD have been under experimental investigation for as much as a decade, and are correspondingly more mature than others of more recent origin. In addition, this attribute is intended to capture both the ease-of-use and construction of a QKD approach. For example, an approach that requires a large proportion of non-COTS ingredients or requires highly-trained personnel (PhD-level physicist) to operate a system would receive a “low” score.

5. **Relative robustness.** This attribute is intended to capture the reliability of a QKD approach and how robust it is against variations in the operating parameters such as loss or noise on the quantum channel.

**Table 4.0-1.**  
**Attributes of QKD implementations**

QKD Implementation	Attributes				
	1	2	3	4	5
Weak laser pulses	M	H	H	M	M
Single-photon source	H	H	M	L	M
Entangled pairs	H	H	M	M	M
Continuous variables	L	L	H	L	L

Attributes:

1. Relative theoretical security status
2. Relative transmission distance potential
3. Relative speed potential
4. Relative maturity
5. Relative availability

Scores:

- L** = low  
**M** = medium  
**H** = high




These attributes will be updated in future revisions of the roadmap. Table 4.0-1 presents a snapshot of the variety of approaches being pursued: each approach has its own particular strengths and weaknesses that will ultimately determine its suitability for the desired roadmap high-level goal applications. However, the attributes alone do not adequately characterize the state of QKD research and development. The panel decided on a second mid-level table of “development status metrics” for QKD approaches, to characterize their progress toward the roadmap high-level desired goals. For this purpose, it was decided to make a second segmentation of approaches to QKD, to separate them into either optical fiber-based or line-of-sight through an atmospheric path (“free space”) ones, because the challenges and implementation issues in each case are quite distinct. For example, for lowest losses in present-day optical fiber implementations, photon wavelengths need to be constrained to either the 1,310-nm or 1,550-nm telecommunication bands. However, this constraint leads to the challenging issue of high-efficiency, low-noise single-photon detection at these near infra-red wavelengths. In contrast, in free-space QKD several low-loss wavelength regions are available, some of which coincide with well-developed single-photon detection technologies. Free-space QKD faces other challenges, however, associated with optical acquisition, pointing, and tracking (APT) to establish and maintain the quantum channel, as well as stringent synchronization demands.

Within each implementation environment the TEP decided on seven development-status metrics for QKD approaches. There are three “ingredients” metrics and four “systems level” metrics, as follows:

1. **Quantum physics implementation maturity.** This metric captures the extent to which the fundamental quantum communications aspects of the particular QKD approach have been demonstrated within an implementation environment.
2. **Classical protocol implementation maturity.** This metric captures the completeness with which the essential classical post-processing parts of the QKD approach have been demonstrated within an implementation environment.
3. **Maturity of components and operational reliability.** This metric captures the status of the light sources, detectors, other electro-optical, optical and electronic components, and random number generation ingredients of a QKD approach, as well as the ease-of-use and quality-of-service of a QKD approach within an implementation environment.
4. **Practical security.** This metric captures the extent to which practical security of a QKD approach has been implemented and evaluated.
5. **Key transfer readiness.** This metric captures the extent to which the interface between a QKD system and key transport/generation of symmetric cryptographic keys has been developed. Target secret bit rates for these purposes are at least 100 bits per second. “Sufficient demonstration” would include incorporation of the QKD approach within a key management architecture.
6. **Network readiness.** This metric characterizes the development of a QKD approach beyond a point-to-point configuration as well as its integration and co-existence with conventional network traffic.

7. **Encryptor readiness.** This metric captures the extent to which an interface for a QKD approach to provide one-time-pad based encryption has been developed. Target secret bit rates required for QKD to be useful as an encryption technology are several orders of magnitude higher than for key transport/generation.

Each metric is scored on a three-level basis:

-  = sufficient demonstration
-  = preliminary status achieved, but further work is required
-  = no experimental demonstration

Because QKD is a physical-layer technology, its performance depends on properties of the quantum channel including attenuation, background noise and time-dependence of these and other features. Different implementation environments present strikingly different challenges for QKD. The TEP decided to characterize the development status of QKD approaches for each of four “implementation environments”, characteristic of the different challenges involved in practice. The implementation environments are:

1. Laboratory or local-area distances (< 200 m)
2. Campus distances (< 2 km)
3. Metro-area distances (< 70 km)
4. Long distances (> 70 km)



Table 4.0-2. QKD Implementation Development Status Metrics

QKD Implementation Status	Laboratory or local-area distances (< 200 m)							Campus-area distances (< 2 km)						
	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	2.3	2.4	2.5	2.6	2.7
Optical fiber	Weak laser pulses													
	Single-photon source													
	Entangled pairs													
	Continuous variables													
Free-space	Weak laser pulses													
	Single-photon source													
	Entangled pairs													
	Continuous variables													
QKD Implementation Status	Metro-area distances (< 70 km)							Long distances (> 70 km)						
	3.1	3.2	3.3	3.4	3.5	3.6	3.7	4.1	4.2	4.3	4.4	4.5	4.6	4.7
Optical fiber	Weak pulses													
	Single-photon source													
	Entangled pairs													
	Continuous variables													
Free-space	Weak laser pulses													
	Single-photon source													
	Entangled pairs													
	Continuous variables													

Legend: = sufficient demonstration  
 = preliminary status achieved, but further work is required  
 = no experimental demonstration

As was previously stated, different implementation environments present strikingly different challenges for QKD. For example, a “dark” optical fiber dedicated to QKD quantum transmissions over a short distance within a single building is a much more benign environment than a metro-area all-optical fiber network with optical amplifiers, switches and other network traffic on the same fiber. For this reason, the TEP has characterized the development status of QKD approaches for each of four implementation environments. Some specifics of these implementation environments are:

1. **Laboratory or local-area distances (< 200 m).** This category captures both proof-of-principle laboratory demonstrations and “intranet” prototype implementations.
2. **Campus distances (< 2 km).** The extension to relatively short fiber or line of sight transmission distances brings in new challenges beyond those of the relatively benign local-area environment. For example, a line-of-sight implementation would need to cope with strong background levels, while an optical fiber implementation would need to be compatible with a passive optical network environment.
3. **Metro-area distances (< 70 km).** Over these distances line-of-sight QKD faces new challenges associated with acquisition, pointing and tracking and fiber-based implementations must be compatible with the all-optical network environment. Both fiber and line-of-sight approaches face challenging synchronization demands.
4. **Long distances (> 70 km).** The fourth environment category covers both long-haul fiber links and earth-to-satellite and inter-satellite QKD.

The development-status metrics will be revised at each roadmap update to reflect research advances. From Table 4.0-2 it can be seen that the roadmap 2007 desired high-level goal corresponds to achieving metrics 3.1–3.6 for weak laser pulse approaches in the metro-area implementation environment, whereas the 2010 goal corresponds to achieving metrics 3.1–3.7 for second wave approaches.

## 5.0 ROADMAP DETAILED-LEVEL VIEW

The roadmap includes more detailed information with several summary sections.

1. **Implementation summaries.** For each of the approaches to QKD a detailed-level summary provides a short description of the approach, along with explanations of the graphical representation of the metrics in the mid-level view and descriptions of the likely developments over the next decade. A common set of points are addressed in each summary:
  - who is working on this approach,
  - the location,
  - a brief description of the essential idea of the approach and how far it is developed,
  - a summary of the attributes of the approach,
  - a list of what has been accomplished, when it was accomplished, and by whom, for the development status metrics
  - the “special strengths” of this approach,
  - the unknowns and weaknesses of this approach,

- the 5-year goals for this approach,
- the 10-year goals for this approach,
- the necessary achievements to make the 5- and 10-year goals for the approach possible,
- what developments in other areas of QIST or other areas of science will be useful or necessary in this approach,
- how will developments within this approach have benefits to others areas of QIST or other areas of science in general, and
- the role of theory in this approach.

**Note:** The TEP decided that assessments of individual projects within an approach would not be made a part of the roadmap because this is a program-management function.

2. **Theory summary.** In addition to the theory component of the detailed-level summary for each approach, there is a separate summary for fundamental theory. This summary provides historical background on significant theory contributions to the development of quantum cryptography and also spells out general areas of theoretical work that will be needed on the way to achieving the 2007 and 2010-year high-level goals.

## 6.0 DETAILED SUMMARIES

The roadmap includes the following detailed summary sections:

- QKD Implementations
  - Weak laser pulses in fiber (C. Elliott and D. Bethune)
  - Weak laser pulses in free-space (R. Hughes, J. Nordholt and J. Rarity)
  - Entangled photon QKD (P. Kwiat and J. Rarity)
  - Single-photon source QKD (S.-W. Nam)
  - Continuous variable QKD (J. Rarity)
- QKD Theory (C. Bennett, G. Brassard, A. Ekert, C. Fuchs and J. Preskill)

Additional sections on detectors and architectures will be added in the near future.

## 7.0 THE PATH FORWARD

Major strengths of quantum cryptography research are the breadth of concepts being pursued, the high level of experimental and theoretical innovations, the quality of the researchers involved, and the very encouraging rate of progress and level of achievements. The desired 2014 QKD destination and the high-level goals that are set out in this roadmap, although ambitious, are within reach if experimenters and theorists work together, appropriate strategic basic research is pursued, relevant technological developments from closely related fields are incorporated, and the conventional information assurance and communications research communities actively engaged.

In developing this document the TEP members have noted several areas where additional attention, effort, or resources would be advantageous.

- **Theoretical security:** the TEP members encourage research to further close the gap between the assumptions of rigorous security proofs for QKD and the inevitably imperfect realizations of the underlying quantum of experimental approaches.
- **Practical security** of QKD has received almost no attention but is essential if it is to become an information assurance tool as envisioned in this roadmap. The TEP encourage QKD researchers to engage the information assurance and security engineering communities to explore how to integrate QKD with conventional secure communications infrastructures.
- **Robust synchronization** is the essential hardware foundation for QKD, and significant advances in this area will be required to support the demands of a high-speed quantum generated one-time-pad.
- **Protocol development:** The TEP encourages additional research effort into the three information theoretic ingredients of QKD: authentication, error correction and privacy amplification. Authentication is the foundation on which QKD's information assurance capabilities are built. Research into authentication architectures to support QKD in a network setting will be essential. Efficient forward error correction algorithms capable of operating close to the Shannon limit will be essential for using QKD as an encryptor. Fast privacy amplification algorithms are likewise necessary.
- **Entanglement based QKD** appears to offer additional security features over single-photon based schemes, but has not received a correspondingly high level of theoretical analysis or experimental investigation.
- **Components:** There is a need for fast, efficient, low-noise, low dead-time, low-jitter, photon number resolving detectors at both optical and telecom wavelengths. Likewise, fast, high-rate, narrow bandwidth single photon and entangled photon pair light sources need to be developed at both optical and telecom wavelengths. The device fabrication community should be engaged to more effectively pursue the necessary research.
- **Quantum repeater development:** In addition to enabling long-haul optical fiber QKD quantum repeater development along with quantum memory would open up the larger field of experimental quantum communications
- **Network architectures:** The communications research community should be engaged to explore how to most effectively use QKD to support secure, scalable network communications. In parallel, research to take QKD implementation beyond point-to-point topologies should be encouraged.
- **Optical communications:** The possibility that QKD could be incorporated as a physical layer cryptographic foundation to secure optical communications should be explored.
- **Evaluation:** Conventional cryptographic are frequently evaluated according to nationally or internationally accepted practices, relative to accepted standards. It will be useful to develop standards and evaluation methodologies for QKD.

Much could be learned by setting up dedicated QKD testbeds in the fairly benign environments of either local area or campus area settings before setting out to reach the roadmap desired goals. Such a testbed would provide an opportunity to explore the communications research,

information assurance, security engineering and device fabrication aspects of QKD in a network environment. Hardware-based experimentation should proceed in conjunction with end-to-end system modeling and sensitivity analyses.

The desired developments set out in this roadmap cannot happen without an adequate number of highly skilled and trained people to carry them out. The panel believes that additional measures should be adopted to ensure that an adequate number of the best physics, mathematics, and computer-science graduate students can find opportunities to enter this field, and to provide a career path for these future researchers. Additional graduate-student fellowships and postdoctoral positions are essential, especially in experimental areas, and there is a need for additional faculty appointments, and the associated start-up investments, in quantum information science.

The quantum information assurance destination that we envision in this roadmap will open up fascinating, powerful new secure communications capabilities. The journey to this destination will lead to many new scientific and technological developments with myriad potential societal and economic benefits. Quantum light sources will be developed that will be enabling technologies for other applications, and the quantum communications techniques will open the door to other new quantum technologies. The journey ahead will be challenging but it is one that will lead to unprecedented advances in both fundamental scientific understanding and practical new technologies.

## **8.0 BRIEF OVERVIEW OF SALIENT FEATURES OF QUANTUM KEY DISTRIBUTION**

The science of cryptography provides two parties (“Alice” and “Bob”) with the ability to communicate with long-term confidentiality: they have the assurance that any third party (an eavesdropper, “Eve”) will not be able to read their messages. Using symmetric key cryptography Alice can encrypt a message (“plaintext”),  $P$ , before transmitting it to Bob, using a cryptographic algorithm,  $E$ , to produce a “ciphertext”,  $C = E_K(P)$ . Here  $K$  is a secret parameter, known as a cryptographic key, used to specify a particular instance of  $E$ . Keys are typically random binary number sequences. For instance, in the unconditionally secure one-time pad (or Vernam cipher) the key contains as many bits as the plaintext, and encryption and decryption proceed by modulo 2 addition (“XOR”) in which each bit of the plaintext is added to each bit of the key, but dropping any “carry” bits. On the other hand, in the modern Advanced Encryption Standard (AES) for instance, entire messages are encrypted with keys that are up to 256 bits in length. Upon reception of the ciphertext transmission, Bob is able to invert the encryption process using the decryption algorithm,  $D$ , to recover the original message,  $D_K(C) \equiv P$ , provided he too knows the secret key,  $K$ . Although the encryption and decryption algorithms  $E$  and  $D$  may be publicly known, Eve passively monitoring transmission  $C$  would be unable to discern the underlying message,  $P$ , because of the randomization introduced by the encryption process—provided the cryptographic key,  $K$ , remains secret. The algorithms  $E$  and  $D$  are designed so that without knowledge of  $K$  Eve’s best strategy is no better than an exhaustive search over all possible keys: a computationally infeasible task, even with a quantum computer. (Symmetric key cryptography can also provide Alice and Bob with the distinct information security service of authentication: they can verify that they are communicating with each other and that their

messages have not been altered.) In symmetric key cryptography, the secrecy of key material is of paramount importance, but there is an underlying problem: before Alice and Bob can communicate securely it is essential that they have a method of securely distributing their keys.

Today, public key cryptography is widely used to distribute the keys for symmetric key cryptosystems, but public key methods possess a latent, retroactive vulnerability to future computational surprises. For instance, in 1977 *Scientific American* presented a code-breaking challenge to its readers: a short encrypted message was published, along with the 129-digit “public key” that had been used in its encipherment [9]. By finding the two, secret prime number factors of this large number (known as RSA129) it would be possible to recover the original message, but the inventors of this (now widely used RSA cryptosystem) estimated that factoring RSA129 would require a computational time longer than the age of the universe, providing a long-term confidentiality assurance for the message. However, by 1994 advances in algorithms and in distributed computing, unanticipated in 1977, allowed RSA129 to be factored in only 8 months [10]. Today, much larger and correspondingly harder to factor numbers are used as the security basis of the RSA cryptosystem, but this celebrated example illustrates a concern with these powerfully enabling information assurance tools: the hard mathematical problems on which their security is based are not *provably* hard, and unanticipated mathematical and technological advances can dramatically reduce the intended security lifetime. One particularly challenging threat may come from quantum computation: if large-scale quantum computers can be built in the future, public-key cryptosystems in use today will be rendered insecure no matter how large the key size, together with all communications previously secured by those cryptosystems that have been passively monitored and recorded by adversaries. Today it is neither possible to predict that quantum computers could be constructed of sufficient scale to factor large numbers, nor to rule it out. It is therefore prudent to develop alternative, “surprise-proof” methods of key distribution, such as QKD.

From a foundation of authenticated but non-secret (“public”) conventional communications [11], QKD enables Alice and Bob to produce copious quantities of shared, secret random bits for use as cryptographic keys, by using quantum communications in conjunction with an information theory procedure known as “privacy amplification” [12]. A typical QKD protocol comprises eight stages [13]:

1. random number generation by Alice,
2. quantum communications,
3. sifting,
4. reconciliation,
5. estimation of Eve’s partial information gain,
6. privacy amplification,
7. authentication of public messages, and
8. key confirmation.

First, Alice (the transmitter) generates a sequence of random numbers from a hardware or software random number generator, or quantum mechanically. Then, using the algorithm specified in a pre-determined QKD protocol, she encodes these random bits into the quantum states of a

sequence of signals from her quantum light source and sends them over a “quantum channel” to Bob (the receiver). Bob applies a quantum measurement to each received signal and assigns it a bit value.

Next, Bob informs Alice over a conventional (“public”) communications channel in which time slots he detected photons, but without revealing the bit value he assigned to each one. The bit strings corresponding to the signals detected by Bob are known as raw keys. Then, Alice and Bob post-select by public discussion a random portion of their raw keys, known as their sifted keys, for which they used compatible quantum state preparations and measurements: in an ideal system Alice and Bob’s sifted key bits would be perfectly correlated.

In practice, Bob’s sifted key is not perfectly correlated with Alice’s: it contains errors arising from background photons, detector noise and polarization imperfections. These errors must be located and corrected: Bob reconciles his sifted key with Alice’s using post facto error correction over their public channel, during which parity information about the sifted key is leaked; their perfectly correlated reconciled keys are only partially secret.

From the number of errors that Alice and Bob find in Bob’s sifted key they are able to estimate an upper bound on any partial information that Eve might have been able to obtain on Alice’s transmitted bit string: quantum mechanics ensures that Eve’s measurements would introduce a disturbance (errors) into Bob’s sifted key that would be strongly correlated with Eve’s partial information gain from them.

Alice and Bob extract from their reconciled keys a shorter, final bit string on which they agree with overwhelming probability and on which Eve’s expected information is much less than one bit after an information-theoretic procedure known as “privacy amplification”. In this procedure they use further public communications to agree to hash their reconciled keys into shorter final secret keys. For example, if Alice and Bob have 6 reconciled bits and their bound on Eve’s information tells them that at most she knows 3 of these bits, they can agree to form two secret bits by XOR-ing together the first 4 bits and the final 4 bits: Eve would have to guess at least one of the bits being XOR-ed in each case and so would be ignorant of the outcome. These two bits are therefore suitable for use in a cryptographic key. More generally, Alice and Bob can form their final secret bits from the parities of random subsets of their reconciled bits.

It is one of the most striking security features of QKD that its combination of quantum physics and information theory allows Alice and Bob to both detect eavesdropping and to defeat it, up to a point. For instance, in the BB84 protocol, if Eve performs her own measurements on Alice’s transmitted quantum states (“intercept/resend eavesdropping”), Alice and Bob can produce a shared secret key from their sifted bits up to a sifted bit error rate (for Bob) of about 16%, if Alice uses an ideal source of single photons. For higher bit error rates than this, Alice and Bob cannot establish any secret key even though they are still able to produce sifted bits.

Although Eve is unable to gain any information about the key material from passively monitoring Alice and Bob’s public channel communications, it is essential that these messages are authenticated: that is, Alice and Bob must be able to verify that they are communicating with each other, and that their public communications have not been altered in transit. This is to ensure that Eve cannot perform a “man-in-the-middle” attack in which she would masquerade to Alice that she is Bob and to Bob that she is Alice, while forming separate keys with each.

Alice and Bob can protect against this possibility by appending an authentication tag to their public messages that they compute using a keyed hash function. On receiving a message they can each verify that the received tag value matches the value computed from the message using the keyed hash function. One might object that QKD therefore requires Alice and Bob to share an initial key. But while this is correct, this initial key need only be short and have short-term security: it is of no benefit to Eve to break the authentication *after* Alice's photons are received by Bob. The QKD procedure produces copious quantities of shared long-term secret bits, a few of which can be siphoned off to authenticate the next QKD session. For example, unconditionally secure Wegman-Carter authentication [14] requires Alice and Bob to share a key that is only logarithmic in the size of the message being authenticated. Thus, once started from this authentication foundation, Alice and Bob can use QKD to generate exponentially more shared secret bits in self-sustaining fashion.

If the final key is also included in the authentication procedure, it can also provide a key confirmation function: in the event of an incomplete reconciliation of Bob's sifted key with Alice their authentication tags would disagree. This would prevent them from attempting to use non-identical keys.

Multiple quantum protocols for QKD have been described in the literature. Perhaps the most well-known and well-analyzed is the original BB84 protocol in which Alice sends Bob a sequence of bits as linearly polarized single photons randomly encoded in either of two conjugate polarization bases with  $(0, 1) = (H, V)$ , where "H" ("V") denotes horizontal (vertical) polarization (respectively), in the "rectilinear" basis, or  $(0, 1) = (+45^\circ, -45^\circ)$ , where "+45°" and "-45°" denote the polarization directions in the "diagonal" basis. Bob randomly analyzes the polarization of arriving photons in either the (H, V) or the (+45°, -45°) basis, assigning the corresponding bit value to detected photons. Sifting then amounts to Alice and Bob's post-selection of the random 50% portion of their raw keys for which they used the same polarization bases.

As originally envisioned by Bennett and Brassard, the final keys produced by QKD could be used directly for encryption as a one-time pad ("encryptor-mode QKD"). Once started up from the initial authentication key this type of QKD could provide strong link encryption to secure conventional communications between Alice and Bob without any need for further cryptographic keys.

Since then it has been proposed that a more practical use of QKD (with present day technology) would be for the transfer or generation of conventional symmetric cryptographic keys. For example, "key-transfer mode" QKD could be used by Alice to one-time pad encrypt a previously-generated 256-bit AES key and send it to Bob. Alice and Bob could then establish high-bandwidth secure communications protected by AES using their shared key. Alternatively, instead of using 256 bits of QKD final key bits to encrypt a previously generated AES key, Alice and Bob could use their shared secret QKD bits directly as an *ad hoc* AES key ("key generation"). In either mode QKD would provide a quantum computation resistant alternative to public key methods of distributing symmetric keys.



## 9.0 REFERENCES

- [1] For a review, see:  
Massey, J.L. "An introduction to contemporary cryptology," *Proceedings of the IEEE* **76**(5), 533–549 (1988).
- [2] For example, see:  
Singh, S. *The Code Book* (Doubleday, New York, 1999).
- [3] Shannon, C.E. "Communication theory of secrecy systems," *The Bell System Technical Journal* **28**, 656–715 (1949).
- [4] For example, see:  
Anderson, R., *Security engineering* (John Wiley & Sons, New York, 2001).
- [5] Wiesner, S., "Conjugate coding," *Sigact News* **15**(1), 78–88 (1983).
- [6] Bennett, C.H. and G.Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp.175–179.
- [7] Ekert, A.K., "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663 (1991).
- [8] Vernam, G.S. "Cipher printing telegraph systems," *Transactions of the American Institute of Electrical Engineers* **45**, 295 (1926).
- [9] Gardner, M., *Scientific American*, **237**, 120 (August 1977).
- [10] Atkins, D. *et al.*, "The magic words are squeamish ossifrage," *Advances in Cryptology—ASIACRYPT'94* (Springer-Verlag, New York, 1994) pp. 263.
- [11] For a survey, see:  
Simmons, G.J. "A survey of information authentication," in *Contemporary Cryptology*, G.J.Simmons, Ed., (IEEE, Piscataway, 1992) pp.379–419.
- [12] Bennett, C.H., G.Brassard, C.Crepeau, and U.M.Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory* **41**, 1915–1923 (1995).
- [13] For example, see:  
Lütkenhaus, N., "Estimates for practical quantum cryptography," *Physical Review A* **59**, 3301–3319 (1999).
- [14] Wegman, M.N. and J.L.Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences* **22**, 265–279 (1981).



# **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 be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004

**Version 1.0**



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Don Bethune and Chip Elliott

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

<b>A. Weak Laser Pulses over Fiber (“One-Way”)</b> .....	<b>1</b>
1. Brief description and background for “One-Way” weak laser pulse systems through fiber	1
2. Attributes for “One-Way” weak laser pulse systems through fiber .....	2
3. Development-status metrics .....	3
4. Special strengths.....	4
5. Unknowns/weaknesses .....	4
6. Five-year goals.....	4
7. Ten-year goals .....	5
8. Necessary achievements to make five- and ten-year goals possible .....	5
9. Developments in other areas that would be useful (connections to other technologies) ...	5
10. How will developments in this approach benefit other areas & follow-on potential.....	5
11. Role of theory/security-proof status for “One-Way” weak laser pulse systems through fiber .....	5
<b>B. Weak Laser Pulses over Fiber (“Plug-and-Play”)</b> .....	<b>6</b>
1. Brief description and background for “Plug and Play” weak laser pulse systems through fiber .....	6
2. Attributes for “Plug and Play” weak laser pulse systems through fiber .....	7
3. Development-status metrics .....	7
4. Special strengths.....	9
5. Unknowns/weaknesses .....	9
6. Five-year goals.....	10
7. Ten-year goals: .....	10
8. Necessary achievements.....	10
9. Developments in other areas that would be useful (connections to other technologies) .	10
10. How will developments in this approach benefit other areas & follow-on potential.....	11
11. Role of theory/security-proof status for “Plug and Play” weak laser pulse systems through fiber.....	11
<b>C. References for Weak Laser Pulses over Fiber</b> .....	<b>11</b>

## List of Tables and Figures

Table 6.1-1. Groups Pursuing Weak Laser Pulses over Fiber “One-Way” Implementations of QKD.....	1
Table 6.1-2. Groups Pursuing Weak Laser Pulses over Fiber “Plug and Play” Implementations of QKD .....	6

## 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 be 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  $\mu$ , the mean number of photons/pulse. The frequency of pulses that contain multiple photons relative to single-photon pulses ( $\sim \mu/2$ , for small  $\mu$ ) must be kept small to limit the efficacy of beamsplitter attacks. Typically values  $\mu \in [0.1-0.5]$  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 be 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  $>10,000 \text{ bits} \cdot \text{sec}^{-1}$  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  $>100,000 \text{ bits} \cdot \text{sec}^{-1}$  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. <i>et al.</i>	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 (<math>\leq 200\text{ m}</math>) 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 (<math>\leq 2\text{ km}</math>) 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 (<math>\leq 70\text{ km}</math>) 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 (>math>70\text{ km}</math>) 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  $>10,000 \text{ bits} \cdot \text{sec}^{-1}$  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  $>100,000 \text{ bits} \cdot \text{sec}^{-1}$  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. Hjelm, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics* **48**, 2023–2038 (2001).

# **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 be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004

**Version 1.0**



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

**6.2 Weak Laser Pulses through Free-Space Approaches to QKD ..... 1**

- 1. Brief description and background for weak laser pulses through free space approaches to QKD ..... 1
- 2. Attributes for weak laser pulse systems through free space ..... 2
- 3. Development-status metrics ..... 3
- 4. Special Strengths ..... 4
- 5. Unknowns/weaknesses ..... 4
- 6. Five-year goals ..... 4
- 7. Ten-year goals ..... 4
- 8. Necessary achievements to make five- and ten-year goals possible ..... 5
- 9. Developments in other areas that would be useful (connections to other technologies) .. 5
- 10. How will developments in this approach benefit other areas & follow-on potential ..... 5
- 11. Role of theory/security-proof status for weak laser pulses through free space QKD ..... 5

**References ..... 5**

## List of Tables and Figures

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

## 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  $\mu$ , 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 ( $\sim \mu/2$  for small  $\mu$ ) 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  $\mu \in [0.1-0.5]$  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  $\sim 30$  m 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 ( $\sim 70$  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  $\sim 1,000$  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  $>100,000 \text{ bits} \cdot \text{sec}^{-1}$  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. Lamoreaux, 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).

# **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 be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004

**Draft 1.0**



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

<b>6.3 Single Photon Light Source Approaches to QKD .....</b>	<b>1</b>
1. Brief description and background for single-photon light source approaches to QKD .....	1
2. Attributes for single-photon source approaches to QKD .....	1
3. Development-status metrics .....	2
4. Special strengths.....	2
5. Unknowns/weaknesses .....	3
6. Five-year goals.....	4
7. Ten-year goals .....	4
8. Necessary achievements to make five- and ten-year goals possible .....	4
9. Developments in other areas that would be useful (connections to other technologies) ...	4
10. How will developments in this approach benefit other areas & follow-on potential.....	4
11. Role of theory/security-proof status for single-photon source QKD .....	5
<b>References .....</b>	<b>5</b>

## List of Tables and Figures

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

## 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,  $g^{(2)} \equiv 0$  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  $g^{(2)} \gg 0$ , additional privacy amplification is required to remove the extra information obtainable by an eavesdropper looking at multiple-photon pulses. Although the limiting case  $g^{(2)} \equiv 0$  is ideal and will never be achieved in practice, one can nevertheless do much better than simply using attenuated laser pulses for which  $g^{(2)} \equiv 1$ . For the purposes of this section we apply the term “single-photon source” to any source with  $g^{(2)} \leq 0.1$ . At this point in time, the lowest reported value is  $g^{(2)} \leq 0.05$  [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).



# **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 be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004

**Version 1.0**



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

**6.4 Entangled Photon Pair Approaches to QKD..... 1**

- 1. Brief Description and Background for entangled-photon approaches to QKD..... 1
- 2. Attributes for entangled-photon approaches to QKD..... 2
- 3. Development-status metrics..... 3
- 4. Special strengths ..... 5
- 5. Unknowns/weaknesses..... 5
- 6. Five-year goals ..... 5
- 7. Ten-year goals..... 5
- 8. Necessary achievements to make five- and ten-year goals possible ..... 6
- 9. Developments in other areas that would be useful (connections to other technologies).. 6
- 10. How will developments in this approach benefit other areas & follow-on potential ..... 6
- 11. Role of theory/security-proof status for entangled-photon QKD..... 6

**References ..... 6**

## List of Tables, Figures, and Equations

Table 6.4-1. Groups Pursuing Entangled-Photon Implementations of QKD ..... 1  
Figure 6.4-1. Schematic entangled-pair key exchange system..... 1

## List of Acronyms and Abbreviations

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



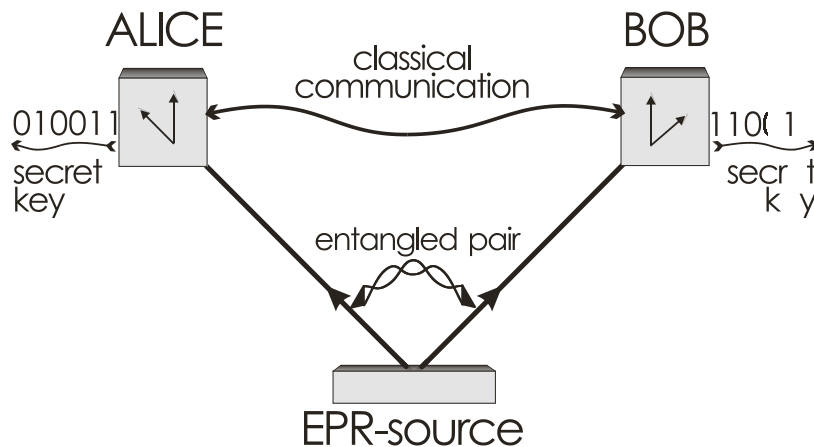
## 6.4 Entangled Photon Pair Approaches to QKD

**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.<sup>†</sup> 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.,

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) \quad (\text{Equation 6.4-1})$$

which is in a superposition of two possible 100% correlated states ( $|1\rangle_1|1\rangle_2$  or  $|0\rangle_1|0\rangle_2$  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.

---

<sup>†</sup> 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  $\sim 1$  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 $\cdot$ sec $^{-1}$  (this implies a background rate of only 1 millicoincidence $\cdot$ 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  $4 \times 10^5$  to  $1.3 \times 10^6$  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<sup>†</sup> [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].

<sup>†</sup> 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  $\ll 1$  per second), and the resulting final entangled states are not of exceedingly high quality (maximum fidelity  $\sim 93\%$ , 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  $\mu$ s 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  $1 \times 10^6$  pair photons  $\bullet \text{sec}^{-1}$ , and to date the highest *detected* pair rates range  $4 \times 10^5$  to  $1.3 \times 10^6$  coincidences  $\bullet \text{sec}^{-1}$  [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  $\bullet \text{sec}^{-1}$  source (detected in laboratory)
- Free-space systems operating out to 10 km (per arm)
- $10^5$  coincidence  $\bullet \text{sec}^{-1}$  into a single mode
- Prototype systems for fiber communications to 50 km
- Quantum memory with high fidelity storage
- Quantum repeater with bit rate exceeding  $10^4$  qubits  $\bullet \text{sec}^{-1}$

#### 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  $1000 \text{ qubits} \cdot \text{sec}^{-1}$

## 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 ( $\sim 1 \text{ nm}$  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  $100 \text{ km}$  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 39<sup>th</sup> 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<sub>4</sub> 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).

# **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 be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004

**Version 1.0**



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

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

**6.5 Continuous-Variable Approaches to QKD..... 1**

- 1. Brief description and background for continuous-variable approaches to QKD..... 1
- 2. Attributes for continuous variable Approaches to QKD..... 2
- 3. Development Status Metrics ..... 2
- 4. Special strengths ..... 3
- 5. Unknowns/weaknesses..... 4
- 6. Five-year goals ..... 4
- 7. Ten-year goals..... 4
- 8. Necessary achievements to make five- and ten-year goals possible ..... 4
- 9. Developments in other areas that would be useful (connections to other technologies).. 4
- 10. How will developments in this approach benefit other areas & follow-on potential ..... 4
- 11. Role of theory/security-proof status for continuous-variable QKD..... 4

**References ..... 4**

## List of Tables and Figures

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

## 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. Blisdir, 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 6<sup>th</sup> 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).



# **Summary of the Theory Component of Quantum Key Distribution and Quantum Cryptography**

## **A Quantum Information Science and Technology Roadmap**

### **Part 2: Quantum Cryptography**

Disclaimer:

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

July 19, 2004

**Version 1.0**



Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Charles Bennett, Gilles Brassard, Artur Ekert, Chris Fuchs and John Preskill

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

<b>Theoretical Approaches to Quantum Cryptography .....</b>	<b>1</b>
<b>A. Quantum Key Distribution .....</b>	<b>1</b>
<b>B. Beyond Quantum Key Distribution .....</b>	<b>6</b>
1. Quantum bit commitment.....	6
2. Quantum coin flipping .....	6
3. Quantum fingerprints and digital signatures .....	7
4. Quantum data hiding .....	7
5. Authentication of quantum messages .....	8
6. Encryption of quantum states.....	8
7. Secure multiparty quantum computation .....	8
8. Quantum-computational security.....	9
<b>References .....</b>	<b>9</b>

## List of Tables, Figures, and Equations

Equation A-1 .....	3
Equation A-2.....	5

## List of Acronyms and Abbreviations

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





## Theoretical Approaches to Quantum Cryptography

In a cryptographic protocol, two or more parties perform an information-processing task in the presence of adversaries who are trying to gain some advantage relative to the honest parties. Roughly speaking, we say that the protocol is *secure* if it is infeasible for the adversaries to achieve their objective. In many cases, the honest parties want to prevent the adversaries from acquiring private information. For example, Alice might wish to send a secret to Bob, without allowing the eavesdropper Eve to learn the secret; the communication is secure if the probability is negligible that Eve can learn more than a negligible part of the secret.

A central goal of modern classical cryptography is to devise protocols that are *computationally secure*. This means that the security is founded on an (unproven) assumption that a certain computation that would break the protocol is too *hard* for the adversary to execute. Thus, even though a computationally secure protocol may be invulnerable to the strongest attacks that are currently foreseen, the discovery of a better classical algorithm could threaten its security. Furthermore many protocols that are believed to be secure against attacks by classical computers are known to be vulnerable to quantum attacks. Therefore, if and when quantum computers become readily available, much of classical cryptography will be obsolete.

A major goal of quantum cryptography is to devise protocols, involving the exchange of quantum states, that are *information-theoretically secure*. This means that the security is maintained even if the adversary has unlimited computational power. The most celebrated achievement in quantum cryptography is the formulation of quantum protocols for key distribution that are provably secure information theoretically. There are also some important negative results, most notably that information-theoretically secure bit commitment is impossible even in the quantum world.

In this section of the quantum cryptography roadmap, we review the current status of research on the information-theoretic security of quantum key distribution (QKD). We also discuss briefly some other aspects of theoretical research on quantum cryptography, pointing out some noteworthy recent advances and some important remaining challenges.

### A. Quantum Key Distribution

The purpose of QKD is to establish a string of random bits (the “key”) shared by Alice and Bob, where Alice and Bob can be highly confident that eavesdropper Eve knows almost nothing about the key. Then the key can be used by Alice and Bob as a one-time pad for enciphering and deciphering a message. Because the key is random and unknown by Eve, she can’t learn anything about the message by intercepting the ciphertext.

The promise of quantum cryptography was first glimpsed by Stephen Wiesner, [1] who proposed a quantum realization of unforgeable bank notes in the early 1970s. A decade later, Charles Bennett and Gilles Brassard [2] proposed the first QKD scheme, which was published in 1984 and became known as the “BB84” protocol. In BB84, Alice repeatedly sends to Bob one of four possible states of a qubit, and Bob measures each signal in one of two complementary

bases. This protocol was reinvented a few years later by Douglas Wiedemann, [3] who was unaware at the time of the work of Bennett and Brassard.

In 1990, Artur Ekert, also initially unaware of the earlier work, began developing a different approach to quantum cryptography that ultimately proved very fruitful. Ekert proposed a key-distribution protocol [4] in which entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits. Bennett, Brassard, and Mermin [5] then noted that a simplified version of entanglement-based QKD can be cast in a form closely resembling BB84, where each party measures the qubit in one of two complementary bases. Many other variations on QKD were proposed later, such as

- a “six-state protocol” [6], in which Alice sends each qubit in one of six possible states;
- Bennett’s B92 protocol [7], in which Alice sends one of two nonorthogonal states;
- the “time-reversed” EPR protocol [8], in which Alice and Bob send the BB84 states to a central switching station (where their shared key is established via an entangled measurement); and
- protocols using continuous quantum variables [9], in which Alice sends a squeezed state or a coherent state of a harmonic oscillator.

In their original paper and in subsequent work with other collaborators [10], Bennett and Brassard analyzed “individual” attacks on BB84, in which Eve attacks the quantum signals one at a time. However, a complete proof of information-theoretic security is more challenging. In principle, Eve could attack all of the signals sent by Alice to Bob collectively, entangling the qubits with an ancilla that she controls. Eve could then monitor the public classical communication between Alice and Bob, in which they reveal their basis choices and exchange further information to correct errors in their shared key and to amplify its privacy. The information Eve learns from this public discussion might help her decide how to measure her ancilla to optimize her information about the key.

New techniques for analyzing collective attacks by the eavesdropper were developed by Andrew Yao [11] in 1995, and the first complete proof of information-theoretic security for BB84 was obtained by Dominic Mayers [12] in 1996. Around the same time, Bennett, Brassard, Popescu, Schumacher, Smolin, and Wootters [13] discovered that noisy quantum entanglement can be distilled, and Deutsch, Ekert, Jozsa, Macchiavello, Popescu, and Sanpera [14] noted that if Alice and Bob have reliable quantum computers, they can use an entanglement-distillation protocol to achieve a secure version of entanglement-based key distribution. This observation was developed into a formal proof of security by Lo and Chau [15] in 1998. The approaches of Mayers and of Lo and Chau were united in 2000 by Shor and Preskill, [16] who showed that entanglement distillation can be invoked to formulate a relatively simple proof of the security of the original BB84 protocol.

The Shor-Preskill analysis relies on the idea that Alice and Bob could use a quantum error-correcting code to prevent Eve from becoming entangled with the protected qubits that are used to generate the key. Furthermore, this code can be chosen to have the property that bit-flip error correction and phase error correction can be performed separately. However, for the final key to be private, it is not necessary to actually perform the phase error correction—it is enough to know, based on the verification test included in the protocol, that phase error correction would

have succeeded *if it had been done*. By this reasoning based on *virtual quantum error correction*, a protocol invoking quantum error correction reduces to BB84 augmented by classical error correction and classical privacy amplification, which is therefore provably secure against any possible eavesdropping strategy.

Another novel approach to proving the security of BB84 (long in gestation but still unpublished) has been pursued by Ben-Or [17]. In Ben-Or's proof, one uses the results of the verification test to infer that the quantum state of Eve's ancilla is highly compressible. Then results regarding the quantum-communication complexity of the binary inner product function are cited to establish that Eve cannot possibly have enough information to compute the final key generated by Alice and Bob. Quite different technical tools were developed by Biham, Boyer, Boykin, Mor, and Roychowdhury [18], who were the first after Mayers to obtain a complete proof of security.

The formal security proofs establish that, if the bit error rate (BER),  $\Delta$  observed in the verification test is low enough, then the secure final key can be extracted from the sifted key at a nonzero asymptotic rate. For example, in the case where error correction and privacy amplification are carried out using only one-way communication from Alice to Bob, the ratio of the length  $k$  of the final key (after error correction and privacy amplification) to the length  $n$  of the sifted key satisfies

$$R = \lim_{n \rightarrow \infty} k/n \geq 1 - 2H_2(\Delta), \quad (\text{Equation A-1})$$

where  $H_2(\Delta) \equiv -\Delta \log_2 \Delta - (1-\Delta) \log_2 (1-\Delta)$  is the binary Shannon entropy function. Hence, secure key exchange can be achieved for any  $\Delta \leq 11\%$ . The proof shows the following: Suppose Eve uses a strategy that passes the verification test with a probability that is not exponentially small. For *any* such attack by Eve, if the verification test succeeds then Alice and Bob agree with high probability on a final key that is nearly uniformly distributed, and Eve's information about the final key is exponentially small. Here "exponentially small" means bounded above by  $(e^{-ck})$  where  $k$  is the length of the final key and  $C$  is a positive constant, "high probability" means exponentially close to 1, and "nearly uniformly distributed" means exponentially close to a uniform distribution. Informally, for any attack, either Alice and Bob are almost certain to catch Eve, or else Eve knows almost nothing about the final key.

The Shor-Preskill method was adapted by Lo [19] to prove the security of the six-state protocol for BERs up to 12.7%, and by Tamaki, Koashi, and Imoto [20] to prove the security of B92. Gottesman and Lo [21] have shown that if Alice and Bob use two-way communication to correct errors and amplify privacy, then secure key distribution is still possible in BB84 for BERs up to 18.9%, and in the six-state protocol for BERs up to 26.4%. On the other hand, it is known that information-theoretically secure key distribution is impossible if the BER is above 25% in BB84 or 33% in the six-state protocol—these are the error rates that arise if Eve measures each signal in a randomly selected basis and then sends onto Bob the state resulting from her measurement ("intercept/resend attack"). If Alice and Bob are limited to one-way communication, then secure key distribution is impossible if the BER is above 14.6% in BB84 or 16.7% in the six-state protocol—these are the error rates that arise if an optimal approximate cloner diverts to Eve a state identical to that received by Bob. It is an interesting challenge to close the gaps between the best known upper and lower bounds on the BER.

The Shor-Preskill method was also applied by Gottesman and Preskill [22] to a continuous-variable key-distribution protocol, in which Alice sends a squeezed state and Bob performs a homodyne measurement. This scheme is information-theoretically secure if Alice's signals are squeezed sufficiently. Protocols in which Alice's signals are coherent states have been shown to be secure against certain types of individual attacks [23], but whether information-theoretic security can be established for a coherent-state protocol remains an important open question.

QKD has also been called *quantum key expansion*, emphasizing that Alice and Bob must share a short private key at the start of the protocol, which expands to a much longer key when key distribution is successful. The initial key is used for *authentication*; Alice and Bob need a way to guarantee that they are really talking to one another. Otherwise, Eve could pretend to be Alice when talking to Bob and pretend to be Bob when talking to Alice ("man-in-the-middle attack"). Information-theoretically secure classical protocols for authentication are known, but these require Alice and Bob to share the initial secret key. Suppose that the initial key used for authentication was in fact generated during a previous round of quantum key expansion—might the eavesdropper exploit this feature to sharpen her attack? This subtle question was answered recently by Ben-Or and Mayers, [24] who showed that QKD can be safely composed with authentication without compromising security. This work also highlights the importance of formulating careful definitions of security that are amenable to composability.

Information-theoretic security has also been called "unconditional security," to emphasize that there are no assumptions about the technological sophistication or computational power of the adversary. But of course there are conditions that must be satisfied for security proofs to apply—in any analysis of security we have to decide what to trust and what to mistrust. For example, in discussions of QKD, we typically accept that Alice's random number generator is reliable, and that Eve has no *a priori* knowledge of the bases chosen by Alice and Bob in the protocol. Furthermore, assumptions are needed about the performance of the equipment used in the protocol, and these should be carefully considered to assess whether QKD is really secure in realistic implementations.

In the original BB84 security proof by Mayers, it is assumed that Alice's source is perfect, but Bob's detector can be completely uncharacterized; the flaws in the detector cannot fool Alice and Bob into accepting a key that Eve knows, and the rate of key generation  $R$  for a given BER  $\square$  is independent of the detector's performance. Koashi and Preskill [25] showed that an analogous result holds if the detector is perfect and the source is uncharacterized, as long as the source does not leak to Eve any information about Alice's basis choice.

The security analysis is more delicate if the faulty performance of the source *does* reveal some information about the basis choice. Of particular practical importance is the case where the source emits weak coherent states rather than single photons, and Alice's qubit is encoded in the photon polarization. The source occasionally emits more than one photon in the same polarization state, and Eve can skim off the extra photon(s), wait until Alice and Bob announce their bases, and then measure in the correct basis, obtaining perfect polarization information at no cost in disturbance. The privacy-amplification scheme must be sufficiently powerful (and the coherent states sufficiently weak), to nullify this advantage. Inamori, Lütkenhaus, and Mayers [26] proved the information-theoretic security of BB84, where Alice's source emits weak

coherent states and Bob's detector is uncharacterized, establishing that secure final key can be extracted from sifted key at an asymptotic rate

$$R \geq (1 - \epsilon) - H_2(\epsilon) - (1 - \epsilon) H_2(\epsilon/(1 - \epsilon)); \quad (\text{Equation A-2})$$

here  $\epsilon$  is the BER observed in the verification test, and  $\epsilon = p_M/p_D$ , where  $p_M$  is the probability that the source emits multiple-photons, and  $p_D$  is the probability that a photon emitted by the source is detected by Bob.

More generally, if we trust a characterization of the equipment ensuring that the flaws in the source and detector are sufficiently small, then in many cases information-theoretic security can be proven, and lower bounds on the asymptotic key generation rate established; various examples have been analyzed by Gottesman, Lo, Lütkenhaus, and Preskill [27]. Furthermore, Mayers and Yao [28] have formulated the concept of a "self-testing" source and detector, which can be reliably characterized even if we do not trust the devices used to test the equipment. However, we are still lacking a complete proof of security that applies to arbitrary attacks by the eavesdropper and fully realistic implementation.

Another difficulty for the implementation of QKD using polarization encoding is that optical fibers rotate the polarization, and the amount of rotation may fluctuate over time. Boileau, Gottesman, Laflamme, Poulin, and Spekkens [29] proposed a means of overcoming this difficulty, in which the key bits are encoded in a noiseless subsystem. Their scheme requires Alice to have a source of entangled photons.

A serious limitation on practical QKD is that losses in optical fibers limit the range over which a secure key can be established. In principle, the range could be extended dramatically using "quantum repeaters" that implement quantum error correction; this might be an important application for quantum computers of modest scale. For example Dür, Briegel, Cirac, and Zoller, [30] among others, have described how, with reasonable resources, a nested cascade of entanglement distillation protocols can establish high-fidelity entangled pairs over long distances, which could then be used for key distribution. Further theoretical work aimed at optimizing the efficiency of quantum repeaters may prove fruitful.

Let us summarize the current status of the theory of QKD. The designer of a cryptographic system should ensure that the security of the system rests on a firm foundation. It is reckless to underestimate the ingenuity of the adversary and inherently risky to assume that the eavesdropper will use a particular strategy, even if that assumption seems to be warranted by apparent technological limitations. Therefore, theorists have focused primarily on establishing the security of QKD against unrestricted attacks by the eavesdropper ("information-theoretic" or "unconditional" security). Satisfactory proofs of security have been found for protocols executed under ideal conditions. However, existing quantum cryptosystems are far from ideal, and the demanding criteria that these systems must meet to provide genuine security pose new challenges for the system designer, quite distinct from the problems encountered in classical cryptography. Recent results show that information-theoretic security can be maintained in the presence of certain kinds of system faults. An important goal for future research is to sharpen our understanding of the conditions that ensure adequate security, so that practitioners of QKD can achieve high confidence in the reliability of their systems.

## B. Beyond Quantum Key Distribution

While QKD has attracted much attention because it is relatively close to practical realization, there are many other cryptographic tasks for which quantum protocols offer significant potential advantages over classical protocols. In the past few years, there has been impressive progress in our understanding of the security of various quantum protocols other than key distribution, but many challenging questions remain. Here we give a brief overview of some of the recent developments and highlight a few open problems.

### 1. Quantum bit commitment

In bit commitment, Alice chooses a bit and keeps it secret until she is ready to reveal it to Bob. A bit-commitment protocol is “binding” if Alice is unable to change the value of her bit after committing to it, and “concealing” if Bob is unable to learn the bit before Alice unveils it. The protocol is secure if it is both binding and concealing. Classical bit-commitment protocols are known that are computationally secure under unproven cryptographic assumptions, but these are vulnerable to quantum attacks.

In the paper that introduced the BB84 protocol, Bennett and Brassard also proposed a protocol for coin tossing that in retrospect can be seen to be a quantum bit-commitment protocol. They demonstrated its security against some attacks but showed that it can be defeated by a cheating Alice who exploits quantum entanglement to alter her bit after committing. Further developing this idea, Mayers [31] and Lo and Chau [32] eventually showed that information-theoretically secure quantum bit commitment is impossible.

Kent [33] has devised a *classical* bit-commitment protocol founded on the impossibility of sending signals faster than light—it is secure against arbitrary classical attacks and is conjectured to be secure against all quantum attacks as well. However, this scheme has the drawback that the security is lost unless Alice and Bob communicate continually from the time of the commitment to the time of unveiling.

Although no quantum bit-commitment protocol can be both perfectly binding and perfectly concealing, it is possible to devise protocols that are both partially binding and partially concealing. The tradeoff between the degree of bindingness (the probability that Alice can change her bit successfully) and the degree of concealment (the probability that Bob can estimate the bit correctly) has been studied by Spekkens and Rudolph [34]. Furthermore, *cheat sensitive* bit-commitment protocols have been proposed [35], such that for any cheating strategy by either party, there is a nonzero probability that the other party detects the cheating.

### 2. Quantum coin flipping

In coin flipping, Alice and Bob (who might live in different cities) want to flip a fair coin “over the telephone.” That is, they are to play a game in which they exchange information and make alternate moves, where each player prints out the outcome of the coin flip at the end of the game. If the players are honest, the outcome should be random and both players should agree on the outcome; furthermore, neither player should be able to bias the other player’s outcome

by cheating. Coin flipping appears to be an easier task than bit commitment (we can use bit commitment to achieve coin flipping, but not vice versa), and it has important cryptographic applications.

While computationally secure classical coin-flipping protocols exist (under plausible cryptographic assumptions), information-theoretically secure classical coin flipping is known to be impossible. Suppose that Alice wins the game if the outcome is heads, and Bob wins if the outcome is tails. Then for any classical coin flipping game, one player or the other has a strategy that ensures a win every time! In contrast, Ambainis [36] and Spekkens and Rudolf [37] have shown quantum coin flipping-protocols (such that Alice and Bob exchange quantum states instead of classical information) in which a cheater's ability to bias the outcome of the coin flip is limited: a cheater can force a win with probability no greater than  $2^{-1/2}$ .

Are there quantum coin-flipping protocols in which a cheater's probability of winning is arbitrarily close to  $1/2$ ? This is an important open question in quantum cryptography. Ambainis [38] has shown that if the maximum probability of winning for a cheating player is  $1/2 + \epsilon$  then the number of rounds of communication in the protocol must grow with  $\epsilon$  at least as fast as  $\log(\log(1/\epsilon))$  (still a quite modest rate of growth). And Kitaev [39] has shown that in any quantum coin-flipping protocol, a cheater can force either a win *or a loss* with probability at least  $2^{-1/2}$ .

### 3. Quantum fingerprints and digital signatures

A fingerprint is a short bit string associated with a long string, such that any two long strings can be distinguished with high probability by comparing their fingerprints alone. Classically, the fingerprint can be exponentially shorter than the original string, but only if the parties preparing the fingerprints share a random key. Buhrman, Cleve, Watrous, and de Wolf [40] have shown that fingerprints consisting of quantum information can be exponentially shorter than the original strings even without any correlations between the parties. This is possible because the number of  $n$ -dimensional quantum states such that the angle between any two of the states is independent of  $n$  can grow exponentially with  $n$ . Gottesman and Chuang [41] used quantum fingerprinting as the basis for an information-theoretically secure public-key quantum digital signature scheme. This scheme has the drawback that Alice needs to send a copy of her public key (a quantum state) to each potential recipient of a message signed by Alice, and that each copy of the public key can be used only once. Can information-theoretically secure quantum digital signature schemes be developed that do not have such disadvantages? What other applications of quantum fingerprints are possible?

### 4. Quantum data hiding

In quantum data hiding, Charlie encodes quantum (or classical) information in a bipartite quantum state that is distributed to Alice and Bob in such a way that Alice and Bob can recover the encoded information with high fidelity if they get together or communicate quantumly. But if Alice and Bob are limited to classical communication, they cannot learn more than a negligible amount about the encoded information, even if their local computational power is unlimited. Schemes for hiding classical data in bipartite quantum states were first formulated by

DiVincenzo, Leung, and Terhal [42] and Hayden, Leung, Shor, and Winter [43] have shown that when the amount of hidden information is large, one hidden qubit can be encoded per each pair of physical qubits shared by Alice and Bob.

## 5. Authentication of quantum messages

In classical authentication, Alice and Bob use a shared private random key to verify with information-theoretic security that a message sent from Alice to Bob has not been modified during transmission. Barnum, Crépeau, Gottesman, Smith, and Tapp [44] have shown that quantum states sent from Alice and Bob can be similarly authenticated. Furthermore, Oppenheim and Horodecki [45] and Gottesman, Hayden, Leung, and Mayers [46] have shown that when authentication is successful, most of the classical key can be safely reused in further rounds of authentication. In what other quantum protocols might key material be recycled without compromising security? Gottesman [47] has shown that a quantum authentication scheme can be used for *uncloneable encryption* of classical messages; this means that an eavesdropper cannot decipher the message even if she later discovers the classical key that was used to encode it. In what other novel ways might quantum authentication be applied?

## 6. Encryption of quantum states

Both quantum data hiding and quantum authentication make use of an important cryptographic primitive, the encryption of quantum states (also known as the “private quantum channel” or “quantum one-time pad”). If Alice and Bob share a secret random classical key, Alice can use the key to encrypt a quantum state  $\rho$  that she wishes to send to Bob, and if the encrypted signal arrives undamaged, Bob can use the key to recover  $\rho$ . Furthermore, an eavesdropper who intercepts the encrypted signal will be unable to learn anything about  $\rho$ . Boykin and Roychowdhury [48] and Mosca, Tapp and de Wolf [49] showed that two bits of shared classical key per transmitted qubit are necessary and sufficient for perfect encryption. A surprising recent discovery<sup>43</sup> is that for a sufficiently long quantum message, just one bit of key per transmitted qubit suffices for arbitrarily good encryption.

## 7. Secure multiparty quantum computation

In multiparty classical computation, each of  $n$  parties receives part of the input to a computation. The parties, communicating via secure pairwise channels, then execute a circuit, with each party receiving a portion of the output. This procedure is secure if no coalition of cheaters can learn more about the computation than can be inferred from their inputs and outputs, and if furthermore the cheaters are unable to alter the output, beyond their ability to choose their inputs. Information-theoretically secure classical multiparty computation is possible if fewer than a third of the parties are cheaters. Crépeau, Gottesman, and Smith [50] have studied multiparty quantum computation, in which the inputs and outputs are quantum states, and have established information-theoretic security if fewer than one sixth of the parties are cheaters. It is an open question whether this result can be improved to the case where fewer than a quarter of the parties are cheaters. It will also be interesting to determine whether more cheaters can be tolerated in “cheat-sensitive” protocols that abort when cheating is detected.



## 8. Quantum-computational security

Classical cryptosystems are often founded on the concept of a *one-way function* that is easy to compute but hard to invert, and especially the notion of a *trap-door one-way function* that can be inverted easily when some helpful auxiliary information is provided. There are various plausible candidates for such one-way functions, but no proofs that they exist, and furthermore many of these candidates are known to be efficiently invertible with a quantum computer. In contrast, most work on quantum cryptography has focused on establishing security without any computational assumptions. One goal for future research is to find plausible candidates for quantum one-way functions, which are easy to compute but hard to invert on a quantum computer, and to formulate cryptosystems based on these functions that can be presumed immune to quantum cryptanalysis. For example, Dumais, Mayers, and Salvail, [51] and Adcock and Cleve [52] have described how a quantum one-way function could be exploited to formulate bit-commitment protocols with quantum-computational security. One particularly intriguing open question concerns secure two-party evaluation of a classical function, where each party provides an input to the function, and each is to learn the output without finding out anything about the other party's input. Computationally secure classical protocols are known, but these are vulnerable to quantum attack. Can two-party function evaluation be achieved with quantum-computational security? Clearly, much more can be done to develop a theory of computationally secure cryptography that is suitable for a world in which quantum computers are commonplace.

## References

- [1] Wiesner, S., "Conjugate coding," originally written *c.*1970 but unpublished until *Sigact News* **15**(1), 78–88 (1983).
- [2] Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
- [3] Wiedemann, D., "Quantum cryptography," *Sigact News* **18**(2), 48–51 (1987); Bennett, C.H. and G. Brassard, "Quantum public key distribution reinvented," *Sigact News* **18**(4), 51–53 (1987).
- [4] Ekert, A.K., "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663 (1991).
- [5] Bennett, C.H., G. Brassard, and N.D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters* **68**, 557–559 (1992).
- [6] Brass, D., "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters* **81**, 3018–3021 (1998), [preprint *quant-ph/9805019*].
- [7] Bennett, C.H., "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters* **68**, 3121–3124 (1992).
- [8] Biham, E., B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Physical Review A* **54**, 2651–2658 (1996), [preprint *quant-ph/9604021*].

- [9] Ralph, T.C., "Continuous variable quantum cryptography," *Physical Review A* **61**, 010303 (2000), [preprint *quant-ph/9907073*].  
 Hillery, M., "Quantum cryptography with squeezed states," *Physical Review A* **61**, 022309 (2000), [preprint *quant-ph/9909006*].  
 Reid, M.D., "Quantum cryptography with a predetermined key, using continuous variable Einstein-Podolsky-Rosen correlations," *Physical Review A* **62**, 062308 (2000), [preprint *quant-ph/9909030*].  
 Pereira, S.F., Z.Y. Ou, and H.J. Kimble, "Quantum communication with correlated nonclassical states," *Physical Review A* **62**, 042311 (2000), [*quant-ph/0003094*].
- [10] Bennett, C.H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology* **5**(1), 3–28 (1992).
- [11] Yao, A.C.-C., "Security of quantum protocols against coherent measurements," in *Proc. 27th ACM Symposium on the Theory of Computing* (ACM press, New York, 1995), pp. 67–75.
- [12] Mayers, D., "Unconditional security in quantum cryptography," *Journal of the ACM* **48**(3), 351–406 (2001), [preprint *quant-ph/9802025*].
- [13] Bennett, C.H., G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters* **76**(5), 722–725 (1996), [preprint *quant-ph/9511027*], Erratum: *Physical Review Letters* **78**(10), 2031 (1997).
- [14] Deutsch, D., A.K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Physical Review Letters* **77**(13), 2818–2821 (1996), [preprint *quant-ph/9604039*], Erratum: *Physical Review Letters* **80**(9), 2022 (1998).
- [15] Lo, H.-K. and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science* **283**(5410), 2050–2056 (1999), [preprint *quant-ph/9803006*].
- [16] Shor, P.W. and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters* **85**(2), 441–444 (2000), [preprint *quant-ph/0003004*].
- [17] Ben-Or, M., "Simple security proof for quantum key distribution," (presentation available at URL: <http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html>).
- [18] Biham, E., M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," in the *Proceedings of the 32<sup>nd</sup> Annual ACM Symposium on Theory of Computing* (ACM press, New York, 2000), pp. 715–724, [preprint *quant-ph/9912053*].
- [19] Lo, H.-K., "Proof of unconditional security of six-state quantum key distribution scheme," *Quantum Information and Computing* **1**(2), 81–94, (2001), [preprint *quant-ph/0102138*].
- [20] Tamaki, K., M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Physical Review Letters* **90**, 167904 (2003), [preprint *quant-ph/0210162*].
- [21] Gottesman, D. and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Transactions on Information Theory* **49**(2), 457–475 (2003), [preprint *quant-ph/0105121*].

- [22] Gottesman, D. and J. Preskill, "Secure quantum key distribution using squeezed states," *Physical Review A* **63**, 022309 (2001), [preprint *quant-ph/0008046*].
- [23] Grosshans, F. and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters* **88**, 057902 (2002), [preprint *quant-ph/0109084*].
- [24] Mayers, D. and M. Ben-Or, "Composing quantum protocols," (presentation available at URL: <http://www.msri.org/publications/ln/msri/2002/qip/mayers/1/index.html>).
- [25] Koashi, M. and J. Preskill, "Secure quantum key distribution with an uncharacterized source," *Physical Review Letters* **90**, 057902 (2003), [preprint *quant-ph/0208155*].
- [26] Inamori, H., N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," preprint available at <http://arxiv.org/abs/quant-ph/0107017>.
- [27] Gottesman, D., H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," preprint available at <http://arxiv.org/abs/quant-ph/0212066>.
- [28] Mayers, D. and A. Yao, "Self testing quantum apparatus," preprint available at <http://arxiv.org/abs/quant-ph/0307205>.
- [29] Boileau, J.-C., D. Gottesman, R. Laflamme, D. Poulin, and R.W. Spekkens, "Robust polarization-based quantum key distribution over collective-noise channel," preprint available at <http://arxiv.org/abs/quant-ph/0306199>.
- [30] Dür, W., H.-J. Briegel, J.I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A* **59**(1), 169–181 (1999), [preprint *quant-ph/9808065*], Erratum: *Physical Review A* **60**(1), 725 (1999).
- [31] Mayers, D., "Unconditionally secure quantum bit commitment is impossible," *Physical Review Letters* **78**(17), 3414–3417 (1997), [preprint *quant-ph/9605044*].
- [32] Lo, H.-K. and H.F. Chau, "Is quantum bit commitment really possible?" *Physical Review Letters* **78**(17), 3410–3414 (1997), [preprint *quant-ph/9605026*].
- [33] Kent, A., "Unconditionally secure bit commitment," *Physical Review Letters* **83**(7), 1447–1450 (1999), [preprint *quant-ph/9810068*].
- [34] Spekkens, R.W. and T. Rudolph, "Degrees of concealment and bindingness in quantum bit commitment protocols," *Physical Review A* **65**, 012310 (2002), [preprint *quant-ph/0106019*].
- [35] Hardy, L. and A. Kent, "Cheat sensitive quantum bit commitment," preprint available at <http://arxiv.org/abs/quant-ph/9911043>;  
Aharonov, D., A. Ta-Shma, U.V. Vazirani, and A.C. Yao, "Quantum bit escrow," in the *Proceedings of the 32<sup>nd</sup> Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 705–714, [preprint *quant-ph/0004017*].
- [36] Ambainis, A., "Lower bound for a class of weak quantum coin flipping protocols," preprint available at <http://arxiv.org/abs/quant-ph/0204063>.
- [37] Spekkens, R.W. and T. Rudolph, "A quantum protocol for cheat-sensitive weak coin flipping," *Physical Review Letters* **89**, 227901 (2002), [preprint *quant-ph/0202118*].

- [38] Ambainis, A., “A new protocol and lower bounds for quantum coin flipping,” in the *Proceedings of the 33<sup>rd</sup> Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2001), pp. 134–142, [preprint *quant-ph/0204022*].
- [39] Kitaev, A., “Quantum coin-flipping,” (presentation available at URL: <http://www.msri.org/publications/ln/msri/2002/qip/kitaev/1/index.html>); Ambainis, A., H. Buhrman, Y. Dodis, and H. Roehrig, “Multiparty quantum coin flipping,” preprint available at <http://arxiv.org/abs/quant-ph/0304112>.
- [40] Buhrman, H., R. Cleve, J. Watrous, and R. de Wolf, “Quantum fingerprinting,” *Physical Review Letters* **87**, 167902 (2001), [preprint *quant-ph/0102001*].
- [41] Gottesman, D. and I. Chuang, “Quantum digital signatures,” preprint available at <http://arxiv.org/abs/quant-ph/0105032>.
- [42] DiVincenzo, D.P., D.W. Leung, and B.M. Terhal, “Quantum data hiding,” *IEEE Transactions on Information Theory* **48**(3), 580–599 (2002), [preprint *quant-ph/0103098*].
- [43] Hayden, P., D. Leung, P.W. Shor, and A. Winter, “Randomizing quantum states: Constructions and applications,” preprint available at <http://arxiv.org/abs/quant-ph/0307104>.
- [44] Barnum, H., C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, “Authentication of quantum messages,” in the *Proceedings of the 43<sup>rd</sup> Annual IEEE Symposium on the Foundations of Computer Science* (FOCS '02), (IEEE Press, New York, 2002), pp. 449–458, [preprint *quant-ph/0205128*].
- [45] Oppenheim, J. and M. Horodecki, “How to reuse a one-time pad and other notes on authentication, encryption and protection of quantum information,” preprint available at <http://arxiv.org/abs/quant-ph/0306161>.
- [46] Gottesman, D., P. Hayden, D. Leung, and D. Mayers, unpublished, 2003.
- [47] Gottesman, D., “Uncloneable encryption,” *Quantum Information and Computing* **3**(6), 581–602 (2003), [preprint *quant-ph/0210062*].
- [48] Boykin, P.O. and V. Roychowdhury, “Optimal encryption of quantum bits,” *Physical Review A* **67**, 042317 (2003), [preprint *quant-ph/0003059*].
- [49] Mosca, M., A. Tapp, and R. de Wolf, “Private quantum channels,” in the *Proceedings of the 41<sup>st</sup> Annual IEEE Symposium on the Foundations of Computer Science* (FOCS '00), (IEEE Press, New York, 2000), pp. 547–553, [preprint *quant-ph/0003101*].
- [50] Crépeau, C., D. Gottesman, and A. Smith, “Secure multi-party quantum computing,” in the *Proceedings of the 34<sup>th</sup> Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2002), pp. 643–652, [preprint *quant-ph/0206138*].
- [51] Dumais, P., D. Mayers, and L. Salvail, “Perfectly concealing quantum bit commitment from any one-way permutation,” *Lecture Notes in Computer Science* **1807**, 300–315 (2000).
- [52] Adcock, M. and R. Cleve, “A quantum Goldreich-Levin theorem with cryptographic applications,” *Lecture Notes in Computer Science* **2285**, 323–334 (2002), [preprint *quant-ph/0108095*].