Quantum Cryptography: Potential, Limitations, & Future

Hanif I. Lumsden

University of Maryland Global Campus

ITEC 625

Dr. Goulding

March 16, 2021

i. **Introduction**

Cryptography, according to the National Institute of Standards and Technology's *An Introduction to Information Security*, is "a branch of [advanced] mathematics based on the transformation of data" that "can… provide data confidentiality and integrity" (Nieles, Dempsey, & Pillitteri, 2017, p. 52). Typically, cryptography is used for electronic signatures and user authentication. It is the only way to protect data (Nieles, Dempsey, & Pillitteri, 2017).

This paper divides cryptography into two main types: classical and quantum. Classical cryptography is within classical mechanic constraints, which "deals with the motion of objects through absolute space and time in the Newtonian sense" (Fowles & Cassiday, 2004). Through the years, the mathematical tools to describe the Newtonian sense of space and time were applied to non-rigid particle physics. Classical mechanics began to be inadequate to explain the experimental observations of wave mechanics and statistical mechanics ("The History and Limitations,"n.d.). Quantum mechanics successfully supplied a mathematical description of experiments in wave and statistical mechanics; it "describes… microscopic systems by means of mathematical formalism" (Scherer, 2019, p. 1). Quantum cryptography relies on quantum theory to "break classical algorithms used for key distribution and digital signatures" (Cavaliere, Mattsson, & Smeets, 2020).

The fields of quantum theory and cryptography have been intertwined for more than 50 years now. First, it was 'quantum money,' money that is impossible to counterfeit, that introduced the concept of 'oblivious transfer,' where the sender does not know if the receiver received the sent information (Rabin, 1981; Weisner, 1983). Quantum money and oblivious transfer is the first instance of quantum physics in cryptography. The two concepts are still closely tied to quantum cryptography, except in the case of quantum money, it is the key that is

impossible to counterfeit. Quantum key distribution (QKD) is the central concept in quantum information that dominates quantum cryptography research (Broadbent & Schaffner, 2015). QKD is further defined, as well as it is limitations and setbacks.

1. **Explaining Quantum Mechanics**

Before going any further, the concept of the uncertainty principle, Hilbert space, and quantum states must be explained. There is much literature regarding quantum mechanics' fundamental principles. The definition need not be too strenuous in computing as opposed to theoretical physics. The time-independent Schrödinger equation can be interpreted into Eq. 1 in this paper. Essentially, postulates in quantum mechanics theorize the statistics of entities on the microscopic level (Griffith & Schroeder, 2019, p. 32; Scherer, 2019, p. 10). For said entities, measurements of microscopic quantities or particles can be done with real numbers, R, as the outcome ("P.1: Review – Real Numbers," 2020). The particle is compelled to assume a position from an observation a la observable ("Copenhagen Interpretation," n.d.). Like classical systems, the observable's position and momentum cannot yield precise measurements simultaneously. When the position is measured, one will find that the momentum measurements are widely scattered and vice versa; this logic is Heisenberg's famous uncertainty principle (Griffith & Schroeder, 2019). Along with the position and momentum, the polarization angle $(0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4})$ cannot be measured simultaneously with angular momentum (Svennson, 2013). Quantum cryptography is based on the Heisenberg uncertainty principle and photon polarization; these two concepts will be expounded in section **3**. Any quantifiable measurement obtained from a particle said quantifiable measurement is termed an eigenstate and is associated with an eigenvector of an operator, the Hamiltonian, associated with an observable (Scherer, 2019, p. 34). The position of observables is classified as an eigenstate, mathematically presented as a vector in Hilbert space:

$$\psi,\phi \in H \;\&\; a,b \in C \Rightarrow a\psi + b\phi \in H \; [\textbf{Eq. 1}]$$

Two-dimensional Hilbert space of the qubits uses the symbol H with vectors in Hilbert space representing multi-particles denoted by ket-notation: $|\psi\rangle$ and $|\phi\rangle$ (Scherer, 2019, p. 7, 12; Broadbent & Schaffner, 2015). Any one qubit may be represented in a two-dimensional Hilbert state as:

$$|\psi\rangle = \alpha|0\rangle + \beta\,|1\rangle \; [\textbf{Eq. 2}]$$

Where α and β are complex numbers such that $|\alpha|2+|\beta|2 = 1$, and neither α nor β are zero (Broadbent & Schaffner, 2015). When $|\psi\rangle$ is in a superposition, the eigenstate of $n \geq 2$ qubits is described by a tensor product of n-bit basis states can be abbreviated as $|00\ldots\ 0\rangle$, $|00\ldots 1\rangle$, $|11\ldots 0\rangle$, $|11\ldots 1\rangle$ (Broadbent & Schaffner, 2015; Zwiebach, 2013). Any eigenstates involving two parties can be used to find which of the stated party holds a qubit in a particular state. This phenomenon is the functionality behind quantum key distribution (QKD) expounded in section 3.

2. **Classical Cryptography and the reason for Quantum Cryptography**

Classical cryptography uses traditional public-key (PuK) cryptography, private key (PrK) cryptography, and one-time pad (Panhwar et al., 2021). PuK and PrK systems need the sender and receiver (S&R) to exchange the secure key composed of bits to make a private key. These algorithms use the mathematical technique Rivest-Shamir-Adleman (RSA) to factor a large prime number based on calculating the discrete logarithm (Singh & Supriya, 2013). The current classical cryptography system has historically been exposed for loopholes in communication; there is no key refreshing that results in key expansion, causing information and network security networks to be compromised (Panhwar et al., 2021; cite occurrences). Classical random number generators are prone to small biases leading to a key compromise (Cavaliere, Mattsson, &

Smeets, 2020). Eavesdroppers are not detected during data transmission over a medium using the advanced encryption standard (AES) and RSA. Therefore, measurements performed by an eavesdropper on a channel can be monitored without users realizing eavesdropping is taking place (Bhatt, Aneja, & Tripathi, n.d.). Quantum cryptography is sought after to develop a secure communication network that detects eavesdroppers. Quantum cryptography generates true random numbers, exploits the Heisenberg principle, and uses photon polarization and other quantum phenomena to allow users to develop a secure key and detect eavesdropping.

3. **Quantum Key Distribution**

Discrete variable Quantum key distribution (DV-QKD) can be partitioned into two portions, the quantum communication portion utilizing Heisenberg's uncertainty principle and photon polarization followed by classical post-processing (Cavaliere, Mattsson, & Smeets, 2020; Panhwar et al., 2021; Pirandola et al., 2020). During the first portion of quantum communication, non-orthogonal eigenstate α is encoded from a random classical variable and is sent over a quantum channel (Panhwar et al., 2021). An eavesdropper who attempts to steal the encoded information using Gaussian attacks will only disturb the quantum signals and obtain partial information because linearity forbids perfect cloning of keys (Grosshans et al., 2003; Pirandla et al., 2020). Raw data in the quantum transmission is used to estimate the transmissivity and noise, determining the post-processing amount for a private shared key extraction. During raw data analysis, error correction, detection and elimination of errors, and privacy amplification allow the eavesdropper information to obtain an insignificant amount. In the end, the receiver measures the signal and obtains the eigenstate β; the sender and receiver share data described by two variables, α and β (Pirandla et al., 2020). A shared key is enabled by communication through protocol BB84, seen in fig. 1 below. This protocol allows the sender and receiver to create a

secure key using polarized qubits (Panhwar et al., 2021). Recall back to the mention of measurements influencing the outcome or position of a particle. In the case of DV-QKD, the polarization of photons is measured. Through protocol BB84, the sender and receiver must agree on a specific bit sequence or stream before communication starts (Panhwar et al., 2021). The sender and receiver guesses are variable through direct or reverse reconciliation aided by forwarding and backward classical communication. Direct and reverse reconciliation limits cloned Gaussian states so that various attacks from the eavesdropper have no influence on the achievable secret key shared between sender and receiver (Grosshans et al., 2003). The sender reconstructs and processes their outcome to infer the receiver's encoding; the classical information vector is equivalent to the initial quantum information vector regarding the direction (Pirandla et al., 2020). DV-QKD depends largely on precision: polarization filters act as quality control of sorts if the quantum channel transmission quality falls below ½, the channel is not secure, the attacker hoard majority of the information, and a shared key generation is no longer possible (Grosshans et al., 2003; Panhwar et al., 2021). BB84 protocol works for high losses as photons received by the sender are considered for the key. In case of high losses, the receiver initiates reverse reconciliation to correct their outcome value to match the sender's key outcome. The sender and receiver cross a loss limit and successfully extract a secret key for a low transmission quality; however, information can leak to the attacker in this case. (Grosshans et al., 2003).

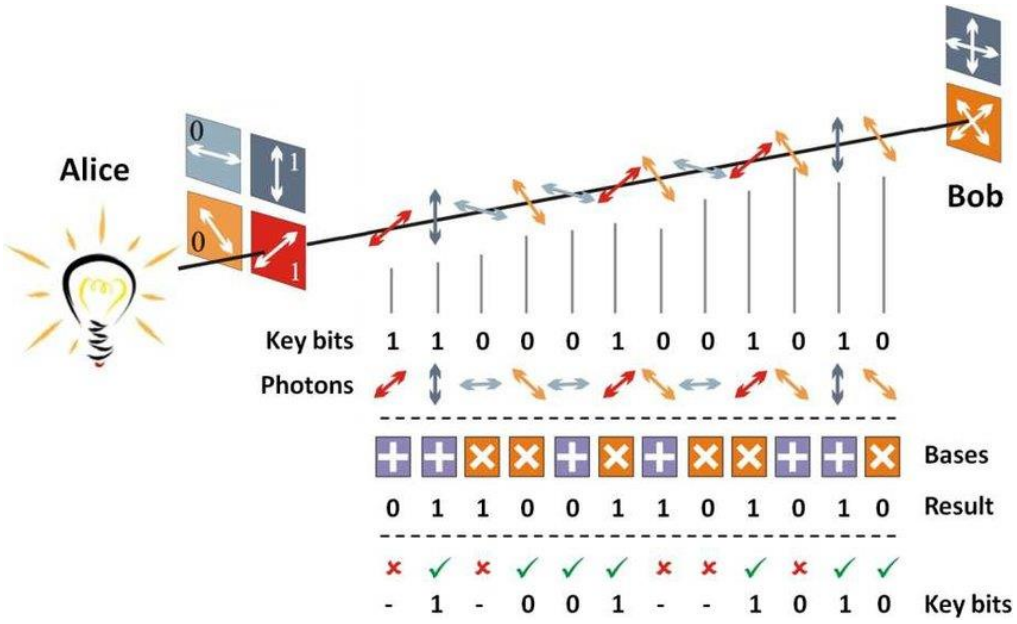

Figure 1: Basic schema for the BB84 protocol. "Alice" is the sender, and "Bob" is the receiver in this scenario. Free-Space Quantum Key Distribution - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/BB84-protocol-basic-scheme_fig11_309731586 [accessed 16 Mar, 2021]

Post-communication, if the eavesdropper still tries to extract information, the sender and receiver estimate the error rate in a generated or received key (Panhwar et al., 2021). A key with an error rate exceeding 25 percent will be discarded; otherwise, the key is kept by the sender and receiver. Heisenberg's Uncertainty Principle confirms that the transmission is secured by an eavesdropper (Panhwar et al., 2021). Recall that the act of observation causes a particle to assume a particular position; thus, the act of eavesdropping changes the state of the photon, and the secured key between sender and receiver cannot be extracted.

Continuous variable QKD (CV-QKD) uses pulses of energy sent through quadrature in an optical fiber rather than single photons. Pulses are transmitted through one or two quadratures (Cavaliere, Mattsson, & Smeets, 2020). The receiver follows the logic seen in the BB84 protocol. They randomly choose the quadrature during measurement. The value is kept for the correct quadrature chosen; the resulting values are Gaussian distributions. An apparent difference

between DV-QKD and CV-QKD is that QV-QKD uses devices made for classical systems to reduce cost instead of a dedicated device (Cavaliere, Mattson, & Smeets, 2020). CV-QKD security practicality is still under research.

One of the most valuable exploits of the QKD is the generation of true random numbers. However, quantum random number generation (QRNG) can exist outside of QKD and is currently being used in some IoT devices (Cavaliere, Mattson, & Smeets, 2020). Quantum random numbers (QRN) or random eigenstates and keys are naturally probabilistic in that uncorrelated, uniformly distributed numbers are generated. QRN generators consist of a quantum entropy source portion and a post-processing portion. True randomness and raw random data are generated through the quantum entropy source. Simultaneously, the post-processing portion verifies the degree of randomness in the raw data through auto-correction and minimum entropy estimation (Cavaliere, Mattson, & Smeets, 2020).

4. **Limitations & Projections**

DV-QKD provides impenetrable security, but there are setbacks to implementing this. This technology cannot function over long distances. The entangled photon polarization state may be destroyed if a qubit network radius extends over 10 kilometers (Panhwar et al., 2021). Another limitation involves implementation. The QKD process is slow compared to classical key distribution. For this issue, QKD cannot be used for bulk data transmission (Panhwar et al., 2021). Panhwar et al. state that QKD can be used only to communicate the key and classical algorithms like RSA & Diffie-Hellman is used for key exchange between remote parties. (2021). Satellite technology is offered as a solution to overcome the limited qubit network where the satellite acts as a station, and the photon faces low attenuation in free space (Panhwar et al., 2021).

Broadbent & Schaffner explain that the ongoing work and research on quantum cryptography will improve existing schemes and explore applications and proof techniques. It is asserted that more research on quantum algorithms for quantum cryptanalysis is required to grasp the computational problems studied in post-quantum cryptography and understand what security parameters are needed for post-quantum cryptographic schemes (Broadbent & Schaffner, 2015). Other challenges for quantum cryptography include developing device-independent protocols for essential distribution purposes to tolerate a reasonable amount of noise. Questions have been posed that tie to the open problems of quantum cryptography. These include the construction of quantum-secure pseudorandom permutations, the limits of a delegated quantum computation, and building a quantum public key instead of a private one. Researchers are exploring these problems and more (Broadbent & Schaffner, 2015).

Currently, the QRNG aspect of QKD is commercially available for implementation but at a high cost and slow speed (Cavaliere, Mattsson, & Smeets, 2020). Costs can range from $400 - $3000 as a function of output and form factor ("QRNGs: Real market drivers," 2019), and the bit rate does not exceed Mbps. However, in development are QRNGs based on photonic chips that can exceed the Gbps bit rate. Photonic-based QRNGs use two-path single-photon splitting, "photon arrival time, amplified spontaneous emission, detection of vacuum field and laser phase noise" (Cavaliere, Mattsson, & Smeets, 2020, p. 13).

With any development that seeks to be deployed and implemented into the information technology stratosphere of advanced computing, QKD systems must be standardized. The International Telecommunications Union (ITU) currently standardizes the network aspects of QKD communication systems. There are currently recommendations Y.3800 and Y.3801 for networks that can support QKD (Cavaliere, Mattsson, & Smeets, 2020; Y.3800, 2019; Y.3801,

2020). The ITU also standardizes the security aspects (Cavaliere, Mattsson, & Smeets, 2020). The transition to a post-quantum cryptographic algorithm, a classical cryptography infrastructure built to withstand quantum attacks, will be followed with complete standardization; However, the United States government will not complete the transition to post-quantum cryptography until 2030 (Cavaliere, Mattsson, & Smeets, 2020).

Classical cryptography is the norm, but aspects of quantum cryptography, such as QKD and QRNG, will leave the research laboratory and be implemented as cryptography solutions in the next decade. The most practical solution in this current moment for QKD is a hybrid between classical and quantum cryptographies. Implementation of QKD takes the form of a hybrid between itself and an authenticated classical channel (Cavaliere, Mattsson, & Smeets, 2020). In hybrids, QKD's QRNG is used solely for key creation. Therefore, any entity concerned about security measures in their organization should invest in a QRNG. QRNGs are being sold through distributors such as Quintessence Labs, Quantum Numbers Corp, and ComScire currently provide QRNG solutions, and the market is said to expand in the next five years ("QRNGs: Real market drivers," 2019).

5. **Conclusion**

Quantum cryptography will see large implementation in the next decade following complete standardization. Qubits are expected to develop at the same rate as classical bits in accordance with per Moore’s Law, now called Neven’s Law. Today, the QRNG aspect of QKD is in the market; however, when the current setbacks of QKD, such as range, speed, and efficiency, are overcome, quantum cryptography will be integral to computer security and the integrity of our data.

References

21 of the best free to download closed-source applications. (2018, February 26). LinuxLinks. https://www.linuxlinks.com/closed-source/

Abbas, A. M., Goneid, A., El-Kassas, S. (2014). Privacy Amplification in Quantum Cryptography BB84 using Combined Univarsal2-Truly Random Hashing. https://www.researchgate.net/publication/263887574

Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In: D. J. Bernstein, J. Buchmann, E. Dahmen (eds.) *Post-Quantum Cryptography*, p. 1-14. Springer. https://doi.org/10.1007/978-3-540-88702-7

Bhatt, M., Aneja, A., & Tripathi, S. (n.d.). Classical Cryptography v/s Quantum Cryptography A Comparative Study. *International Journal of Electronics and Computer Science Engineering*, *1*(1), p. 121-129. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.303.5619&rep=rep1&type=pdf

Broadbent, A. & Schaffner, C. (2015). Quantum Cryptography Beyond Quantum Key Distribution. Design, Codes and Cryptography,78(1), 351-382. https://doi.org/10.1007/s10623-015-0157-4

Brassard G., Høyer P., Kalach K., Kaplan M., Laplante S., Salvail L. (2011) Merkle Puzzles in a Quantum World. In: Rogaway P. (eds) *Advances in Cryptology – CRYPTO 201131st Annual Cryptology Conference Santa Barbara, CA, USA, August 14-18, 2011Proceedings, 6841*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22792-9_22

Cavaliere, F., Mattsson, J., & Smeets, B. (2020). The security implications of quantum cryptography and quantum computing. Network Security, 2020(9), 9-15. https://doi.org/10.1016/S1353-4858(20)30105-7

Copenhagen interpretation of quantum mechanics (Stanford encyclopedia of philosophy). (n.d.). Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/qm-copenhagen/

Crépeau, C., Salvail, L., Simard, J. R., Tapp, A. (2011). Two Provers in Isolation. In: Lee D.H., Wang X. (eds) *Advances in Cryptology – ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings, 7073*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25385-0_22

Damgård I., Dupuis F., Nielsen J.B. (2015) On the Orthogonal Vector Problem and the Feasibility of Unconditionally Secure Leakage-Resilient Computation. In: Lehmann A., Wolf S. (eds) *Information Theoretic Security: 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings, 9063*. Springer, Cham. https://doi.org/10.1007/978-3-319-17470-9_6

Damgård, I., Pedersen, T. B., & Salvail, L. (2014). How to re-use a one-time pad safely and almost optimally even if P = NP. *Natural Computing*, *13*(4), 469–486. https://doi.org/10.1007/s11047-014-9454-5

Fowles, G. R., & Cassiday, G. L. (2004). Fundamental Concepts: Vectors. In Analytical Mechanics (7th ed., p. 1). Brooks/Cole Publishing Company.

Griffiths, D. J., & Schroeter, D. F. (2019). Introduction to quantum mechanics (3rd ed.). Cambridge University Press.

Grosshans, F., Cerf, N. J., Wenger, J., Tualle-Brouri, R., & Grangier, P. (2003). Virtual Entanglement and Reconcilation Protocols for Quantum Cryptography with Continuous Variables. *Quantum Information & Computation, 3*, 535-552. https://www.researchgate.net/publication/220435954

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security. *NIST Special Publication 800-12,1*, p. 52. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

P.1: Review - Real numbers: Notation and operations. (2020, August 24). Mathematics LibreTexts. https://math.libretexts.org/Courses/Monroe_Community_College/MTH_165_College_Algebra_MTH_175_Precalculus/01.0%3A_Preliminary_Topics_for_College_Algebra/P.01%3A_Review_Real_Numbers%3A_Notation_and_Operations

Panhwar, M. A., Khuhhro, S. A., Mazhar, T., ZhongLiang, D., Qadir, N. (2021). Quantum Cryptography: A way of Improving Security of Information. International Journal of Mathematics and Computer Science, 16(1), 9-21. https://www.researchgate.net/publication/341508453_Quantum_Cryptography_A_way_of_Improving_Security_of_Information

QRNGs: Real market drivers (2019, August 14). Inside Quantum Technology. https://www.insidequantumtechnology.com/qrngs-real-market-drivers

Rabin, M. O. (1981). How to Exchange Secrets with Oblivious Transfer. *Technical Report TR-81 Harvard University*. https://eprint.iacr.org/2005/187.pdf

Scherer, W. (2019). Mathematics of quantum computing: An introduction. Springer Nature.

Singh, G. & Supriya. (2013, April) A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for information Security. *International Journal of Computer Applications (0975 – 8887)*, *67*(19), p. 33-38. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.5601&rep=rep1&type=pdf

Stebila, D., Mosca, M., & Lütkenhaus, N. (2010). The case for quantum key distribution. *Quantum Communication and Quantum Networking*, *36*, p. 283–296. https://doi.org/10.1007/978-3-642-11731-2 35

Svensson, S. (2013). Testing Heisenberg's Uncertainty Principle with Polarized Single Photons. *Research Academy for Young Scientists***.** p. 1-14. https://static1.squarespace.com/static/56b6357e01dbaea0266fe701/t/56c433792b8dde24de99e52a/1455698810284/Sofia-Svensson-Testing-Heisenbergs-Uncertainty-Principle-with-Polarized-Single-Photons.pdf

The History and Limitations of Classical Mechanics (n.d.) https://www.lehman.edu/faculty/anchordoqui/chapter01.pdf

Unruh D. (2013) Everlasting Multi-party Computation. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, vol 8043. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40084-1_22

Wiesner, S. (1983). Conjugate Coding.. *ACM SIGACT News*, *15*(1), 78-88. https://doi.org/10.1145/1008908.1008920

Y.3800 : Overview on networks supporting quantum key distribution (2019). *International Telecommunication Union*. https://www.itu.int/rec/T-REC-Y.3800-201910-I/en

Y.3801 : Function requirements f or quantum key distribution networks (2020). *International Telecommunication Union*. https://www.itu.int/rec/T-REC-Y.3801-202004-I/en

Zwiebach, B. (2013, December 13). MULTI-PARTICLE STATES AND TENSOR PRODUCTS. MIT OpenCourseWare | Free Online Course Materials. https://ocw.mit.edu/courses/physics/8-05-quantum-physics-ii-fall-2013/lecture-notes/MIT8_05F13_Chap_08.pdf