A Review of Quantum Cryptography

Antonius Torode[1,2,3]

1. National Superconducting Cyclotron Laboratory, East Lansing, MI 2. Joint Institute for Nuclear Astrophysics, Michigan State University, East Lansing, MI 3. Physics & Astronomy Department, Michigan State University, East Lansing, MI

December 3, 2017

Abstract

Many flaws exist with traditional encryption methods which leave new innovations like quantum cryptography as a subject of high interest. As quantum computing advanced, the security of traditional methods are greater threatened. Quantum cryptography is a method of sending quantum transmissions to create a secure random key shared between two parties so that traditional encryption methods can be utilized effectively. The process utilizes the Robertson uncertainty principle with further advances using quantum entanglement. This process, including flaws and current hacking attempts are discussed in detail.

I. Introduction

Communication through a technological mean play a major role in todays society. Whether it be through a phone call, email, or other means, there is a large demand for reliable communication. Unfortunately, although many means of communication appear to function well today, they may not necessarily be secure. In some cases, like banking transactions or relaying strategic military commands, it is important to ensure that the communication is secure from being heard from an outside party. Because of this, something known as cryptology has been widely used for many years. Cryptology is the process, study and application of cryptography and cryptanalysis, which represent the act of encrypting and decrypting information or messages, respectively. For the purpose of this paper, we will focus on cryptography.

An important example of when information requires secure encoding is within a country's voting system. Vote tampering has been prevalent in the United States and other countries throughout history [1]. Being able to properly safeguard votes between a voting precinct and where all of the ballots are tallied is important to maintaining the privacy of citizens and protecting unanimity. Cryptology is utilized in this process to secure communication between two parties. Switzerland is one country that has been on the cutting edge of research in a field known as quantum cryptography, which is a more recent cryptology development [2]. Unlike traditional forms of cryptography, quantum cryptography depends on physical properties of atoms rather than mathematical equations and large prime numbers [1][3][4].

Quantum cryptography has only been of primary interest for researchers within the last 50 year or so [4]. The first time it was used to experimentally exchange information was in October of 1989 [4]. The first main breakthrough came when it was realized by Bennett and Brassard that photons can be used to *transmit* information, rather than to *store* it. In order to understand how the process works, it is important to understand methods of historically typical encryption and then see how quantum encryption solves flaws that pertain to it.

II. Traditional Encryption

Cryptology has traditionally been based on algorithms that are generally mathematical procedures or processes. In conjunction with the algorithm, a key is generally used to encrypt or decrypt a message in a unique way. This key can be a phrase or string of numbers which are usually stored as bits. When a message is properly encrypted, it is nearly impossible to decipher it without the proper key.

There are two main methods used in traditional encryption methods. These are public-key cryptology (PKC) and secret-key cryptology (SKC). In PKC, there are two related keys that are used. One is released publicly for encrypting messages and the other is used for decrypting. By keeping the code used for decrypting private, this allows for messages to be securely sent to one person or party such that only they can decrypt it. The public key can then be given freely to anyone to send an encrypted message knowing that once it is encrypted only those with the private key can retrieve information from it. With current day algorithms and computers, this method utilizes very large prime numbers. Currently, to crack a key that was encrypted using a 128-bit key, the possible numbers used can be as high as 10^{38} [1].

In SKC only one key is used in both the encryption and decryption process of information. The algorithm can be shared over public channels because the idea is that if the key remains private, it cannot be cracked. One problem with this is that it requires a sufficiently complicated key in order to not be cracked by brute force. Similarly, it is not easy to have an agreed upon key between multiple parties that remains a secret. The main problem with SKC is that there is almost always a way for third parties to gain information about the secret key which is referred to as *the key problem* [1].

In both of these methods, there is a heavy use of mathematical algorithms that can be cracked and reproduced. With current computers, there is little threat to more sophisticated cryptology methods, but with the advancements of quantum computing, this is becoming a concern for the near future. Quantum Cryptography utilizes physics instead of math to provide a secure means of sharing a key with another party such that a third party would not be able to retrieve information without being noticed.

III. Basic Quantum Cryptography

The basis of quantum cryptography utilizes something known as quantum key distribution (QKD). QKD is a process by which a random key can be shared between two parties without having to share any secret information beforehand. In principle, by encoding digital information into a quantum system such as a stream of photons, it can be transmitted without being reliably read without information used in forming the transmission [4]. The quantum phenomenon that makes this possible is a generalization of the Heisenberg uncertainty principle, known as the Robertson uncertainty principle. It states that for any two hermitian operators X and Y,

$$\Delta X \Delta Y \geq \frac{1}{2} |\langle i[X,Y]\rangle| \ \ [5]. \tag{1}$$

In the case of photons, the linear and circular polarizations do not commute and thus cannot be measured simultaneously. By measuring the linear or circular polarization of a

1.	↺	↕	↻	↺	↕	↔	↻	↕	↔	↺	↔	↔	↻	↕	↔	↺	↔	↺	↺
2.		↕	↻		↕		↻	↕	↔		↔	↔	↻		↔	↺	↔		↺
3.		⊕	⊙		⊙		⊕	⊕	⊙		⊕	⊕	⊕		⊙	⊙	⊙		⊕
4.		↕	↻		↻		↕	↕	↺		↔	↔	↔		↺	↺	↻		↕
5.		⊕	⊙		⊙		⊕	⊕	⊙		⊕	⊕	⊕		⊙	⊙	⊙		⊕
6.		✓	✓					✓			✓	✓				✓			
7.		⊕	⊙					⊕			⊕	⊕				⊙			
8.		1	1					1			0	0				0			

Figure 1. A basic QKD protocol [4]. **1.** Alice sends a stream of randomly polarized photons (↔, ↕, ↺, or ↻) to Bob. **2.** The photons that are received by Bob. **3.** Bob measures the received photons randomly for either a rectilinear (⊕) or circular (⊙) polarization. **4.** The results of the measurements by Bob. **5.** The basis used for the measurements are sent back to Alice. **6.** The basis are either confirmed or rejected as to whether they were correct or not. **7.** Both parties only keep the results of those that were measured by the correct basis. **8.** The results are converted to a binary key based a coding scheme (↔=↺= 0 and ↕=↻= 1).

single photon, the other is randomly assigned. This is directly utilized in QKD.

For a system of photons, there exists two pairs of observables (polarization states) which can be reliably measured. These are referred to conjugate basis. Each basis consists of two polarizations such that when a measurement is taken, the photon will appear to be in only one. They are conjugate because between the two basis, when one is measured, the other is randomized. For photons, there is a rectilinear basis (which represents horizontal and vertical polarization) and a circular basis (which represents left-circular and right-circular). A conical polarization is thus either horizontal (↔), vertical (↕), left-circular (↺) or right-circular (↻).

A basic QKD protocol begins with two parties Alice and Bob. When information is required to be sent, Alice will send a stream of random conical photons consisting of all four polarizations to Bob. In reality, not all photons may make it through. Of the received photons, Bob will then choose randomly whether to measure the rectilinear (⊕) or circular (⊙) polarizations of each atom. Next, Bob tells Alice which basis he used to measure each photon that was received and Alice tells Bob whether that was the correct basis to use. Alice and Bob both decide to discard all photons that were not received by Bob and all of the ones that were measured using the wrong basis. Both parties then agree to create a binary key using a coding scheme (i.e. ↔=↺= 0 and ↕=↻= 1). This resulting key that is shared between the two parties is referred to as the *quantum transmission* [4]. And example of an uninterrupted quantum transmission is demonstrated in Fig. 1.

In the example from Fig. 1, there are only 6 bits of transmitted data. If we neglect experimental error, then Bob will know his measurements are correct because a rectilinear or circular polarized photon will not change when going through a rectilinear or circular filter respectively. In reality, a much larger sequence of photons would be sent and the same process would be carried out, thus giving a large string of random bits for the final key. Since Bob never reveals over a public channel the results of his measurement, only he knows the outcome. For a third party Eve that is listening in (eavesdropper), they can determine the filter used (since this is announced over public channels) but they will not know what Bob measured and thus only have a 50% chance of guessing the correct conical polarization. The final key will be a single string of binary which can then be translated into any language, number, or code for Alice and Bob to use for communication. If an eavesdropper has approximately 50% of the bits wrong, there is no way he can recover the same code that Alice and Bob have agreed on.

After the exchange, it is required to perform what is known as a parity check [1]. In principle, Eve could be between Alice and Bob making measurements and impersonating either of them. However, if Eve makes any measurements on the photons, it will have to be done in a similar way to how Bob would measure them, with random filters. When Eve makes a measurement, due to the uncertainty relation some of the photons will be altered from how Alice sent them. If Eve then forwards them to Bob after some have been altered, he will be able to tell through the parity check. The parity check is where Alice and Bob choose a random subset of bits from their key and compare the results of their binary outputs. If they match then they can be assured that their channel is secure. However, if Eve had altered some of the conical states by making her own measurements, then the parity check between the two parties will show some discrepancies [3]. If, for example, Eve measured a rectilinear polarized photon with a circular filter, the rectilinear polarization will randomize, and then if Bob measures it using the correct basis, there is some probability that his measurement will not yield the correct conical polarization that Alice had originally set.

IV. Flaws

Based on the process described above, except in the cases with arbitrarily small probability, there is no way for Eve to interfere with the quantum transmission without Alice and Bob being aware of it. However, in reality, detectors are not perfect and so there would be a small amount of noise regardless of whether an eavesdropper was present [4]. Similarly, it is very difficult to produce a single photon. What is likely to happen is a stream of photons in a superposition of quantum states can be sent. In this case, there is a small probability that an *Eve* could measure one of these photons without disturbing another, which would allow for Eve to measure a fraction of the bits without introducing any error for Alice and bob [4]. In Bennett et al., they outline a method and attempt to remedy these flaws and still have a viable quantum transmission [4].

Other flaws with quantum transmissions pertain to the length that we are able to perform the transmissions at. The original quantum cryptography system was only able to send a signal approximately 36 cm [1]. In newer systems, distances up to 150 km have been achieved. With today's communication ranging across continents, this is not ideal. The reason that it is difficult for large distances to reach is due to interference between photons. Photons can interact with any other particles, which can change the conical polarizations. As the distance a photon travels increases so does the probability that it could be changed from its original polarization.

V. Quantum Entanglement

Via a phenomenon called quantum entanglement, some believe that they could be able to improve the flaws pertaining to distance by entangling photons at both ends of a communication [1]. Unfortunately, there are some sources pointing out insecurities of methods that utilize this [6]. A group at the Massachusetts Institute of Technology (MIT) in Cambridge was able to successfully listen in on a quantum transmission by utilizing quantum entanglement [7]. They were able to obtain almost half of the transmitted data without being detected by those who were sending or receiving the signal. Fortunately, they admit that this method is not yet capable of eavesdropping on a real network. The team at MIT were able to entangle the conical polarizations of photons with the momentum of the photons, and thus by measuring the momentum of photons they could deduce the conical polarizations without disturbing the polarizations. They claim that the trick is not perfected and sometimes perturbs the polarization. The reason they were able to only retrieve almost half of the data is due to this reason. As they tried to retrieve more data, the error from this flaw began to rise noticeably [7].

VI. Conclusion

Through the use of physical properties of matter, a transmission can be sent to ensure a random creation of a key that two parties can agree upon. This key can be used in conjunction with traditional encryption methods to create a form of secure cryptographic communication. Although flaws exist, technology and new innovations allow us to continue advancements towards a more secure form of communication. With an implementation of quantum entanglement, security threats become introduced. With research in the field of quantum cryptography continuing, the idea becomes more likely to be adaptable for use on a large scale.

References

[1] Clark, Josh. How Quantum Cryptology Works. HowStuffWorks Science, HowStuffWorks, 23 Oct. 2007.

[2] Messmer, Ellen. ”Quantum Cryptography to Secure Ballots in Swiss Election.” Network World. October 11, 2007.

[3] Vittorio, Salvatore. ”Quantum Cryptography: Privacy through Uncertainty.” CSA. October 2002.

[4] Bennett H. C. et al. ”Experimental Quantum Cryptography.” September 1991.

[5] Torode, A. ”Antonius Handbook.” Michigan State University - Department of Physics & Astronomy. Volume I. Version: 2.030. 2017.

[6] Lau Hoi-Kwan. et al. ”Insecurity of position-based quantum-cryptography protocols against entanglement attacks.” Physical Review A83, 012322. 2011.

[7] Brumfiel, Geoffrey. ”Quantum Cryptography is Hacked.” Nature. April 27, 2007