Chapter 6

CRYPTOGRAPHY

INTRODUCTION

Secure communication is one of the areas of key importance for modern society in which quantum information transmission and processing seems to be able to bring significant contributions. For example, quantum cryptography may be the main defence against quantum code breaking in the future.

An important new feature of quantum cryptography is that security of quantum key generation and quantum cryptographic protocols is based on a more reliable fact, on the laws of nature as revealed by quantum mechanics, than in the case of classical cryptography, whose security is based on unproven assumptions concerning the computational hardness of some algorithmic problems.

It is difficult to overemphasize the importance of quantum cryptography for an understanding and utilization of quantum information processing. Quantum cryptography was the first area in which quantum laws were directly exploited to bring an essential advantage in information processing.

Closely related are quantum teleportation and quantum superdense coding—special ways of the transmission of quantum or classical information using one of the most puzzling phenomena of the quantum world—non-locality features of the quantum entanglement.

LEARNING OBJECTIVES

The aim of the chapter is to learn:

1. several methods of secret key generation by two parties;
2. a method of multiparty secret key generation;
3. the unconditional security of quantum key generation;
4. the basic quantum cryptographic protocols;
5. the problems related to the security of quantum cryptographic protocols;
6. the main principles, circuits and some applications of quantum teleportation;
7. the quantum superdense coding procedure.

"Amazing, Holmes."
"Elementary, my dear Watson, elementary."

Security of a significant portion of the public-key cryptography and cryptographic protocols in use today depends directly or indirectly on the essential difficulty of either factoring of integers, or computing discrete logarithms. Shor's results therefore indicate that quantum mechanics has the potential to ruin a large part of the contemporary cryptography.[1] That is also a reason why Shor's results were taken as very significant by all those whose well-being can be much influenced by significantly new tools for breaking codes. This is so far also the main reason why quantum computing research finds support in institutions much depending on security of communication.

However, quantum mechanics allows also to design cryptographic systems of a completely new type and thereby also new cryptography—significantly more secure than so far. One can say that quantum cryptography brought a new dimension to security of communications. Its main new feature are mechanisms for detecting eavesdropping. The very basic idea is simple. If classical information is encoded in a special quantum way, for example, with nonorthogonal quantum states, and transmitted, then any attempt of an eavesdropper to access transmitted information spoils, with high probability, information irreversibly in a way which can be detected by the legal receiver. Quantum cryptography provides a technologically feasible approach to harnessing quantum physics for communication and security purposes. In doing that quantum cryptography makes a positive use of fundamental limitations of quantum physics—for example of Heisenberg's uncertainty principle.

While security of classical cryptosystems is based on unproven assumptions of computational complexity (and can be jeopardized by progress in technology, computing theory and algorithmic design), security of quantum cryptographic systems is based on the laws of nature—or at least on basic assumptions of quantum mechanics (such as its completeness).

The idea of quantum cryptography goes back to S. Wiesner around 1970, but it was practically only in 1983 when his ideas received an attention, mainly due to Ch. Bennett. Subsequent development was very fast and already in 1994 transfer of quantum information along an ordinary optic fibre of several kilometers length had been performed.

Interestingly enough, the main reason why quantum cryptography went from science fiction to science in such a short term was not technological progress but the discovery of how to make reasonable use of quantum mechanics for cryptographic purposes.

6.1 Prologue

Quantum cryptography is like classical cryptography, a continuous fight between good and bad. The basic setting is that Alice tries to send a quantum system to Bob and an adversarial eavesdropper, Eve, tries to learn, or to change, as much as possible without being detected.

An eavesdropper has this time an especially hard task. Quantum states cannot be copied and cannot be measured without causing, in general, a disturbance.

The key problem can be formulated as follows (see Fuchs and Peres, 1996). Alice prepares a quantum system in a specific way unknown to Eve and sends it to Bob. The question

[1] Secret-key cryptography, such as DES, has not yet been shown to be efficiently breakable by quantum computing. Whether this can be done is an interesting but hardly practical problem because DES is expected to be obsolete before any quantum computer is built.

is how much information can Eve extract of that quantum system and what the cost of that information is, in terms of the disturbance of the quantum system. Two concepts are therefore crucial here: *information* and *disturbance*.

Let us consider two extreme cases within the scheme that Alice sends a state $|\psi\rangle$ to Bob. The first is that Eve has no information about how $|\psi\rangle$ was prepared. The only thing Eve can then do is to choose some basis $\{|e_i\rangle\}$ of orthonormal states and to use the corresponding projection measurement on $|\psi\rangle$. In such a case $|\psi\rangle$ collapses into one of the states $|e_i\rangle$ and by that the only information Eve has learned is that $|\psi\rangle$ is not orthogonal to $|e_i\rangle$. At the same time $|\psi\rangle$ can get much destroyed.

The second extreme case is that Eve knows that $|\psi\rangle$ is one of the states of the basis $\{|e_i\rangle\}$. In such a case Eve gets, by measuring $|\psi\rangle$ with respect to the basis $\{|e_i\rangle\}$ full information about $|\psi\rangle$ because $|\psi\rangle$ collapses into itself. No disturbance to $|\psi\rangle$ occurs.

The most interesting, important and hard case for quantum cryptography is the third case, where Eve knows that $|\psi\rangle$ is one of the states $|\psi_1\rangle, \ldots, |\psi_n\rangle$ that are mutually nonorthogonal and p_i is the probability that $|\psi_i\rangle$ is the state Alice sends. In this case the question is how much information Eve can get by a measurement and how much disturbance she causes by that.

How to measure information gain of Eve? Shannon entropy $\sum_{i=1}^{n} p_i \lg p_i$ is a measure of her ignorance about the system before the transmission takes place. She can try to decrease this entropy by some measurement. What she gets is called *mutual information*.

In the case of eavesdropping Bob does not get a pure state but a mixed state specified by a density matrix ρ_i for the case Alice sends $|\psi_i\rangle$. The **disturbance** detectable by Bob is given by $D = 1 - \langle\psi_i|\rho_i|\psi_i\rangle$.

An important case is that $n = 2$, $p_1 = p_2$ and $|\psi_1\rangle$ and $|\psi_2\rangle$ are states of H_2 such that a measurement of $|\psi_b\rangle$ with respect to $|\psi_{\bar{b}}\rangle$ produces both states with the same probability. In such a case Eve has a 50% chance to make a correct guess for her measurement. In the case of the correct guess she gets $|\psi\rangle$ for 100%, otherwise for 50%. In the average she gets 75% of information. Can she do better? By doing some other measurements? As we shall see in this chapter, she can get up to 85% of information but not more, no matter what she does. This may sound pretty good, but not enough for cryptography, as we shall see.

Of course, when Alice sends a sequence of states Eve has also other options for eavesdropping than to try to measure immediately, one-by-one each sent state. For example, she can postpone measurements to the end of the transmissions.

In such a general case the problem of Eve's information gain versus disturbance is one of the central one for security of quantum cryptography protocols.

How to send quantum states in general and qubits in particular is another general problem. Transmission of polarized photons is so far one of the basic tools in quantum cryptographic protocols for sending qubit states.[2] The main property to be used is that if a θ-polarized photon is subjected to a polarization measurement along axis ϕ, it behaves like a ϕ-polarized photon with probability $\cos^2(\theta - \phi)$ and like a $(\phi + 90)^\circ$-polarized photon with probability $\sin^2(\theta - \phi)$. Moreover, such a measurement can be performed by using a ϕ-oriented piece of birefringed material, such as calcite, to split the incoming light beam into two beams (polarized at ϕ and $\phi + 90^\circ$).

[2] For more about polarization of photons see Section 9.1.2 and 9.2.6.

6.2 Quantum Key Generation

Quantum secret key generation discussed next is so far the most important application of quantum mechanics to cryptography. A secret key can be generated by several parties. The most important case is that of two parties.

6.2.1 Basic ideas of two parties quantum key generation

One of the main problems of cryptography is the so-called **key distribution problem**. How can two parties, Alice and Bob, come into the possession of a secret key in such a way that the third party, an eavesdropper Eve, cannot acquire useful information about the key.

Indeed, the main idea of the classical **secret key cryptography** is to use cryptosystems S in which both **encrypting algorithms** e_S and **decrypting algorithms** d_S are publicly known and if two parties, Alice and Bob, want to be engaged in a secure communication, then they have to share a **secret random key** k. With the key k the **encryption** of a **plaintext** w and the **decryption** of a **cryptotext** c are performed by the computations

$$c = e_S(k, w) \quad \text{and} \quad w = d_S(k, c).$$

This way such well-known and practically important cryptosystems as DES and ONE-TIME PAD work. The second cryptosystem is **perfectly secure** under the assumption that each key has the same length as the plaintext w and each time the cryptosystem is used with a new randomly chosen key. In the case of binary plaintexts and keys the encryption and decryption algorithms of ONE-TIME PAD cryptosystem are very simple

$$c = k \oplus w \quad \text{and} \quad w = k \oplus c,$$

where $\oplus$ stands for a component-wise exclusive-or operation. (Observe that using ONE-TIME PAD cryptosystem we need one secret bit to transfer securely one bit—quite a price.)

Since the search for limitations concerning security is also one of the main tasks of the quantum computing research, let us look a bit more closely into the problem in which sense ONE-TIME PAD cryptosystem is perfectly secure. Let $\mathbf{w}$ and $\mathbf{c}$ be random variables for plaintexts and cryptotexts. ONE-TIME PAD cryptosystem is perfectly secure in the sense that $Pr(\mathbf{w}|\mathbf{c}) = Pr(\mathbf{w})$, or, equivalently $Pr(\mathbf{c}|\mathbf{w}) = Pr(\mathbf{c})$.

Exercise 6.2.1 *Show why it is necessary for the security of ONE-TIME PAD cryptosystem to require that each key is used only once.*

Classical cryptography can therefore be so much secure, how secure key distribution methods are available.

The main practical importance of **public key cryptography** is therefore for key distribution. It provides **computationally secure** key distribution under some unproven assumptions of computational complexity. For example, on the assumption that no polynomial time algorithm exists for integer factorization.

In the classical setting no unconditionally secure key distribution is possible. On the other hand, as discussed in this and the next section, unconditionally secure key generation is possible, with respect to our current knowledge of quantum physics, using communications through quantum channels.

In the classical setting we speak about the key distribution because the basic scheme is that one party (Alice) sends (distributes) the key to the other party (Bob) in a secure way. In quantum setting we speak about quantum key generation (QKG) because in such a process both parties play a more symmetrical role, and only in the course of their communication do they generate (or agree on), a secret key.[3]

Quantum key generation can be done in such a way that

- no eavesdropper can obtain, with non-negligible probability, the transmitted key,
- any attempt of an eavesdropper to obtain a transmitted key can be detected (with as large probability as needed),
- both parties can be as sure as needed that they share a secret key.

Any interception by an eavesdropper is actually a set of measurements on the communication channel. Classical key distribution can in principle be passively monitored (no matter how difficult this may be technologically), without the legitimate users being aware that any eavesdropping has taken place. On the other hand, quantum cryptography provides means to detect any attempt of an eavesdropper to tap the channel.

Protocols

The basic idea behind key generation is simple. If Alice and Bob want to share a binary key of length n, then each of them first generates independently a private random binary sequence of length $m \gg n$. In order to extract from this random sequence a common key of length n, Alice prepares a sequence of m tokens, one type for bit 1 and another type for bit 0 and sends through a sequence of such tokens her random sequence to Bob. Bob reports to Alice the order, but not the value, of those of Alice's bits that are the same as his. From this sequence of bits they select n bits, say the first n.

The idea is simple but not secure in the classical setting because Eve can tamper transmissions and read Alice's tokens and Bob's report.

In the quantum setting the above idea can be implemented in such a way that its security is based on the following basic principle of quantum mechanics.

1. Non-orthogonal states cannot be copied.[4]
2. Any measurement of states can change them, with high probability, irreversibly and can create a significant and detectable rate of errors.

The quantum version of the basic idea for key generation goes as follows. Alice sends Bob a sequence of photons randomly polarized. Bob measures them using a randomly chosen basis. This necessarily disturbs some of the photons. Any eavesdropping by Eve introduces additional disturbance. After all transmission of photons Alice and Bob determine, in a public communication, the amount (probability) of eavesdropping. If it is not too much, they select from the sent and received photons a shared secret key.

Three QKG protocols are discussed in the following. All of them are both historically and practically of importance.

---

[3] In the literature, for historical reasons, the term "quantum key distribution" (QKD) is mostly used even though the term "quantum key generation" is more logical.

[4] Encodings with a nonorthogonal set of states, for example $\{|0\rangle, |1\rangle, |0'\rangle, |1'\rangle\}$ were first used by Wiesner (1983) to suggest money that could not be counterfeit without detection. The idea is simple, The bank embeds qubits, randomly chosen from a nonorthogonal set into the bank notes and puts notes into circulation, keeping the record which quantum states were embedded into notes. When a note returns to the bank its qubit is meausred, according to the record. If there was no attempt to counterfeit the note, the readout corresponds to the record and, in addition, the embedded state is not disturbed. (The main problem with this idea, not solved yet, is how to store qubits for a long time.)

1. Protocol BB84, or 4-state protocol, with encodings and decodings based on the existence of two non-commuting observables (Bennett and Brassard, 1984). BB84 has been the first fully successful attempt to exploit quantum laws to obtain a fundamental advantage in information processing.

2. Protocol E91 with encodings based on quantum entanglement (Ekert, 1991).

3. Protocols B92, or 2-state protocol, with encodings based on two non-orthogonal states (Bennett, 1992).

6.2.2 Security issues of QKG protocols

The security of QKG protocols is interesting, important and a very complex problem, both practically and theoretically. The ultimate aim is to achieve unconditional security, i.e., to develop QKG protocols that withstand all attacks quantum mechanics allows, according to our current knowledge of it. It is far from easy to determine how secure are particular QKG protocols. Several security claims in the past were found later to be wrong.

Problems concerning security of quantum cryptographic protocols brought up new fundamental questions concerning quantum information processing. For example, how much information can be measured from a quantum system for a given amount of expected disturbance? All such questions are of fundamental importance and not only for quantum cryptography.

Security problem

The aim of a QKG protocol is to allow two parties, Alice and Bob, that share no information initially, to share a secret key (a binary string) at the end.

There are two potential obstacles to overcome. First, the communication channel between Alice and Bob can be noisy and faulty (some photons can get lost). Second, communication during the key extraction phase has to be assumed to be performed "before the eyes" of Eve, who can do her best to achieve that Alice and Bob do not meet their aim. (Eve can try to learn the key Alice and Bob generate, or at least to get some information about it. She can also try to achieve that at the end of the generation protocol Alice and Bob actually do not share the same key.)

We shall not consider here the case that Eve can just disrupt communication between Alice and Bob. We shall consider only the more difficult case that Eve tries to meet her aims without being detected. We shall also not consider the case that Eve tries to alter public communication between Alice and Bob or to pretend to be one of those parties. Alice and Bob can use some authentication protocols for communication, to avoid such an interference.

We shall also consider the worst case, the usual one for cryptography, that Eve knows which protocol is used. All she does not know is the private random keys of the parties.

What are the means Eve can use to achieve her goals? First observe she cannot be only a passive eavesdropper because the key is extracted only from bits Bob receives. She cannot "tap" quantum transmissions. A single photon cannot be split and no quantum system can clone nonorthogonal quantum states. Therefore it would seem that the only thing Eve can do is to measure transmitted states (according to one of the observables Bob uses[5]) and then forward to Bob the states she gets as results of her measurement. In such a case, as already discussed, she has a 25% chance to make an error. (As a consequence, if Alice sends

[5]It is assumed that Eve knows the protocol and therefore observables Bob can use.

n bits and Eve measures all, then there is only a $(\frac{3}{4})^n$ chance that there will be no error introduced by her. For the case $n = 100$ there is therefore probability only $3 \cdot 10^{-13}$ that no error will be introduced by Eve.) However, this is not the whole story. There are various attacks/measurements she can make.

Several types of attack have been identified so far. The two extreme types are the following ones.

1. **Intercept–reset attacks**. Eve tries to learn as much as possible from particular transmissions of Alice, qubit by qubit (photon by photon) using von Neumann measurements.

2. **Coherent** or **joint attacks**. Instead of measuring the particles while they are in transit from Alice to Bob, one–by–one, Eve regards all the transmitted particles as a single entity. She then couples this entity with a simple auxiliary system (ancilla), prepared in a special state, and creates the compound system. Afterwards, she sends the particles to Bob and keeps the ancilla. After the end of the public interactions between Alice and Bob (for error detection, error correction and privacy amplification), Eve extracts from her ancilla some information about the key. Such attack are directed against the final key. They represent the most general type of attacks that is possible. (However, no particular attack of this type has been suggested so far.)

Error rate

In practice eavesdropping is not the only source of errors in transmission. Imperfections of source, channels and detectors may also produce errors, usually up to a few per cent. The number of such errors, as a fraction of the total number of detected bits, is called the **quantum bit error rate**, and it is one of the parameters that characterizes how well a transmission system works.

When a noisy channel is used to transmit quantum states the problem is to detect eavesdropping. One way out for Alice and Bob is first to calculate the likely error rate caused by a noisy channel, and then to consider the real error rate to be suspicious if it is higher than estimated. Of course this is not a very secure method. Usually the best is to assume the worst case, namely that all errors are due to an eavesdropper.

Test for eavesdropping and errors

What kind of tools do Alice and Bob have to detect an eavesdropping or/and errors? They can, for example, measure the key generation rate and the error rate in a portion of extracted keys and they can make some tests of randomness of the extracted key (for example 0/1 bias). However, in order to make a mathematical proof of unconditional security of some QKG protocols a much more general view of testing methods they can use is needed. This will be discussed later in this chapter.

Secure key generation

The basic method is straightforward.[6] From the set of extracted bits Bob chooses, randomly, a subsequence, sufficiently large, and makes it public. Alice compares these bits with her and if the error rate is too large, they conclude that an eavesdropping took place and they

[6] We assume again that Alice and Bob need an n bit key but Alice starts the protocol by transmitting $m \gg n$ photons.

repeat the key generation protocol. Otherwise, the remaining part of the extracted bits form the key they generate. Details of the method depend on the degree of security Alice and Bob want, or need, to achieve.

Error correction

One way to deal with the problems of noisy channels and faulty detectors is for Alice to first encodes the sequence she wants to transmit using an error correction code.

Privacy amplification

Privacy amplification is a tool developed by Bennett, Brassard and Robert (1988) to select a short and very secret binary string s from a longer but less secret string s'.

The main idea is simple. If $|s| = n$, then one picks up n random subsets $S_1, \ldots, S_n$ of bits of s' and let s_i, the ith bit of S, be the parity of S_i. One way to do it is to take a random binary matrix of size $|s| \times |s'|$ and to perform multiplication Ms'^T, where s'^T is the binary column vector corresponding to s'.

The point is that even in the case where an eavesdropper knows quite a few bits of s', she will have almost no information about s.

More exactly, if Eve knows parity bits of k subsets of s', then if a random subset of bits of s' is chosen, then the probability that Eve has any information about its parity bit is less than $2^{-(n-k-1)}/\ln 2$.

Of particular importance is the case that a linear error correcting code is used to encode at first the transmitted sequence and then a syndrome of it is distributed by public channel. In such a case if Eve knows already t bits of s', and if no more than $n-t-r-1$ bits are given to Eve as the syndrome of s', where r is a security parameter, then the expected amount of information Eve knows on the parity of a random subset of bits of s' is less than $\frac{2^{-r}}{\ln 2}$.

6.2.3 Quantum key generation protocols BB84 and B92

Protocols BB84 and B92 will be described in terms of Hilbert space constructs and illustrated using transmissions of single photons randomly polarized. Protocols BB84 and B92, for generation of a key of length n, have several phases:

Preparation phase

BB84 protocol. Alice generates independently two private random binary sequences of length $m \gg n$ bits and Bob generates one such private sequence of random bits.

B92 protocol. Both Alice and Bob generate their two private random binary sequences of length m.

Quantum transmission phase

Assumptions: Alice is assumed to have four transmitters of photons in one of the following four polarizations—$0, 45, 90$ and 135 (or -45) degrees—in the case of BB84 protocol (see Figure 6.1a); and in one of two polarizations—90 and 135 degree—in the case of B92 protocol (see Figure 6.1b).[7]

[7]Expressed in a more general form, Alice uses for encoding states from the set $\{|O\rangle, |1\rangle, |0'\rangle, |1'\rangle\}$a in the case of the BB84 protocol and staes from the set $\{|0\rangle, |1' \; rangle\}$ in the case of the B92 protocol.

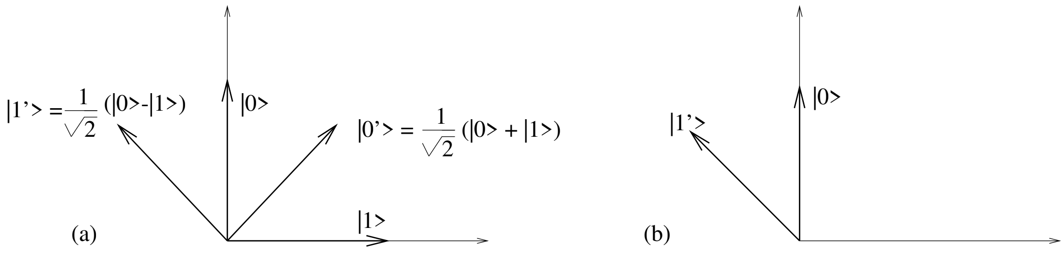

Figure 6.1: Polarizations of photons for BB84 and B92 protocols

In accordance with the laws of quantum physics Bob has a detector that can be set up to distinguish between rectilinear polarizations (0 and 90 degrees) or can be quickly reset to distinguish between diagonal polarizations (45 and 135 degrees). However, again in accordance with the laws of quantum physics, there is no detector that could distinguish between unorthogonal polarizations. In a more formal setting, Bob can use either the standard observable $\mathcal{B} = \{|0\rangle, |1\rangle\}$ or the dual observable $\mathcal{D} = \{|0'\rangle, |1'\rangle\}$, discussed on page 44, to measure the incoming photon.

Transmissions

BB84 protocol: To send a bit 0 (1) of her first random sequence through a quantum channel[8], Alice chooses, on the base of her second random sequence, one of the encodings $|0\rangle$ or $|0'\rangle$ ($|1\rangle$ or $|1'\rangle$), i.e., the standard or dual basis, and sends the photon of the corresponding polarization.

It is assumed here and in the following that photons are sent one by one in regular intervals. As a consequence Bob knows when some photon does not get through and the order index of all received bits.

Bob chooses, each time on the base of his private random sequence, one of the observables $\mathcal{B}$ or $\mathcal{D}$ to measure the photon he is to receive. Bob records the results of his measurements and keeps them secret. Observe that there are three situations Bob can encounter: photon is not received, Bob uses the correct basis (with respect to Alice's choice) for his measurement, and Bob uses the incorrect basis for measurement.

Figure 6.2 shows the possible results of the measurements and their probabilities. When Bob guessed correctly the polarization chosen by Alice he obtained for 100% the same bit as Alice had sent. However, when Bob failed to guess polarization, and did not used the corresponding observable, he obtained the correct result only with probability $\frac{1}{2}$. An example of an encoding–decoding process is in the Figure 6.3.

B92 protocol. Alice uses encodings $0 \rightarrow |0\rangle$ and $1 \rightarrow |1'\rangle$ and sends each bit by a photon in one of the two nonorthogonal states.

Bob chooses, on the base of his random sequence, observable $\mathcal{D}$ for 0 and $\mathcal{B}$ for 1, and checks whether the photon he has received was polarized as $|0'\rangle$ or $|1\rangle$.[9] He records the results of his measurements and keeps them secret.

---

[8] Quantum channel is a transmission medium that isolates the quantum state from interactions with the environment.

[9] Yes, this way, this is not an error. It has a perfect sense.

Alice's encodings	Bob's observables	Alice's state relative to Bob	the result and its probability	correctness
$0 \to \|0\rangle$	$0 \to \mathcal{B}$	$\|0\rangle$	0 (prob. 1)	correct
	$1 \to \mathcal{D}$	$\frac{1}{\sqrt{2}}(\|0'\rangle + \|1'\rangle)$	0/1 (prob. $\frac{1}{2}$)	random
$0 \to \|0'\rangle$	$0 \to \mathcal{B}$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	0/1 (prob. $\frac{1}{2}$)	random
	$1 \to D$	$\|0'\rangle$	0 (prob. 1)	correct
$1 \to \|1\rangle$	$0 \to \mathcal{B}$	$\|1\rangle$	1 (prob. 1)	correct
	$1 \to \mathcal{D}$	$\frac{1}{\sqrt{2}}(\|0'\rangle - \|1'\rangle)$	0/1 (prob. $\frac{1}{2}$)	random
$1 \to \|1'\rangle$	$0 \to \mathcal{B}$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	0/1 (prob. $\frac{1}{2}$)	random
	$1 \to D$	$\|1'\rangle$	1 (prob. 1)	correct

Figure 6.2: Quantum cryptography with BB84 protocol

1	0	0	0	1	1	0	0	0	1	1	Alice's random sequence
$\|1\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0'\rangle$	$\|1\rangle$	$\|1'\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1'\rangle$	Alice's polarizations
0	1	1	1	0	0	1	0	0	1	0	Bob's random sequence
$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	Bob's observable
1	0	R	0	1	R	0	0	0	R	R	outcomes

Figure 6.3: Quantum transmissions in the BB84 protocol—R stands for the case that the result of the measurement is random

Table 6.4 shows the possible results of the measurements and their probabilities. Where the corresponding bits of their random sequences are different, the test fails with probability 1. Otherwise, it fails with probability $\frac{1}{2}$. An example of an encoding/decoding procedure is in Figure 6.5.

Exercise 6.2.2 *Could we modify B92 protocol in such a way that Bob makes test not for $O'\rangle$ and $1\rangle$ but for $|0\rangle$ and $|1'\rangle$ or for $|0\rangle$ and $|1\rangle$?*

Basic key extraction phase

BB84 protocol: Bob makes public the sequence of observables he used to measure the photons he received—but not the results of the measurements—and Alice tells Bob, through a classical channel, in which cases he has chosen the same basis for observable as she did for encoding. The corresponding bits then form the basic key both parties agree on.

Alice's bit	Alice's encoding	Bob's bit	Bob's test for	Test's result and probability	Correctness
0	$\|0\rangle$	0	$\|0'\rangle$	Yes/No (prob. $\frac{1}{2}$)	random
		1	$\|1\rangle$	No (prob. 1)	correct
1	$\|1'\rangle$	0	$\|0'\rangle$	No (prob. 1)	correct
		1	$\|1\rangle$	Yes/No (prob. $\frac{1}{2}$)	random

Figure 6.4: Encodings/decodings with B92 protocol

1	0	0	0	1	1	0	0	0	1	1	Alice's random seq.
$\|1'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$	Alice's polarizations
0	0	1	1	0	1	1	0	0	1	0	Bob's random sequence
$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{D}$	Bob's observables
No	R	No	No	No	R	No	R	R	R	No	outcomes of test

Figure 6.5: Quantum transmissions within B92 protocol

B92 protocol: Those bits for which Bob's tests don't pass he takes as the key being extracted and reports their positions to Alice through a public channel.

B92 protocol is simpler because only two polarizations of photons are used and that is why this protocol is sometimes said to be the "minimal protocol" for QKG.

The basic description of the BB84 and B92 protocols is by that finished. In the following we describe a more involved test for errors and a more involved protocol for key extraction in the case of the BB84 protocol. This will be used later when discussing unconditional security of the BB84 protocol. The basic ideas presented below (see Mayers and Yao, 1998), are of a general importance for making quantum key generation protocols more robust to the noise of various types.

Test for errors

Denote by $A_{\mathcal{B}}$ and $B_{\mathcal{B}}$ vectors of the bases Alice and Bob have chosen, respectively, and by A_b (B_b) the sequences of bits Alice sent (Bob got as the outcomes of his measurements).

The test is done with respect to the following two parameters Alice and Bob had to agree on before the transmission:

δ —tolerated error rate,

β —key extraction parameter.

1. Bob makes public the vector $B_{\mathcal{B}}$ (but not B_b). Alice lets Bob know the set $T = \{i \mid A_{\mathcal{B}}[i] = B_{\mathcal{B}}[i]\}$ of those cases where Bob chose the correct basis (and therefore he should get the same bit Alice sent).

2. Bob chooses randomly a set R of $\frac{n}{2}$ indices $i \in [1, 2, \ldots, n]$ and makes public the set $\{(i, B_b[i]) \mid i \in T \cap R\}$. Alice verifies whether the number of positions $i \in T \cap R$ such that the number of $A_b[i] \neq B_b[i]$ is smaller than $\delta\frac{|T|}{2}$. If not, they stop the key generation process because of the suspiciously large rate of errors. Otherwise, they continue to find out whether there are still enough bits to use for key extraction.

3. Alice and Bob verify whether $|T \cap R| \geq \bar{n} = (\frac{1}{4} - \beta)n$. If this is not the case, the protocol is stopped. The parameter β is needed to make sure, using Chernoff's bound[10] that $|T - R| \geq \bar{n}$ with probability larger than $(1 - e^{-2\beta^2 n})$.

4. If $|T - R| \geq \bar{n}$, a set E of size $\bar{n}$ is randomly chosen from the set $T - R$.

[10] **Chernoff's bound.** Let $X_1, \ldots, X_n$ be independent Bernoulli variables and $S = \sum_{i=1}^{n} X_i$. If $Pr(x_i = 1) = p_i$ for $1 \leq i \leq n$, then for all $0 < \varepsilon \leq 1$ it holds: (a) $Pr(S - pn \leq -\varepsilon n) \leq e^{\frac{-n\varepsilon^2}{2n}}$; (b) $Pr(S - pn \leq -\varepsilon n) \geq e^{\frac{-n\varepsilon^2}{3n}}$.

Final key extraction

The set E is used to extract the key.[11] To do that two procedures are used: one for error correction, the second for privacy amplification.[12] The procedure for error correction is needed to correct errors among bits in the strings $A_b[E] = \{A_b[i] \mid i \in E\}$ and $B_b[E] = \{B_b[i] \mid i \in E\}$. The privacy-amplifying procedure is used to reduce the chance that Eve could make use of the few bits she could learn.

When Alice uses a linear code to encode her randomly chosen sequence of bits, she computes and sends to Bob the syndrome $s = F \cdot A_b[E]$, where F is an $r \times \bar{n}$ parity check matrix—see Section 7.4.1—of the chosen linear code. Bob uses the syndrome s to correct errors in $B_b[E]$ to get exactly $A_b[E]$. As the outcome, Alice and Bob share a common key $A_b[E]$.

As the last step, a privacy-amplifying procedure is used. For example, a random binary matrix K of dimension $m \times \bar{n}$ is used and $K \cdot A_b[E]$ is computed to yield the final common key of the length m.

Efficiency improvements

Protocols BB84 and B92 were presented above in their most basic form. Several generalizations, modifications and improvements have already been developed (see Brassard, 1994, and Brassard and Crépeau, 1996, for older references). For example, B92 protocol can be based on any two nonorthogonal states $\cos\theta|0\rangle + \sin\theta|1\rangle$ and $\cos\theta|0\rangle - \sin\theta|1\rangle$. Bruß (1998) explored the security and efficiency of a generalized BB84 protocol in which three bases have been used: classical, dual and circular.

A modification of the BB84 protocol that can almost double its efficiency was developed by Ardehali et al. (1998). The basic idea behind such an increase of efficiency is very simple and will now be presented.

In the original BB84 protocol, as presented above, both Alice and Bob choose their bases with equal probabilities. As a consequence in about 50% of the cases Bob uses a different polarization than Alice and therefore about 50% of polarized photons are discarded.

Two modifications were suggested in the protocol developed by Ardehali et al. (1998).

To select the basic key Alice chooses her polarizations with probabilities p and $1-p$ and Bob with probabilities p' and $1-p'$, $0 < p, p' < 1$. If $p \neq \frac{1}{2} \neq p'$ this creates a larger probability that the same basis is used for encoding and for measurement. This way efficiency can be in the limit doubled, to approach 100%.

To make the protocol secure a refined error analysis is used. Instead of creating one sequence of agreed-upon bits and computing a single error rate, two sequences are created: one if both of them use the rectilinear polarization; the other for the case where they use the diagonal polarization. The error rate is considered small if it is small for both of these sequences.

[11] Observe that key is extracted only from those bits Bob received. This fact makes such QKG protocols robust against losses during transitions.

[12] Error correction is used mainly to protect transmissions against errors due to imperfections of the quantum channel and Bob's detectors. In such a case Alice does not transmit to Bob a randomly chosen sequence of bits but Alice first encodes her random sequence of bits using a linear error correcting code both Alice and Bob agree on beforehand.

6.2.4 Multiparty key generation

There are various applications at which several parties need to possess a secret key. One approach to such a multiparty key generation, that works even in the case of one unreliable party, due to Hillery, Bužek and Berthiaume (1998), will now be presented.

At first the story: Alice, Bob and Charles want to generate a common secret key and Alice knows that one of the other two is not to be trusted, but she does not know which one. In addition, she knows that if the other two act together then the honest one can make the second one behave properly.

Assume that Alice, Bob and Charles share three particles P_a, P_b and P_c in the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and each of them measures her (his) particle with respect to the randomly chosen basis (either the standard basis $\{|0\rangle, |1\rangle\}$, or the dual basis $\{|0'\rangle, |1'\rangle\}$ or the circular basis $\{|0''\rangle, |1''\rangle\}$). Since $|\psi\rangle$ can be expressed in any of the following four ways:

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{8}}((|0'\rangle|0'\rangle + |1'\rangle|1'\rangle)(|0\rangle + |1\rangle) + (|0'\rangle|1'\rangle + |1'\rangle|0'\rangle)(|0\rangle - |1\rangle)) \\
&= \frac{1}{\sqrt{8}}((|0'\rangle|0''\rangle + |1'\rangle|1''\rangle)(|0\rangle - i|1\rangle) + (|0'\rangle|1''\rangle + |1'\rangle|0''\rangle)(|0\rangle + i|1\rangle)) \\
&= \frac{1}{\sqrt{8}}((|0''\rangle|0'\rangle + |1''\rangle|1'\rangle)(|0\rangle - i|1\rangle) + (|0''\rangle|1'\rangle + |1''\rangle|0'\rangle)(|0\rangle + i|1\rangle)) \\
&= \frac{1}{\sqrt{8}}((|0''\rangle|0''\rangle + |1''\rangle|1''\rangle)(|0\rangle - |1\rangle) + (|0''\rangle|1''\rangle + |1''\rangle|0''\rangle)(|0\rangle + |1\rangle)),
\end{aligned}
$$

once Alice and Bob make their measurements of the first two qubits, the state of Charles particle is uniquely determined. If Charles measures his particle, then from the outcome he can deduce whether Alice and Bob used for their measurements the same basis or not. In addition, a knowledge of the bases they used allows him to determine whether their outcomes were the same or not.

Observe also that if Alice and Bob use the same (different) basis for their measurements and Charles uses the dual basis (circular basis), then he gets his outcome with probability 1 (probability $\frac{1}{2}$, i.e. randomly).

Let us now assume that all three of them make public which of the bases they used for their measurements (but not the results of their measurements). If Charles's basis is not the one that provides the correct measurement, as happens 50% of times if he chooses his basis randomly, then they discard the measurements outcomes and repeat the process. Otherwise, if Charles's choice of measurement is a proper one, then from his outcome he knows whether the results of Alice's and Bob's measurements were the same or not.

Moreover, by exchanging the outcomes of their measurements, Bob and Charles can determine the outcome of Alice's measurement and then that result can be taken as specifying the bit all three of them agree on.

However, we know that either Bob or Charles can be dishonest. In order to deal with this problem the announcement of the choices of the bases should be done as follows: First both Bob and Charles send their bases for measurement to Alice and then she sends all of them to both Bob and Charles. This ensures that neither Bob nor Charles, the one who is dishonest, postpones his choice of the bases until he learns which bases were chosen by Alice and the other one.

Exercise 6.2.3 *(a) Verify the first of the following decompositions and complete the second one.*

$$\begin{aligned}|000\rangle + |111\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + (|0\rangle - |1\rangle)(|00\rangle - |11\rangle) \\ &= \frac{1}{2}(|0\rangle + i|1\rangle)(?...?)\end{aligned}$$

(b) Show that

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2}[e^{-i\pi/4}(|0'\rangle|0''\rangle + |1'\rangle|1''\rangle) + e^{i\pi/4}(|0'\rangle|1'\rangle + |1'\rangle|0''\rangle)].$$

(c) Show that in the following cheating scheme for the multiparty key generation, the probability of error is 25%. Bob succeeds to get Charles's particle. Alice measures her particle using either the dual or the circular basis. Bob measures his two particles either in $(|00\rangle \pm |11\rangle)/\sqrt{2}$ basis or in the $(|00\rangle \pm i|11\rangle)/\sqrt{2}$ basis and after that he sends one particle to Charles. Both Bob and Charles measure now their particles with respect to either the dual or the circular basis.

6.2.5 Entanglement-based QKG protocols

In 1991 A. Ekert discovered a new type of QKG protocols, security of which is not based on Heisenberg's uncertainty principle, as in the case of BB84 and B92 protocols, but on the completeness of quantum mechanics. Completeness (see Section 9.1.8), here means that quantum mechanics provides maximum possible information about any quantum system and an eavesdropping can then be seen as "an introduction of some elements of physical reality (see Section 9.1.7), to the measurement" (see Ekert, 1991). To each specific entanglement-based QKG protocol a (generalized) Bell inequality is formed and by a statistical test of this inequality, on the basis of probability statistics on rejected data, it is possible to determine whether eavesdropping took place. (Eve plays here the role of a hidden variable and disturbs the quantum nature of the correlations between probabilities of occurrence of various outcomes for various measurements.)

In the following we first describe a general scheme of entanglement-based QKG protocols, then two examples, and finally we demonstrate how entanglement-based protocols can be reduced to protocols which do not use entangled pairs of particles and security of which is not based on the Bell theorem.

Protocols

1. **Preparation phase.** Alice chooses three vectors $\alpha_1, \alpha_2, \alpha_3$ in H_2 and Bob vectors β_1, β_2 and β_3, also from H_2, such that they have at least one vector in common.

2. **Key generation phase.** A source produces a sequence of maximally entangled states (say maximally entangled pairs of photons), for example in the state

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

and sends one particle of each pair to Alice, second to Bob.

Both Alice and Bob measure their particles with respect to one of the randomly chosen vectors of their sets of vectors.

Both Alice and Bob make public sequences of vectors they used for measurements. From the outcomes of measurements obtained using the same vector for measurements they establish the common key.

3. **Test for eavesdropping.** How secure is the above protocol? Eve has no chance to get some information about the key from the particles while they are in transit because there is no information encoded there. She has two possibilities:

   (a) To measure one or both particles on their way from the source to Alice and Bob and by that to disturb the protocol and to ensure that Alice and Bob do not share at the end a common key.

   (b) To substitute her own, carefully prepared, particles for those generated by the ideal source.

Let us discuss at first the case of eavesdropping. If vectors α_1, α_2 and α_3 and β_1, β_2 and β_3 are properly chosen, then one can design the so-called generalized Bell inequality which can be used to detect eavesdropping. Bell inequality uses as its parameters values $Pr(C,i,b)$–the probability that the party C (Alice or Bob) gets by measuring with respect to the ith vector the value $b \in \{0,1\}$.

Bell inequality is formed in such a way that it is violated if there is no eavesdropping and satisfied if there is an eavesdropping.

Examples

Example 6.2.4 (Ekert, 1991) *The source emits spin-$\frac{1}{2}$ particles in the state* $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. *Alice performs her measurement with respect to the angles* $0°$, $45°$, $90°$ *and Bob with respect to angles* $45°$, $90°$ *and* $135°$.

Denote $E(i,j,b_1,b_2)$ *the probability that if Alice measures with respect to vector* α_i, *Bob with respect to* β_j, *then Alice (Bob) gets as the outcome* b_1 (b_2). *Let us also denote*

$$E(i,j) = E(i,j,1,1) + E(i,j,0,0) - E(i,j,1,0) - E(i,j,0,1).$$

In such a case quantum mechanics requires that for

$$E(1,1) - E(1,3) + E(3,1) + E(3,3) = S$$

it holds $S = -2\sqrt{2}$ *but if an eavesdropping introduces an element of physical reality, then it holds*

$$-2 \leq S \leq 2.$$

Example 6.2.5 (Phoenix and Townsend, 1995) *The source emits pairs of photons linearly polarized in the state* $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, *where* $|0\rangle$ ($|1\rangle$) *corresponds to the vertical (horizontal) polarization. Both Alice and Bob perform measurement with respect to the bases corresponding to polarizations* $\{0°, 90°\}$, $\{30°, 120°\}$ *and* $\{60°, 150°\}$.

Denote by $D(i,j)$ *the difference between probabilities of obtaining a different outcome and the probability to obtain the same outcome if Alice uses* i*th basis and Bob uses* j*th basis for measurement and let*

$$B = 1 + D(2,3) - |D(1,2) - D(1,3)|.$$

From quantum mechanics one derives $B = -\frac{1}{2}$ *and Bell inequality is* $B \geq 0$.

Entanglement protocols seem to be very different from BB84 and B92 protocols. However, this is not really so. Bennett, Brassard and Merman (1992) showed that a simplified version of such a protocol, in which both Alice and Bob randomly choose for their measurement 0° or 90°, is actually equivalent to the BB84 protocol. In addition, as shown by Barnett and Phoenix (1993) and Phoenix and Townsend (1995), and as will be illustrated below, one can have with only one particle a protocol equivalent to an entanglement-based protocol which has the same level of security.

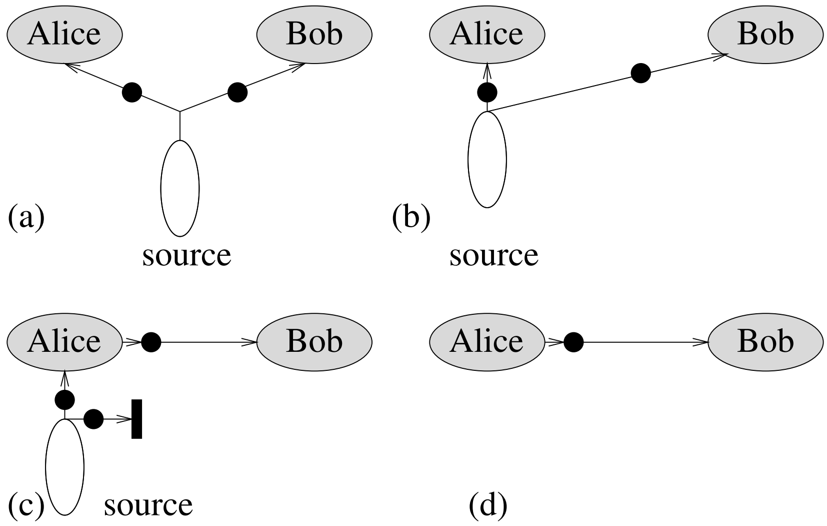

Figure 6.6: Entanglement-based QKG protocols without entanglement

The basic setting discussed above is illustrated in Figure 6.6a. A far-away source of the maximally entangled particles sends one photon of each pair to Alice and the second to Bob, and they perform their measurements. The same protocol can be used and the same claim about security and Bell inequality holds, if the source of photons is in Alice's environment (see Figure 6.6b), or if the second particle is not sent to Bob, (see Figure 6.6c), but after Alice's measurement she makes a copy of the to-be-Bob particle in the corresponding state (Alice knows this state after her measurement) and sends it to Bob who performs a measurement on it. Again the same holds about Bell inequality and its validity as in the original case. Now it is evident that Alice actually does not need at all entangled particles. She can randomly choose one of the six possible states Bob's original particle could be in[13] and she can send the particle in such a state to Bob—see Figure 6.6d.

Similarly as in the case of BB84 and B92 protocols, the question arises whether one can have entanglement-based protocol secure even in the case of noise and eavesdropping. Entanglement purification technique introduced in Section 8.3.2 is a way to deal with these problems.

6.2.6 Unconditional security of QKG*

Once the first QKG protocol was designed, the problem of unconditional security of QKG protocols was approached by a variety of authors and with respect to a variety of assumptions

[13]As the consequence of the possibility for Alice to choose one of the three measurement bases.

concerning the tools the key generating parties and also the eavesdroppers can use. Step-by-step proofs covered a larger and larger range of situations. This process culminated with the so-called unconditional security proof due to Mayers (1998) and Mayers with Yao (1998). We discuss here the main ideas, methods and results of their approach.

Concerning the environment, it is assumed that the initial coding into quantum channel is perfect, i.e., Alice has a perfect source of photons. The case of a less perfect source will be discussed later. Concerning the detector, it is only assumed that whether or not the received system (photon) is detected is independent of the observable used to measure the system.

Security criteria

Two security criteria are considered: the **privacy criterion** and the **security against tampering criterion**. Privacy means that the eavesdropper cannot learn the key, no matter what she does. More exactly, that the eavesdropper is able to obtain only negligible information (less than one bit), about the final key. Security against tampering means that the eavesdropper cannot make Alice and Bob believe that they share a secret key if they do not.

Usually, Alice and Bob perform a test and decide accordingly whether or not they share a secret key. If the result of the test is negative the key generation process is repeated. A very general view of the test will be used in the following —anything Alice and Bob consider to decide whether or not they share a secret key. Denote by $\mathcal{P}$ such a test.

In the formal definitions of the security criteria we use the concept of a quantity Q_n which is **exponentially small**. By that is meant that there are $c, \varepsilon > 0$, such that $Q_n \leq c2^{-\varepsilon n}$ for almost all n. (n will be used in this context as a security parameter. For example, the number of qubits to be transmitted.)

Definition 6.2.6 *A key generation protocol is secure against tampering if the joint probability that each test P defined above is fulfilled and the keys of Alice and Bob are different is exponentially small.*

The basic idea of the privacy criterion defined below is that whatever Eve's attack is, information i she can gather is such that either the test P is not passed or i has negligible value.

To be more formal, let $\mathbf{k}$ be the random variable values of which are potential keys and $\mathbf{i}$ the random variable each value of which is an information i Eve can obtain either from the public communication or through her measurements of the transmitted qubits. For a particular key k, let $Pr(k)$ be the probability Alice and Bob generate the key k and let $Pr(i|k)$ be the probability Eve gathers information i if the key generated has the value k. The formal definition is based on the concept of the "noninformative information" of Eve.

Definition 6.2.7 *Let $0 \leq \theta < 1$. The information i of Eve is θ-noninformative if there exists a real number p such that for every key k*

$$|Pr(i|k) - p| \leq \theta Pr(k). \tag{6.1}$$

In addition, $N_\theta(i)$ will denote the event that the information i of Eve is θ-noninformative.

The basic idea behind the inequality 6.1 is that the difference $Pr(i|k) - p$ should be small. However, $Pr(i|k)$ itself is small and therefore it would not be sufficient to ask only that $|Pr(i|k) - p|$ is small. It is needed that this difference is small even with respect to small $Pr(k)$.

Definition 6.2.8 *A key generation protocol is secure with respect to privacy, if there are two exponentially small positive real numbers γ and θ such that $Pr(P \cap \overline{N_\theta(i)}) \leq \gamma$.*

Informally, Definition 6.2.8 says that except with the probability θ, Eve's activity cannot be such that the test P pass and Eve obtains "informative" information.

A variety of other security criteria have been investigated. Those presented above seem to be strong enough. They take into consideration all known types of attacks including coherent attacks. The development of these criteria has been a significant step that allows to study the idea of "unconditional security" of QKG protocols.

Security requirements

It has been shown, as discussed below, that QKG protocol BB84 is secure and its security holds:

1. against all attacks of an eavesdropper allowed by quantum mechanics—this is the so-called **unconditional security**;
2. against imperfections of the channel and of the detectors.

Main result

In order to illustrate some proof methods we show first security against tampering of a special version of BB84 protocol with the following two properties.

1. The set T has size exactly $\frac{n}{2}$. (This can be achieved if Bob first stores all received photons and only after Alice announces $A_{\mathcal{B}}$, Bob chooses $B_{\mathcal{B}}$ such that the set T has the size $\frac{n}{2}$).
2. When the size of $T - R$ is not large enough, the protocol does not stop and the error correction is done on all bits with indices in $T - R$.

Lemma 6.2.9 *For every $\varepsilon > 0$ and $\delta > 0$, it holds*

$$Pr(P \wedge \bar{\mathcal{E}}) \leq \mu(\varepsilon),$$

where $\mathcal{E}$ is the event that the Hamming distance on bits with indices in $T - R$ between A_b and B_b is smaller than $(\delta + \varepsilon)\frac{n}{4}$ and

$$\mu(\varepsilon) = e^{\frac{-n\varepsilon^2}{32(\delta + \frac{\varepsilon}{2})}}.$$

Proof is based on the fact that the set R is random and remains secret until Alice's quantum transmissions are over. Eve is therefore not able to distinguish between the sets $R \cap T$ and $R - T$ when an error is created. We can therefore consider as fixed the sequences $A_{\mathcal{B}}$, $B_{\mathcal{B}}$, A_b and B_b, and therefore also T. Let $e = A_b \oplus B_b$.

The rest of the proof is based on the fact that the weight of $e(T)$ (see Section 7.4.1), namely $w(e(T))$, is either larger or smaller than $(\delta + \frac{\varepsilon}{2})\frac{n}{2}$. In the first case, the probability that P holds is small. In the second case, the probability that $\bar{\mathcal{E}}$ holds is small. In both cases, the probability that $P \wedge \bar{\mathcal{E}}$ holds is small, as required.

Case 1. $w(e(T)) \geq (\delta + \frac{\varepsilon}{2})\frac{n}{2}$. The test P was defined in such a way that P holds only if $w(e(T \cap R)) \leq \frac{\delta n}{4}$. R is constructed in such a way that every $i \in T$, and also every i with $A_b[i] \neq B_b[i]$, belongs to $T \cap R$ with probability $\frac{1}{2}$. Therefore, each of the $(\delta + \frac{\varepsilon}{2})\frac{n}{2}$ errors is in $T \cap R$ with probability $\frac{1}{2}$. According to Chernoff's bound (see footnote, page 223), the number of errors in $T \cap R$ is smaller than

$$\left[\frac{1}{2} - \frac{\varepsilon}{4(\delta + \frac{\varepsilon}{2})}\right](\delta + \frac{\varepsilon}{2})\frac{n}{2} = \frac{\delta n}{4}$$

with the probability less than $\mu(\varepsilon)$.

Case 2. $w(e(T)) < (\delta + \frac{\varepsilon}{2})\frac{n}{2}$. In this case it follows from Chernoff's bound that the number of errors in $T - R$ is greater than

$$\left[\frac{1}{2} + \frac{\varepsilon}{4(\delta + \frac{\varepsilon}{2})}\right](\delta + \frac{\varepsilon}{2})\frac{n}{2} = (\delta + \varepsilon)\frac{n}{4}.$$

□

Lemma 6.2.9 sounds very technical. Less formally it says that only with the exponentially small probability it may happen that the test P succeeds on $R \cap T$ and yet the number of errors in $T - R$ is greater than $(\delta + \varepsilon)\frac{n}{4}$. This further implies that if an adequate error-correcting technique is used, then Eve cannot succeed to make Alice and Bob believe that they share the key if they do not.

The main result about security of BB84 protocol, proven by Mayers and Yao (1998a) has the following form.

Theorem 6.2.10 *Let* $\varepsilon, \varepsilon' > 0$ *and*

$$\gamma = \left[\frac{e^{-4\beta^2 n}}{1 - e^{-2\beta^2 n}} + 2e^{\frac{(4\beta-1)n\varepsilon^2}{32(\delta+\varepsilon/2)}}\right]^{\frac{1}{2}}.$$

Security against tampering*: The probability that the test P passes and there is more than $(\delta + \varepsilon)\bar{n}$ errors in E is smaller than γ^2.*

Security with respect to privacy*: If*

$$m + r \leq [1 - H(2(\delta + \varepsilon)) - \varepsilon'] \cdot \bar{n},$$

where $H(x)$ is Shannon entropy of x and the matrix K (used for privacy amplification), is random, then with probability at least $1 - 2^{-\varepsilon' \bar{n}}$ we get K such that

$$I(\mathbf{i}, \mathbf{k}') \leq \frac{2\eta}{\ln 2} + m\gamma,$$

where $\mathbf{k}' = \mathbf{k} \oplus \mathbf{w}$ and w is a random string chosen by Alice and announced to Bob, $I(\mathbf{i}, \mathbf{k}')$ is mutual information and $\eta = 2^m(2\sqrt{\gamma} + \gamma)$.

Remark 6.2.11 Theorem 6.2.10 is both a significant achievement and a questionable result. Technically, it is correct. The problem is only whether such a complicated result fully justifies its interpretation as "the ultimate proof of unconditional security of the BB84 protocol". Because of its very complex claim and dependence on several parameters, it is unlikely that the result will be fully accepted soon by the whole quantum computing community as a final step concerning the unlimited security of the BB84 protocol. At the same it is unclear whether a significantly simpler, more elegant and equally powerful proof is possible.

Security of the BB84 protocol and the quality of the photon source

Unconditional security of the BB84 protocol was obtained only under the assumption that there is a perfect source of photons. It is known that imperfect sources may seem to behave quite normally and, at the same time, seriously compromise security of the BB84 protocol. The security problem for an imperfect source is a difficult problem to deal with. An interesting and promising step in this direction was done by Mayers and Yao (1998a). They proposed a concrete design for a new concept of a **self-checking source**. It is required, from the manufacturer of a photon source, to provide certain tests designed in such a way that if they pass, then the source is guaranteed to make the BB84 protocol secure.

6.2.7 Experimental quantum cryptography

Experimental QKG has been based so far mainly on the BB84 and B92 protocols. However, Ekert's idea (1991) to use non-locality has also received attention, as a principally different approach to QKG, especially after the development of quantum purification techniques. They allow one to exchange imperfect quantum entanglement through a noisy channel and then to distil from it almost perfect entanglement (see Deutsch et al. 1996, Bennett et al. 1996b). A survey of other approaches to QKG can be found in Brassard and Crépeau (1996).

The first experimental quantum bit transmission by photons, in a tube over a distance of 32 cm, was done in 1989 (see Bennett and Brassard, 1989, and Bennett et al. 1992). A series of longer distance experimental transmissions of qubits by photons followed soon. Marand and Townsend (1995) reported transmission over 30 km of commercial optical fibre in the same room. Muller, Zbinden and Gisin (1995) reported transmissions using optical cable below Lake Geneva over the distance of 22.7 km, with bit error 3.4%. The experiments with outdoor transmissions culminated so far in the transmissions over an outdoor optical path of almost 1 km (Buttler et al. 1998), with error rate 1.5% in night-time. (The key problem is the quality of the transmission and detection of single photons against a high background through a turbulent medium; because of the presence of background photons and difficulties of directing photons into a remote detector, this problem was considered of immense difficulty.) On the base of these experiences QKG between a ground station and a satellite in a low-earth orbit seems to be feasible (Buttler et al. 1998).

Photons seem to be the best medium to carry qubits. They are relatively easy to produce and photons of certain wavelength can be sufficiently reliably transmitted using existing optical fibres. They are also quite well detected. Photons of wavelength 1.3μ m can travel 10 km in a fibre before half of them get absorbed. This should be enough to perform QKG in local networks. (Unfortunately amplifiers cannot be used. This follows from "No-cloning theorem".) However, one could use "quantum repeaters" (see Briegel, 1998).

In the experimental quantum state transmissions two main methods of encoding of quantum states by photons are through polarization of photons (using photons of shorter wavelength) and through photon's phase. (The last set-up was used by BT (British Telecom) (see Phoenix and Townsend, 1995) and in Los Alamos National Laboratory (see Hughes, 1995).)

A practically very useful technique to realize QKG protocols was introduced by Bennett (1992). The technique uses a Mach–Zehnder interferometer. Alice and Bob each controls one of the phase modulators on one of the arms of the interferometer. Encoding and measurements are done by setting the corresponding phase modulator. We describe very briefly the basic ideas only for the BB92 and BB84 protocols. For implementation details see Hughes et al. (1995).

An interferometric implementation of the QKG scheme for B92 protocol is shown in Figure 6.7. Alice has a single photon source that she can use to send photons into a Mach–Zehnder interferometer, in which she controls the phase ϕ_A along one of the optical paths. Bob has a single photon detector at one of the interferometer's outputs and controls the phase ϕ_B along the other optical path. (In Figure 6.7 we indicate the phases corresponding to Alice's and Bob's random bits.) The probability that a photon sent by Alice is detected by Bob is

$$P = \cos^2(\frac{\phi_A - \phi_B}{2})$$

and it depends on both paths. If Alice and Bob use the phase angles $(\phi_A, \phi_B) = (0, \frac{3\pi}{2})$ for their 0-bits, and $(\phi_A, \phi_B) = (\frac{\pi}{2}, \pi)$ for their 1-bits, we get the situation the B92 protocol requires.

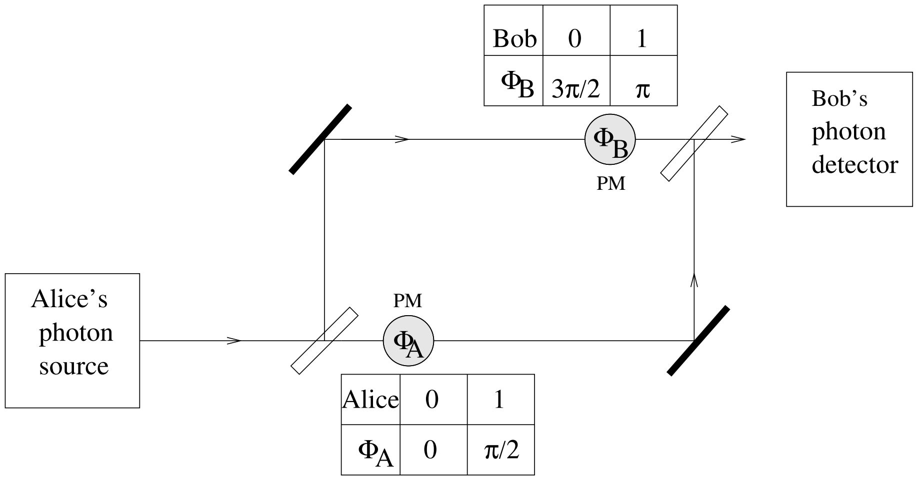

Figure 6.7: B92 protocol implementation

In the case of the BB84 protocol, both Alice and Bob use identical Mach–Zehnder interferometers with one path longer than the other (see Figure 6.8), and a phase modulator (PM) on the shorter path. In order to send a random bit Alice randomly adds, through her PM, a phase shift of 0, $\frac{\pi}{2}$, π or $\frac{3\pi}{2}$, to her photon. Bob can add only phase shifts 0 or $\frac{\pi}{2}$. By adding 0 ($\frac{\pi}{2}$) shift, Bob can detect whether Alice's phase has a phase shift 0 or π ($\frac{\pi}{2}$ or $\frac{3\pi}{2}$). If shifts 0 and $\frac{\pi}{2}$ are interpreted as 1 and other two as 0, we get a basic setting for the BB84 protocol.

Both theoretical and experimental work proceeds also to develop multiuser quantum cryptographical networks. Biham, Huttner and Mor's (1996) approach makes a use of non-locality and assumes a quantum memory is kept in a transition centre to which users "bring their particles". An approach of Phoenix et al. (1995) uses optical networks and has been experimentally tested, see also Phoenix and Townsend (1995).

From experimental to practical quantum cryptography

Progress in two areas seems to be of key importance for quantum cryptography to go from the experimental stage to practical developments: reliability and transmission rate. While

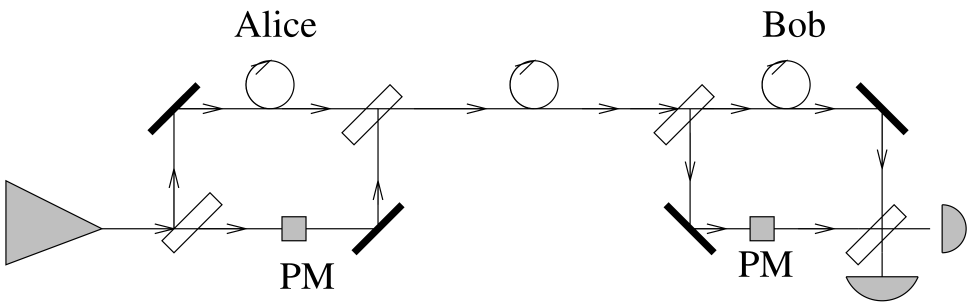

Figure 6.8: Mach–Zehnder interferometer implementation of BB84 protocol, adapted from Tittel et al. (1998a)

the progress in the first area is already significant, transmission rate is still an issue. The highest transmission rate of 1.2 MHz so far exhibited the system tested by BT.

Moreover, in order to succeed for quantum cryptography as a fully competitive method of secure data transmission, it seems that quantum cryptography must be capable of implementation on multiuser optical quantum networks.

6.3 Quantum Cryptographic Protocols

Cryptographic protocols are specifications how two parties, say Alice and Bob, should prepare themselves for a communication and how they should behave during a communication in order to achieve their goal and be protected against an adversary (Eve). It is assumed that parties involved in a protocol know and follow it fully. Two parties participating in a protocol may want to share their secrets in order to compute some value, generate jointly random numbers, convince each other of their identity, simultaneously sign a contract or participate in a secret voting. Cryptographic protocols that accomplish such tasks have radically changed our views of what mutually distrustful parties can accomplish over networks.

A variety of interesting and important classical cryptographic protocols have been designed (see Schneier, 1996, Gruska, 1997). Three of them are of a special importance because they are often the crucial ingredients of more sophisticated protocols.

In the **coin-flipping protocols**, Alice and Bob can flip coin over a distance ("by phone") in such a way that neither of them can determine the outcome of the flip but both can agree on the outcome in spite of the fact that they do not trust each other.

In the **bit commitment protocols** (BCP), Alice can choose a bit and **get committed** to it in the following sense. Bob has no way of knowing what Alice has chosen, and Alice has no way of changing her commitment once she has made it; say after Bob announces his guess as to what Alice has chosen.

Design of a BCP consists of two procedures *commit*(x) and *open*(x) that have the following properties.

If Alice has a bit b in mind to which she wants to commit herself, then she can, through the procedure *commit*(b), provide Bob with a piece of evidence that she has the bit b in her mind to which she commits herself. *commit*(b) should be such that Bob has no way to use it to get b. At a later time, if needed, Alice can use the protocol *open*(b) to reveal x and to prove to Bob that the information she sent, as the consequence of the procedure *commit*(b), really corresponds to that bit.

Alice can choose the probability distribution for b before her commitment process starts. The commitment obtained after the procedure *commit*(b) is realized is said to be **binding** if Alice cannot change the distribution of the probability for b, and it is called **concealing** if Bob cannot obtain any information about b without Alice's help. The commitment is **secure** if it is both binding and concealing. The commitment is **unconditionally secure** if it is secure against any cheater, Alice or Bob, with unlimited computational power.

An example of a "pre-computer era" BCP is that Alice writes her commitment on a piece of paper, locks it in a box, sends the key to Bob and, in the opening phase, she sends also the box to Bob. A "complexity era" solution is that Alice chooses a one-way function f and an integer x, say even for the commitment "1" and odd, otherwise, and then sends to Bob $f(x)$ and f.

There are two types of the oblivious transfer protocols (OTP). In the **1-out-of-2 oblivious transfer protocols** (due to Even et al. 1983), Alice transmits two messages, m_1, m_2, to Bob who can choose whether to receive m_1 or m_2, but cannot learn both, but Alice has no idea which message Bob chosed to receive.

In the **standard oblivious transfer protocols**, in short oblivious transfer protocols, due to Rabin (1981), Alice can send a message to Bob in such a way that Bob receives the message with probability $\frac{1}{2}$ and a garbage (no information) with probability $\frac{1}{2}$. Moreover, at the end Bob knows whether he got a message or garbage, but Alice has no idea which of them Bob has received.

It has been shown by Crépeau (1987) that both types of OTP are equivalent in the sense that either of them can be implemented from a primitive that implements the other.

From the practical point of view, there is one essential difference between QKG protocols and protocols for coin-flipping, bit commitment and oblivious transfer. The first ones are of practical interest only for longer distance transmissions; the other three have perfect sense also for short distances.

In the classical setting using an oblivious transfer protocol one can design a bit commitment protocol and with it a coin-flipping protocol. The reversed reductions are believed to be impossible. OTP are therefore very significant protocols in spite of the fact that at the first glance they look almost like a bizarre idea.

Exercise 6.3.1 *Show how to design a bit commitment protocol once an oblivious transfer protocol is given.*

None of the classical BCP and OTP is absolutely secure. Their computational security is always based on some unproven assumptions of the computability theory.

The history of cryptographic protocols started with the following Blum's coin-flipping protocol (1981):

Protocol 6.3.2 (Coin-flipping by telephone)

1. *Alice chooses two large primes p, q, sends Bob $n = pq$, and keeps p, q secret.*

2. *Bob chooses a random number $y \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and sends Alice $x = y^2 \bmod n$.*

3. *Alice computes four square roots $(x_1, n - x_1)$ and $(x_2, n - x_2)$ of x. (Alice can compute them because she knows[14] p and q.) Let $x_1' = \min\{x_1, n - x_1\}$, $x_2' = \min\{x_2, n - x_2\}$. Since $y \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor)\}$, either $y = x_1'$ or $y = x_2'$. Alice then guesses whether $y = x_1'$*

[14] See, for example, Gruska (1997).

or $y = x'_2$ and tells Bob her choice (for example, by reporting the position and the value of the leftmost bit in which x'_1 and x'_2 differ).

4. Bob tells Alice whether her guess was correct (head) or not correct (tail).

Later, if necessary, Alice can reveal p and q, and Bob can reveal y.

Blum's coin-flipping protocol has actually been also the first non-trivial example of the bit commitment protocol. In the field of the classical cryptographic protocols BCP play an important role. For example, with such a protocol one can construct zero-knowledge proofs for a variety of statements.[15]

6.3.1 Quantum coin-flipping and bit commitment protocols

Also the history of quantum cryptographic protocols started with the following coin-flipping protocol by Bennett and Brassard (1984).

Protocol 6.3.3 (Quantum coin-flipping protocol) *—see Figure 6.9*

Alice's random bits	1	0	1	1	0	1	1	0	0	1	1
Alice polarization choice						rectilinear					
photons sent	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
Bob's observable	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$
Bob's table for $\mathcal{B}$	1			1			1		0	1	
Bob's table for $\mathcal{D}$		1	1					0			0
Bob's guess of Alice's pol.						rectilinear					
Alice's message						you WON					
Alice's original bits	1	0	1	1	0	1	1	0	0	1	1
comparison with $\mathcal{B}$	Y			Y			Y		Y	Y	
comparison with $\mathcal{D}$		N	Y					Y			N

Figure 6.9: Illustration of a quantum coin-flipping protocol

1. Alice randomly chooses a sequence of bits (for example 1000 should be enough) and a polarization (rectilinear or diagonal—standard or dual). Finally, Alice sends the resulting sequence of the polarized photons to Bob.

2. Bob chooses, for each received photon, randomly, an observable, $\mathcal{B}$ or $\mathcal{D}$, and measures the incoming photon. He records the result into two tables—one for the observable $\mathcal{B}$ and the second for the observable $\mathcal{D}$. Since some photons can get lost during the transmissions, there can be holes in both tables. At the end of all transmissions, Bob makes a guess whether Alice chose rectilinear or diagonal polarization and announces his guess to Alice. He is to win if the guess is correct and to lose otherwise.

3. Alice tells Bob whether he won or lost by telling him the polarization she chose. She can certify her claim by sending Bob the random sequence of bits she chose at Step 1.

[15] Actually for the whole class **IP** (see, for example, Gruska, 1997).

4. Bob verifies Alice's claim by comparing his records in the table for the basis she claims to choose. There should be a perfect agreement with the entries in that table and no correlation with the other table.

Can Alice or Bob cheat? Bob is not able to cheat. Indeed, he would be able to cheat only in the case he would be able to determine, with probability larger than $\frac{1}{2}$, on the base of the sequence of photons he received, which polarization Alice has chosen. However, it can be shown (see, for example, Glaubner, 1988), that any measuring device capable to distinguish polarization from the stream of incoming photons, could be used, together with the EPR phenomenon, to transmit information faster than light.

Alice has two possibilities to cheat: either at Step 1 or at Step 3. Let us first discuss the second case. The only way she could cheat is by sending a sequence of bits that would match entries of Bob's table for others from the two possible polarizations (in our example for the diagonal one). However, she has no way to find out the results of the measurements Bob made using his observables, because they were just randomly chosen. She can only guess, but the probability of making correct guesses gets exponentially small with length of the transmitted sequence and, consequently, the probability that her cheating could be discovered approaches fast 1.

Alice also cannot cheat at Step 1 by sending a mixture of diagonally and rectilinearly polarized photons. In such a case, almost certainly, she would not be able in Step 3 to ensure that the sequence of bits she sent agrees with any of Bob's tables. However, there is a special way Alice can cheat in Step 1—by making a clever use of the entangled photons.

In Step 1, instead of sending a sequence of photons polarized in one way or another, she produces pairs of polarization-entangled photons, each pair in the state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, sends to Bob one member of each pair, and stores the other one. After Bob announces his guess in Step 2, she measures her photons in the opposite basis as was Bob's guess. By that she receives a sequence of bits perfectly correlated with Bob's table corresponding to the basis he did not choose as his guess in Step 2 and completely uncorrelated with the other table. She then announces the sequence in Step 3.

The cheating Alice can do this way is theoretically perfectly acceptable. However, practical problems with storing entangled photons for a longer period are large. Moreover, every error in this process could result, with high probability, in an error Bob could discover and that would make him, at least, suspicious about the whole process.

Quantum bit commitment protocols

The coin-flipping protocol presented above has actually been the first quantum bit commitment protocol published. An important further step in developing QBCP was protocol BCJL, due to Brassard, Crépeau, Jozsa and Langlois (1993), an improvement to the protocol due to Brassard and Crépeau (1991), which played an important role in our understanding of the problems of security of the cryptographic protocols.

In order to describe the BCJL protocol we need to describe its subprotocols *commit* and *open*. The protocol *commit* uses, as a parameter, an $\varepsilon > 0$—an upper bound on the error rate of the quantum channel. ε is the probability that an encoded bit b is decoded as $\bar{b}$.

Protocol 6.3.4 (*commit*(x))

1. Bob chooses a Boolean matrix G as a generator matrix (see Section 7.4.1), of a binary linear (n, k, d)-code C such that $\frac{d}{n} > 10\varepsilon$ and $\frac{k}{n} = 0.52$ and announces it to Alice.

2. Alice chooses:

   (a) a random string r of length n and announces it to Bob;

   (b) a random k-bit vector s, such that $r \cdot c = x$, where $c = sG$;

   (c) a random sequence b of length n of the polarizations, $\mathcal{B}$ or $\mathcal{D}$, and sends to Bob a sequence of n photons with the polarization of the ith photon $P_{b_i}(c_i)$, where $P_0(0) = 0°$, $P_0(1) = 90°$ and $P_1(0) = 45°$, $P_1(1) = 135°$.

3. Bob chooses a random string b' of n bits and measures the ith photon according to the basis $M(b_i')$, where $M(0) = \mathcal{B}$ and $M(1) = \mathcal{D}$. Let c' be the n-bit vector where c_i' is the result of the measurement of the ith photon.

Alice keeps the bit x and vectors c and b secret, until the opening takes place, and Bob keeps vectors b' and c' secret.

To open the commitment x, Alice initiates the following protocol:

Protocol 6.3.5 (*open* (c, b, x, c', b'))

1. Alice sends c, b and x to Bob.

2. Bob verifies that c is a codeword of C and computes $B = \sum_{\{i \mid b_i' = b_i\}} \frac{c_i \oplus c_i'}{n/2}$, in order to verify that the error rate is under the limit of those pairs of outgoing and measured bits that were polarized/measured by the same basis.

3. if $B < 1.4\varepsilon$ and $x = r \cdot c$, then Bob accepts, otherwise Bob rejects.

There are two features of this protocol that need an explanation. The use of a linear code C and bounds 10ε and 0.52 on its parameters.

Both C and bounds were chosen in order to be able to prove that the protocol is secure also in the case of a noisy channel. They have been chosen well to show that Bob can obtain only exponentially small amount of Shannon information about b. However, not only the original proof that Alice cannot cheat had a flaw but, as shown in Section 6.3.4, this flaw cannot be corrected. The way Alice can cheat is in principle similar to the one described in the protocol for coin-flipping.

In the BCJL protocol, Alice first chooses a random string r and a codeword c such that $r \cdot c = x$. She sends r to Bob through a classical channel and c by a quantum channel in a similar way as in the case of QKG protocols. As already mentioned, see page 215, this way Bob can obtain correctly roughly 75% bits. We show in Section 6.3.3 that cheating Bob could obtain as much as 85% of bits, but this is the best possible outcome for Bob.

The binary code C was chosen in such a way that there are exponentially many codewords around the vector c'—the result of Bob's measurements. To show that the bound $\frac{d}{n} = 0.52$ was used. This bound can also be used to show that if G is chosen randomly, then it defines, with large probability, an (n, k, d)-linear code.

6.3.2 Quantum oblivious transfer protocols

The so-called "quantum multiplexing" (due to Wiesner, 1983), can be seen as the first protocol close to a quantum oblivious transfer protocol (QOTP).

It is easy to design a simple QOTP which is perfectly secure provided transmissions and detectors are perfect and no party cheats.

Protocol 6.3.6 (Ideal one-photon standard QOTP)

1. Alice chooses a bit b and sends it to Bob through one photon encoded using a randomly chosen basis—standard or dual.
2. Bob measures the photon with respect to a randomly chosen basis—standard or dual.
3. Alice lets Bob know the basis she chosed. □

At the end Bob has a 50% chance to know b for sure and he knows whether he knows b for sure. Alice has no information whether Bob knows the bit for sure.

There are two problems with this protocol.

1. An imperfect Alice's source, or a noisy channel, or a faulty Bob's detector could much affect the probability of success of Bob's measurement.
2. Bob could cheat by making his measurement in Breidbart basis (see page 241, for details). This way he could learn b with large probability $\cos^2 \frac{\pi}{8} \approx 0.85$.

The first nontrivial QOTP was due to Crépeau and Kilian (1988). A more robust version of this protocol (due to Bennett et al. 1991), will now be presented. At first in an idealized form, where polarized photons are used to transmit bits. A more practical version of the protocol will be briefly discussed next.

Let b_0 and b_1 be Alice choices of bits and c be Bob guess.

Protocol 6.3.7 (BBCS—1-out-of-2 QOTP)

1. **Parameters–agreeing phase.** Alice and Bob engage in a public communication concerning the quality of the source, the channel and the detectors and into a process of determining and verifying their parameters. During this process four parameters are determined or chosen.
   (a) ε—the expected error rate
   (b) α—the fraction of photons Bob is expected to detect successfully;
   (c) n—the security parameter specifying the number of photons to be transmitted;
   (d) C—a binary linear error-correcting code capable of correcting, with large probability, n-bit words transmitted with the expected error rate ε.
2. **Transmission phase.** Alice chooses a random binary string of length $\frac{2n}{\alpha}$ and sends each of the bits through a polarized photon using randomly either the standard/rectilinear (0° or 90° degrees) or the dual/diagonal polarization (45° or 135°).
3. **Measurement phase.** Bob measures each incoming photon by a randomly chosen basis—either standard or dual—and records both the bases chosen and the results of the measurements into tables.

   In this step Bob is expected to receive $2n$ photons. In the case he gets more, he ignores those over $2n$. In the case he gets less, he completes the table to $2n$ by chosing the remaining entries randomly. At the end Bob reports to Alice the arrival times of all $2n$ photons—so she knows which photons got through—but neither the bases nor the results of his measurements.

4. **Bases-revealing phase.** Alice tells Bob, through a public channel, the bases she used to encode her random sequence of bits.

5. **Design of good and bad sequences phase.** Bob partitions his $2n$ bits into two sequences, each of length n. Into the "good" sequence he puts as much as possible of bits he obtained when he used the correct basis for measurements. Into the "bad" sequence he puts as much as possible of bits he obtained when using the incorrect basis for measurements.

   Bob then tells Alice "addresses" (or indices) of the particular bits of both sequences, but not which one is good and which bad.

   At this point Bob shares with Alice a binary word of his good sequence (with respect to an expected error rate not greater than ε). Concerning the bad sequence, Bob shares almost nothing with Alice.

   Of course, the above process is not ideal. There can be some errors introduced by the fact that Bob did not use exactly n times the correct basis for his measurement. However, the number of errors introduced this way should be negligible, with respect to the expected noise in the transmissions.

6. **Error-correction phase.** Using the error-correcting code C, Alice computes syndromes of her words corresponding to the good and bad sequence of Bob, and she sends syndromes to Bob. (Alice knows which bits of her correspond to the good and bad sequences of Bob, even she does not know the values of these bits.) Using these syndromes Bob performs error correction on his good and bad sequences.

7. **Privacy-amplification phase.** Alice chooses randomly two subsets of bits, one from her "good" and one from her "bad" sequence and computes their parities. She let Bob know the "addresses" of bits she chose, but not their values. This way Bob can compute the parity of the corresponding subset of his good sequence, but he will have no idea about the parity Alice obtained for the subset of bits corresponding to his bad sequence. Alice knows both, but she has no idea which one Bob knows. Let x_1 and x_2 be parity bits Alice knows and $\bar{c}$ the one Bob knows.

8. **Oblivious transfer phase**

   (a) Bob tells Alice whether or not $c = \bar{c}$.

   (b) If $c = \bar{c}$, then Alice sends Bob bits $x_0 \oplus b_0$ and $x_1 \oplus b_1$, in this order. If $c \neq \bar{c}$, Alice sends Bob bits $x_0 \oplus b_1$ and $x_1 \oplus b_0$, again in the given order.

   (c) Bob computes b_c out of two bits he got from Alice.

Remark 6.3.8 The paper by Bennett et al. (1991) discussed also the ways how to derive and verify parameters mentioned in Step 1 of the above protocol. In addition, it is there assumed that instead of single photons dim light pulses are used for transmission, to have a more realistic setting.

The security of the BBCS protocol will be discussed in Section 6.3.3. The main result shown by Bennett et al. (1991) is:

Theorem 6.3.9 *Let Δ be data Bob obtained by the protocol. At least one of $H(b_0|\Delta, b_1)$ or $H(b_1|\Delta, b_0)$ is exponentially close (in n) to 1; in no case does Alice learn something (where $H(b_0|\Delta, b_1)$ is the conditional Shannon entropy).*

For another improvement of the ideas presented by Crépeau and Kilian (1991) see to Crépeau (1994),

General cryptographic protocols

A two-party cryptographic protocol, called also two-party oblivious circuit evaluation protocol, is a communication algorithm that allows to two parties, say Alice and Bob, to compute $f(x, y)$, for a publicly known function f, in the case Alice knows, but does not want to reveal, x, and Bob knows y, but keeps it secret, in such a way that Alice learns nothing about y and Bob learns nothing about x, except for what can they deduce from their private inputs and the public value of $f(x, y)$.

It has been shown by Kilian (1988) that in the classical setting 1-out-of-2 oblivious transfer protocol can be used to implement any two-way cryptographic protocol securely. In the quantum setting it is not clear whether there is unconditionally secure QOTP and, consequently, it is not clear whether the standard reduction of a general quantum cryptographic protocol to OTP works, concerning the security, in the quantum setting.

Exercise 6.3.10 *Design a quantum protocol* identify(x, y) *for Alice and Bob to decide whether strings x and y are the same provided Alice knows only x and she does not want to reveal it and Bob knows only y and does not want to reveal it. Assume they communicate through: (a) noiseless channel; (b) noisy channel.*

6.3.3 Security of the quantum protocols

The quantum cryptographic protocols presented in the previous section are simple. On the other hand, problems concerning their security (unconditional and provable) are complex and the attempts to solve them have led to new fundamental questions in both quantum mechanics and computing.

The difficulty of the problems lies in the richness, not fully understood yet, of **cheating strategies** quantum mechanics offer. (A party is said to be cheating if it deviates from the protocol while appearing to follow it.)

Security of the BCJL protocol

The results presented below (due to Brassard et al. 1993), refer to the BCJL protocol, but both the results and their proofs are of a broader interest for the verification of the security of cryptographic protocols.

The first result shows that Bob can obtain maximum information about the vector c sent to him through polarization 0° and 45°, by the measurement with respect to the so-called Breidbart basis

$$\mathcal{B}_0 = \{\theta_0, \theta_1\},$$

where

$$\theta_0 = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle; \quad \theta_1 = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$$

Lemma 6.3.11 *The measurement with the basis $\mathcal{B}_0$ provides Bob with the maximum possible information about x.*

Proof. Density matrices ρ_0 and ρ_1 describing the mixed states representing bits 0 and 1, respectively, have the form

$$\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0'\rangle\langle 0'| = \left(\begin{array}{cc} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} \end{array}\right) \quad \rho_1 = \frac{1}{2}(|1\rangle\langle 1| + |1'\rangle\langle 1'|) = \left(\begin{array}{cc} \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} \end{array}\right).$$

Let us now denote by *commit'* the protocol which is like the protocol *commit*, but it has instead of the step 2.c the following step:

> Alice chooses a binary sequence b of length n randomly in such a way that 0 (1) is chosen with probability $\cos^2\frac{\pi}{8}$ ($\sin^2\frac{\pi}{8}$), and sends Bob a sequence of n photons with polarizations $\mathcal{B}_0(c_i \oplus b_i)$.

It is easy to verify that for the protocol *commit'* the density matrices ρ_0' and ρ_1' that describe the quantum mixtures representing the states 0 and 1 are identical to matrices ρ_0 and ρ_1. Namely,

$$\rho_0' = \cos^2\frac{\pi}{8}|\theta_0\rangle\langle\theta_0| + \sin^2\frac{\pi}{8}\langle\theta_1\rangle\langle\theta_1| = \rho_0.$$

and, similarly, $\rho_1' = \rho_1$.

Moreover, if we denote by ρ_c (ρ_c') the density matrix associated with the mixture of pure states used by the procedure *commit* (*commit'*) to send c, then

$$\rho_c = \bigoplus_{i=1}^{n} \rho_{c_i} = \bigoplus_{i=1}^{n} \rho_{c_i}' = \rho_c'.$$

Since $|\{c \in C \,|\, c \cdot s = 0\}| = |\{c \in C \,|\, c \cdot s = 1\}| = 2^{k-1}$, the density matrices ρ_0, ρ_1, ρ_0' and ρ_1', describing the quantum mixture of all states sent to Bob to commit to 0 (to 1), have the form

$$\rho_0 = \sum_{\{c\in C \,|\, c\cdot r=0\}} \frac{\rho_c}{2^{k-1}} = \sum_{\{c\in C \,|\, c\cdot r=0\}} \frac{\rho_c'}{2^{k-1}} = \rho_0', \quad \rho_1 = \sum_{\{c\in C \,|\, c\cdot r=1\}} \frac{\rho_c}{2^{k-1}} = \sum_{\{c\in C \,|\, c\cdot r=1\}} \frac{\rho_c'}{2^{k-1}} = \rho_1'.$$

Since mixed states represented by the same density matrices cannot be distinguished by any quantum measurement, the above result implies that Bob is able to get about c and x the same information in both protocols *commit* and *commit'*. The point now is that the measurement performed in the protocol *commit'* maximizes Bob's information about c (and therefore about x), because in the measurement performed in that protocol Bob gets all information available! Hence the optimal measurement for Bob in protocol *commit* is the same. This implies that no coherent measurement on all photons could provide more information for Bob. $\square$

As the next step we show that even if Bob performs the optimal measurement, he can get only a very little information about x, and therefore he cannot cheat. As the first step we show that the code c' received by Bob must be quite away from the vector c sent by Alice.

Lemma 6.3.12 *Even if Bob performs the optimal measurement, there exists an* $0 < \alpha < 1$ *such that the probability that* $hd(c, c') < \gamma n$, *where* $\gamma = H^{-1}(\frac{1}{2}) = 0.1100279$, *is at most* α^n.

Proof. Let us assume the most ideal situation for Bob—a noiseless channel. If Bob performs the optimal measurement, then $Pr(c_i = c'_i) = \cos^2\frac{\pi}{8}$ and $Pr(c_i \neq c'_i) = \sin^2\frac{\pi}{8}$. Hence the Hamming distance $hd(c,c')$ is expected to be $\sin^2\frac{\pi}{8}n \approx 0.14644n$. In order to estimate the probability that the number of errors will be less than γn, we use Bernstein law of large numbers[16] as follows: $hd(c,c') = \sum_{i=1}^{n} x_i$, where $x_i = c_i \oplus c'_i$ and $Pr(x_i = 1) = \sin^2\frac{\pi}{8}$. Hence the probability that $hd(c,c') < \gamma n$ can be estimated as follows

$$Pr(\sum_{i=1}^{n}\frac{x_i}{n} \leq \gamma) \leq Pr(|\sum_{i=1}^{n}\frac{x_i}{n} - \sigma^2| \geq \sigma^2 - \gamma) \leq 2e^{-n(\sigma^2-\gamma)^2} \approx 2e^{-0.001326},$$

and $2e^{-0.001326} < \alpha^n$, for an $\alpha < 1$ and an n sufficiently large. □

The main result about Bob's chance to learn the commitment bit has now the form:

Theorem 6.3.13 *Even if Bob knows the Hamming distance $hd(c,c') = d$ he would have asymptotically small information about x if $d > \gamma n$.*

Sketch of the proof. The number of codewords of length n at Hamming distance d from c' is $\binom{n}{d}$. Using the assumption $d > \gamma n$ and a standard/clever approximation of $\binom{n}{d}$ one can derive that the average number of codewords at distance d from c' is greater than $\frac{2^{k-\frac{n}{2}+\alpha n}}{\sqrt{n}}$ except with probability $2^{-\alpha n}$ for any $\alpha > 0$.

The codeword c is one of the $\frac{2^{k-\frac{n}{2}+\alpha n}}{\sqrt{n}}$, at least, many equally likely codewords at distance d from c'. The following lemma (due to Bennett et al., 1998),will be used to determine the number of bits Bob can learn.

Lemma 6.3.14 *If E is the set of equally probable candidates for c and a random subset of bits of c is chosen, then the expected amount of Shannon information available to Bob about the parity of this subset is less than $\frac{2}{|E|\ln 2}$ bits.*

It follows from the above lemma that the number of bits of information Bob can learn about Alice's commitment, after seeing c', is less than $\frac{2\sqrt{n}}{2^{k-n/2-\alpha n}\ln 2}$. This number is exponentially small if $k > \frac{n}{2} + \alpha n$. Since $\frac{k}{n} = 0.52$ we have for $\alpha = 0.1$, $\frac{2\sqrt{n}}{2^{k-n/2-\alpha n}\ln 2} \leq \frac{2^{-0.1n}\sqrt{n}}{\ln 2}$.

Security of the quantum oblivious transfer protocols

The first protocol (due to Crépeau and Kilian, 1988), was considered as secure provided neither party could store photons for a longer time and only projection measurements were used by Eve. Mayers (1998) made the final contribution to the numerous attempts to show that there is an unconditionally secure quantum oblivious transfer protocol provided there is an unconditionally secure QBCP. At that time this was considered as very encouraging results for quantum cryptography because it was believed that unconditionally secure QBCP do exist.

The result mentioned above, and discussed in the next section, namely that unconditionally secure QBCP is impossible, implies that one cannot have an unconditionally secure QOTP the security of which is based on security of a QBCP. However, this result does not rule out the possibility that there is unconditionally secure QOTP.

[16] Bernstein law of large numbers: Let $x_1, x_2, \ldots, x_n$ be independent Bernoulli variables. If $Pr(x_i = 1) = p$ for $1 \leq i \leq n$, then for all $0 < \delta \leq p(1-p)$ we have $Pr(|\sum_{i=1}^{n}\frac{x_i}{n} - p| \geq \delta) \leq 2e^{-n\delta^2}$.

The BBCS protocol was shown secure (see Bennett et al. 1991) even against cheating by Bob with unlimited computing power under the assumption that Bob measures each photon (or pulse), before the next one arrives, using a projection measurement, or else he loses the opportunity to measure it at all.

Let us now discuss security of the BBCS protocol against the so-called photon (pulse) storing attacks (due to Bennett et al. 1991). The basic idea is that Bob does not measure the incoming photons in Step 3, he only stores them and waits with the measurement until Alice makes clear in Step 4 which bases she used. In this way it seems that Bob could present Alice with two good sequences and therefore he could get both bits b_0 and b_1.

From the practical point of view this attack is very unlikely to succeed. First of all it is technically hard to store photons (pulses) for a longer period. Secondly, even if such a storage were to be available this would not be sufficient. The problem is that Bob needs to tell Alice in Step 3 which photons (pulses) arrived successfully and were measured. However, no technique is available or foreseeable to determine whether a measurement will succeed without actually doing the measurement.

In addition, it is possible to change the BBCS protocol in such a way that it is fully secure against any photons (pulses) storage attack, providing there exists (unconditionally) secure QBCP. The basic idea goes as follows.

Alice sends to Bob not $\frac{2n}{\alpha}$, but at least $\frac{3n}{\alpha}$ of photons to achieve that $3n$ of them arrive successfully. Then, before Step 4, Bob is required to use a QBCP to commit himself both to bases he used in his measurements and to the outcomes of the measurements. Immediately after that Alice would choose randomly n of the reported successful measurements and ask Bob to unveil his commitments. This would allow Alice to check whether Bob's commitments are correct (subject to the error rate ε) when his commmited bases are correct and uncorrelated otherwise. In addition, this way Alice could be sure that Bob's measurements took place before Step 4 and that he used bases as he was required to do.

6.3.4 Security limitations of the quantum cryptographic protocols

Security of QBCP has been one of the most intriguing and important problems in the area of the security of quantum cryptography.

The first QBCP (see page 235), was shown insecure already by its authors. The second important one, the BCJL protocol, see page 237, has been claimed to be unconditionally secure by its authors and it was believed for a few years that their claim is true. A flaw in the proof was discovered in 1995 by Mayers and, independently, by Lo and Chau (1996). In addition, Lo and Chau were the first to argue that unconditionally secure QBCP may not exist. This suspicion was then shown to be valid by Mayers (1998).[17]

The very basic idea behind breaking BCJL is that Alice can use ancilla to create a compound quantum state that allows her to cheat as follows: She sends a part of the state to Bob and keeps the rest. By measuring her part appropriately, without touching Bob's part, she can modify her state in such a way that she can cheat concerning her commitment.

General form of quantum bit commitment protocols

The main idea behind the Mayers–Chau–Lo proof that unconditionally secure QBCP do not exist, as presented by Chau and Lo (1998) and Mayers (1998), assumes that each QBCP has the following form:

[17] For a detailed treatment of the history of the attempts to deal with security of QBCP see Brassard et al. (1998b).

1. **Commitment phase.**
   (a) Alice and Bob put particles in their hands to some prescribed initial states.
   (b) Alice and Bob repeat several times the following steps:
      i. Depending on her commitment b Alice applies a unitary transformation U_b on her particles and sends *some* of her particles to Bob.
      ii. After receiving particles from Alice, Bob applies a unitary transformation to particles in his hands and then sends *some* of his particles to Alice.

2. **Opening phase.**
   (a) To open her commitment Alice sends all her particles to Bob.
   (b) After receiving particles from Alice Bob performs some measurements on particles in his hands to verify Alice's honesty.

In the terms of Hilbert space concepts the above general scheme of QBCP has the following transcription.

Let H_A and H_B be Hilbert spaces of Alice and Bob, and let H_C correspond to their communication channel and the environment. They execute their QBCP in $H = H_A \otimes H_B \otimes H_C$.

As the first step Alice prepares a state $|0_A\rangle$ or $|1_A\rangle$ in $H_A \otimes H_C$, according to her commitment, and Bob prepares a state $|a\rangle$ in $H_B \otimes H_C$. The overall initial state is then $|b_A\rangle \otimes |a\rangle$.

In Step 1.b, in each communication round, each party $D \in \{A, B\}$ performs a unitary transformation on $H_D \otimes H_C$ (and therefore also on H).

The key insight is now that since each product of unitary transformations is again a unitary transformation the whole communication process can be characterized by a single unitary transformation U applied to $|b_A\rangle \otimes |a\rangle$. Since both Alice and Bob know the protocol they also know U. Bob can therefore readily verify Alice's commitment after she sends him all her particles.

Remark 6.3.15 As is often the case, once the impossibility proof was made public attempts started to show that it does not cover all cases, all possible QBCP. Two ideas were explored: to introduce also classical communications, and to make Alice use classical BCP to commit herself, during the protocol, to some values, steps or measurements. All these attempts failed. For some discussion of such ideas see, for example, Brassard et al. (1997). In addition, Brassard et al. (1998b), have shown that even unconditionally secure classical BCP does not help.

Exercise 6.3.16 *Show that both QBCP on page 235 and 237 are special cases of the above general scheme of QBCP.*

Cheating

We show now that either Bob or Alice can cheat. More precisely, it will be shown that if Bob cannot learn Alice's commitment with high probability, then Alice can change her commitment at the beginning of the opening phase, without Bob noticing it, and therefore she can cheat—provided she has a quantum computer to perform unitary transformations.

Without loss of generality we can consider H_C as a part of H_A or H_B, depending on who is just making a transformation on H and therefore let $H = H_A \otimes H_B$.

The key tool to do cheating is the Schmidt decomposition theorem—see page 372. According to this theorem, the total state of H at the end of the commitment phase can be seen as having the following form in the case of the commitment to 0:

$$|0_{final}\rangle = \sum_i \sqrt{\alpha_i}|e_i, \phi_i\rangle \tag{6.2}$$

and in the case of the commitment to 1:

$$|1_{final}\rangle = \sum_i \sqrt{\beta_i}|e'_i, \phi'_i\rangle, \tag{6.3}$$

where $\{e_i\}_i$ and $\{e'_i\}_i$ are orthonormal bases of H_A.

The quantum state of Bob's particles, without the extra information coming from Alice, is described by the density matrix $\rho_B = Tr_{H_A}(|b_{final}\rangle\langle b_{final}|)$, if the commitment bit was b. By (6.2) and (6.3) we have

$$\rho_0 = \sum_i \alpha_i|\phi_i\rangle\langle\phi_i|, \qquad \rho_1 = \sum_i \beta_i|\phi'_i\rangle\langle\phi'_i|.$$

If ρ_0 and ρ_1 are very different, then Bob can learn, with high probability, Alice's commitment and therefore Bob can cheat. If ρ_0 and ρ_1 are not too different there are still two cases to consider.

Ideal case: $\rho_0 = \rho_1$. In such a case[18] for all i

$$\alpha_i = \beta_i \quad \text{and} \quad |\phi_i\rangle = |\phi'_i\rangle$$

and therefore

$$|1_{final}\rangle = \sum_i \sqrt{\alpha_i}|e'_i, \phi_i\rangle.$$

Alice can therefore cheat by mapping $|0_{final}\rangle$ into $|1_{final}\rangle$ by applying on $|0_{final}\rangle$ a unitary transformation (on H_A only!) that maps, for all i, $|e_i\rangle$ into $|e'_i\rangle$.

This means that at the beginning of the commitment phase Alice can proceed by the protocol as she would make commitment 0 and at the end of the commitment phase, or better at the beginning of the opening phase, she can, without getting caught by Bob, change her commitment if she wishes to do so.

Non-ideal case: the difference between matrices ρ_0 and ρ_1 is small, with respect to the fidelity $F(\rho_0, \rho_1)$, defined as follows.

$$F(\rho_0, \rho_1) = \max\{|\langle\theta_0|\theta_1\rangle| \,|\, \theta_i \text{ is a purification of } \rho_i, i = 0, 1\}.$$

This measure of fidelity has the following property: to any purification θ_1 of ρ_1 there exists a purification θ_0 of ρ_0 such that $F(\rho_0, \rho_1) = |\langle\theta_0|\theta_1\rangle|$. Clearly, $0 \le F(\rho_0, \rho_1) \le 1$.

[18] It is assumed here that all eigenvalues are non-degenerate. The case of degenerate eigenvalues can be considered in a similar way.

Let us now assume that there is a small $\delta > 0$ such that $F(\rho_0, \rho_1) = 1 - \delta$. In such a case there is a state θ_1 which is a purification of ρ_0 and

$$|\langle \theta_1 | 1_{final} \rangle| = F(\rho_0, \rho_1) = 1 - \delta \tag{6.4}$$

It is now clear that Alice's strategy for cheating in this non-ideal case can resemble that in the ideal case. Namely, Alice chooses 0 as her "preliminary commitment" at the beginning of the commitment phase and performs the commitment phase according to the protocol. If, at the beginning of the opening phase, Alice decides to cheat, she makes public that her commitment was 1 and she applies a local unitary transformation to change $|0_{final}\rangle$ to $|1_{final}\rangle$ such that $\langle 0_A | 1_{final} \rangle = 1 - \delta$. Since the difference between $|0_A\rangle$ and $|1_{final}\rangle$ is very small, Bob is not able to distinguish it and Alice can cheat with large probability.

6.3.5 Insecurity of quantum one-sided two-party computation protocols

Let us consider again the problem that Alice knows x, Bob knows y and they both want to compute $f(x, y)$ for a function f they both know—see Section 5.3.1 and page 241. However, this time the condition is that at the end of the protocol Alice learns nothing (about y and $f(x, y)$), Bob learns $f(x, y)$, but nothing about x (except what can be learned from x and $f(x, y)$ alone)—the so-called discrete function evaluation problem.

Lo (1998) has shown that in any quantum protocol to solve this problem Bob can cheat in the sense that he can learn $f(x, y)$ for all y. Cheating can be done as follows: Bob starts with some y_1 and uses the protocol to learn $f(x, y_1)$. Afterwards Bob changes y_1 to y_2 and learns $f(x, y_2)$ and so on. Such a cheating works for the following reason. When learning $f(x, y_1)$ by a measurement Bob will not change the measured state because it has to be the eigenstate of $f(x, y_1)$—this follows from the requirement that Bob learns $f(x, y)$ for 100%. Bob can therefore apply a unitary transformation to change y_1 to y_2 because Alice is supposed to learn nothing about y_1 when cooperating on computation of $f(x, y_1)$. In other words, the state of all particles of Alice and Bob when computing $f(x, y_1)$ and $f(x, y_2)$ is related by a unitary transformation that involves only Bob's particles.

6.4 Quantum Teleportation and Superdense Coding

Quantum teleportation[19], due to Bennett et al. (1993), allows transmission of quantum information to a distant place in spite of the impossibility of measuring or broadcasting information to be transmitted. It is an interesting demonstration of quantum entanglement as a communication resource.

[19] The term "teleportation" comes originally from science fiction and refers to making a person or an object disappear while an exact replica appears somewhere else. An underlying implicit assumption is that the teleported object does not traverse directly to its destination. Only necessary information for its assembly is first extracted, then transferred and finally used to assemble the original. This idea has been discarded by scientists as deferring physical laws, for example, Heisenberg's uncertainty principle, that does not allow measurement of all needed information about the object to be teleported. "Quantum teleportation", on the other hand, defers no physical law and therefore it is a term that sounds perhaps stronger than its real meaning is. Of course, this does not mean that it is not a very attractive concept (see Bennett et al, 1993).

6.4.1 Basic principles

We start with an informal presentation of the basic ideas behind quantum teleportation. Technical details, as well as the teleportation circuit, follow.

Assume that Alice and Bob share a pair of entangled particles A and B and let Alice be given a particle C in an unknown state $|\psi\rangle$. What should she do if she wishes Bob has $|\psi\rangle$ instead of her? She cannot measure the particle to learn the information which she could then transmit to Bob over a classical channel because such a measurement would almost certainly spoil the information irreversibly.[20] However, she can make the particle C in the unknown state $|\psi\rangle$ interact, in the proper way, with her part A of the entangled pair and then she can measure a shared property of both C and A. As the result, the state of Bob's particle B of the entangled pair instantaneously becomes a replica of $|\psi\rangle$—up to a rotation. At the same time Alice's particles C and A lose their information but she obtains, as the result of her measurement, two purely random bits of classical information that tell her which operation (rotation) Bob should perform on his particle B to make the particle get into the state $|\psi\rangle$. Alice then has to communicate these two bits to Bob over a classical channel, because Bob's particle B remains indistinguishable from a purely random qubit until he performs the required rotation, to get the particle into the state $|\psi\rangle$. Alice can therefore divide information encoded in $|\psi\rangle$ into two parts, classical and nonclassical, and send them to Bob through two different channels, a classical one and an EPR channel. One can also say that by performing a proper measurement on C and A a part of quantum information in C is immediately transmitted to B and Alice gets the remaining part of information on $|\psi\rangle$ in the classical form, and this can then be used by Bob to make his particle B get to the unknown state $|\psi\rangle$.

At the end neither Alice nor Bob knows the state $|\psi\rangle$ but both of them know that at the end of the teleportation not Alice but Bob has a particle in the state $|\psi\rangle$. This way the unknown quantum state $|\psi\rangle$ can be disassembled into, and later reconstructed from two classical states and an entangled, purely nonclassical, state. Observe also, that this way an intact and unknown quantum state can be "teleported" from one place to another by a sender who does not need to know—for teleportation itself—either the state to be teleported or the location of the intended receiver.

Finally, observe that the above process cannot be used to transmit information faster than light but it can be argued that part of the information that was present in the particle C is transmitted instantaneously (except two random bits that needed to be transported at the speed of light at most).

Mathematical details are as follows: Assume that Alice and Bob share the EPR pair $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the unknown quantum state of the particle owned by Alice. She first couples her particle A with C to create the state

$$|\phi\rangle = |\psi\rangle|EPR\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$

The key point for teleportation is now that $|\phi\rangle$ can be expressed in a special way using the Bell basis $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$.

Indeed, since

$$|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle), \qquad |01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle),$$

[20] She could do that were she to have a whole set of particles all in the state $|\psi\rangle$. In such a case Alice could perform measurements on all these particles and determine $|\psi\rangle$ pretty well and then send this information to Bob who could prepare his source of qubits to produce $|\psi\rangle$.

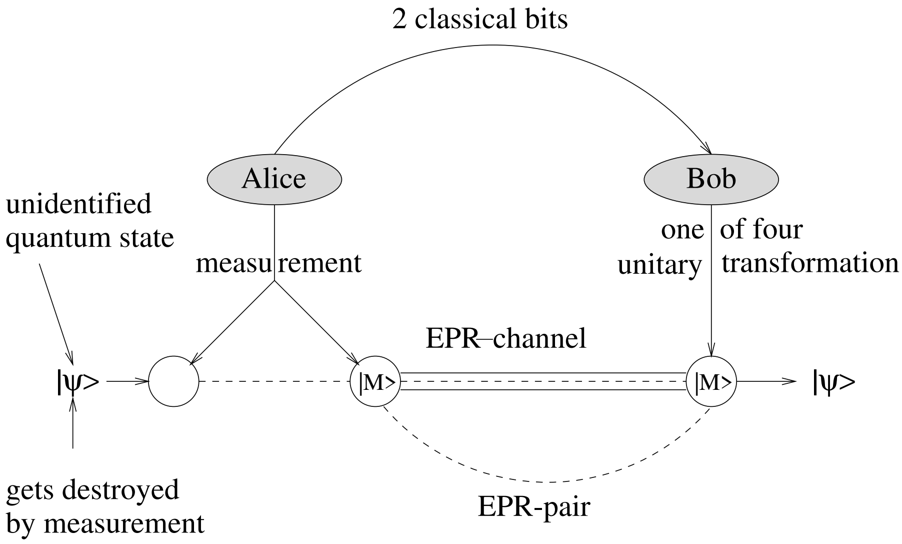

Figure 6.10: Quantum teleportation

$$|10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle), \qquad |11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle),$$

we get

$$\begin{aligned}
\alpha|000\rangle &= \alpha|00\rangle|0\rangle = \frac{1}{\sqrt{2}}(\alpha|\Phi^+\rangle|0\rangle + \alpha|\Phi^-\rangle|0\rangle), \\
\alpha|011\rangle &= \alpha|01\rangle|1\rangle = \frac{1}{\sqrt{2}}(\alpha|\Psi^+\rangle|1\rangle + \alpha|\Psi^-\rangle|1\rangle), \\
\beta|100\rangle &= \beta|10\rangle|0\rangle = \frac{1}{\sqrt{2}}(\beta|\Psi^+\rangle|0\rangle - \beta|\Psi^-\rangle|0\rangle), \\
\beta|111\rangle &= \beta|11\rangle|1\rangle = \frac{1}{\sqrt{2}}(\beta|\Phi^+\rangle|1\rangle - \beta|\Phi^-\rangle|1\rangle)
\end{aligned}$$

and therefore

$$\begin{aligned}
|\phi\rangle &= \Phi^+\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + \Psi^+\frac{1}{\sqrt{2}}(\beta|1\rangle + \alpha|1\rangle) \\
&\quad +\Phi^-\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + \Psi^-\frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle).
\end{aligned}$$

If Alice now makes a measurement of the first two qubits of $|\phi\rangle$, with respect to the Bell basis, then she will get one of the four possible outcomes: $00+$, $01+$, $00-$ and $01-$, and therefore two classical bits of information, and $|\phi\rangle$ gets reduced to one of the states

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle), \quad \frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle), \quad \frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle), \quad \frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle), \tag{6.5}$$

and to the same state Bob's particle gets into. In order to tell Bob into which of the above four states $|\phi\rangle$ got reduced, she needs to send him two classical bits of information. Bob needs them to know which of the following four unitary transformations

$$U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_{10} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad U_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad U_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

to apply to his particle in order to transform it to the original unknown state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$.

The sending of two classical bits plays the key role in quantum teleportation. Indeed, it can be shown that if it was sufficient to send less than two classical bits of information in the above teleportation scheme, this could be used by Bob to send messages faster than light—see Bennett et al. (1993)—i.e. to send the so-called *superluminal messages.*

6.4.2 Teleportation circuit

Despite the fact that the idea of teleportation sounds more like science fiction, it is expected to be implemented sooner than some nontrivial quantum processors. The hardest problem to solve for teleportation seems to be, for most technologies, the development of an efficient long-term storage for quantum information, especially for entangled particles.

Quantum circuit to perform teleportation can be made very simple (see Brassard, 1998), and his circuit will now be presented.

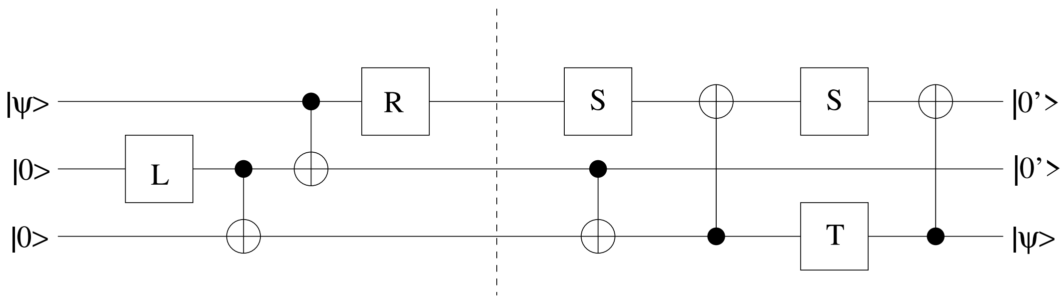

Figure 6.11: Brassard's teleportation circuit

Consider the circuit in Figure 6.11 where L, R, S, and T are the gates implementing the following unitary transformations

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad L = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad S = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad T = \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$$

Let $|\psi\rangle$ be a qubit state. If the state $|\psi 00\rangle$ is processed by the circuit from Figure 6.11, i.e. $|\psi\rangle$ is put on the topmost input and $|0\rangle$ on the other two, then the output will be $|0'0'\psi\rangle$.

Exercise 6.4.1 *Design unitary matrices corresponding to circuits: (a) in Figure 6.12a; (b) in Figure 6.12b; (c) in Figure 6.11 before the dashed line; (d) in Figure 6.11 after the dashed line; (e) for the whole circuit in Figure 6.11.*

Exercise 6.4.2 *Determine the intermediate states of the computation of the circuit from Figure 6.11 on input $|\psi 00\rangle$ after all gates.*

In the state of the circuit at the dashed line all three qubits are entangled. A measurement of the two upmost qubits provides two random classical bits, say u, v. Surprisingly enough (verify it), if these two bits are "returned" into the circuit, i.e. if the computation of the circuit to the right of the dashed line starts with input $|uvz\rangle$, where z is the state of the third qubit of the dashed line, then the output of the circuit will be $|uv\psi\rangle$.

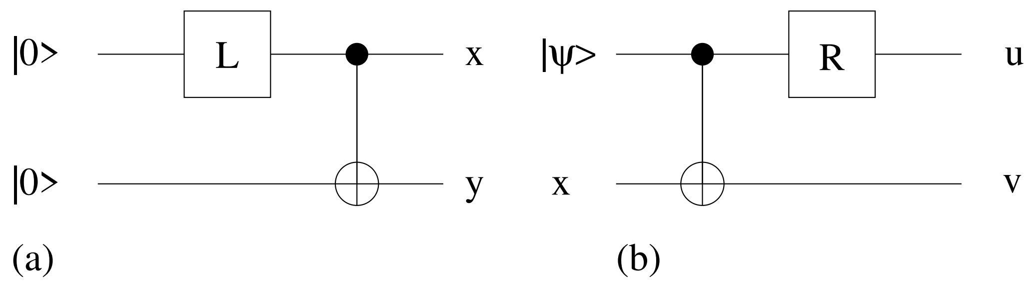

Figure 6.12: A teleportation device

Out of the teleportation circuit shown in Figure 6.11 we can make, by a "cut along the dashed line", two circuits, one for Alice, one for Bob, to use for teleportation (see Figure 6.13).

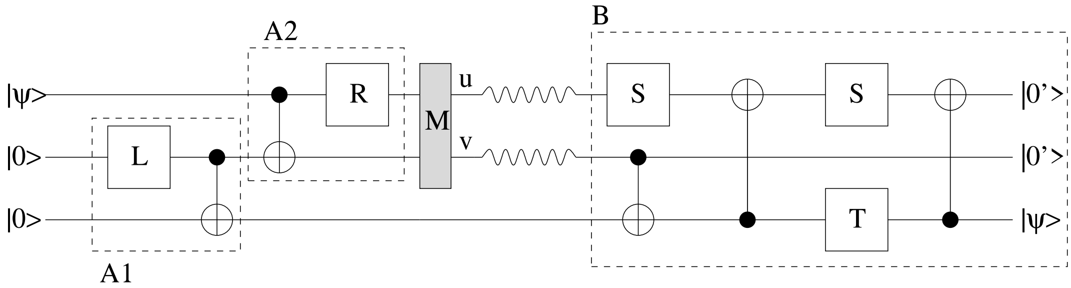

Figure 6.13: Two teleportation circuits of Alice and Bob

Alice's circuit consists of two subcircuits. Using the first one, A1 (see also Figure 6.12a), with the initial states $|0\rangle$, Alice can create a pair of particles Q2 and Q3 in the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice keeps Q2 and sends Q3 to Bob.

At some time later, let Alice want to teleport to Bob the unknown state $|\psi\rangle$ of her new particle Q1.[21] She can then use the second subcircuit A2 (see Figure 6.12b), to entangle $|\psi\rangle$ with particles Q2 and Q3. (Observe that at the output of the second subcircuit all three qubits are entangled.)

Alice now makes a measurement of Q1 and Q2, with respect to the Bell basis. As the result she gets two classical bits of information, the states of Q1 and Q2 will collapse and Q3 will get into one of the states shown in (6.5). The two bits she gets Alice sends, using a classical channel, to Bob.

If Bob gets two bits he can add them as inputs to his teleportation circuit with Q3 as the third input. Bob's circuit is to choose, on the basis of two inputs, the proper rotation to apply to Q3 and to perform the required rotation to have his qubit Q3 in the state $|\psi\rangle$.

[21] More exactly Alice does not need to know the state $|\psi\rangle$ in order to teleport it to Bob. Without loss of generality we can therefore assume the state is unknown to her.

Applications? Let us first explore a natural question whether teleportation could be useful for quantum information processing. Yes, because teleportation can provide another way to transmit information inside quantum computers and information systems, which can be of interest especially if information has to be kept secret and should never be transmitted over an insecure channel. Actually, it is in the area of quantum computers and communication systems where the first applications of quantum teleportation are expected.

In addition, if Bob already possesses the state $|\psi\rangle$, then teleportation can be used by Bob to determine $|\psi\rangle$ more completely by making measurements on both copies of $|\psi\rangle$. Moreover, teleportation is possible without Alice knowing the exact position of Bob. It is sufficient to broadcast classical bits to all the possible locations Bob could be in (or to send him an email).

Methods of quantum teleportation have been improved to work with arbitrarily high fidelity even if the quantum channel is imperfect and the quantum noise is too strong to use some quantum error-correction techniques (see Section 8.3.2 and Bennett et al. 1996a).

Partial implementations (without the last stage—Bob's transformations), of quantum teleportation over macroscopic distance have already been reported by Bouwmeester et al. (1997), for the distance of 1m, and Boschi et al. (1998), using optical systems and photons. A complete implementation of quantum teleportation over inner-atomic distance using liquid state NMR technology was reported by Nielsen, Knill and Laflamme (1998).

Remark 6.4.3 In spite of the remarkable power of quantum entanglement for quantum teleportation, and also as a substitute for communication, see Section 7.4.1, the power of entanglement to facilitate direct communication between two parties is quite restricted. For example, let two entangled particles be possed by Alice and Bob. If Alice receives an unknown bit of information there is no operation she can perform on her particle in such a way that Bob could then get the bit by performing an appropriate operation on his particle.

6.4.3 Quantum secret sharing

The idea of teleportation can be used to solve communication problems in several ways, see especially Chapter 8. One of them will now be discussed. It provides quantum realization of the classical secret sharing ideas.

Splitting of information

There is a simple method, due to Hillery, Bužek and Berthiaume (1998), how Alice can teleport a (secret) qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob and Charles in such a way that they have to cooperate in order to have $|\phi\rangle$.

The basic idea is that Alice couples a given particle P in the state $|\phi\rangle$ with the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ of three particles P_a, P_b and P_c she shares with Bob and Charles and then performs a measurement on the state of particles P and P_a, with respect to the Bell basis $\{\Phi^\pm, \Psi^\pm\}$. Since

$$\begin{aligned} |\phi\rangle|\psi\rangle &= \frac{1}{2}(|\Phi^+\rangle(\alpha|00\rangle + \beta|11\rangle) + |\Phi^-\rangle(\alpha|00\rangle - \beta|11\rangle) \\ &\quad +|\Psi^+\rangle(\beta|00\rangle + \alpha|11\rangle) + |\Psi^-\rangle(-\beta|00\rangle + \alpha|11\rangle)), \end{aligned}$$

the outcome of the measurement is that particles P_b and P_c get into one of the states

$$\frac{1}{\sqrt{2}}(\alpha|00\rangle + \beta|11\rangle), \frac{1}{\sqrt{2}}(\alpha|00\rangle - \beta|11\rangle), \frac{1}{\sqrt{2}}(\beta|00\rangle + \alpha|11\rangle), \frac{1}{\sqrt{2}}(-\beta|00\rangle + \alpha|11\rangle)$$

and Alice gets two bits to tell her about which of these four cases happened. However, neither Bob nor Charles has information about which of these four states their particles are in.

Bob now performs a measurement of his particle with respect to the dual basis. He gets out of it one bit of information and Charles's particle P_c gets into one of 8 possible states, which is uniquely determined by bits both Alice and Bob got as the results of their measurements, and which can be transformed into the state $|\phi\rangle$ using one or two applications of Pauli matrices.

Exercise 6.4.4 *(a) Determine the density matrix of Charles's particle after Alice's measurements; (b) determine* 8 *possible states into which Charles's particle can get after Alice's and Bob's measurements; (c) determine transformations Charles has to perform in order to have his qubit in state* $|\phi\rangle$ *in dependence on bits learned by Alice and Bob in their measurements.*

Exercise 6.4.5 *Show how to generalize the idea of splitting information between two parties to the case of (a)* 3 *parties; (b)* n *parties.*

Quantum secret sharing among n parties

A more general problem is to design methods how one can "partition" or "share" a quantum "secret" (state) among n parties in such a way that, for a fixed k, any k of parties can, by cooperation, reconstruct the secret, but no combination of $k-1$ of parties is able to do that.

Exercise 6.4.6 *Show (Cleve et al. 1999), that using the mapping*

$$\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle \to \alpha(|000\rangle+|111\rangle+|222\rangle)+\beta(|012\rangle+|120\rangle+|201\rangle)+\gamma(|021\rangle+|102\rangle+|210\rangle)$$

one can distribute a "secret qutrit" to three qutrits in such a way that if each qutrit is owned by a different party, then any two of them can reconstruct the secret state, but no single party can do that alone.

The secret sharing problem, a quantum analogue of the classical one, is in full generality solved by Cleve et al. (1999). They showed that such a secret sharing does exist if $n < 2k$. The last restriction is due to "No-cloning theorem".

6.4.4 Superdense coding

Teleportation uses two classical bits to transmit one qubit. Superdense coding, Bennett and Wiesner (1992), is a dual to teleportation. It uses a single qubit, i.e. a single photon, to transmit two classical bits. This can be done as follows—see Figure 6.14.

Assume that Alice and Bob share two particles in the EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which forms the EPR-channel. If Alice receives two classical bits, b_1, b_2, she performs on her particle one of the Pauli rotations as shown in the second column of Figure 6.15. The resulting state is shown in the third column and this state she then sends to Bob. He performs first on both states XOR operation and this way he disentangles the state with the result shown in column 5. Finally, Bob performs the measurement of Alice's qubit in the dual bases and

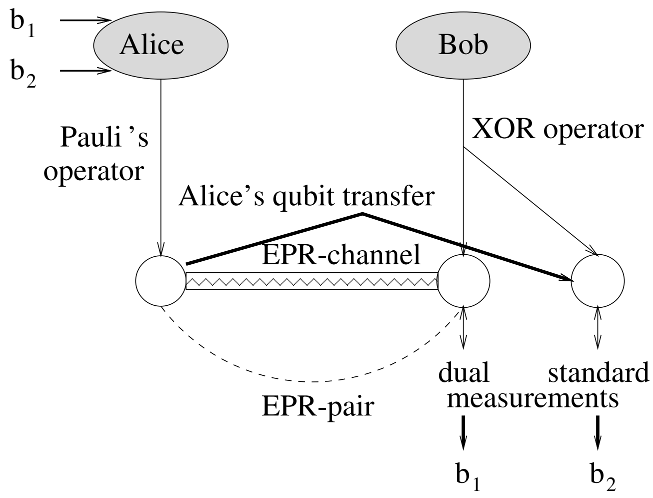

Figure 6.14: Superdense coding

of his qubit in the standard basis to get two bits (see column 6), Alice has sent him in one qubit. In a simplified form the resulting system is depicted in Figure 6.16.

Alice's bits	Pauli's rotations	Alice's particle: new state	$\rightarrow$	Bob's XOR transformation	Bob's bases $\mathcal{D}, \mathcal{B}$	Bob's bits
00	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|0\rangle$	00	00
01	σ_x	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|1\rangle$	01	01
10	σ'_y	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|1\rangle$	11	10
11	σ_z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|0\rangle$	10	11

Figure 6.15: Superdense coding steps

Remark 6.4.7 1. Quantum superdense coding transmission was first put into practice in Innsbruck by Zeilinger's group with polarization-entangled photons (see Matte et al. 1996).

2. In the superdense coding presented above, it is essential that Alice and Bob use a maximally entangled state. Indeed, Barenco and Ekert (1995) and Hausladen et al. (1996) have shown that the amount of information communicated by the superdense coding decreases from its maximum, 2 bits per qubit, with the decrease in the amount of entanglement, and it becomes 1 bit when the entanglement is zero. When the initial state of the entangled pair of qubits is mixed, capability to do superdense coding in terms of various measures of entanglement has been investigated by Bose et al. (1998).

Remark 6.4.8 Experimental progress in the quantum key generation, creation of entangled pairs over a long distance and in quantum teleportation has been such that the vision of small quantum networks does not have to be far away. This puts the problems of quantum multiparty communications and quantum distributed computing into a promising research agenda.

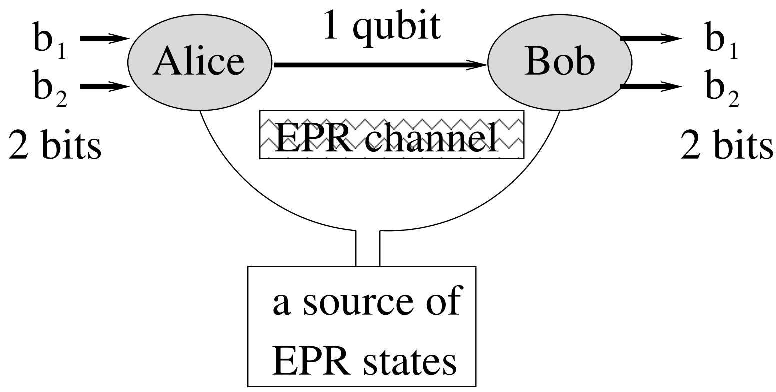

Figure 6.16: Superdense coding scheme