A Computing Perspective of Quantum Cryptography

Ashish Nanda, Deepak Puthal, Saraju P. Mohanty, and Uma Choppali

Abstract

In the continuous evolution process of the computer age, the next big step in security is being achieved by embracing quantum cryptography. As the unit of information shifts from the currently used 'bit' towards the 'Qubit' (Quantum bit), it offers a new realm of untapped features, which can be used to ensure the confidentiality of the information being shared amongst participants. This confidentiality of the system is ensured by the use of a quantum channel for exchanging secret keys. These keys are then used to encrypt the data being shared. The system is a combination of cryptography and quantum computing that are aided by the laws of Physics.

I. Quantum Computing

The history of computing starts with humans performing mathematical tasks by hand (using pen and paper) in order to get a result. The first big leap started with a hand operated abacus in 2300 BC followed by mechanical calculators and culminating in the 18th Century with Charles Babbage's automatic difference and analytical engine. In the 19th century, the next major transition occurred with the introduction of digital computers, which uses bits (0's and 1's). These digital computers were deemed Turing-Complete, i.e., being able to compute every Turing-Computable Function. Now, we are taking yet another great leap with the introduction of quantum computers.

Quantum computers are based on quantum-mechanical principles, such as quantum superposition [1], quantum annealing [2], [3], and quantum entanglement [4]. Hence, they use a much complex unit known as Qubit. A Qubit, in classic computer terminology, can have a value of 1 or 0 or any superposition of both 1 & 0 together as shown in Figure 1. In computational terms, it implies that a quantum computer can process several combinations of zeros and ones at the same time with very high speeds. Current quantum computers, can however, only implement quantum annealing [5], (a way to find an optimal solution for problems with multiple variables) which is essentially a subset of what a quantum computer can truly perform. Even so, a true quantum computer may just be around the corner as various tech giants race towards achieving the goal [6], [7], [8].

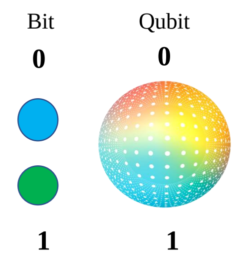

Fig. 1: Bit and Quantum Bit.

II. Quantum Cryptography

The term cryptography (also referred to as cryptology) meaning "Hidden/Secret Writing" is a practice to enable secure communication. The basic principle of cryptography involves the two parties, that wish to communicate securely, agree upon a method to encrypt (encode) and decrypt (decode) the data. Once a method is agreed upon, a secret key (also known as the encryption key) is shared between the parties using which the data is encrypted and decrypted as illustrated in Fig. 2. The strength of the encryption depends upon the method/algorithm used for encryption or decryption of data and the size of the secret key used to do so.

Quantum cryptography uses quantum mechanical principles to perform cryptographic tasks in order to provide a fool-proof security system [9], [10]. Quantum cryptography is applicable to several areas requiring true quantum computer. Hence, the applications are currently theoretical in nature. At present, one of the applications, Quantum Key Distribution (QKD), is implementable as it does not require any quantum computation and can be implemented using currently available lasers and fiber optics [11]. In current computing systems such as cloud, edge/fog, computing really requires a secure channel for key distribution to build secure infrastructure [12]. QKD can also be applied to most recent security technology such as blockchain for secure key distribution [13].

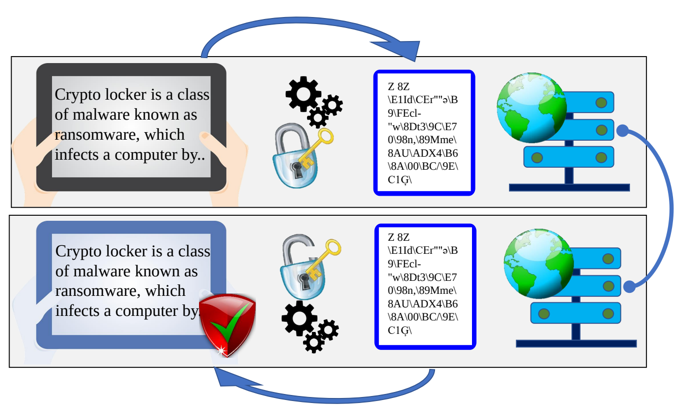

Fig. 2: Cryptography - The encryption and decryption process.

III. Quantum Key Distribution (QKD)

Quantum Key Distribution can be used to securely share secret keys or encryption keys using Qubits over a quantum channel. This application is guaranteed by Heisenberg's uncertainty principle. The Heisenberg's uncertainty principle states that it is impossible to simultaneously measure the position and momentum of an atomic particle with high precision. The principle states that even with perfect instrumentation and techniques, there is inherent uncertainty in calculation of momentum if position is precisely located and vice versa.

The security in QKD is achieved by providing totally secure key distribution technique as shown in Figure 3. For instance, if Jerry and Sue wish to exchange secret information, Jerry must initially create a secret key "K_S" using random numbers as the seed value. The K_S can be of any desired bit length, where the length of the key is directly proportional to the strength of encryption. Once created, K_S is then converted into Qubits, which are then sent across the quantum channel. The quantum channel can be formed with any atomic particle that follows the laws of quantum physics like the currently implementable photons.

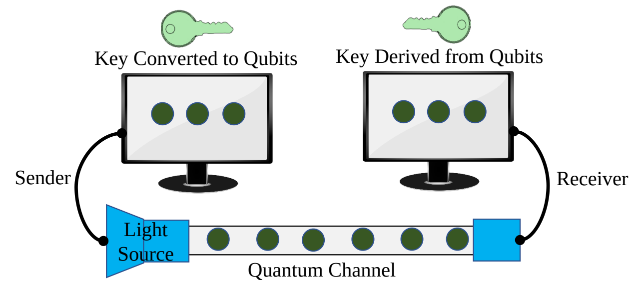

Fig. 3: Quantum Key Distribution.

If an intruder, say Tom, were to intercept the quantum channel in order to eavesdrop/steal the secret key, Tom would unwillingly create errors or changes in the original state of the transmitted data as stated by Heisenberg's uncertainty principle as shown in Figure 4. These errors/changes can be detected by Sue in the form of transmission errors. Once the K_S is verified, it can be used through current encryption schemes to send and receive data securely over the public classical authenticated channel.

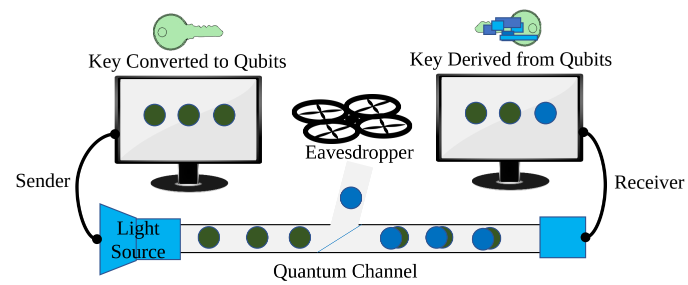

Fig. 4: Impact of eavesdropping on a quantum channel.

In a scenario where Sue has detected transmission errors, the received secret key is dropped and Jerry is requested to start the process once again unless an un-tampered transmission is received. This however raises a concern when settling on a secret key as Tom might not give up on eavesdropping. In addition, a practical implementation cannot be perfect and may be influenced by various environmental disturbances (such as noise) causing transmission errors. In this particular case, secret-key distillation is used to make a new K_S. This is achieved by calculating the 'bit error rate' which can deduce the information that may be known to Tom. Hence, using the remaining bits of information, Jerry and Sue will be able to distill a new K_S.

IV. Limitations of QKD

As pointed out above, the quantum key distribution technique can only ensure the security of the initial secret exchange. The actual strength of the security provided depends upon the length of the key and the complexity of the algorithm used [11]. Although QKD is tamper-proof, it can still be compromised if the process is not setup properly. The various aspects of QKD that must be followed are as below:

1) As QKD is not used for encryption and can only provide a safe distribution channel, the strength of the secret key used must be strong enough. In addition, the encryption/decryption algorithm used must also be impossible to break using current technology (excluding quantum computers).
2) The equipment used in order to send the secret must be setup properly. If the equipment itself causes major errors/changes in the transmission, Jerry and Sue will keep discarding the secret keys.
3) The people involved in the exchange, Jerry and Sue, must keep K_S safe in order to prevent Tom from impersonating one of them.
4) The seed value used to generate K_S should be truly random numbers (and not pseudo-random) to provide a true K_S.

V. Future of Quantum Cryptography

Our current understanding regarding quantum cryptography is only the beginning towards a new era. As true quantum computers render the legacy encryption systems useless, quantum cryptography can open the door towards an enhanced system, which unlike the current encryptions, is not protected by the complexity of mathematics but are bound by the laws of quantum physics. At present, much of the quantum cryptography is theoretical as the equipment required is still under development or exists as a prototype yet to be named a true quantum computer. However, the introduction of true quantum computers will bring about a major change in the technological world by not only enabling other theoretical components of quantum cryptography but also begin a domino effect potentially taking the digital world into the next big leap.

VI. About the Authors

Ashish Nanda (ashish.nanda@student.uts.edu.au) is a Ph.D. student in the Faculty of Engineering and IT at University of Technology Sydney, Australia.

Deepak Puthal (deepak.puthal@uts.edu.au) is a Lecturer (Assistant Professor) in the Faculty of Engineering and IT at University of Technology Sydney (UTS), Australia. He is an author of 50 research articles.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the University of North Texas. Prof. Mohanty's research is in Smart Electronic Systems. He is an author of 250 research articles, and 3 books. He is the Editor-in- Chief of the IEEE Consumer Electronics Magazine.

Uma Choppali (umachoppali@gmail.com) is a faculty at Brookhaven College, Dallas. She has authored a dozen of peer-reviewed articles.

REFERENCES

[1] J. Cirac, M. Lewenstein, K. Mølmer, and P. Zoller, "Quantum superposition states of bose-einstein condensates," *Physical Review A*, vol. 57, no. 2, p. 1208, 1998.
[2] P. Goddard, S. Mniszewski, F. Neukart, S. Pakin, and S. Reinhardt, "How Will Early Quantum Computing Benefit Computational Methods?" https://sinews.siam.org/Details-Page/how-will-early-quantum-computing-benefit-computational-methods, last visited on 06 February 2018.
[3] A. Finnila, M. Gomez, C. Sebenik, C. Stenson, and J. Doll, "Quantum annealing: a new method for minimizing multidimensional functions," *Chemical physics letters*, vol. 219, no. 5-6, pp. 343–348, 1994.
[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of modern physics*, vol. 81, no. 2, p. 865, 2009.
[5] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, and H. Neven, "What is the computational value of finite-range tunneling?" *Physical Review X*, vol. 6, no. 3, p. 031015, 2016.
[6] A. Trabesinger, "Quantum computing: towards reality," *Nature*, vol. 543, no. 7646, pp. S1–S1, 2017.
[7] "IBM Q and quantum computing," https://www.research.ibm.com/ibm-q/learn/, last visited on 15 December 2017.
[8] K. L. Pudenz, "Quantum computing meets the real world," in *International Conference on Unconventional Computation and Natural Computation*. Springer, 2015, pp. 66–70.
[9] "Hack-Proof Technology: High-Speed Quantum Encryption Comes Closer to Reality," https://www.siasat.com/news/hack-proof-technology-high-speed-quantum-encryption-comes-closer-reality-1265676/, last visited on 12 Decemebr 2017.
[10] A. Pathak, R. Srikanth *et al.*, "Quantum cryptography: key distribution and beyond," *arXiv preprint arXiv:1802.05517*, 2018.
[11] G. Van Assche, *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.
[12] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyber threats [future directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 4, pp. 24–27, 2017.
[13] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.