The Ekert Protocol

Nikolina Ilic

Department of Physics, University of Waterloo, Waterloo, ON, Canada N2L 3G1

A brief history of Quantum Cryptography needed in order to understand the 1991 Ekert protocol is discussed. In particular, the Einstein-Podolsky-Rosen thought experiment and its relation to the Ekert protocol is described. The violation of Bell's theorem that results from measuring states described by Ekert is explained. Error Correction and Privacy Amplification techniques that are associated with standard protocols are briefly discussed.

In cryptography, encryption is the process of transforming information (plaintext) in such a way that it is readable, only by people it is intended for. Decryption describes the process of transforming encrypted information (ciphertext) into an understandable format using special knowledge. Ciphers are algorithms which describe steps for encrypting and decrypting information. In its early stages cryptography was based on securely transmitting entire encrypting and decrypting procedures. However, modern ciphers include the secure transmission of a key which is sent with the plaintext and the encryption algorithm. The parties involved exchange and decipher messages with a key that only they should have access to. This means that the plaintext and encryption algorithms can be made public, as long as the secrecy of the key is preserved.

Since the security of cryptography depends on the secure transmission of a key, the goal is to make a very secure channel through which the key is sent. In principle transmitting messages using classical channels allows an eavesdropper to gain information about the key without being detected. However, constructing transmission techniques based on quantum mechanics allows parties to transmit messages and detect the presence of an eavesdropper every time. This is because quantum principles state that the key being transmitted does not actually exist until it is observed, so naturally it is hard to gain information about it while it it "traveling" to the involved users, named Alice and Bob.

A thought experiment performed by Einstein, Podolsky, and Rosen, in 1935 explains the conceptual basis for why quantum cryptography works. Named the EPR paradox, it was initially designed to demonstrate that quantum mechanics is not a complete physical theory, but quickly became an illustration of how quantum mechanics defies classical intuition. The EPR trio relied on classical principles such as locality and realism. The principle of locality states that distant objects cannot have direct influence on one another. This assumption implies that the outcome of a measurement made on one object cannot influence the properties of another object. Realism is the idea that there exists a reality that is independent of observer, and implies that objects have definite properties which are unaffected by different types of measurements made on them. Both of these seemingly reasonable conditions are violated in the realm of quantum cryptography.

Using ideas introduced in EPR thought experiment, Stephen Weisner made a proposal for Quantum Cryptography in the 1970's. While formulating his theory, he considered some fundamental rules of Quantum Physics:

1. The polarization of a photon cannot be measured in non-compatible bases(ie: the vertical-horizontal basis/diagonal bases) at the same time.

2. Individual quantum processes cannot be distinctly described.

3. It is not possible to take measurements of a quantum system without disturbing it.

4. It is not possible to duplicate unknown quantum states.

The first axiom reinforces the idea that particles cannot be measured in incompatible bases at the same time. The second rule states that, although the whole state of the system is well defined, one cannot know information about individual objects in that state, such as the spin of an electron or polarization of a single photon. The third axiom plays an essential role in ensuring that the most valued property of quantum cryptography, its security, is preserved. It implies that and eavesdropper, named Eve, cannot eavesdrop on a message sent between Bob and Alice, without changing its meaning, and therefore exposing herself. Furthermore, Eve cannot conceal her presence by recreating her detected particles, because the fourth axiom prevents her from doing so.

In 1984 Charles H. Bennett of IBM and Gilles Brassard of the University of Montral incorporated Weisner's ideas into what is today known as the BB84 protocol[4]. The protocol used 4 quantum states, making up 2 bases. Alice sent particles to Bob in one of the four states, and Bob randomly selected bases in which to measure the particles

in. The protocol discussed in this article is a modification of the original Bennett and Brassard protocol and takes into consideration EPR states.

In 1991 Artur Ekert proposed that quantum key distribution be implemented using the quantum entangled states explored in the EPR thought experiment. In Ekert's protocol instead of Alice sending particles to Bob, there is a central source creating entangled particles and sending one to Alice and one to Bob. The Ekert protocol more accurately reflects future real life situations, since due to distance limitations, a practical implementation of quantum cryptography would involve a central source, such as a satellite, sending signals to multiple receivers.

Although many physical quantities (observables) can be used to explain the creation of quantum entanglement, Ekert used quantum states called spin singlets. Quantum entanglement is the inability to define the quantum state of one object without reference to the quantum state of another object far away from the first. Although no conclusions can be made about the individual states of the objects, the quantum state of both objects is well defined. Rather than trusting the source, which could be in Eve's hands, Ekert set up the protocol, such that the source emits pairs of spin- 1/2 particles in singlet states :

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

The equation above demonstrates that in state I (first bracket), particle A has a spin pointing up and particle B has a spin pointing down . In state II (second bracket) particle A has spin pointing down and particle B has spin pointing up. This can be called the superposition of states, in which the combined state of both particles is well defined, however it is unknown which way either particle is spinning. It other words, although it is known that one particle is spinning up, and the other spinning down, it is impossible to tell which particle is which until a measurement is made.

Both Alice and Bob must randomly pick one of three coplanar axes in which to measure the incoming particles. These three bases can be mathematically represented by defining the vectors a_i (i = 1,2,3) (for Alice) and b_j (j=1,2,3) (for Bob)[2]. If the particles are traveling along the z direction, the vectors a_i and b_j are defined as being located in the x-y plane (perpendicular to the trajectory of the particles). By using the vertical x axis from which to measure the angles, the vectors a_i and b_j can be described by $\phi_1^a = 0\,^\circ$, $\phi_2^a = 45\,^\circ$, $\phi_3^a = 90\,^\circ$, and $\phi_1^b = 45\,^\circ$, $\phi_2^b = 90\,^\circ$ and $\phi_3^b = 135\,^\circ$ [2]. The a and b superscripts describe the orientation of Alice and Bob's analyzer's respectively. Figure one shows a visual representation of the above described bases.

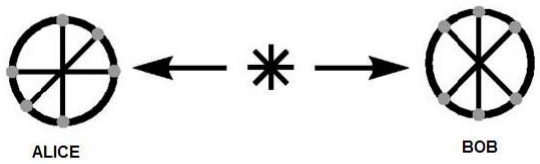

FIG. 1: An illustration of the described bases on the Poincare sphere. Measuring from the positive x-axis, one can see that Alice's bases are lined up at 0 °, 45 ° and 90 ° angles, while Bob's are located at 45 °, 90 ° and 135 °.

It is clear from the explanation above that there is a 1/3 chance that Alice and Bob will chose compatible basis in which to measure the incoming particles. If Alice and Bob chose a compatible basis, and Alice measures a spin up particle, the quantum state of the system collapses into state I, and the probability of Bob measuring a spin down particle is 100%. Similarly, if Alice observes a particle with spin down, Bob will detect a spin up particle with 100% certainty. However, when Alice and Bob decide to measure the spins in incompatible bases, this experiment becomes interesting. If Alice measures the particles in one basis, Bob's measurement outcome will be random when measured in a non-compatible basis. For example, if Alice detects a spin up particle in the 45 ° basis, there exists an equal probability that Bob will uncover a spin up or spin down particle in the 90 ° basis. This implies that Bob's particle "knows" how Alice's particle was measured, and orients itself accordingly. There must exist some form of action at a distance that informs Bob's particle which basis Alice used, so that Bob's particle can decide weather it should compliment Alice's measurement in the same basis, or pick a random orientation if incompatible bases are chosen. The fact that Alice and Bob's particles are aware of each other's presence, is what makes the entanglement phenomenon defy the classical rules of locality and realism. Quantum cryptography experiments have proved that this "spooky action at a distance" Einstein ridiculed, is a reality.

So if Alice and Bob choose compatible bases, their measurement results will be anti-correlated, meaning Bob's particle will have spin up, and Alice's will have spin down, and vice versa. In order to discard the random measurements Alice and Bob made in incompatible basis, the two participants must publicly announce which basis the particles were measured in. They can then discard results obtained in incompatible basis, without actually revealing the outcomes of their measurements. This sifting process shrinks the key down to 30% of its original size, leaving them with a sifted key. Within the sifted key, the spin up and spin down states of the particles correspond to bit values 1 and 0 respectively.

The fact that entangled states are used is one the things that makes it hard for eavesdropper to gain in-

formation about the key. Since the states of the particles are not collapsed until a measurement is made, trying to gain information about the system is analogous to looking for information that does not yet exist. For example, if both Alice and Bob choose to measure a particle in the 45 ° basis, and Alice detects a spin up particle, Bob expects to discover a spin down particle. If Bob's expectation is not fulfilled, it might mean that Eve has intercepted the line. If Eve is trying to detect particles coming from the source, she must choose a basis in which to measure her particle. In the process of detecting the particle in her basis, Eve destroys it. If Eve's choice of basis does not correspond to Alice's and Bob's, the result of her measurement will be random. She will then recreate her detected particle, and send it to Bob. After Eve's intervention, the orientation of the particle Bob receives will be random. If he measures an orientation that does not correlate to Alice's result, he will get an error.

Other types of quantum key distribution protocols, such as the BB84, and BBM92, involve utilizing only 4 or 2 states as opposed to Ekert's 6 states. The reason Ekert included an additional basis was because he wanted the ability to directly detect the presence of an eavesdropper, without having to leak out information about his key. Referring to the a_i and b_j vectors defined earlier, the correlation coefficient[2] of Alice's (a_i) and Bob's (b_j) measurements is

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) \quad (2)$$
$$P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j) \quad (3)$$

Where P± is the probability of obtaining ±1 along $a_i$and ±1 along b_j.

Now, one can define a quantity S, which is the sum of all correlation coefficients for which Alice and Bob used differently oriented analyzers (incompatible basis).

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) \quad (4)$$

Using local realism, Bell proved that the value of S is ≤ 2. However, quantum mechanics gives [1] that

$$S = 2\sqrt{2} \quad (5)$$

This means that that if the original states were truly entangled states, and defied the rules of local realism, Bell's theorem should be violated. Therefore, by publicly announcing the values Alice and Bob measured in incompatible basis, they can figure out a value for S. If the particles were not disturbed by an eavesdropper, S should equal $2\sqrt{2}$. If Alice and Bob receive their expected value of S, they can be sure that the values they measured in compatible basis are anti-correlated and that their sifted key is secure.

However, even if the possibility of an eavesdropper is eliminated, the sifted key may contain errors due to imperfections in the system[3]. Classical algorithms are used to correct the amount of error introduced during the key distribution. This error is referred to as the Quantum Bit Error Rate (QBER). After a sifted key is obtained Alice and Bob randomly choose a small portion of their secret key bit pairs, and compare them over a public channel. They are trying to find how much of their data is anti-correlated. As explained earlier, anti-correlation means that if Alice obtains a bit value of 1, Bob will get a value of 0, and vice versa. If both Bob and Alice receive a 1 or a 0, it means that an error has occurred in the system. The QBER is calculated by dividing the number of errors by the size of the sample and multiplying by 100%. A QBER gives an experimentalist an idea of how efficient the system is. In other protocols, which do not involve testing the violation of Bell's theorem, a QBER is used to confirm the presence of an eavesdropper. An error rate that exceeds approximately 15% is a good indication that there is an eavesdropper present.

Assuming that the possibility of an eavesdropper was eliminated, Alice and Bob proceed onto refining their keys through error correction. The simplest error correction technique, is one which includes XOR operations. Alice randomly chooses pairs of bits and announces their XOR value. Bob can either "accept" or "reject" this XOR value in his reply, depending on whether his XOR value is the same for the corresponding bits. If Bob accepts, Alice and Bob keep the first bit of the pair and discard the second. If Bob rejects, they discard both bits. After error correction, Alice and Bob both have identical keys. It should be noted that most real life implementations of the Ekert protocol contain more complicated and efficient error correction algorithms[3].

Because error correction was performed using a public channel, some information about the key might have been leaked out to Eve. The process of privacy amplification ensures that Eve cannot deduce any information about the final secret key from the data she received during error correction. The idea was introduced in 1988 by Bennett, Brassard, and Robert, [3] and has been incorporated in most implementations of the Ekert protocol. During this process Alice randomly chooses pairs of bits and computes their XOR value. However this time Alice only announces which bits she choose, and not what their XOR value was. Bob then finds the corresponding bits in his key. Alice and Bob then replace each of the bits by their XOR value. In other words, Alice and Bob XOR parts of their keys together, so that the final key is much shorter. This means if Eve where to know a value in the final key, she would have to know what the values of Alice's and Bob's bits were before the XOR operation was applied to them. This explanation is a simplification of standard privacy amplification procedures, but gives a general idea of how a final key secure key is obtained.

Error correction and privacy amplification are both classical algorithms, used to make the final key more secure. Privacy amplification, was originally developed for Quantum Cryptography, but has since then has been used in many classical cryptographic applications. After the two process are applied to the sifted key, Alice and Bob may use the resulting final key to transmit messages. A common practice is for messages to be encrypted and decrypted by Alice and Bob using the same XOR operation described above. Alice's encrypted message usually consists of a message and a secret key XORed together. The encrypted message is sent to Bob over the internet, and Bob uses his key to decrypt the message using the XOR operation.

The Ekert protocol extends the ideas developed by Bennett and Brassard in their 1984 quantum key distribution protocol [3]. It provides the theoretical physics necessary to transform the ideas developed in the EPR paradox into a physically testable experiments. Furthermore, it provides physicists with a way of obtaining experimental evidence that suggests classical ideas such as realism and locality do not form the basis for explaining how the universe works.

Acknowledgements - I would like to thank Devin Smith and Chris Erven for helpful comments on this manuscript.

[1] Chaung I., Nielson M, *Quantum Computation Information*, 137, (2000).
[2] Ekert. A, *Phys. Rev. Lett.* **67**, 661-663 (1991).
[3] Gisin N., Ribordy G., Tittel W.and Zbinden H., *Review of Modern Physics* **74**, 149-156 (2002).
[4] Stix. G *Scientific American*, 000479 (2004).