Chapter 3

Quantum key distribution

One of the first applications of quantum mechanics to the field of information theory has been the 1984 proposal of Bennett and Brassard for a secure protocol to distribute a secret private key that is common to two distant parties. Since then there have been a few other similar protocols and a new field has emerged nowadays called "quantum cryptography". In this chapter we limit ourself to original protocol - now called BB84 - and to a simpler one found by Bennet in 1992 - in a later chapter we will also give the EPR protocol proposed by Ekert in 1991. The general idea of BB84 is as follows. Alice sends a string of classical bits - the secret key - to Bob by using intermediate quantum mechanical Qbits (in pratice these are photons transmitted in optic fibers). Any attempt by Eve to capture some information about the key amounts to *observe* the Qbits and, according to the postulates of QM *this observation will perturb the quantum system.* Alice and Bob are then able to detect this perturbation, thus the presence of Eve, and abort communication.

The subject is in fact more complicated because in reality the channel (the optic fiber) is noisy and it is non-trivial to distinguish Eve from noise. The full proof of security[1] for BB84 requires a combination of non-trivial methods from classical and quantum information theory and is beyond the scope of this course. Here we will analyze only the two basic attacks from Eve, that were originaly considered by Bennett and Brassard, and we will assume the channel is not noisy.

Quantum cryptography is not only a theoretical idea. It is also a truly experimental subject since the protocols have been implemented and shown to work in the laboratory (first at IBM by Bennett et al in 1989 over a distance of 32 cm) and later outside the lab on distances of few tens of kilo-

[1] completed by a number of authors around 1993-1996

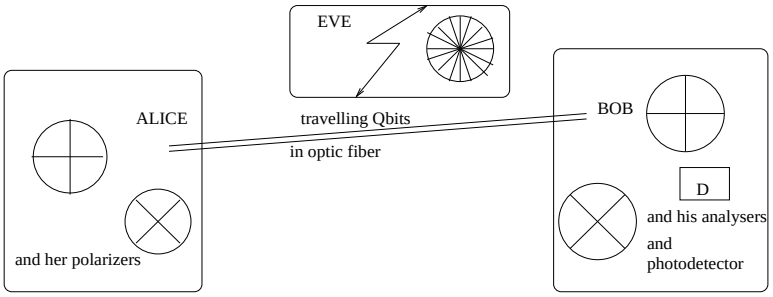

Figure 3.1: Alice and Bob exchange a private key over an optic fiber

meters (Geneva, Los Alamos ...). Nowadays there exist companies proposing commercial systems[2]. These technological implementations require extensive knowledge of optics and will not be discussed here.

3.1 Key generation according to BB84

There are four essential phases: encoding procedure of Alice, a decoding procedure of Bob, a public discussion between the two parties and finaly the common secret key generation.

Encoding procedure of Alice. She generates a classical random binary string $x_1, ..., x_N$, $x_i \in \{0, 1\}$ that she keeps secret (the common key will be a subset of these bits). She also generates a second classical random binary string $e_1, ..., e_N$, $e_i \in \{0, 1\}$ that she keeps secret *for the moment*. Alice then *encodes* the classical bits into Qbits as follows:

- For $e_i = 0$ she generates a Qbit in the state $|x_i\rangle$. Concretely this can be done by sending a beam through a polarizer in the Z basis (figure 1)

  $$\{|0\rangle, |1\rangle\}$$

  If the polarizer is oriented horizontaly (resp. verticaly) only photons in polarization state $|0\rangle$ go through, and if it is oriented verticaly only photons in polarization state $|1\rangle$ go through. A single photon is then selected from the outgoing beam (this of course is an idealisation)

- For $e_i = 1$ she generates a Qbit in the state[*3] $H|x_i\rangle$. Concretely this

[2]Idquantique, MagiQ

[3]We remind the reader that H is the Hadamard matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Figure 3.2: preparation of photons in Z basis

Figure 3.3: preparation of photons in X basis

can be done by sending a photon through a polarizer in the X basis

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

If the polarizer is rotated to the right (resp. verticaly) only photons in polarization state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ go through, and if it is rotated to the left only photons in polarization state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ go through.

Summarizing, Alice sends a string of Qbits $|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$, $i = 1, ..., N$ through a channel (in pratice the channel is an optical fiber).

Decoding procedure of Bob. Bob generates a random classical binary string $d_1, ..., d_N$, $d_i \in \{0, 1\}$ that he keeps secret *for the moment*. He decodes the received Qbits of Alice as follows:

- If $d_i = 0$ Bob performs a measurement of the received Qbits $|A_{e_i,x_i}\rangle$ in the Z basis

  $$\{|0\rangle, |1\rangle\}.$$

  The result of the measurement is

  $$|y_i\rangle \in \{|0\rangle, |1\rangle\}.$$

  and he records the bit y_i. To do this concretely he uses the analyser-detector apparatus described in the first chapter: the analyser is placed horizontaly (figure 3); if the detector clicks this means the photons state has *collapsed* in the $|0\rangle$ state and if the detector does not click, it means that the photon state has collapsed to $|1\rangle$. We stress that, according to the measurement postulate, these outcomes are *truly random* and that only Bob observes them.

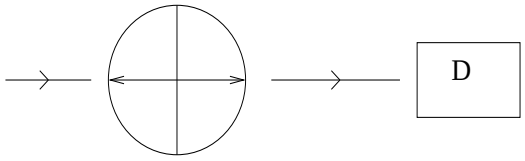

Figure 3.4: measurement of polarization in Z basis

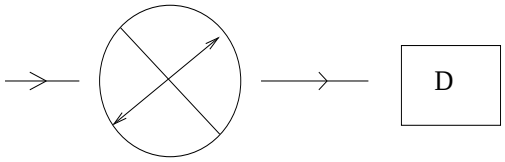

Figure 3.5: measurement of polarization in X basis

- If $d_i = 1$ Bob performs a measurement of the received Qbits $|A_{e_i,x_i}\rangle$ in the X basis
$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle\}.$$
The result of the measurement is in $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ if the output is $H|y_i\rangle$ and he records the bit
$$y_i \in \{0, 1\}$$
To do this concretely he uses the analyser-detector apparatus described in the first chapter: the analyser is rotated to the right (figure 4) at 45 degrees; if the detector clicks this means the photons state has *collapsed* in the $H|0\rangle$ state while if the detector does not click it means that the photon state has collapsed to $H|1\rangle$. We stress again that, according to the measurement postulate, these outcomes are *truly random* and that for the moment only Bob observes them.

In summary Bob has decoded the Qbits sent by Alice to a classical binary string $y_1, ..., y_N$. This string is the outcome of measurements of Bob and cannot be predicted (God does play with dice ... the statistics of these outcomes can however be calculated according to the measurement postulate).

Public discussion. Alice has at her disposal two binary strings: $e_1, ..., e_N$ used to choose the encoding basis, and $x_1, ..., x_N$ that was mapped to Qbits. Bob also has two binary strings: $d_1, ..., d_N$ used to choose a measurement basis and $y_1, ..., y_N$ that are his measurement outcomes.

Alice and Bob compare $e_1, ..., e_N$ and $d_1, ..., d_N$ over a public channel, but keep their two other strings $x_1, ..., x_N$ and $y_1, ..., y_N$ secret. We will see that

it is *important that the public discussion starts only after Bob has finihed his measurements*. They can deduce the following information (and anybody else also can):

- If $d_i = e_i$, i.e. if they used the same basis, then it must be the case that $y_i = x_i$ (the reader should convince himself of that by going through some examples with polarizer, analyser pairs - basicaly if Bob and Alice used the same basis it is as if they lived in a classical world).
- If $d_i \neq e_i$, i.e. if they did not use the same basis, then quantum effects came into play when Bob did the measurement. According to the measurement postulate: $y_i \neq x_i$ with probability $\frac{1}{2}$; $y_i = x_i$ with probability $\frac{1}{2}$. Let us formaly prove this. Bob receives the Qbit

  $$|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$$

  and measures in the basis

  $$\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}.$$

  The outcome will be one of two possibilities

  $$H^{d_i}|0\rangle, \qquad \text{with prob } |\langle 0|H^{d_i}H^{e_i}|x_i\rangle|^2$$

  or

  $$H^{d_i}|1\rangle, \qquad \text{with prob } |\langle 1|H^{d_i}H^{e_i}|x_i\rangle|^2$$

  The reader can check that for $e_i \neq d_i$ both probabilities are equal to $\frac{1}{2}$ (and that for $e_i = d_i$ they are 0 and 1).

Key generation. Bob and Alice erase all bits x_i and y_i corresponding to i such that $e_i \neq d_i$. They keep the remaining substrings of $x_1, ..., x_n$ and $y_1, ..., y_n$ such that $e_i = d_i$. They are assured that these two substrings are equal so this can potentialy constitute the common secret key. The length of this substring is close to $\frac{N}{2}$ since $\text{prob}(e_i \neq d_i) = \frac{1}{2}$. Finaly Alice and Bob perform a security test: according to quantum mechanics for this perfect setting (without noise or Eve) one must have

$$\text{prob}(x_i = y_i | e_i = d_i) = 1$$

Alice and Bob test this by exchanging a small fraction of the common substring over the public channel. If the test succeeds they keep the rest of the common substring secret: they have succeeded in generating a common secret key.

3.2 Attacks from Eve

Here we suppose that there is no noise in the channel so that all errors that Alice and Bob will detect, when performing the security test above, come from attacks of Eve. Furthermore we suppose that Eve may attack by performing operations on one Qbit at a time. We consider two possible attacks : "the measurement" and "unitary" attacks. For each of them we will see that the basic postulates of QM imply that Eve fails.

Measurement attack. Suppose Eve captures a single photon in the optic fiber (this is not very hard in principle: when fibers are twisted enough so that their radius of curvature become small enough some light escapes). The captured photon is in the state

$$|A_{e_i,x_i}\rangle \in \{|0\rangle, |1\rangle, H|0\rangle, H|1\rangle\}$$

and she tries to measure it. We consider a "dangerous" situation where Eve knows that Alice and Bob use the Z and X basis, in other words she knows what the two parties call the vertical axis. But she does not know the successive choices Z or X that Alice and Bob do. If Eve uses the Z basis her outcome is in $\{|0\rangle, |1\rangle\}$ and according to it she records a bit $y_i^E \in \{0, 1\}$. If she uses the X basis her outcome is in $\{H|0\rangle, H|1\rangle\}$ and she records a corresponding bit $y_i^E \in \{0, 1\}$. Once she has finished the measurement she sends the photon to Bob (in the state left over by the measurement) who does not yet know about her presence. Two possibilities may occur:

- Eve uses the same basis than Alice: then her outcome is $y_i^E = x_i$ and the photon state received by Bob is the "correct one",
- Eve uses a different basis than Alice: then her outcome $y_i^E = x_i$ only half of the time, so she sends the "correct" photon state to Bob only half of the time.

Let us see what Alice and Bob find when they perform the security test. Denote by EA the event "Eve uses the same basis than Alice".

$$\begin{aligned}
\text{prob}(x_i = y_i | e_i = d_i) &= \text{prob}(x_i = y_i | e_i = d_i, EA)\text{prob}(EA) \\
&\quad + \text{prob}(x_i = y_i | e_i = d_i, \text{not } EA)\text{prob}(\text{not } EA) \\
&= 1 \cdot \text{prob}(EA) + \frac{1}{2} \cdot (1 - \text{prob}(EA)) \\
&= \frac{1}{2}(1 + \text{prob}(EA))
\end{aligned}$$

where we used

$$\text{prob}(x_i = y_i | e_i = d_i, EA) = 1, \qquad \text{prob}(x_i = y_i | e_i = d_i, \text{not EA}) = \frac{1}{2} \quad (3.1)$$

Assuming that Eve has no information about the basis choices of Alice we take $\text{prob}(EA) = \frac{1}{2}$. Then $\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}$ so that Alice and Bob notice that when they used the same basis about a fourth of their bits do not agree. They conclude that an eavesdropper is at work and abort the communication.

Unitary attack. The problem of Eve is that when she makes a measurement she has no information about the basis that Alice chose. One possible solution would be to copy the travelling Qbits $|A_{e_i,x_i}\rangle$, then let the original state go to Bob, and keep the copy. When Alice and Bob enter in the public discussion phase she learns about the basis of Bob in which to measure the Qbit and thus for i such that $e_i = d_i$ she gets the same outcome as Bob $y_i^E = y_i = x_i$. However the *no-cloning theorem* (which is a consequence of the unitary evolution postulate) garantees that there does not exist a unitary "machine" such that

$$U(|A_{e_i,x_i}\rangle \otimes |\text{blank}\rangle) = |A_{e_i,x_i}\rangle \otimes |A_{e_i,x_i}\rangle$$

The point here is that $|A_{e_i,x_i}\rangle$ is one of

$$\{|0\rangle,\ |1\rangle,\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

which is a set of non-orthogonal states.

Eve could try to use two copy machines: one for copying the two states of the Z basis and another for copying the two states of the X basis. But this time she has no way of knowing which machine to use. She will use the wrong machine half of the time and again Alice and Bob will find that

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}$$

Full proof of security. In a more realistic context there are various problems with the arguments above. First it is very difficult to produce single photons. One produces a very low intensity beam and the photon number is a Poisson random variable with mean related to the intensity. Often more than one photon is produced and Eve might capture a few of these leaving the others to Bob. In this case she doesnt have to copy anything and all she does is wait for the public discussion phase. A second problem is

that Alice and Bob will make errors in their measurements, there is channel noise also and these have to be distinguished from the perturbations inccured by the eavesdropper. A third one is that Eve migth perform operations on many traveling photons at the same time (and not on single ones as assumed above).

In order to deal with such problems one has to add two more phases to the original BB84 protocol. These are called information reconciliation and privacy amplification and are in fact classical protocols that belong to classical coding and information theory.

3.3 The Bennett 1992 scheme

The analysis of BB84 has shown that the security ultimately relies on the fact that Alice encodes Qbits in non-orthogonal states. The B92 scheme retains this very fact and is even simpler than BB84. Below we just sketch the main idea. There are again four main phases:

Alice encodes. Alice prepares a random binary string $e_1, ..., e_N$. She sends to Bob $|A_{e_i}\rangle = |0\rangle$ if $e_i = 0$ and $|A_{e_i}\rangle = H|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ if $e_i = 1$. The encoding is thus $H^{e_i}|0\rangle$.

Bob decodes. Bob generates a random binary string $d_1, ..., d_N$ and measures the received Qbit according to the value of d_i in the Z or X basis and obtains an outcome in $\{|0\rangle, |1\rangle\}$ or in $\{H|0\rangle, H|1\rangle\}$. He decodes the bit as $y_i = 0$ if the outcome is $|0\rangle$ or $H|0\rangle$ and $y_i = 1$ if the outcome is $|1\rangle$ or $H|1\rangle$.

Public discussion. Bob announces over the public channel the bits y_i. Note that when $e_i = d_i$ we have $y_i = 0$ with probability 1. On the other hand when $e_i \neq d_i$ we have $y_i = 0$ with probability $\frac{1}{2}$ and $y_i = 1$ with probability $\frac{1}{2}$. Therefore from the public discussion Alice and Bob deduce that, given $y_i = 1$, surely $d_i = 1 - e_i$.

Key generation. Alice and Bob keep the secret bits $(e_i, d_i = 1 - e_i)$ for i such that $y_i = 1$ and discard the rest. The length of this substring is about $\frac{N}{2}$. they perform a security test on a fraction of the substring on the public channel by checking that

$$\text{prob}(d_i = 1 - e_i | y_i = 1) = 1$$

Again it is not hard to check that this security condition is violated under a measurement or a unitary attack of Eve. If that is the case Alice and Bob abort communication.

3.4 Conjugate coding

In the encoding method of Alice above the two basis that are used correspond to the basis diagonalizing the two Pauli matrices

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.2}$$

These two observables do not commute and are called conjugate observables by analogy with position and momentum; therefore the two basis are sometimes called *conjugate* and the corresponding scheme called *conjugate coding*.

In fact this scheme was first introduced in 1969 by Wiesner then a graduate student. Wiesner, basing himself on the principles of QM, indicated how to "fabricate unforgeable bank notes". Unfortunately nobody took him seriously, except for Bennett then also a graduate student, and his paper didnt get published till*[4] 1983. Bennett was one of the few persons who kept thinking about such problems and, with Gilles Brassard a computer scientist, had the idea to reconsider conjugate coding in the context of cryptography.

Let us briefly explain the original idea of Wiesner. One generates a random binary string $e_1, ..., e_{20}$, and prepares 20 photons in $|0\rangle, |1\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, polarization states using Z or X polarizers. Then one traps the 20 photons in 20 small cavities inside the bank note. The bank note also contains a readable serial number which corresponds to the random string $e_1, ..., e_{20}$. Only the bank knows what is the mapping from the serial number to the binary string.

Suppose somebody attempts to copy the bank note. Because of the no-cloning theorem there is no single machine U which copies simultaneously vertical and diagonal photon polarizations. If one uses two different machines one will make mistakes (with prob $1-2^{-20}$) because one doesnt know when to use a U_Z or a U_X. Moreover the bank can check if a bank note has been forged or not. Indeed from the serial number it deduces the binary string $e_1, ..., e_{20}$ and therefore knows the sequence of basis used to prepare the photons. A measurement in the correct basis (for each little cavity) is done to observe if the photons have the correct polarization. Note that if the bank note has *not* been forged it will *not* be destroyed by such a procedure. To summarize, one may say that the bank knows what exact sequence of analysers to use so that the system behaves classicaly for the bank. For any other person that doesnt possess this information the system behaves quantum mechanicaly.

[4] around 1982 quantum computation came into fashion because of an equaly pioneering work of Feynman

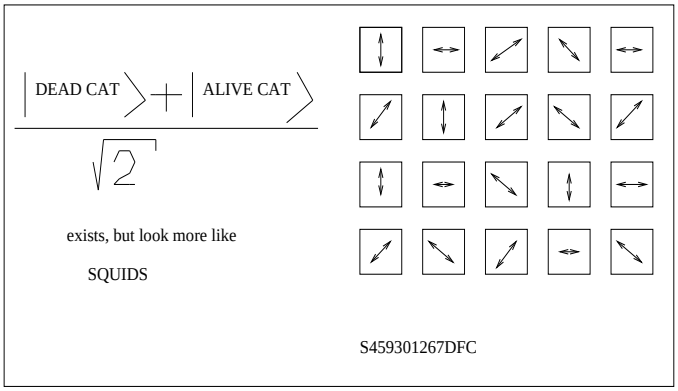

Figure 3.6: unforgeable bank note: it buys one Schroedinger cat