Quantum Key Distribution

Emmanuele Lotano - ID number: 918608
Course of Cybersecurity for Data Science - Professor C. Ferretti
Università degli Studi di Milano-Bicocca, CdLM Data Science

February 28, 2025

1 Why quantum cryptography?

Currently, the state-of-the-art in cryptography is asymmetric public/private key cryptography (such as RSA), which is based on the difficulty of a chosen mathematical problem. Although these problems are hard to solve, they are not impossible, and therefore the private key is potentially vulnerable. In particular, future development in hardware and software, such as algorithms ran on quantum computers, could provide a solution to the prime factorization problem, which is a cornerstone in many asymmetric cryptographic protocols, in polynomial time.

However, quantum mechanics not only introduces a vulnerability but also offers a potential solution to the problem. The solution is to use symmetric cryptographic protocols, such as the XOR cipher, coupled with a quantum-mechanical method to create a shared symmetric key, without worrying about possible eavesdroppers.

The XOR protocol works as follows:

1. The plaintext is written as a binary sequence.
2. The key is a random binary sequence of the same length as the plaintext.
3. The ciphertext is obtained by taking the bitwise XOR (addition modulo 2) of the plaintext and the key.

Let us consider a simple example:

001010011 plaintext,
100111010 secret key
101101001 ciphertext.

If the key is kept secret, the XOR cipher is unbreakable. However, a secure channel to exchange the key in advance is required. For this reason, it is used today only in special contexts, for example in diplomatic communications, where the key is exchanged in person.

Quantum technologies provide a solution to the problem of key distribution: how can Romeo and Juliet agree on a key (to be used in the XOR protocol) if the communication channel is insecure, protecting themselves from Tybalt's eavesdropping?

The basic assumption that we take for granted, in classical physics, is that any piece of data can be copied without significantly altering it. On the other hand, a peculiar feature of quantum states is that *they cannot be copied* without being corrupted. This is known as the no-cloning theorem.

2 The no-cloning theorem

Definition. Let us consider the quantum state of a photon's polarization, which is described by a direction in $\mathbb{R}^2$. The horizontally polarized state is denoted by $|0\rangle$, and the vertically polarized state by $|1\rangle$. A general state, which forms an angle β with the horizontal axis, is expressed as

$$|\psi\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle \tag{1}$$

When a photon is sent to a polarization analyzer, there's a probability $p_{\text{hor}} = |\langle 0|\psi\rangle|^2 = \cos^2\beta$ that it emerges horizontally polarized, and a probability $p_{\text{ver}} = |\langle 1|\psi\rangle|^2 = \sin^2\beta$ that it comes out vertically polarized. The outcome of the measurement if thus not deterministic for states different from $|0\rangle$ and $|1\rangle$, but the only possible final states are these two.

A measurement of the polarization state of a single photon gives a single bit of information, corresponding to the polarization state of the photon after going through the analyzer. Therefore, if the photon was in a mixed state, characterized by the polarization angle β, it is impossible to measure β with only just one measurement, the outcome of the measurement being probabilistic. Furthermore, repeated measurements do not provide additional information, because the state collapses onto one of the two pure states, $|0\rangle$ or $|1\rangle$, after the first measurement.

The only possible way to measure precisely the polarization of a state would be to have prepared in advance a set of identical photons. For example, if we prepare 1000 photons and measure them all, obtaining 250 times the state $|0\rangle$ and 750 times the state $|1\rangle$, we could infer that the original angle was $60°$, since

$$\cos^2 60° = \frac{1}{4} = 25\%, \quad \sin^2 60° = \frac{3}{4} = 75\%. \tag{2}$$

Why cannot we take a single photon, *make 999 copies of it*, and then, by measuring those copies, determine its state precisely? This turns out to be in contradiction with the basic principles (postulates) of quantum mechanics.

It must be stressed that this is not a mere engineering problem (how do you physically photocopy a photon?) but a conceptual one, given by the very laws of quantum mechanics. Indeed we can formally prove it:

Theorem. *It is impossible to build a machine that operates linear transformations and is able to clone the generic state of a qubit.*

Proof. Let us consider a system composed of the qubit to be cloned $|\psi\rangle$, a second "blank" qubit $|\phi\rangle$ and the cloning machine (a third quantum state) $|M_i\rangle$. The first qubit is prepared in a generic state

$$|\psi\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle \tag{3}$$

The cloning machine should be able to perform a transformation U such that

$$U(|\psi\rangle|\phi\rangle|M_i\rangle) = |\psi\rangle|\psi\rangle|M_{f(\psi)}\rangle = (\cos\beta|0\rangle + \sin\beta|1\rangle)(\cos\beta|0\rangle + \sin\beta|1\rangle)|M_{f(\psi)}\rangle \tag{4}$$

where the final state of the machine will in general depend on the state $|\psi\rangle$ to be cloned. We show now that such a transformation cannot exist. If the first qubit is in the state $|0\rangle$ (i.e. $\beta = 0°$), the action of the cloning machine must be

$$U(|0\rangle|\phi\rangle|M_i\rangle) = |0\rangle|0\rangle|M_{f(0)}\rangle \tag{5}$$

Analogously, if the first qubit is prepared in the state $|1\rangle$ (i.e. $\beta = 90°$),

$$U(|1\rangle|\phi\rangle|M_i\rangle) = |1\rangle|1\rangle|M_{f(1)}\rangle \tag{6}$$

Therefore, the action of the cloning machine on a generic state $|\psi\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle$ is given by

$$U((\cos\beta|0\rangle + \sin\beta|1\rangle)|\phi\rangle|M_i\rangle) = (\cos\beta)U(|0\rangle|\phi\rangle|M_i\rangle) + (\sin\beta)U(|1\rangle|\phi\rangle|M_i\rangle) \tag{7}$$

where we have invoked the linearity of quantum mechanics. We now insert the two previous equations into the last one, obtaining for the right hand the state

$$\cos\beta|0\rangle|0\rangle|M_{f(0)}\rangle + \sin\beta|1\rangle|1\rangle|M_{f(1)}\rangle \tag{8}$$

which is clearly different from the desired one

$$(\cos\beta|0\rangle + \sin\beta|1\rangle)(\cos\beta|0\rangle + \sin\beta|1\rangle)|M_{f(\psi)}\rangle. \quad \square \tag{9}$$

3 The BB84 protocol

We have seen that a quantum state cannot be copied without being disturbed. It is in way, so delicate, so shy that it frightens away and changes its color at a mere glance. This inherently quantum property allows *intrusion detection*: Romeo and Juliet can always know if Tybalt is eavesdropping their lovely conversation.

The BB84 protocol, discovered by Bennet and Brassard in 1984, uses this feature to allow Romeo and Juliet to agree on a secret key (to be used in a symmetric cryptographic protocol) even if they can only communicate on an insecure channel.

The protocol requires two binary alphabets x, z with two states each: $|0\rangle_x$, $|1\rangle_x$, $|0\rangle_z$, $|1\rangle_z$. The states are related according to

$$|0\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle_z + |1\rangle_z) \tag{10}$$

$$|1\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle_z - |1\rangle_z) \tag{11}$$

where the denominator ensures all vectors have unit length. We can picture the two alphabets (bases) and the four states as in table

Alphabet	basis	$\|0\rangle$	$\|1\rangle$
z	$+$	$\rightarrow$	$\uparrow$
x	$\times$	$\nearrow$	$\searrow$

Table 1: Basis and Polarization States

The protocol is as follows:

1. Juliet has a plaintext binary sequence to transmit p. Juliet generates a random *seed* sequence s_{c} of 0's and 1's. For example

$$s_{\mathrm{c}} = 0100\ldots \tag{12}$$

2. Juliet encodes each bit of the random sequence s_{c} in a qubit. To do this, for each bit Juliet chooses with a coin flip which alphabet to use, x or z. The encoded random sequence s_{q} could end as something like

$$s_{\mathrm{q}} = |0\rangle_x|1\rangle_z|0\rangle_x|0\rangle_z\ldots \tag{13}$$

3. The resulting string s_{q} is sent to Romeo (for example, as a series of laser pulses in a optical fiber).

4. For each qubit in s_{q}, Romeo decides with a coin flip which alphabet to use to measure it. For example he could use the sequence $zzxx\ldots$ and get as results

$$|0\rangle_x \xrightarrow{z} 0 \text{ wrong alphabet, "lucky" coin flip} \tag{14}$$
$$|1\rangle_z \xrightarrow{z} 1 \text{ right alphabet, deterministic outcome} \tag{15}$$
$$|0\rangle_x \xrightarrow{x} 0 \text{ right alphabet, deterministic outcome} \tag{16}$$
$$|0\rangle_z \xrightarrow{x} 1 \text{ wrong alphabet, "unlucky" coin flip} \tag{17}$$
$$\ldots \tag{18}$$

   - About half of the times (qubit 2 and 3), Romeo will choose the same alphabet chosen by Juliet. In this case, after a measurement, he will recover the original bit in the sequence s_{c} with 100% accuracy.
   - The remaining times (qubit 1 and 4), Romeo will choose the wrong alphabet and will fail to recover correctly the original bit in 50% of these cases (in this example, bit 1 is recovered correctly, bit 4 is not).

     From now on, Juliet and Romeo exchange only classical information on a public channel. The only "quantum data exchange" in the protocol is the sequence s_{q}.

5. Juliet and Romeo exchange the sequences of alphabets they used, in this case $xzxz\ldots$ for Juliet and $zzxx\ldots$ for Romeo. This exchange happens on a classical public channel.

   Note that Juliet and Romeo do not share the original bits or the results of the measurements, only the alphabets they used.

6. Juliet and Romeo *delete* all bits corresponding to the cases in which they used different alphabets. In the example, they delete bit 1 and 4, among others.

   The remaining binary (classical) sequence k is the so-called *raw key*, about half as long as the original s_{c}.

   This is the first time some of the bits are removed, but it won't be the last. The next steps delete or replace large chunks of the key, therefore the initial sequence s_{c} must be sufficiently long for Romeo and Juliet to end up with an usable secret key.

Initial classical sequence s_{c}	0	1	0	0	$\ldots$
Juliet's alphabet	$\times$	$+$	$\times$	$+$	$\ldots$
Quantum encoded sequence s_{q}	$\nearrow$	$\uparrow$	$\nearrow$	$\rightarrow$	$\ldots$
Romeo's alphabet	$+$	$+$	$\times$	$\times$	$\ldots$
Romeo's measurement	$\rightarrow$	$\uparrow$	$\nearrow$	$\searrow$	$\ldots$
Raw key		1	0		$\ldots$

Table 2: Steps from 1 to 6 of the BB84 protocol

7. Over a public communication channel, Romeo and Juliet announce and compare a part of their raw key, which is then deleted. From this comparison they can estimate the *error rate* R due to eavesdroppers or noise effects. If this rate is too high, this indicates either issues with the apparatus or the presence of an eavesdropper, so they restart the protocol from the beginning. If not, they perform *information reconciliation* and *privacy amplification* on the remaining bits of their raw key.

8. Information reconciliation is just classical error correction over a public transmission channel. A simple scheme is given by performing parity checks:

   - Romeo and Juliet divide the remaining bits of their raw key into subsets of length l. This length is chosen in order that it is highly unlikely to have more than one error per subset ($Rl \ll 1$).

   - Romeo and Juliet compute the parity of each subset, deleting each time the last bit of the chunk from the key[1].

     For example, let Romeo's and Juliet's raw keys begin with:

     $$\text{Romeo: } 11010011010010\ldots \tag{19}$$
     $$\text{Juliet: } 10010011010010\ldots \tag{20}$$

     If for example $l = 7$, we then consider the first subsets

     $$\text{Romeo: } 1101001 \tag{21}$$
     $$\text{Juliet: } 1001001 \tag{22}$$
     $$\text{Romeo: } 1010010 \tag{23}$$
     $$\text{Juliet: } 1010010 \tag{24}$$

     Disregarding the last bit, the parities are

     $$\text{Romeo: } 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 1 \tag{25}$$
     $$\text{Juliet: } 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0 \tag{26}$$
     $$\text{Romeo: } 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 1 \tag{27}$$
     $$\text{Juliet: } 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 1 \tag{28}$$

   - The parity of each subset is publicly announced, and by comparing the parities, under the assumption that each subset contains at most one error, Romeo and Juliet can detect chunks of their raw key that do not agree, as in the first subset of this example.

   - If a disagreement is found, Romeo and Juliet locate and delete the erroneous bit by binary search, that is, they bisect the subset (each time deleting the last bit) until all the parity checks on smaller subsets agree.

[1] This ensures that Tybalt does not gain any type of information on the original key from the parity checks

In the above example, the first subset has a different parity in Romeo's and Juliet's keys, so it is split into two 3-bit subsets, each of which gets the last bit deleted, then Romeo and Juliet compare the parities of these two smaller subsets:

$$\text{Romeo: } 1 \oplus 1 = 0 \tag{29}$$
$$\text{Juliet: } 1 \oplus 0 = 1 \tag{30}$$
$$\text{Romeo: } 1 \oplus 0 = 1 \tag{31}$$
$$\text{Juliet: } 1 \oplus 0 = 1 \tag{32}$$

This shows that the erroneous bit belonged to the first subset, which can be deleted.

At the end of this step, Romeo and Juliet will share with high probability (if every subset actually contained at most one error) the same string of bits of length n.

9. Privacy amplification reduces Tybalt's information about the final secret key to arbitrarily small values. A simple protocol works as follows:

   - Romeo and Juliet estimate from the error rate R obtained previously the maximum number of bits $k \approx Rn$ known by Tybalt.
   - After choosing a security parameter j, Romeo and Juliet choose at random $n-k-j$ subsets of their key.
   - The parities of these subsets become the final secret key. This key is more secure than the previous one, since Tybalt must know something about each bit of a subset in order to obtain information about its parity.

   For example, say Romeo and Juliet have $n = 100$ bits left, and previously estimated an error rate of $R = 10\%$. They infer that Tybalt cannot know more than $k = 100{\cdot}0.1 = 10$ bits. They choose $j = 70$, and so divide the remaining 100 bits into $100 - 10 - 70 = 20$ subsets of 5 bits. The final secret key will be 20 bits long, with each bit the parity of the corresponding subset.

$$\text{Bits after reconciliation: } 10101101101100010000\ldots \tag{33}$$
$$\text{Chosen subsets: } 10101 \quad 10110 \quad 11000 \quad 10000\ldots \tag{34}$$
$$\text{Secret key: } 1 \quad 1 \quad 0 \quad 1 \quad \ldots \tag{35}$$

10. With this final secret key f Romeo and Juliet can now encrypt their lovely messages using symmetric protocol such as the XOR cipher. The encoded message will be $c = p \oplus f$, and Romeo will decrypt it performing another bitwise XOR $p = c \oplus f$.

    Note that the remarks at the end of step 8 regarding the possibility of having errors in the key still apply, even if this possibility is extremely unlikely.

4 Experimental implementations and vulnerabilities

In quantum key distribution protocols, the quantum degrees of freedom are usually the properties of a laser beam, such as polarization (as in our first example), intensity, impulse rate and duration. The exchange of photons usually happens through optical fibers, which can ensure faithful transmission over a few tens of kilometers. Note that quantum cryptography experiments use standard optical communication channels and it is not necessary to construct special-purpose cables.

The bottleneck in quantum communication via optical fibers is that the probability for both absorption losses (e.g. the photon is absorbed by the walls of the cable) and depolarization (e.g. successive reflections can alter the initial polarization with time) grows exponentially with the length of the fiber. A solution to these limitations is to switch to satellite-based networks, which have proved to guarantee kilohertz key rates over thousands of kilometers, many orders of magnitude higher than with optical fibers of the same length.

In spite of the theoretical inviolability of quantum key distribution protocols, even if we discard shortcomings related to experimental realizations, there are still practical vulnerabilities related to hardware attacks and the need for authentication.

On one hand, when we take into account that photons have to be generated and measured by a (classical) pieces of hardware, such as a lasers, many ways to potentially spy or interfere with the protocols become possible. Technical imperfections in those devices can give away precious information on the (impenetrable) quantum states they create and measure.

The issue with authentication is even more fundamental: it turns out that QKD cannot provide a secure method to ensure Romeo is communicating with Juliet in the first place. They must rely on a (classical) authentication method, otherwise Tybalt may act as he was Juliet and Romeo could unknowningly perform all the protocol's steps, without ever Juliet knowing the conversation is even taking place. If a method to exchange digital signatures can be initially trusted, QKD really unleashes its full potential.