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 key that is common to two distant parties. Since then, there have been a few other similar protocols and a new field has emerged, called "quantum cryptography". In this chapter we limit ourself to the original protocol - now called BB84 - and to a simpler one found by Bennet in 1992. In a later chapter we will also give another protocol proposed by Ekert in 1991, and based on entangled Einstein-Podolsky-Rosen pairs of particles.

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 practice these are photons transmitted in optic fibers). Any attempt by Eve to capture some information about the key amounts to *observe* the Qbits, but 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. Besides the operations performed by Alice and bob are not perfect. The proof of security (see [2]) for BB84 is therefore dependent on precise assumptions on the physical set-up. It involves 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 two basic attacks from Eve, assuming the channel is not noisy and the operations of Alice and Bob are perfect.

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 in 1989 over a distance of 32 cm) and later outside the lab on distances of few tens to hundreds of kilometers

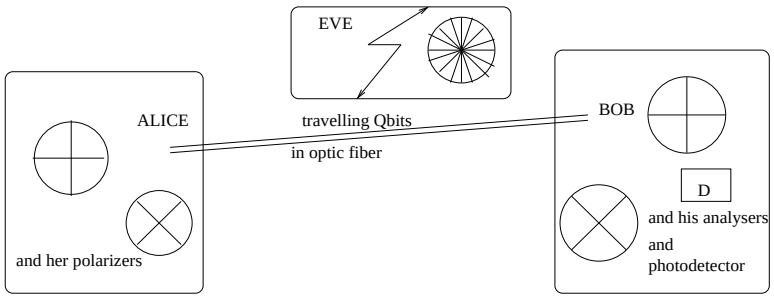

Figure 3.1: Alice and Bob exchange a private key over an optic fiber

(Geneva, Los Alamos ...). See [1] for a general review. Nowadays there exist companies proposing commercial systems[1]. Recent implementations allow the exchange of secret keys over a distance of $100km$ (resp. $250km$) at a rate of 6000 (resp. 15) bits per second [3]. require extensive knowledge of optics and will not be discussed here. Recently the commercial systems have been challenged by a hacking procedure exploiting the physical limitations of photo-detectors on Bob's side [4].

3.1 Key generation according to BB84

There are four essential phases: the encoding procedure of Alice, the decoding procedure of Bob, a public discussion between the two parties, and finally the common secret key generation. Figure 3.1 illustrates the general set-up described below.

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 x_i 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 3.2)

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

  For $x_i = 0$ (resp. $x_i = 1$) the polarizer is oriented horizontally (resp. vertically) and so photons are prepared in polarization state $|0\rangle$ (resp. $|1\rangle$). A single photon is then selected from the outgoing beam (this of course is an idealization)

[1] Idquantique, MagiQ

Figure 3.2: orientations of polarizer for preparation of photons in Z basis

Figure 3.3: orientations of polarizer for preparation of photons in X basis

- For $e_i = 1$ she generates a Qbit in the state*[2] $H|x_i\rangle$. Concretely this can be done by sending photons through a polarizer in the X basis (figure 3.3

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

  For $x_i = 0$ (resp,. $x_i = 1$) the polarizer is rotated to the right (resp. left) and photons are prepared in polarization state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (resp. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$).

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

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

  The photon state after the measurement

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

  is recorded in the bit y_i. To do this concretely he uses the analyzer-detector apparatus described in the first chapter: the analyzer is placed

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

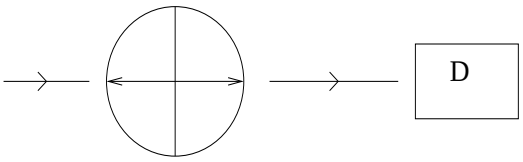

Figure 3.4: analyzer-detector set-up for the measurement of polarization in Z basis

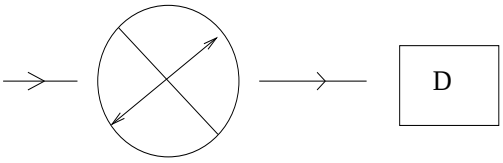

Figure 3.5: analyzer-detector set-up for the measurement of polarization in X basis

horizontally (figure 3.4); 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*. Only Bob knows about them.

- If $d_i = 1$ he 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 photon sate after the measurement is in
$$H|y_i\rangle \in \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$
When the output is $H|y_i\rangle$, and he records the bit y_i.

  To do this concretely he uses the analyzer-detector apparatus described in the first chapter: the analyzer is rotated to the right (figure 3.5) 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 only Bob knows about 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 the 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. *It important that the public discussion starts only after Bob has finished his measurements.* They can deduce the following information (and anybody else hearing the public discussion 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, analyzer pairs - basically 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 genuine quantum effects came into play when Bob did the measurement. According to the measurement postulate: $y_i \neq x_i$ with probability $\frac{1}{2}$ and $y_i = x_i$ with probability $\frac{1}{2}$. Let us formally 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 basis states

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

  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 sub-strings of $x_1, ..., x_n$ and $y_1, ..., y_n$ such that $e_i = d_i$. They are assured that these two sub-strings are identical, so this can potentially constitute the common secret key. The

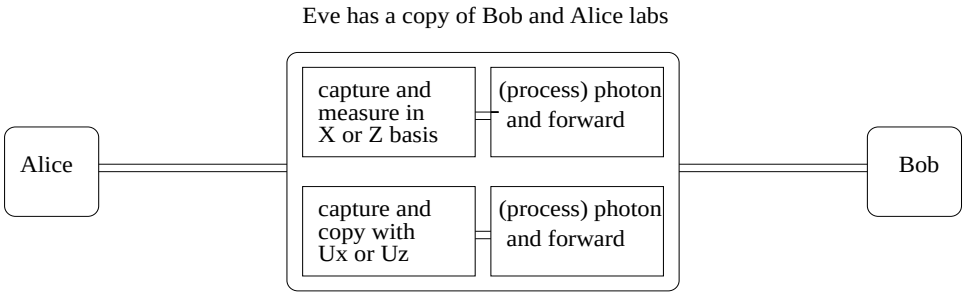

Figure 3.6: Set up of Eve's lab along the optic fiber

length of this sub-string is close to $\frac{N}{2}$ since $\text{prob}(e_i \neq d_i) = \frac{1}{2}$. Finally 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 sub-string over the public channel. If the test succeeds they keep the rest of the common sub-string secret: they have succeeded in generating a common secret key.

3.2 Attacks from Eve

We assume that Alice has a perfect single-photon source, state preparation is perfect, there is no channel noise, Bobs analyzer-detector apparatus makes no detection errors. In summary when Eve is absent communication is error-free, and any error discovered in the security test would come from Eve. Furthermore we suppose that Eve may attack by performing operations on one Qbit at a time on captured photons along the optic fiber and that she has no access to the Alice and Bob's labs. We also suppose that Eve has perfect knowledge of the set-up in Alice and Bob's labs: she knows that they use X and Z basis (but not the successive random basis choices), she knows what is their common vertical and horizontal directions, and the timing of the photons.

We consider two possible attacks : "the measurement" and "unitary" attacks. The two attacks consist of two steps. First Eve captures a photon, and second she forwards the photon to Bob (see figure 3.6). For each attack we will see that the basic postulates of QM imply that Bob and Alice discover the presence of Eve. when this is the case they abort the protocol.

Measurement attack. Suppose Eve captures a single photon in the optic fiber. The captured photon is in one of the the states

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

and she tries to measure it. 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[3]. Two possibilities may occur:

- Eve has used 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.

[3]She could also further process this state by a unitary transformation but this will not improve her performance

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 traveling 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) guarantees 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

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

Discussion of security issues. In the above error-free set-up it is relatively easy to generalize the proof of security in order to take into account any local operation of Eve on single photons. In a more realistic context one has to take into account the fact that the system is noisy. For example the optic fiber is not perfect and the photo-detectors may give false counts. Therefore the string sequences of Alice and Bob do not match perfectly even when $e_i = d_i$. For this reason one adds to the protocol two classical post-processing steps: information reconciliation and privacy amplification. Both steps are carried on the public classical channel. The first step is an error correcting phase while the second allows to reduce the information that Eve might have gained about the key during the correction phase. The detailed analysis is non-trivial and the interested reader may consult the literature [2].

There are various problems that may arise due to physical limitations that do not quite enter into the framework of the security proofs. Recently a successful attack was implemented [4] by exploiting the fact that after a photo-detector click, the detectors enter in a mode were they operate classically. By shining light on them Eve is able to maintain them in a classical mode and in effect the Eve-Bob part of the transmission line is in effect classical. In this Eve can achieve complete control of the key.

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 sub-string is about $\frac{N}{2}$. they perform a security test on a fraction of the sub-string 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*.

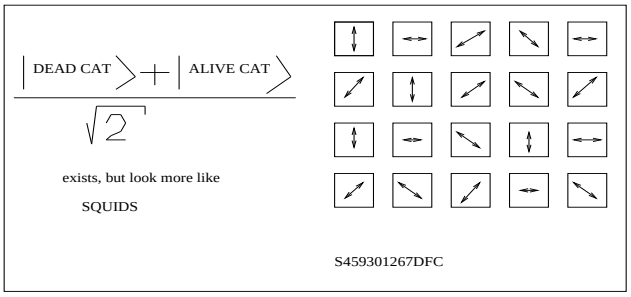

Figure 3.7: unforgeable bank note: it buys one Schroedinger cat

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 didn't 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 binary string $e_1, ..., e_{20}$. Only the bank knows what is the mapping between the serial number and the binary string (see figure 3.7).

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 doesn't 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 basis sequence 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 analyzers to use so that the system behaves classically for the bank. For any other person that does not possess this information the system behaves quantum mechanically.

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

Bibliography

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics, vol 74, (2002) pp. 145-195

[2] D. Mayers, Advances in Cryptology CRYPTO 96, LNCS 1109, p. 343357 (1996); P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, p. 441, (2000); H.-K. Lo, QIC 1, No. 2, pp. 8194 (2001); D. Gottesman and H.-K. Lo, IEEE Transactions on Information Theory, 49, pp. 457475 (2003); K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. 90, 167904, (2003).

[3] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery and S. Ten, *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres*, new Journal of Physics vol 11 (2009) 075003.

[4] I. Gerhardt, Q Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer1 and V. Makarov, *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*, Nature communications 2: 349 (2001) pp. 1-6