Quantum Cryptography Presentation Notes

Francesco Stern

April 2024

1 Introduction

Definition 1.1. Cryptography (or **Cryptology**) is the practice and study of techniques for secure communication in the presence of an adversary.

Remark. The practice that an adversary implements to intercept a message is called *eavesdropping*

Now, the premise of cryptography then is: how can I communicate a message through a public channel (where there could be someone trying to capture that information) in a way that ensures that only the intended receiver of this message is able to comprehend it.

To be able to achieve this objective what we already know what we need, and that is what is known as a **Cryptographic Key**

Definition 1.2. A **Cryptographic Key** is a piece of information (a string of numbers or a sequence of letters perhaps) that, when processed through a cryptographic algorithm, has the ability to encode or decode a message.

Actually, we don't just know this, but we also have what is the single safest way of sharing information: the **One-Time Pad**.

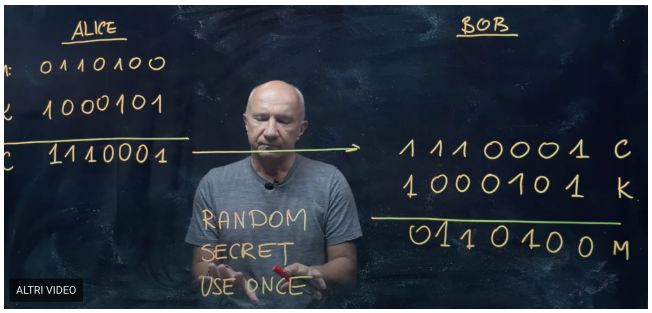

Figure 1: One-Time Pad

Of course, then, our problem becomes to manage to distribute a Cryptographic Key in a way that is safe: the **Key Distribution Problem**.

There are two ways to approach it, one one is what we can call the "classical" way, which is Public Key Cryptosystems, and that uses Mathematics and relies on the Computational Complexity of certain operations (e.g. the factorization of large integers) to make it so that intercepting and extracting a key becomes too computationally complex to do.

Unfortunately, Public Key Cryptosystems have no way of ensuring being entirely safe, in fact we know that with the computational power of Quantum Computers some of these can be broken (like RSA).

The other way is "Quantum Cryptography", that instead aims at using quantum phenomena (like Quantum Entanglement) to secure the process of key distribution, which is what we will be focusing on.

2 BB84 Protocol

The BB84 Protocol was first developed by Charles Bennett and Gilles Brassard in 1984, and it is the first quantum cryptography protocol ever developed.

In this protocol, the participants (Alice and Bob) wish to agree on a secret key about which no eavesdropper (Eve) can obtain significant information.

This is a quantum protocol, therefore Alice and Bob can utilize a public quantum channel, as well as their public classical channel.

What Alice does to begin the protocol is she generates two n-bit strings a and b

$$a = a_1 a_2 a_3 ... a_n \tag{1}$$

$$b = b_1 b_2 b_3 ... b_n \tag{2}$$

And then what she does is she creates quantum states according to these bit strings as follows:

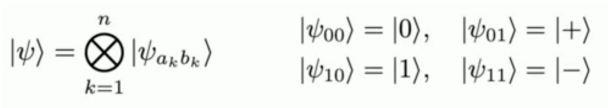

Figure 2: Caption

For each two bits from a and b, she takes them and creates one qubit, and then she creates n such qubits and the whole state will be denoted by $|\psi\rangle$.

So, we can see that the bit coming from the bit string b, determines the basis of Alice's encoding, while bit string b will determine the encoded state.

The key notion here is that states prepared in the X basis will not be orthogonal to states prepared in the Z basis, and thus the inner product between them will not be 0.

When the inner product is non-zero, it means that the two states are not perfectly distinguishable, which is the crucial passage in the protocol.

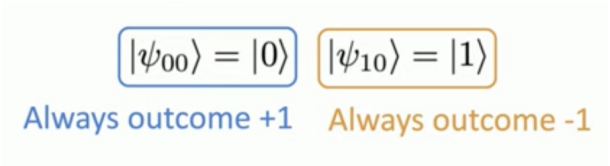

Figure 3: Caption

In this case, the two states are always distinguishable when measured in the Z basis, as each will give +1 or -1, depending on which one of the two states we are measuring, but if instead we are given these two states:

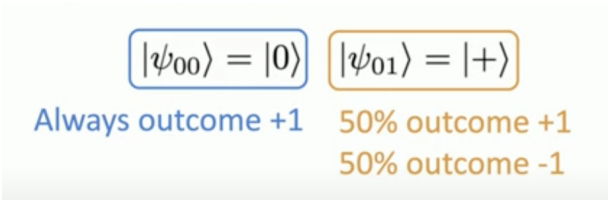

Figure 4: Caption

Here, however, if the second qubit, prepared in the X basis, is measured in the Z basis, we will have a 50% of the outcome being +1 and 50% of it being

-1, thus they are not distinguishable.

Now, how BB84 works is by cross referencing these bases, as we now show with an example for $n = 5$:

string a	0	1	1	0	1
string b	1	1	0	0	1
basis	X	X	Z	Z	X
Encoded qubits	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$

Figure 5: Caption

What she does after is she sends the encoded qubits over to Bob, who measures them according to a randomly generated n-bit string $b' = b'_1 b'_2 ... b'_n$

As Alice did then, if $b'_i = 0$, he will measure the qubit in the Z basis, and if $b'_i = 1$, he will measure the qubit in the X basis.

Once he's done measuring, he will then have his own n-bit string $a' = a'_1 a'_2 ... a'_n$, where if he gets +1 then $a'_i = 0$, and if he gets -1 then $a'_i = 1$.

What Alice and Bob do now is they publicly share strings b and b'. If $b_i = b'_i$, then they will keep that bit, and if discard it otherwise.

Then, they will end up with two, shorter strings $\bar{a}$ and $\bar{a}'$ such that $\bar{a} = \bar{a}'$, which they will then be able to use as their encryption key.

But what if we introduce our eavesdropper Eve in this scenario? Well, to start with, we don't have to worry about Eve copying the qubits sent by Alice and sending them over to Bob, which would give her access to the encryption key, as the No-Cloning theorem tells us that she can't "clone" a qubit in a quantum state.

This being said, what else could she try to do?

She could try to intercept and measure the qubit's state, but keep in mind that she would have to guess the basis in which the qubit was prepared, as the b string has not been made public by Alice.

This attempt would also be risky though, as if she guesses the wrong basis and after that Bob measures the qubit he receives in the right basis, then upon checking b and b' Alice and Bob would see that that qubit's state would have been disturbed.

In this case, for a single qubit, she would have a 1/4 probability of being detected. In an n-qubit string, then the probability Alice and Bob have of catching Eve would be

$$P(n) = 1 - (3/4)^n$$

The differences can be caused by eavesdropping, but also by imperfections in the transmission line and detectors. As it is impossible to distinguish between these two types of errors, guaranteed security requires the assumption that all errors are due to eavesdropping.

Provided the error rate between the keys is lower than a certain threshold (27.6% as of 2002), two steps can be performed to first remove the erroneous bits and then reduce Eve's knowledge of the key to an arbitrary small value: Information Reconciliation and Privacy Amplification.

3 SARG04

Before going to E91, let's take a detour through SARG04, which is a clever modification of the BB84 protocol.

In it, we proceed the exact same way all through Bob's b' string generation.

Once he has done and communicated that publicly, Alice, instead of sharing b, will pick for each of the qubits sent two states, one in each of the two bases (one of the two states will be the actual one of her qubit, which she will note down), and communicate them to Bob.

Bob then will discard every qubit is in a state contiguous to either of the bits, and only consider valid the ones that would be in a state "impossible" according to the states communicated by Alice, from which he will be able to deduce the state he was sent and the secret bit.

Thus, once that's done, Alice will choose half of the bits for which Bob ran a conclusive test and run a check with Bob to see if they are correct. If the check passes, then they're done (except for Information Reconciliation and privacy Amplification).

4 E91 Protocol

As ingenious as BB84 was and still is, there is one fundamental aspect that hinders its security, an aspect that is inherent to the nature of the protocol itself.

Both Alice and Bob (we focus on Alice for obvious reasons), need a source that generate random bits, a "secured randomness" source, to ensure that the

n-bit string b, from which Alice derives her measurement bases, is indeed secure. If this is a premise on a theoretical level, when we get practical it becomes a very obvious vulnerability, as Eve could corrupt this source and send her own bit string, which would allow her to break the protocol, **without being noticed**.

Is it possible, then, to make it so that Eve's threat to get the Key is made null? As a matter of fact we can, and a solution involves Quantum Entanglement.

The E91 protocol, named after Artur Ekert who developed it in 1991, is an Entanglement-based QKD protocol that relies on maximally entangled states to ensure security.

For this protocol, we start with a Bell State chosen at will.
Say we choose

$$| \Psi^+\rangle_{AB} = 1/\sqrt{2}(| 01\rangle + | 10\rangle)_{AB}$$

The basic idea here is that if Alice and Bob receive two qubits entangled in this Bell State and perform the same measurement on them, then they will be either correlated or anti-correlated:

Consider measurements in the X basis:

$$\text{Prob}\{|++\rangle_{AB}\} = \frac{1}{2} \quad \text{Prob}\{|--\rangle_{AB}\} = \frac{1}{2}$$
$$\text{Prob}\{|+-\rangle_{AB}\} = 0 \quad \text{Prob}\{|-+\rangle_{AB}\} = 0$$

Figure 6: Caption

Consider measurements in the Z basis:

$$\text{Prob}\{|00\rangle_{AB}\} = 0 \quad \text{Prob}\{|11\rangle_{AB}\} = 0$$
$$\text{Prob}\{|01\rangle_{AB}\} = \frac{1}{2} \quad \text{Prob}\{|10\rangle_{AB}\} = \frac{1}{2}$$

Figure 7: Caption

Now, the second main aspect of this protocol has to do with entanglement as well, and it is in fact here that it sets itself apart from BB84 from a security perspective.

Alice and Bob, once they get their qubits, need to verify that they are entangled, not just because that is how they can verify they share the same secret key, but because if they are maximally entangled, as in an EPR pair, then they

can use a property called "Monogamy of Entanglement" to ensure security from eavesdroppers.

Definition 4.1. The **Monogamy of Quantum Entanglement** refers to the fundamental property that it cannot be freely shared between arbitrarily many parties.

In order for two qubits A and B to be maximally entangled, they must not be entangled with any third qubit C whatsoever.

This means that the more entangled the two qubit states, the more secure the communication will be from an eventual eavesdropper!

So, how do they verify the entanglement? Via the CHSH Inequality.
Say Alice and Bob share a state $|\psi\rangle$ and measure observables A, $\bar{A}$, B and $\bar{B}$.

Knowing that the expectation value for an observable where Alice measures A and Bob measures B is

$$\langle AB\rangle = \langle\psi \mid A \otimes \langle B \mid \psi\rangle$$

then we get:

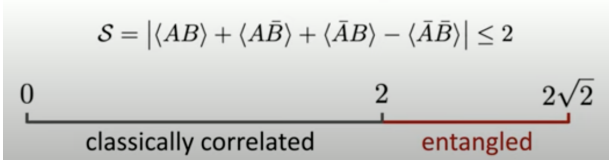

Figure 8: Caption

What we will find is that Entangled States exceed the boundary value of 2, and actually can reach up to $2\sqrt{2}$ when maximally entangled.

Now, this fact becomes key in verifying the entanglement of the states and thus in ensuring the safety of the protocol.

What Alice and Bob will do then is they will choose their bases:

$$A_1 = Z \qquad B_1 = Z$$
$$A_2 = X \qquad B_2 = \frac{1}{\sqrt{2}}(Z - X)$$
$$A_3 = \frac{1}{\sqrt{2}}(Z + X) \qquad B_3 = \frac{1}{\sqrt{2}}(Z + X)$$

They will receive their qubits, measure their states in the bases and then, just like in BB84, they will share the bases sequence.

Alice's basis	A_1	A_3	A_1	A_2	A_3	A_3	A_1	A_3
Bob's basis	B_2	B_3	B_1	B_2	B_1	B_2	B_1	B_3

They will choose the bases that are correlated or anti-correlated and use those as their key, but what changes is what they do with the keys that are mismatched.

They can use those to calculate the CSHS inequality and see if and how entangled the qubits' states are.

If CSHS function returns a value that is ≤ 2 then they can choose to abort the protocol and start again, and if it is > 2 they can not only choose to proceed but estimate the degree of security that the protocol is at.

Again, the conditions for such a protocol in practice will never be ideal, thus the keys that they end up with (whether due to noise or eavesdropping) will more likely be nearly identical rather than the exact same.

This, however, can be intervened upon in much the same way as the BB84 protocol, by utilizing Information Reconciliation and Privacy Amplification.

5 Attacks

5.1 Faked States Attacks

Definition 5.1. A **Faked states attack** on a quantum cryptosystem is an intercept-and-resend attack where Eve does not try to reconstruct the original states, but generates instead light pulses that get detected by the legitimate parties in a way controlled by her while not setting off any alarms.

The idea for this attack relies on the fact that Alice or Bob could sometimes be fooled, using imperfections of their set-ups, into thinking they are detecting original quantum states while they are just detecting light pulses generated by Eve. These light pulses are what we call "faked states".

Remark. Faked states are specific to each particular scheme or even particular sample of equipment being attacked.

5.2 Photon Number Splitting Attack

In practice most often QKD experiments use Weak Coherent Pulses to send the quantum states. These pulses' probability of emitting 0, 1 or more than one photons are distributed according to a Poisson distribution. Most most pulses contain no photons (no pulse is sent), some pulses contain 1 photon (ideal) and **a few pulses contain 2 or more photons.**

Definition 5.2. A **Photon Number Splitting Attack** works by splitting a multiphoton signal via a physical interaction.

Eve, in this scenario, retains one photon and Bob receives the other photons such that the polarization of both parts remains undisturbed.

In this situation, Eve then waits for Alice to share her key, so that she can find the bases each photon she intercepted was prepared in and thus gain significant information on the key.

Ideally, if Alice and Bob are talking via a "lossy" channel, she could even plan to have Bob only receive multiphoton emissions and block all the single-photons, thus effectively gaining all the information she needs to get a key once Alice and Bob go through the basis-sharing step.

5.3 Trojan Horse Attack

Definition 5.3. A **Trojan Horse Attack** works by sending a bright pulse inside Alice's device and analyzing its back-reflections.

Through this, Eve could obtain information about the setting of the polarizer or the phase modulator responsible for encoding the secret bit.