Review of Quantum Key Distribution

Hyunjo Kim

February 2023

Abstract

In this short review paper, I will be looking into Quantum Key Distribution (QKD) in detail. With short introductions to basic ideas of qubits, quantum gates, and quantum teleportation, we explore the inner workings of QKD protocols, such as the BB84 Protocol, BBM92 Protocol, and E91 Protocol.

1 Introduction

Quantum Cryptography is an important concept within quantum computing. Not only does it offer a novel way to view encryption, it requires us to re-design our security measures. QKD offers solutions to create private keys in a post-quantum world, using properties of quantum mechanics. As IBM introduces their new 433-qubit processors, there are both increasing benefits and concerns as quantum hardware progresses.

2 Quantum Bits, Gates, and Important Results

2.1 Qubits

As a reader of this paper, you may already be aware of the formulation of a qubit. It is generally written in the form of:

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

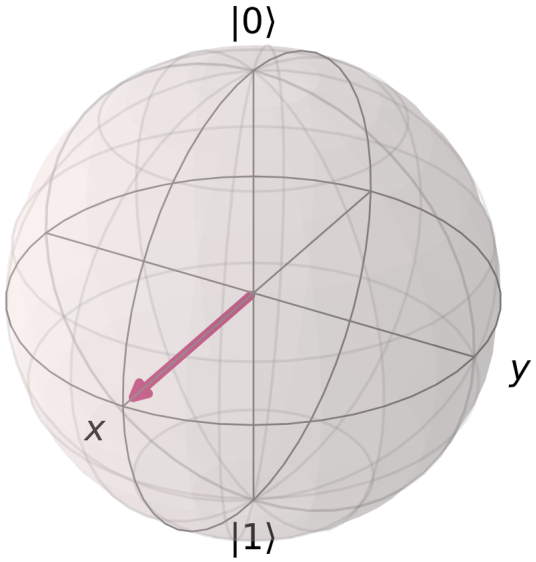
Now, $|0\rangle$ and $|1\rangle$ are the computational basis states, which we will use most frequently in quantum computing and quantum cryptography. The quantum bit is an abstract mathematical framework through which we view quantum information and manipulate it. This is quite an abstract concept, but this allows us to make higher-level calculations without necessarily relying on physical equipment.

There are also multi-qubit cases, where we may have N qubits. This means we have a Hilbert space of 2^n. This is just a case of permutations, if we have two qubits, we have the following computational basis states:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

2.1.1 Visualizing Qubits

We can also visualize (normalized) qubits using something called a bloch



sphere [1]:

Given that a quantum state can be described as such:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers known as the probability amplitudes, following this: $|\alpha|^2 + |\beta|^2 = 1$. Hence, in exponential form, it can be written as:

$$|\psi\rangle = r_\alpha e^{i\phi_\alpha} |0\rangle + r_\beta e^{i\phi_\beta} |1\rangle$$
$$e^{-i\phi_\alpha} |\psi\rangle = r_\alpha |0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)} |1\rangle$$

But the phase on state $|psi\rangle$ has no observable effects. And using the fact this is normalized, we can rewrite it as such:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right) e^{i\phi}$$

It may seem weird to have $\frac{\theta}{2}$, but this is just entirely dependent on our definitions for the interval. There are, in fact, infinitely many points on the bloch sphere, and we can plot such qubit states on this. However, after measurement, it will collapse into some state according to the measurement basis.

2.2 Quantum Gates

2.2.1 Hadamard Gate

Just like in classical computing, when we try to manipulate our information, we use logic gates. In our case, the quantum gates can be defined as unitary transformations, meaning that they follow the condition that $U^\dagger U = I$. An important example is the Hadamard Gate, where it essentially transforms states into superpositions:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

For example, when a Hadamard Gate acts on $|0\rangle$, we have the following:

$$H |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

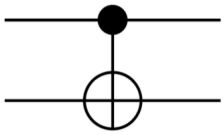
In fact, there are infinitely many two by two unitary matrices, hence infinitely many single qubit gates. This is just a general introduction to quantum bits and gates, but we can see how we can start applying them in the latter sections.

2.2.2 CNOT Gate

Let's have a look at the important CNOT gate - the quantum version of the traditional XOR Logic Gate.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

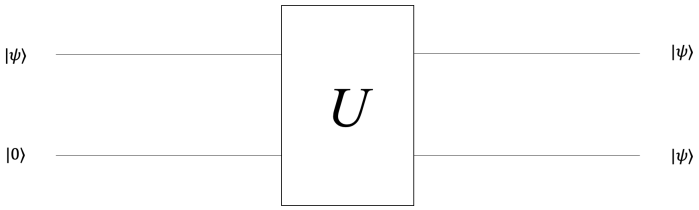
which looks like this in quantum circuit representation:



The Controlled NOT gate, is a two qubit gate, which has a control qubit and a target qubit. If the control qubit state is $|1\rangle$, the target qubit state will be flipped from $|1\rangle$ to $|0\rangle$ and vice versa. If the control qubit is $|0\rangle$, the target qubit state will not undergo any change.

2.3 No-cloning Theorem

This is an important result in quantum cryptography. Unfortunately, cloning of an unknown arbitrary quantum state is impossible. To prove the no cloning theorem, let's assume there is some unitary transformation that can clone states. The figure below demonstrates what it might look like on an arbitrary state ψ. [2]



If we consider two quantum states, $|\psi\rangle$ and $|\phi\rangle$, such that we want to copy our first state, $|\psi\rangle$ onto the second slot which starts off with $|\phi\rangle$, hence the initial state is:

$$|\psi\rangle \otimes |\phi\rangle$$

If there is some unitary evolution for cloning for any two arbitrary states:

$$\mathbf{U}(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$\mathbf{U}(|\alpha\rangle \otimes |\phi\rangle) = |\alpha\rangle \otimes |\alpha\rangle$$

After taking innerproducts of the two equations (NB $U^{\dagger}U = 1$):

$$\langle\psi|\alpha\rangle = (\langle\psi|\alpha\rangle)^2$$

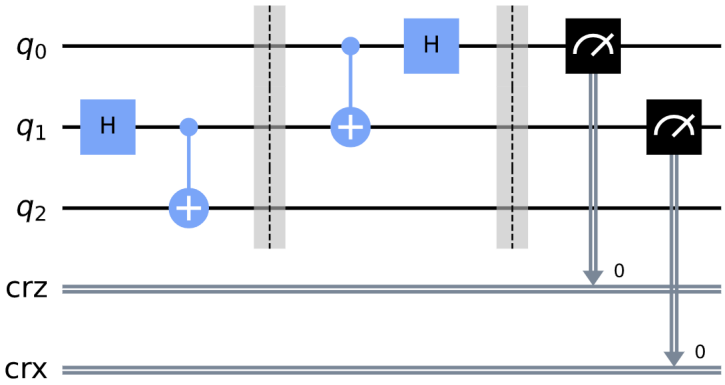
Which means either the two states must be identical or orthogonal. Hence, there does not exist a unitary evolution that clones arbitrary states.

3 Is Quantum Computing the end of cryptography?

When the idea of a quantum computer emerged in the early 1980s - proposed by physicists such as Feynman - it was imagined that computations and simulations would speed up. For example, Grover's algorithm and Shor's algorithm shows clear speeds up compared to classical algorithms. The currently widely used RSA cryptosystem can theoretically be broken between tens of seconds to months, whereas current classical methods will take billions of years to crack.

4 Quantum Teleportation

Quantum teleportation is a neat protocol to transfer quantum information remotely without the aid of a quantum communications channel. This process involves three qubits: $|\psi\rangle$, which is Alice's quantum state, $|\beta\rangle_A$, which is one of the entangled particles, and $|\beta\rangle_B$, which is other half of the entangled pair that is currently in Bob's possession. So, without measuring the quantum state, how can Alice send $|\psi\rangle$ to Bob?



Now, what does this quantum circuit actually do? So if we look at our initial state, where Alice's EPR state is $|\beta_0 0\rangle$ (after our first barrier):

$$|\psi_{initial}\rangle |\beta_A\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)]$$

With two qubits in her possession, Alice sends them through a CNOT Gate, through which she gets the following state:

$$\frac{1}{\sqrt{2}}[\alpha |0\rangle (|00\rangle + |11\rangle + \beta |1\rangle (|10\rangle + |01\rangle)]$$

which you can verify using matrix multiplication. And after the Hadamard Gate, our state can be simplified to this:

$$\frac{1}{2}[|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)]$$

After performing a measurement, Alice can get four possible results: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Hence Bob's corresponding measurememnts are:

$$|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle$$
$$|\psi_2\rangle = \alpha |1\rangle + \beta |0\rangle$$
$$|\psi_3\rangle = \alpha |0\rangle - \beta |1\rangle$$
$$|\psi_4\rangle = \alpha |1\rangle - \beta |0\rangle$$

Now based on Alice's measurement (she can encode her results using two classical bits), he should apply these quantum logic gates:

$$\begin{aligned} 00 &\longrightarrow I \\ 01 &\longrightarrow X \\ 10 &\longrightarrow Z \\ 11 &\longrightarrow Y \end{aligned}$$

And after using these logic gates, Bob should get Alice's state which she wanted to teleport.

5 Quantum Key Distribution

5.1 BB84 Protocol

One of the oldest protocols was demonstrated by Brassard and Bennett in 1984 [3]. We must establish necessary conditions for it to work. They share a secure quantum channel, a classical communication channel without losses and errors, and they have trusted devices. Let's say we have two friends, Alice and Bob, who wish to find a secure key through this protocol. Alice begins by choosing a random bit using a random generator: 10100. She then chooses a random basis, either in x or z, and thus encodes the bit and sends it through the quantum channel. So, if her bases were as follows, B_x, B_z, B_z, B_x, B_x, the qubits she sends are:

$$|-\rangle, |0\rangle, |1\rangle, |+\rangle, |+\rangle$$

Now, Bob also chooses a random basis to measure the qubit in: B_z, B_z, B_x, B_z, B_x. When the bases are the same, Alice and Bob will share the same classical bit. When they are not, the measurement will give either outcome with a probability of 1/2, hence it is important that they repeat this process of encoding and decoding a reasonable amount of times. After, they can decide which bases to discard.

To summarise the steps:

- Alice chooses a random bit and a random basis
- Alice encodes the bit with the chosen basis and sends a qubit to Bob

- Bob chooses a random basis
- Bob measures the received qubit in chosen basis and decodes the bit
- Alice and Bob repeat these steps, then they share the bases used in a public channel
- They discard the bases which are not the same and agree on a key without revealing the value of the bits

But, how does it protect against possible eavesdroppers? First, in order to test whether there even is an eavesdropper, Alice and Bob will share some bases and then Alice will send the classical bits. Eve, our eavesdropper, measures in a random basis and re-encodes the bit according to her measurement. For example, if Alice's bit was 1 and encoded it in the x basis, her qubit would be $|-\rangle$. If Eve's measurement basis was in the z basis, her measurement could either encode it through $|0\rangle$ or $|1\rangle$. If Bob's measurement was in the x basis, B's qubit can either be $|+\rangle$ or $|-\rangle$, but if Bob's corresponding measurement led to bit 0, despite them knowing they have the same basis, they will know that there was an eavesdropper that changed the original qubit. This leads us to another question: how many bits does Alice and Bob have to send to ensure that there is no eavesdropper?

Let's try to find the probability of not finding Eve. For Eve, she has a $\frac{1}{2}$ chance of getting the right basis. And even if she does get it wrong, she has a $\frac{1}{2}$ chance of not being detected, given that Alice and Bob have the same basis, which also has a $\frac{1}{2}$ chance. Hence the probability of not being detected after k bits is:

$$p = \left(\frac{1}{2} + \frac{1}{2} \times \frac{1}{2}\right)^k = \left(\frac{3}{4}\right)^k$$

For Alice and Bob, the probability of detecting her is:

$$p = 1 - \left(\frac{3}{4}\right)^k$$

You may notice that as k gets large, the probability of detecting Eve converges. This is crucial as it demonstrates how secure the BB84 Protocol is in detecting possible eavesdroppers.

5.2 BBM92 Protocol

The BBM92 Protocol is conceptually very similar to the BB84 Protocol, but this time we use an EPR pair. An EPR Pair is created and sent to Alice and Bob:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

They then measure in a random basis without telling each other. Alice and Bob share the bases that they used over a classical channel and discards any measurements where they used different bases. Because of the entangled pairs, if they share the same basis, Alice and Bob should always have the same measurement outcome. Hence, after the protocol, they should have the same key. One of the advantages of the BBM92 Protocol is that Alice and Bob can decide to complete a measurement just before the key is used so that the information is secured within this quantum state.

5.3 E91 Protocol

5.3.1 Bell's Inequality

Bell's inequality is a key concept in the E91 Protocol. Hence, I will explore it before delving into the specifics of the Ekert91 Protocol. Bell's inequality demonstrated the clear difference between classical and quantum physics. [2]

Let's say we send one particle each to Alice and Bob. They both are able to perform two types of measurements on this particle: Q or R for Alice and S or T for Bob. Each of the measurements can only give out either +1 or -1. And for the sake of argument, they perform this measurement at the same time so that there can be no physical influences affecting the outcome of the measurement.

Now, there are two reasonable assumptions we can make with regards to this experiment:

- Local Determinism: Alice's measurement should not be affected by Bob's. It only depends on the locally determined physical state that Alice receives.

- Objective Reality: The result of the measurement is not probabilistic, meaning that the value is already encoded in the particle's internal state.

We will consider this quantity (which proves to have a meaningful result):

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T$$

Because the values they are allowed is either +1 or -1, it is easy to see that $(Q + R)S = 0$ or $(R - Q)T = 0$ In either of these cases, our starting quantity will be +2 or -2. Now, let's consider a probabilistic model, where:

$$P = p, Q = q, R = r, S = s$$

where the lower cases represent the probability distribution corresponding to the measurement performed. Hence, if we consider the expectation value of the quantity, we can find an inequality:

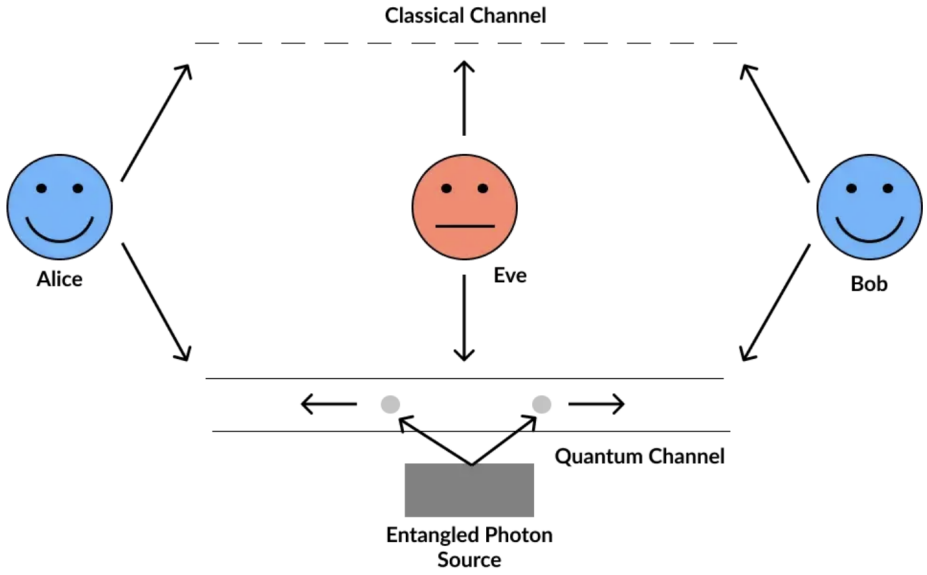
$$\mathbf{E}(QS + RS + RT - QT) = \sum_{qrst} p(q, r, s, t)(qs + rs + rt - qt)$$

where $p(q, r, s, t)$ represents some joint probability distribution. But, because the average value of this quantity will always be less than two, we can separate the summation and write it like this:

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2$$

Now, this is the classical picture. The nature of quantum mechanics violates the above inequality, and this is what we use in the Ekert91 Protocol.

5.3.2 The Protocol



[4]

The protocol [5] uses Bell inequality to detect a possibe eavesdropper. After receiving an EPR pair, Alice and Bob both measure in a certain basis: $\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}$ and $\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}$.

If they happen to choose the same orientations/basis, they will end up with the same measurement outcome. After quantum communication, Alice and Bob separates the bases they used into two groups after sharing. The first group is where Alice and Bob used different bases, and the second group is where they used the same bases.

Now, we can assign Alice and Bob such observables:

$$\mathbf{A} = (+1)\,|a\rangle\,\langle a| + (-1)\,|a^{\perp}\rangle\,\langle a^{\perp}|$$
$$\mathbf{B} = (+1)\,|b\rangle\,\langle b| + (-1)\,|b^{\perp}\rangle\,\langle b^{\perp}|$$

where a and b can be one of the bases as mentioned before.

Now, to check for an eavesdropper, they use the instances when they have these bases:

$$(\mathbf{a_3}, \mathbf{b_3}), (\mathbf{a_3}, \mathbf{b_1}), (\mathbf{a_1}, \mathbf{b_1}), (\mathbf{a_1}, \mathbf{b_3})$$

Which are the same arguments used for the CHSH Bell Inequality we looked in the section before. The reason Ekert added another basis was because he wanted to detect the presence of an eavesdropper without openly exposing his key. Before showing how this relates to the Bell Inequality, we will use the correlation coefficients as follows:

$$E(\mathbf{a_i}, \mathbf{b_j}) = P_{11}(a_i, b_j) + P_{00}(a_i, b_j) - P_{10}(a_i, b_j) - P_{10}(a_i, b_j)$$

Which allows us to create a sum with such correlation coefficients, directly leading us to the Bell Inequality.

$$S = E(a_1, b_1) + E(a_3, b_1) + E(a_3, b_3) - E(a_1, b_3) \leq 2$$

If there is no eavesdropper, we should have $S = 2\sqrt{2}$, but if there is an eavesdropper, the system behaves classically so that $S \leq \sqrt{2}$

References

[1] The Qiskit Team. Learn quantum computation using qiskit, Nov 2022.

[2] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[3] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, dec 2014.

[4] IIT Roorkee Quantum Computing Group. Fundamentals of quantum key distribution-bb84, b92 amp; e91 protocols, Sep 2021.

[5] Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67 6:661–663, 1991.