A first Glimpse at Quantum Cryptography

Andrea Pasquinucci

UCCI.IT

0. Abstract

In this document, a short introduction to Quantum Cryptography is presented. Starting from the basic idea, it will be explained which are the physics principles, the most relevant protocols, the main attacks and why Quantum Cryptography is a *secure* way to solve the Key Creation and Distribution problem.

Table of Contents

1. What is Quantum Cryptography ?

A better name for Quantum Cryptography (QC) is Quantum Key Distribution (QKD), that is a solution to the problem of creating and distributing secret keys to use for encryption. In this paper we will not consider what can be the use of the secret keys generated with QKD, but we will discuss only how QC proposes to solve the problem of distributing secret keys between two parties which will need them for use with some (classical) cryptographical algorithms.

The Problem: to be able to create and distribute a secret key to two distant parties in a completely secure way; classically this is done by means of a secure courier who carries a book (CD-rom etc.) with written the keys, or by means of asymmetric (public/private) cryptographical algorithms and protocols.

The Solution: Quantum Physics offers a new way of creating and distributing secret keys between two distant parties by using ***elementary particles*** which follow the rules of Quantum Mechanics. Quantum Mechanics, as opposed to Classical Mechanics, states that elementary particles behave quite differently from what one would expect based on everyday human experience. By leveraging on these particular properties of Quantum Mechanics, it is possible to devise some protocols which make it possible to create and distribute secret keys.

Thus to be able to use QKD, the two parties, conventionally called Alice and Bob, whereas Eve is the attacker or eavesdropper, must share some communication channels, in practice QKD requires that Alice and Bob have:

1. a Quantum channel through which they can exchange elementary particles, usually this can be a one-way channel, but for technical reasons which will be discussed in [2] some implementations require a bi-directional quantum channel;
2. a Classical channel through which Alice and Bob can communicate in a authenticated way, again uni- or bi-directional.

In practice only two Quantum Channels have been considered up to now:

1. *optical fibers*
2. *free space*

where **photons** propagate. Photons are the elementary particles which constitute light, and more generally electromagnetic waves. The QKDs today on the market use optical fibers, thus Alice and Bob must have an optical fiber (with some additional constraints that we will describe) which connects them. They will also need some devices which will send and detect photons in this fiber. Other Quantum channels could be considered in future if other elementary particles, like for example electrons, will be found to be usable in QKD protocols.

Alice and Bob will also need a Classical communication channel, like an ordinary telephone line. Usually, having a optical fiber already at their disposal as QKD communication channel, this can be

used also for the classical communication. For what concerns QKD protocols, what is important is that Alice and Bob can exchange some classical communications which *cannot be modified* on the transmission channel. The requests on the communication channels can be seen perhaps more easily from the point of view of what Eve is allowed to do:

1. Eve is allowed to do whatever Physics permits her to do on the Quantum channel
2. Eve can only listen passively on the Classical channel but she cannot modify the information exchanged between Alice and Bob on this channel nor interrupt the communication.

Thus the Classical channel of communication must guarantee the authentication and integrity but not the privacy of the communication between Alice and Bob.

Summarizing:

1. Alice and Bob exchange photons through an optical fiber which connects them
2. after that, they exchange some classical information
3. at the end of this process Alice and Bob share a secret key which Eve has not been able to eavesdrop, or, if Eve has successfully eavesdropped the key, Alice and Bob are aware of the eavesdropping and discard the key.

How is this possible? We will explain this in the next sections, but we have to start by explaining some of the particular properties of elementary particles (photons in this case) on which is based the security of the QKD protocol.

It is important to note already at this point that the protocol allows Eve to eavesdrop and learn the secret key. The point is that if Eve does succeed in doing this, *Alice and Bob are guaranteed to be informed!* Thus Alice and Bob will discard the key and go out to look for Eve. Notice that it is not possible to use QKD to exchange data (real information) since only after having completed the protocol Alice and Bob will know if Eve has eavesdropped or not. If what Eve obtains is a key which will never be used, no harm is done to Alice and Bob, but if Eve actually gets some real information, then there will be a serious problem for Alice and Bob. Thus QKD is inherently a Key Distribution protocol, and cannot be used to transfer real information.

2. Physics Principles

Quantum Mechanics describes the behavior of elementary particles, among them also the photons which are elementary quantum massless particles being the fundamental constituent of light. Quantum Mechanics dictates laws for elementary particles which depart from what we know and experience every day for macroscopic objects. The fundamental Quantum Mechanical laws most relevant to QKD

are:

1. Quantum mechanics is inherently statistical, which means that often we cannot predict with certainty what will be the outcome of an experiment but only the statistics of the results when we repeat the experiment many times
2. one cannot duplicate an *unknown* quantum state, that is a quantum photocopy machine does not exist
3. every measurement *perturbs* the measured system (unless the system is in a state which is *compatible* with the measurement)
4. one cannot measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.

The last point can be stated more generally by saying that if the system is in one of either of two (or more) *orthogonal* states and the measuring device is able to measures these states, then a certain result will be obtained by the measurement and no perturbation of the system will happen (this is a compatible measurement, see point 3). But a measuring device cannot measure a system in a state prepared in a different non-orthogonal state without perturbing it; moreover by repeating the measurement on many identical states, each possible outcome of such measurement will appear with a certain probability.

This point is difficult and fundamental at the same time. We will try to explain it directly on the example of the photons which will concerns us later.

As already said, the fundamental constituent of light are elementary quantum massless particles called photons. The *polarization* of a photon is a property associated to its angular momentum, which can be imagined as related to the axis and speed of rotation of the photon. Suppose to do the experiment as in Figure 1. Some unpolarized photons are sent through a first polarization filter, only photons which are polarized vertically will appear on the other side of the filter, and some photons will be absorbed. Suppose then to put a second filter, at the beginning with the same orientation of the first but which we can rotate. As we rotate the second filter, some photons will be absorbed and the photons which will appear after the second filter will be polarized in the direction of the second filter. The more we rotate the filter, the higher the **probability** that a photon will be absorbed. When the angle is 45 degrees, 50% of the photons will be absorbed. At 90 degrees the probability is exactly zero, no photons pass and we have reached the so called *orthogonal state*. The *state* of a photon is a photon for which we know also some properties, like the polarization, which allows us to specify it completely.

Indeed the vertical and horizontal polarization states are *compatible*, which means that there exists a device which can tell us exactly if a photon has vertical or horizontal polarization. But if a photon has 45 degrees polarization, this device will fail 50% of the times. Rotating by 45 degrees the device we will be able to distinguish exactly photons with diagonal polarization, 45 or -45 degrees, but we will make 50% of mistakes every time we try to distinguish vertical vs. horizontal polarized photons.

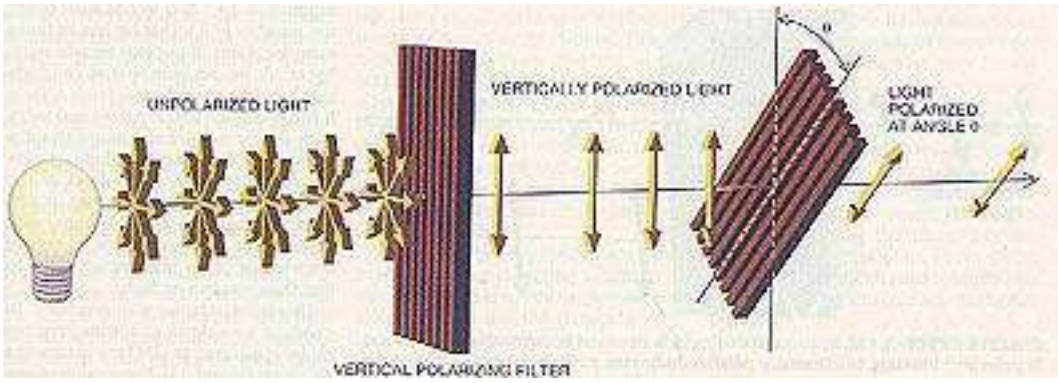

Fig. 1 Polarization by filters [4]

We have reached the following important conclusions. If a photon is polarized in the vertical/horizontal basis and we measure it in these polarization directions (in other words, we measure in this basis), we will know exactly the photon polarization. If we measure in the diagonal 45 degrees basis, we will make a 50% error and modify the polarization of the photon.

The same holds with many other properties of photons and in general of elementary particles. The important consequence of this is that if we do not know in which basis has been prepared an elementary particle, and we choose at random to measure some properties in one basis, we will make some mistakes, the statistics of which depends on the details of the system that we are considering. Indeed for QKD various protocols have been proposed which encode the information not in the polarization of the photons but for example in their phase or other properties. We will not consider these protocols in this paper, but see [2] for more informations.

From this it also follows that it is impossible to make a photocopy of an unknown quantum state. If we do not know in which basis the state has been prepared, we will make some errors in trying to measure it and then copy it, so that the copy will be different from the original. Notice moreover that differently from the classical case, once we have made a measurement which is not exact, we also modify the original particle ! In practice trying to make a photocopy of an unknown quantum state, we end up with two states, but both are different from the original state with some probability.

3. The BB84 protocol

The Bennet-Brassard 1984 (BB84) protocol was the first to exploit the properties of photons discussed in the previous section to realize a QKD system. We will briefly describe the protocol here in one of its

simplest implementations.

Setup. Alice and Bob choose 4 quantum states which constitute two *mutually unbiased bases*. What this means is that the states are orthogonal two by two (horizontal/vertical, left/right diagonal) and that if we measure in the wrong basis anyone of the states of the other basis we have exactly 50% probability of error. In the simplest implementation of BB84, the first basis is polarization horizontal and vertical, the second basis is polarization diagonal +45 (right) and -45 (left). We also assign to the states the following values:

- vertical = 1
- horizontal = 0
- right = 1
- left = 0

In this way Alice can use either of the two basis to send to Bob a binary message using photons as carriers.

Protocol. Alice and Bob perform the following steps:

1. Alice chooses *at random* one of the 4 states and sends the corresponding photon to Bob on the Quantum channel, she records her choice but she does not tell Bob or anyone about it;
2. Bob chooses *at random* (independently from Alice) one of the two basis, either the vertical/horizontal or the diagonal basis, and measures the received photon in this basis; Bob records the basis he has chosen and the result obtained by the measurement but he does not tell to anybody these values;
3. Alice and Bob repeat point 1 and 2 a sufficiently high number of times which depends on the length of the secret key they want to create (as we will see this should be at least twice as many as the number of bits of the resulting key);
4. Using the Classical communication channel, Bob tells Alice which basis he had used to measure each photon, but he does not say which result he had obtained;
5. For each photon Alice replies to Bob saying if Bob 's basis has been correct or wrong (that is if he had used the compatible basis or not); both Alice and Bob discard all measurements where Bob has used the non-compatible (wrong) basis, what remains is the *sifted key*, that is the first proposal for the secret key.

This protocol is depicted in Fig. 2 and the experimental setup in Fig.3. In practice the protocol does not stop here, but we will discuss the remaining steps after having looked into Eve ' sactivities.

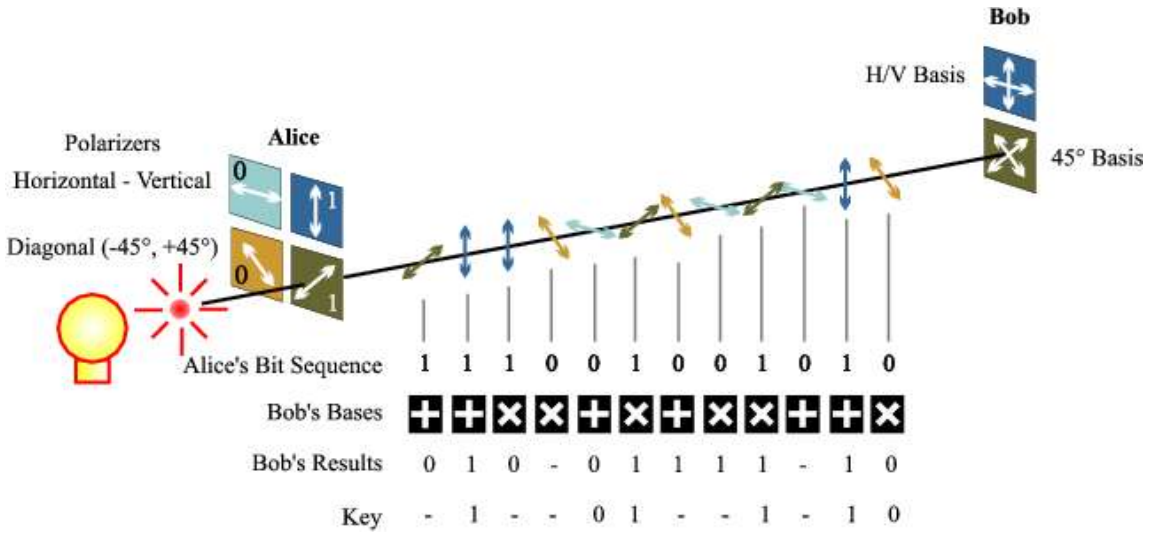

Fig. 2 The BB84 protocol

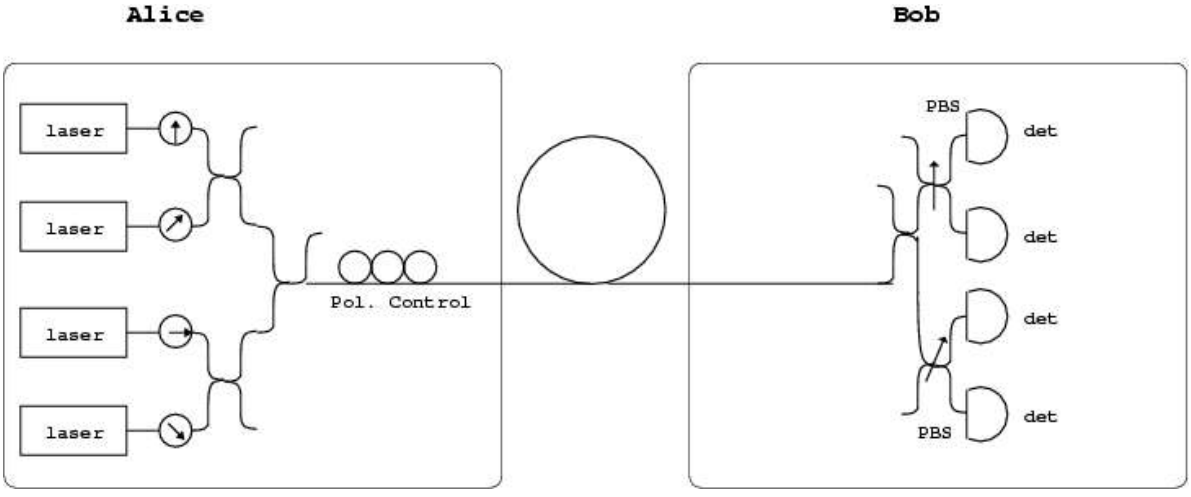

Fig. 3 Scheme of experimental setup (PBS = Polarization Beam Splitter)

A few comments on the protocol are necessary. After steps 1 and 2, Bob has a *raw key* in which 25% of the bits are wrong. This is due to the fact that in average Bob uses 50% of the times the wrong basis to measure the photons, and when Bob uses the wrong basis, 50% of the times he gets the wrong value for the bit since the two bases are maximally conjugated. 25% of errors is too much to be corrected using classical error correcting protocols, thus Alice and Bob proceed with points 4 and 5 to

eliminate all possible errors due to the use of the wrong basis by Bob. Notice that in all this no information is given to Eve. After all steps, *in theory*, Alice and Bob share a secret exact key.

Moreover neither Alice nor Bob can decide which key will result from the protocol. Indeed is the intersection of both their random choices which produces a random key!

4. Eavesdropping

Up to now we have not shown how this protocol is secure and how Quantum physics plays a central role in guaranteeing this. To show this we discuss in this section what Eve can do. We will consider only the simplest strategy as an example, a more complete discussion can be found in the companion paper [2].

The simplest attack that Eve can do is called *intercept-resend* strategy. This is the simplest of the man-in-the-middle (MitM) kind of attacks. Eve sets herself in the middle of the quantum channel, she receives all photons sent by Alice and resends them to Bob. BUT ! Physics and the BB84 protocol do not allow her to be successful.

Remember that *Eve cannot make an exact copy of an unknown quantum state*, what she can do, for example, is to measure each photon sent by Alice as Bob would do. But, as Bob, Eve will choose 50% of the time the wrong basis and in this case her measurement gives a random result, exactly as for Bob. After Eve has received and measured a photon from Alice, she will record her choice of basis and the result of the measurement, and then she will send to Bob a photon polarized accordingly.

Notice that physics gives Eve few other choices, some of which will be described later and in [2], because in whichever way she tries to learn something on a unknown photon sent by Alice, she will disturb and modify it.

Now what happens when Bob receives the photons sent by Eve? Well, obviously errors will go up, since Eve has sent to Bob 50% of the photons in the wrong basis with respect to the basis chosen by Alice. Now Alice and Bob perform steps 4 and 5 of the protocol without knowing of the errors introduced by Eve. Thus Alice and Bob think to have a perfectly identical sifted key, but instead half of the time in the sifted key Bob has used a photon received from Eve in the wrong basis, and since all choices are random and the result of a measurement in the wrong basis is random, it follows that 25% of Bob ' s bits in the sifted key are wrong.

Of course Eve can try to reduce the amount of errors she introduces in the photons that Bob receives. The simplest way is for Eve to eavesdrop not on all photons sent by Alice but only on some of them. Obviously, intercepting less photons Eve introduces less errors, but at the same time she learns less about the key! This is a general result for any eavesdropping strategy that Eve can adopt and it follows from Information Theory: the less errors Eve introduces the less information Eve obtains on the key, in

other words the key that Eve will be able to get at the end will be different from the one of Bob, the less errors she induces the more different will be her key from the one of Bob.

To check for the presence of Eve, Alice and Bob must then add a few other steps to the protocol. If communications would be perfect, quite impossible with any kind of real instrument, Alice and Bob would just have to check if there is one error in the sifted key. What they can do is to choose a random set (statistically not too small) of bits of the sifted key and compare them explicitly on the Classical channel. Obviously these bits must be dropped from the key and cannot be used anymore. If there are no errors, Eve has not been eavesdropping, if there is even a single error, Eve has been eavesdropping. Of course, all this only in theory!

The general result is that Eve will *always* introduce errors in the sifted key, physics guarantees this, and thus Eve can *always* be detected.

In practice things are quite different since there will always be errors due to the real instruments and communication channels.

5. Error correction, one-way privacy amplification and other security considerations

As we have just seen, there are always errors due to the devices used, also called experimental errors. How can we distinguish Eve's induced errors from experimental errors? In general we cannot, so we have to adopt the opposite point of view:

> there will always be errors which will always be *all* attributed to Eve.

This seems to be a dead end for QKD, but instead it is not. The point is to be able to evaluate which is a maximum amount of errors that we can allow and from which we can recover. In other words, we know that there are errors all attributed to Eve in the sifted key, we should first correct all of them and then we should add a procedure which will reduce to zero (more precisely to as little as desired) the information that Eve has on the final key. Indeed if Eve knows one bit of the final secret key out of a few million bits, in some situation we could consider to have created a sufficiently secure key. If this is not secure enough, then we should continue the procedure to reduce practically to zero the knowledge that Eve has on the final secret key.

The procedure to reduce the information Eve has on the sifted key from the errors is successful only if the amount of errors, which means the information Eve has to start with, is less than some maximum. This maximum must be evaluated, and indeed it has been. The way of evaluating the maximum amount of information that Eve can obtain from the errors and from which it is possible to recover, requires the introduction of classical and quantum information theory. This will be discussed in [2].

Here we just mention the more general and restrictive result:[1]

> the amount of error found in the sifted key must be less than 11% to be able to produce a secure key.

Here we just describe the simplest, classical procedures to add to the BB84 protocol to cancel all errors introduced by Eve and to reduce to zero the knowledge that Eve has on the secret key (more advanced, efficient and quantum algorithms exist to do this than the ones described here). These algorithms are called Error Correction and (One-way) Privacy Amplification.

Error Correction

The simplest error correction algorithm, which is actually not used in practice due to its un-reliability and little efficiency, consists in Alice choosing at random a pair of bits, computing the XOR of their value (their sum modulo 2) and announcing to Bob which bits she has chosen and the value of the XOR, but not the value of each single bit. Bob computes the XOR of the same bits and tells Alice if the two XOR agree. If they do, Alice and Bob keep the first bit and discard the second, if they don't they discard both bits. This is a highly inefficient algorithm since more than half of the key is discarded at the end, but gives the idea of how it is possible to check if there are errors in the sifted key and to discard them without leaking information to Eve. In this way Alice and Bob obtain two identical keys. Moreover at the end of the algorithm it is possible to compute the percentage of error bits in the sifted key, that is the amount of errors attributed to Eve. If this is more than 11% (in the case we are considering) Alice and Bob discard the key and go out to look for Eve.

Obviously Eve can listen on the communication channel and can do the same as Alice and Bob, but notice that if Eve does not want to be detected, she must have introduced less than 11% of errors in the sifted key. This means that Eve 's sifted key is different from Bob ' s sifted key and that Eve has less information than Bob. Thus, even if Eve follows step by step the error correction procedure done by Alice and Bob and repeats all what they do, since she starts with a different key from the one of Bob, at the end she will have a key with some errors with respect to the identical keys of Alice and Bob.

One-way Privacy Amplification

After having eliminated all errors introduced by Eve, Alice and Bob have identical keys. The problem now is that Eve knowns some of it. Assuming that the errors introduced by Eve in the sifted key are less than 11%, which implies that the information obtained by Eve is less than the maximum allowed, now Alice and Bob proceed to reduce the knowledge of Eve practically to zero. The simplest classical One-way Privacy Amplification algorithm is very similar to the error correction algorithm just presented. Alice chooses at random 2 bits and computes the XOR. She tells Bob which two bits she has chosen

1 More recent results suggest that this limit can be increased, that is the amount of error allowed and from which it can be recovered can be higher.

but not their value nor the value of the XOR. Bob computes the XOR of the two bits and both Alice and Bob substitute the two bits with their XOR. Again the final key is reduced in length by applying many times this procedure. Eve learns by listening on the classical communication channel which bits to XOR and can do the same. Unfortunately for EVE her key is quite different from the one that Bob and Alice share, since the error she has originally induced is less than 11%. This means that doing the XOR she will replace quite often two bits, one right and one wrong, with one wrong bit. At the end, most bits in the Eve'skey will be wrong and her key totally useless. Alice and Bob have practically reduced to zero the information learned by Eve on the key.

Of course the attacks that Eve can do on the photons sent by Alice can be more complicated than the simplest intercept-resend strategy presented. Similarly the error-correction and privacy-amplification algorithms are more complicated and sophisticated than the simple examples presented. Nevertheless the basic principles of QKD remain the same. Moreover there are some kind of technical attacks, like Trojan Horses or the Quantum non Demolition Attacks, that are related to some technical problems of the current implementations of QKD and which will be solved by the advances of technology in the next years.

In any case, QKD does not solve the problem of the initial identification of Alice and Bob, has some technical disadvantages due to the current implementation in optical fibers using single photons, but even if it is a very young technology, has already an extremely high security level.

QKD produces a secret key, which then can be used together with some classical cryptographical algorithm to encrypt some information and deliver it. Typically QKD can be used with the One-Time-Pad algorithm, the only mathematically proven secure algorithm, but in practice it can be used also with 3DES or AES, just to mention the most famous symmetric algorithms, obtaining a very secure and reasonably fast communication channel.

6. Bibliography

[1] *Quantum Cryptography Pros & Cons*, Andrea Pasquinucci, http://www.ucci.it/

[2] *The Physics and Technology behind Quantum Cryptography*, Andrea Pasquinucci, to appear on http://www.ucci.it/

[3] *Quantum Cryptography*, N.Gisin, G.Ribordy, W.Tittel, H.Zbinden, *Reviews of Modern Physics,* Vol. 74, p. 145 (2002), http://arXiv.org/abs/quant-ph/0101098 (this is a very technical introduction to Quantum Cryptography)

[4] Some other references can be found for example at http://www.csa.com/hottopics/crypt/overview.html and http://jfi.uchicago.edu/~pelton/reading.html