Quantum Key Distribution: Boon or Bust?

Logan O. Mailloux
Air Force Institute of Technology

Michael R. Grimaila
Air Force Institute of Technology

Douglas D. Hodson
Air Force Institute of Technology

Colin V. McLaughlin
Naval Research Lab

Gerald B. Baumgartner
Laboratory for Telecommunication Sciences

ABSTRACT: *Quantum Key Distribution (QKD) is an emerging cybersecurity technology which exploits the laws of quantum mechanics to generate shared secret keying material between two geographically separated parties. The unique nature of QKD shows promise for high-security applications such as those found in banking, government, and military environments. However, real-world QKD systems contain a variety of implementation non-idealities which can negatively impact system security and performance. This article provides an introduction to QKD for security professionals and describes recent developments in the field. Additionally, comments are offered on QKD's advantages (i.e., the boon), its drawbacks (i.e., the bust), and its foreseeable viability as a cybersecurity technology.*

Quantum Key Distribution (QKD) is an emerging cybersecurity technology which provides the means for two geographically separated parties to grow "unconditionally secure" symmetric cryptographic keying material. Unlike traditional key distribution techniques, the security of QKD rests on the laws of quantum mechanics and not computational complexity. This unique aspect of QKD is due to the fact that any unauthorized eavesdropping on the key distribution channel necessarily introduces detectable errors (Gisin, Ribordy, Tittel, & Zbinden, 2002). This attribute makes QKD desirable for high-security environments such as banking, government, and military applications. However, QKD is a nascent technology where implementation non-idealities can negatively impact system performance and security (Mailloux, Grimaila, Hodson, Baumgartner, & McLaughlin, 2015). While the QKD community is making progress towards the viability of QKD solutions, it is clear that more work is required to quantify the impact of such non-idealities in real-world QKD systems (Scarani & Kurtsiefer, 2009).

Written for security practitioners, managers, and decision makers, this article provides an accessible introduction to QKD and describes this seemingly strange quantum communications protocol in readily understandable terms. Additionally, this article highlights recent developments in the field from the 5th international Quantum Cryptography conference (QCrypt) hosted in fall of 2015 with an eye towards the US hosted conference in 2016. Lastly, we comment on several of

QKD's advantages (i.e., the boon) and its drawbacks (i.e., the bust) while also considering QKD's viability as a cybersecurity technology.

What is QKD?

The genesis of QKD traces back to the late 1960s, when Stephen Wiesner first proposed the idea of encoding information on photons to securely transfer messages (Wiesner, 1983). In 1984, the physicist Charles Bennett and cryptographer Gilles Brassard worked together to mature this idea by introducing the first QKD protocol, known as "BB84" (Bennett & Brassard, 1984). Five years later, they built the first QKD prototype system which was said to be "secure against any eavesdropper who happened to be deaf" as it made audible noises while encoding crypto key onto single photons (Brassard, 2006). From its relatively humble beginnings, QKD has gained global interest as a unique cybersecurity solution with active research groups across North America, Europe, Australia, and Asia. Moreover, commercial offerings are now available from several vendors around the world: ID Quantique, SeQureNet, Quintessence Labs, MagiQ Technologies, Qasky Quantum Science Technology, and QuantumCTek (Oesterling, Hayford, & Friend, 2012).

Figure 1 illustrates a notional QKD system architecture consisting of a sender "Alice," a receiver "Bob," a quantum channel (an optical fiber or line-of-sight free space path), and a classical channel (a conventional network connection). Alice is shown with a laser source configured to generate single photons, while Bob measures them using specialized Single Photon Detectors (SPDs). The QKD system provides a point-to-point solution for generating shared secret key, , which can be used to encrypt sensitive data, voice, or video communications as desired by the user.

Commercial QKD systems often use the secret key to increase the security posture of traditional symmetric encryption algorithms through frequent re-keying. For example, a QKD system can be used to update a 256-bit AES key once a second. This increases the cryptosystem's security posture by significantly reducing the time and information available to an adversary for performing cryptanalysis.

Alternatively, QKD systems can be used to provide an unlimited supply of secret keying material for use in the one-time pad encryption algorithm – the only known cryptosystem to achieve perfect secrecy (Vernam, 1926), (Shannon, 1949). However, the one-time pad has strict keying requirements, which are not easy to meet with conventional technologies. More specifically, the keying material must be: 1. truly random, 2. never reused, and 3. as long as the message to be encrypted. Thus, the appeal of QKD is found in its ability to generate (or grow) shared cryptographic key, making unbreakable one-time pad encryption configurations possible.

How Does QKD Work?

To understand how QKD works, we describe the original BB84 prepare-and-measure, polarization-based protocol as it remains a popular implementation choice and is relatively easy to understand compared to other QKD protocols (Gisin, Ribordy, Tittel, & Zbinden, 2002).

Figure 2 illustrates the QKD protocol as a series of eight steps. While these steps (or processes) can be depicted in a number of ways, we have chosen this flow to clearly illustrate how the QKD protocol behaves. In an actual system, these steps would most likely overlap and/or execute in parallel. Note that *Quantum Exchange* is the only step where the laws of quantum mechanics are directly applicable.

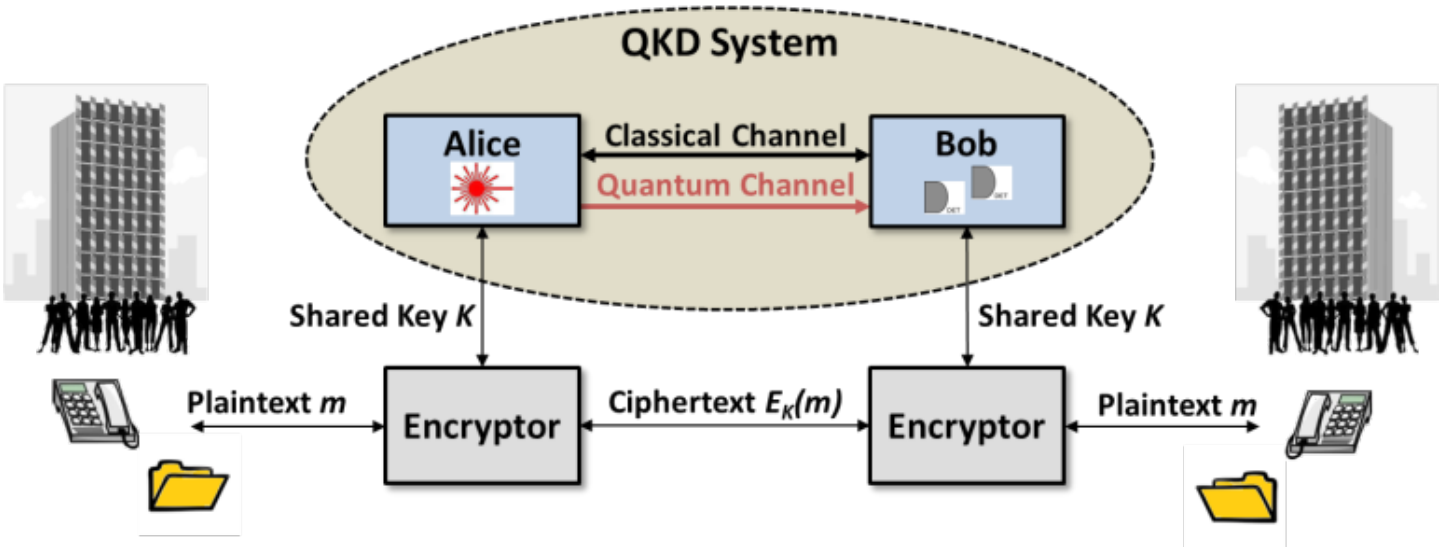


Figure. 1. Quantum Key Distribution (QKD) system context diagram. The sender "Alice" and receiver "Bob" are configured to generate shared secret key for use in bulk encryptors, where the quantum channel (i.e., a free space or optical fiber link) is used to securely transmit single photons and the classical channel is used to control specific QKD processes and protocols.

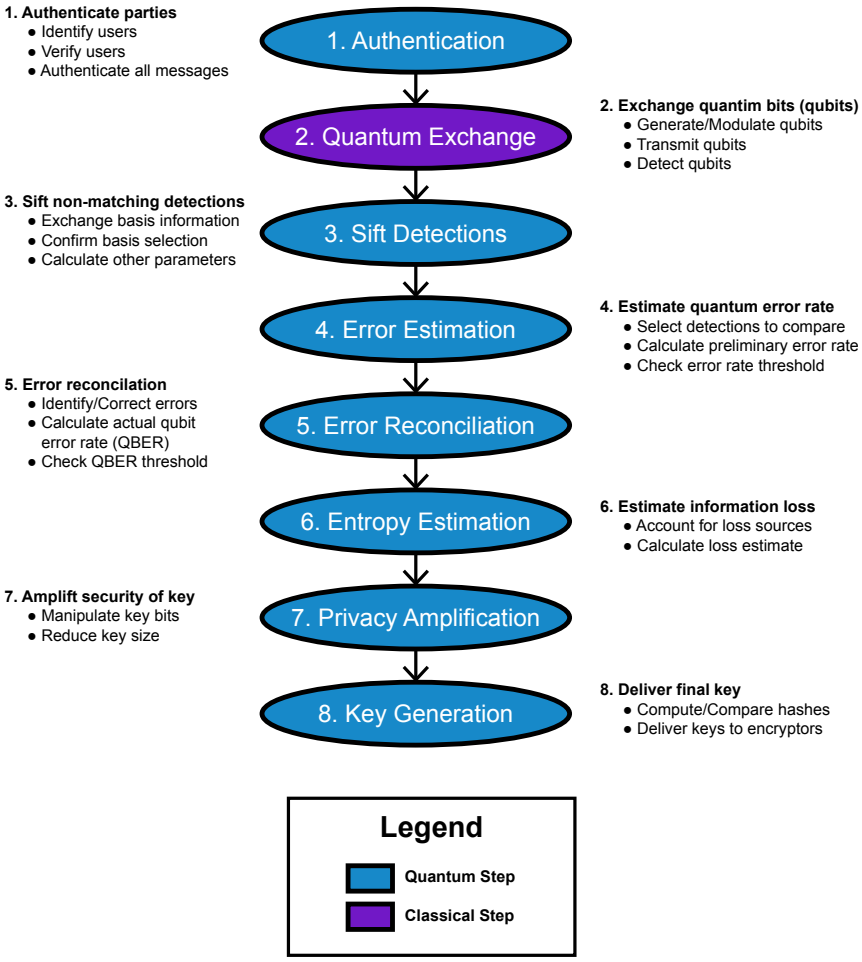


Figure. 2. Eight steps of the Quantum Key Distribution (QKD) process.

Somewhat of a misnomer, most of the QKD protocol is achieved through classical information theory "post-processing" steps.

In step 1, Alice and Bob authenticate with each other to ensure they are communicating with the expected party. Typically, this authentication is accomplished with the lesser known Wegman-Carter authentication technique to meet QKD's unconditional security claim (Scarani, et al., 2009). Moreover, unlike most cyber systems which authenticate only when initiating communications, QKD systems often utilize a transactional authentication scheme where authentication occurs after each step (or a sequence of steps) according to the specific system implementation.

Table 1. The prepare and measure, polarization-based BB84 QKD protocol.

Alice prepares single photons			Bob measures single photons	
Random encoding basis	Random bit value	Prepared photon state	Random decoding basis	Measurement result
⊕	0	$\|\leftrightarrow\rangle$	⊕	0 or 1
⊕	1	$\|\updownarrow\rangle$	⊗	Random
⊗	0	$\|\swarrow\rangle$	⊕	Random
⊗	1	$\|\searrow\rangle$	⊗	0 or 1

During quantum exchange (step 2), Alice prepares single photons, known as quantum bits or "qubits," in one of four polarization states $|\leftrightarrow\rangle$, $|\updownarrow\rangle$, $|\swarrow\rangle$, or $|\searrow\rangle$. The photon's polarization state is prepared according to a randomly selected basis and bit value as shown in Table 1. Each photon is then transmitted to Bob through the quantum channel, where it can be subject to significant loss (e.g., >90% loss is common). This is due to the loss that is experienced by single photons when they propagate over long distances through optical fiber or line-of-sight free space links. Due to the inherent challenges of single photon propagation, a majority of Alice's photons are lost during transmission, thereby limiting the system's effective operational distance to <100 km (Scarani, et al., 2009).

Assuming Alice's encoded photon arrives at Bob, he must randomly select a measurement basis for each detected photon. If Bob measures the photon with the correctly matching basis, the encoded bit value (0 or 1) is obtained with a high degree of confidence. Conversely, if Bob measures the photon with the incorrect basis, a random result occurs and the originally prepared bit value is destroyed. This quantum mechanical phenomenon underpins QKD's secure key generation where measuring a photon in flight forces its encoded state to collapse and prevents accurate copies from being made (i.e., the No Cloning Theorem) (Wootters & Zurek, 1982). Quantum exchange results in a series

of detections at Bob, which need to be correlated with Alice's sent photons through a sifting process.

In step 3, Bob's detections are sifted to eliminate incorrect (non-matching) basis measurements. In general, 50% of Bob's detections will be in the wrong basis and sifted out because of his random basis selection. This results in a shared sifted key, known as the "raw key," in both Alice and Bob approximately half the size of Bob's initial set of detections.

Next, an estimate of the quantum exchange error rate is calculated in step 4. Typically, a random percentage of bits are selected and compared over the classical channel. The estimated error rate is used to inform the error reconciliation technique (step 5), and can also be used to conduct an initial security check. This step is particularly important for QKD's theoretical security posture as all errors during quantum exchange are attributed to eavesdroppers since the QKD protocol cannot discriminate between noise and malicious interference. Thus, if the estimated error rate exceeds the predetermined QKD error threshold (e.g., 11%), the raw key must be discarded as an adversary is assumed to be listening (Scarani, et al., 2009). Typically, the key generation is then restarted.

In step 5, error reconciliation is performed to correct any errors in Alice and Bob's raw keys. Due to device non-idealities and physical disturbances during quantum exchange, expected error rates are typically 3-5% (Gisin, Ribordy, Tittel, & Zbinden, 2002). Error reconciliation techniques employ specialize bi-directional correction algorithms (e.g., Winnow, Cascade, or Low-Density Parity-Check) to minimize the amount of information "leaked" over the classical channel to eavesdroppers (Scarani, et al., 2009). With a high probability, this step results in a perfectly matched, error free shared secret key between Alice and Bob. The error reconciliation step results in a formalized Quantum Bit Error Rate (QBER), which is again checked against the QKD security proof threshold (e.g., 11%) to determine if an eavesdropper is listening on the quantum key distribution channel (Scarani, et al., 2009). If the security threshold is exceeded, the key must be discarded and the process is restarted.

Next, entropy estimation (step 6) accounts for the amount of secret key information leaked while executing the QKD protocol steps. For example, during quantum exchange, information leakage occurs from non-ideal laser sources which produce insecure multi-photon pulses. In another example, error reconciliation communications over the classical channel leaks information about the secret key. In general, conservative loss estimates are made; however, implementations may differ considerably (Slutsky, Rao, Sun, Tancevski, & Fainman, 1998). The entropy estimate is then passed to the privacy amplification step, which corrects for the information leakage and ensures the eavesdropper has negligible information regarding the QKD-generated shared secret key. More specifically, step 7 employs advanced information theory techniques such as a universal hash function to produce a more secure final shared secret key (Scarani, et al., 2009).

Lastly, in order to ensure the final symmetric crypto keys are the same, a hash of Alice and Bob's keys are compared. If they match, the keys are delivered to the system owner. These unconditionally secure shared symmetric keys can then be used as desired by the user to protect sensitive information with the unbreakable one-time pad encryption scheme or supplement more practical encryption schemes such as AES. For readers interested in more details, a security-oriented description of QKD is available in (Mailloux, Grimaila, Hodson, Baumgartner, & McLaughlin, 2015) with comprehensive physics based discussions in (Scarani, et al., 2009) and (Gisin, Ribordy, Tittel, & Zbinden, 2002).

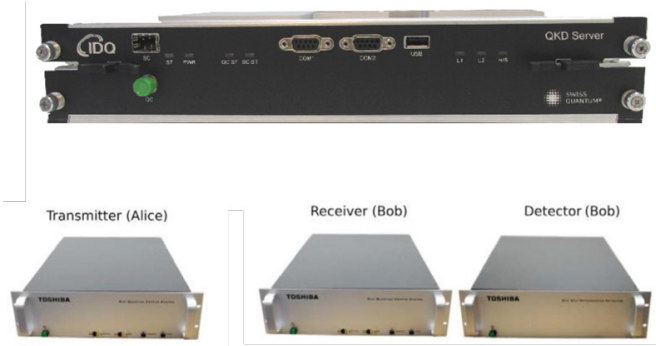


Figure 3. The ID Quantique (IDQ) rack mountable QKD system is shown on the top (ID Quantique, 2016) and the Toshiba record holding hybrid QKD system is shown on the bottom (Dixon, et al., 2015).

Observations from Quantum Cryptography Conference (QCrypt) 2015

Over the past several years, the annual QCrypt conference has served as the world's premier forum for students and researchers to present and collaborate on all aspects of quantum cryptography. QCrypt is also the primary forum for announcing the year's best QKD results. In late 2015, the fifth QCrypt conference was hosted in Tokyo, Japan and attended by more than 275 participants with a largely international audience of physicists, information theorists, and cryptographers (Quantum Cryptography Conference, 2016). From this conference, key observations are offered for the reader to gain perspective on recent developments in the quantum cryptography field.

- **Striving for Commercial Viability** – QCrypt 2105 began with several demonstrations and talks focused on practically-oriented QKD systems which balance cost, performance, and security trades towards affordability. In particular, the QKD industry leader, ID Quantique, unveiled a completely redesigned QKD blade system which employs a new quantum exchange protocol, anti-tamper precautions, and additional security features to mitigate quantum attacks (ID Quantique, 2016). Likewise, Toshiba Research Laboratory Europe, supported by Japan's National Institute of Information and Communications Technology, prominently displayed their record breaking QKD system. The Toshiba system boasts the world's highest key rates, improved user interface, and automated synchronization for increased usability over metropolitan distances (Dixon, et al., 2015). Unlike early experimental QKD configurations, these systems are designed to be rack mountable and more

easily integratable into existing communications structures. Figure 3 shows both the commercially viable ID Quantique and Toshiba QKD systems.

- **Fielding QKD Networks –** For distributed networks and long distance operation, QKD requires the use of either quantum repeaters or satellite-based solutions. While fully functional quantum repeaters are years away from being realized, simpler stop-gap "trusted node" configurations have been successfully fielded (Scarani, et al., 2009). These QKD networks utilize a series of back-to-back QKD systems to cover larger metropolitan areas and support long-haul backbone distances. Using this method, China is building the world's largest QKD network along its west coast employing 46 nodes to cover some 2,000 km (Wang, et al., 2014). Similarly, one of the conference's keynotes, the US research organization Battelle, described their development of trusted nodes with ID Quantique to support a 1,000 km planned run from Columbus, Ohio to Washington, D.C. (Quantum Cryptography Conference, 2016). With respect to satellite-to-ground QKD, research centers in America, Canada, Europe, Japan, and China are exploring the feasibility of and conducting experiments to prove the feasibility of transmitting single photons from a Low Earth Orbit (LEO) satellite through the Earth's turbulent atmosphere. Most notably, China is actively pursuing their goal of launching a QKD satellite by 2016 (Bieve, 2016). Figure 4 depicts both China's terrestrial QKD network and their planned space-based QKD links.
- **Barriers to Acceptance –** While a majority of the research-focused conference is focused on improvements to QKD protocols, quantum hardware, and information theory advancements, arguably, the most important theme of the conference pertained to the acceptance of QKD (or lack thereof) as a cybersecurity solution. As repeatedly recognized during QCrypt 2015, several significant barriers to QKD's acceptance exist. This was perhaps best captured by the field's most recognized researcher, Dr. Nicolas Gisin, who boldly stated "The quantum technology era has started… In 10 years either QKD will have found its markets or will be dead" (Gisin, 2015). In a cybersecurity community that typically adopts new technological solutions rather quickly, quantum based security technologies are slow to be adopted. Perhaps, security professionals are uncomfortable with the topic of quantum mechanics? Or perhaps, QKD developers are just now starting to make progress on critical implementation security issues, interoperability standards, and formal certifications (ETSI, 2015).

From these overarching conference themes, we next elaborate on some of QKD's advantages and disadvantages in order to help security professionals better understand the technology and its application. Thus, while a bit subjective in nature, and not without debate, we've chosen to describe three ways in which QKD is a boon to the cybersecurity community and three ways in which it is a bust.

The Boon

While there are several ways to describe the advantages of QKD, in this article the authors' have chosen to approach this challenge from the user's perspective. Meaning, we desire to provide a useful commentary which addresses the utility of QKD (and its related developments) for an end user and not merely elaborate on the merits of its research or what it could be.

1. **Generates Unconditionally Secure Keying Material –** Leveraging the laws of quantum mechanics, QKD is the only known means which can grow unlimited amounts of symmetric keying material to effectively employ the one-time pad cryptosystem (the only unbreakable encryption scheme known). This formalized information-theoretic security foundation is much stronger than conventional encryption techniques which depend on demonstrated computational complexity. This is precisely why QKD has gained global recognition as an emerging cybersecurity technology in the face of quantum computing advances which threaten other conventional cryptosystems such as RSA.
2. **Quantum Random Number Generators –** In order to maintain their information-theoretic security posture, QKD systems require true sources of randomness. Thus, the advancement of QKD has successfully facilitated the development of quantum random number generators. These devices provide a physical source of randomness based on quantum phenomenon which is desirable for cryptographic devices, software applications, and other industries. Of note, the gaming/gambling industry is said to be the world's largest consumer of random number generators and a fiscally rewarding enterprise. While QKD upstarts seem to come and go, there is a definite need for cheap and reliable sources of entropy in the commercial market.
3. **Strengthens the Cybersecurity Field –** QKD encourages multidisciplinary collaboration amongst information theorists, engineers, cryptography experts, security professionals, and physicists that may not occur otherwise. Establishing these types of interactions is critical for advancements in several cyber related fields such as quantum communication, quantum sensing, and quantum computing. For example, the integration of computer scientists and quantum physicists is necessary for the development and utilization of quantum computing algorithms. On a related note, QKD has also brought about the occurrence of "Quantum Hacking" (Institute of Quantum Computing, University of Waterloo, 2014). This growing specialty area is testing the security of new quantum technologies and protocols, and perhaps someday, we'll even have security assessments which include quantum red teams.

The Bust

QKD systems have performance limitations, device non-idealities, and system vulnerabilities which are not well understood (Scarani & Kurtsiefer, 2009). Thus, potential users often question both the effectiveness of the technology and its system security posture. For QKD to be accepted as a cybersecurity technology the following critical issues (at a minimum) should be addressed.

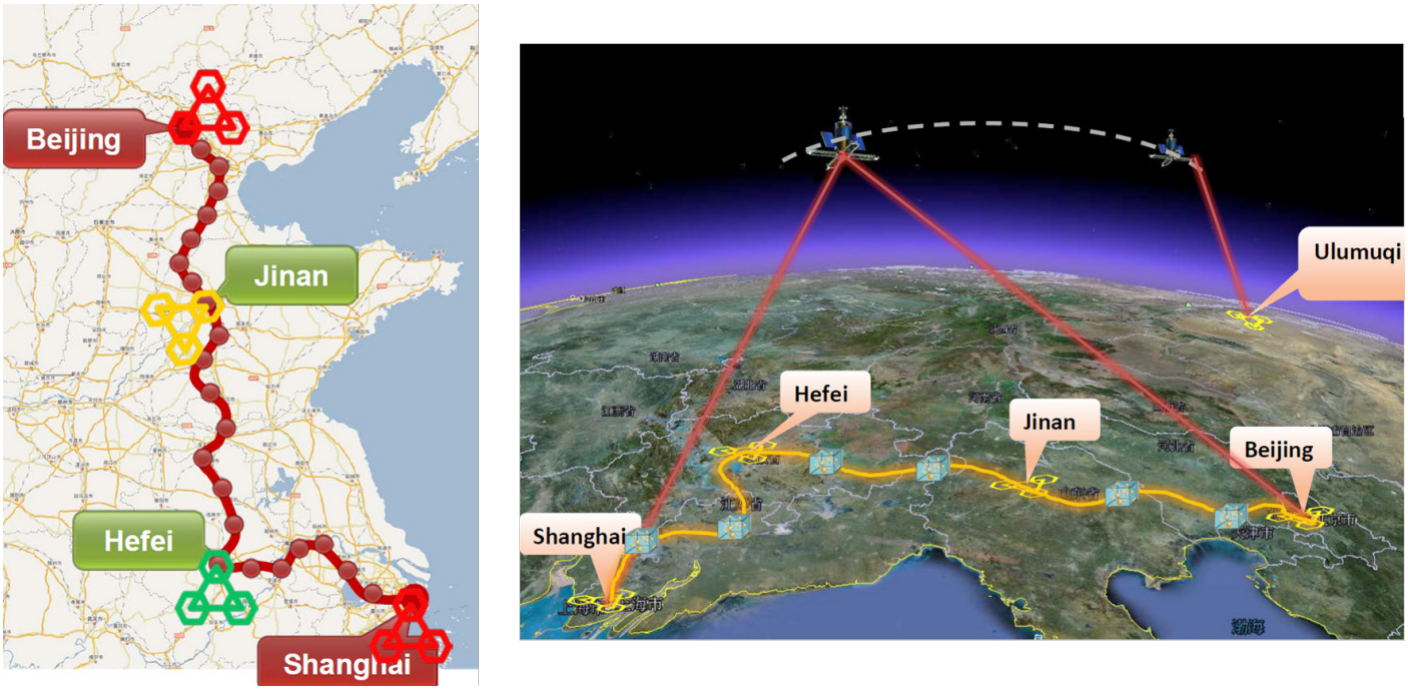


Figure 4. China's 46 node terrestrial QKD network is shown on the left and the planned space-based QKD network is shown on the right (Quantum Cryptography Conference, 2016).

1. **QKD is Point-to-Point Technology –** Because QKD is a point-to-point solution, it does not scale well for modern communications infrastructures. While gains are being made towards networked key management solutions, they are fundamentally limited by QKD's quantum underpinnings, which prevent the amplification of single photons (Wootters & Zurek, 1982). Given this critical limitation, QKD does not appear to be a good fit for wide scale implementation and may only be viable for specialized two site applications such as encrypted voice communications in a metropolitan area.
2. **Implementation Security Vulnerabilities –** QKD systems have implementation non-idealities which introduce vulnerabilities and negatively impact both performance and security. For example, these "unconditionally secure" QKD systems protocols are vulnerable to attacks over the quantum channel, including man-in-the-middle (authentication failures), intercept/resend (measuring and replacing photons), photon number splitting (stealing photons), and blinding optical receivers (unauthorized laser sources). Additionally, QKD systems are also vulnerable to common cybersecurity attacks against computers, applications, and protocols. These implementation security issues and their resulting vulnerabilities must be well-studied and addressed through established architectural design principles, verifiable designs, and assured operational configurations to provide trustworthy systems to end users.
3. **No Formal Certification Method –** As high-security crypto devices, QKD systems should undergo formal security assessments and certification processes to address (at a minimum) physical attacks, side channel analysis, and data manipulation. However, within the QKD community there is little discussion thereof, and arguably sluggish progress towards an independent certification process (ETSI, 2015). Furthermore, QKD developers must adopt a more holistic view of security including proactive techniques such as assuring secure operational baselines and continuous monitoring of the system's communication links.

Despite QKD's drawbacks, the technology does show promise as an enabler to unbreakable encryption (i.e., generating unlimited amounts of random key for use in On-Time Pad encryption) for niche applications such as point-to-point communications and data transfer.

Conclusion

Security professionals recognize that ongoing advancements in quantum computing (along with Shor's algorithm for quickly factoring large prime numbers) threaten the security of modern public key cryptography techniques such as RSA (Monz, et al., 2015). Thus, new *post-quantum* security solutions need to be given serious consideration as indicated by the National Security Agency's recent announcement specifying "a transition to quantum resistant algorithms" for their cryptographic Suite B algorithms (NSA, 2015). While this transition will occur slowly over time, organizations with significant data protection requirements such as the US Government (i.e., 25 years of data protection) must start thinking about post-quantum crypto solutions now.

While unbreakable one-time pad encryption solutions enabled by QKD provide the ultimate protection available (they are proven secure against advances in quantum computing), they do not fit well into the established communications infrastructure. Conversely, quantum resistant algorithms (encryption techniques which are shown to not be easily broken by quantum computers) have the benefit of fitting nicely into the existing infrastructure (Bernstein, 2009).

With an eye towards QCrypt 2016, hosted by the US based Joint Center for Quantum Information and Computer Science, perhaps the QKD community will begin to adopt a wider perspective on the field of quantum cryptography. For example, the US's premier quantum center seeks to more broadly advance the state of the art in quantum algorithms, quantum communication, and quantum computing instead of merely focusing on QKD (University of Maryland, 2016). Moreover, the US National Institute of Standards and Technology (NIST) recently stood up a multi-year project to explore quantum resistant algorithms (2016) and a new international conference series on post-quantum cryptography is quickly gaining attention (2016). Perhaps, these events are evidences that a change is occurring in the QKD community, an evolution towards more viable cryptographic solutions. ■

Acknowledgments

This work was supported by the Laboratory for Telecommunication Sciences [grant number 5743400-304-6448].

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

BIBLIOGRAPHY

[1] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, *175, no. 0.*

[2] Bernstein, D. J. (2009). *Post-quantum cryptography.* Springer.

[3] Bieve, C. (2016, January 13). *China's quantum space pioneer: We need to explore the unknown*. Retrieved from Nature: http://www.nature.com/news/china-s-quantum-space-pioneer-we-need-to-explore-the-unknown-1.19166

[4] Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., . . . al., e. (2015). High speed prototype quantum key distribution system and long term field trial. *Optics Express, 23*(6), 7583-7592.

[5] ETSI. (2015, June 08). *Quantum key distribution standards*. Retrieved from www.etsi.org/technologies-clusters/technologies/quantum-key-distribution

[6] Gisin, N. (2015, October 21). *Quantum Cryptography: where do we stand?* Retrieved from https://www.youtube.com/watch?v=Vk9T-tVAI4c&feature=youtu.be

[7] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1), 145-195. Retrieved from 10.1103/RevModPhys.74.145

[8] ID Quantique. (2016). Retrieved from http://www.idquantique.com/

[9] Institute of Quantum Computing, University of Waterloo. (2014). *Quantum hacking lab*. Retrieved Mar 14, 2014, from http://www.vad1.com/lab/

[10] Mailloux, L. O., Grimaila, M. R., Hodson, D. D., Baumgartner, G., & McLaughlin, C. (2015). Performance evaluations of quantum key distribution system architectures. *IEEE Security and Privacy, 13*(1), 30-40.

[11] *Science, 351*(6277), 1068-1070. Monz, T., Nigg, D., Martinez, E. A., Brandl, M. F., Schindler, P., Rines, R., . . . Blatt, R. (2015). Realization of a scalable Shor algorithm.

[12] NIST. (2016, March 07). *Post-Quantum Crypto Project*. Retrieved April 09, 2016, from http://csrc.nist.gov/groups/ST/post-quantum-crypto/

[13] NSA. (2015, August 19). *Cryptography Today*. Retrieved from Information Assurance: https://www.nsa.gov/ia/programs/suiteb_cryptography/

[14] Oesterling, L., Hayford, D., & Friend, G. (2012). Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, (pp. 156-161). Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6459842

[15] Post-Quantum Cryptography. (2016, January 18). *Post-Quantum Crypto 2016*. Retrieved January 18, 2016, from https://pqcrypto2016.jp/

[16] Quantum Cryptography Conference. (2016). *QCrypt 2015*. Retrieved from 2015.qcrypt.net

[17] Scarani, V., & Kurtsiefer, C. (2009). The black paper of quantum cryptography: real implementation problems. *Theoretical Computer Science, 560(1), 27–32.*

[18] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301-1350. Retrieved from ttp://dx.doi.org/10.1103/RevModPhys.81.1301

[19] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal, 28*, 656-715.

[20] Slutsky, B., Rao, R., Sun, P.-C., Tancevski, L., & Fainman, S. (1998). Defense frontier analysis of quantum cryptographic systems. *Applied Optics, 37*(14), 2869-2878.

[21] University of Maryland. (2016, April 30). *Joint Center for Quantum Information and Computer Science*. Retrieved from http://quics.umd.edu/

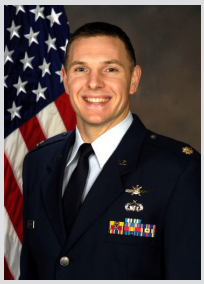
[22] Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *American Institute of Electrical Engineers, Transactions of the, 45*, 295-301.

[23] Wang, S., Chen, W., Yin, Z.-Q., Li, H.-W., He, D.-Y., Li, Y.-H., . . . et al. (2014). Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express, 22*(18), 21739-21756.

[24] Wiesner, S. (1983). Conjugate coding. *ACM Sigact News, 15*(1), pp. 78-88. Retrieved from http://dx.doi.org/10.1145/1008908.1008920

[25] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature,* 299(5886), 802-803. doi:10.1038/299802a0

ABOUT THE AUTHORS



Logan O. Mailloux
Air Force Institute of Technology

Logan O Mailloux, CISSP, CSEP (BS 2002, MS 2008, PhD 2015) is a commissioned officer in the United States Air Force and Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. His research interests include system security engineering, complex information communication and technology implementations, and quantum key distribution systems. He is a member of Tau Beta Pi, Eta Kappa Nu, INCOSE, the ACM, and IEEE.

Douglas D. Hodson
Air Force Institute of Technology

Douglas D Hodson (BS 1985, MS 1987, PhD 2009) is an Assistant Professor of Software Engineering at the AFIT, Wright-Patterson AFB, Ohio, USA. His research interests include computer engineering, software engineering, real-time distributed simulation, and quantum communications. He is also a DAGSI scholar and a member of Tau Beta Pi.

Michael R. Grimaila
Air Force Institute of Technology

Michael R Grimaila, CISM, CISSP (BS 1993, MS 1995, PhD 1999, Texas A&M University) is Professor and Head of the Systems Engineering department and member of the Center for Cyberspace Research (CCR) at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. He is a member of Tau Beta Pi, Eta Kappa Nu, the ACM, a Senior Member of the IEEE, and a Fellow of the ISSA. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management and security, and systems engineering.

Colin V. McLaughlin
Naval Research Lab

Colin V McLaughlin, PhD (BA 2003, PhD 2010) is a Research Physicist at the United States Naval Research Laboratory, Washington, D.C., USA. He specializes in photonic communication devices and systems.

Gerald B. Baumgartner
Laboratory for Telecommunication Sciences

Gerald B. Baumgartner, PhD (BS 1971, MS 1973, PhD 1980, Illinois Institute of Technology) is a Research Physicist at the Laboratory for Telecommunications Sciences, College Park, Maryland, USA. He is a member of the American Physical Society, the Optical Society of America and the Society for Industrial and Applied Mathematics. Dr Baumgartner's research interests include quantum optics, quantum communications, quantum information, communications security, communications system modeling and simulation and statistical signal processing.