Quantum Cryptography: Numerical Example

**Simplified case.** Let us consider the simplified case, when \( n = 4 \), and when we do not check for eavesdroppers.

**Sending preliminary signals – general case: reminder.** Let us assume that Alice wants to send a preliminary signal consisting of \( n \) bits. For each \( i = 1, 2, \ldots, n \), Alice selects two random bits \( b_i \) and \( r_i \). Then:

- if \( r_i = 0 \) and \( b_i = 0 \), she sends the signal \( |0\rangle \);
- if \( r_i = 0 \) and \( b_i = 1 \), she sends the signal \( |1\rangle \);
- if \( r_i = 1 \) and \( b_i = 0 \), she sends the signal \( |0'\rangle \); 
  \[ |0'\rangle \equiv \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle; \]
- if \( r_i = 1 \) and \( b_i = 1 \), she sends the signal \( |1'\rangle \); 
  \[ |1'\rangle \equiv \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle. \]

Here:

- signals \( |0\rangle \) and \( |1\rangle \) corresponding to \( r_i = 0 \) are called the + orientation; and
- signals \( |0'\rangle \) and \( |1'\rangle \) corresponding to \( r_i = 1 \) are called the \( \times \) orientation;

**Alice sends the preliminary signals: our case.** First, Alice uses the random number generator to generate 4 random bits \( b_i \) that will be sent to Bob. Let us take

\[
\begin{align*}
b_1 &= 0, & b_2 &= 1, & b_3 &= 0, & b_4 &= 1.
\end{align*}
\]

Then, Alice gets 4 random bits to select orientations \( r_i \). Let us take

\[
\begin{align*}
r_1 &= 1, & r_2 &= 0, & r_3 &= 1, & r_4 &= 1.
\end{align*}
\]

According to the algorithm, Alice sends the following 4 signals to Bob:

\[
|0', \ 1, \ 0', \ 1'\rangle.
\]
Receiving signals – general case: reminder. We can measure the signal in the + orientation or in the \( \times \) orientation. If the signal was sent and received in the same orientation, the measurement result \( b'_i \) coincides with the original signal \( b_i \). Examples:

- if we sent \( |0\rangle \) and we measure it in the + orientation, we get 0;
- if we send \( |1'\rangle \) and we measure it in the \( \times \) orientation, we get 1.

If the signal was sent in one orientation and is measured in another orientation, then, instead of the original signal, we get 0 or 1 with equal probability, i.e., the original signal is lost.

In the preliminary stage of the quantum cryptography scheme, Bob selects \( n \) random bits \( s_1, \ldots, s_n \). Then:

- if \( s_i = 0 \), he measures the received signal in the + orientation, and
- if \( s_i = 1 \), he measures the received signal in the \( \times \) orientation.

Bob receives preliminary signals: our example. To receive the signals, Bob takes 4 random bits \( s_i \) as orientations:

\[
\begin{align*}
s_1 &= 0, \\
s_2 &= 0, \\
s_3 &= 1, \\
s_4 &= 1.
\end{align*}
\]

This means that he measures the 4 signals that he received from Alice in the following 4 bases:

\( +, +, \times, \times \).

After the measurement, he gets the following results:

\[
?, 1, 0, 1.
\]

Here, ? means that he can get 0 or 1 with equal probability \( 1/2 \).

Alice and Bob exchange orientations – general case: reminder. Alice and Bob send, to each other, their orientations \( r_i \) and \( s_i \), by an open channel. If \( r_i = s_i \), then the sending and receiving orientations coincide, so the bit \( b_i \) sent by Alice is equal to the value \( b'_i \) measured by Bob. For these values \( i \), Bob and Alice have common secret bits \( b_i \) that they know but no one else knows. These bits will be used to send the actual signal.

Alice and Bob exchange orientations: our example. After this exchange, Alice and Bob realize that \( r_i = s_i \) for

\[
i = 2, \quad i = 3, \quad i = 4.
\]

For these values \( i \), they have common bits

\[
b_2 = 1, \quad b_3 = 0, \quad b_4 = 1
\]
that they both know and no one else knows. They can use these three bits to send a 3-bit message.

**Alice encrypts and sends a message.** Alice want to send a message 110, with

\[ m_2 = 1, \quad m_3 = 1, \quad m_4 = 0. \]

Alice encrypts this message with the commonly known bits, producing:

\[ m'_2 = m_2 \oplus b_2 = 1 \oplus 1 = 0, \]
\[ m'_3 = m_3 \oplus b_3 = 1 \oplus 0 = 1, \]
\[ m'_4 = m_4 \oplus b_4 = 0 \oplus 1 = 1. \]

**Bob receives and decrypts the message.** Upon receiving the message \( m'_i \), Bob decrypts is as follows:

\[ m_2 = m'_2 \oplus b_2 = 0 \oplus 1 = 1, \]
\[ m_3 = m'_3 \oplus b_3 = 1 \oplus 0 = 1, \]
\[ m_4 = m'_4 \oplus b_4 = 0 \oplus 1 = 0. \]