Chapter 1

Quantum cryptography

Quantum cryptography offers a secure communication between two parties against eavesdroppers with unlimited computing power. It is based on physical laws and does not rely upon any complexity assumptions. This chapter presents some mathematical foundation for the study of quantum cryptography which will be of great help to understand how the first quantum cryptography named BB84 works. Before going into details, we shall first introduce the postulates of quantum physics.

1.1 The postulates of Quantum physics

In this section we review the most important postulates of quantum physics.

1. **The state of a system:**
   Quantum state is mathematical object which behaves like vector. It is represented in [Dirac notation](https://en.wikipedia.org/wiki/Dirac_notation) by ket vector $|\psi\rangle$. A vector space $V$ is a nonempty set with elements called vectors for which the two operations, addition and scalar multiplication are defined. One particular vector space that is very important in our chapter is the complex vector space $\mathbb{C}^2$.

2. **Observable quantities representation:**
   To every dynamical variable that is physically measurable is represented by a Hermitian Operator.

3. **Measurement:**
   The possible results of measurement of a dynamical variable $A$ are the eigenvalues of $A$. After the measurement the state of the system immediately collapses to the eigenvector (state) of the obtained eigenvalue. The measurement in quantum physics is irreversible.
4 Time evolution of a System:
The time evolution of a closed system is governed by the Schrödinger equation.

1.2 No-cloning theorem

Perfect cloning is possible in classical physics. However, in quantum physics we cannot perfectly clone an unknown state. This fact is called the no-cloning theorem. We can proof it by contradiction. Let assume that we have a quantum device which can clone an arbitrary state $|\psi\rangle$ perfectly. This device would do the following action upon the state and some arbitrary blank state $|b\rangle$

$$|\psi\rangle|b\rangle|Q_i\rangle \longrightarrow |\psi\rangle|\psi\rangle|Q_f\rangle,$$

where $|Q_i\rangle$ is the initial state of the quantum device and $|Q_f\rangle$ its final state. This device would copy any state. For example, it copies the states $|0\rangle$ and $|1\rangle$

$$|0\rangle|b\rangle|Q_{00}\rangle \longrightarrow |0\rangle|0\rangle|Q_{00}\rangle,$$
$$|1\rangle|b\rangle|Q_{11}\rangle \longrightarrow |1\rangle|1\rangle|Q_{11}\rangle,$$

as well as their superposition $\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$

$$\left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right)|b\rangle|Q_{i+}\rangle \longrightarrow \left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right)\left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right)|Q_{f+}\rangle.$$

Since our device should act as a linear operator, so, we have

$$\left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right)|b\rangle|Q_{i+}\rangle = \frac{1}{\sqrt{2}}|0\rangle|b\rangle|Q_{i+}\rangle + \frac{1}{\sqrt{2}}|1\rangle|b\rangle|Q_{i+}\rangle,$$
$$\longrightarrow \frac{1}{\sqrt{2}}|0\rangle|0\rangle|Q_{f+}\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle|Q_{f+}\rangle,$$
$$\neq \left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right)\left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right)|Q_{f+}\rangle.$$

This contradiction implies that there is no quantum device which can clone any state. Of course, if we know a state, we can make as many copies as we like.

1.3 Qubit

In classical information, the bit is the basic unit of information processing. It takes one of the two states that are labeled 0 and 1. Accurate measurement
and perfect cloning are possible for classical bit. Whereas, in quantum information, quantum bit (qubit) is the basic unit information processing. According to the no-clone theorem, unknown arbitrary qubit cannot be cloned perfectly.

The state of the qubit is represented in Dirac notation by a vector called ket $|\psi\rangle$. Qubit can also be in a superposition state

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

where, $\alpha$ and $\beta$ are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$. The ket vectors $|0\rangle$ and $|1\rangle$ are the computational bases states. They are represented by column vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$  

The following definitions are important to understand quantum cryptography protocols

1. A state $|\psi\rangle$ is normalized if the inner product is one, $\langle\psi|\psi\rangle = 1$.
2. We say that two qubits are orthogonal if their inner product is zero, $\langle\psi_1|\psi_2\rangle = 0$.
3. A projector operator $\hat{P}$ that projects a state on a normalized state $|\psi\rangle$ can be written as $|\psi\rangle\langle\psi|$.

One can show that the two states $|0\rangle$ and $|1\rangle$ form an orthonormal bases

$$\langle0|0\rangle = \langle1|1\rangle = 1,$$  
$$\langle0|1\rangle = \langle1|0\rangle = 0.$$  

The sum of the two probabilities should be one, i.e., $|\alpha|^2 + |\beta|^2 = 1$. The physical meaning of the coefficients $\alpha$ and $\beta$ are as follows.

The probability of finding the qubit $|\psi\rangle$ in the state $|0\rangle$ is given by the magnitude of the inner product $|\langle\psi|0\rangle|^2$. Similarly, The probability of finding the qubit $|\psi\rangle$ in the state $|1\rangle$ is $|\langle\psi|1\rangle|^2$. Thus,

$$|\langle\psi|0\rangle|^2 = |\alpha|^2 : \text{ the probability of finding } |\psi\rangle \text{ in state } |0\rangle,$$
$$|\langle\psi|1\rangle|^2 = |\beta|^2 : \text{ the probability of finding } |\psi\rangle \text{ in state } |1\rangle.$$  

Since $\alpha$ and $\beta$ are complex numbers, we can use the polar representation of a complex number to write the state of an arbitrary qubit as

$$|\psi\rangle = e^{i\xi}(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle). \quad (1.1)$$
The parameter $\xi$ is a global phase and has no physical meaning. Thus, the state is uniquely determined by the two parameters $\phi$ and $\theta$ with, $0 < \theta < \pi$ and $0 < \phi < 2\pi$. This representation corresponds to a point on the unit three-dimensional sphere (see fig.1.1). This unit sphere is called **Block sphere**. Therefore, any point on the sphere corresponds to a unique state of the qubit. For example, the north pole corresponds to the state $|0\rangle$, while, the south pole corresponds to the state $|1\rangle$. Qubit can be implemented physically as Electron (spin values $\pm 1/2$). or photon (polarizations, $\uparrow$ or $\downarrow$).

![Bloch sphere diagram](image.png)

**Figure 1.1**: Representation of a qubit in the Bloch sphere. Any state $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$, corresponds to a point in the sphere with the angles $\theta$ and $\phi$.

### 1.4 Quantum banknotes

The fundamental concepts of quantum cryptography started in the early 1970, when Stephen Wiesner came up with a beautiful idea, quantum banknotes. A quantum banknote has a unique serial number and a sequence of isolated **qubits**. A qubit can be represented by photon in one of the four polarizations, rectilinear $0^\circ$, $90^\circ$ or diagonal $45^\circ$, $135^\circ$. The bank randomly and independently chooses one of the four polarizations for each qubit and keeps it secret. Thus, the record of any banknote consists of one public number (the serial number) and one secret key known to the bank only (the random sequence of polarizations). A counterfeiting who doesn’t know the polarization basis has no way of counterfeiting a banknote. This is due to the **no-cloning theorem**. In other word, A measurement on a qubit of unknown state will introduce disturbance and changes its state. Consider these events:
Figure 1.2: The banknote with \( N \) qubits passes the test with probability equals to \( \left( \frac{3}{4} \right)^N \).

- \( C_f \) : the counterfeiting choose the correct basis
- \( W_f \) : the counterfeiting choose the wrong basis
- \( C_b \) : the bank obtains the correct polarization
- \( W_b \) : the bank obtains the wrong polarization

The probability for a counterfeiting to choose the correct or wrong basis is given by

\[
P(C_f) = P(W_f) = \frac{1}{2}.
\]

If the counterfeiting chooses the correct basis, then the bank and the counterfeiting share the same basis. This means

\[
P(C_b|C_f) = 1.
\]

If the counterfeiting chooses the wrong basis, the conditional probability is then given by

\[
P(C_b|W_f) = \frac{1}{2}.
\]

Now, we can calculate the probability that the bank obtains the same polarization as in the record (see Fig. 1.2). It is given by

\[
P(C_b) = P(C_b \cap C_f) + p(C_b \cap W_f),
\]

\[
= P(C_b|C_f) P(C_f) + p(C_b|W_f) P(W_f),
\]

\[
= \frac{3}{4}.
\]

If the banknote contains \( N \gg 1 \) qubits, the probability that the banknote passes the test is exponentially small, i.e., \( \lim_{N \to \infty} \left( \frac{3}{4} \right)^N \to 0 \).

Now, we are ready to explore the first quantum protocol named BB84.
1.5 The BB84 protocol

In quantum cryptography, we usually encounter three names, Alice, Bob, and Eve. Alice wishes to send Bob a confidential message and Eve is trying to steal this message without disclosing her presence. She is an eavesdropper. The first quantum cryptography was discovered by Bennett and Brassard in 1984. It is called BB84 protocol. It works as follows.

- Alice and Bob agree on the following code.

<table>
<thead>
<tr>
<th>Basis</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>rectilinear</td>
<td>↔</td>
<td>↔</td>
</tr>
<tr>
<td>diagonal</td>
<td>↓</td>
<td>↔</td>
</tr>
</tbody>
</table>

- Alice prepares a sequence of random qubits from the following four states \( \{\uparrow, \leftrightarrow, \downarrow, \swarrow\} \) and sends them to Bob one by one. She has to record the encoded sequence and keep it secret.

- Bob measures the received qubits using random choice of rectilinear or diagonal bases. He has to keep his results of measurement secret.

- Bob publicly informs Alice about his choice of measurement bases without disclosing his results.

- Alice keeps only the bits where both have chosen the same basis and tells Bob publicly what bits he has to discard. After this stage Alice and Bob share a set of a sifted data bits.

- In realistic experiment, this sifted data is not the same for both parties. To check for errors rate, Bob sends to Alice over a public channel few random selected bits from the sifted data. Alice checks for errors.

- If the errors rate is low, they can perform classical privacy amplification on the remaining bits to distill a secure shared key.

- If the errors rate is high, this indicates that an eavesdropper is trying to intercept their communication. Quantum cryptography doesn’t not prevent eavesdropping, but it does provide a way for detecting any sort of attack.

If there is no Eve, the sifted data will be the same for both parties as shown in Table. 1.1. If Eve is intercepting the communication, then she introduces errors in the sifted data which can be discovered by Alice when she compares the selected data sent by Bob against her own (see Table.1.2). To understand how the protocol works, we can calculate the inner product of the state sent
by Alice and the basis used by Bob to measure the polarization of the received qubit. Assume that there is no body intercepting the communication between Alice and Bob. If Alice, for example, sends the state \(| \leftrightarrow \rangle\) to Bob who uses the rectilinear basis to measure the polarization of the photon, he gets \(| \leftrightarrow \rangle\) with probability one

\[
|\langle \leftrightarrow | \leftrightarrow \rangle|^2 = 1.
\]

However, if he uses diagonal basis, he will get either \(| \uparrow \rangle\) or \(| \downarrow \rangle\) with probability 0.5 each. This is due to the fact that

\[
|\langle \uparrow | \leftrightarrow \rangle|^2 = |\langle \downarrow | \leftrightarrow \rangle|^2 = \frac{1}{2}.
\]

This is why Alice and Bob should discard this bit. We note here that the diagonal basis consists of two bases

\[
| \uparrow \rangle = \frac{1}{\sqrt{2}} (| \uparrow \rangle + | \leftrightarrow \rangle),
\]

\[
| \downarrow \rangle = \frac{1}{\sqrt{2}} (| \downarrow \rangle - | \leftrightarrow \rangle).
\]
In other hand, if Eve is intercepting the communication, she doesn’t know which basis she has to use to measure the qubit. If she uses the rectilinear basis, the state is not perturbed. However, if she uses diagonal basis, the state is perturbed, i.e., Bob will receive either $\nearrow$ or $\nwarrow$. Then, an error may occur in the Bob side since he uses rectilinear basis as Alice does.

Before we end our chapter, we shall briefly review other quantum cryptography protocols.

- In 1992 Bennett came up with a protocol (B92) that uses only two non-orthogonal basis rather than four. It is a simplification of BB84.

- In 1991 Artur Ekert proposed a protocol which relies on quantum entanglement and Bell’s inequality.

- All these protocols we have discussed so far, are based on discrete variables, i.e., the output of the measurement is always discrete. They rely on single photon schemes. Due to the difficulty of implementation, a continuous variables quantum cryptography was introduced in 1999 as an alternative approach where the output of the measurement can be continuous.

**Reference**

