Development of Quantum Key Distribution and Attacks against It

Yusheng Zhao
College of arts and science, New York University, New York 10012, US
Yz2188@nyu.edu

Abstract. Secure and efficient communication between two parties always incents scholars for further research. Creation of such a means of communication yields commercial benefits for our society. With the creation of a quantum computer, some classical protocols used for secure communication is no longer secure. Quantum key distribution is created to solve this problem. Although a quantum key distribution protocol is in theory guaranteed to be secure, there has been ways to breach its security in real life application. Since the creation of the first quantum key distribution protocol, there has been a rival between the defending and attacking side of quantum key distribution. In this paper, we first seek to discuss the basics of the first quantum key distribution protocol. Secondly, we discuss about the attacks against that protocol and the modifications made to the protocol in response to these attacks. Currently, researchers have permanently closed one side of the implementation loophole that could give rise to potential means of hacking of the protocol.

1. Introduction

In the speech of British physicist Lord Kelvin on April 27th, 1900, he begin by saying, “The beauty and clearness of the dynamical theory, which asserts heat and light to be modes of motion, is at present obscured by two clouds” (Thomson, 1901). One of the two clouds was the ultraviolet catastrophe. The later developed quantum mechanics dictates that the electromagnetic radiation could only be transmitted in discrete packets of energy and thus solved the problem of allowing an infinite amount of power been radiated by a cavity. As quantum mechanics and other areas of physics developed, they not only explained an enormous amount of the phenomena in our universe, but also made possible of numerous applications. For example, these applications include laser, electron microscope, and transistors. Nevertheless, the most intriguing application of quantum mechanics is quantum key distribution.

The publication of Bennett and Brassard’s paper marks the first quantum key distribution protocol. However, the development of many different protocols came along later. Some of these protocols differ from the previous ones by just some minor modifications. Nevertheless, some other protocols are results of huge modifications on previous ones. Although it is by the laws of physics that a correctly implemented and well-designed quantum key distribution protocol could never be hacked, there has been successful attempts of people trying to challenge the security of these protocols. The main purpose of this article will be to track the development of these attacks alongside with the evolution of the quantum key distribution protocols in response to these attacks. In this article, I will firstly present the details of the first quantum key distribution protocol, BB84. Following that, the article will discuss possible attack schemes against BB84 protocol and how researchers have modified BB84 in response to these attacks.
Before our investigation on quantum cryptography, let us first understand the basics of public-key cryptography. If Alice wants to send some information to Bob without letting anyone else know, she will have to use a public key distributed by Bob to first encrypt this message. We call the encrypted message ciphertext. When Bob receives this ciphertext from Alice, he will decrypt it with his private key. Public-key cryptographies’ security relies on the fact that some mathematical problems are hard to solve using current mathematical knowledge and with classical computational powers. For example, RSA cryptosystem’s security is based on the hardship in factoring the product of two large prime numbers, a semiprime. For an eavesdropper to get the private key, he has to be able to factor this semiprime and use the factors to retrieve the private key. Currently, the best we could do that with the help of classical computer still requires a super-polynomial time with respect to the size of this semiprime (Pomerance, 1996). With a large enough semiprime, we could be made sure that no one could retrieve our secret key. However, implementing Shor’s algorithm, a quantum computer could easily factor out the semiprime and thus get the private key (Shor P. W., 1997). Furthermore, Alice and Bob will never know whether their secret message has been acquired by a third party. Nevertheless, both problems will be solved by a quantum cryptography protocol.

2. BB84

2.1. Details of Protocol and Proof of Security
Since Shor’s Algorithm can be used to find the prime factors of a semiprime N, a quantum computer implementing it could easily break the message encrypted by RSA (Shor P. W., 1997). To deal with this situation, Bennett and Brassard devised a protocol whose security level relies on the uncertainty principle of quantum physics and the non-cloning theorem of quantum mechanics. The original paper “Quantum cryptography: Public key distribution and coin tossing” was published on the proceeding of the International Conference on Computers, Systems and Signal Processing in December 1984 (Bennett & Brassard, 4 December 2014). Bennett and Brassard proposed this first protocol of quantum key distribution to achieve a secure communication between two parties. The basics of the protocol work as followings.

The protocol realizes the communication that utilizes two channels. One of the two channels is public and classic. The other one is quantum and secret. For the sake of clarity, we will follow the convention and call the message sender Alice and the receiver Bob. At first, Alice will send Bob a sequence of photons via a quantum channel. Before sending the photons, Alice will polarize them each randomly to one of two degrees of one of the two bases. In the original paper, Bennett and Brassard used rectilinear and diagonal bases. In rectilinear basis, the photon could be polarized in either 0 or 90 degrees. In diagonal basis, the photon could be polarized in either 45 or 135 degrees. Alice will then remember for each photon in which basis and which degree she polarized it. For the photons in 0 or 45 degrees, Alice denotes them as bit 0. For the photons in 90 or 135 degrees, Alice denotes them as bit 1. When Bob is receiving these photons, he tries to measure each of them in one basis. Bob chooses a basis randomly for the filter every time he receives a photon. For each photon then, Bob will have a result of what degree the photon is sent in. However, this result may not be correct since Bob may not have chosen the correct basis to apply the filter. He then converts the degree of these photons into bit values of 0 or 1 using the same rules as Alice. After measuring the photons, Bob will have a string of 0s and 1s. He will also have a record of which basis he applied the filters on each photon. He will then communicate with Alice on which basis he measured each photon in. However, this sequence of 0s and 1s will in general be different from the sequence of 0s and 1s that Alice has because of the uncertainty principle. The uncertainty principle tells us that only when the sent basis and measurement basis of a photon is the same, will Bob definitely have the same bit as Alice does for that photon then. Otherwise, Bob’s bit value will not be correlated to Alice’s bit value in any way. Alice will then have to discard all the bits that come from the photons whose sent and measurement basis is not the same. We are now one step away from getting the final encryption key for Alice and Bob.
As in all tales of cryptography, there always have to be a third party, Eve, who tries to breach the protocol. Eve could try to intercept the photons sent by Alice to Bob, measure it, and then try to resend the photon she intercepted to Bob. However, it would be impossible for Eve to do so because she does not know which basis Alice sent those photons out originally. If Eve measures the photon in the wrong basis, she would have projected the photon onto that wrong basis. When she tries to resend the “exact” photon to Bob, she would then send a photon polarized differently as the one she receives. Thus, Eve alters the result of Bob’s measurement. This could be detected by Alice and Bob when they later publicly compare a part of their bits information. The reason why Eve could not make a perfect copy of that photon she intercepted and then resend the original one to Bob is due to the non-cloning theorem (Wootters & Zurek, 1982). A naïve intercept and resend attack for BB84 will not work.

Finally, Alice will tell Bob which photons have the same measurement and sent basis. For Alice and Bob, the bit values they have for these photons are going to be the same. Now, they share a sequence of bits that are the same and completely random. By publicly comparing some of the bits that are supposed to be the same, Alice and Bob will have an idea of how much eavesdropping Eve has done. If Eve has done too much eavesdropping and it is impossible for Alice and Bob to still use this sequence of bits as secret keys, they will discard it and then repeat the process again to get another secret key. If not, Alice and Bob will keep the secret part of the bits as their final encryption key. For each message, Alice and Bob will generate such a key and use it as a one-time pad for that message only. It is claimed by Information Theory that a protocol of one-time pad that reuses no secret key for encrypting messages could never be broken by any eavesdropper (Shannon, Oct. 1949). Thus, BB84 is in theory unbreakable.

2.2. Means of Attack

Although BB84 mentioned above is in theory unbreakable, there is no way to implement the theory in real life perfectly. Due to imperfection in both generating the photons and measuring the photons, there are multiple ways to perform quantum hacks, breaking quantum key distributions by exploiting imperfections of the implemented system. One of the most crucial ways of attacking BB84 protocol is the phase-remapping attack. The importance of this method comes from the fact that it is the first method that is devised and successfully implemented onto a widely-used commercial quantum key distribution system (Xu, Qi, & Lo, 2010).

In Xu’s paper, his team successfully implemented the phase remapping attack on the ID-500 quantum key distribution system (Xu, Qi, & Lo, 2010). During the testing cases, Eve was able to gain full information about the keys that Alice and Bob are going to use. Since the quantum bit error rate caused by eavesdropping is lower than the alert bound for that system, Alice and Bob will not notice the act of Eve. Thus, the BB84 protocol is no longer secure anymore. However, this attack could be defeated without doing a lot of changes to the original protocol. Mentioned in Xu’s paper, Alice only need to carefully monitor the phase difference of her reference pulse and signal pulse to make sure that no time delay is introduced between the two pulses. If there is, Alice knows that Eve has successfully phase-shifted the two pulses and the security of her communication with Bob is compromised. Furthermore, Alice could also detect Eve’s attack by estimating the statistics of the BB84 states (Xu, Qi, & Lo, 2010).

There is also another way to attack the BB84 protocol which could not be solved easily by doing extra checks. It is known as the photon number splitting attack. The basics of this attack method is the following. In theory, Alice should send single photon to Bob one at a time in BB84 protocol. Because of the limitation in generating single photon in real life, most of the implementation of BB84 uses phase-randomized weak coherent pulses (Lo, Curty, & Tamaki, 2014). This means that sometimes there will be more than one photon sent at one time. These photons are completely the same. Eve could thus intercept the photons Alice sent to Bob. Whenever she sees multiple photons arriving at the same time, Eve could split some photons and let only one or a few pass. In this way, Eve would have the ability to retrieve as much information from the photon as Bob would. Even better for Eve, her attack on the system would not have been noticed by Alice and Bob if they only compare the bits they
got after sending and measuring the photons. Since Eve does not alter the physical property of photon but merely the number of photons Bob receives, Bob’s bit sequence would not have been altered had there be no Eve at all. Although Eve does not have the exact same sequence of bits that Alice and Bob shares, the probability of multiple photons been sent at the same time decreases exponentially with the increase of number of photons. It is still possible that Eve will be able to decrypt some secret information sent between Alice and Bob. In order to make quantum key distribution completely safe, the source loophole has to be closed. This is later achieved by decoy state modification of BB84.

3. DECOY STATE

Since the only difference photon number splitting attack made is that now Alice and Bob have no idea of whether they are attacked or not, an improvement on the original protocol should only need to reveal the existence of Eve. In the paper “Decoy State Quantum Key Distribution”, Hoi Kwong Lo devised an improvement on the original BB84 that would allow Alice and Bob to detect whether Eve is eavesdropping on them or not.

Lo’s method to detect eavesdropping is to use decoy stat. In his implementation, there are two kinds of signals sent to Bob from Alice. One of them is the regular BB84 signal that serves as the generator of key bits. The other ones are the decoy signals. These decoy signals differ from the regular one only in their intensity. It might seem like Eve is more likely to gain information about the photon polarization since there is a higher probability of multiple photons occurrence. However, Alice and Bob are now able to detect Eve’s intrusion on their channel. To avoid altering the state of photons, Eve should not do any measurement on the photons except for measuring the number of photons she receives at a particular spot of time when she is doing the photon number splitting attack. Eve could not maintain the yield rate and error rate that is easily calculable for both Alice and Bob (Lo, Curty, & Tamaki, 2014). Thus, Alice and Bob could easily know whether Eves had eavesdropped or not.

A benefit of using decoy state improvement upon BB84 is that it does not require much fancier equipment. The only extra equipment you would need is a variable optical attenuator that could change the intensity of each signal and thus creating the decoy state (Lo, Curty, & Tamaki, 2014).

4. Measurement Device Independence QKD

The wide implementation of decoy states in similar protocols as BB84 has once and for all ended the possibility of photon number splitting attack and securing the source side problem. However, this does not stop quantum hackers from breaking BB84 protocol and variations of it from exploiting the loopholes of the measurement side. Attacks like Time Shift, Time Information, and Detector dead time were still threatening the security of the BB84 protocol and its variations.

Several improvements have been made in attempt to solve the measurement side security loophole. The first attempt people came up whenever a new loophole is found is to find a patch for that. However, it is easy to see that this way you are never guaranteed to be completely out of security problem forever. The second method people came up with relies on the violation of Bell’s inequality (Lo, Curty, & Tamaki, 2014). However, since a loophole free Bell experiment has never been achieved, this method of Device Independent Quantum Key Distribution is currently not available technologically.

That leaves us to the final promising candidate, Measurement Device Independent Quantum Key Distribution (MDI-QKD). This candidate is again proposed by Hoi-Kwong Lo. As its name suggests, MDI-QKD does not rely on the security of measurement side. In other words, the measurement side could be handled by a completely untrustworthy person. In the worst case scenario, even Eve could be the one carrying out the measurement.

Although MDI-QKD gives us the benefit of not having to worry about any attack aimed on the measurement side, it still has some draw backs. Firstly, MDI-QKD assumes that Alice and Bob has a perfect source. If the source from Alice and Bob is tampered with, the security of MDI-QKD falls apart. Secondly, the key generation rate of MDI-QKD is much lower than the regular BB84 (Lo, Curty, & Qi, Measurement-device-independent quantum key distribution., 2012). Which means to
generate the same length of encryption key, MDI-QKD would take longer time and thus slowing down the efficiency of the whole protocol.

5. Conclusion
Ever since the existence of the possibility of having a quantum computer and Shor’s algorithm, many people in the fields of cryptography have been living under a fear. They fear that one day our existing ways to encrypt messages will be easily cracked by a quantum computer. All our precious information about our bank account, transitions between businesses, and etc. will be readily available to the hackers. In theory, BB84 could save the day by generating shared secret bits between two parties. The two parties could then use these shared bits to communicate safely. Furthermore, an intrusion during the process of generating secret bits could be detected which alerts the two parties. However, things did not work out so well in reality. There exist loopholes from both source and measurement side of the implementation of quantum key distribution protocols. People developed different means to attack these loopholes and make the protocol unsafe. In response to that, our protocol evolved to defend against these attacks. Now that the measurement side loopholes have been forever closed by MDI-QKD, we would only have to worry about the source side loophole. Even though by careful processing, we could prevent Eve from utilizing the source side loophole, there is still benefit for us to develop better way to implement the protocols. Perhaps a way to achieve a perfect single photon generator could benefit us in terms of closing the source side loophole.

References
[1] Bennett, C. H., & Brassard, G. (4 December 2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, Pages 7-11.
[2] Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503. Retrieved 9 10, 2017, from https://ncbi.nlm.nih.gov/pubmed/22540686
[3] Lo, H.-K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595-604. Retrieved 9 10, 2017, from http://nature.com/nphoton/journal/v8/n8/full/nphoton.2014.149.html
[4] Pomerance, C. (1996). A Tale of Two Sieves. Notices of the American Mathematical Society, 43(12). Retrieved 9 10, 2017, from http://www.ams.org/notices/199612/pomerance.pdf
[5] Shannon, C. E. (Oct. 1949). Communication theory of secrecy systems. The Bell System Technical Journal, vol. 28, no. 4, 656-715.
[6] Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Scientific and Statistical Computing, 26, 1484. Retrieved 9 10, 2017
[7] Thomson, B. K. (1901). Baltimore Lectures on Molecular Dynamics and the Wave Theory of Light: NINETEENTH CENTURY CLOUDS OVER THE DYNAMICAL THEORY OF HEAT AND LIGHT. Philosophical Magazine Series 1, 2(7), 1-40. Retrieved 9 10, 2017, from http://tandfonline.com/doi/abs/10.1080/14786440109462664
[8] Wootters, W., & Zurek,. W. (1982). A Single Quantum Cannot be Cloned. Nature299, 802–803.
[9] Xu, F., Qi, B., & Lo, H.-K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New Journal of Physics, 12(11), 113026. Retrieved 9 10, 2017, from http://iopscience.iop.org/article/10.1088/1367-2630/12/11/113026/pdf