Computer and Information Science; Vol. 13, No. 1; 2020
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Quantum Cryptography for Nuclear Command and Control

Derek Hall[1], & Timothy Sands[2]

[1] Graduate School of Engineering and Applied Sciences, Naval Postgraduate School, Monterey, USA

[2] Fu Foundation School of Engineering and Applied Science (CVN), Columbia University, New York, USA

Correspondence: Timothy Sands, Fu Foundation School of Engineering and Applied Science (CVN), Columbia University, New York, USA.

Received: December 17, 2019 Accepted: January 15, 2020 Online Published: January 16, 2020

doi:10.5539/cis.v13n1p72 URL: https://doi.org/10.5539/cis.v13n1p72

Abstract

The nuclear inventory of Russia and the USA currently comprises 12,685 warheads in a large network of vehicles; and the interconnected network is managed by a command and control communication system. This command and control communication system (C3) must also relay information from numerous airborne, space-born, and ground sensors throughout the network in potentially degraded environments and are nonetheless meant to securely hold transmissions that must be held to the highest standards of encryption. C3 systems are also arguably one of the most challenging systems to develop, since they require far more security, reliability, and hardening compared to typical communication systems, because they typically must (absolutely) work while other systems fail. Systems used for C3 are not always cutting-edge technology, but they must be upgraded at crucial junctures to keep them at peak performance. This manuscript outlines a blueprint of a way to embed current and future systems with revolutionary encryption technology. This will transform the security of the information we pass to our C3 assets adding redundancy, flexibility, and enhanced speed and insure vehicles and personnel in the system receive network message traffic. Quantum key distribution (QKD) has the potential to provide nearly impregnable secure transmissions, increased bandwidth, and additional redundancy for command and control communication (C3). While QKD is still in its adolescence, how QKD should be used or C3 must be charted out before it can be engineered, tested, and implemented for operations. Following a description QKD functionality, its pros and cons, we theorize the best implementation of a QKD system for C3.

Keywords: quantum key distribution, secret-key cryptography, quantum safe cryptography, applied cryptography, wireless technologies for advanced applications, security and privacy issues, CPS security and privacy, CPS fault detection and recovery, quantum internet

1. Introduction

1.1 The Problem

The nuclear inventory of Russia and the USA currently comprises 12,685 warheads in a large network of bombers, intercontinental ballistic missiles and submarine-launched ballistic missiles, in addition to bombs carried on a host of vehicles; and the interconnected network is managed by a command and control communication system.

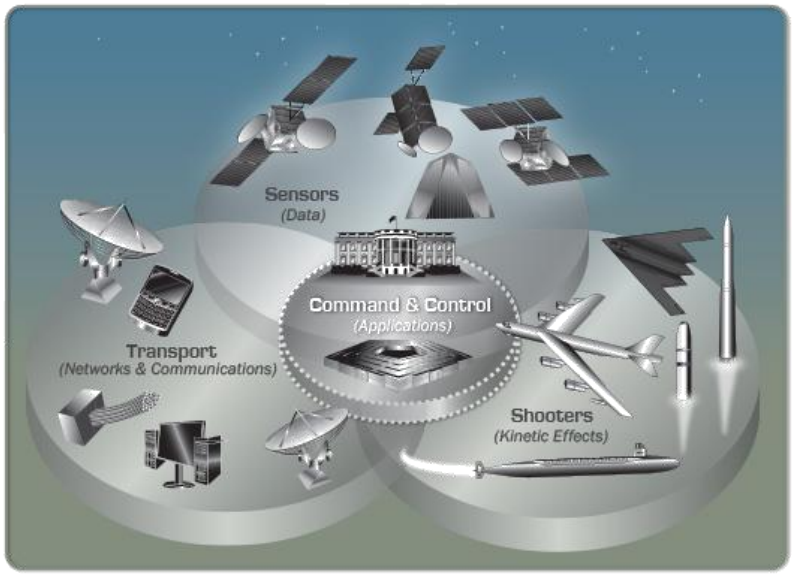

Figure 1. Schematic of sensor and vehicles and coordinating systems that must collaborate in often degraded environments with high throughput and data security (OSD, 2016]

This command and control communication system (C3) in Figure 1 must also relay information from numerous airborne, space-born, and ground sensors throughout the network in potentially degraded environments and are nonetheless meant to securely hold transmissions that must be held to the highest standards of encryption. C3 systems are also arguably one of the most challenging systems to develop, since they require far more security, reliability, and hardening compared to typical communication systems, because they typically must (absolutely) work while other systems fail. Systems used for C3 are not always cutting-edge technology. Currently, networks typically use copper, fiber, or radio waves (some are being upgraded with conventional fiber optic communications) to send information encrypted by conventional cryptography like Advanced Encryption Standard (AES) (Alapatt, et al. 2018), and High Assurance Internet Protocol Encryptor (HAIPE) (Irani, 2010). These conventional encryption methods, while useful, are increasingly becoming obsolete in an age where a quantum computer can crack them in mere hours (Morris, 2017). However, to combat quantum computing, companies and countries are turning to quantum encryption methods to enable more secure information (Morris, 2017). One such method is Quantum Key Distribution (QKD) (Morris, 2017). Bricout and Chailloux studies classical attacks on the relative bit commitment scheme using timing and location constraints, demonstrating efficacy as long as the number of rounds in the protocol was not large. (Bricout, et al., 2017) Kashefi and Pappa sought to guarantee input and computational secrecy without the necessity of universal quantum computers for everyday users by isolating the implementation of quantum computation to the server on a network (Kashefi, et al., 2017). This manuscript proposes a similar scheme of limiting quantum implementation to the most practical subset. An interesting application of quantum protocols was studied by Sikora where two dishonest die-rollers compared favorably to optimal coin-tossing protocols, finally revealing protocols very close to Kitaev's lower bound for any $D \geq 3$ (Sikora, et al. 2017). Kashefi and Wallden explored extending quantum computation protocols enabling an almost-classical client to delegate a quantum computation to an untrusted quantum server in the form of a garbled circuit (Kashefi, et al., 2017). Usenko and Fili address the role of the phase-insensitive trusted preparation and noise detection in the security of a continuous-variable quantum key distribution by considering the Gaussian protocols on the basis of coherent and squeezed states and studying them in the conditions of Gaussian lossy and noisy channels. (Usekno, et al., 2016)). Jacobsen, et al., proposed loosening the requirement for shot-noise limited operation in existing experimental implementations of continuous-variable quantum key distribution, which permits the cheaper laser sources, and potentially integrated systems (Jacobsen, et al., 2015. Further developments in quantum key distribution with coherent light were studied by Curty, et al. (Curty, et al., 2015). Shaari, et al., introduced a security proof for two-way quantum key distribution protocols, against the most general eavesdropping attack, that utilize an entropic uncertainty relation (Shaari, et al., 2015). Most recently, Luyen (Luyen, 2019) elaborated Multivariate Public Key Cryptography (MPKC) as one of the main candidates in the area of signature schemes for post-quantum cryptography instantiating a secure and

efficient multivariate signature scheme, in fact a certificate Identity-Based Signature (IBS) scheme based on a scheme called Rainbow.

1.2 The Hypotheses and Research Design

This manuscript follows the line of thinking of Morris by illustrating implementation protocols for a command and control communications system (i.e. C2 or C3). The protocols are heuristically explained following Morris's methodology (Morris, 2017), and implementation is proposed resulting in QKD utilization with current copper, fiber, or radio communication systems, thereby taking all the positives from QKD without its weaknesses.

2. Method

Generically, Quantum Key Distribution utilizes the unusual effects that photons display on a quantum level, specifically, talking about the angular momentum of a photon and its measurements. When a photon is split into two via a beam splitter, these two photons' angular momentum is now entangled. As such, each has equal and opposite angular momentum typically considered up and down spin or 1 and 0. However, neither photon's angular momentum can be known until one is measured. Once a photon is measured, the momentum will change, thereby disentangling them. If two separated entangled photons are measured by different people (or quantum modems), they can compare their answers (unencrypted). If their answers agree with what they expected to measure, they both know they used the correct measurement for that photon; if not, they can discard that measurement (Morris, 2017). Referencing Figure 2, according to (Morris, 2017), a quantum cryptographic system will allow two people, say Alice and Bob, to exchange a secret key. The system includes a transmitter and a receiver. Alice uses the transmitter to send photons in one of four polarizations: 0, 45, 90, or 135 degrees. Bob uses the receiver to measure the polarization. According to the laws of quantum mechanics, the receiver can distinguish between rectilinear polarizations (0 and 90), or it can quickly be reconfigured to discriminate between diagonal polarization (45 and 135). It can never however distinguish both types. The key distribution requires several steps. Alice sends photons with one of four polarizations, which she can chosen at random. Figure 3 reveals that for each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (x). Bob records his measurement in Figure 4, but keeps it secret, and then publicly announces the type of measurements he made (Figure 4), and Alice tells him which measurements were correct (in Figure 5). Alice and Bob then keep all the cases where Bob's measure type was correct. These cases, translated into binary bits (ones and zeros) are kept as the key.

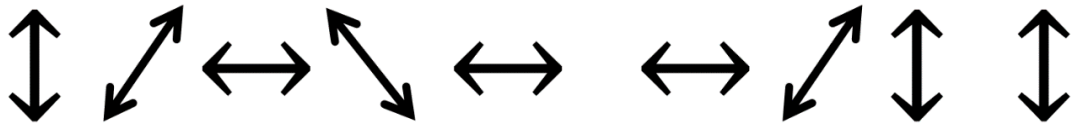

Figure 2. Alice uses the transmitter to send photons in one of four polarizations: 0, 45, 90, or 135 degrees. Bob uses the receiver to measure the polarization

Figure 3. for each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (x)

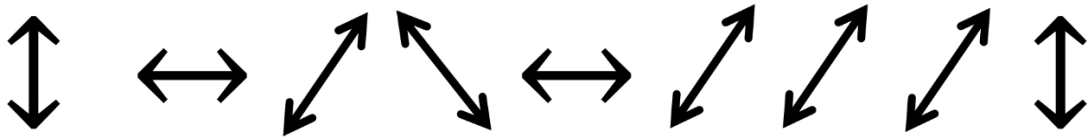

Figure 4. Bob's recorded measurements (that he kept secret)

Figure 5. Bob publicly announces the measurements be made, and Alice tells him which of his measurements were of the correct type

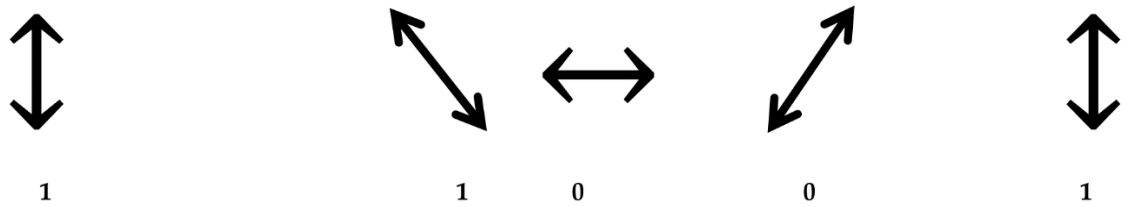

Figure 6. The key derived from all cases in which Bob measures correctly

If this is done for a series of photons, then each person has a series of correct measurements (and discarded incorrect measurements) of up and down spin or zeros and ones that are equal and opposite of each other. This series of zeros and ones are now the quantum encryption key which is completely random and could not have been intercepted. (See Figure 2 below for another explanation) If any of the photons were intercepted, measured, and passed along by a third party, known as the "man in the middle," whenever the photon was measured, it would change the photon's angular momentum thus changing the measurement the intended receiver would get and invalidate the measurement (Bub, 2015). Photons also cannot be duplicated, so even if it was measured, it couldn't be duplicated and forwarded to the intended receiver (Morris, 2017).

Systems enhanced with QKD not only provides assured link security but also allows for various other enhancements (Benslama, et al., 2017). Utilizing QKD requires photon transmission, which also enables laser and fiber optical communication. This would be far more bandwidth than typical copper or radio communications. Laser communications have been shown to reach assets that radiofrequency cannot. Laser communications can also be more discreet, making it harder to track transmitters and receivers. Further, QKD is based on quantum measurements which could easily be used to pass quantum information, also known as qubits.

Qubits have a couple of redeeming properties. First and most useful to C3, qubits can be used to pass more information than traditional bits. This can be done using super condensing coding and would exponentially increase the throughput of data. Second, qubits can be used to enable exchanges between quantum computers. However, for now, I would recommend the continued usage of classical computers within the C3 system for a couple of reasons. First, today's quantum computers are not mature enough to be placed within a viable C3 system. Also, C3 information systems are not complicated enough to require a quantum computer (Diamanti, 2016). A quantum computer would be part of the command and control construct, not embedded into the communication (IDQuantique, 2018).

Many of the limitations of quantum key distribution have to do with the maturity of the technology and should not be considered definitive. Most of these limits revolve around the equipment that develops the photons and measures them. Current systems are too slow and not accurate enough to deliver always entangled photons at extended distances (Bub, 2016). Typically, quantum keys can be created and measured around once a minute. Therefore, current technologies are not capable as QKD was initially envisioned (Jenner, 2014). As such, current usable quantum encryption systems are not wholly un-hackable, but still far superior to traditional systems.

Further, current equipment has a somewhat limited range. The current range of fiber systems is less than 100km, and in free space, entanglement has been seen at just over 1200km. While these limits can be problematic, they are only limitations of current systems and imaginations. Quantum technology, as it stands, will only get better. Improvements in photon generation and measurement systems will improve range, accuracy, and speed.

That said, some limits are more definitive. In free-space, photons used for quantum communication and encryption are susceptible to scintillation (Andrews, et al., 2002) and require line of sight. This means it will

almost certainly require a backup communication system, like radio frequency, copper, or fiber transmission to provide the guaranteed communication that is required for C3. Further, fiber connections, while being able to work around the line of sight and scintillation issues, have unavoidable limitations as well. Correctly, fiber nodes and lines can be easily identified as critical vulnerabilities if not thoroughly diversified and hardened. Fiber lines are more susceptible to the destruction of degradation than copper, radio, or satellite communications because if a fiber terminal loses power, it will not be able to pass information. While all these limits of QKD are daunting, the current and future benefits are worth the hardship. Solutions to most of these difficulties may seem daunting (Jian-Wei, 2001), but most can be solved by developing a well-integrated system (Mailoux, 2016).

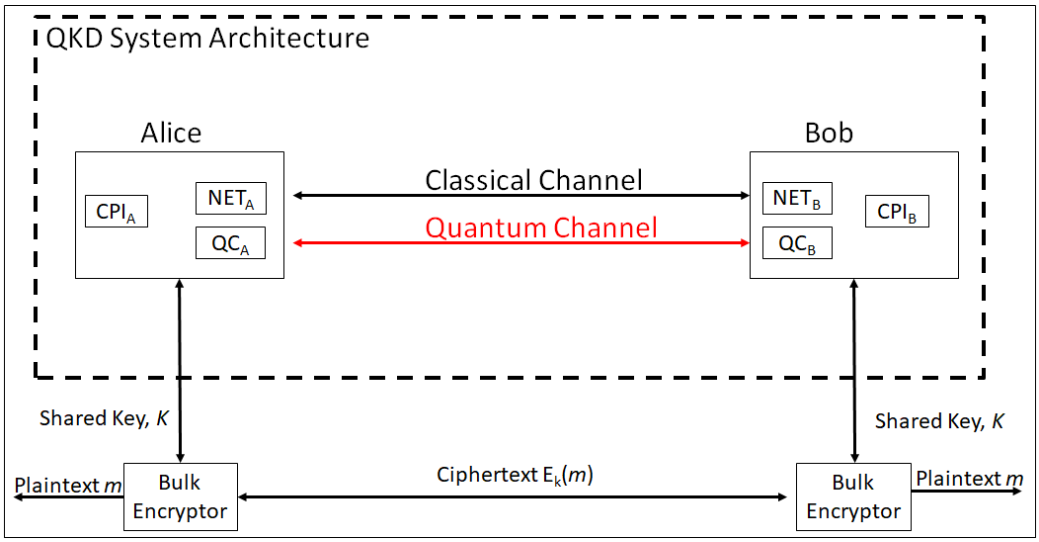

Figure 7. Reference QKD architecture

3. Results

Consider allowing the network with a baseline configuration depicted in Figure 7 (Morris, 2017) to be piecemealed together and linked with already-operational systems. In this sense, a communication system with QKD would have multiple layers of security and transmission types. Fundamentally QKD would act as an extra layer of encryption and would only update encryption codes and pass extra increased data when connections are capable. This is due primarily to the fact free-space laser communications are susceptible to scintillation, but it is also because the encryption keys can't be generated quickly enough. As earlier mentioned, the reduced speed of encryption keys implies QKD systems do not work as ideally envisioned. Instead, QKD is typically used to generate and pass encryption keys for other encryption types. This method allows encrypted transmissions in-between key creation, and updates the encryption keys: more frequently, automatically, and with entirely random numbers. This also allows QKD to be attached to current copper, fiber, or radio communication systems, thereby taking all the positives from QKD and leaving its weaknesses, making it a force multiplier, not a limiting factor. The following paragraphs explain how both classical and quantum encryption can be fused.

The proposed method involves both classical and quantum encryption. Since classical encryption is the backbone of typical network, all terminals must be able to switch from quantum encryption to classical encryption arbitrarily. Such a system would always require shared-keys between each possible link if quantum encryption is interrupted to maintain the integrity links. Next, consider how all nodes establish both quantum and classical links.

The first links established must be quantum encrypted links. Once the quantum encrypted links are established, they will pass shared encrypted keys for the classical links. Therefore, when photons are exchanged, and a quantum encrypted connection has been made, the link must be established as friendly. This will ensure the quantum mechanically secure connection was not made with the wrong a foreign player. Therefore, all nodes will have an established number like an Internet Protocol (IP) number. To pass the IP numbers without giving away the number will require a challenge and response. Each node will pass a random number, and the other node must return a counter number mathematically based on the random number to indicate its IP number. If the node does not return a number indicating the correct IP number, the connection is broken, and incursion is expected. Follow on connections may be attempted a limited amount of times before node is considered

compromised and cut off for maintenance.

After the QKD connection is set and verified, the shared secure key can be updated based on the most recent key passed. After the latest key is passed, encrypted information can be passed over the QKD connection until it is disconnected. At that point, the nodes will reconnect via classical encryption methods utilizing the last QKD passed shared key until another QKD connection can be made or until the shared key expires. Since shared keys will expire, there must be a balance between key expiration, encryption security, and QKD connections' dependability. Next, consider how QKD can be integrated into different systems.

Place nodes into categories: mobile ground, stationary ground, sea, underwater, air, and space. Sea nodes will include ships in command and/or control of weapons. Underwater nodes will primarily include submarines (Baker, 2013), (Powell, 2017) but may include future C3 underwater communication nodes. Land nodes include any kind of C3 terminal in a building or on a vehicle or even a person. Space nodes will primarily be satellites but could include manned spacecraft. Most nodes will have multiple connections and link modes to include systems in and outside their grouping. On account of this, connections are generalized like the stationary ground to stationary ground, stationary ground to mobile ground, stationary ground to air, or stationary ground to space. Examples follow.

Stationary ground to stationary ground networks is perhaps the most straightforward because these connections will be relatively stable and secure. These connections are also the easiest to update (Rijmenants, 2019). Intra-stationary ground networks will be very much like other fiber internet systems where there are nodes and repeaters connected by fiber links. However, nodes and repeaters will be able to create, distribute, and evaluate quantum-entangled photons as well as pass classical fiber-optic information (Wever, et al., 2016). Something to consider is if these systems are separated by long distances, QKD connections can be made via satellites or line of sight laser communication to pass shared keys instead of fiber and then copper or radiofrequency links can be used as the primary link. Depending on the fiber network's infrastructure reliability and security, classical redundant communication, may not be required for intra-stationary ground networks.

Stationary ground nodes may also connect with other terrestrial assets; however, these links will be limited by line of sight and will typically only be used to make initial connections to mobile ground, air, sea, and underwater assets. These initial links will be useful to initialize systems that are not always connected like an aircraft that hasn't been connected since the shared key expired or a new submarine that has never been connected. Beyond that, stationary ground nodes will typically connect to space systems to pass information for command and control purposes.

Space connected networks will handle the preponderance of the rest of the connections. Other mobile assets may assist as a relay in remote areas if their hardware provides the necessary directionality to be a secure relay, but space assets will be the primary due to their global reach. Whether it is space to space, space to air, space to water, space to ground, or even space to underwater, most of these connections will operate similarly. To connect, these assets will require the free-space transmission of quantum entangled photons. These connections will be linked similarly to the stationary ground to stationary ground connections, except instead of fiber connection, they will use free space laser connections to initial setup the secure connection and pass the shared key to encrypt the connection for further use. The rest of the data will be passed via either laser communications (Weiner, et al., 1980), (Wu, 2017) depending on the fidelity or via classical communications encrypted by the last transmitted, shared key. As straightforward as this may seem, there are multiple caveats to these connections.

The most important thing to consider with QKD via space communications is that it is still highly experimental as is using lasers for space communication. However, there is a lot of promising research showing both are highly capable (Yin, et al., 2017). QKD can pass entangled photons between locations over 1200km. Studies are also showing quantum-entangled photons can be sent through the water to connect to submarines. Further, laser communications are proving to be useful for sending large amounts of data at farther and farther distances. These developments may or maybe not prove to be fruitful; however, it should not be a limiting factor as there are other options for mobile QKD connections.

Under current asset constructs, satellite relays would be the obvious choice over aircraft relays for worldwide communication. However, newly developed High-Altitude Platforms (HAPs) could be able to provide mobile communication in a highly customizable fashion. These assets could be especially boon for QKD if they were used to replace space-based assets. Their flexibility and long endurance could provide strategic connections at a moment's notice. They would also be able to provide far better fidelity due to the reduced atmospheric interference. HAPs would be something to consider if laser communications are shown to be limited to Low Earth Orbit (LEO) as it may be too difficult to get the needed coverage with LEO satellites.

4. Discussion

Quantum Key Distribution is a viable advanced quantum key encryption system. A system with quantum keys should be developed and used. This manuscript describes through current and future methods of implementing QKD within a command and control system. Individual parts of the QKD network must be developed and tested. To what level it should be used is a question to be investigated, but regarless quantum information systems can add superior attributes to conventional systems.

Acknowledgments

Conceptualization, D.H. methodology, D.H.; formal analysis, D.H.; writing—original draft preparation, T.S.; writing—review and editing, T.S.; visualization, T.S.; funding acquisition, T.S., please turn to the CRediT taxonomy for the term explanation. Authorship has been limited to those who have contributed substantially to the manuscript. The education that lead to this self-funded research was funded by the U.S. Strategic Command's distance learning education program (Mihalik, et al., 2018), (Sands, et al., 2017) in response to an increased need for critical thinking in the nuclear enterprise in a period of global uncertainty (Bittick, et al., 2019), (Sands, et al., 2018), (Nakatani, et al., 2018), (Sands, et al., 2016), (Sands, Mihalik, Camacho, 2018). The APC was funded by corresponding author.

References

Alapatt, B. P. (2018). An Enhanced Advanced Encryption Standard (Eaes) Algorithm For Secure Fiber Optic Communication. *International Journal of Advanced Research in Computer Science*, 167-171. https://doi.org/10.26483/ijarcs.v9i1.5285

Andrews, L. C., & Ronald, L. P. (2002). Impact of Scintillation on Laser Communication Systems: Recent Advances in Modeling. *Journal of Biomedical Optics, International Society for Optics and Photonics*. https://doi.org/10.1117/12.453235

Baker, B. (2013). *Deep Secret – Secure Submarine Communication on a Quantum Level.* Retrieved from www.naval-technology.com/features/featuredeep-secret-secure-submarine-communication-on-a-quantum-level

Benslama, M. et al (2017). *Quantum Communications in New Telecommunications Systems.* https://doi.org/10.1002/9781119332510

Bittick, L., & Sands, T. (2019). Political Rhetoric or Policy Shift: A Contextual Analysis of the Pivot to Asia. *Journal of Social Sciences, 15,* 92-125. https://doi.org/10.3844/jssp.2019.92.125

Bricout, R., & Chailloux, A. (2017). Recursive Cheating Strategies for the Relativistic FQ Bit Commitment Protocol. *Cryptography, 1,* 14. https://doi.org/10.3390/cryptography1020014

Bub, J. (2015). *Quantum Entanglement and Information.* Stanford Encyclopedia of Philosophy, Stanford University. Retrieved from plato.stanford.edu/entries/qt-entangle/#2

Curty, M., Jofre, M., Pruneri, V., & Mitchell, M. W. (2015). Passive Decoy-State Quantum Key Distribution with Coherent Light. *Entropy, 17,* 4064-4082. https://doi.org/10.3390/e17064064

Diamanti, E. et al (2016). *Practical Challenges in Quantum Key Distribution.* Nature News. Nature Publishing Group. https://doi.org/10.1038/npjqi.2016.25

IDQuantique. IDQuantique. QUANTUM-SAFE CRYPTOGRAPHY. 2016. *Website Brochure.* Retrieved from marketing.idquantique.com/acton/attachment/11868/f-021b/1/-/-/-/-/Quantum-SafeCryptography_Brochure.pdf

Irani, M. (2010). High Assurance Internet Protocol Encryptor (HAIPE). *SPAWAR Systems Center Pacific.* Retrieved from info.publicintelligence.net/NSA-HAIPE.pdf

Jacobsen, C. S., Gehring, T., & Andersen, U. L. (2015). Continuous Variable Quantum Key Distribution with a Noisy Laser. *Entropy 2015, 17,* 4654-4663. https://doi.org/10.3390/e17074654

Jeffrey, B. (2006). Quantum Information and Computation. A Determination of the Hubble Constant from Cepheid Distances and a Model of the Local Peculiar Velocity Field. *American Physical Society.* Retrieved from arxiv.org/abs/quant-ph/0512125

Jenner, N. (2018). *Five Practical Uses for 'Spooky' Quantum Mechanics.* Ed. Smithsonian Institution. Retrieved from www.smithsonianmag.com/science-nature/five-practical-uses-spooky-quantum-mechanics-180953494

Jian, W. P., Simon, C., Brukner, C., & Zeilinger, A. (2001). Entanglement purification for quantum communication. *Nature*. Retrieved from http://dx.doi.org.libproxy.nps.edu/10.1038/35074041

Kashefi, E., & Pappa, A. (2017). Multiparty Delegated Quantum Computing. *Cryptography, 1,* 12. https://doi.org/10.3390/cryptography1020012

Kashefi, E., & Wallden, P. (2017). Garbled Quantum Computation. *Cryptography, 1,* 6. https://doi.org/10.3390/cryptography1010006

Luyen, L. V. (2019). An Improved Identity-Based Multivariate Signature Scheme Based on Rainbow. *Cryptography, 3,* 8. https://doi.org/10.3390/cryptography3010008

Mailoux, L. O. et al. (2016). Quantum key distribution boon or bust. *CSIAC, Journal of Cyber Security and Information Systems.* Retrieved from www.csiac.org/journal-article/quantum-key-distribution-boon-or-bust/7

Mihalik, R., Camacho, H., & Sands, T. (2017). Continuum of learning: Combining education, training and experiences. *Education, 8,* 9-13.

Morris, J. D. (2017). Implications of Quantum Information Processing On Military. United States Military Academy, Army Cyber Institute Scholarly Publication. 2017. *West Point, New York.* Retrieved from Cyber.army.mil. This publication is the work of the U.S. government, and is not subject to copyright protections in the United States.

Nakatani, S., & Timothy, S. T. (2018) Eliminating the Existential Threat from North Korea. *Science and Technology, 8*(1), 11-16.

Office of the Secretary of the Deputy Assistant Secretary of Defense for Nuclear Matters, Nuclear Matters Handbook, 2016. Chapter 6. Retrieved November, 18, 2019, from https://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/chapter_6.htm

Powell, D. (2017). First Underwater Entanglement Could Lead to Unhackable Comms. *New Scientist.* First Underwater Entanglement Could Lead to Unhackable Comms.

Rijmenants, D. (2014). *One-Time Pad.* Retrieved from http://users.telenet.be

Sands, T., & Mihalik, R. (2016). Outcomes of the 2010 & 2015 Nonproliferation Treaty Review Conferences. *World Journal of Social Sciences and Humanities, 2*(2), 46-51.

Sands, T., Camacho, H., & Mihalik, R. (2017). Education in nuclear deterrence and assurance. *J. Def. Manag, 7,* 166. https://doi.org/10.4172/2167-0374.1000166

Sands, T., Camacho, H., & Mihalik, R. (2018). Nuclear Posture Review: Kahn Vs. Schelling…and Perry. *Journal of Social Sciences, 14,* 145-154. https://doi.org/10.3844/jssp.2018.145.154

Sands, T., Mihalik, R., & Camacho, H. (2018). Theoretical Context of the Nuclear Posture Review. *Journal of Social Sciences, 14,* 124-128. https://doi.org/10.3844/jssp.2018.124.128

Shaari, J. S., & Mancini, S. (2015). Finite Key Size Analysis of Two-Way Quantum Cryptography. *Entropy, 17,* 2723-2740. https://doi.org/10.3390/e17052723

Sikora, J. (2017). Simple, Near-Optimal Quantum Protocols for Die-Rolling. *Cryptography, 1,* 11. https://doi.org/10.3390/cryptography1020011

Usenko, V. C., & Filip, R. (2016). Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense. *Entropy 2016, 18,* 20. https://doi.org/10.3390/e18010020

Weber, J., & Valter, P. (2016). *Introduction to Quantum Cryptography.* 1 December 2016. Retrieved from howdoesinternetwork.com/2016/quantum-cryptography-introduction

Wiener, T., & Karp, S. (1980). The Role of Blue/Green Laser Systems in Strategic Submarine Communications. *IEEE Transactions on Communications,* 1602-1607. https://doi.org/10.1109/TCOM.1980.1094858

Wu, T. C. et al. (2017). Blue Laser Diode Enables Underwater Communication at 12.4 Gbps. *Nature*. https://doi.org/10.1038/srep40480

Yin, J. et al. (2017). Satellite-Based Entanglement Distribution over 1200 Kilometers. *Science, American Association for the Advancement of Science* (2017). https://doi.org/10.1126/science.aan3211