LA-UR-04-4085

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

July 19, 2004

Version 1.0

ARDA

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

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

List of Tables

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. Crepeau, 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 technology. 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

	Attributes				
QKD Implementation	**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

		Laboratory or local-area distances (< 200 m)							Campus-area distances (< 2 km)						
QKD Implementation Status		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	🟩	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

		Metro-area distances (< 70 km)							Long distances (> 70 km)						
QKD Implementation Status		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, scaleable 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, $D_K(C) = P$, 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°, -45°), 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 used 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).