Review of *Quantum Cryptography with Entangled Photons* and Related Literature

PHYS 468 Winter 2020

Alexander Cooper

20629774

Introduction

The paper *Quantum Cryptography with Entangled Photons* [1] sets out to create the first fully realized implementation of a quantum key distribution (QKD) system. The authors claim to successfully distribute keys between two parties (Alice and Bob) through the implementation of two novel distribution schemes. Implementation is achieved with the use of polarized entangled photon pairs.

Classical Cryptography

The goal of cryptographic systems is to allow Alice and Bob to share information with no possibility of a third party (Eve) gaining the information. Secure transfer of information is achieved through the distribution of keys to Alice and Bob which are used to encode their information with a cryptographic function. A common and theoretically uncrackable cryptographic protocol is a one time pad protocol [2]. The key in a one time pad protocol is a random bit string equal in length to the message being sent. The bit string is combined with the message through a cryptographic function, (for example XORing each message bit with its corresponding key bit) to produce an encrypted message. Decrypting the message is achieved by reapplying the function to the encrypted message with the key. Without at least partial knowledge of the key, the encrypted message is uncrackable to an attacker (Even through methods of brute force).

Quantum Key Distribution

Classically, key distribution is the main weak point of a cryptographic system. It cannot be known if Eve has intercepted Alice and Bob’s keys during their distribution or even replaced them with her own. QKD addresses this flaw by introducing a scheme where by exploiting quantum mechanical properties it can be known to Alice and Bob if an attacker has gained knowledge of their keys.

Combined with a one time pad protocol, a secure encryption scheme can be realized. Messages are uncrackable due to the nature of one time pad protocols and Bob and Alice always know if their keys have been tampered with due to the nature of QKD.

BB84 Protocol

One of the first conceived QKD protocols, BB84 exploits of conjugate states to achieve QKD [3]. If Alice is in possession of a classical key, (made of 0s and 1s) she transmits it by randomly selecting a polarization basis for each bit (either rectilinear or diagonal) and encoding the bit in a polarized state. (E.g. a 0 corresponding to 0° and 1 to 90° in the rectilinear basis, 0 corresponding to 45° and 1 corresponding to 135° in the diagonal basis). This state is sent along a quantum channel to Bob. Bob measures along a random axis for each particle received, with successful measurements corresponding to a transmitted bit from Alice. When Bob measures along an incorrect axis (E.g. diagonally on a rectilinearly polarized photon) all information is lost. Bob communicates to Alice over a public channel the index of the bits he has successfully measured, with these bits making up the key.

If an attacker has tapped the communication channel, they can only hope to successfully measure and pass along ½ of the photons to Bob. Since Bob only measures ½ of the photons passed to him correctly, he will be in disagreement ¼ the time with Alice. If Alice and Bob share a small percentage of their received photons, they can determine if eavesdropping has occurred based on the number of photons they disagree upon.

Ekert Protocol

The Ekert scheme is another early and important QKD protocol [4]. In the Ekert scheme, Alice and Bob both receive a particle from a source producing singlet states (E.g. spin ½ particles or polarized photons). Alice and Bob each measure the polarization of the incoming photon along one of three independent randomly selected angles azimuthal to the beam. (Alice and Bob each have their own set of angles, Alice being $\mathbf{a}_1$=0, $\mathbf{a}_2$=π/4, $\mathbf{a}_3$=π/2 and Bob's being $\mathbf{b}_1$=π/4, $\mathbf{b}_2$=π/2, $\mathbf{b}_3$=3π/4). A measurement along an axis will either yield a state of +1 or -1. Measurements are broken into two groups, one in which the analyzers are aligned ($\mathbf{a}_2$ and $\mathbf{b}_1$) and one in which they are not. Aligned measurements are anticorrelated, and can be mapped to the bits of the generated key (One party inverts sign). Non aligned measurements must follow the CHSH inequality:

$$S = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3)$$

Where $E(\mathbf{a}_i, \mathbf{b}_j)$ is the correlation coefficient between $\mathbf{a}_i$ and $\mathbf{b}_i$. The correlation coefficient is defined as:

$$E(\mathbf{a}_i \mathbf{b}_j) = P_{++}(\mathbf{a}_i \mathbf{b}_j) + P_{--}(\mathbf{a}_i \mathbf{b}_j) - P_{+-}(\mathbf{a}_i \mathbf{b}_j) - P_{-+}(\mathbf{a}_i \mathbf{b}_j)$$

where $P_{\pm\pm}(\mathbf{a}_i \mathbf{b}_i)$ is the probability of measuring ± 1 along $\mathbf{a}_i$ and ± 1 along $\mathbf{b}_i$. It is required that $S = -2\sqrt{2}$ from Bell's inequality. Bob and Alice publicly share their values of $\mathbf{a}_i$ and $\mathbf{b}_i$ for this set and calculate S. If S differs from the expected value, it is a signature of an attacker making measurements along the communication channel and disrupting the correlations between the two particles.

BB84 vs Ekert Protocols

A natural question is why the BB84 and Ekert protocols are chosen and what are the advantages/disadvantages between the two?

The fact the security of the Ekert protocol comes from the CHSH inequality adds a layer of security that BB84 lacks. It negates the possibility of attacking the system with a beam splitter, a possibility while using the BB84 protocol. In the case of multiple photons emissions from the source, Eve can attack the system through measurement of one emitted photon and the passing on the other.

Implementation of the Ekert protocol at long ranges poses an experimental challenge, as maintaining entanglement over long ranges is a non-trivial task, although it has been established at 1000km via a satellite [5].

Another difference between the two protocols is the amount of bits used for attacker detection. In the Ekert protocol, 2/3rds of all incoming photons are used for detection, while in the BB84 protocol a predetermined amount is set aside for testing. This allows the BB84 protocol to achieve a faster bitrate than the Ekert protocol in certain cases, albeit at the sacrifice of some security.

Implementation of BB84 Protocol

There is a slight variation between the implementation of BB84 presented and the originally conceived protocol. Instead of Alice starting with a randomly generated key and transmitting it to Bob by sending one particle from a conjugate state, Alice and Bob each receive one half of the conjugate state at the same time from a random source. In this implementation, they measure the states by independently and randomly measuring along either 0° or 45°.

Implementation of Ekert Protocol

The experimental implementation of the Ekert Protocol in this paper is slightly different than the originally theorized protocol. It makes use of the Wigner inequality instead of the CHSH inequality, thus reducing the number of measurements needed to make along axis to just angles ψ and χ for Alice and ψ and ω for Bob. Again, the measurements along the same axis (ψ) are perfectly anti-correlated, and are used to generate the key. Wigner's inequality relates the probabilities of both parties measuring $+1$:

$$p_{++}(\chi,\psi) + p_{++}(\psi,\omega) - p_{++}(\chi,\omega) \geq 0$$

For analyzer angles α and β the probability of obtaining $+1$ along both axis is:

$$p_{++}(\alpha,\beta) = \frac{1}{2}\sin^2(\alpha-\beta)$$

This allows the maximization of the Wigner inequality:

$$p_{++}(-30^\circ,0^\circ) + p_{++}(0^\circ,30^\circ) - p_{++}(-30^\circ,30^\circ) = -\frac{1}{8}$$

This inequality is then used to test for violations in correlations and detect an eavesdropper, just like in the traditional Ekert scheme. Using the wigner inequality over the CHSH inequality is advantageous for a number of reasons, one being that there are significantly less required analyzer configurations (4 instead of 6). This simplifies the experimental setup greatly. Additionally less bits are used for equality testing, increasing the bitrate.

Experimental Setup

The pair of entangled photons is generated through parametric down conversion of a laser beam (pump beam). Parametric down conversion is the process in which a photon spontaneously splits into a photon pair [6]. The down conversion is achieved by passing the beam through a nonlinear crystal, in this case β-barium borate (BBO). The experiment uses Type-II parametric down conversion. Type-II describes the polarization of the produced photon pair, in this case the polarization is perpendicular to each other. The wavefunction of the polarized state is as follows:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}[|H_A\rangle|V_B\rangle - |V_A\rangle|H_B\rangle]$$

$|H\rangle$ describes the horizontally polarized state, and $|V\rangle$ describes the vertically polarized state. A and B refers to the photon sent to Alice and Bob respectively. This state is perfectly anticorrelated, any measurement of polarization on photon A will yield the opposite polarization on B. The keys are generated by exploiting the property that the polarization of a generated photon is inherently a random process. The paper assumes and presents $|\Psi^-\rangle$ as a pure state. In reality, pure states are not truly realizable as there will always be interaction with the environment. An interesting followup could be an investigation into how coupled this apparatus is to the outside environment and to what degree an attacker could influence or weaken the generation of random keys.

An important experimental parameter is the nature in which random polarizations are selected to be measured. If the polarizations are not measured along a truly random axis there is potential for an attacker to gain some information about the key. This experiment utilized a novel quantum random number generator [7] to ensure against this form of attack. The generator was developed explicitly for the purpose of this experiment. It is implemented through the passing of a single photon source through a beam splitter with a detector on each side. The side the photon lands is used as an uniform sample from a set of 2 choices.

The implementation of the BB84 protocol uses polarized photons. Many other implementations use phase encoded states to transmit information. Polarized photons provide an advantage as sources produce fewer two pair events (~10^{-3} ratio in the case of this experiment) meaning they are less susceptible to beam splitter attacks [8]. Phase encoded states are more susceptible to beam splitter attacks but provide the advantage of easier implementation over long ranges, due to the it's ease of use in fiber optic networks [9].

Experimental Outcome

For the Ekert scheme, the observed LHS of the wigner inequality of this experiment was -0.112 ± 0.014, with the expected value being $1/8$ or 0.125. The experiment generated roughly a kilobit of a key with a bit error rate of about 3.4, and bitrate of 420 bit/s. The BB84 scheme generated about 80 kilobits of key data at 850 bit/s with an error rate of 2.5%. Using the BB84 scheme, an image was able to be encrypted and sent over a classical channel to be from Alice to Bob, and decrypted again successfully. For both schemes, the bitrates and amount of data sent are far too small to be used in today's day to day computing, but are sufficient for the encryption of simple messages.

Lack of Attacker Simulation

The authors successfully demonstrate an implementation of a QKD system capable of transmitting information between two parties. A relevant follow up not investigated is the effect an attacker has on the system. The paper does not demonstrate that an eavesdropping party does indeed break the CSHS inequality in reference to the

Ekert protocol, or that Alice and Bob will detect an attacker when comparing bits while using the BB84 protocol. While the ability to detect an attacker sits on a airtight theoretical foundation for both protocols, it must be demonstrated if all of the features of a QKD system are to be experimentally verified.

Subsequent Progress and Implementations

Significant progress has been made in subsequent implementations of various QKD schemes after the publication of this paper [10]. A small handful of companies have started to offer commercial QKD systems. QKD has been demonstrated over long ranges between satellites in earth orbit. Bitrates up to 10 MB/s have been demonstrated. Fields have been created entirely around the hacking of quantum networks.

Conclusions

The paper *Quantum Cryptography with Entangled Photons* successfully implements two different schemes of QKD. It also opens up the door for a number of new research opportunities, such as physical investigation into attacks on both BB84 and Ekert schemes. Other possible avenues for research would be various methods of increasing the bitrate and amount of data sent over channels to allow for bigger key sizes. If quantum computers ever allow for efficient computation of the shor algorithm, QKD may be one of our only secure methods of communication. All things considered, the future of research into QKD looks bright.

References

[1] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., & Zeilinger, A. (2000). Quantum Cryptography with Entangled Photons. *Physical Review Letters*, *84*(20), 4729–4732. doi: 10.1103/physrevlett.84.4729

[2] Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography engineering: design principles and practical applications*. Indianapolis, IN: Wiley.

[3] Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. *International Conference on Computers, Systems and Signal Processing*, *1*, 175–179.

[4] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67*(6), 661–663. doi: 10.1103/physrevlett.67.661

[5] Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., … Pan, J.-W. (2017). Satellite-to-Ground Entanglement-Based Quantum Key Distribution. *Physical Review Letters*, *119*(20). doi: 10.1103/physrevlett.119.200501

[6] Couteau, C. (2018). Spontaneous parametric down-conversion. *ArXiv*. Retrieved from https://arxiv.org/abs/1809.00127

[7] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., & Zeilinger, A. (2000). A fast and compact quantum random number generator. *Review of Scientific Instruments*, *71*(4), 1675–1680. doi: 10.1063/1.1150518

[8] Brassard, G., Lütkenhaus, N., Mor, T., & Sanders, B. C. (2000). Limitations on Practical Quantum Cryptography. *Physical Review Letters*, *85*(6), 1330–1333. doi: 10.1103/physrevlett.85.1330

[9] Feifei, G., Zhihui, L., Chengji, L., & Duo, H. (n.d.). A polarization quantum key distribution scheme based on phase matching. Retrieved from https://arxiv.org/pdf/2003.00750.pdf

[10] Advances in Quantum Cryptography. (n.d.). Retrieved from https://arxiv.org/abs/1906.01645