

An Overview of Quantum Key Distribution Protocols and Experimental Implementations

Aileen Zhai

December 4, 2022

Abstract

Quantum key distribution (QKD) is a method of distributing secure keys for encryption and decryption by exploiting properties of quantum states, such as single or entangled photons. QKD protocols are algorithms that allow two parties to generate and securely share secure keys for one-time-pad encryption by being able to detect the presence of an eavesdropper. In this report, we explore several QKD protocols including the BB84 and E91 protocols, as well as the results of several experimental implementations of QKD. In the BB84 protocol, an eavesdropper can be detected by finding a statistically significant number of incorrect qubits that are measured in the same basis as they were sent, thus implying that the photon has been measured in the wrong basis before it was received, or that the photon has been measured and then resent in the wrong basis. In the E91 protocol, an eavesdropper can be detected by finding that measured photons from an entangled pair were not maximally entangled. Then, the remaining qubits form a secure key. QKD has been demonstrated experimentally several times, both on the ground, and with satellites.

1 Introduction

As quantum computing technologies become more developed, the computational ability of computers to crack encryption will improve. As such, there is increased importance in developing secure communications protocols. Quantum key distribution (QKD), is a method of using physical properties of quantum particles, to ensure the security of a key used for one-time-pad encryption or decryption. For single photons, the main property ensuring security of the distributed key is how a photon measured in a basis different from the one it was transmitted in causes the measurement to essentially be random. Thus, if an eavesdropper measures the photon before the intended recipient does, this will cause a detectable error. For entangled quantum states, an eavesdropper measuring one of the photons in the entangled pair will destroy the correlation between the two photons in a very detectable way. Since these protocols can detect when there is an eavesdropper, when no eavesdropper is detected, the two parties can be reasonably sure that their shared key is secure, ensured by the physical properties of quantum states.

However, QKD is not only a theoretical proposal. There have been many demonstrations of several different QKD protocols that were successful in distributing secure quantum keys both on the ground through optical fibers, and in free space by uplinking and downlinking from satellites. These experiments lay the groundwork for a future global network for secure quantum communications.

This paper will first discuss the Bennett-Brassard 1984 (BB84) protocol and the Ekert 1991 (E91) protocol. Then it will give an overview of the results of the Micius satellite experiment performed in 2017 that demonstrated a 1200 km distribution of a secure key using QKD.

2 Quantum Key Distribution Protocols

2.1 The BB84 Protocol

The BB84 QKD protocol is a discrete-variable QKD protocol named for its inventors Charles H. Bennett and Gilles Brassard and the year the paper was published (1984). This is the first QKD protocol to be proposed.

The BB84 algorithm is as follows. Alice sends and records random data qubits (1 or 0), in a random basis (for example, the horizontal-vertical basis, or the diagonal-antidiagonal basis), to Bob. Bob makes measurements of the qubits in a random choice of basis. Once Alice has transmitted a sufficiently long string of qubits, she and Bob communicate over an authenticated classical channel, where Alice shares with Bob the bases in which her qubits were transmitted. Bob then checks which qubits he measured in the wrong basis. These qubits are then discarded, as a qubit measured in the wrong basis is randomly projected on one of the two axes, thus resulting in a 50% probability that the qubit is wrong. Once Alice and Bob have discarded the qubits measured in the wrong basis, Alice then randomly chooses half of the qubits left and communicates her data choices to Bob, who compares against the values he measured. If more than a certain number disagree, then Alice and Bob discard the entire bit string and start the process over. However, if the check passes, then Alice and Bob will use privacy amplification and information reconciliation to create shared keys out of the remaining qubits measured in the correct basis [1,2].

An example of generating a secure key using the BB84 protocol is shown in the table below.

Alice data	0	1	1	1	0	0	1	0
Alice basis	+	X	X	+	X	+	+	X
Polarization	↑	↖	↖	→	↗	↑	→	↗
Bob basis	X	X	+	X	X	+	X	+
Bob measurement	↗	↖	→	↖	↗	↑	↖	↑
Shared key		1		0		1		

Table 1. Example trace of the BB84 protocol using horizontal-vertical and diagonal-antidiagonal bases

If an eavesdropper, Eve, is attempting to access the information, she will intercept the photon as it transmits from Alice to Bob, and make a measurement. However, Eve's basis choice will be wrong 50% of the time, thus causing the state to randomly project and therefore interfere with Bob's measurement. Therefore, the BB84 protocol can be used to check for eavesdroppers because a certain number of qubit data measurements on Bob's side will disagree with what Alice has sent, even if he measured in the correct basis, because Eve has measured in the incorrect basis [1,2].

Since an eavesdropper can be detected, this is a method of distributing a secure key between two parties using one-time-pad encryption.

2.2 The E91 Protocol

Artur Ekert's E91 protocol relies on entangled pairs of photons rather than single photons as in BB84. Entanglement is important in this protocol because entangled states are perfectly correlated, and any eavesdropper making a measurement on the photons destroys these correlations in a detectable way.

The entangled pair can be created either by Alice, Bob, or by a third party. The E91 protocol is as follows. Alice and Bob each make a measurement of the photons they receive in a randomly chosen basis. Alice measures in a basis with a direction randomly chosen between $\{0, \frac{\pi}{8}, \frac{\pi}{4}\}$, while Bob randomly measures from $\{-\frac{\pi}{8}, 0, \frac{\pi}{8}\}$ keeping their respective measurement basis information a secret until the measurements have been completed. Then, Alice and Bob share basis information

and group the qubits into qubits measured in different measurement bases, and the qubits measured in the same basis [3].

The first group, qubits measured in different bases, is then used to calculate the test statistic S which uses correlation coefficients between Alice's bases and Bob's. If the photons are found to be not maximally entangled due to the presence of an eavesdropper making measurements that destroy the correlations of the entangled pair, then Alice and Bob will discard the entire qubit string and start the process over. If Alice and Bob find the photons to be maximally entangled, then the second group of qubits that were measured in the same basis, form the secure key [3].

This is another method of distributing a secure key between two parties using one-time-pad encryption.

3 Demonstrations of Quantum Key Distribution

QKD has been implemented both on the ground through optical fiber, and through satellite-to-ground links.

One of the recent most compelling demonstrations of practical QKD occurred in 2020, when physicists at the University of Science and Technology of China reported on the results of using the satellite Micius as a relay to distribute secure keys between China and Austria. A picture of the philosopher Micius was transmitted from Beijing to Vienna, and a picture of Schrodinger was transmitted from Vienna to Beijing. These images were encrypted and decrypted using a secure quantum key generated using the BB84 protocol with very few errors done over 1120 km [4].

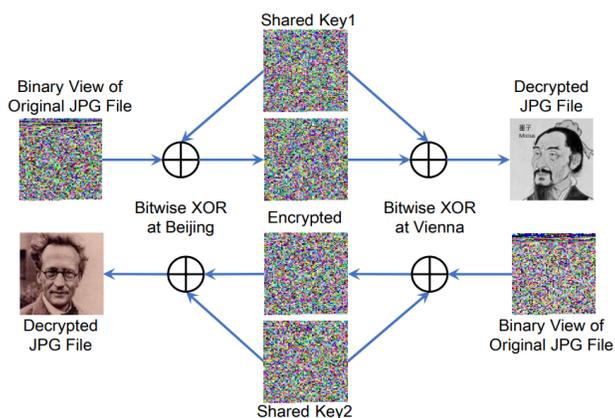


Figure 1: Encrypted and decrypted images using a secure quantum key sent via the Micius satellite between Beijing and Vienna [4, 5].

In 2018, the same group reported on the results of using the Micius satellite to perform entanglement-based QKD over 1120 km. This was done by downlinking photons from an entangled pair created on the Micius satellite to two ground stations. The experiment increased the ground distance of secure quantum communications by a factor of ten [4, 5].

4 Conclusions

QKD protocols are designed with the goal of securely distributing a key by transmitting qubits between two parties such that the presence of an eavesdropper can be detected. The BB84 protocol does so by detecting errors in the shared key that would not exist without the existence of an

eavesdropper. The E91 protocol can find an eavesdropper by exploiting properties of entangled photons. By developing these protocols, it is possible to generate keys for one-time-pad encryption that are ensured to be secure by physical properties of the qubits.

The successful implementations of QKD show that it is a promising quantum technology that can improve secure communication by exploiting quantum mechanical properties of photons in a way that is actually applicable in the real world. Additionally, these demonstrations lay the groundwork for a future global quantum network, a few continents at a time.

5 References

[1] C.H. Bennett, G. Brassard. *Public key distribution and coin tossing*. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (1984).

[2] C.H. Bennet, F. Bessette, et al. *Experimental quantum cryptography*. J. Cryptology 5, 3-28 (1992).

[3] A.K. Ekert. *Quantum cryptography based on Bell's theorem*. Phys. Rev. Lett. 67, 661 (1991).

[4] J. Yin, Y-H. Li, et al. *Entanglement-based secure quantum cryptography over 1120 kilometres*. Nature 582, 501–505 (2020).

[5] S-K. Liao, W-Q. Cai, et al. *Satellite-relayed intercontinental quantum network*. Phys. Rev. Lett. 120, 030501 (2018).