Creating Secure Encryption with Quantum Cryptography

Ananya Teklu
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA 56267
teklu009@morris.umn.edu

ABSTRACT

This paper discusses how quantum cryptography can be used to create secure communication channels for keys and create unbreakable encryptions. I explore two methods for creating these secure connections. The first is called prepare-and-measure protocol. This protocol uses quantum properties of light to create a secure connection. I focus on a specific implementation of this protocol as BB84. This protocol works by encoding each bit of a secret key into a polarization state of a single photon. The second one is entanglement-based protocol. This protocol uses the properties of quantum physics called entanglement to create secure communication channels. I also discuss Ekert protocol that is an implementation of entanglement-based protocol to create a secure connection.

Keywords

Quantum Key Distribution, Entanglement, Superposition, Photons, Cryptography

1. INTRODUCTION

Having a reliable and strong cryptographic system is more important than ever. We use it to securely send our passwords over the internet, transmit information between different kinds of IoT devices, and verify people's identities. Most of our current cryptographic methods work by using keys to scramble and unscramble messages. For instance, if Alice and Bob want to send a secret message to each other, they would have to agree on a key beforehand or use a secure communication channel to communicate their key to create their secret message. Alice can then use the key to scramble her message and send that to Bob. Bob then receives the scrambled message and unscramble it using the key. A third party won't be able to read their message as long as the key is known only to Alice and Bob. As a result, cryptographers try to create powerful keys that can be used between two legitimate parties using different kinds of systems that is also known as the "key distribution problem" [6]. Cryptographers currently rely on computational difficulty of certain mathematical problems to encrypt and decrypt information. For example, the RSA cryptosystem was invented in 1977 by Adi Shamir, Leonard Adleman, and Ronald Rivest exploits the difficulty of factoring two prime numbers for generation of keys. Since these systems rely on the computational difficulty of mathematical problems, they can in theory be broken when a powerful computer becomes available. There is one noteworthy technique that is not susceptible to such scenario called One-Time-Pad that uses a random key generated once to be used to encrypt and decrypt our messages [6]. However, in current cryptosystems, sharing a long non-reusable key is a difficult as sharing the message it encrypts, thus its usage is not practical. I will discuss One-Time-Pad in detail in later sections.

Quantum cryptography strengthens the power of current classical cryptography by using the physical laws of quantum mechanics to facilitate secure communications [2]. One example of this cryptographic method is Quantum Key Distribution. Quantum Key Distribution solves the problem of transmitting cryptographic keys securely between legitimate parties over insecure channel. Researchers are using quantum systems to manipulate atoms, photons, or electrons to create quantum effects such as superposition and entanglement. These quantum effects enables researchers to create new communication channels that allow them to detect any eavesdropping. This paper will explore how we can use these properties in different Quantum Key Distribution protocols.

Section 2 provides background on how some of the important quantum effects work as well as describe our current cryptographic standards. Section 3 describes how it is possible to use the effects of quantum mechanics and some of our current cryptographic systems to create a new system that is more secure. Section 4 will synthesize those topics by exploring some of the implementations in real world systems and simulations. The conclusiin Section will summarize the advantages and disadvantages of QKD protocols and discusses what challenges may be faced implementing these systems.

2. BACKGROUND

The background covers some important concepts for understanding the security protocols.

2.1 Quantum Computation

Quantum Computation is based on quantum mechanics which uses the quantum nature of particles to store and manipulate information. Unlike classical computing which uses bits that have state 1 and 0, quantum computers use quantum bits or qubits. Qubits can have states 1 and 0 just like classical bits but they can also have states that are both 1 and 0 at the same time which is called a superposition

UMM CSci Senior Seminar Conference, November 2020 Morris, MN.

state. [4]

2.1.1 Qubit

A qubit can be represented physically by the spin of an atom or a polarization of a photon. To illustrate this mathematically, a qubit commonly denoted as $|\Psi\rangle$ is an element of a finite dimentional complex vector space known as a Hilbert space. It is comprised of orthogonal bases of two states $|0\rangle$ and $|1\rangle$. This quantum state can be in any logical superposition of the bases states. [2]

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where α and β are usually the complex number coefficients. These coefficients are called the probability amplitudes. For example, when we want to represent the classical "0" with a qubit, the state is written as $|0\rangle = 1\,|0\rangle + 0\,|1\rangle$. If we measure the value of this qubit, the result would come out "0" 100% of the time since the probability amplitude of the state $|0\rangle$ is 1. On the other hand, when we want to represent the classical bit "1", the state is written as $|1\rangle = 0\,|0\rangle + 1\,|1\rangle$. When we measure the value of this qubit, the result would come out "1" 100% of the time since the probability amplitude of the state $|1\rangle$ is 1.

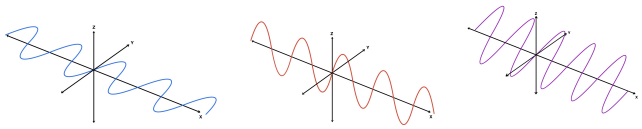
Qubits can also represent states that are impossible to be represented in classical computers. This states are called superposition states. One example of these states can be written as $|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$. the measurement of this qubit has the probability of yielding "0" 50% of the time and "1" 50% of the time. The probability amplitude can be any combination of two complex numbers as long as the squared values of those complex numbers sums up to 1 meaning the probability amplitudes $|\alpha|^2 + |\beta|^2 = 1$, where $|\ |$ denotes the absolute value [2].

2.2 Physical Quantum States

Section 2.1.1 describes how we can represent qubits abstractly using 0s and 1s. Those states however are usually encoded into different physical states. We will discuss those states below.

2.2.1 Photon Polarization

Photons are light particles that are viewed in physics as waves. They can be useful for encoding different quantum states. The photons can oscillate in different directions depending on their polarization. For example photons can wave horizontally or vertically with respect to the x,y, and z plane represented in figure 1(a) and figure 1(b) respectively. The quantum state of the horizontally polarized photon can represented with $|\rightarrow\rangle$ and vertically polarized photon can be represented with $|\uparrow\rangle$. photons can also exist in a superposition of the two waves.



(a) Horizontally $|\rightarrow\rangle$ polarized photon

(b) Vertically $|\uparrow\rangle$ polarized photon

(c) Superposition of $|\rightarrow\rangle$ and $|\uparrow\rangle$ polarized photon

Figure 1: Photon polarization states

The superposition of the horizontal $|\rightarrow\rangle$ and vertical $|\uparrow\rangle$ wave creates a new wave which we can call a diagonally polarized photon or 45° polarized photon $|\nearrow\rangle = |\rightarrow\rangle + |\uparrow\rangle$ that is represented in Figure 1(c).

We can use polarization filters to measure photon polarization states. We discuss different kinds of filters to measure the photon's polarization states. Suppose we have two different types of filters. Rectilinear filter (+) and a diagonal filter (×). If someone measures a horizontally or vertically polarized photon using a rectilinear filter (+) and another person repeats the process using the same filter, the two people would get same results. On the other hand, if two people use different types of filters to measure the same photon, their results would be completely random. This property is used to create encryptions that are provably secure. I discuss this in detail in later sections.

2.2.2 Particle Spin

Particle spin states can also be used to encode quantum states. A particle can have a spin-up state $|\uparrow\rangle$ or spin-down state $|\downarrow\rangle$ represented in Figure 2A) and B) respectively. Particles can also have a superposition of a spin-up and down state $|\uparrow\downarrow\rangle$ represented in Figure 2C). We use this concept in section 3.3.1.

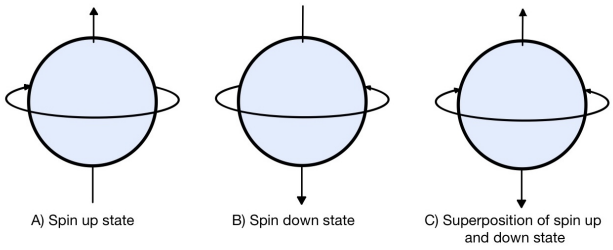


Figure 2: Particle spin states

2.3 Entanglement

Entanglement is quantum phenomenon where two particles can exist in an entangled state where a measurement on one of the particle's state will simultaneously change the other to be in an opposite state. Suppose we have particle A in state $|0\rangle$ and particle B in state $|1\rangle$. If we want to represent the comprehensive state of the two particles, we would write them as $|01\rangle$. However, it is not possible to write the entangled state as a combination of single particle states. When the two particles are in an entangled state, they cannot be described independently of each other. It is mathematically written as follows. [8]

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B) \tag{1}$$

2.3.1 Entanglement Between Spin-Particles

As discussed in above section, particles can exist in entangled state where a measurement on one of the particles, influences the other. To illustrate this, if we have entanglement between two spin particles shown in Figure 3. A measurement on either of the particle's spin would influence the spin of the other particle. For instance, if we find the

first particle to be spin-up state using a certain basis, we will instantly find that the measurement of the second particle to be in spin-down as long as we are using the same basis. when particles are entangled, it is not known how they are spinning even though one of the particle is known to be spinning up and the other spinning down or vice versa before a measurement. This phenomenon is used in quantum cryptography to generate keys. We will use this concept in Section 3.3.1.

Figure 3: Entanglement between spin particles

2.4 Classical Cryptography

In the current cryptographic systems, people communicate securely by using two different kinds of cryptographic methods. One is symmetric key cryptography that uses a shared key to encode and decode the message, and the other is asymmetric key cryptography that uses pairs of keys, one public and one private, to encrypt and decrypt messages. We discuss both in detail below.

Symmetric key cryptography uses a shared key where the sender uses the key to hide his/her information (encryption) and the receiver uses the same key the sender used to retrieve the hidden information (decryption). If the two parties use a key with same length as the message they are sending, and if the key is randomly generated every time it is used, they will have a provably secure cryptographic system. We will further discuss this in Section 2.4.1. A cryptographic algoritm is said to be provably secure if its not possible to break even with unlimited computational power [3].

Asymmetric cryptography (public key cryptography) uses two matching keys a public and private key. For instance, if two parties want to send cryptographic messages using public key cryptography, both generate a public key and a private key. The public key can be accessed by anyone and the private key is hidden. The public key can be used to encrypt data and only the matching private key is able decrypt the message. The generation of these keys is mainly dependent on what is called "one-way" functions. These functions are easy to compute one way and almost impossible to compute the other way due to the computational complexity growing exponentially as the number of bits on the key increases. One draw back of these current crypto systems is the possibility of an eavesdropper finding out the key. If the eavesdropper copies the key, he/she will be able to decrypt the message.

2.4.1 One-Time Pad

One-time pad is a symmetric cryptography that is provably secure. A message can be encoded into binary and any message that consists of binary symbols can be encoded with a secret key of same length to get an encrypted message shown in figure 5. Encoding is done by using bit-wise exclusive or also known as XOR ($\oplus$). The XOR of two bits returns 0 when the value of the two bits is the same. It returns 1 when the values of the two bits is different as presented in Figure 4. The encryption is done by XORing all of the bits with their corresponding bits of the key (the first bit of the message with the first bit of the key, the second with the second, and so on). The person who knows the key would be able to decrypt the message by XORing the key and the message shown in Figure 5. This cryptographic method is impossible to break as long as the key is used only once. This is because every message is encoded with the same length of its corresponding key which it impossible to know since two equally probable messages are encrypted with their keys are also equally probable. Quantum Key Distribution uses a one-time pad with quantum channel to generate the key securely.

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Figure 4: Bit-wise exclusive or operation (XOR)

Encrypting binary HELLO

Message	01001000 01000101 01001100 01001100 01001111
	⊕
Key	11100101 01000111 01110000 01010100 10101011
Ciphertext	10101101 00000010 00111100 00011000 11101100

Decrypting the ciphertext

Ciphertext	10101101 00000010 00111100 00011000 11101100
	⊕
Key	11100101 01000111 01110000 01010100 10101011
Message	01001000 01000101 01001100 01001100 01001111

Figure 5: Encryption and Decryption using One-Time-Pad

3. QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) protocol uses quantum computing to create a secure communication channels for sending keys between two parties. This process can be done using quantum properties of light, lasers, and some other technologies to enable the two parties to send keys securely. QKD uses two principal properties of quantum mechanics. The Heisenberg's uncertainty principle that states, a measurement on a quantum state changes the state. As a result, "When exchanging quantum information, the two communicating parties are able to determine if the quantum channel is compromised by a third party before they start the key transmission. They repeat the test process until they find a secure quantum channel over which they can safely exchange

the secret key." [4] In addition, the "no cloning theorem" [1] states that a measurement on a quantum state destroys the state. That makes it impossible for an eavesdropper to make a copy of the state to steal information.

QKD generates the key needed for one-time pad discussed in Section 2.2.1 using a quantum channel to generate the secret key between the two parties. QKD uses two different types of protocols to transmit the key to the legitimate parties. 1) prepare-and-measure protocol that uses the Heisenberg's uncertainty principle and 2) entanglement-based protocols that use entangled qubits. Both of these protocols use two channels; a quantum communication channel and a classical communication channel which is any communication channel such as the internet or phone call that is assumed to be insecure.

3.1 Prepare-and-measure protocols

Prepare and measure protocols utilize Heisenberg's Uncertainty principle which states that measuring a quantum state changes that state in some way. This allows eavesdropping to be detected. In case of eavesdropping, the data the eavesdropper accessed gets altered. This allows the sender and receiver to dispose of the corrupted data as well as to calculate the of data that has been lost [9].

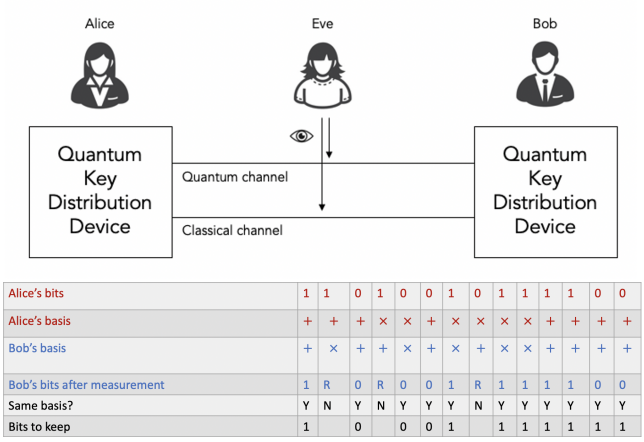
3.1.1 BB84 protocol

BB84 is the first quantum cryptographic protocol that was proposed by Bennett et al in 1984 [7]. This protocol uses Heisenberg's uncertainty principle in a "single-photon" quantum channel discussed in 2.2.1. Photons are sent through filters in a clever way that allows Alice and Bob to both detect eavesdropping and to randomly generate bits to be used in a secrete key. If Alice and Bob want to generate a private key using this protocol, they would use quantum channel to send their quantum states. Optical fiber can be used as a quantum channel if they use photons to carry their quantum states. BB84 is designed to detect a third party tapping into this quantum channel. [7].

To start the protocol, Alice uses a photon source that generates random photons polarized in one of four different directions. Horizontal (0°), vertical (90°), diagonal right (45°), and diagonal left (135°). She then chooses the polarized state of each photon to represent her bits that will be sent to Bob as shown in Figure 6. These photons are associated with two types of bases: rectilinear basis (+) which measures the horizontal and vertical states of a photon and diagonal basis (×) which measures the diagonal left and right states of a photon. According to Heisenberg's uncertainty principle, one can not measure both the rectilinear and diagonal bases of a photon at the same time.

Alice then sends the photons to Bob using a quantum channel. When Bob receives incoming photons, he uses random sets of bases to measure the photons. If he uses the same bases as Alice indicated on the first column of the table on Figure 6, the measured photons yield the same results as Alice. If he uses different bases indicated on the second column on figure 6, his photon yields random states that have a 50-50% chance of matching Alice's 0/1 meaurement. After measuring all the photons, Alice and Bob use the classical channel to declare what kind of bases they used and disregard all the bits that were measured with incompatible filters (last row of Figure 6) 6. Since the values of the photons measured in different bases is purely random, it will not be used for the key generation process. To check for a potential eavesdropper, Alice and have to sacrifice a random subset of n bits whose values they compare using the classical channel. Those bits are discarded from the key as well. For example, if Alice and Bob compare the first three bits of their key to check for an eavesdropper, both would observe the was same bit pattern (1 0 0) if no eavesdropper was present. However, if eavesdropper Eve measured the bits and incorrectly chose the filter-type, then Bob's values would be randomized. If Alice and Bob compare a sufficient number of bits the are likely to detect the presence of an eavesdropper.

Under purely random circumstances, Eve has a 50% chance of randomly matching the shared filter-type of Alice and Bob (and thus intercepting the bit undetected), but she has a 50% chance of randomly selecting the wrong filter-type. Using the wrong filter randomizes Bob's measurement and so there is a 50% chance of his 0/1 measurement not matching Alice. In total this means that each bit being observed by Eve has a 25% chance of producing a discrepancy between Alice's observation and Bob's observation. There's a better than 94% chance that at least 1 out of 10 bits would show a discrepancy (1-0.75^{10}) as a result of Eve's surveillance. [6, 7]



Alice's bits	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's bits after measurement	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	1	1

Figure 6: BB84 protocol performed with polarization of photons

3.2 Simulating BB84 protocol

More aspects of quantum cryptography have moved into the experimental phase over the last few years. Some technologies enabled researchers to develop Quantum Key Distribution protocols that are practical enough to be implemented for real world applications and are currently commercially available. They are also currently in use by governments and military. For instance, The firm MagiQ Technologies which is based in the United States, provides a variety of communication technologies for United States military and NASA. They offer various brand-new quantum mechanics based technologies for maximum security. The QPN 8505 quantum key distribution system is one example of this technology, that can be incorporated with classical networking to give extra layer of security to important military and financial systems. [10].

According to Shuangbao Wang, Matthew Rohde, and Amjad Ali [10], the BB84 protocol can be simulated using OptSim™

and OptiSystem™. Both of these implement BB84 protocol using "optical network simulation software" [10]. OptSim™ provides implementation for examining the polarization of single photons in addition to simulating photon detectors [10]. It also offers a wide variety of light sources and transmission mediums. Researchers also modeled BB84 using MATLAB and compared the results with experiments done using physical equipment. They mainly focused on finding the efficiency of creating a secure key between two parties. They considered numerous attributes of the hardware used to ensure accuracy [10].

The researchers concluded that the results they found prove that their models accurately represent the QKD setup that uses fiber optic cables and laser pulses. This shows that individual photon sources can be implemented once the hardware infrastructure becomes available.

3.3 Entanglement-based protocols

Entanglement-based (EB) protocols utilize sets of entangled particles which are shared between two parties. As clarified in Section 2.3 , entanglement is a quantum phenomenon that links two objects together in such a way that they start acting as one object. Moreover, a measurement on one of the objects would impact the other as well. Practically, if two entangled particles are distributed between two parties, any interception in either of the particles disrupts the entanglement connection. This allows for the detection of any eavesdropper. EB protocols give more advantages over prepare-and-measure protocols since they create an "inherent randomness" to the results of the measurement on the entangled systems creating purely random keys. [6]

3.3.1 Ekert Protocol

The Ekert protocol was first proposed by Artur Ekert in 1991 and uses a modification of the BB84 protocol that was put forward by Bennett and Brassard [5]. This protocol utilises entangled pairs of quantum particle's spin instead of single photons used in BB84. A central source is used to send the entangled particles to the two legitimate parties that want a secret key for encryption. The Ekert protocol uses quantum states called "spin singles" to describe the formation of quantum entanglement. As described in the previous sections, when two particles are in an entangled state, their states can not be described independently of each other. While we don't know the separate states of these entangled particles, composite state of the system is well defined. As an illustration, If Alice and Bob want to create a secure key using the Ekert protocol, a central source generates entangled particles and sends one to Alice and one to Bob [5]. The central source can not be trusted since the source might be in possession of Eve (eavesdropper). As a result, Ekert protocol establishes the source to emit pairs of 'entangled particles explained in section 2.3.1. [5]

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{2}$$

In the equation above, the first bracket represents the state where the first particle is pointing up and the second particle is pointing down. The second bracket represents the first particle pointing down and the second particle pointing up. This is called the superposition of the states, where the joined state of the two particles is well defined. This concept is covered in the background section and Figure 2 gives visual details. Nonetheless, it is not known how the particle is spinning even though one of the particle is known to be spinning up and the other spinning down or vice versa before a measurement is made. [5]

Alice and Bob must choose bases randomly in three different axes to measure the incoming particles. If the particles are in the xyz plane, they can be measured in (0°), (45°), (90°), and (135°) starting from (0°) from x axis as shown in Figure 7.

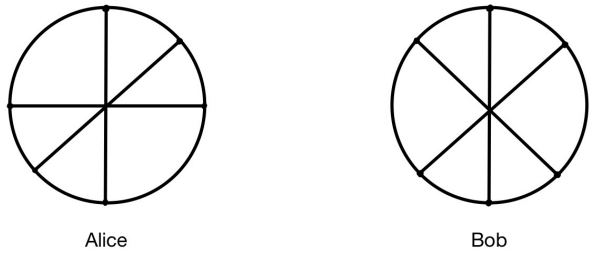


Figure 7: By measuring from the positive x axis, we can see that Alice used the bases that are lined up at (0°), (45°), and (90°), and Bob used the bases (45°), (90°) and (135°) [5]

Since it is possible for Alice and Bob to pick three axes, there is 33% chance for Alice and Bob to pick the same basis to measure their particles. If they choose the same basis, and Alice measures a spin-up particle, the whole quantum state collapses into the first state (the spin-up and down state) shown in Equation 3 and Bob will measure a spin-down state with 100% probability. If Alice measures spin-down state, Bob will detect a measurement of a spin-up state. On the other hand, if Alice and Bob use different bases to measure the states, their measurements will be completely uncorrelated. This suggests that the particle of Bob "knows" how Alice's particle was observed and aligns itself accordingly. This is possible because of the entanglement between the two particles. [5]

Alice and Bob can measure their multiple entangled particles sent to them as stated above and dispose of all the ones they measured in different basis. They do this by declaring what kind of basis they used using a classical channel similar to the BB84 protocol. This process shrinks their key down on average to 1/3 of its previous size which then can be used as a secure key for encryption. spin-up and spin-down represent the bits 1 and 0 respectively. [5]

3.4 Entanglement-based protocol Implementation

A group of researchers in Chinese academics of science were able to conduct a satellite based quantum communication using entanglement-based quantum cryptography using entangled photons (This is different from Ekert's protocol). They achieved an entanglement over 1100 km using a satellite and two ground stations. This is very significant when compared to the previous record of approximately 100km. They claim that the efficiency of their link is over 12 orders of magnitude greater than the direct two directional communication of two photons through the best commercial fibers. [11]

They conducted their experiments located at the two

ground stations Delingha in Qinghai province at an altitude of 3153m, and Nashan in Xinjinang province at an altitude of 2028m. The two stations are 1120km apart. The stations use ground telescopes that are precisely built for entanglement-based key distribution experiments. The satellite used orbits on a "Sun-synchronous orbit", and appears on both Delingha's and Nashan's sky once every single night, starting from 2:00AM Beijing time appearing for about 285 seconds. This satellite weighs 23.8kg and is fitted with spaceborne entangled photon source" [11]. This source generates entangled photon pairs with the form $|\Phi\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2)$ where $|H\rangle$ represents the horizontal polarization states and $|V\rangle$ represents the vertical polarization states. The subscripts 1 and 2 represent the two output modes. The researchers claim that this source generates and distributes up to 5.9×10^6 entangled photon pairs per second.

The photons are collected using the two ground telescopes at the stations. These telescopes are equipped with beam splitters that examine the polarization state of the entangled photons randomly in the Rectilinear (horizontal or vertical) bases and the diagonal bases and detected by four single photon detectors (SPDs). By carefully picking the four SPDs, the researchers claim that the detector efficiency was consistently above 98.5%. The output signal from the SPDs is then recorded using a device called "time-to-digital converter". After creating a key for QKD, the researchers claim that they achieved a quantum bit error rate of about 4.5%. They believe that this will allow the realization of satellite-based entanglement quantum key distribution.

4. CONCLUSIONS

Quantum Key Distribution is an infant field that is growing. Some implementations are being realized in US government military and financial institutions to hide sensitive data. More experiments are also being done using simulations and real equipment such as satellites to implement these protocols. Prepare-and-measure protocols are less susceptible to weather and other environmental problems. However, most implementations are still in experimental phases and will only work for no more than 100km. On the other hand, entanglement-based-protocols have been implemented using satellites and quantum repeaters to work over longer distances but more work needs to be done to create more stable entanglement to use them over wider scale.

Acknowledgments

I would like to thank my advisor Dr. Elena Machkasova for giving me helpful feedback though-out the semester. I would also like to thank professor Peter Dolan and Melissa Helgeson for their thorough feedback.

5. REFERENCES

[1] Quantiki, the no-cloning theorem.

[2] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe. Quantum cryptography: A survey. *ACM Comput. Surv.*, 39(2):6–es, July 2007.

[3] Christof Paar & Jan Pelzl. *Understanding Cryptography*. Springer Science and Business Media, 2009.

[4] T. Curcic, M. E. Filipkowski, A. Chtchelkanova, P. A. D'Ambrosio, S. A. Wolf, M. Foster, and D. Cochran. Quantum networks: From quantum cryptography to quantum architecture. *SIGCOMM Comput. Commun. Rev.*, 34(5):3–8, Oct. 2004.

[5] N. Ilić. The ekert protocol. 2007.

[6] M. Javed and K. Aziz. A survey of quantum key distribution protocols. In *Proceedings of the 7th International Conference on Frontiers of Information Technology*, FIT '09, New York, NY, USA, 2009. Association for Computing Machinery.

[7] W. Jia, Y. Zhang, H. Yu, and Y. Bian. A quantum key distribution protocol based on ldpc error correcting codes. In *Proceedings of the ACM Turing Celebration Conference - China*, ACM TURC '19, New York, NY, USA, 2019. Association for Computing Machinery.

[8] W. Kozlowski and S. Wehner. Towards large-scale quantum networks. In *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication*, NANOCOM '19, New York, NY, USA, 2019. Association for Computing Machinery.

[9] V. Mavroeidis, K. Vishi, M. D., and A. Jøsang. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, 9(3), 2018.

[10] S. Wang, M. Rohde, and A. Ali. Quantum cryptography and simulation: Tools and techniques. In *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, ICCSP 2020, page 36–41, New York, NY, USA, 2020. Association for Computing Machinery.

[11] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.