UNIVERSITÀ DEGLI STUDI DI ROMA
"LA SAPIENZA"

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE
E NATURALI

DOTTORATO DI RICERCA IN FISICA
XVI CICLO

QUANTUM DECOHERENCE AND QUANTUM CRYPTOGRAPHY

Marco Lucamarini

Ph.D. Thesis

Relatori:
Prof. Ferdinando de Pasquale
Dr. Stefano Mancini

To my parents,
for their optimism.

Abstract

The title of the present dissertation "Quantum Decoherence and Quantum Cryptography" sounds very general and all-inclusive. Indeed it embraces two topics from the area of Quantum Mechanics each of which is described in all respects by a huge literature developed in the last three decades. Of course this thesis has not the ambition for an exhaustive treatment of the two issues. It rather describes some particular aspects and applications within them.

The structure in two parts of the manuscript reflects the formative path of the author during his Ph.D. in the university of Rome "La Sapienza" . The two parts are vaguely connected by the quantum nature of the few-particle systems involved, and by the information-theoretical approach used to study them. A more stringent relation comes from the observation that *coherent quantum systems* (Part I) are the essential bricks with which *quantum cryptography* (Part II) is built up.

Quantum decoherence, as the name lets it mean, is the mechanism that makes a quantum system loose its coherence properties, and with them the capability of giving rise to interference phenomena or to other interesting quantum effects. The usual picture considers a two-level quantum system (i.e. a *quantum bit*, usually shortened with a terminology from information science to "*qubit*") in contact with a wide thermal environment. The flow of energy and, more generally, of information between system and environment spoils the purity of system's quantum state, rendering it a statistical classical mixture. Systems at issue are generally composed by one or two particles; in the latter case they are referred to as *bipartite quantum systems*.

The first part of the dissertation concerns the study of decoherence induced on qubits by a fermionic environment endowed with a symmetry-breaking mechanism, in mean-field approximation. This is quite a recent issue, introduced in 2002 by prof. F. de Pasquale and his group of Rome's university; its general lines are summarized in Chapter 1.

I extended this approach to bipartite quantum systems with the intent of studying *entanglement dynamics*. Entanglement is the way we describe non-classical correlations between distant particles. The most famous example related to entanglement is represented by the violation of Bell inequalities, that reveals the non-local nature of quantum mechanics. Besides the attractiveness pertaining to a gathering of quantum correlations and classical ones (those leading to a phase transition in the environment) in an unique topic, the analysis of entangled bipartite systems plunged in a symmetry-breakable fermionic environment led to original results. There emerges a counter-intuitive effect of time-persistence of quantum correlations below the critical temperature T_c of the environment, despite the strong interactions involved in the model. Furthermore peculiar *entanglement oscillations* and *decoherence free subspaces* appear below T_c, both of which have no classical analogues. These results are reported and discussed in Chapter 2. They represent, with some other minor calculations of Chapter 1, my personal contribution to the subject treated in Part I of this thesis.

Quantum Cryptography (QC) is a special issue of Quantum Information Theory that aims at exploiting coherence properties of quantum systems to increase the security of certain communication

protocols between distant parties. The transmission of a message between two users, traditionally called Alice and Bob, is known to be perfectly secure when both users, and only them, possess a random key with which encrypt-and-decrypt the message itself. If Alice and Bob do not share in advance a common secret key then they must resort to a distribution protocol that provides them with a new secret key. But a distribution protocol that uses only classical means, for instance the postal service or a phone call, undergoes attacks by a malicious presence, usually called Eve, who can eavesdrop information about the key without being revealed by legitimate users. Thus the consequent communication results to be not perfectly secure.

QC uses laws of quantum mechanics to solve the problem of a secure key distribution between distant parties. In particular *No-Cloning theorem* and its corollaries forbid Eve to tamper with the quantum channel of the communication without being revealed by Alice and Bob with high probability. This is the physical mechanism that makes *Quantum Key Distribution* (QKD) completely secure, and definitely preferable to classical one.

Early quantum cryptosystems were proposed in 80s and are nowadays widely feasible with current Quantum Optics technology; in this sense photons are preferred particles speaking about QC. The mechanism these protocols are based on is intrinsically random: the final key available to legitimate users is not really "distributed" by anyone, but it is rather "generated" during the protocol according to certain choices brought about randomly by the users themselves. In this respect we should more precisely speak of a *quantum key generation* rather than of a QKD. As a consequence, the final key returned by the protocol remains *undetermined* until the very moment of communication's end, none of the users can foresee it beforehand. Thence we term this kind of QC *Non-Deterministic Quantum Cryptography* (NDQC). In Chapter 3 we give a short review of the main protocols in NDQC.

Recently novel forms of QC have been proposed that realize a real distribution of the random key: one of the user, say Alice, owns the key and *deterministically* transfers it to another user in a secure manner. As such we refer to this sort of QC as *Deterministic Quantum Cryptography* (DQC). DQC is as secure as NDQC but it allows for a higher efficiency of the transmission. Moreover, quite remarkably, DQC can also issue tasks different from QKD, and impossible to achieve with NDQC. One of these is the *Quantum Direct Communication* (QDC), i.e. the direct transmission of the plain-text message itself, without any demand for an encryption process. This sort of communication is not as safe as the encrypted one, but it has the advantage of a faster delivery of the message.

The first deterministic cryptosystem was invented in 2002 and took the name of *Ping-Pong* protocol (PP): it is entanglement-based and resulted to be not secure enough for any realistic communication. I began to devote to the problem of PP's security in November 2003, under the suggestion of dr. S. Mancini, of the university of Camerino. The first step has been to study in detail PP and other entanglement-based deterministic protocols. The results of this analysis are reported in Chapter 4. Afterwards I proposed a novel deterministic protocol, namely PP84, that does not make use of entanglement, thus resulting more practical to implement; it is capable of the same performance of PP, but avoids its drawbacks. The complete and detailed analysis of this communication scheme is covered in Chapters 5 and 6, which constitute the main contribution of the author to the topic of DQC.

Table of Contents

List of Symbols

Qubit	Quantum bit
$\mathcal{K}_n$	Hilbert space of dimension n
$\mathcal{H}_s$	System Hamiltonian
$\mathcal{H}_{sB}$, $\mathcal{H}_I$	Interaction Hamiltonian s
$\mathcal{H}_B$, $\mathcal{H}_E$	Bath Hamiltonians
H	Shannon Entropy
S	von Neumann Entropy
I	Information, Mutual information
POVM	Positive Operator Value Measure
BSC	Binary Symmetric Channel
BEC	Binary Erasure Channel
XOR	Exclusive OR
$\oplus$	Bitwise XOR of two strings
$\otimes$	Tensor product
log	Logarithm in base two: $\log_2$
ln	Natural logarithm: $\log_e$

T_c	Critical temperature of the environment
IM	Ising Model
TIM	Transverse Ising Model

QC	Quantum Cryptography
DQC	Deterministic Quantum Cryptography
NDQC	Non-Deterministic Quantum Cryptography
QKD	Quantum Key Distribution
QBER	Quantum Bit Error Rate
QDC	Quantum Direct Communication
QD	Quantum Dialogue
(Q)EC	(Quantum) Error Correction
(Q)PA	(Quantum) Privacy Amplification
ED	Entanglement Distillation

OTP	One-Time Pad (Vernam, 1926)
RSA	Rivest, Shamir and Adleman's protocol [48]
BB84	Bennett and Brassard's protocol [49]
PP	Ping-Pong protocol [63]
CL	Cai and Li's protocol [76]
PP84	Lucamarini and Mancini's protocol [77]

Notation

In the text we use the following notation.

We indicate Pauli matrices ($\hat{\sigma}_k$), spin operators ($\hat{S}_k$), and measurement bases (B_k) with the equivalent expressions:

$$\begin{aligned}
\hat{\sigma}_z &= Z = 2\hat{S}_z = 2\mathsf{B}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
\hat{\sigma}_x &= X = 2\hat{S}_x = 2\mathsf{B}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\hat{\sigma}_y &= Y = 2\hat{S}_y = 2\mathsf{B}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.
\end{aligned}$$

The corresponding eigenstates are defined as:

$$\begin{aligned}
Z &: \ |0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ ; \ |1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
X &: \ |+\rangle = |\rightarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \ ; \ |-\rangle = |\leftarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
Y &: \ |\cdot\rangle = |\circlearrowright\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \ ; \ |\times\rangle = |\circlearrowleft\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}
\end{aligned}$$

We will be also using the following identity for operators in bi-dimensional Hilbert space ($\mathcal{K}_2$):

$$e^{-i\frac{\theta}{2}(\hat{n}\cdot\overrightarrow{\sigma})} = \left(\cos\frac{\theta}{2}\right)\mathbb{1} - i\left(\sin\frac{\theta}{2}\right)(\hat{n}\cdot\overrightarrow{\sigma}).$$

$\mathbb{1}$ is the identity operator in $\mathcal{H}_2$, $\hat{n}$ is the unit vector in the Bloch sphere and $\overrightarrow{\sigma}$ is the vector whose components are the Pauli matrices $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$.

Part I

Quantum coherence and entanglement dynamics in a symmetry-broken environment

In the last decade a huge amount of resources has been devoted to the study of new topics in the field of quantum mechanics. Protocols like quantum teleportation [1, 2] or quantum cryptography [3, 4] contributed to show, also from a practical point of view, how coherent superpositions of quantum states can perform tasks not realizable by classical means. The resource of *entanglement* [5] has been widely exploited to show nonlocality of quantum mechanics to a very high degree of precision, and became during years, a valuable tool for experimental physics, in particular in the field of quantum optics. Finally, the parallel calculation performed upon coupled two-level quantum systems (qubits) promises to issue tasks not accessible to even the fastest classical bit-based computer [6].

Notwithstanding, quantum systems are open systems, and continuously interact or exchange information with an external environment whose degrees of freedom are too numerous to be monitored. The resulting correlation between the system and the environment spoils quantum coherence and brings about the transition from a pure ensemble of quantum bits to a mixture of classical ones, in a certain preferred basis known as *pointer basis* [7, 8, 9, 10, 11]. This mechanism is called "decoherence" and it plays a crucial role in many aspects of quantum mechanics, from the theory of measurement to the problem of Schrödinger-cat states.

Several strategies has been adopted to protect coherence of open quantum systems from decay [12, 13, 14, 15]. A first class of these techniques exploits the redundancy in encoding information, in analogy with what happens in classical computation, by means of so-called error-correcting codes [16, 17, 18]. A second class considers qubits that are symmetrically coupled with the same environment to design states that are hardly corrupted by the decoherence (*decoherence free subspaces*) [19, 20]. A generalization of this latter protection strategy are the *decoherence free subsystems* [21].

In 2002 a different approach to the problem was proposed [22, 23]. It consists in making entanglement between system and environment difficult because of the macroscopic nature of environment's state under certain circumstances. We report the essential features of this model in Chapter 1.

In 2003 I extended this approach, initially developed for systems composed by a single qubit, to bipartite systems, i.e. to systems composed by two qubits [24]. Such an extension revealed to be not trivial specially because entanglement between system's qubits can occur in this case. The word "entanglement" is used to describe non-classical correlations among quantum systems. Its bizarre behavior, that leads for instance to *non-locality* of quantum mechanics, makes entanglement-related matters a very appealing field of research. In Chapter 2, after a mean-field approximation for the hamiltonian of the environment and the introduction of a particular measure of entanglement called "concurrence" , we study entanglement dynamics of a system plunged in a fermionic environment. We analytically find out *entanglement oscillations* and *decoherence-free subspaces*. Noteworthy are the references to topics like *thermal entanglement* in spin chains and *disentanglement* during the discussion.

Chapter 1

Quantum coherence dynamics

We introduce quantum decoherence through a simple model that contains all the essential features of the problem. Then we describe the fermionic environment and the mechanism of phase transition, studied with a mean field approximation. Finally we find out the time evolution of the coherence of a quantum system plunged in this kind of environment.

1.1 The decoherence process

As a general definition of "decoherence" we use the intuitive meaning given by the word itself: QUANTUM DECOHERENCE IS THE PROCESS THAT LEADS A QUANTUM SYSTEM TO LOOSE ITS COHERENCE PROPERTIES. In order to define the coherence of a quantum system we introduce the quantum state of a bi-dimensional system, written with eigenstates of $\hat{S}_z$ [1],

$$|\Psi\rangle_s = a\,|\uparrow\rangle + b\,|\downarrow\rangle\,, \tag{1.1}$$

and the associated density matrix

$$\rho_s = |\Psi\rangle_s \langle\Psi| = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}, \tag{1.2}$$

where $|a|^2 + |b|^2 = 1$. The diagonal terms of Eq.(1.2) represent the probabilities of the two possible values 'up' and 'down', and are usually referred to as the *occupation* or *population*. The off-diagonal terms are defined *coherences*: they are associated with the amplitude of the interference patterns and quantify the coherence of the pure state. This definition is widespread in the field of nuclear magnetic resonance. Its extension to systems of higher dimensionality presents no difficulties, as the only request is of being able to individuate density matrix's off-diagonal elements in any dimension. By canceling off-diagonal coefficients, that express purely quantum correlations, from Eq.(1.2) we obtain a *reduced density matrix* with only classical correlations [9]:

$$\begin{aligned} \rho_r &= \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix} \\ &= |a|^2\,|\uparrow\rangle\langle\uparrow| + |b|^2\,|\downarrow\rangle\langle\downarrow|\,. \end{aligned} \tag{1.3}$$

[1] We remark that we will indifferently adopt by convenience either the *arrow notation* $\{|\uparrow\rangle, |\downarrow\rangle\}$ or the *computational notation* $\{|0\rangle, |1\rangle\}$ for the $\hat{S}_z$ eigenstates.

The process leading from Eq.(1.2) to Eq.(1.3) is non-unitary and represents just what we mean for "decoherence" . The same process is sometimes described as a transition from "quantum" to "classical" world. The study of the entropy can help to clarify this point.

The entropy S of a quantum system represented by a density matrix ρ is called von Neumann entropy and it is defined as [25]:

$$S(\rho) = -Tr\left(\rho \log \rho\right), \tag{1.4}$$

where logarithms are intended in base two. When ρ represents a pure state, i.e. when $\rho^2 = \rho$, its eigenvalues are 0 and 1, and infinities appear in Eq.(1.4). In this case von Neumann entropy is defined equal to zero: $S(\rho) = 0$.

Now we can note that entropy increases when decoherence occurs: ρ_s in Eq.(1.2) is a pure state, hence its von Neumann entropy is zero, while ρ_r in Eq.(1.3) is a mixed state whose von Neumann entropy amounts to

$$\begin{aligned} S(\rho_r) &= -Tr\left(\rho_r \log \rho_r\right) \\ &= -\left|a\right|^2 \log \left|a\right|^2 - \left|b\right|^2 \log \left|b\right|^2 . \end{aligned} \tag{1.5}$$

Entropy (1.5) is equal to the classical Shannon entropy H of a biased coin toss which gives heads with probability $p = \left|a\right|^2$ and tails with probability $q = 1 - p = \left|b\right|^2$:

$$\begin{aligned} H(p) &= -\sum_i p_i \log p_i \\ &= -p \log p - q \log q. \end{aligned} \tag{1.6}$$

This means that density matrix (1.3) allows a classical description in terms of ensemble preparation: as the coin is prepared in the state 'head' or 'tail' a fraction $\left|a\right|^2$ or $\left|b\right|^2$ of times, the system represented by ρ_r can be thought as prepared in the state $\left|\uparrow\right\rangle$ or $\left|\downarrow\right\rangle$ respectively a fraction $\left|a\right|^2$ or $\left|b\right|^2$ of the times. It is evident that the state ρ_s does not allow the same classical interpretation.

The necessity for a classical interpretation for the outcomes of a quantum system's measurement led von Neumann in the early 30s to *postulate* the non-unitary process today called quantum decoherence. Nonetheless this postulate can be removed when the dynamics of an *open* quantum systems is taken into account.

Let us suppose the quantum system S and the environment E, whose eigenstates $\{\left|\varepsilon_\uparrow\right\rangle, \left|\varepsilon_\downarrow\right\rangle\}$ are mutually orthogonal, to be initially uncorrelated. Their joint initial state can be written as:

$$\left|\Phi_0\right\rangle = \left|\Psi\right\rangle_s \otimes \left|\varepsilon_\uparrow\right\rangle . \tag{1.7}$$

The state (1.7) can always be prepared by means of a projective measurement on the system that decouples it from the environment. Then we imagine an interaction between system and environment leading to the following dynamics:

$$\begin{aligned} \left|\Phi_0\right\rangle &= a\left|\uparrow\right\rangle_s \left|\varepsilon_\uparrow\right\rangle + b\left|\downarrow\right\rangle_s \left|\varepsilon_\uparrow\right\rangle \\ &\longrightarrow a\left|\uparrow\right\rangle_s \left|\varepsilon_\uparrow\right\rangle + b\left|\downarrow\right\rangle_s \left|\varepsilon_\downarrow\right\rangle = \left|\Phi_t\right\rangle , \end{aligned} \tag{1.8}$$

i.e. environment's state is flipped when system's state is *down*, and it is left unaltered when system's state is *up*. This entails that at time t the environment becomes quantum correlated, or rather *entangled*, with the system, because its eigenstates are differently modified by system's ones. The environment is supposed to be a huge collection of modes whose states are impossible to know or to control anyhow; as a consequence, the density matrix of the system at time t is obtained from

Eq.(1.8) by ignoring (tracing over) the information contained in the unknown degrees of freedom of the environment:

$$\begin{aligned}\rho_s(t) &= Tr_E\left[|\Phi_t\rangle\langle\Phi_t|\right] \\ &= \langle\varepsilon_\uparrow|\Phi_t\rangle\langle\Phi_t|\varepsilon_\uparrow\rangle + \langle\varepsilon_\downarrow|\Phi_t\rangle\langle\Phi_t|\varepsilon_\downarrow\rangle \\ &= |a|^2|\uparrow\rangle\langle\uparrow| + |b|^2|\downarrow\rangle\langle\downarrow|\,. \end{aligned} \tag{1.9}$$

The state written above is equal to the *reduced density matrix* of Eq.(1.3); indeed the term "reduced" refers just to the reduction process that occurs in Eq.(1.9) when the bath degrees of freedom are traced over. We see that the interaction between system and environment described above leads to decoherence, and realizes in all respects the non-unitary evolution postulated by von Neumann. We refer to this kind of decoherence as *environment induced decoherence*, and it is the only we will consider in the present work.

At this point a little remark is mandatory. So far we have been using the basis $\hat{S}_z$ to describe the decoherence process, but it is not the only possible choice. Yet, the mixed state (1.9) could be written in the basis $\hat{S}_x$ as well, with new coefficients c and d:

$$\rho_s(t) = |c|^2|\rightarrow\rangle\langle\rightarrow| + |d|^2|\leftarrow\rangle\langle\leftarrow|\,. \tag{1.10}$$

So, why is the basis $\hat{S}_z$ special? The answer is in the dynamics described by Eqs.(1.8): we can see that the eigenstates of $\hat{S}_z$ are not modified by the interaction. On the contrary if we used, for example, the upper eigenstate of $\hat{S}_x$ we would obtain:

$$\begin{aligned}|\rightarrow\rangle_s|\varepsilon_\uparrow\rangle &= \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_s|\varepsilon_\uparrow\rangle + |\downarrow\rangle_s|\varepsilon_\uparrow\rangle\right) \\ &\longrightarrow \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_s|\varepsilon_\uparrow\rangle + |\downarrow\rangle_s|\varepsilon_\downarrow\rangle\right) \\ &= \frac{1}{2}\left[|\rightarrow\rangle_s\left(|\varepsilon_\uparrow\rangle + |\varepsilon_\downarrow\rangle\right) + |\leftarrow\rangle_s\left(|\varepsilon_\uparrow\rangle - |\varepsilon_\downarrow\rangle\right)\right], \end{aligned} \tag{1.11}$$

i.e. the state changes under the action of the interaction because the states of the environment vary according to $\hat{S}_z$. So the environment selects in a natural way a preferred basis for decoherence, and this clarifies in some respects the expression *environment induced decoherence* utilised above. This privileged basis is for historical reasons called the *pointer basis*, because originally it represented the only basis of an ideal quantum detector capable of maintaining the information about the measured system also in presence of an environment [7, 8]. In practice the pointer basis coincides often with the basis of the system that diagonalizes the interaction hamiltonian $\mathcal{H}_I$ between system and environment. Nevertheless $\mathcal{H}_I$ acts both on system and on environment states, so its eigenvectors are not necessarily given by the direct product of system eigenvectors and environment ones; moreover the interaction with the environment could result not dominant over the self-hamiltonian of the system. For these reasons the search of the pointer basis could ensue in a quite difficult undertaken, and a more general *predictability sieve* criterium to find it out has been formulated [26, 27, 28]. In the present work such a complicated situation does not occur, and the choice of the pointer basis results always clear by the context.

A slightly more involved example of decoherence is represented by the following toy-model due to Preskill [29], whose aim is to introduce a purely dephasing mechanism of decoherence in a simple way. The interest of such a model is that decoherence occurs only via phase-related exchanges of information between system and environment, while no energy transfer takes place.

We take a bosonic environment constituted by a large number of photons each of which interacts with the system for a short time Δt and then is scattered off in random directions. Given the *arrow basis* (see Note 1) for a two-level system and the states $\{|0\rangle, |1\rangle, |2\rangle\}$ for a three-level mode of radiation, the interaction between the system and the k-th degree of freedom of the environment can be described as:

$$|\uparrow\rangle_s |0\rangle_k \longrightarrow \sqrt{1-p}\,|\uparrow\rangle_s |0\rangle_k + \sqrt{p}\,|\uparrow\rangle_s |1\rangle_k \tag{1.12}$$

$$|\downarrow\rangle_s |0\rangle_k \longrightarrow \sqrt{1-p}\,|\downarrow\rangle_s |0\rangle_k + \sqrt{p}\,|\downarrow\rangle_s |2\rangle_k . \tag{1.13}$$

The interaction above is similar to that occurring in a *phase damping channel* [25] during the time Δt of the photon transit, and is not too different from that of Eq.(1.8). The system does not make any transition, while the environment scatters off with probability p. Writing the matrix representation of the above states, and evaluating the partial trace over the k-th degree of freedom of the environment, in analogy to Eq.(1.9), we obtain the reduced system density matrix:

$$\rho_s^k(t) = \begin{bmatrix} \rho_{\uparrow\uparrow} & (1-p)\,\rho_{\uparrow\downarrow} \\ (1-p)\,\rho_{\downarrow\uparrow} & \rho_{\downarrow\downarrow} \end{bmatrix}, \tag{1.14}$$

where $\rho_{\uparrow\uparrow}$ is the coefficient of the term $|\uparrow\rangle_s \langle\uparrow|$ at the initial time.

In this case the attenuation of the off-diagonal elements is only partial while the diagonal terms remain unaffected by the interaction. However expression (1.14) concerns only one interaction, that of a single mode of radiation of the environment with the system, that eventually scatters it away. Other photons from the bath are going to interact with the system, and the whole trace over environment is obtained when all its N degrees of freedom are taken into account, repeating the two steps of temporal evolution and partial trace N times. This leads to a final system density matrix of the form:

$$\rho_s(t) = \begin{bmatrix} \rho_{\uparrow\uparrow} & (1-p)^N\,\rho_{\uparrow\downarrow} \\ (1-p)^N\,\rho_{\downarrow\uparrow} & \rho_{\downarrow\downarrow} \end{bmatrix}. \tag{1.15}$$

Being p a quantity less than one, we have an exponential attenuation of the off-diagonal elements. Suppose the probability of a scattering event per unit time is Γ, so that $p = \Gamma\Delta t << 1$ when time Δt elapses. The term $(1-p)^N$ values

$$(1-p)^N = (1-\Gamma\Delta t)^{\frac{t}{\Delta t}} \longrightarrow \exp(-\Gamma t) \tag{1.16}$$

when $\Delta t \longrightarrow 0$. This represents an exponential decay of the coherence of the quantum system.

The result above is attainable both by means of a superoperator formalism and by the formulation of a *master equation* [10, 30]. The latter approach describes the evolution of the reduced system density matrix by means of a differential equation. There are several ways to obtain such an equation, but all of them contain more or less explicitly a *Markov approximation*, which establishes that the system density matrix $\rho_s(t+\Delta t)$ is completely determined by $\rho_s(t)$. This is an approximation because, for what we said above, the evolution is supposed to be predictable only when the whole combination system-environment is taken into account. This approximation leads to an intrinsically irreversible dynamics similar to Eq.(1.16), and is as worse as short times are taken into account. The evolution described by Eqs. (1.12), (1.13) is unitary. This means that there exists an interaction hamiltonian that governs it. This hamiltonian is of the form $\mathcal{H}_I = \sum_i \chi a^\dagger a (b_i^\dagger b_i)$ [29] and describes a loss of quantum information from the system without a loss of energy, a purely quantum mechanical effect. This effect is determined by the randomization of the phase of the system by the environment and takes the name of *phase damping*. This mechanism is of the utmost importance because it is much faster than other relaxation mechanisms involving energy

exchanges. All the same, the phase damping channel applied to harmonic oscillator models, is used to find out the exponentially fast decay of macroscopic objects, thus contributing to explain Schrödinger paradox [25]. The effect of phase damping is reported in Fig.1.1: the Bloch sphere is shrunk uniformly in the $x-y$ plane, while is left unchanged along the z axis. We can thus affirm

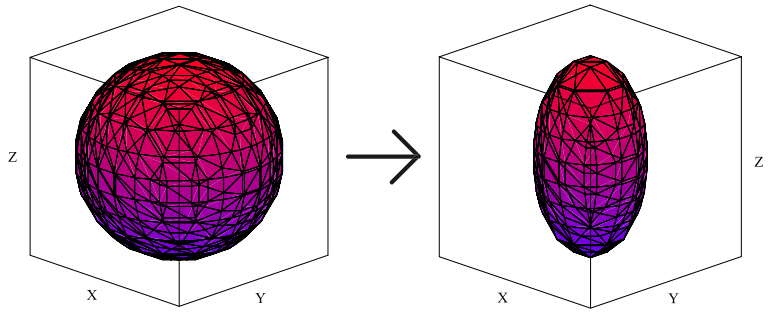

Figure 1.1: Effect of phase damping (Eqs.(1.12) and (1.13)) on system's density matrix when $p = 0.3$. It is evident that the preferred decoherence basis (*pointer basis*) is along z axis, because it is the only one left unaltered by interaction with environment.

that $\hat{S}_z$ is the pointer basis of the phase damping described by Eqs.(1.12) and (1.13).

Henceforth we consider only phase damping-like decoherence. It is usually the most important kind of decoherence both because it is by far the fastest one and because when energy exchanges between system and environment do not occur analytical solutions to system's density matrix temporal evolution can be provided, as will be clear in the next sections.

1.2 Fermionic environment

Now we are going to consider a less popular model of decoherence, in which the qubit interacts with an environment composed by other N fermionic systems, that we assume to be spin-1/2 particles.

We rewrite the general state of a qubit as a combination of eigenstates of $\hat{S}_z$, in the *arrow notation*:

$$|S\rangle = \cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}\sin\frac{\theta}{2}|\downarrow\rangle. \tag{1.17}$$

The associated density matrix is given by the projector on this state:

$$\begin{aligned}\rho_S &= |S\rangle\langle S| = \frac{1}{2} + \mathbf{n}\cdot\mathbf{S} \\ &= \begin{pmatrix} \cos^2\frac{\theta}{2} & \frac{1}{2}e^{-i\phi}\sin\theta \\ \frac{1}{2}e^{i\phi}\sin\theta & \sin^2\frac{\theta}{2} \end{pmatrix} \\ &= \frac{I}{2} + \cos\theta\hat{S}^z + \frac{1}{2}\sin\theta\left(e^{-i\phi}\hat{S}^+ + h.c.\right),\end{aligned} \tag{1.18}$$

with $\mathbf{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ vector that lies on the surface of the Bloch sphere. As a consequence of the Schrödinger equation, the temporal evolution of the isolated qubit is unitary and so an initial pure state evolves into another one, maintaining its coherence. Likewise, the evolution of the density matrix allows the vector n to move only on the surface of the sphere.

Introducing an external environment, we enlarge the Hilbert space and we must consider the evolution of the overall system including the bath. Analogously to Eq.(1.7), we can take without

loss of generality the initial density matrix of the composed system to be $\rho(0) = \rho_S \otimes \rho_B$; in general, during the evolution, it will not maintain the form of a product, as the environment tends to become entangled with the qubit. The single qubit dynamics is then obtained via the partial trace on the states of the bath of the total density matrix evolved in time:

$$\rho_S(t) = Tr_B \left\{\rho(t)\right\} = Tr_B \left\{e^{-i\mathcal{H}t}\rho(0)e^{i\mathcal{H}t}\right\}, \tag{1.19}$$

where the Hamiltonian $\mathcal{H}$ is given by the unperturbed contribution of qubit and bath to the energy and by their mutual interaction:

$$\mathcal{H} = \mathcal{H}_s + \mathcal{H}_{sB} + \mathcal{H}_B \tag{1.20}$$

The temporal evolution of the reduced matrix in Eq.(1.19) is no longer unitary [29] and can determine a suppression of the off-diagonal elements of ρ_S. Likewise, the vector $\mathbf{n}$ leaves the surface of the Bloch sphere and evolves into its internal vectors, so the initial pure state of the qubit collapses into a statistical mixture of classical bits, losing its coherence. We can note that the system evolves under a *continuous interaction* with the environment. This makes the dynamics very different from that of the previous model, allowing the evolution to keep an intrinsic reversibility.

If the combination of system and bath counts a finite number of degrees of freedom, the space of accessible configurations is limited, and some general theorems [31], similar to the Poincaré's in classical mechanics [32], assure that the total state $|\Phi(t)\rangle$ will return arbitrarily close to the initial state an infinite number of times. Thus given $\epsilon > 0$ exists a time T such that

$$|\langle\Phi(T)|\Phi(0)\rangle|^2 = 1 - \epsilon.$$

This recurrence property will reflect also on the off-diagonal coefficients of the density matrix, and on its partially traced version. As a consequence there will be a periodicity also in the non-unitary evolution of system's coherence. The times in which coherence travels back from the environment to the system are often called *recoherences*. Recoherences occur in a time that increases with the number of the degrees of freedom of the environment, i.e. on a Poincaré temporal scale. This could make the phenomenon undetectable because these times can be longer than the age of universe. Anyhow the conceptual difference is relevant: the functional form of the evolution described by Eq.(1.16) presents no particular time symmetry; on the contrary it is evident that a substitution of t with $(-t)$ in Eq.(1.19) provides just a temporal inversion of the evolution. This point will result clearer after the following example, also due to Zurek [8].

We suppose that only the interaction hamiltonian $\mathcal{H}_I$ of Eq.(1.20) is taken into account. Bath and system hamiltonians are assumed to be constant. The interaction we want to study is given by a linear coupling in the z component of the spin:

$$\mathcal{H}_I = -\frac{J}{\sqrt{N}} \sum_{k=1}^{N} \hat{S}^z \hat{S}^z_k, \tag{1.21}$$

where J is a positive constant and the factor $\sqrt{N}$ is present for normalization reasons that will be clear later on. We suppose that the initial state of system and bath can be written as

$$|\,\psi(0)\,\rangle = |\,S\,\rangle \prod_k (\alpha_1^k|\uparrow\rangle_k + \alpha_2^k|\downarrow\rangle_k). \tag{1.22}$$

We can think this to be possible in the limit of high temperature; the normalized coefficients α_1^k, α_1^k get random values, and $|\downarrow\rangle_k$ e $|\uparrow\rangle_k$ are $\hat{S}^z_k$ eigenstates. The state, evolved under (1.21), becomes:

$$|\,\psi(t)\,\rangle = \cos\frac{\theta}{2}|\uparrow\rangle|\,\epsilon_\uparrow(t)\,\rangle + e^{i\phi}\sin\frac{\theta}{2}|\downarrow\rangle|\,\epsilon_\downarrow(t)\,\rangle \tag{1.23}$$

with

$$|\,\epsilon_\uparrow(t)\,\rangle = |\,\epsilon_\downarrow(-t)\,\rangle = \prod_k (\alpha_1^k e^{-i\frac{J}{\sqrt{N}}t}|\uparrow\rangle_k + \alpha_2^k e^{i\frac{J}{\sqrt{N}}t}|\downarrow\rangle_k). \tag{1.24}$$

By rewriting state (1.23) as a density matrix $\rho_S(t) = |\,\psi(t)\,\rangle\langle\,\psi(t)\,|$ we find that only its off-diagonal terms evolve in time. They are mutually complex conjugate for the hermicity condition of the density matrix, hence it suffices to study only one of them. Easy calculations lead to:

$$\langle\downarrow|\rho_S(t)|\uparrow\rangle = \langle\downarrow|\rho_S(0)|\uparrow\rangle r(t), \tag{1.25}$$

with

$$r(t) = \prod_k \left(\cos\frac{Jt}{2\sqrt{N}} - i(2|\alpha_1^k|^2 - 1)\sin\frac{Jt}{2\sqrt{N}}\right). \tag{1.26}$$

Eq.(1.25) shows that the off-diagonal matrix element differs from the corresponding coefficient at $t = 0$ only for a multiplicative factor $r(t)$ that, henceforth, we will call *decoherence factor*. Every phase factor in $r(t)$ is not essential for the suppression of the interference terms; only the absolute value is relevant, and it amounts to

$$|r(t)|^2 = \prod_k \left(1 - 4|\alpha_1^k|^2(1 - |\alpha_1^k|^2)\sin^2\frac{Jt}{2\sqrt{N}}\right). \tag{1.27}$$

At the initial time we have of course $|r(0)|^2 = 1$; thus we can see that the function is periodic with period $T = \frac{\pi\sqrt{N}}{J}$ (see Fig.1.2). Furthermore it results an even function of time; hence each substitution of t with $(-t)$ will leave it unaltered. This entails the complete temporal reversibility mentioned above.

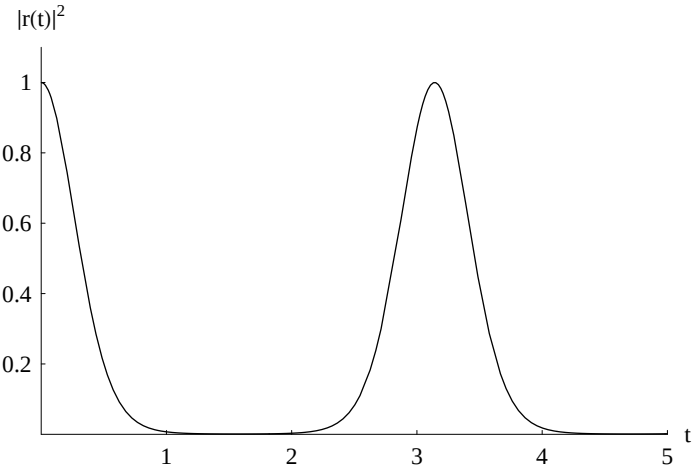

Figure 1.2: Decoherence factor as a function of time. In this plot we set J=20 and N=100.

As we saw, general theorems state that for a finite number N of degrees of freedom of the bath we expect that the value of $|r(t)|^2$ will pass closely to its initial value an infinite number of times, with a periodicity T. This result is analogous to the Poincaré theorem; its rational assure us that the initial information is not lost irreversibly in the bath, but rather the bath gives back it to the system after a while. However it is intuitive that the period of such a recurrence depends on the

number N itself. As a consequence, when N is very high, an effective irreversible loss of coherence will occur.

A further effect of this kind of approach, not independent from the above considerations about reversibility, is the horizontal tangent to the curve in its initial point, i.e. for short times, in contrast to what obtained from the dynamics described by Eq.(1.16). This means that a quantum system looses its coherence slowly until time is much less than the characteristic time of interaction. In turn this entails that if a measurement is performed on the system in this temporal range, the probability the system collapses into its initial state (for which $|r(t)|^2 = 1$) is very high, approaching unity. Fast repeated measurements on the system could thus prevent it from decohering at all. This is a particular aspect of what is known as *Zeno effect* [33, 34, 35].

It is interesting to expand to the first order Eq.(1.27) for $t \ll \sqrt{N}$:

$$|r(t)|^2 \simeq \prod_k \left(1 - |\alpha_1^k|^2(1 - |\alpha_1^k|^2)\frac{J^2t^2}{N}\right). \tag{1.28}$$

The obtained result can be approximated further on by an exponential

$$|r(t)|^2 \simeq e^{-f^2J^2t^2} \tag{1.29}$$

introducing the factor f

$$f^2 = \frac{1}{N}\sum_k |\alpha_1^k|^2(1 - |\alpha_1^k|^2) = \langle |\alpha_1^k|^2(1 - |\alpha_1^k|^2)\rangle. \tag{1.30}$$

In this expression we used the fact that each contribution is equally probable in the limit of high temperature. Decoherence time can be evaluated as $\tau_{dec} = \frac{1}{fJ}$. In this temporal range the agreement between the approximated and exact functions is fine also for a small number of bath degrees of freedom.

We notice that the number N enters the above expressions only in the period of recurrence, but not in the decoherence time. This is due to the choice of $\sqrt{N}$ for the normalization constant in (1.21). On the contrary a weaker interaction, with N instead of $\sqrt{N}$, would lead to a decoherence time $\tau_{dec} = \frac{\sqrt{N}}{fJ}$, i.e. decoherence would never occur in this regime, making it of no interest. Nevertheless a stronger interaction would lead to a faster decoherence; but, as the attenuation of the off-diagonal terms is already exponential, it would add no interest to the problem.

As far as the factor f is concerned we note that it assumes in the limit of high temperature its maximum value $f = \frac{1}{2}$, corresponding to a decoherence time of $\tau_{dec} = \frac{2}{J}$. Its range belongs to the interval $0 \leq f \leq \frac{1}{2}$; the value 0 (decoherence time is infinite in this case) corresponds to a completely ordered configuration, in which the spins of the environment are all oriented in the same direction. This case is not compatible with the limit of high temperature we conjectured, but it anticipates the effect of a bath phase ordering on the process of decoherence.

1.3 Ising-Model and the role of an ordered environment

So far we have been supposing a constant bath hamiltonian, and the only role of the environment was to land its states in the limit of high temperature to permit decoherence to take place. The states of environment were all independent from one another. Now we want to introduce a statistical correlation inside the bath owned to a spontaneous symmetry breaking, and study the effect of this change on the decoherent process envisaged in the previous section.

We require the bath hamiltonian to be separable into the single elements hamiltonians of the bath,

$$\mathcal{H}_B = \sum_k \mathcal{H}_B^k$$

with $\left[\mathcal{H}_B^k, \mathcal{H}_B^{k'}\right] = 0$. This condition can be exactly satisfied (for example, in a set of non-interacting spins in an external magnetic field), or a mean field approximation can be introduced, as we will see later. We are mainly interested in a temporal range that is small in comparison to the characteristic time of the interaction. In particular, we will study an interaction with coupling constants $g_k \propto 1/\sqrt{N}$ in a temporal range $t \ll \tau \sim 1/g_k$; N is the number of environment elements and is typically very large, so this hypothesis is not restrictive. Note that such an assumption prevents us from observing any periodic recoherence phenomenon because it occurs after a time longer than the effectiveness of the model.

We also assume that the interaction with the qubit does not affect the dynamics of the bath, or its contribution is negligible. This hypothesis is known as *molecular chaos-ansatz* or *Stosszahl-ansatz*. The rational behind this approximation is that the bath has so many degrees of freedom that the effects of the interaction with the system dissipate away in it and will not influence the system back to any significant extent. This entails that the bath remains at thermal equilibrium at constant temperature, irrespective of the amount of energy diffusing into it from the system. As a consequence, for a bath whose density matrix is represented by the Boltzmann distribution

$$\rho_B(0) = \frac{e^{-\beta\mathcal{H}_B}}{Z} \tag{1.31}$$

we have that the mean value of any bath operator can be considered time independent. In Eq.(1.31) $Z = Tr_B\left(e^{-\beta\mathcal{H}_B}\right)$ is the partition function, $\beta = 1/k_BT$ is the inverse temperature of the bath, T the temperature and k_B the Boltzmann constant. The *Stosszahl-ansatz* traduces into the following commutation relation:

$$[\mathcal{H}_I, \mathcal{H}_B] = [\mathcal{H}, \mathcal{H}_B] = 0. \tag{1.32}$$

In some of the models we examine Eq.(1.32) will be exactly satisfied. In other cases it will be only approximately true.

We observe that usually the following picture is adopted: the initial state of the full system is given by

$$\rho(0) = \rho_S(0) \otimes \rho_B(0). \tag{1.33}$$

When the interaction is switched on at time $t = 0$, the full system's evolution is assumed to be given approximately by:

$$\rho(t) \simeq \rho_S(t) \otimes \rho_B(0), \tag{1.34}$$

that is, the state of the heat bath does not change in time to any significant extent. A deeper observation of equations (1.33) and (1.34) reveals that they describe precisely the *Markov approximation* mentioned above, since only the system density matrix ρ_S changes in time to a considerable extent. Then, by virtue of Eq.(1.19), one can notice that the Stosshal-ansatz implies the Markov approximation through Eqs.(1.33, 1.34). This would entail that also the Stosshal-ansatz leads to an intrinsically irreversible decoherence process, along to that described by the master equations after the Markov approximation is established.

Nevertheless in our description we do not assume Eq.(1.34) to hold, because entanglement makes system and environment not separable as soon as interaction is switched on. This allows our picture to mantain the intrinsic reversibility of the decoherence process.

We finally notice that the following commutation rules can easily occur:

$$[\mathcal{H}_S, \mathcal{H}] = [\mathcal{H}_S, \mathcal{H}_I] = 0, \tag{1.35}$$

Their physical meaning resides in the conservation of the energy of the system, i.e. the system does not exchange energy with the bath. As we said, phase decoherence occurs in a time far shorter than that pertaining to relaxation due to exchanges of energy with the bath. Thus, commutation rule (1.35) can be considered always approximately true for short times. This led several authors to make large use of this relation, since it results very useful to extract analytical results. We implicitly adopt it too when we will assume a constant system hamiltonian.

1.3.1 Phase transition

Now we are going to study what happens to system's coherence when an ordered phase appears in the environment. The simplest model endowed with a phase transition is the *Ising model* [36], indicated as IM, represented by a collection of spins coupled by means of an infinite range interaction:

$$\mathcal{H}_B = -\frac{J}{N}\sum_{i,j}\hat{S}_i^z\hat{S}_j^z. \tag{1.36}$$

Here the coupling constant J has been scaled with the number of particles of the bath to make energy an extensive quantity. In the double sum of Eq.(1.36) appear also terms corresponding to $i = j$ that is a self-interaction without any physical meaning. Nonetheless being $(\hat{S}_i^z)^2 = \frac{1}{4}$, the apport of such terms represent an identical constant for all the configurations which, by recalibrating the zero of the energy, does not modify the physical properties of interest. So, henceforth, the bath coupling constant J is intended to be the recalibrated one.

A method commonly used to study Eq.(1.36) is the *mean field approximation* [37]. In such an approximation each particle is plunged in a magnetic field generated by all the other spins that spontaneously order below a certain temperature. It is worth remarking that mean field approximation, although takes into account the total effect of the interactions among the particles, neglects the effect of entanglement between them. In other words the spin are not considered independent anymore, but remain uncorrelated.

In a phase transition the ensemble of possible configurations is restricted to a limited portion of space in which the system remains for times that increase with the dimension of the system itself. Therefore only averages performed on such regions are meaningful. In the case of a spontaneous symmetry breaking such regions are usually associated to a non-zero average value of a suitable operator (order parameter). Assuming then that the average of the spin variables is the same in all configurations we can write:

$$\left(\frac{1}{N}\sum_k \hat{S}_k^z - m\right)^2 \simeq 0. \tag{1.37}$$

In this case is the value of m to play the role of an order parameter, and the approximation is the better the higher the number of spins in the bath. This expression lets us linearize Eq.(1.36) in the operator defined by the sum of spin operators. Expanding the square in Eq.(1.37) it is possible to substitute the square of the sum with the product of the sum itself versus the mean field m, plus a constant contribution proportional to m^2. We can thus define a new approximate hamiltonian

$$\mathcal{H}_B^{cm} = -2Jm\sum_k \hat{S}_k^z + m^2 JN. \tag{1.38}$$

The average value of $\hat{S}_k^z$ must be self-consistently determined with the introduced field. This average, as conjectured, is nothing but the order parameter m. To find out its value we must minimize the density of free energy relative to the new hamiltonian, defined as

$$\begin{aligned} \overline{E} &= \frac{F}{N} = -\frac{1}{N\beta}\log Tr\{e^{-\beta\mathcal{H}_B^{cm}}\} = \\ &= m^2 J - \frac{1}{\beta}\log[2\cosh\beta Jm]. \end{aligned} \tag{1.39}$$

This is equivalent to minimize the average value of the total energy.

By derivating Eq.(1.39) with respect to m and by posing the result equal to zero we obtain the trascendental Curie-Weiss equation for the spontaneous magnetization of the environment

$$m = \frac{1}{2}\tanh\beta Jm. \tag{1.40}$$

Eq.(1.40) can be solved graphically: its solutions correspond to intersections of the straight line $y_1 = m$ with the function $y_2 = \frac{1}{2}\tanh\beta Jm$, as reported in Fig.1.3. As it is easily seen

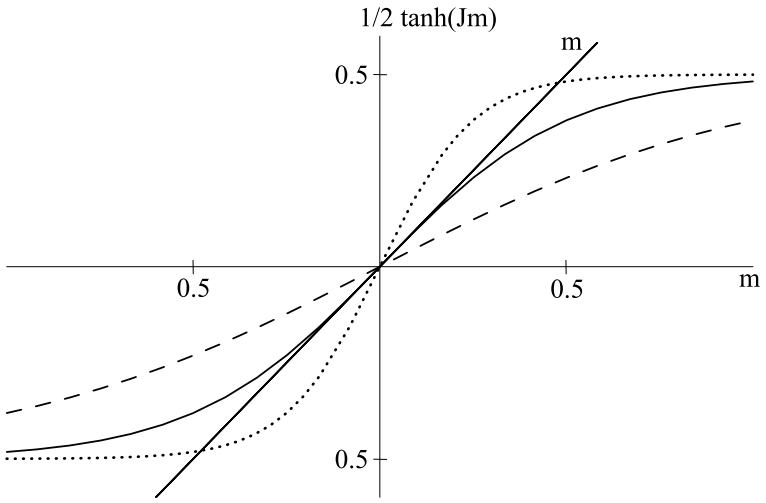

Figure 1.3: Graphical solution of the Curie-Weiss equation. The straight line represents the curve $y_1 = m$; the other lines are the curves $y_2 = \frac{1}{2}\tanh\beta Jm$ for various temperatures. Above the critical value T_c (dashed line) the only intersection is in the origin. At T_c (solid line) there is a tangential point in the origin. Below T_c (dotted line) there are two other intersections beside the origin corresponding to the two opposite values of the order parameter m.

the number of solutions depends on the slope of the latter function: if its derivative is less than one the intersection with the line will be unique and coincident with zero. This occurs when the temperature exceeds a critical value T_c determined by condition of tangency in the origin of the two functions y_1 e y_2. This condition is obtained by making equal the derivatives and corresponds to

$$\beta_c = \frac{1}{KT_c} = \frac{2}{J}\ . \tag{1.41}$$

For $T \geq T_c$, the density of free energy assumes its minimum for $m = 0$, the system does not order and mean field approximation is no more valid. On the opposite, when $T < T_c$, we have three intersections: one is zero and the others are $\pm m(\beta)$, symmetrically distributed by the origin. The origin is not a maximum this time, and therefore is unstable. The equilibrium configurations correspond to the two possible values of the magnetization $\pm m(\beta)$. It is possible to see that, in the limit of zero temperature such a magnetization tends asymptotically towards the value $m(\beta \to \infty) = \pm\frac{1}{2}$.

With this new formalism in hands we can trace back the steps leading to the decoherence factor $r(t)$ in the preceding example. The new expression for the decoherence factor becomes:

$$|r(t)|^2 \simeq e^{-J^2 t^2 (\frac{1}{4} - m^2)}, \tag{1.42}$$

with m given by Eq.(1.40). It is possible to see from Eq.(1.42) how a symmetry breaking in the environment can reduce the loss of coherence. In fact, by decreasing temperature, the order parameter m tends to the value $1/4$, and the decoherence factor tends to become constant. In other words decoherence time increases indefinitely. This is quite a counter-intuitive effect since collective quantum properties of materials endowed with phase transition disappear as ordering increases (see for instance Ref. [38]). The phase transition and the consequent ordering of the spins of the bath are essential for slowing down the flow of coherence and information of the initial qubit state towards the bath. The factor t^2 in the exponent denotes the intrinsically reversible nature of the process. Decoherence takes place in the limit of an environment with infinite degrees of freedom; besides, the same limit is necessary to support the mean field theory approach we adopted. Thus in this context the limit $N \to \infty$ has a double function: to take into account the decoherence process and to give a meaning to the mean field approximation written above.

In the next section we are going to add a transverse field to the long ranged IM-like bath hamiltonian (1.36), thus obtaining a *Transverse Ising Model* bath hamiltonian, in short TIM. TIM environment will be studied by using again a mean field approximation.

1.4 Transverse-Ising-Model

The following hamiltonians define the energy of the system, of the TIM-bath and of the interaction between them:

$$\mathcal{H}_s = -\mu_0 \hat{S}_0^z, \tag{1.43}$$

$$\mathcal{H}_{sB} = -\frac{J_0}{\sqrt{N}} \hat{S}_0^z \sum_k \hat{S}_k^z \,, \tag{1.44}$$

$$\mathcal{H}_B = -w \sum_k \hat{S}_k^x - \frac{J}{N} \sum_{i,k} \hat{S}_i^z \hat{S}_k^z \,, \tag{1.45}$$

where μ_0 is the coupling constant with an external magnetic field parallel to the $\hat{z}$ axis, J_0, J are exchange coupling constants and w is the strength of the transverse field; they are all non-negative constants. The indices of the sums run from 1 to N. Eq.(1.45) describes a material in which spins compete to align along the positive direction of $\hat{x}$ axis or along $\hat{z}$ axis following a ferromagnetic behaviour; of course in the latter case the absolute direction of alignment is not important since the hamiltonian is symmetric in z-operators. We can notice that energy exchanges between system and bath are not included in the interaction hamiltonian; this will generate a pure dephasing dynamics, in which energy will be conserved, and temporal evolution analytically solved, according to relation (1.35).

The mean field approximation for TIM environment is analogous to Eq.(1.38), and reads:

$$\mathcal{H}_B^{mf} = -w \sum_k \hat{S}_k^x - 2Jm \sum_k \hat{S}_k^z + m^2 JN \,. \tag{1.46}$$

In the above equation m is again the order parameter of the phase transition. Its absolute value ranges from 0 to $\frac{1}{2}$ as long as temperature ranges from the critical value $T_c = \frac{J}{2}$ to 0 : the greater $|m|$ the larger the magnetic order of the bath along $\hat{z}$ axis. In the following we are going to consider only positive values for m since results are sign-independent. Everything remains true with the substitution $m \to -m$. This is a consequence of $\mathcal{H}_B$ z -symmetry, that is not lost in $\mathcal{H}_B^{mf}$. Also in this case the order parameter m is implicitly defined by the following self-consistent equation for the quantity $\Theta = \pm\sqrt{w^2 + 4m^2J^2}$ (also Θ's sign, written here for sake of precision, is irrelevant, for the same reasons of m's):

$$\frac{\Theta}{J} = \tanh \frac{\Theta}{2T}. \tag{1.47}$$

The graphical solution is reported in Fig.1.4. It is worth noting that from Eq.(1.47) we have $\Theta \to J$ for $T \to 0$; furthermore, from the definition of Θ, we can see it tends to $2mJ$ in the limit of no transverse field ($w \to 0$).

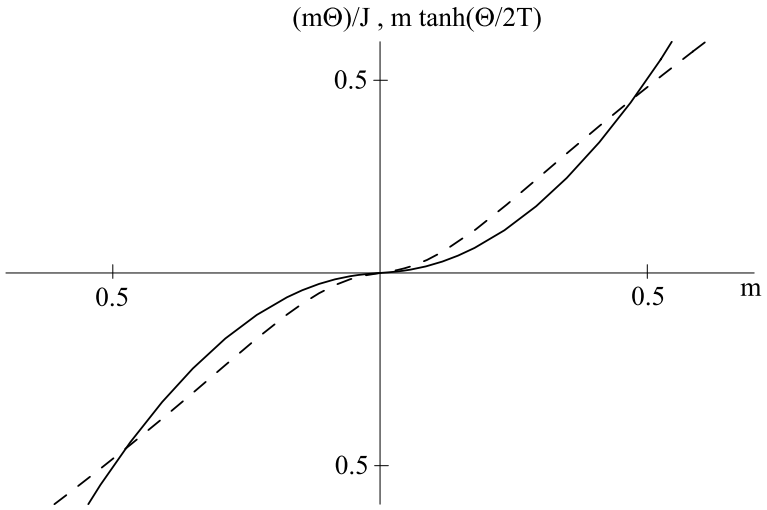

Figure 1.4: Graphical solution of the Curie-Weiss equation (1.47) with $T_c/T = 2$ and $w/J = 0.1$. The dotted line represents the curve $m\tanh(\Theta/2T)$; the solid line represents the curve $m\Theta/J$.

Together with Eq.(1.47) we must consider the following condition on the transverse field to obtain an ordered phase with TIM:

$$\frac{w}{J} < \tanh\left(\frac{w}{2T}\right). \tag{1.48}$$

This condition is not satisfied in the range of temperatures above T_c; for this reason the whole formalism we are using is valid only in the broken (ordered) phase.

With the linearized mean field bath hamiltonian it is possible to evaluate the coherence of the

system (see Appendix B):

$$\begin{aligned}\hat{S}_0^-(t) &= tr_B\left[e^{-i\mathcal{H}^{mf}t}\left(\hat{S}_0^-(0)\otimes\rho_B\right)e^{i\mathcal{H}^{mf}t}\right] \\ &= \frac{1}{Z}tr_B\left[e^{-i\mathcal{H}^{mf}t}\left(|0\rangle\langle 1|\otimes e^{-\mathcal{H}_B^{mf}/T}\right)e^{i\mathcal{H}^{mf}t}\right] \\ &= \hat{S}_0^-(0)r_{TIM}(t) \end{aligned} \tag{1.49}$$

where $\mathcal{H}^{mf}=\mathcal{H}_s+\mathcal{H}_{sB}+\mathcal{H}_B^{mf}$, and

$$r_{TIM}(t)=\left[\cos\left(\frac{tmJJ_0}{\Theta\sqrt{N}}\right)+i\frac{\Theta}{J}\sin\left(\frac{tmJJ_0}{\Theta\sqrt{N}}\right)\right]. \tag{1.50}$$

Also in this case we obtain that time evolution of the off-diagonal terms of the system density matrix, responsible for the coherence of the system, is enclosed in the time behaviour of the complex valued decoherence factor $r_{TIM}(t)$. In analogy with Eq.(1.27) we analyze decoherence factor's absolute value. In the limit of large N we can approximate it as:

$$|r_{TIM}(t)|\approx\exp\left[-\frac{J_0^2m^2t^2}{2}\left(\frac{J^2}{\Theta^2}-1\right)\right]. \tag{1.51}$$

We can see from (1.51) that the system coherence decays exponentially with time. The coherence time is:

$$\tau_{TIM}=\frac{|\Theta|}{J_0m}\sqrt{\frac{2}{J^2-\Theta^2}}, \tag{1.52}$$

and increases as temperature decreases; for $T=0$ it is $\tau=\infty$, and the system remains coherent. Considerations analogous to those pertaining Eq.(1.42) can be made. The periodicity of $r_{TIM}(t)$ in Eq.(1.50) leads to the *recoherences* on a Poincaré time scale.

1.4.1 Limit of no transverse field

In the limit of $w\to 0$ we obtain the same result seen in Eq.(1.42), but we gain some new insight into the mechanism at issue. In this limit decoherence factor's absolute value reads:

$$|r_{IM}(t)|\approx\exp\left[-\frac{J_0^2t^2}{2}\left(\frac{1}{4}-m^2\right)\right]. \tag{1.53}$$

We can notice the same behaviour as for TIM-bath, but slightly more transparent: the coherence time is $\tau_{IM}=\frac{2}{J_0}\sqrt{\frac{2}{1-4m^2}}$ and its limits are $\tau_{IM}^{(T=T_c)}=\frac{2\sqrt{2}}{J_0}$ and $\tau_{IM}^{(T=0)}=\infty$. We note that coherence explicit dependence on bath coupling constant J has disappeared in this case; only interaction coupling constant J_0 enters coherence expression when the bath is an IM-one. Otherwise the J coupling is indirectly present in (1.53) because it has a role in determining the order parameter m by means of Eq.(1.47).

Chapter 2

Two-qubits entanglement dynamics

So far we have been describing decoherence of a single system plunged in a fermionic environment. Now we are going to study what happens to a couple of two-level systems (qubits) when posed in the same environment. In particular attention will be paid to the feature of *entanglement*. Entanglement is definitely one of the most intriguing features of quantum mechanics. It is a widespread resource in many field of quantum optics and condensed matter systems. For these reasons it deserves to be analyzed in all respects.

Recently, attention has been devoted to the problem of *thermal entanglement* [39] i.e. quantifying entanglement arising in spin chains at thermal equilibrium with a bath. In this approach environment determines the temperature T to allow for a thermal distribution of system energy levels, while the detailed interaction between system and environment is not an essential part of the matter. The same is true also for those works that focus on entanglement decoherence [40] (also known as *disentanglement* [41, 42]). In this context the study of entanglement time behaviour is carried on with a master equation formalism and markovian approximation or, more generally, with arguments provided by spin-boson models.

Here we are going to apply the approach we described for coherence to entanglement (a similar outline but supported by numerical means is also present in [43]). We then consider a couple of qubits interacting with a fermionic environment endowed with a structure capable of symmetry-breaking. We expect that along to coherence behaviour also entanglement coherence increases as magnetic order enlarges or, in other terms, as temperature decreases. Here, along to previous sections, we consider *Transverse Ising model* (TIM) and *Ising model* (IM). We shall examine the time evolution of concurrence of the bipartite system [44], and find environment-limited concurrences as well as unlimited ones according to environment ordering level.

Let us take a system composed by two qubits, labeled by 01 and 02, interacting between them and with environment, that is symmetry-breakable and modeled by TIM hamiltonians generalizing those of Eqs.(1.43-1.45):

$$\mathcal{H}_s = -\xi_0 \hat{S}^z_{01} \hat{S}^z_{02}, \tag{2.1}$$

$$\mathcal{H}_{sB} = -\frac{J_0}{\sqrt{N}} \left(\hat{S}^z_{01} + \hat{S}^z_{02} \right) \sum_k \hat{S}^z_k \,, \tag{2.2}$$

$$\mathcal{H}_B = -w \sum_k \hat{S}^x_k - \frac{J}{N} \sum_{i,k} \hat{S}^z_i \hat{S}^z_k \,, \tag{2.3}$$

In above equations ξ_0 represents the coupling constant between the qubits. We have discarded both local interactions, like that between qubits and an external magnetic field, and local couplings with environment degrees of freedom, a situation resembling a "collective" system-environment pairing [20].

As a measure of entanglement between two qubits we adopt the so called "concurrence" [44], which ranges from 0 for separable states to 1 for maximally entangled states. The concurrence is given by:

$$C = \max\left\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\right\}, \tag{2.4}$$

where λ_1, λ_2, λ_3 and λ_4 are the square roots of the eigenvalues, in decreasing order, of the matrix $R = \rho_s\widetilde{\rho}_s$. Here ρ_s is the density matrix of the 2 system qubits, and $\widetilde{\rho}_s$ is the "time reversed" matrix given by

$$\widetilde{\rho_s} = \left(\hat{\sigma}_{01}^y \otimes \hat{\sigma}_{02}^y\right)\rho_s^*\left(\hat{\sigma}_{01}^y \otimes \hat{\sigma}_{02}^y\right), \tag{2.5}$$

where $\hat{\sigma}$'s are the usual Pauli matrices. The symbol ρ_s^* means complex conjugation of the matrix ρ_s in the standard basis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

We assume that the qubits are initially decoupled from the environment, and the bath having a thermal density matrix $\rho_B = (e^{-\mathcal{H}_B/T})/Z$. Therefore, we can write the whole state as:

$$\rho = |\Psi\rangle\langle\Psi| \otimes \rho_B \tag{2.6}$$

with a generic system pure state:

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \qquad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1. \tag{2.7}$$

The steps to find time evolution of Eq.(2.6) are similar to those leading to Eq.(1.49) (see Appendix B), but now operators are represented by 4×4 matrices, being our system composed by two qubits. After mean field approximation (1.46) for the bath hamiltonian and some elementary algebra we obtain the reduced density matrix as:

$$\begin{aligned}\rho_s(t) &= tr_B\left(\rho(t)\right) \\ &= \begin{pmatrix} |\alpha|^2 & \alpha^*\beta A^* e^{-\frac{1}{2}it\xi_0} & \alpha^*\gamma A^* e^{-\frac{1}{2}it\xi_0} & \alpha^*\delta B^* \\ \alpha\beta^* A e^{\frac{1}{2}it\xi_0} & |\beta|^2 & \beta^*\gamma & \beta^*\delta A^* e^{\frac{1}{2}it\xi_0} \\ \alpha\gamma^* A e^{\frac{1}{2}it\xi_0} & \beta\gamma^* & |\gamma|^2 & \gamma^*\delta A^* e^{\frac{1}{2}it\xi_0} \\ \alpha\delta^* B & \beta\delta^* A e^{-\frac{1}{2}it\xi_0} & \gamma\delta^* A e^{-\frac{1}{2}it\xi_0} & |\delta|^2 \end{pmatrix},\end{aligned} \tag{2.8}$$

where the coefficients

$$A = \left[\cos\left(\frac{tmJJ_0}{\Theta\sqrt{N}}\right) + i\frac{\Theta}{J}\sin\left(\frac{tmJJ_0}{\Theta\sqrt{N}}\right)\right]^N, \tag{2.9}$$

$$B = \left[\cos\left(\frac{2tmJJ_0}{\Theta\sqrt{N}}\right) + i\frac{\Theta}{J}\sin\left(\frac{2tmJJ_0}{\Theta\sqrt{N}}\right)\right]^N, \tag{2.10}$$

characterize the time dependence of the concurrence. From the above expression of $\rho_s(t)$ we can find the matrix $R(t)$ and its eigenvalues, and from them, as explained, the final concurrence of the system. The complete expressions for $R(t)$ and for coefficients A and B are given in Appendix C.

In the limit $w \to 0$ we obtain the constants analogous to (2.9) and (2.10), but for IM-environment:

$$A = \left[\cos\left(\frac{J_0 t}{2\sqrt{N}}\right) + i\,2m\sin\left(\frac{J_0 t}{2\sqrt{N}}\right)\right]^N, \tag{2.11}$$

$$B = \left[\cos\left(\frac{J_0 t}{\sqrt{N}}\right) + i\,2m\sin\left(\frac{J_0 t}{\sqrt{N}}\right)\right]^N. \tag{2.12}$$

In the following we are going to consider some paradigmatic cases for the initial state (2.6).

2.1 Paradigmatic cases

In the following we provide examples of entanglement dynamics by assigning special values to the coefficients α, β, γ and δ of the state (2.7).

2.1.1 Case 1: Decoherence-free state

Let us set $\alpha = \delta = 0$ in Eq.(2.7) for the initial state of the system. We obtain:

$$|\Psi\rangle = \beta\,|01\rangle + \gamma\,|10\rangle$$

and R matrix reduces to:

$$R(t) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2\,|\beta|^2\,|\gamma|^2 & 2\beta^*\,|\beta|^2\,\gamma & 0 \\ 0 & 2\beta\gamma^*\,|\gamma|^2 & 2\,|\beta|^2\,|\gamma|^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.13}$$

whose square rooted eigenvalues are:

$$\lambda_1 = 2\,|\beta|\,|\gamma|\,, \tag{2.14}$$
$$\lambda_2 = \lambda_3 = \lambda_4 = 0\,, \tag{2.15}$$

This leads to the following concurrence:

$$C_{_{TIM}} = 2\,|\beta|\,|\gamma|\,. \tag{2.16}$$

The entanglement results time independent, so the state does not perceive the presence of the environment. The reason is that $|\Psi\rangle$ is an eigenstate of the interaction hamiltonian and so it represents a *decoherence free state* [20]. Since w is not present in the concurrence written above, we know that the expression for the concurrence would be exactly the same for an IM-environment.

2.1.2 Case 2: Entanglement decoherence

Now we set $\beta = \gamma = 0$ in Eq.(2.7) and obtain the state

$$|\Psi\rangle = \alpha\,|00\rangle + \delta\,|11\rangle\,.$$

The R matrix becomes:

$$R(t) = \begin{pmatrix} |\alpha|^2\,|\delta|^2\left(1+|B|^2\right) & 0 & 0 & 2\alpha^*\,|\alpha|^2\,\delta B^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2\alpha\delta^*\,|\delta|^2\,B & 0 & 0 & |\alpha|^2\,|\delta|^2\left(1+|B|^2\right) \end{pmatrix}, \tag{2.17}$$

with square rooted eigenvalues in decreasing order:

$$\lambda_1 = |\alpha|\,|\delta|\,(|B|+1)\,, \tag{2.18}$$
$$\lambda_2 = |\alpha|\,|\delta|\,(||B|-1|)\,, \tag{2.19}$$
$$\lambda_3 = \lambda_4 = 0\,. \tag{2.20}$$

From Eqs. (2.9) and (2.10), for large N, we get:

$$|B| \approx \exp\left[-2J_0^2 m^2 t^2 \left(\frac{J^2}{\Theta^2}-1\right)\right]. \tag{2.21}$$

Then, by using concurrence definition we arrive at:

$$C_{_{TIM}} = 2\,|\alpha|\,|\delta|\,|B| = 2\,|\alpha|\,|\delta| \exp\left[-2J_0^2 m^2 t^2 \left(\frac{J^2}{\Theta^2}-1\right)\right]. \tag{2.22}$$

The time behaviour of the concurrence just obtained is shown in Fig.2.1 for different values of the ratio $\frac{T}{T_c}$. We notice that in this case the qubits perceive the presence of the thermal bath, which spoils entanglement between them; in fact the initial state is no longer an eigenstate of the interaction hamiltonian. Only for zero temperature the order parameter reaches its saturation value and the concurrence remains constant. The behaviour is very similar to that of one qubit system coherence described by Eq.(1.49), but entanglement decoherence is exactly twice faster than one qubit decoherence. This result agrees with what found in [40]. Furthermore, together with the previous case, it falls within the general limitations represented by the *Universal Disentangling Machine* [41].

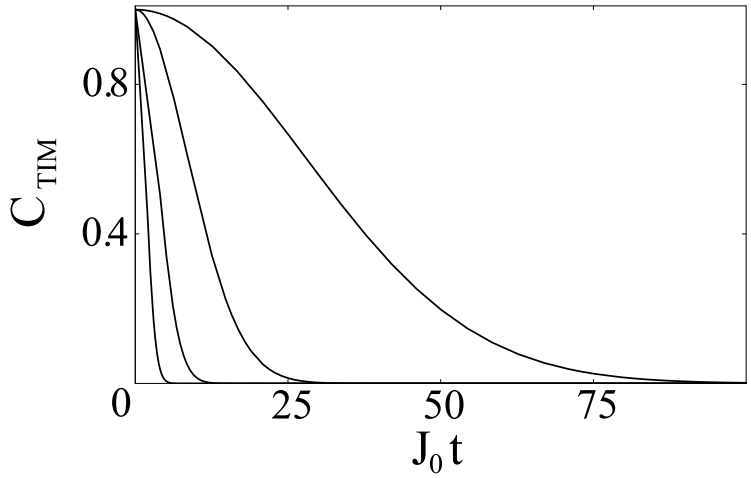

Figure 2.1: Concurrence versus scaled time $J_0 t$. The plot shows how interaction with the environment spoils entanglement between the qubits. Curves from the left to the right are for $\frac{T}{T_c} = \{.75, .50, .35, .25\}$. Values of the other parameters are $w = 0.1$, $J = 2$.

In the limit $w \to 0$ we obtain the concurrence for an IM-bath:

$$C_{_{IM}} = 2\,|\alpha|\,|\delta| \exp\left[-2J_0^2 t^2 \left(\frac{1}{4}-m^2\right)\right]. \tag{2.23}$$

Analogously to what already noticed for the single qubit coherence, in this limit the factor J disappears from the explicit concurrence expression. The only exchange coupling constant that enters in the decoherence time for the concurrence is J_0.

2.1.3 Case 3: No entanglement

If we set $\alpha = \beta = 0$ we obtain a product state

$$|\Psi\rangle = \gamma\,|10\rangle + \delta\,|11\rangle = (\gamma\,|0\rangle + \delta\,|1\rangle)\,|1\rangle\,,$$

which trivially gives:

$$R(t) = (\mathbf{0}) \Longrightarrow C = 0\,. \tag{2.24}$$

In this case TIM hamiltonians are not able to induce entanglement between system qubits.

2.1.4 Case 4: Concurrence oscillations

If we set $\alpha = \beta = \gamma = \delta = \frac{1}{2}$ we obtain again a separable initial state, but different from the previous one:

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \end{aligned}$$

In this case the R matrix is not trivial:

$$R(t) = \frac{1}{16}\begin{pmatrix} 1+|B|^2-2\,|A|^2\,\varsigma^* & U_{\xi_0} & U_{\xi_0} & 2B^*-2\,(A^*)^2\,\varsigma^* \\ -V_{\xi_0} & 2-2\,|A|^2\,\varsigma & 2-2\,|A|^2\,\varsigma & -U_{\xi_0} \\ -V_{\xi_0} & 2-2\,|A|^2\,\varsigma & 2-2\,|A|^2\,\varsigma & -U_{\xi_0} \\ 2B-2A^2\varsigma^* & V_{\xi_0} & V_{\xi_0} & 1+|B|^2-2\,|A|^2\,\varsigma^* \end{pmatrix}, \tag{2.25}$$

where:

$$U_{\xi_0} = \left(2A^* e^{-\frac{1}{2}it\xi_0} - (A^* + AB^*)\,e^{\frac{1}{2}it\xi_0}\right) \tag{2.26}$$

$$V_{\xi_0} = \left(2Ae^{-\frac{1}{2}it\xi_0} - (A + A^*B)\,e^{\frac{1}{2}it\xi_0}\right) \tag{2.27}$$

$$\varsigma = e^{it\xi_0} \tag{2.28}$$

Concurrence is valuable explicitly, but the expression is too much cumbersome and therefore it is not reported here. We only show in Fig.2.2 its behaviour. Concurrence starts from its null value and increases because of the interaction between system qubits. If there was not disentanglement it would reach its maximum and decrease again giving rise to oscillations of equal amplitude. Nevertheless, the presence of environment alters this temporal behaviour damping the oscillations. For suitable values of coupling constants it can even prevent qubits from entangling at all. The interesting question of the maximal entanglement generation under dephasing processes arises naturally in this case [40].

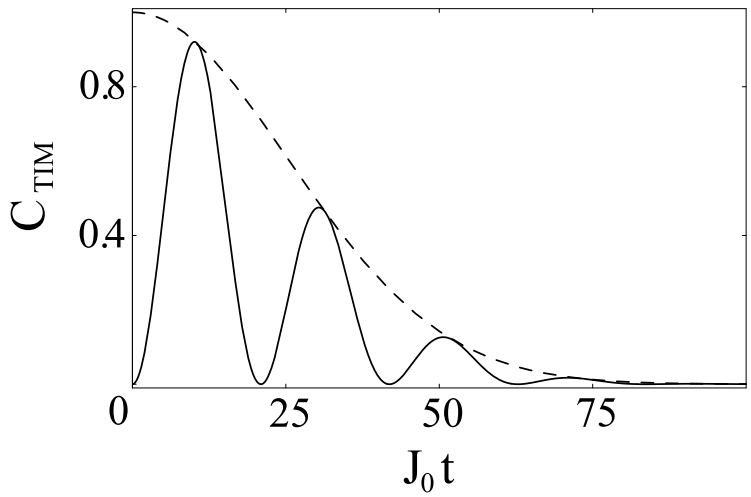

Figure 2.2: Concurrence versus the scaled time $J_0 t$. The plot shows entanglement oscillations (continuous line) between the two system qubits, created by the hamiltonian (2.1). Concurrence is limited by decoherence (dotted line), that falls down exponentially. The value of parameters are $w = 0.1$, $\xi_0 = 0.3$, $J = 2$, $\frac{T}{T_c} = .25$.

2.2 High Temperature Limit

It could be interesting to compare entanglement coherence below T_c with that above it. Nevertheless nonlinearity of TIM and IM-bath hamiltonians represents a serious obstacle to this end, and it can be only partially accomplished in the limit of infinite temperature. For high temperatures bath density matrix becomes identity, since each energy level has the same weight:

$$\lim_{T\to\infty} \rho_B = \lim_{T\to\infty} \frac{e^{-\mathcal{H}_B/T}}{Z} = I \tag{2.29}$$

In this way temporal evolution of the total density matrix becomes:

$$\rho(t) = e^{-i\mathcal{H}t}(\rho_S \otimes \rho_B)e^{i\mathcal{H}t} = e^{-i(\mathcal{H}_B+\mathcal{H}_{sB}+\mathcal{H}_s)t}\rho_S e^{i(\mathcal{H}_s+\mathcal{H}_{sB}+\mathcal{H}_B)t} \tag{2.30}$$

We take hamiltonians in the exponent to be IM-like, i.e. like (2.1) but with $w = 0$. As they commutes among them partial trace performed on bath degrees of freedom simplifies, and explicit dependence on bath properties disappears:

$$\rho_S = Tr_B\{\rho(t)\} = Tr_B\left[e^{-i\mathcal{H}_B t}e^{-i\mathcal{H}_{SB}t}\left(e^{-i\mathcal{H}_S t}\rho_S e^{i\mathcal{H}_S t}\right)e^{i\mathcal{H}_{SB}t}e^{i\mathcal{H}_B t}\right] \tag{2.31}$$

$$= Tr_B\left[\prod_k e^{it\frac{J_0}{\sqrt{N}}(\hat{S}^z_{01}+\hat{S}^z_{02})\hat{S}^z_k}\rho'_S e^{it\frac{J_0}{\sqrt{N}}(\hat{S}^z_{01}+\hat{S}^z_{02})\hat{S}^z_k}\right], \tag{2.32}$$

In above equations we have set $\rho'_S = e^{-i\mathcal{H}_S t}\rho_S e^{i\mathcal{H}_S t}$. Then reduced density matrix is:

$$\rho_s(t) = \begin{pmatrix} |\alpha|^2 & \alpha^*\beta A^* e^{-\frac{1}{2}it\xi_0} & \alpha^*\gamma A^* e^{-\frac{1}{2}it\xi_0} & \alpha^*\delta B^* \\ \alpha\beta^* A e^{\frac{1}{2}it\xi_0} & |\beta|^2 & \beta^*\gamma & \beta^*\delta A^* e^{\frac{1}{2}it\xi_0} \\ \alpha\gamma^* A e^{\frac{1}{2}it\xi_0} & \beta\gamma^* & |\gamma|^2 & \gamma^*\delta A^* e^{\frac{1}{2}it\xi_0} \\ \alpha\delta^* B & \beta\delta^* A e^{-\frac{1}{2}it\xi_0} & \gamma\delta^* A e^{-\frac{1}{2}it\xi_0} & |\delta|^2 \end{pmatrix} \tag{2.33}$$

with $A = A^* = e^{-\frac{J_0^2 t^2}{8}}$ and $B = B^* = e^{-\frac{J_0^2 t^2}{2}}$. It is evident that the form obtained for ρ_s is equal to Eq.(2.8). Hence concurrence between qubits will be equal to those found below the critical temperature, but with different A and B coefficients. In particular from (2.22) we have:

$$C_{_{HighT}} = 2\,|\alpha|\,|\delta|\,|B| = 2\,|\alpha|\,|\delta|\,e^{-\frac{J_0^2 t^2}{2}} \tag{2.34}$$

A straightforward comparison can be settled with concurrence expressed by Eq.(2.23), deduced within the Ising model. Actually concurrence found here is nothing but high temperature limit of that equation, obtained by putting $m = 0$ in it. In this limit entanglement dynamics becomes independent of temperature.

Part II

Deterministic quantum cryptography

Quantum information theory investigates the information content of quantum systems, hence it generalizes classical information theory [45]: instead of bits we have *quantum bits*, or *qubits*, i.e. two-level quantum systems capable, unlike classical bits, of being in a superposition of their basis states. Moreover, several qubits can be entangled to each other, and entanglement is acknowledged to be an important resource in many quantum protocols.

Besides the differences between the basic logic units of classical and quantum computation, we must consider also the deep unsimilarity of the *operations executable on* the logic units. Laws from quantum mechanics pose two main limitations in this sense, indirectly but not exactly related to Heisenberg's uncertainty principle [46]:

1. A qubit can not, in general, be duplicated (*"No-Cloning" Theorem*)

2. A qubit can not, in general, be measured without altering its state (*Lo-Chau Lemma*)

These properties were used to suggest a new type of cryptography, *Quantum Cryptography* (QC), which exploits quantum bits to encode classical bits, before providing them to legitimate users. The main advantage of quantum schemes over any classical scheme is the fact that quantum information can not be passively intercepted; hence any eavesdropping attempt causes disturbance and can be revealed.

Within QC we can roughly recognize two principal classes: *Non-Deterministic* QC (NDQC) and *Deterministic* QC (DQC). The former is the older too, and the more widespread; for "non-deterministic" we mean that the sequence of symbols circulating between the users is not determined by any of them. Examples of NDQC protocols are BB84, B92 and BBM92. On the opposite, DQC, invented in 2002, is "deterministic" because one of the users can decide a sequence of symbols and deterministically transmit it to another user. Examples of DQC protocols are Ping-Pong and PP84.

In chapter 3, after giving a brief review of some useful tools widely used in Information Theory, we illustrate the essential features of Classical Cryptography and NDQC. The intent is that of leading the reader to learn about DQC, that represents the central theme of the dissertation, through a gradual path.

In chapter 4 we describe an example of DQC that makes use of entanglement: Ping-Pong protocol (PP). From this first scheme DQC widespread over a considerable extent. For this reason PP has been studied in every respect, and it represents the best way to get acquainted with DQC.

In chapter 5 we deal with DQC without entanglement by using two specific examples: the protocol by Cai and Li (CL) and that by Lucamarini and Mancini (PP84). It is important to remark that these two protocols have been developed independently from each other. The study I did about CL, reported in chapter 5, is subsequent to the submission of PP84 for publication, and I wrote it here only for explicative purposes; in fact CL results to be not secure against a particular kind of eavesdropping called *opaque attack*. Section 5.2 is a very wide one: it contains description of the quantum cryptosystem PP84 and the related analysis of security against eavesdropping, with particular emphasis to the so called *individual attacks*.

In chapter 6 we extend the analysis to other features of PP84 and DQC in general. We study theoretical and practical efficiency: the former attests that DQC is preferable to NDQC, the latter that PP84 is preferable to all deterministic protocols using entanglement. We study also unconditional security and the possibility of performing Direct Communication (DC) and Quantum Dialogue (QD).

Chapter 3

Introduction

The art of cryptography has a long history. It begins with Julius Caesar, who sent encrypted messages to his trusted acquaintances. Since he did not trust the messengers he replaced every A by a D, every B by a E, and so on through the alphabet. In this way only the receivers, who knew the "shift by 3" rule, could decipher his messages.

We begin the discussion by providing a short "dictionary of cryptography" :

a *cryptosystem* or *cipher* is a method of disguising messages so that only certain people can see through the disguise. *Cryptography* is the prowess of creating and using cryptosystems. It is part of the broader field of *cryptology*, which is the study of both cryptography and *cryptanalysis*, the art of code breaking. The original message is called a *plain-text* or simply *message*. The disguised message is called *cipher-text* or *cryptogram* or *scrambled-text*. *Encryption* means any procedure to convert plain-text into cipher-text. *Decryption* means any procedure to reverse encryption. The people who are supposed to be able to see through the disguise are called *legitimate users* or *recipients*, and are traditionally indicated as *Alice* (user 'A') and *Bob* (user 'B'). Unauthorized people are called *eavesdroppers*, *enemies*, *opponents*, *interlopers* or simply *third parties*; all of them are included in the name *Eve*.

In this chapter we give a brief description of classical cryptography, and introduce its quantum counterpart, which will be given the appellative of "Non-Deterministic Quantum Cryptography" (NDQC). The main role of NDQC is that of distributing a random key between two recipients in a completely secure way. This key is then used in classical cryptosystems for a secure communication. In this sense NDQC does not substitute classical cryptography but rather integrates it, because the task of a safe distribution of a random key is impossible to achieve by only classical means. NDQC is non-deterministic because the random key distributed to legitimate users is not established beforehand. The random key can also be deterministically distributed, but this is the matter of chapters 4 and 5.

We point out that despite quantum cryptography's protocols only aim at distributing a random key to be used in classical ciphers, nothing forbids to envisage a scheme for cryptography entirely quantum, with quantum channels making the work of classical ones, and quantum algorithms substituting the classical. This is possible because classical realm lies in a quantum description of nature. The opposite is not true of course. For this reason we often use here and hereafter the terms "quantum ciphers" or "quantum cryptosystems" to generally indicate any protocol exploiting quantum mechanics for cryptographic purposes.

We begin by reviewing some Information Theory-related mathematical tools, frequently used in the sequel of the work.

3.1 Useful tools

3.1.1 Measurements

Given a set of operators $\left\{\hat{E}_a\right\}$ such that

$$\hat{E}_a = \hat{E}_a^\dagger,\ \hat{E}_a\hat{E}_b = \delta_{ab}\hat{E}_a,\ \sum_a \hat{E}_a = 1,$$

we can carry out a measurement procedure that will take a pure state $|\Psi\rangle\langle\Psi|$ to

$$\frac{\hat{E}_a|\Psi\rangle\langle\Psi|\hat{E}_a}{\langle\Psi|\hat{E}_a|\Psi\rangle}$$

with probability

$$\text{Prob}(a) = \langle\Psi|\hat{E}_a|\Psi\rangle.$$

The measurement outcomes can be described by a density matrix obtained by summing over all possible outcomes weighted by the probability of that outcome (rather than by choosing one particular outcome) in which case the measurement modifies the initial pure state according to

$$|\Psi\rangle\langle\Psi| \longrightarrow \sum_a \langle\Psi|\hat{E}_a|\Psi\rangle\left[\frac{\hat{E}_a|\Psi\rangle\langle\Psi|\hat{E}_a}{\langle\Psi|\hat{E}_a|\Psi\rangle}\right] = \sum_a\left(\hat{E}_a|\Psi\rangle\langle\Psi|\hat{E}_a\right).$$

This is the ensemble of pure states describing the measurement outcomes, i.e. it is the description we would adopt if we knew a measurement had been performed, but we did not know the result. Hence, the initial pure state has become a mixed state unless the initial state happened to be an eigenstate of the observable being measured. If the initial state were a mixed state with density matrix ρ, then by expressing ρ as an ensemble of pure states we find that the effect of the measurement is

$$\rho \longrightarrow \sum_a\left(\hat{E}_a\rho\hat{E}_a\right).$$

3.1.2 Classical Information

Classical information theory quantifies the idea of information.

The self information of an event u is defined to be

$$I(u) = \log(1/P(u)), \tag{3.1}$$

where $P(u)$ is the probability of the event, and where we used log to indicate $\log_2$ (so the basic unit is a bit). A multiplication of probabilities yields summation of information. The entropy of an ensemble A of events (letters) $a_1, ..., a_n$ where each letter a_i appears with probability $P(a_i)$ is the expected value of the self information

$$H(A) = E[\log(1/P(A))] = -\sum_{i=1}^{n} P(a_i)\log(P(a_i)) \tag{3.2}$$

and can be thought of as a measure of our lack of information on the unknown event in A. For instance, for a binary alphabet, $H = -\sum_{i=1}^{2}\frac{1}{2}\log\frac{1}{2} = 1$ if the letters appear with equal probability,

and $H = 0$ if one letter appears with certainty. The entropy of a binary alphabet with probabilities p and $(1-p)$ is denoted by $H(p)$

$$H(p) = -p\log p - (1-p)\log(1-p) \tag{3.3}$$

Two ensembles of letters A and B might have dependent probability distributions. The trivial example is when A is the input alphabet for some information channel and B is the output. The source is assumed to be memoryless and stationary. An average distortion between input vector and output vector is a measure for the channel quality. Usually an additive distortion measure is used

$$d(\mathsf{u},\mathsf{v}) = \sum_{i=1}^{m} d(u_i, v_i)$$

where $d(u_i, v_i)$ is a one letter distance. It is called the Hamming distance if $d(u_i, v_i) = 0$ for $u_i = v_i$ and $d(u_i, v_i) = 1$ for $u_i \neq v_i$. For instance, the Hamming distance between the strings 000 and 111 is three. This measure can also be used as a measure of distinguishability of two input vectors (code words). In channel coding we increase the number of bits which encode each code word so that the additive Hamming distance between any two legitimate code words is increased. Hence, they can be distinguished even when the channel is noisy. Such techniques (known as error-correction techniques) enable receiving a reliable output when the channel is noisy.

The relation between input and output of a transmission channel is described in terms of information, and the Hamming distance can be a measure for the distortion of a string transmitted through the channel. The conditional probability of $B = b_i$ given that $A = a_j$ is $P(B = b_i|A = a_j)$ (we write $P(b_i|a_j)$ for convenience.) The joint probability for both a_j and b_i is $P(b_i, a_j)$. In case of independent probability distributions it is equal to $P(b_i)P(a_j)$, and in general it is given by the Bayes probability law

$$P(b_i|a_j)P(a_j) = P(b_i, a_j) = P(a_j|b_i)P(b_i) \tag{3.4}$$

The Bayes probability law presents the symmetry of input and output. The conditional entropy is defined by

$$H\left(B|A\right) = -\sum_i \sum_j P(a_j, b_i)\log P(b_i|a_j)$$

where the sum is over the size of the input and the output alphabets. When A and B are independent, $H(B|A) = H(B)$, meaning that we gain no information on B by being told what A is. Otherwise $H(B|A) < H(B)$, meaning that our lack of knowledge about B is decreased when A is given. The gain in information when A is given is called the *mutual information* and is a very important notion in information theory. The mutual information $I(A:B) = I_{AB}$ is defined as:

$$\begin{aligned} I(A:B) = I_{AB} &= H(B) - H(B|A) = H(A) - H(A|B) \\ &= \sum_i \sum_j P(a_j, b_i)\log\frac{P(a_j, b_i)}{P(a_j)P(b_i)} \end{aligned} \tag{3.5}$$

and is symmetric in A and B.

In a perfect channel the output signals are completely determined by the input signals. The channel introduces no errors. A *Binary Symmetric Channel* (BSC) with input A and output B is a channel with binary alphabet where the signals are transported with symmetric distortion (i.e., equal error probabilities P_e). The optimal mutual information in this case is achieved when the input probabilities are also equal (hence also the output probabilities). It is

$$\begin{aligned} I_{BSC}(A:B) &= H(B) - H(B|A) = 1 - H(P_e) \\ &= 1 + P_e\log P_e + (1-P_e)\log(1-P_e) \\ &= P_e\log 2P_e + (1-P_e)\log 2(1-P_e) \end{aligned}$$

For a given channel, the optimal mutual information (over all possible input probabilities) is called the channel capacity. The channel capacity $\mathcal{C}$ is a measure of the minimal distortion caused by the channel. For a binary channel $\mathcal{C} \leq 1$. The 'Channel Coding Theorem' states that it is possible to derive an error-free code using a non-perfect channel: for any positive ϵ, we can choose an integer m and N vectors, $N < 2^{m\mathcal{C}}$, of length m (to be used as code words), such that all code words can be distinguished with error probability smaller than ϵ.

Another important channel is the *Binary Erasure Channel* (BEC) which is actually not a binary channel since its output contains, in addition to noughts and ones also the letter "?" which stands for an inconclusive result. This channel introduces no error but the output of either inputs is inconclusive with probability $P_?$. Channel capacity is derived with equal input probabilities and is calculated using eq.(1.3), (1.4) and (1.5) to be

$$I_{BEC}(A:B) = H(A) - H(A|B) = 1 + \sum_j P(b_j) \sum_i P(a_i|b_j) \log P(a_i|b_j) = 1 - P_?.$$

Note that the error probability P_e and the probability $P_?$ (of an inconclusive result) have a different weight in their contribution to the mutual information.

3.1.3 Quantum Information

Contrary to a classical state, a quantum state cannot be identified unless additional information is provided. Suppose that a spin measuring device is aligned in the z direction, so that it can identify the spin of an electron unambiguously if it is prepared along the z direction. An electron with some arbitrary (pure) spin state, say

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

(with $|\alpha|^2 + |\beta|^2 = 1$), will yield a result '0' (electron went *up* in a measuring device) or '1' (electron went *down* in that measuring device), unpredictably. The only clue that the state was as stated is that the probability for each result can be calculated. These probabilities are $|\alpha|^2$ for the result '0' and $|\beta|^2$ for the result '1'. Only if the physical state is taken from a set of orthogonal states in a known basis can it be identified in one measurement as in the classical case.

The n letters of a quantum communication channel can be any different (not necessarily orthogonal nor pure) quantum states $\rho_1 ... \rho_n$ on an N-dimensional Hilbert space $\mathcal{K}_N$. The mutual information of such a channel is a function not only of the input probabilities, but also of the choice of measurement performed by the receiver. Even in case of two orthogonal states, the receiver may select a bad choice of measurement direction which will tell him nothing. Therefore, one of the main questions is how to maximize the mutual information. For given signals and given input probabilities of the source, that is, for a given density matrix

$$\rho = \sum_{i=1}^{n} p_i \rho_i,$$

what is the optimal measurement, and what is the mutual information in this case?

In classical information theory, the only parameter controlled by the legitimate users is the input probabilities: optimizing the mutual information over all possible input probabilities yield the "channel capacity" . In quantum information theory, the users control both the input probabilities and the measurement, and optimizing both to maximize the mutual information yields the channel capacity. We usually deal with given (and equal) input probabilities, and care only about the accessible mutual information and not about the channel capacity.

Let us consider the simple case of two non-orthogonal pure states in $\mathcal{H}_2$. A generalization of this to $\mathcal{H}_N$ is trivial since two pure states always span some 2-dimensional subspace of $\mathcal{H}_N$. Suppose that the sender of the information, Alice, emits particles in one of the two non-orthogonal states $|\mathtt{u}\rangle$ and $|\mathtt{v}\rangle$, which represent bits 0 and 1, respectively (the state of each particle is known to Alice). The states are sent with equal probabilities. Since these two states are not orthogonal, the receiver, Bob, cannot identify with certainty the state of a given photon. By a suitable choice of basis, the two non-orthogonal states $|\mathtt{u}\rangle$ and $|\mathtt{v}\rangle$ can be written as

$$|\mathtt{u}\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \ , \ |\mathtt{v}\rangle = \begin{pmatrix} \cos\alpha \\ -\sin\alpha \end{pmatrix}$$

where $0 < \alpha < 45^\circ$. The angle between the two states is 2α. Note that the overlap between the two states is

$$\langle \mathtt{u}|\mathtt{v}\rangle = \cos^2\alpha - \sin^2\alpha = \cos 2\alpha.$$

A *standard measurement* in an orthogonal basis symmetric to the two states optimizes the mutual information; it is analogous to a BSC. This measurement introduces an error

$$P_e = \sin^2\left(\frac{\pi}{4} - \alpha\right) = \frac{1 - \sin 2\alpha}{2},$$

hence,

$$I_{BSC} = 1 - H(P_e)$$

Although a standard measurement is optimal in this case a *non-standard measurement* may be better for certain purposes. The receiver can build a device which gives a definite answer in a fraction of the cases, and an inconclusive answer otherwise. A measurement of this type (with a perfect channel) creates an analogy to the BEC. It lets the receiver derive the optimal deterministic results. It is useful if the receiver is permitted to use a subset of selected bits and throw undesired result. In such a case, a measurement which optimizes the mutual information regarding the selected bits is preferable to the one which optimizes the average mutual information regarding all bits. A simple way to perform a deterministic measurement is to perform a standard measurement in the basis of one of the vectors. We define two vectors,

$$|\mathtt{u}'\rangle = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} \ , \ |\mathtt{v}'\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix},$$

which are orthogonal to $|\mathtt{u}\rangle$ and $|\mathtt{v}\rangle$ respectively. Suppose Bob measured in the $|\mathtt{u}\rangle$ $|\mathtt{u}'\rangle$ basis: if the result is $|\mathtt{u}'\rangle$ which is orthogonal to $|\mathtt{u}\rangle$, it must have been the other state $|\mathtt{v}\rangle$ prior to the measurement; if the result is $|\mathtt{u}\rangle$, it is inconclusive, since it could be either of the two possibilities prior to the measurement.

The above can also be described in terms of non-standard measurements, a description which is sometimes more appropriate for such analysis. The generalization of the standard projection measurement is called a *positive operator valued measure* (POVM). A POVM is a set of positive operators $A_1 ... A_k$ which sum up to the unit matrix $\mathbb{1}$. Each operator corresponds to a possible outcome of the measurement. The probability that this generalized quantum measurement yields the μ'th element of the POVM, if the system was prepared in a pure state ψ, is $\langle\psi|A_\mu|\psi\rangle$. More generally, for a preparation represented by a density matrix ρ, this probability is $tr\,(\rho A_\mu)$. Contrary to the two positive operators which define a standard (projection) measurement, the operators which build up the POVM do not have to fulfill the condition that $A_i A_j = 0$ for $i \neq j$, nor that $A_i A_i = A_i$.

To derive the optimal POVM in our case, we use the vectors $|\mathsf{u}'\rangle$, $|\mathsf{v}'\rangle$ and a third vector

$$|\mathsf{w}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{3.6}$$

equidistant from $|\mathsf{u}\rangle$ and $|\mathsf{v}\rangle$. It is easy to verify that the three positive operators

$$A_\mathsf{v} = |\mathsf{u}'\rangle\langle\mathsf{u}'|/(1+C), \qquad A_\mathsf{u} = |\mathsf{v}'\rangle\langle\mathsf{v}'|/(1+C), \qquad A_\mathsf{w} = 2C\,|\mathsf{w}\rangle\langle\mathsf{w}|/(1+C), \tag{3.7}$$

(where $C = \cos 2\alpha$) sum up to the unit matrix $\mathbb{1}$, and that A_u and A_v are maximal (increasing them further will violate the conditions for a POVM). A quantum test yielding A_v rules out the initial state u which is orthogonal to it. The same is true for A_u while A_w yields an inconclusive result. The probability of an inconclusive result is

$$\langle\mathsf{u}|A_\mathsf{w}|\mathsf{u}\rangle = \langle\mathsf{v}|A_\mathsf{w}|\mathsf{v}\rangle = C, \tag{3.8}$$

hence,

$$I_{BEC} = 1 - C\ . \tag{3.9}$$

It is always possible to extend the Hilbert space $\mathcal{K}$ of states in which this POVM is defined, in such a way that there exists in the extended space, $\mathcal{K}'$, a set of *orthogonal* projection operators, P_μ, summing up to the unit operator, and such that each one of the A_μ in Eq. (3.9) is the projection of one of these P_μ from $\mathcal{K}'$ to $\mathcal{K}$. This is Neumark's theorem. The physical interpretation of this theorem is that the extended space $\mathcal{K}'$ corresponds to a combination of the system to be measured with another system, called *ancilla*, prepared in a known state.

Another POVM, less efficient but simpler to realize than the above one, is the one we described earlier (a standard measurement in one of the basis). This POVM is made of the positive operators:

$$A_\mathsf{v} = (|\mathsf{u}'\rangle\langle\mathsf{u}'|)/2, \qquad A_\mathsf{u} = (|\mathsf{v}'\rangle\langle\mathsf{v}'|)/2, \qquad A_\mathsf{w} = (|\mathsf{u}\rangle\langle\mathsf{u}| + |\mathsf{v}\rangle\langle\mathsf{v}|)/2\ . \tag{3.10}$$

3.2 Classical cryptography

Several classical ciphers have been invented to achieve secure private communication. They can be grouped into two main categories: *public key* and *private key* cryptosystems.

The most widespread and easy-to-use cryptosystems are the *public key* ones, proposed by Diffie and Hellman in 1976 [47], and actually implemented by Rivest, Shamir and Adleman in 1978 [48]. Their protocol, the RSA cryptposystem, is the basis for the most important public key schemes used nowadays.

The idea of public key cryptography is that the receiver chooses a pair of mutually inverse transformation E_K and D_K, one used for encryption and one for decryption, such that $D_K(E_K(P)\,) = P$ for any plaintext P. The sender does not need to know the receiver's secret key. Instead, the receiver publishes the encryption method E_K so that any user can use it (by calculating $C_K = E_K(P)\,$) to send the receiver any message. The decryption algorithm D_K, also called 'trapdoor function', remains secret, so that only the receiver can compute it and read the message $P = D_K(C_K)$.

Public key cryptography is not *unconditionally secure*, but, only *computationally secure*. It is based on the presumed existence of 'one-way functions', E_K in the example above, which are easy to calculate in one direction while very difficult to calculate in the inverse direction. This would still

be fine if we could prove that a huge computing power is indeed required. Unfortunately, this is only assumed, and none of the suggested transformations is proven to yield a reasonable and useful one way function. To be useful for public key cryptography a one-way function must have a "trapdoor" which is employed by legitimate users to decode encrypted messages; unfortunately the same trapdoor can help sometimes an adversary in reversing the one-way function and eavesdropping information.

Among private key cryptography the best known cryptosystem is the *One Time Pad* (OTP), also called *Vernam cipher* from Gilbert Vernam who invented it in 1926. In OTP a random key K, long as the plain-text P, is added to the text itself to give a meaningless string S, the *scrambled-text* (also *cryptogram* or *cipher-text*). In mathematical terms addition is represented by the XOR operation (binary addition modulo 2 without carry): the i-th bit of the plain-text is XOR-ed with the i-th bit of the key to yield the i-th bit of the cryptogram, $S_i = P_i \oplus K_i$ (so that S_i is zero if $K_i = P_i$ and one otherwise). For example for two bytes we have,

$$\begin{array}{lll} P & 01000101 & 10011110 \\ K & 00010011 & 00111001 \\ S & 01010110 & 10100111 \end{array} . \tag{3.11}$$

This cipher cannot be broken at all since the key randomizes the message completely. It is easy to see that knowing the cryptogram $S = P \oplus K$ gives no information about P to an eavesdropper.

The safety of the transmission depends on the safety of the key, which has to be random, secret and shared only by the legitimate users. Moreover, safety can be guaranteed only if the key is used not more than once (hence the name of the cryptosystem). If it is used twice Eve can XOR the scrambled-texts to obtain the sum of the plain-texts: $S_1 \oplus S_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$, thus gaining some information on the private discussion.

The problem is therefore HOW TO DISTRIBUTE THE RANDOM KEY BETWEEN LEGITIMATE USERS IN A SECURE WAY. Classically, the only possibility is either through personal meetings or trusted couriers; hence one time pads are very expensive, and are impractical for many applications. On the contrary quantum mechanics provide tools to accomplish this task in a simple and completely secure way. The term "Quantum Key Distribution" (QKD) embeds all those devices that aim at distribute a random key, necessary for OTP or for other cryptosystems, by using Quantum Mechanics-related tools.

3.3 Quantum cryptography

Quantum cryptography was suggested by Wiesner [3] in 1969 and concretized by Bennett&Brassard [49] in early 80s. The basic idea behind QKD is to use quantum systems as carriers of information. For reasons related to Heisenberg's uncertainty principle we can in general assert that quantum mechanics prevents quantum systems to be copied or measured without being also perturbed. This general statement can be made more precise by a brief description of two theorems:

NO-CLONING THEOREM [50]: IT IS NOT POSSIBLE, IN GENERAL, TO MAKE A PERFECT COPY OF AN UNKNOWN QUANTUM STATE.

Let us take two non-orthogonal states $|\mathsf{u}\rangle$, $|\mathsf{v}\rangle$, $\langle \mathsf{u}|\mathsf{v}\rangle = \cos 2\alpha$. Now imagine we want to make a copy of such states. Then we prepare a new ancillary state $|0\rangle_a$ and we postulate the action of an ideal *quantum cloning machine* as the following unitary operation:

$$\begin{aligned} U_{Clon}|\mathsf{u}\rangle|0\rangle_a &= |\mathsf{u}\rangle|\mathsf{u}\rangle_a \\ U_{Clon}|\mathsf{v}\rangle|0\rangle_a &= |\mathsf{v}\rangle|\mathsf{v}\rangle_a . \end{aligned} \tag{3.12}$$

We can see that the action of the cloning machine is that of completely transferring the information contained in the original state on the ancillary state, thus creating a perfect copy of the original state. We notice that in general the ancillary state $|0\rangle_a$ is known, because we prepare it, but the state that is going to be cloned *is not known*. Now we show that linearity of quantum mechanics should be violated to allow operations described by Eqs.(3.12) to be possible. We consider a general quantum state of a two-level system $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. A perfect cloning of this state should provide:

$$U_{Clon}|\psi\rangle|0\rangle_a = |\psi\rangle|\psi\rangle_a = \alpha^2|0\rangle|0\rangle_a + \alpha\beta(|0\rangle|1\rangle_a + |1\rangle|0\rangle_a) + \beta^2|1\rangle|1\rangle_a. \tag{3.13}$$

Nonetheless linearity of quantum mechanics permits us to apply the cloning transformation to the basis kets of ψ:

$$\begin{aligned} U_{Clon}|\psi\rangle|0\rangle_a &= \alpha(U_{Clon})|0\rangle|0\rangle_a + \beta(U_{Clon})|1\rangle|0\rangle_a \\ &= \alpha|0\rangle|0\rangle_a + \beta|1\rangle|1\rangle_a. \end{aligned} \tag{3.14}$$

It is apparent from Eqs.(3.13) and (3.14) that the same cloning operation applied to the same initial state leads to different results unless $\alpha = 0$ or $\beta = 0$, i.e. we reached a contradiction. We must then conclude that *a perfect quantum cloning machine is forbidden by linearity of quantum mechanics*. It is worth remarking that this statement is true in general, for unknown non-orthogonal quantum states. In the particular case of orthogonal states (obtained when $\alpha = 0$ or $\beta = 0$) a perfect quantum cloning is still possible. By the way we mention that a perfect quantum cloning is forbidden also by reasons related to the impossibility of transmitting superluminal signals.

LO-CHAU LEMMA [51, 25]: It is not possible, in general, to measure an unknown quantum state without perturbing it.

We consider again the non-orthogonal states $|\mathsf{u}\rangle$ and $|\mathsf{v}\rangle$. What we ask now is to distinguish between these two states. It is something easier than a perfect measurement, in which one must guess one state in the infinity of Hilbert space; nevertheless we are going to show that it is impossible to perform a measurement capable of a perfect distinction between two non-orthogonal states. The argument is very similar to that used for No-Cloning theorem, because every measurement can be thought of as an unitary interaction between the measured state and an ancillary state prepared in a known state [25]:

$$\begin{aligned} |\mathsf{u}\rangle|0\rangle_a &\rightarrow |\mathsf{u}\rangle|\varphi_\mathsf{u}\rangle_a \\ |\mathsf{v}\rangle|0\rangle_a &\rightarrow |\mathsf{v}\rangle|\varphi_\mathsf{v}\rangle_a. \end{aligned} \tag{3.15}$$

In order to distinguish between $|\mathsf{u}\rangle$ and $|\mathsf{v}\rangle$ we would like $|\varphi_\mathsf{u}\rangle_a$ and $|\varphi_\mathsf{v}\rangle_a$ in Eqs.(3.15) to be different. However, since the inner products must be preserved under unitary operations, we must have (we remove the subscript of ancillary states for ease of writing):

$$\begin{aligned} \langle\mathsf{u}|\mathsf{v}\rangle\langle 0|0\rangle &= \langle\mathsf{u}|\mathsf{v}\rangle \\ \langle\mathsf{u}|\mathsf{v}\rangle\langle 0|0\rangle &= \langle\mathsf{u}|\mathsf{v}\rangle\langle\varphi_\mathsf{u}|\varphi_\mathsf{v}\rangle \end{aligned} \tag{3.16}$$

that entails $\langle\varphi_\mathsf{u}|\varphi_\mathsf{v}\rangle = 1$, i.e. $|\varphi_\mathsf{u}\rangle$ and $|\varphi_\mathsf{v}\rangle$ must be identical.

Thus it seems convenient for the legitimate users, traditionally called Alice and Bob, to exploit non-orthogonal quantum states as information carriers, since they are protected by the very laws of quantum mechanics. This protection does not consist in preventing an eavesdropper, Eve, from listening to the information exchange, but rather it makes Alice and Bob notice Eve's presence,

and in such a case they will not use the non-secret information. This kind of protection is stronger than that issued by classical public key cryptograms. In fact in this last case the safety of the communication was committed to the processing power of the computer possessed by Eve during her attempt of breaking Alice and Bob's code; hence we only gain a "computational security" . On the contrary *No-Cloning theorem* and *Lo-Chau lemma* make QKD "unconditional secure" , because no conditions on Eve's computer are posed. In particular, even if Eve had at disposal a *quantum computer*, the security of QKD would not decrease at all.

The noise caused by Eve can be detected by authorized users during a second stage of the transmission, which includes discussion over an "unjammable" or "authenticated" public classical channel to compare results of their measurements. Hence a classical channel is mandatory as well as the quantum channel for the final success of a QKD. Conditions on the classical channel are discussed further on.

In principle, this is sufficient to ensure the safety of the transmission: Alice and Bob exchange a string of bits larger than required for the final key, and use the extra part to test for eavesdropping. If they find no errors the channel is secure hence also the transmitted key. This can be verified to any degree of safety by checking a larger fraction of the bits transmitted. On the contrary if they do find errors during the control stage they know that Eve was listening to the communication and abort it. Thus, Eve can force them to abort the protocol, but she cannot cheat them into thinking she is not listening while she still gets information about their key.

However in practice to demonstrate that a certain protocol is unconditional secure is far from being an easy task. About 15 years have been spent before the first protocol for QKD, BB84 [49], was acknowledged unconditional secure [51, 52, 53], and the research in this direction continues nowadays. The main difficulties with these security proofs arise when natural noise is taken into account. Thus far we treated communication as a noiseless process, in which every error is attributed to the malicious intervention of an eavesdropper. Nevertheless in the real world transmissions are imperfect, due to losses, non-unitary efficiency of detectors, errors during the encoding phase, and so forth. In this case it becomes impossible to distinguish between noise induced by Eve and noise due to intrinsic imperfections of apparatuses used; classical algorithms like *Error Correction* (EC) and *Privacy Amplification* (PA) [54, 55] must be added to the quantum protocol, and sophisticated mathematical tools are required in order to demonstrate security of the whole scheme.

In the next sections we describe the most widespread protocols used for QKD, and gather all of them under the name of "Non-Deterministic Quantum Cryptography" (NDQC) for reasons that will become clear in the subsequence of the work. The most straightforward application of the two theorems reported above is represented by BB84, the protocol invented by Bennett and Brassard in 1984: it exploits four non-orthogonal quantum states for key distribution; as we saw they can not be cloned or perfectly measured and this guarantees the security of the communication. In 1991 Artur Ekert, while elaborating on a suggestion of David Deutsch [56], discovered independently of BB84 a scheme that exploits entanglement for cryptographic purposes [57]. The connection of this scheme to BB84 was demonstrated by Bennett, Brassard and Mermin in 1992 [58]; they also proposed a simplified version of Ekert's protocol that we call the "EPR scheme" . We notice that few years later Lo and Chau will be using EPR scheme to demonstrate the unconditional security of BB84 [51]. Another important protocol was proposed in 1992 by Bennett [59], showing that quantum key distribution can be performed even if one uses only two non-orthogonal states. We refer to this scheme as B92. Any of these protocols can be used to design an effective *non-deterministic* quantum key distribution.

3.3.1 The BB84 scheme

The first quantum key distribution scheme is the one envisaged by Bennett and Brassard in 1984, the BB84 [49]. The usual way to describe it makes use of two characters, Alice and Bob, who try to communicate in a secure way. They decide to encode their classical bits into qubits, and to use them as carriers of information. We can think these qubits to be photons' polarization states, as realistically speaking photons have already been used to realize QKD. We treat the photon as a spin 1/2 particles[1], and use operators like $\hat{S}_z$ and $\hat{S}_x$.

As a first step Alice decides a basis, say $\hat{S}_z$, and associate the classical information '0' to the quantum state $|\uparrow\rangle$, and the information '1' to the state $|\downarrow\rangle$ (Sec.). She then repeats this step for all the bits she has to send Bob. Nevertheless, if she sends Bob photons prepared in such a way, the communication would not be secure. In fact a potential eavesdropper, usually called Eve, could measure the traveling photon in the basis $\hat{S}_z$, learn the encoded information, and forward the photon to Bob without having altered it in any way.

Then Alice adds a cunning to her encoding. She associates the classical information '0' to a quantum state *randomly chosen* between $|\uparrow\rangle$, eigenstate of $\hat{S}_z$, and $|\rightarrow\rangle$, eigenstate of $\hat{S}_x$, and the information '1' to a quantum state *randomly chosen* between $|\downarrow\rangle$, eigenstate of $\hat{S}_z$, and $|\leftarrow\rangle$, eigenstate of $\hat{S}_x$ (Sec.). We notice that $\hat{S}_z$ and $\hat{S}_x$ do not commute; by consequence the states chosen by Alice this time are *non-orthogonal*, and limitative theorems like *No-Cloning* [50] become effective. This entails that if Alice sends Bob qubits prepared in non-orthogonal state Eve can not anymore copy of measure them without disturbing them some how. This is the principle Alice and Bob exploit to test the safety of the communication. Then Alice's preparation can be summarized as a random choice of one of the following states:

$$\hat{S}_z : |\uparrow\rangle, |\downarrow\rangle \quad \hat{S}_x : |\rightarrow\rangle, |\leftarrow\rangle . \tag{3.17}$$

Bob, in his turn, chooses, also at random, whether to measure $\hat{S}_z$ or $\hat{S}_x$. When his measurement is along the same axis as Alice's preparation (e.g., they both use $\hat{S}_z$), the measured value should be the same as hers (if no Eve is in the line!), whereas when they use conjugate axes, there is no correlation between his result and Alice's original choice, and in this case the run is discarded. How can the legitimate users know when preparation and measurement axes coincide? In addition to the quantum channel, Alice and Bob also use a *classical channel*. By discussing over this channel they agree to discard all the instances where they did not use the same axes. The result should be two strings of perfectly correlated bits, i.e. these two strings shall be identical in case no eavesdropper interferes.

An important assumption that is always made on the classical channel, but is often forgotten, is that:

CLASSICAL CHANNEL IS EITHER *UNJAMMABLE* OR *AUTHENTICATED*.

In the former case we assume that the classical channel is a sort of big network managed by many different parties *open to everyone but not modifiable by anyone*. Thus Eve can listen to it but she can not alter the information traveling on it. In the latter case we assume that *legitimate users share in advance a prior secret information* by means of which they can test the safety of the classical channel through an authentication procedure. In this way Eve can not make Alice believe she is Bob and viceversa with Bob.

[1] To be precise photons are spin 1 massless bosons but *behave like* spin 1/2 particles because the *little group* contracts to the rotation group in two dimensions for relativistic reasons. For a photon this corresponds to the familiar polarizations of classical light transverse to the direction of propagation [29].

Also the comparison of data possessed by Alice and Bob is performed on the classical channel: if they find out different results when using equal bases then they can be sure Eve tampered with the quantum channel, and they abort communication. Indeed this is the game: Eve tries to steal information; if Alice&Bob find her out the transmission is aborted, and a new transmission is going to be settled after the line is controlled. If Alice&Bob do not find any interference, then they consider the line safe and share a key. We remark that Bob can not know Alice's preparation basis before the public discussion, and all the same Alice can not know whether Bob guessed the preparation basis or not. Hence they can not establish in any way whether the qubit they prepared/measured will be included in the final key or not. In this sense we speak of BB84 as a "non-deterministic" protocol for QKD; in a certain sense the final key is randomly given by the protocol itself during its course. We will see that a deterministic transmission of a sequence of symbol is instead possible with DQC (chapters 4, 5 and 6).

Let us summarize the usage of the two channels present in BB84 protocol: the *classical channel* is assumed to be public but which cannot be altered or which can be authenticated by legitimate users. Its tasks are: to allow Alice and Bob to share information; to prevent some kinds of eavesdropping; to transmit the classical information required for each step of the protocol; to check for possible eavesdropping. The *quantum channel* (for photons it is an optical fiber or free space) is a transmission medium for quantum signals (usually they are the phase or the polarization of photons) very sensitive to interactions with an external (often undesirable) agent.

In the above description of BB84 we made the implicit assumption of a perfect quantum channel, completely noiseless. In practice however, the transmission will never be perfect and there will be some errors, caused by noise, even in the absence of an eavesdropper. Alice and Bob use the classical channel to compare some portion of their data and calculate the error rate in the transmitted data. The quantity resulting from this operation takes the name of QBER, Quantum Bit Error Rate, and is important to give upper bounds to the information stolen by Eve. The users decide about some *permitted* QBER, Q_e, which they can accept according to the properties of the channel and their devices. Eve could take advantage of that, and attack some of the bits to gain information, as long as the error rate she induces, q_e, plus the natural errors, do not exceed the permitted QBER. For all further discussions we assume that Eve is powerful enough to replace the channel by a perfect channel so she can induce as many errors as accepted by the legitimate users: $q_e \approx Q_e$. This can be achieved by Eve detecting the travelling qubits very close to Alice's site (where not many "natural" channel errors are yet occurred) and release them very close to Bob's site.

Let us illustrate some simple eavesdropping strategy. Assume Alice and Bob used the same basis, and that Eve decides to eavesdrop a fraction η of the qubits sent by Alice to Bob. Her strategy is to perform a standard measurement on the qubits in one of the two bases, randomly chosen (as Bob does). In this case the created QBER amounts to $q_e = \eta/4$: in fact when Eve uses the correct basis, she does not introduce any error, while she creates a 50% error rate when she uses the wrong basis. Since Eve knows the permitted QBER (agreed by the users through the classical channel), she chooses $\eta = 4Q_e$, in order to remain below the threshold for QBER tolerated by the users. The average mutual information she obtains is $\eta/2$: she has total information when she used the correct basis, and none when she used the wrong one. Note that the scheme is completely symmetric, so that Eve shares the same information with Alice and with Bob. Therefore, we can write the mutual information shared by Alice and Eve and shared by Eve and Bob as a function of the error rate: $I_{AE}(Q_e) = I_{EB}(Q_e) = 2Q_e$. More complicate attacks are possible for Eve, but even from this simple example we can learn how Alice and Bob can value the information Eve shares with them by measuring the QBER revealed on the quantum channel.

As long as Q_e is not too high, Alice and Bob might be able to use classical information processing

techniques, such as *Error Correction* (EC) and *Privacy Amplification* (PA) [54, 55], to obtain a *reliable* and *secure* final key. It is called "reliable" if they succeed to reduce the error rate to zero, and it is called "secure" if they succeed to reduce the information obtained by Eve to zero as well (by "zero" we mean close to zero as they wish). Both techniques are based on the use of parity bits of long strings where the parity of a string is zero if it contains an even number of 1's and the parity is one if the string contains an odd number of 1's. For a two-bit string, this is exactly the XOR of the two bits.

3.3.2 The EPR scheme

The second quantum key distribution scheme is based on EPR correlations. It was suggested by Deutsch [56], formalized by Ekert [57] and modified by Bennett, Brassard and Mermin [58]. We describe here the modified version which we call the EPR scheme.

In this scheme Alice creates pairs of spin 1/2 particles (for instance photons[2]) in the singlet state:

$$\begin{aligned} \Psi^{(-)} &= \sqrt{\frac{1}{2}}\left(|\uparrow_A\downarrow_B\rangle - |\downarrow_A\uparrow_B\rangle\right) \\ &= \sqrt{\frac{1}{2}}\left(|\leftarrow_A\rightarrow_B\rangle - |\rightarrow_A\leftarrow_B\rangle\right) \ , \end{aligned} \tag{3.18}$$

where as before $|\uparrow\rangle$ and $|\downarrow\rangle$ are eigenstates of $\hat{S}_z$, $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$ and $|\leftarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$ are eigenstates of $\hat{S}_x$. She labels the photons 'A' and 'B' for Alice and Bob. Then she sends photon B of the singlet to Bob, who will measure it as in BB84, randomly choosing between $\hat{S}_z$ and $\hat{S}_x$. Alice will do the same on photon A.

It is straightforward to realize that when the two photons are measured along the same axis the results obtained for them are necessarily anti-correlated. For example, if both Alice and Bob measure their photons along the axis $\hat{S}_z$, from the upper row of Eq.(3.18) we see that they will obtain $|\uparrow\rangle$ for the particle A and $|\downarrow\rangle$ for the particle B, or $|\downarrow\rangle$ for the particle A and $|\uparrow\rangle$ for the particle B; i.e. the measurements always yield opposite results, regardless of the axis, whenever the measuring axes are the same. On the contrary when the axes differ Alice and Bob simply discard results. The verification of the axes used is made, as in BB84, on the classical channel. It is noteworthy that, in the EPR scheme, the initial singlet pairs could be created by any other party, including Eve herself; in fact any deviation from the protocol by Eve (i.e., any attempt to create a state different from the singlet), will induce errors. This important fact was exploited by Lo and Chau to demonstrate BB84's unconditional security [51]; they used EPR scheme to prove security of BB84 after Bennett, Brassard and Mermin showed the *complete equivalence* between the two schemes [58].

The central idea of EPR-BB84 equivalence is the following. Let us imagine Alice measures her particle A *before* particle B has been sent to Bob. Then, by means of this measurement, she *prepares* one of the states of Eq.(3.17) used in BB84. In fact if she measured particle A along, say, $\hat{S}_x$ and found the state $|\rightarrow\rangle$ then she can be sure particle B is in the state $|\leftarrow\rangle$. By the way we mention that this is exactly the way used in laboratories to implement BB84 with single photons.

EPR-BB84 equivalence let us skip all further details about EPR scheme, since they are all the same as in BB84. As a concluding remark we notice that another consequence of EPR-BB84 equivalence is that also EPR, as well as BB84, turns out to be a *non-deterministic* quantum cryptosystem.

[2]See Note 1 in Sec.3.3.1.

3.3.3 The B92 scheme

The last non-deterministic protocol for QKD we discuss is the B92 [59]. This quantum cipher is interesting because it shows how only two non-orthogonal states are sufficient to achieve a secure QKD between two users. The two states of B92 are intentionally written with the same notation we used for *No-Cloning theorem* and *Lo-Chau lemma* (Sec.3.3), to establish a direct connection between them and security of B92.

In this scheme, Alice chooses randomly one of two non-orthogonal states,

$$|\mathsf{u}\rangle = |\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad \text{or} \quad |\mathsf{v}\rangle = |\rightarrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \tag{3.19}$$

the first of which (u) is eigenstate of $\hat{S}_z$ and encodes the classical information '0', while the second (v) is eigenstate of $\hat{S}_x$ and encodes '1'. She prepared a qubit in the chosen state and sends it to Bob. As these states are not orthogonal, there is no way for Bob to decode them deterministically, hence also this protocol belongs to NDQC.

Bob performs a non-standard measurement, i.e. a POVM of the kind of (3.7) or (3.10); he measures randomly one of the following (non-commuting) projection operators:

$$P_{\mathsf{u}} = \mathbb{1} - |\mathsf{u}\rangle\langle\mathsf{u}| \quad \text{or} \quad P_{\mathsf{v}} = \mathbb{1} - |\mathsf{v}\rangle\langle\mathsf{v}|. \tag{3.20}$$

We notice that P_{u} annihilates $|\mathsf{u}\rangle$, while it yields a positive result (with probability $1-|\langle\mathsf{u}|\mathsf{v}\rangle|^2$) or a negative result (with probability $|\langle\mathsf{u}|\mathsf{v}\rangle|^2$) when applied to $|\mathsf{u}\rangle$. The same argument, reversed, holds for P_{v}. This entails that if there has been no eavesdropping each time Bob obtained a positive result only two things could have happened: either Alice prepared the state v and Bob measured P_{u}, or Alice prepared the state u and Bob measured P_{v}. Then, to complete the transmission, is sufficient that Bob publicly tells Alice in which instances he found a positive result (without telling her which measurement he made!) They will discard all others runs in which useless results occurred.

If, on the contrary, Eve tapped the communication line then there will occur cases in which Bob obtains a positive result measuring P_{u} while Alice prepared the state u (or all the same with P_{v} and v). These events certify the presence of Eve, and the communication must be aborted. The safety of the protocol against eavesdropping is ensured by the fact that also Eve, like Bob, cannot always get deterministic results. Therefore, in many instances where she intercepts the transmission she can not prevent the qubit from being disturbed.

If the channel is very lossy, Eve could take advantage of it by substituting the imperfect channel with a perfect, lossless channel, and performing a POVM similar to that of Eqs.(3.7) or (3.10). In his article Bennett envisaged the possible usage of a non-informative bright pulse together with the informative dim pulse in order to defeat this kind of eavesdropping. The idea is that the bright pulse always arrives at Bob's site, so he can not find out a loss. If no Eve is in the line Bob measures qubits in the right state, otherwise he finds erroneous outcomes with high probability. In other words this technique traduces every loss in an error. This causes a strong increase of the QBER measured by the users and, by consequence, lowers the reliability and practicality of such a quantum cryptosystem.

Chapter 4

DQC using entanglement

In chapter 3 we addressed classical cryptography and non-deterministic quantum cryptography (NDQC). We saw how Alice and Bob are able to safely grow a common key by means of quantum mechanics and classical reliable communication. Nevertheless the growing process is completely random and the two users can not foresee how the final key will be. In BB84 for example the actual final string of bits depends on Alice and Bob's bases choices, and none of them can guess the other's choice until the very moment of public discussion. This is what we call a probabilistic, or better *non-deterministic*, process. In this sense, being the key undetermined until Alice and Bob perform their measurements and public discussion, quantum cryptography is often thought of as a *secret key generation* rather than as a secret key exchange or transfer, because neither Alice nor Bob can pre-determine the key they will ultimately end up with upon completion of the protocol.

On the opposite in this chapter we are going to describe a *deterministic* process to transmit information, remaining in the field of discrete variables[1]. This new scenario takes the name of "Deterministic Quantum Cryptography" (DQC). In DQC Alice and Bob can exchange a determined *sequence* of symbols established by one of them; henceforth the word "sequence" will be meaning any list of symbols conveyed during the protocol. It can assume both the role of a random key and that of a plain-text, the users decide it; in the former case the process will be a Quantum Key Distribution (QKD) while in the latter case it will be a Quantum Direct Communication (QDC). We advise the reader that in DQC the roles of Alice (the sender) and Bob (the receiver) seem to be inverted; notwithstanding, the information about the final sequence always flows from Alice to Bob. All the deterministic quantum ciphers described hereafter work with a double quantum channel: roughly speaking we can say that through the forward channel Bob gives Alice a white paper; then through the backward channel Alice sends back the paper with the sequence written on it to Bob. The information we (and a potential eavesdropper) are interested in is that *written on* the paper.

We begin the discussion with the most famous example of a deterministic quantum communication: Dense Coding protocol.

4.1 Dense coding

Quantum Dense Coding was proposed by Bennett and Wiesner in 1992 [61]. The protocol describes a way to transmit two bits of classical information through manipulation of half of an entangled

[1] Deterministic quantum cryptography with continuous variables, like *position* or *momentum*, is also possible and under examination [60].

pair of two spin-$\frac{1}{2}$ particles, while each of the particles individually could carry only one bit of classical information. The first experimental realization of dense coding was reported in [62].

The first step in the protocol is the preparation of the two-qubits maximally entangled singlet state (Eq.3.18), that we rewrite here with the notation $|0\rangle, |1\rangle$ (eigenstates of $\hat{S}_z$) and $|+\rangle, |-\rangle$ (eigenstates of $\hat{S}_x$):

$$\Psi^{(-)} = \sqrt{\frac{1}{2}}\left(|0_A 1_B\rangle - |1_A 0_B\rangle\right) = \sqrt{\frac{1}{2}}\left(|+_A -_B\rangle - |-_A +_B\rangle\right) \tag{4.1}$$

The state (4.1) is one of the well known Bell states, currently used to test the nonlocality of quantum mechanics. The others are:

$$\Psi^{(+)} = \sqrt{\frac{1}{2}}\left(|0_A 1_B\rangle + |1_A 0_B\rangle\right) = \sqrt{\frac{1}{2}}\left(|+_A +_B\rangle - |-_A -_B\rangle\right) \tag{4.2}$$

$$\Phi^{(-)} = \sqrt{\frac{1}{2}}\left(|0_A 0_B\rangle - |1_A 1_B\rangle\right) = \sqrt{\frac{1}{2}}\left(|+_A -_B\rangle + |-_A +_B\rangle\right) \tag{4.3}$$

$$\Phi^{(+)} = \sqrt{\frac{1}{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right) = \sqrt{\frac{1}{2}}\left(|+_A +_B\rangle + |-_A -_B\rangle\right) \tag{4.4}$$

It is easy to see that the four Bell states can be obtained from anyone of them, for instance $\Psi^{(-)}$, by performing a local operation on one of the two qubits by which it is composed. If for instance we execute on qubit A of $\Psi^{(-)}$ the operation X we obtain the Bell state $\Phi^{(-)}$; if we execute on A the operation Z we obtain the Bell state $\Psi^{(+)}$, and so forth. We summarize this properties as follows:

$$\Psi^{(-)} \xrightarrow{\mathbb{1}^A} \Psi^{(-)} \tag{4.5}$$

$$\Psi^{(-)} \xrightarrow{X^A} \Phi^{(-)} \tag{4.6}$$

$$\Psi^{(-)} \xrightarrow{Z^A} \Psi^{(+)} \tag{4.7}$$

$$\Psi^{(-)} \xrightarrow{iY^A} \Phi^{(+)} \tag{4.8}$$

This is the important feature Alice and Bob can exploit to exchange information. We notice that the four Bell states (4.5-4.8) are mutually orthogonal, and represent a complete basis in the 4-dimensional Hilbert space of the qubits A and B.

The two users establish a correspondence between operations and classical information, for example according to the following table:

Operation	Information
$\mathbb{1}$	00
X	01
Z	10
iY	11

Then Bob prepares the state (4.1) and sends the qubit A to Alice, keeping B with him. Alice performs one of the operations (4.5-4.8) on the qubit A, and then sends it back to Bob. After the arrival of A, Bob performs a complete Bell measurement on the joint state of A and B, aimed at discriminating which of the four Bell states he received; in this way Bob *deterministically* infers the operation executed by Alice and the associated classical information. This procedure is schematically represented in Fig.4.1.

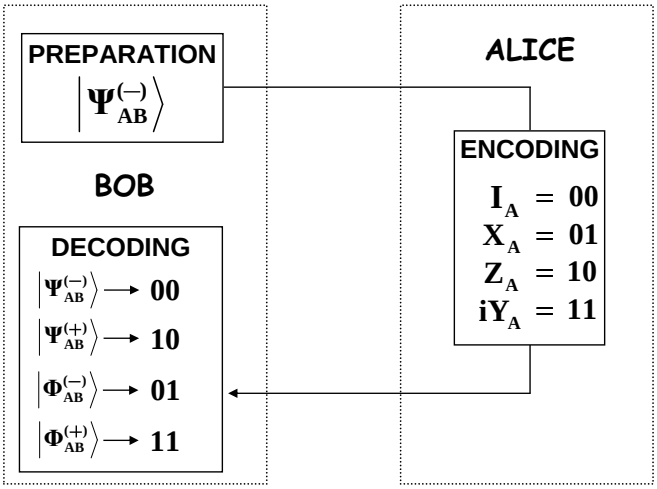

Figure 4.1: The encoding-decoding mechanism in Dense Coding protocol by which Alice can deterministically convey information to Bob.

Dealing with communication matter we can not ignore the eavesdropping problem. We must consider the possibility that an evil presence, Eve, situated between the legitimate users, taps the communication channel with the intention of stealing information. Quantum mechanics assure us that any attempt of tampering with a quantum state causes a disturbance. This feature must be used by Alice and Bob to verify the safety of their communication by introducing an adequate control procedure. A protocol merging Dense Coding's transmission modality with a control procedure was invented by Boström and Felbinger in 2002 [63], who named it "Ping-Pong" (PP) for its peculiar "forward and backward" use of the quantum channel.

4.2 Ping-Pong protocol

In Ping-Pong protocol (PP) Alice and Bob are going to exchange information in the same way used in Dense Coding, but only two Bell states instead of four are used. Moreover a control mode is provided to verify the safety of the channel. The detailed PP's list of commands is reported in Appendix D; here we will give a brief description of its main features.

To begin the transmission Bob prepares two photons in the maximally entangled state (4.1) of the polarization degree of freedom[2]:

$$\Psi^{(-)} = \sqrt{\frac{1}{2}}\left(|0_A 1_B\rangle - |1_A 0_B\rangle\right). \tag{4.9}$$

Bob stores the (*home*) photon 'B' in an ideal quantum memory, and sends the (*travel*) photon 'A' through the quantum channel to Alice. After receiving the travel photon Alice switches with probability c to "control mode" and with probability $(1-c)$ to "message mode". In control mode

[2]To be precise, the original PP makes use of the maximally entangled state $\Phi^{(+)}$, given by Eq.4.4, but we prefer to use $\Psi^{(-)}$ for explicative reasons, because it is the same state we used to describe Dense Coding; furthermore the whole argument is perfectly symmetric in the exchange of the Bell states.

Alice measures the polarization of the travel photon in the basis B_z and announces publicly the result. After receiving Alice's announcement Bob switches to control mode too, and measures the state of the home photon in the same basis B_z. He then compares his result with Alice's, and if the line is safe their results should be perfectly anticorrelated. The appearance of identical results instead is the evidence of Eve's presence and if it occurs the transmission is aborted. If no suspicious result appears the transmission continues with the next run, which will be either another control run or a message run. When the users are in message mode Alice decides which value $j \in \{0,1\}$ she will transmit to Bob. She encodes this value with the use of the unitary operations $\hat{C}_j$, where $\hat{C}_0 := \mathbb{1}$ and $\hat{C}_1 := Z$, performed on the travel photon. These operations correspond to transformations (4.5) and (4.7) of the Dense Coding. After that the travel photon is sent back to Bob, who performs an incomplete Bell measurement on the joint state of both photons. There are only two possible outcomes of this measurement namely $\Psi^{(-)}$ if Alice made $\hat{C}_0$ or $\Psi^{(+)}$ if Alice made $\hat{C}_1$. This restricted Bell measurement can be easily performed also from a practical point of view, while a complete Bell measurement poses serious problems of practicality [64]. Thus it is clear that by his result Bob will easily decode, with probability equal to 1, the information sent by Alice. This feature, as in Dense Coding, makes PP a *deterministic communication protocol*, because the final sequence Alice and Bob share is the result of one of them's choice, and not of a random process. It is straightforward to realize that the sequence transmitted by Alice with the procedure described above can equally well be a list of random symbols, as a key of a One Time Pad, or directly a meaningful message.

What about eavesdropping? Is PP secure? A complete analysis of PP shows that **it is not secure**. Nevertheless it paved the way to other improved versions of deterministic protocols and it deserves to be studied in detail.

Eve has no access to Bob's home photon B but she can manipulate the travel photon A while it goes from Bob to Alice and back from Alice to Bob. Her knowledge about the state that enters Alice's box is zero since:

$$\rho_E = tr_1\rho = tr_1\left(\left|\Psi_{12}^{(-)}\right\rangle\left\langle\Psi_{12}^{(-)}\right|\right) = \frac{1}{2}\mathbb{1} \tag{4.10}$$

Boström and Felbinger argued that the most general operation Eve can do on the forward qubit is a completely positive map $\mathcal{E} : \mathcal{S}(\mathcal{H}_q) \longrightarrow \mathcal{S}(\mathcal{H}_q)$ acting on its state space. According to Stinespring's *Dilation Theorem* [65] any completely positive map can be realized by an unitary operation on a larger Hilbert space[3]. The Hilbert space can be enlarged by using a second qubit, the *ancilla*, whose state and space are indicated respectively with $|\chi\rangle$ and $\mathcal{K}_A$. It turns out that in order to describe the most general transformation on a quantum system is enough to consider an ancilla space such that $\dim \mathcal{K}_A \leq (\dim \mathcal{K}_q)^2$. Thus, being qubit's Hilbert space bi-dimensional, it suffices to consider an ancilla space $\mathcal{K}_A$ with $\dim(\mathcal{K}_A) = 4$. Given an unitary operation $\hat{E}$ on $\mathcal{H}_q \otimes \mathcal{K}_A$, the most general transformation on the travelling qubit can then be described as:

$$\hat{E}(|0\rangle|\chi\rangle) = \alpha|0\rangle|\chi_{00}\rangle + \beta|1\rangle|\chi_{01}\rangle \tag{4.11}$$

$$\hat{E}(|1\rangle|\chi\rangle) = \gamma|0\rangle|\chi_{10}\rangle + \delta|1\rangle|\chi_{11}\rangle \tag{4.12}$$

where we can consider for simplicity ancillary states as orthogonal and normalized, and where $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$. Because of (4.10) from Eve's point of view the situation is indistinguishable from Bob preparing at random states $|0\rangle$ and $|1\rangle$ with equal probability. So let us consider the case where Bob sends $|0\rangle$. Because of (4.11) we can write the total density matrix of state and ancilla after Eve's intervention as:

$$\rho' = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}. \tag{4.13}$$

[3]This theorem represents a generalization of Neumark's theorem ([66], [67])

Now Alice encodes with equal probability 1 and iY and the matrix (4.13) becomes

$$\rho'' = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}. \tag{4.14}$$

The amount of information contained in (4.14) is given by the von Neumann entropy $I_0 = S(\rho'') = -tr\,(\rho'' \log_2 \rho'')$ and is simple to calculate because ρ'' is diagonal:

$$\begin{aligned} S(\rho'') &= -|\alpha|^2 \log_2 |\alpha|^2 - |\beta|^2 \log_2 |\beta|^2 \\ &= -\left(1-|\beta|^2\right) \log_2 \left(1-|\beta|^2\right) - |\beta|^2 \log_2 |\beta|^2 . \end{aligned} \tag{4.15}$$

We notice that the diagonal form of (4.14) made the quantum von Neumann entropy equal to the classical Shannon entropy of a binary channel of probability $|\beta|^2$. A further observation of transformation (4.11) reveals that $|\beta|^2$ is just the probability Eve is detected by Alice and Bob, because it represents the probability that the state of the qubit changes from $|0\rangle$ to $|1\rangle$, thus becoming identical to Bob's state; as we already said this is the evidence of Eve's presence, and is revealed by Alice and Bob during the control mode. Then letting d indicate the detection probability we have:

$$d = |\beta|^2 . \tag{4.16}$$

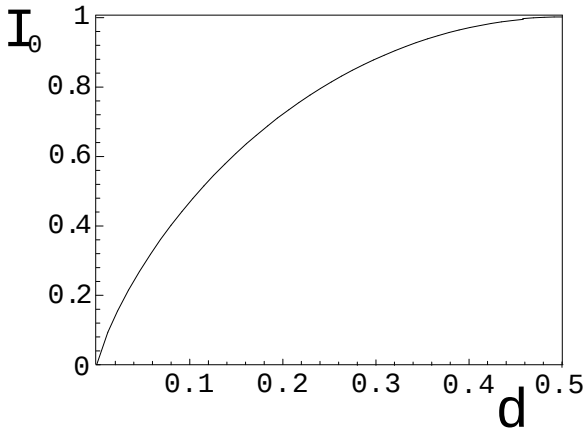

Figure 4.2: Eve's information gain I_0 vs detection probability d in Ping-Pong protocol [63].

Rewriting (4.15) as a function of d we obtain Eve's gain of information versus the probability of being detected:

$$I_0 = -d \log_2 d - (1-d) \log_2 (1-d) . \tag{4.17}$$

We plotted this quantity in Fig.4.2. The picture shows the principle of quantum cryptography: information gain implies disturbance; as soon as the gain of information is greater than zero, the disturbance introduced on the quantum channel is greater than zero too. We notice that approaching the origin the slope of the curve tends to infinite; this entails that for Eve it could be convenient to steal a very small amount of information per run, causing an even smaller amount of disturbance. On the opposite, in order to gain full information Eve must risk to be revealed with probability 1/2. This argument led authors of PP to assert that Alice and Bob's control mode detects every kind of eavesdropping, and in particular that the detection probability of $d = 1/2$ is significantly greater than that of BB84 for the same situation. Unfortunately neither the former nor the latter assertion are true: first, PP's control mode was hiding some bugs that revealed it to be far from secure [68], [69]; second, for a full amount of information stolen by Eve BB84 establishes precisely the same threshold of detection, $d = 1/2$, of PP, while for the threshold $d = 1/4$ claimed by Boström and Felbinger Eve's information gain is 0.5 [4]. In the following we are going to examine the two main flows of the original Ping-Pong protocol. They will result useful to understand practical, although not general, Eve's strategies to tamper with the communication, and to encompass the main solutions against them.

4.2.1 DoS attack

The first bug of PP's control mode becomes evident if we consider the following attack [68]. It is a kind of DoS (Denial of Service) attack, in which Eve aims at preventing Alice and Bob from communicating at all.

Suppose Eve is in the line. Every control mode is announced publicly by Alice; Eve then can decide not to touch the qubit sent by Alice to Bob at all. In this way she introduce no disturbance. On the opposite in every message mode, Eve captures the qubit traveling on the backward path, measures it in the basis B_z and forwards it to Bob. Alice and Bob have zero probability to find out Eve's attack because there is no attack on the forward line, and no attack on the backward line during the control mode. Then Bob lets communication continue. But every measurement by Bob is meaningless and completely uncorrelated with Alice's choice since the two qubits become independent of each other after Eve's measurement. When the communication is terminated, Bob has learned nothing but a sequence of nonsense random bits.

Another way to perform the same attack is to make a quantum operation on the backward qubit after Alice's operation during the message mode. Eve could for example perform randomly the identity $\mathbb{1}$ or the Z gate on the travel qubit. Also in this case the detection by Alice and Bob is impossible and Bob obtains a meaningless information since Eve's operation is not related to Alice's.

How can this happen? There are several, although not all independent, reasons. In order to make the discussion fluent, and since some typical Eve's attacks will concern also other protocols described in next sections, we give Eve's attacks and Alice&Bob's solutions peculiar names, just for ease of reading.

The first weakness we notice in PP is the *declared control*. When Alice and Bob are going to make a joint test on the quantum channel, Alice declares this fact. This allows Eve not to intervene when a control is going on. So in a word the problem is that there is no control on the backward quantum path. Nevertheless this is unavoidable in PP scheme because Bob must make two different measurements depending on the modality of the run: if the run is a control one he must measure along B_z his photon, while if the run is a message one he must perform a Bell measurement on both photons. Without a public declaration he could not know what to do.

The solution to this problem is a procedure called *message authentication*. It consists in a partial revelation on a reliable classical channel of the information encoded by Alice. If N message runs have been performed by Alice and Bob, the two users decide to sacrifice $n < N$ of these runs, randomly chosen, to verify the information arrived at Bob's site. This procedure can also be accomplished in a run-by-run fashion, by simply revealing the bit encoded after Bob received the qubit and performed the Bell measurement. Bob will either confirm the received information or abort the transmission. In case the sequence represents a meaningful message then Alice can insert in the original sequence some nonsense control bits in random positions of her knowledge. Afterwards, she will publicly reveal these uninformative bits during the message runs, letting Bob verify the information in his hands. The message authentication represents a formidable tool to detect DoS attack as well as other kinds of attack. Moreover it is of the utmost importance when we will consider noise affecting the transmission. We notice that during DoS Bob's Bell measurement is completely random and only in 1/2 of the cases it coincides with Alice's operation. This implies that by introducing message authentication Eve can be detected with a probability of 1/2.

Message authentication control procedure can be applied whenever Alice and Bob mutual information, I_{AB} is less than 1, as in DoS attack. The error rate revealed by Bob in I_{AB} by a comparison with Alice on the public channel is usually known as QBER (Quantum Bit Error Rate), and is the quantity measured during the message authentication. Henceforth we will indicate this quantity with the symbol Q.

Another weakness in the PP control procedure is the test of the initial singlet state. It consists in two local measurements of the single particles along the B_z direction only. This is a quite serious mistake since for Alice and Bob the only mean to verify by local measurements the fidelity between the initial state they share and the singlet state they presume to share is by measuring along at least two different bases! This simple observation is a fundamental brick in the unconditional security proof of BB84 by Lo and Chau [51]. Quite surprisingly, also in [70] we can find the implementation of a protocol very similar to PP and the same kind of an oversight. We call this weakness *lack of symmetry*, with reference to the control procedure. From a practical point of view the lack of symmetry allows Eve to attack also every qubit Bob sends to Alice by measuring them in the B_z basis, without being detected by the test on the forward path. This is the starting point for a powerful attack by Eve based on losses, as we will see.

Although the message authentication can help to restrict Eve's range of action it is clear that the control procedure on the forward line must be improved by means of a *symmetrization* process. It consists, as in BB84, in measuring the initial state both along B_z and along B_x. In this way Alice and Bob have at their disposal a powerful test (powerful enough to grant BB84 unconditional security) to detect every Eve's attack on the forward line, and a message authentication to detect any Eve's intervention on the backward line. Of course in this case the detection probability is no more given by (4.16) but becomes the half, $d' = |\beta|^2/2$, because in halves of the cases Eve will choose the same basis as Alice and Bob.

With these two additional security procedures the PP is secure, even if its rate of transmission is slightly decreased because of the message authentication, that requires a number of message bits to be converted in control bits. Nevertheless we must consider that in general a deterministic protocol is more efficient than its non-deterministic counterpart, since no qubits are discarded because of a wrong choice of the bases.

Attacks based on losses

In [69] is presented an effective eavesdropping strategy based on losses which steals information without being ever detected by Alice and Bob's control mode. This strategy exploits the presence of a further state after those considered above, the vacuum state, that produces no detection but conveys information. The price Eve pays is the creation of additional losses in the transmission from Bob to Alice. These losses can be used to detect eavesdropping in the case of an ideal channel but, in any realistic case of a lossy channel, Eve can replace the original channel by a better one and hide the eavesdropping losses in the channel losses. The eavesdropping strategy is reported in Fig.4.3.

Eve prepares two auxiliary modes (or *ancillae*) x and y in the state $|vac\rangle_x |0\rangle_y$, where $|vac\rangle$ denotes the empty mode and $|0\rangle, |1\rangle$ are referred to polarizations of the modes. The initial state of the whole system is then

$$\Phi^{init} = \left|\Psi^-\right\rangle |vac\rangle_x |0\rangle_y . \tag{4.18}$$

After that Eve performs a quantum operation Q that engage the ancillae and the travel qubit. Generally speaking we can look at Q as an operation that transfers the information contained in the travel qubit on Eve's ancillae. State (4.18) becomes:

$$\begin{aligned} \Phi' &= \frac{1}{2} |0\rangle_h \left(|vac\rangle_t |1\rangle_x |0\rangle_y + |1\rangle_t |1\rangle_x |vac\rangle_y \right) \\ &\quad -\frac{1}{2} |1\rangle_h \left(|vac\rangle_t |0\rangle_x |1\rangle_y + |0\rangle_t |0\rangle_x |vac\rangle_y \right), \end{aligned} \tag{4.19}$$

where the subscript 'h' refers to the 'home qubit' and 't' is the 'travel qubit'.

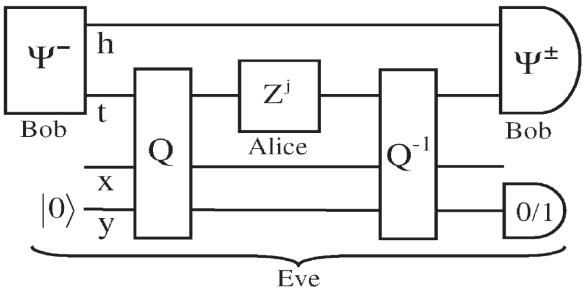

Figure 4.3: Eavesdropping based on losses in the Ping-Pong protocol [69]. The quantum operations Q and Q^{-1} aim at transfer information about Alice's encoding on Eve's ancillae, introducing losses on the channel and altering the initial state. Nevertheless Alice and Bob, with their *imperfect* control mode, can not ascertain Eve's presence.

At this point Alice and Bob could decide to switch to control mode, but from (4.19) is apparent that they cannot detect Eve in any case: the photons h and t, measured respectively by Bob and Alice, are either perfectly anticorrelated or correlated with the empty state. So Alice and Bob will find either a correct response to their control or a loss in the channel which they will ascribe to the bad quality of the transmission.

If on the opposite the two users continue the protocol with a message mode, then a second attack Q^{-1} is performed by Eve on the backward line, after Alice's encoding operation. In this case the final state is

$$\Phi'' = \frac{1}{2}\left(\left|\Psi^+\right\rangle_{ht}\left|j\right\rangle_y + \left|\Psi^-\right\rangle_{ht}\left|j\right\rangle_y - \left|\Psi^+\right\rangle_{ht}\left|0\right\rangle_y + \left|\Psi^-\right\rangle_{ht}\left|0\right\rangle_y\right)\left|vac\right\rangle_x \tag{4.20}$$

and it permits Eve to acquire information about the sequence sent by Alice. The mutual information between two parties A and B is defined as (Sec.3.1):

$$\begin{aligned} I(AB) &= H(B) - H(B|A) \\ &= H(B) - [H(A,B) - H(A)] \\ &= H(B) + H(A) - H(A,B) \end{aligned}$$

and represents a measure of how much A and B contain information about each other. With the above strategy Eve can steal the following informations

$$\begin{aligned} I(AE) &\simeq 0.311 \\ I(BE) &\simeq 0.074 \end{aligned}$$

without being revealed at all.

What we are going to show now is that the solutions provided against the Dos attack of the preceding section, i.e. *message authentication* and *symmetrization* (of the control mode) are effective against this kind of attack too. Rewriting the state (4.19) with X eigenstates we obtain:

$$\begin{aligned} \Phi' &= \frac{1}{2}\left(\frac{\left|+\right\rangle+\left|-\right\rangle}{\sqrt{2}}\right)_h\left(\left|vac\right\rangle_t\left|1\right\rangle_x\left|0\right\rangle_y + \left(\frac{\left|+\right\rangle+\left|-\right\rangle}{\sqrt{2}}\right)_t\left|1\right\rangle_x\left|vac\right\rangle_y\right) \\ &\quad -\frac{1}{2}\left(\frac{\left|+\right\rangle-\left|-\right\rangle}{\sqrt{2}}\right)_h\left(\left|vac\right\rangle_t\left|0\right\rangle_x\left|1\right\rangle_y + \left(\frac{\left|+\right\rangle+\left|-\right\rangle}{\sqrt{2}}\right)_t\left|0\right\rangle_x\left|vac\right\rangle_y\right). \end{aligned} \tag{4.21}$$

It is evident from (4.21) that if Alice and Bob measured along B_x they would obtain vacuum in half of the cases, anticorrelated results 1/4 of the cases but also correlated results (i.e. the evidence for Eve) 1/4 of the cases.

Moreover, from the state (4.20) it is possible to calculate the QBER of the protocol, i.e. the probability that Bob, by a procedure of *message authentication* on the public channel, finds out a discrepancy between his data and Alice's operations. For Ping-Pong protocol QBER amounts to 1/4, showing that message authentication is an effective protection strategy against attacks based on losses.

4.2.2 Improvements and variants

Several protocols have been proposed to improve Ping-Pong [70, 71, 72, 73, 74]. In the next we are going to describe the one by Cai and Li [71].

In their version of Ping-Pong the encoding-decoding phase is precisely the same as in Dense Coding mechanism. Hence, the capacity of the channel results to be double respect to the original Ping-Pong. Furthermore the protocol is endowed with a symmetric control procedure on the forward line and a final message authentication; as outlined above these represent the main solutions to Ping-Pong's problems. The only disadvantage of Cai-Li model is in the decoding phase, that results quite unpractical; in fact, Bob has to perform a complete Bell measurement to determine Alice's transformation, and this is known to be quite a difficult task [64].

Despite of this hindrance, Cai-Li version of Ping-Pong is very interesting from a theoretical point of view. The doubling of the capacity entails at once a doubling in the transmission rate. What is less straightforward is that the increased capacity implies also a higher security of the whole communication. The intuition behind this effect is the following: in the original Ping-Pong Eve must guess one (Alice's) operation between two, while in this version of Ping-Pong she has to guess one among four; in other words since the transformations per single run are four, Alice and Bob mutual information amounts to $I_{AB} = 2$ rather than $I_{AB} = 1$ of the original Ping-Pong. This means that to achieve a full information gain Eve must necessarily cause a higher disturbance d on the line or, the same, a higher error rate Q in the information received by Bob. As will result clearer in next sections to steal this information Eve must risk to be detected with probability $d_{CL} = 1/2$ [4]; this value must be compared with $d = 1/4$ given in the original Ping-Pong protocol after its control procedure has been symmetrized.

As a final remark we observe that high capacity of the quantum channel is even more important when noise is taken into account. In fact we anticipate here that the necessary and sufficient condition to distill a random secure key in presence of noise is:

$$I_{AB} > I_{AE} \quad \text{or} \quad I_{AB} > I_{BE},$$

i.e. the mutual information between the legitimate users must be greater than that between one of them and Eve. Hence, the greater I_{AB}, the more secure the communication on the noisy channel.

[4] the value $d = 3/8$ found by Cai and Li must be revisited. The new value results by the analysis performed in Sec.6.4.

Chapter 5

DQC without entanglement

You must not copy as a monkey,
you must be a monkey!

Lucio Dalla, Italian singer

Entanglement is not a fundamental resource for security of quantum cryptosystems. As Bennett demonstrated in 1992 [59] it is always possible to create a protected quantum communication scheme by using only two *non-orthogonal states*; non-orthogonality substitutes entanglement in guaranteeing security. Furthermore in [58] it is shown a general equivalence between EPR-based schemes for QKD and non-orthogonality-based ones. By consequence it is possible to envisage a deterministic communication that does not make use of entanglement. Although technology greatly widened its horizons in the last decades, protocols that do not need entanglement to function remain definitely more simple to realize in a laboratory.

To our knowledge the first deterministic quantum cryptosystem that does not make use of entanglement is presented in [75]. This quantum cryptosystem results quite involved, for reasons that leave entanglement apart[1]. For this reason we do not discuss it here. On the contrary, we are going to describe the protocol by Cai and Li [76], and the one I proposed and developed during my last year of Ph.D., "PP84" [77]. They both do not require entanglement to work. Particular attention is devoted to the question of PP84's security against *individual attacks*. The next chapter will complete the picture by taking into account other aspects like *asymptotical* and *unconditional* security, and *efficiency*.

For explicative purposes we are going to introduce at first the cryptosystem by Cai and Li, that uses only two non-orthogonal states to convey information in a "quasi-secure" manner. After that we pass to the four-states PP84. This order reflects the chronological order of the scientific publications relative to the Cai-Li and PP84 protocols. However we point out that only after completion and submission of our work we became aware of the manuscript by Cai and Li published on *Chinese Physics Letters*.

[1] We mention that a continuous-variable version of this protocol leads to a very elegant and easy-to-use deterministic quantum cryptosystem [60]. Examples of "continuous" variables are the *position* and the *momentum* of a harmonic oscillator.

5.1 Cai-Li protocol

Cai-Li protocol (CL) [76] is based upon the intuition that it is possible to achieve a deterministic communication between Alice and Bob by using two single-particle states rather than one two-particle entangled state. Security of the transmission is assured by the non-orthogonality of the states involved, analogously to what happens in Bennett's two-state protocol[2]. Thus entanglement is not anymore a fundamental resource neither for the encoding-decoding procedure nor for the control one.

The encoding-decoding procedure goes as follows. Suppose Bob prepares two non-orthogonal states in the x-z plane of the Poincaré sphere representing the polarizations of the photon. These states are $|0\rangle$ and $|+\rangle$, the upper eigenstates of Z and X respectively. The fundamental observation to understand the encoding-decoding modality is represented by the following transformations on these two states:

$$\begin{aligned} \mathbb{1}\{|0\rangle, |+\rangle\} &= \{|0\rangle, |+\rangle\} \\ iY\{|0\rangle, |+\rangle\} &= \{-|1\rangle, |-\rangle\} \end{aligned} \tag{5.1}$$

where $|1\rangle$ and $|-\rangle$ are the lower eigenstates of Z and X respectively; $\mathbb{1}$ is the identity operator and Y is one of Pauli matrices according to the usual definition. From Eq.(5.1) we can see that when identity acts on the two states they do not change, while when iY acts on them they are *flipped*. In this way the absence of a flip can be associated to the information '0', and the presence of a flip to the information '1'.

Bob then prepares a qubit randomly in one of the states $|0\rangle$ (basis: B_z) or $|+\rangle$ (basis: B_x) and sends it to Alice. Alice decides with probability c to switch to *control mode*, and with probability $(1-c)$ to remain in *message mode*, with a procedure similar to that envisaged for Ping-Pong protocol. In message mode she performs the operation $\mathbb{1}$ to encode the information '0' or the operation iY to encode '1'. Then she sends the qubit back to Bob who will measure it in the same basis he used for preparation. This point is not specified in Cai and Li's paper, but it is fundamental to achieve a deterministic communication. In fact Alice's operation does not change the basis of the state prepared by Bob, and this allows Bob to make a deterministic measurement if he uses the same initial basis. If Alice switches to control mode, then she must prepare, without measuring at all the received qubit, a new qubit in one of the four states $|0\rangle, |1\rangle$ (basis: B_z) or $|+\rangle, |-\rangle$ (basis: B_x), and send it to Bob. Bob will measure it in the initial basis; in half of the cases Alice and Bob's preparation bases will coincide, and their measurements will be correlated. These cases must be used by Alice and Bob to detect a malicious Eve. The proof adducted by Cai and Li is the weak version of a security proof i.e. they showed that *Lo-Chau lemma* (see Sec.3.3) holds for their scheme.

Together with the control procedure described above, Cai and Li provided their protocol with a *message authentication* procedure, to prevent DoS attack (Sec.4.2.1). Despite these two procedures of control we show now that CL is not secure against the so called "opaque attacks", that are based on losses.

5.1.1 Opaque attack

An *opaque attack* is performed by Eve substituting the forward line with a BEC (Sec.3.1): Eve exploits the lack of symmetry of the initial states to perform a POVM capable to provide her either with definite results or with inconclusive ones. To be concrete we take a particular case of the

[2]This second assertion is not completely true, as it will be argued later on.

three POVMs defined in Eq.(3.10):

$$\begin{aligned} A_1 &= \frac{1}{2}\left(|1\rangle\langle 1|\right), A_- = \frac{1}{2}\left(|-\rangle\langle -|\right), \\ A_? &= \mathbb{1} - A_0 - A_- = \frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right). \end{aligned} \tag{5.2}$$

Although they do not represent the most efficient choice, they provide a simple view of the attack at issue. A quantum test yielding A_1 (A_-) rules out the initial state $|0\rangle$ ($|+\rangle$) which is orthogonal to it. Instead $A_?$ yields an inconclusive result. Though this *non-standard* measurement is always less effective than a *standard* one in collecting information about the measured state, we must remember that Eve does not aim at guessing the state prepared by Bob, but rather at guessing the operation performed by Alice. Then Eve can proceed as follows: if she obtains the definite outcome A_1 (A_-) then she registers the result and forwards the state $|+\rangle$ ($|0\rangle$) to Alice; in this case a control mode by Alice and Bob can not detect anything, because Eve knows Bob's preparation with certainty. On the contrary if Eve obtains the inconclusive outcome $A_?$ then she does not forward anything to Alice; a control mode detects in this case one loss, attributed by Alice and Bob to the lossy channel. On the backward line, Eve measures along the same basis she used on the forward line, causing no disturbance, and sends the projected qubit to Bob, who will certainly measure in the same, correct basis in order to decode information. A final cunning by Eve is to filter out a fraction of the photons on the backward path; without this trick no losses would occur on the backward, and this would be detected by Alice and Bob. The probability of an inconclusive result on the forward path is

$$\langle 0| A_? |0\rangle = \langle +| A_? |+\rangle = \frac{3}{4}.$$

This implies that on the backward path Eve must filter out about 75% of the photons. The efficiency is then $\eta_{fb} = \eta_f \times \eta_b = (25\%)^2 = 6.25\%$, that represent a very bad channel for Alice and Bob. Notwithstanding the theoretical problem remains, and the security of this protocol is ruled out by this strategy based on losses, since Eve acquires full information by means of it without being detected. Once again we can notice as a lack of symmetry, this time in the initial preparation, leads to a lower level of security.

5.2 PP84 protocol

In the preceding sections we saw how a deterministic communication can be achieved by means of quantum mechanics. Dense Coding, Ping-Pong and Cai-Li protocols represent different ways to perform this task by exploiting entanglement or not. Unfortunately, as we saw, none of them was proved to be completely secure. Now we are going to introduce a secure communication protocol that combines the main advantages of the previous ones while avoiding their drawbacks, and we term it PP84 [77]. We show here its security against a wide variety of attacks called *individual attacks*.

The idea is summarized in Fig.5.1; the detailed protocol is reported in Appendix D. Bob prepares a qubit in one of the four randomly chosen states

$$\begin{aligned} &|0\rangle, |1\rangle \ \text{(eigenstates of operator } \hat{S}_z) \\ &|+\rangle, |-\rangle \ \text{(eigenstates of operator } \hat{S}_x) \end{aligned} \tag{5.3}$$

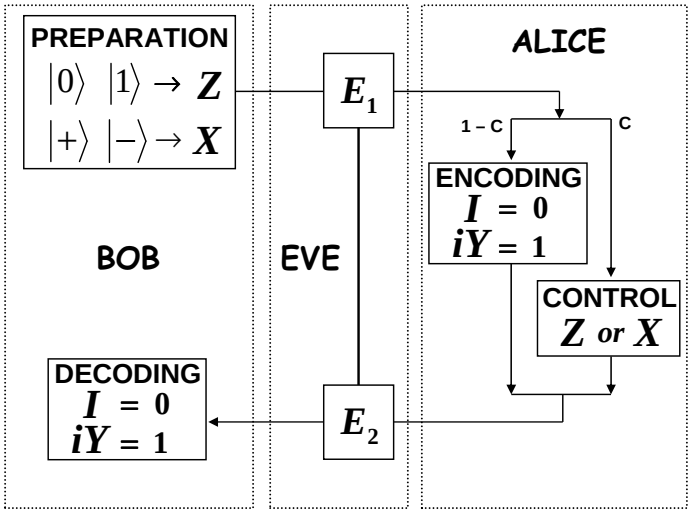

Figure 5.1: PP84 scheme

and sends it to his counterpart Alice. With probability (c) Alice measures the prepared state (control mode) or, with probability $(1-c)$, she uses it to encode a bit (encoding mode). After that she will send the qubit back to Bob. Encoding is represented by a transformation on qubit state rather than by qubit state itself: identity operation $\mathbb{1}$ encodes the bit '0', while operation $iY = ZX$ encodes the bit '1'. Notice that, as in Cai-Li protocol, the essential feature of the encoding-decoding phase resides in the action of the operator iY upon the four initial states:

$$\begin{aligned} iY\left(|0\rangle, |1\rangle\right) &= \left(-|1\rangle, |0\rangle\right) \\ iY\left(|+\rangle, |-\rangle\right) &= \left(|-\rangle, -|+\rangle\right) \end{aligned} \tag{5.4}$$

i.e. it acts as a spin-flip on all the beginning states. In this way Alice does not need to know the incoming state to perform the encoding. In turn Bob can easily decode Alice's message by measuring the qubit in the same basis he prepared it. This feature makes the protocol deterministic, i.e. the information is *deterministically* conveyed from one user to another. By consequence no qubits are discarded because of a wrong choice of the bases, as it happens in BB84, and no public discussion is necessary for the completion of the encoding-decoding procedure. Furthermore, we notice that this scheme provides a real "distribution" of the key: Alice holds the random key *before* the communication begins; then, during the protocol, she *distributes* it to Bob by means of the encoding operations $\mathbb{1}$ and iY. On the contrary, what is called QKD in the non-deterministic BB84 is rather a quantum key "generation", because the final key is not known in advance by anyone, and is *generated* while the protocol is running on. Established this point, it is straightforward to realize that Alice can also send to Bob a meaningful string of bits rather than a random key, that is a *plain-text*. In this case a *Quantum Direct Communication* (QDC) is addressed.

To guarantee security of PP84, Alice has to switch to *control mode* with a probability $c > 0$. In this modality she performs a projective measurement on the incoming qubit along a basis randomly chosen between Z and X, as in BB84. Then, she sends the projected qubit back to Bob. In turn, after declaring on the classical channel the receipt of the qubit, Bob carries out his measurement as exactly he would do if Alice had decided for a *message mode* (actually, he does not still know

Alice's choice). At this point Alice reveals on the classical channel whether she measured (and in which basis) or not, and a public debate on results is settled with Bob in the former case. Notice that if Eve is not on the line a perfect ∨double correlation" (on the forward and backward paths) of measurement outcomes must be found by legitimate users. We point out that the "run-by-run" execution of PP84 just described is only necessary for QDC, which is more demanding on security. On the contrary QKD can be implemented both run-by-run and by deferring all public discussions at the end of the whole transmission. This was not possible in Ping-Pong protocol, where the run-by-run modality is essential for the decoding procedure [63].

Let us describe briefly Eve's possibilities of intervention. As shown in Fig.5.1 Eve can intervene both on the forward path (attack E_1) and on the backward path (attack E_2) with the aim of stealing information or simply disturbing the communication. In the former case she is obliged to intervene on both lines, while in the latter case she can intervene once, either on forward or on backward line. This double attack can be managed by Eve in different ways. She can attach a different probe to every single qubit passing through the quantum channel, and either measure them singularly (in this case we speak of *individual attacks*) or measure them with an unique final measurement (in this case we speak of *collective attacks*). Or she could use only one probe in a very large Hilbert space, makes it interact with all the qubits, and finally measure it (a so called *joint attack*). In any case the disturbance Eve creates with her attacks allows Alice and Bob to upper bound the information she caught. This is the mechanism that assure the protocol is secure. We begin the discussion about eavesdropping from individual attacks, because they are the simplest, yet not trivial, conceivable. Moreover, just because of their easiness, individual attacks represent the most practical ones, and some of them can be issued with current technology. More complicate attacks can be brought by Eve creating coherence between different runs, but this possibilities are for the moment neglected.

5.2.1 Individual attacks

As we already pointed out dealing with Ping-Pong protocol, *individual attacks* are the simplest we can figure out considering eavesdropping. They begin and terminate in the space of a single run. Eve prepares one or more *ancillary qubits* in a known state and makes them interact with the qubit both on the forward and on the backward path. Then she measures the ancillae. Despite their simplicity individual attacks contain all the essential features of the eavesdropping problem.

DoS attack

The name "DoS" stands for *Denial of Service*. With this kind of attack Eve prevents Alice and Bob from communicating. In PP84 the DoS attack can be performed essentially in two ways:

i) by measuring twice the qubit, on the forward and on the backward path, along different bases. For example Eve could use $\hat{S}_z$ on the forward path and $\hat{S}_x$ on the backward path, or viceversa. Bob would find always a nonsense result since at least one basis is certainly wrong, and this makes his measure completely random.

ii) by performing an unitary operation on the qubit either on the forward line or on the backward one. In this way Eve adds her operations to Alice's ones, thus preventing Bob from gaining the correct sequence.

We notice that the latter method can also be used in BB84, while is not so for the former one, since Eve should know the correct basis to actuate it. Let us examine how Alice and Bob can detect the two DoS strategies, beginning from the first one.

Let us suppose Bob prepares the state $|0\rangle$ of $\hat{S}_z$ and that Eve chooses to measure along $\hat{S}_z$ on the forward path and along $\hat{S}_x$ on the backward path. Let us also suppose that Alice decides to

switch to control mode and to measure along the right basis $\hat{S}_z$ (in the other case the run would be discarded). We remember that PP84 control mode establishes that if Alice measures $\hat{S}_z$ then she sends to Bob the qubit projected along this direction. Bob, in turn, will measure along the basis he prepared the qubit in. So if Bob prepares $|0\rangle$ and Eve measures along $\hat{S}_z$ on the forward path she does not perturb the state, and an Alice measuring in the correct basis will find $|0\rangle$ with certainty; everything is fine on the forward path. She then sends this same state back to Bob, but during the backward travel Eve measures it along $\hat{S}_x$, thus projecting it in $|+\rangle$ or $|-\rangle$. This entails that when Bob measures the incoming qubit again in $\hat{S}_z$ he finds a result different from $|0\rangle$ in half of the cases. Then Alice and Bob detect Eve with a probability for each control run equal to $d_2 = 1/2$. Of course the same argument holds when Eve measures with inverted bases, with the only difference that it will be Alice to detect her with probability $d_1 = 1/2$.

Now we consider the second strategy by Eve, a random execution of identity or flip operation on one of the two paths, say on the backward path. During a control mode in which Alice guesses Bob's preparation basis, nothing can be revealed along the forward channel, because nobody tampered with it there. On the contrary, on the backward path, Eve changes the state of the qubit, by flipping it, in half of the cases. Eve is undetectable when she performs the identity, but she is detected with certainty when she flips the state. In fact, let us suppose, as before, that Alice sends out $|0\rangle$ and Eve flips it in $|1\rangle$. A Bob measuring along $\hat{S}_z$ will certainly find a wrong result, i.e. $|1\rangle$, instead of the $|0\rangle$ declared by Alice on the public channel. Therefore also in this case we find an average detection probability of $d = (0 + 1)/2 = 1/2$. We would have obtained the same result if instead of randomly perform 1 or iY Eve had effected the operation $\exp\left(i\frac{\pi}{4}Y\right)$ on the qubit. This operation changes the basis of the qubit:

$$\begin{aligned} \exp\left(i\frac{\pi}{4}Y\right)|0\rangle &= \frac{1}{\sqrt{2}}\left[\mathbb{1} + iY\right]|0\rangle = |-\rangle \\ \exp\left(i\frac{\pi}{4}Y\right)|1\rangle &= \frac{1}{\sqrt{2}}\left[\mathbb{1} + iY\right]|1\rangle = |+\rangle\,. \end{aligned}$$

So the effect would have been the same as the one resulting from the first Eve's strategy we described. Then also in this case the average detection probability is $d = 1/2$. Hence we can conclude that the detection probability pertaining to DoS attack is:

$$d_{PP84}^{DoS} = \frac{1}{2}.$$

We observe that the above detection probability results to be exactly the same found in BB84 for the analogous situation. The two protocols are equally secure against DoS attack.

Quantum man-in-the-middle attack

A "man-in-the-middle" attack includes all those attacks in which Eve tries to pass her off as Alice when talking with Bob and as Bob when talking with Alice. The most dangerous attack of this type is when Eve has full control of the classical channel. There is no solution against this kind of attack except the sharing by legitimate users of a prior secret letting them authenticate the channel and make it reliable. For "quantum man-in-the-middle" (QMM) we mean something similar, but on the quantum channel. Eve intercepts Bob's qubit and put it in an ideal quantum memory. In the while she forwards to Alice a qubit chosen by her that we will call $|\varepsilon\rangle$. Then, on the backward line, she measures $|\varepsilon\rangle$ in the same basis it belongs to, thus decoding Alice's transformation. Finally Eve applies the apprehended transformation to the stored qubit and forwards it to Bob. In other words she substitute to Bob to steal Alice's information and substitute to Alice to send Bob the

stolen information. This justifies the name of this attack. Figure 5.2 helps to understand this strategy.

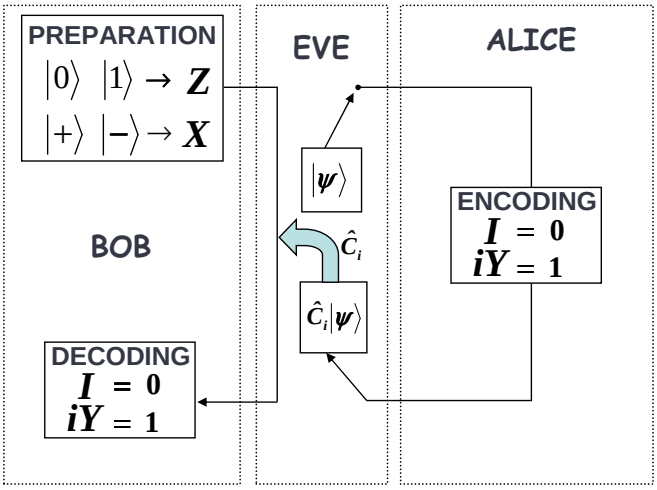

Figure 5.2: Schematics of the QMM attack. Eve substitutes to Bob in sending Alice a qubit state Ψ, and to Alice in performing the operation $\hat{C}_i$ on Bob's qubit.

This is a very interesting example. We can see how a *message authentication* protection strategy does not work in this case. In fact Bob receives exactly what Alice encoded, because Eve performs on his qubit the same operation Alice performed on the faked qubit sent to her by Eve. However with the double control present in PP84 this strategy can be detected by Alice and Bob with high probability. To find out this probability suppose that Bob prepares the state $|0\rangle$, and that Eve substitute it with $|\varepsilon\rangle$. If $|\varepsilon\rangle$ is chosen among the four states (5.3), Eve has 1/4 of possibilities to guess it. If she guesses it she is not revealed at all. If she sends Alice the state $|1\rangle$ she is detected with certainty on both paths. If she sends $|+\rangle$ or $|-\rangle$ then she is detected with probability 1/2 on the forward path, and with the same probability on the backward path. In fact in control mode Alice will measure the incoming state in the basis $\hat{S}_z$ (in the other case the run is discarded). This means that $|\varepsilon\rangle$ is projected with probability 1/2 in the correct state $|0\rangle$ (and Eve is not revealed) and with probability 1/2 in the wrong state $|1\rangle$ (and Eve is revealed). In both cases Alice, during the second phase of the control mode, will send to Bob the state she obtained from her measurement, i.e. a state prepared along the basis $\hat{S}_z$. Eve does not know that a control run is going on, and in order to decode Alice's operation she measures $|\varepsilon\rangle$ along the basis $\hat{S}_x$, thus obtaining a perfectly random result. Then she applies this random result to the qubit she stored. When Bob measures the state entering his site he finds with equal probabilities the same state he prepared or the flipped one. Being the result of his measurement completely random, it is clear that Eve is detected with probability 1/2 on the backward path, i.e the same probability we had on the forward path. This entails that the probability Eve *is not* detected in a whole control run amounts at $(1/2) \times (1/2) = 1/4$, making Eve detectable with probability $1 - 1/4 = 3/4$. We can conclude that the average probability to detect Eve's QMM attack in PP84 is:

$$d_{PP84}^{QMM} = \frac{(0 + 1 + 2 \times 3/4)}{4} = \frac{5}{8}$$

that is more than 1/2, i.e more than the detection probability for the same strategy in BB84. The value 1/2 is easily obtained by calculating the fidelity $F = |\langle\Psi|\Phi\rangle|^2$ between two pure states randomly chosen in a plane of the Bloch sphere (we are interested in the $x - z$ plane to describe the situation in which Eve tries to guess one of the states (5.3)):

$$\begin{aligned} F &= |\langle\Psi|\Phi\rangle|^2 = \frac{1}{2\pi}\int_0^{2\pi} |(\cos\theta)\,\langle 0|0\rangle + (\sin\theta)\,\langle 0|1\rangle|^2 \\ &= \frac{1}{2\pi}\int_0^{2\pi} |(\cos\theta)|^2 = \frac{1}{2} \end{aligned} \tag{5.5}$$

This calculation contains an essential point to note: in this strategy Eve does not try to know which state Bob prepared by measuring it, yet she can still eavesdrop all the information. This means that the price Eve pays in disregarding Bob's preparation is not the limited amount of information she can steal but rather the high detection probability she suffers in a control run. A good strategy by Eve should include the minimization of the fidelity (5.5) to decrease the detection probability. This is very different from BB84 in which the knowledge of the initial state by an appropriate measurement determines both detection probability and the amount of stolen information. We will see an application of this argument in the next section. But there is also a subtle advantage for Eve in this kind of attack. Eve, by preserving Bob's state and subsequently by operating on it a transformation of her choice, can know exactly which result Bob will find during a message mode. In terms of information this means that the mutual information I_{BE} between Bob and Eve is very high. This can reveal a very useful tool for Eve.

Measure-and-resend attack

In this kind of eavesdropping Eve randomly decides a basis, $\hat{S}_z$ or $\hat{S}_x$, along which performing projective measurements on the traveling qubit, both on the forward and on the backward paths. Suppose Bob prepares the state $|0\rangle$. If Eve measures along $\hat{S}_z$ she does not perturb the state. Then Alice transform it into $|0\rangle$ or $|1\rangle$. By a second measurement along $\hat{S}_z$ on the backward path Eve can guess Alice's transformation exactly as Bob would do, without errors nor perturbations. If instead Eve measures along $\hat{S}_x$ then the initial state is projected into $|+\rangle$ or $|-\rangle$. After Alice's encoding she can still make a correct guess by measuring along $\hat{S}_x$, but both on the forward and on the backward paths she perturbed the travelling state.

With this strategy Eve aims at increasing her knowledge on the state prepared by Bob; this could permit Eve to improve the fidelity (5.5) between the state prepared by Bob and the one received by Alice, thus decreasing the detection probability. In fact, if Eve performs a projective measurement on the initial qubit $|\Psi\rangle_B$ it becomes:

$$F = \langle\Psi_B|\,\rho\,|\Psi_B\rangle$$

where

$$\rho = \sum\nolimits_i \left(\langle\Psi_B|\,\hat{P}_i\,|\Psi_B\rangle\right)\hat{P}_i$$

and $\hat{P}_i$ are the projectors representing the measurement (Sec.3.1.1). The quantities $\left(\langle\Psi_B|\,\hat{P}_i\,|\Psi_B\rangle\right)$ are the probabilities p_i that the outcome i of the measurement occurs. We can consider without loss of generality that Eve decides to measure along $\hat{S}_z$. In this case we indicate the projectors as $\hat{P}_1 = \hat{P}_\uparrow$ and $\hat{P}_2 = \hat{P}_\downarrow$ and the fidelity is:

$$\begin{aligned} F &= \left(\langle\Psi_B|\,\hat{P}_\uparrow\,|\Psi_B\rangle\right)^2 + \left(\langle\Psi_B|\,\hat{P}_\downarrow\,|\Psi_B\rangle\right)^2 \\ &= p_\uparrow^2 + p_\downarrow^2 = p_\uparrow^2 + (1-p_\uparrow)^2 = 2p_\uparrow^2 - 2p_\uparrow + 1. \end{aligned}$$

The average fidelity is obtained by the formula above considering an uniform distribution for the results of the measurement, since the initial states are uniformly distributed with respect to the basis $\hat{S}_z$. Then

$$\overline{F} = \int_0^1 dp \left(2p^2 - 2p + 1\right) = \frac{2}{3}. \tag{5.6}$$

The fidelity (5.6) is higher than (5.5), and for this reason Eve expects the detection probability to be lower than that found in the QMM attack. Let us calculate it. As we anticipated in the example at the beginning of this section Eve can guess the right basis with probability 1/2, and in this case she is not revealed at all. If otherwise Eve chooses the wrong basis she still has a probability of 1/2 to evade detection at point E_1 and 1/2 at point E_2 giving in the whole a probability of 1/4 to evade detection. This means that Alice and Bob's double test reveals Eve with an average probability equal to:

$$d_{PP84}^{MR-zx} = \frac{(0 + 3/4)}{2} = \frac{3}{8} = 37.5\% \tag{5.7}$$

that is indeed lower than that obtained with the QMM attack. Remarkably, this value is greater than the one obtained in BB84 (25%) for the same eavesdropping strategy, but we must consider that in BB84 Eve could steal only 1/2 of the full information.

We notice that Eve could perform the same projective measurement along any basis of her choice gaining the same full information, because the important thing to gain full information is to measure twice in the same basis. Furthermore the fidelity (5.6) and the detection probability *on the single line* would not change. Nonetheless, the control mode involves two lines rather than one, and in this case the choice of the measurement basis makes a difference to Eve. Generalizing to any basis the argument leading to Eq.(5.7) we can write the detection probability on the double line of PP84's control mode as:

$$d_{PP84}^{MR} = \frac{1}{2}\left[cs(0) + cs(\frac{\pi}{4})\right], \tag{5.8}$$

where $cs(a)$ is the function:

$$\begin{aligned} cs(a) &= 1 - [\cos^4(x-a) \\ &+ \sin^4(x-a)]^2. \end{aligned}$$

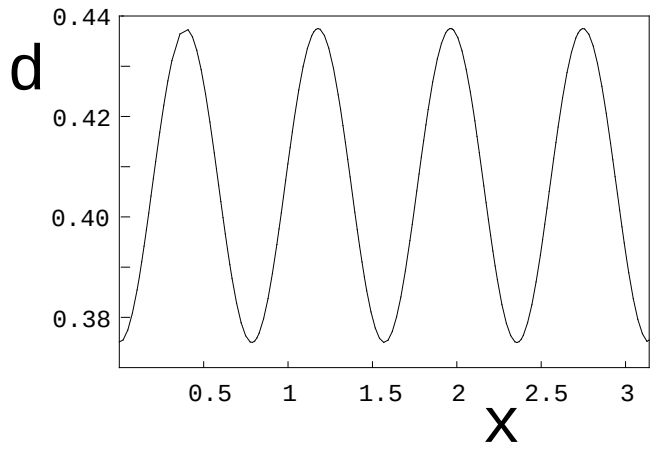

Figure 5.3: Plot of the quantity d_{PP84}^{MR} of Eq.(5.8). x is the angle between the $\hat{z}$ axis and the axis of Eve's measuring basis on the x-z plane; d is the probability Eve is detected by means of PP84's double control. The curve shows that detection probability varies according to the basis used by Eve to eavesdrop information. In other terms the double control brakes the symmetry of Eve's choice. The lowest detection probability $d = 37.5\%$ is obtained for $x = 0$ ($\hat{S}_z$ basis) and $x = \pi/4$ ($\hat{S}_x$ basis).

The quantity d_{PP84}^{MR} is plotted in Fig.5.3. The two main terms within square brackets correspond to Bob's random choice of the initial state's basis; the fourth power comes from the double projection, by Eve and Alice, or by Eve and Bob, of the travelling state. The square is related to the double detection. We can see that the detection probability oscillates between the values $0.375 = 3/8$,

obtained if Eve chooses randomly between $\hat{S}_z$ and $\hat{S}_x$, and $0.437\,5 = 7/16$, obtained in the so called "intermediate basis" or "Breidbart basis", i.e. when $x = \pi/8$. This feature is peculiar of PP84: the double control present in it leads to a preferred couple of basis along which perform the projective measurement, that is the same couple of bases chosen by Bob to prepare the initial state. On the contrary in BB84 any basis led to the same QBER (25%) because the fidelity (5.6) is independent from the choice of the basis. We call this feature of BB84 *bases symmetry* and, correspondingly, we will use the expression *bases symmetry breaking* for PP84. This symmetry breaking will play a role in the study of non-orthogonal attacks.

We would like to note that the value of 3/8 found for the detection probability against this strategy is strongly believed to be the lowest possible when Eve aims at stealing full information. A rigorous proof of this claim is still lacking, even if several indications suggest it is true. This value must be compared with the values 1/2 of BB84's QBER and 1/4 of the improved Ping-Pong protocol for the same situation. From this point of view PP84 reveals to be more secure than Ping-Pong and less secure than BB84 when a full amount of information is stolen by Eve. This could be quite surprising, because PP84 is provided with a double control instead of BB84's single control, and because PP84 does not need any public bases revelation, contrary to BB84; but this is the evidence of the above calculations.

As a final remark we notice that this strategy is not optimal for Eve. In fact Eve, by her first projective measurement on the qubit prepared by Bob, destroys almost any information contained in it, thus making it impossible to guess Bob's final result. This means that Eve has no more control on the mutual information with Bob, I_{BE}, as in QMM strategy, thus loosing a powerful tool of eavesdropping. The lower control by Eve is witnessed by the fact that a *message authentication* protective strategy would be, in this case, perfectly effective.

Non-orthogonal attack

A straightforward generalization of the above argument is given by an attack composed by two non-orthogonal measurements. Given the four states prepared by Bob, and Eve's ancillary states $|\varepsilon\rangle$, we can write the most general operation Eve can do on traveling qubit at point E_1 as:

$$|0\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle = \sqrt{F}|0\rangle|\widetilde{\varepsilon}_{00}\rangle + \sqrt{D}|1\rangle|\widetilde{\varepsilon}_{01}\rangle \tag{5.9}$$

$$|1\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle = \sqrt{D}|0\rangle|\widetilde{\varepsilon}_{10}\rangle + \sqrt{F}|1\rangle|\widetilde{\varepsilon}_{11}\rangle \tag{5.10}$$

$$\begin{aligned} |+\rangle|\varepsilon\rangle &\to \frac{1}{\sqrt{2}}\left[|0\rangle\left(|\varepsilon_{00}\rangle + |\varepsilon_{10}\rangle\right) + |1\rangle\left(|\varepsilon_{01}\rangle + |\varepsilon_{11}\rangle\right)\right] \\ &\equiv |+\rangle|\varepsilon_{++}\rangle + |-\rangle|\varepsilon_{+-}\rangle \end{aligned} \tag{5.11}$$

$$\begin{aligned} |-\rangle|\varepsilon\rangle &\to \frac{1}{\sqrt{2}}\left[|0\rangle\left(|\varepsilon_{00}\rangle - |\varepsilon_{10}\rangle\right) + |1\rangle\left(|\varepsilon_{01}\rangle - |\varepsilon_{11}\rangle\right)\right] \\ &\equiv |+\rangle|\varepsilon_{-+}\rangle + |-\rangle|\varepsilon_{--}\rangle \end{aligned} \tag{5.12}$$

where the states $|\varepsilon_{ij}\rangle$ belong to the Hilbert space of Eve's probe and satisfy $\langle\varepsilon_{00}|\varepsilon_{01}\rangle = \langle\varepsilon_{10}|\varepsilon_{11}\rangle = 0$. Ancillary states with tilde are intended to be normalized. The following conditions make the transformations (5.9-5.12) unitary:

$$\langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle \equiv F + D = 1 \tag{5.13}$$

$$\langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle \equiv D + F = 1 \tag{5.14}$$

$$\langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0 \tag{5.15}$$

Within condition (5.15) we can set, without loss of generality, $\langle\varepsilon_{00}|\varepsilon_{10}\rangle = \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0$ [4]. Furthermore, we specify the angles between non-orthogonal vectors as:

$$\langle\widetilde{\varepsilon}_{00}|\widetilde{\varepsilon}_{11}\rangle = \cos x\,, \qquad \langle\widetilde{\varepsilon}_{01}|\widetilde{\varepsilon}_{10}\rangle = \cos y \tag{5.16}$$

with $0 \leq x\,,\, y \leq \pi/2$. In this sense the present strategy represents a non-orthogonal attack. Here, we don't fix values of the parameters we introduced. In [4] symmetry arguments lead to assume $F = \langle\varepsilon_{00}|\varepsilon_{00}\rangle = \langle\varepsilon_{++}|\varepsilon_{++}\rangle$. This reasoning is not applicable in our case because of what we called *bases symmetry breaking* in the preceding section. The contents of that argument were that not all the bases are equally good for Eve; some of them are less detectable. Moreover we point out here that this symmetry breaking occurs in two steps: the first, just described, suggests Eve that the couple of bases $\hat{S}_z - \hat{S}_x$ is preferable to any other, because Bob is using that couple to prepare the initial states; and this is a feature of PP84's control mode. The second step, on the contrary, is peculiar of PP84's message mode: in fact the absence of a classical discussion during this phase prevents Eve from waiting for a public bases revelation, as happens in BB84, thus forcing her to decide in which basis the measurement must be performed. This breaks the bases symmetry further, but this time within the couple $\hat{S}_z - \hat{S}_x$.

At point E_2 Eve performs an attack similar to that at point E_1, with fresh ancillae $|\eta\rangle$ (hence new parameters F' and D') in order to gain information about Alice's encoding[3]:

$$|0\rangle\,|\eta\rangle \rightarrow \sqrt{F'}\,|0\rangle\,|\widetilde{\eta}_{00}\rangle + \sqrt{D'}\,|1\rangle\,|\widetilde{\eta}_{01}\rangle \tag{5.17}$$

$$|1\rangle\,|\eta\rangle \rightarrow \sqrt{D'}\,|0\rangle\,|\widetilde{\eta}_{10}\rangle + \sqrt{F'}\,|1\rangle\,|\widetilde{\eta}_{11}\rangle \tag{5.18}$$

$$|+\rangle\,|\eta\rangle \rightarrow |+\rangle\,|\eta_{++}\rangle + |-\rangle\,|\eta_{+-}\rangle \tag{5.19}$$

$$|-\rangle\,|\eta\rangle \rightarrow |+\rangle\,|\eta_{-+}\rangle + |-\rangle\,|\eta_{--}\rangle \tag{5.20}$$

At the end of transmission Eve will measure ε and η ancillae and, by comparing results, she will gain information. Our next task is to recover the optimal eavesdropping strategy by Eve, i.e. determine parameters' values that maximize Alice-Eve and Bob-Eve mutual informations ($\mathcal{I}_{AE}$, $\mathcal{I}_{BE}$) minimizing the probability to detect Eve (P_d).

From transformations (5.9-5.12) and conditions (5.13-5.15) we can evaluate the probability that Eve *is not detected* in the forward path, after her E_1-attack:

$$P_{nd}(|0\rangle) = \langle\varepsilon_{00}|\varepsilon_{00}\rangle = F \tag{5.21}$$

$$P_{nd}(|1\rangle) = \langle\varepsilon_{11}|\varepsilon_{11}\rangle = F \tag{5.22}$$

$$P_{nd}(|+\rangle) = \langle\varepsilon_{++}|\varepsilon_{++}\rangle = (1/2)\,[1 + F\cos x + D\cos y] \tag{5.23}$$

$$P_{nd}(|-\rangle) = \langle\varepsilon_{--}|\varepsilon_{--}\rangle = (1/2)\,[1 + F\cos x + D\cos y] \tag{5.24}$$

Similar arguments hold for the backward path, after E_2-attack, with primed parameters replacing not-primed ones. The probability that Eve is not detected after a whole run is then the product of the two partial probabilities; by taking its complement we obtain the probability to detect Eve. Averaging it over all input states we get:

$$\begin{aligned} P_d = (1/8)\{&7 - 4FF' - F\cos x - D\cos y - F'\cos x' \\ &- D'\cos y' - FF'\cos x\cos x' - FD'\cos x\cos y' \\ &- DF'\cos y\cos x' - DD'\cos y\cos y'\} = d + \xi \end{aligned} \tag{5.25}$$

[3]It is important to note that we are making the hypothesis that Eve adopt this strategy, composed by the above two attacks. Nobody forbids Eve to perform a DoS attack on the backward line, but this is not the case we want to examine.

where:

$$d = \frac{1}{2}\left[1 - \frac{1}{4}\left(1+\cos x\right)\left(1+\cos x'\right)\right] \tag{5.26}$$

and:

$$\begin{aligned}\xi &= \frac{1}{2}\{(1-FF') + D\left(1+\cos x'\right)\left(\cos x - \cos y\right) + \\ &+D'\left(1+\cos x\right)\left(\cos x' - \cos y'\right) + DD'\left(\cos x - \cos y\right)\left(\cos x' - \cos y'\right)\}.\end{aligned} \tag{5.27}$$

Now we are going to show that $\xi \geq 0$. This is true because $\cos x$ and $\cos x'$ appear in ξ only with positive sign ($0 \leq x\,,\, y \leq \pi/2$), so we can put them equal to their minimum (zero) obtaining a majorization:

$$\begin{aligned}\xi &\geq \frac{1}{2}\left[1 - FF' - D\cos y - D'\cos y' + DD'\cos y\cos y'\right] \\ &= \frac{1}{2}\left[\left(1 - D\cos y\right)\left(1 - D'\cos y'\right) - \left(1-D\right)\left(1-D'\right)\right] \\ &\geq \frac{1}{2}\left[\left(1-D\right)\left(1-D'\right) - \left(1-D\right)\left(1-D'\right)\right] = 0\end{aligned} \tag{5.28}$$

This implies that d is a minimum for P_d. We notice that it is possible to obtain d by setting in P_d

$$F = F' = 1. \tag{5.29}$$

This condition represents the best Eve can do to conceal her presence. We also notice that the maximum value $d = 3/8$ is obtained when $x = x' = \pi/2$, corresponding, as we will see, to a maximum for $\mathcal{I}_{AE}$.

In order to evaluate $\mathcal{I}_{AE}$ let us write Bob's initial states as:

$$\left|\Psi\right\rangle = \sum_{\alpha=0,1} C_\alpha \left|\alpha\right\rangle \tag{5.30}$$

where we made the following ansatzs correspondingly to the initial states:

$$\begin{aligned}\left|0\right\rangle &\rightarrow C_\alpha = \delta_{\alpha,0} \\ \left|1\right\rangle &\rightarrow C_\alpha = \delta_{\alpha,1} \\ \left|+\right\rangle &\rightarrow C_\alpha = \frac{1}{\sqrt{2}} \\ \left|-\right\rangle &\rightarrow C_\alpha = \left(-1\right)^\alpha \frac{1}{\sqrt{2}}\end{aligned}$$

Now we can rewrite transformations (5.9-5.12) as:

$$\left|\Psi\right\rangle\left|\varepsilon\right\rangle = \sum_{\alpha=0,1} C_\alpha \left|\alpha\right\rangle\left|\varepsilon\right\rangle \rightarrow \sum_\alpha C_\alpha \sum_\beta \left|\varepsilon_{\alpha\beta}\right\rangle\left|\beta\right\rangle$$

The second transformations (5.17-5.19) can be rewritten as:

$$\left|\Psi\right\rangle\left|\eta\right\rangle = \sum_{\alpha=0,1} C_\alpha \left|\alpha\right\rangle\left|\eta\right\rangle \rightarrow \sum_\alpha C_\alpha \sum_\beta \left|\eta_{\alpha\beta}\right\rangle\left|\beta\right\rangle$$

Now suppose Alice performs the identity $\mathbb{1}$ between the two Eve's attacks. The following sequence of algebraic operations describes the temporal sequence of operations:

$$\begin{aligned}|\Psi\rangle|\varepsilon\rangle|\eta\rangle \xrightarrow{E_1} \sum_\alpha C_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{\mathbb{1}} \\ \xrightarrow{\mathbb{1}} \sum_\alpha C_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{E_2} \sum_\alpha C_\alpha \sum_{\beta,\gamma} |\gamma\rangle|\varepsilon_{\alpha\beta}\rangle|\eta_{\beta\gamma}\rangle\,. \end{aligned} \tag{5.31}$$

The ancillary states involved in this operation are:

$$\begin{aligned}&|\varepsilon_{00},\eta_{00}\rangle, |\varepsilon_{00},\eta_{01}\rangle, |\varepsilon_{01},\eta_{10}\rangle, |\varepsilon_{01},\eta_{11}\rangle \\ &|\varepsilon_{10},\eta_{00}\rangle, |\varepsilon_{10},\eta_{01}\rangle, |\varepsilon_{11},\eta_{10}\rangle, |\varepsilon_{11},\eta_{11}\rangle\,. \end{aligned} \tag{5.32}$$

If, instead, Alice performs a flip iY we have:

$$\begin{aligned}|\Psi\rangle|\varepsilon\rangle|\eta\rangle \xrightarrow{E_1} \sum_\alpha C_\alpha \sum_\beta |\beta\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{iY} \\ \xrightarrow{iY} \sum_\alpha C_\alpha \sum_\beta (-1)^{\beta+1}|\beta\oplus 1\rangle|\varepsilon_{\alpha\beta}\rangle|\eta\rangle \xrightarrow{E_2} \\ \xrightarrow{E_2} \sum_\alpha C_\alpha \sum_{\beta,\gamma} (-1)^{\beta+1}|\gamma\rangle|\varepsilon_{\alpha\beta}\rangle\left|\eta_{(\beta\oplus1)\gamma}\right\rangle, \end{aligned} \tag{5.33}$$

and the involved ancillary states are:

$$\begin{aligned}&|\varepsilon_{00},\eta_{10}\rangle, |\varepsilon_{00},\eta_{11}\rangle, |\varepsilon_{01},\eta_{00}\rangle, |\varepsilon_{01},\eta_{01}\rangle \\ &|\varepsilon_{10},\eta_{10}\rangle, |\varepsilon_{10},\eta_{11}\rangle, |\varepsilon_{11},\eta_{00}\rangle, |\varepsilon_{11},\eta_{01}\rangle\,. \end{aligned} \tag{5.34}$$

In order to acquire information from states (5.31) and (5.33) Eve must measure both her ancillae. Keeping in mind orthogonality relations (5.15) and following, we see that the best way to do that is to distinguish orthogonal subspaces before, and then non-orthogonal states within them. The probability to correctly distinguish between two states with scalar product $\cos x$ is $(1+\sin x)/2$ [67]. Observing states (5.31) and (5.33) we can notice that if Eve mistakes to identify her first ancilla (ε states) then she guesses the wrong Alice's operation, since she flips from states (5.31) and (5.33) or viceversa. The same is true if she guesses right ε state but mistakes η state. Nevertheless, if she mistakes twice, then with the first error she misinterprets (5.31) and (5.33) and with the second error she compensates the first, eventually guessing right Alice's operation. This leads to estimate the probability Eve correctly guesses Alice's operation, and from it we find the following expression for $\mathcal{I}_{AE}$:

$$\begin{aligned}\mathcal{I}_{AE} = FF'\left\{1-H\left[\left(\frac{1+\sin x}{2}\right)\left(\frac{1+\sin x'}{2}\right)+\left(\frac{1-\sin x}{2}\right)\left(\frac{1-\sin x'}{2}\right)\right]\right\}+ \\ + FD'\left\{1-H\left[\left(\frac{1+\sin x}{2}\right)\left(\frac{1+\sin y'}{2}\right)+\left(\frac{1-\sin x}{2}\right)\left(\frac{1-\sin y'}{2}\right)\right]\right\}+ \\ + DF'\left\{1-H\left[\left(\frac{1+\sin y}{2}\right)\left(\frac{1+\sin x'}{2}\right)+\left(\frac{1-\sin y}{2}\right)\left(\frac{1-\sin x'}{2}\right)\right]\right\}+ \\ + DD'\left\{1-H\left[\left(\frac{1+\sin y}{2}\right)\left(\frac{1+\sin y'}{2}\right)+\left(\frac{1-\sin y}{2}\right)\left(\frac{1-\sin y'}{2}\right)\right]\right\}. \end{aligned} \tag{5.35}$$

where $H(\cdot)$ indicates the Shannon binary entropy (see [25] and Sec.3.1). $\mathcal{I}_{AE}$ results then to be a function of the six parameters describing relations among ancillae states, but it can be simplified recalling that Eve wants to keep the detection probability P_d as low as possible, and so condition (5.29) applies. In this case Eve's strategy is optimal and $\mathcal{I}_{AE}$ becomes a function of only two real parameters containing the whole information about ancillae's orthogonality:

$$\mathcal{I}_{AE} = 1 - H\left(\frac{1 + \sin x \sin x'}{2}\right) \tag{5.36}$$

We are now in the position to compare relevant quantities we have calculated, in particular Eq.(5.26) for d and Eq.(5.36) for $\mathcal{I}_{AE}$. Unfortunately, both equations are functions of x and x' thus preventing us to write $\mathcal{I}_{AE}$ as a function of d. However, the following lemma holds:

Lemma. The optimal non-orthogonal attack consists in a *BALANCED* one for which $x = x'$.

This lemma has been numerically verified for several values of d up to the fourth digit. However it can be intuitively justified with the following qualitative argument. The orthogonality Eve imposes on her ancillae is somewhat related to the information she can extract from the qubit: the more orthogonal they are, the higher is the information gained. If she sets $x > x'$, the ancillae ε will be more orthogonal than ancillae η, and this entails a loss of information when going from the forward to the backward path. If she sets $x < x'$ we can argue the reverse.

The above lemma allows us to write d (5.26) as:

$$d = (1/2) - (1/8)\,(1 + \cos x)^2 \tag{5.37}$$

and $\mathcal{I}_{AE}$ as:

$$\mathcal{I}_{AE} = 1 - H\left(\frac{1 + \sin^2 x}{2}\right). \tag{5.38}$$

By inverting relation (5.37) we obtain two solution, only the following real:

$$x = \arccos\left(-1 + 2\sqrt{(1 - 2d)}\right). \tag{5.39}$$

Substituting x into Eq.(5.36) we can express the information $\mathcal{I}_{AE}$ as function of d:

$$\mathcal{I}_{AE} = 1 - H\left[\frac{2 - (2\sqrt{1 - 2d} - 1)^2}{2}\right] \tag{5.40}$$

It is easy to see that the maximum of information, $\mathcal{I}_{AE} = 1$, corresponds to a detection probability $d = 3/8 = 37.5\%$. This implies that projective attacks described above are in a certain sense optimal within the group of attacks including a double measurement. The dependance of $\mathcal{I}_{AE}$ from d is shown in Fig.5.4.

Now we know how much information is shared between Alice and Eve. We ask then how much information remained to Bob. The rationale to answer this question is contained in Alice and Bob's mutual information $\mathcal{I}_{AB}$. To find out this quantity we can still exploit condition (5.29), because Bob receives a perturbed state according to Eve's choice of minimizing P_d. This is a very important point since, as we will see, Eve's attempt to gain information causing a small disturbance makes her leave a sensible residue of information in $\mathcal{I}_{AB}$, and Alice and Bob are grateful for that. So, with this condition, and omitting lengthy calculations very similar to those reported above, we

have that the probability Bob makes a right guess on Alice's transformation after preparing $|+\rangle$ or $|-\rangle$, and Eve measures in the basis $|\varepsilon_{0,1}\rangle, |\eta_{0,1}\rangle$, is

$$P_{0,1} = \left(\frac{1+\cos x \cos x'}{2}\right). \tag{5.41}$$

The probability that Bob makes a right guess on Alice's transformation, after preparing the same states and Eve measures in the basis $|\varepsilon_{+,-}\rangle, |\eta_{+,-}\rangle$ is

$$P_{+,-} = 1 \tag{5.42}$$

because in this case Eve does not perturb the state at all. Analogous results hold if Bob prepares states $|0\rangle$ or $|1\rangle$. Averaging the information corresponding to $P_{0,1}$ and to $P_{+,-}$, using the above *Lemma* to pass to a single variable expression, and using Eq.(5.39) we get:

$$\mathcal{I}_{AB} = 1 - \frac{1}{2}H\left[\frac{\left(1+\cos^2 x\right)}{2}\right] \tag{5.43}$$

$$= 1 - \frac{1}{2}H\left[\frac{1+(2\sqrt{1-2d}-1)^2}{2}\right]. \tag{5.44}$$

This result is plotted in Fig.5.4 together with $\mathcal{I}_{AE}$. We notice that minimum Bob's information is 1/2, because in half cases Eve doesn't perturb the channel at all. Nevertheless, if we had used symmetry conditions discussed after Eq.(5.16) we would have obtained $\mathcal{I}_{AE}$ going to zero. The intersection of $\mathcal{I}_{AB}$ and $\mathcal{I}_{AE}$ is approximately at $d \simeq 0.23$.

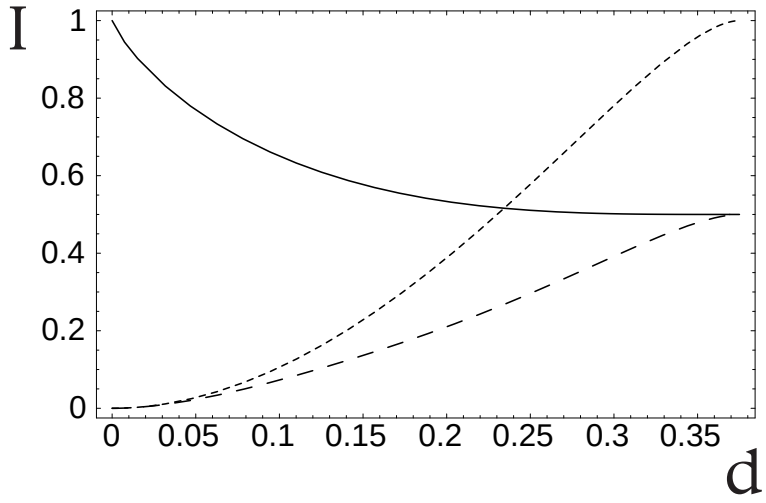

Figure 5.4: PP84 Security: mutual informations vs detection probability in non-orthogonal attacks. The descent curve represents Alice and Bob mutual information $\mathcal{I}_{AB}$. The crescent curves are Alice-Eve mutual information $\mathcal{I}_{AE}$ (dotted line) and Bob-Eve mutual information $\mathcal{I}_{BE}$ (dashed line)

The last question we ask is about the mutual information between Bob and Eve. We can make use of classical probability rules to calculate it. The probability Eve guesses Bob's result and

viceversa is given by the probability that both guess Alice's operation plus the probability that both mistakes it:

$$P^{BE}_{right} = \left(P^{BA}_{right} \cdot P^{EA}_{right}\right) + \left(P^{BA}_{wrong} \cdot P^{EA}_{wrong}\right). \tag{5.45}$$

P^{EA}_{right} is given by the argument of the Shannon entropy in (5.38) i.e.

$$P^{EA}_{right} = \left(\frac{1+\sin^2 x}{2}\right).$$

P^{BA}_{right} depends on Eve's ancillae basis choice, and can be given either by (5.41) or by (5.42). Of course the probabilities of wrong choices follow from the complement of those for the right choice. Rewriting (5.45) considering Eve's choice about the basis x or z we obtain:

$$\begin{aligned} P^{BE}_{right}(x) &= \left(\frac{1+\cos^2 x}{2}\right)\left(\frac{1+\sin^2 x}{2}\right) + \left(\frac{1-\cos^2 x}{2}\right)\left(\frac{1-\sin^2 x}{2}\right) \\ &= \frac{1}{2}\left(1+\frac{\sin^2 2x}{4}\right) \\ P^{BE}_{right}(z) &= 1\left(\frac{1+\sin^2 x}{2}\right) + 0\left(\frac{1-\sin^2 x}{2}\right) = \frac{1}{2}\left(1+\sin^2 x\right). \end{aligned}$$

We can now find the corresponding informations and average them to obtain:

$$\mathcal{I}_{BE} = \frac{1}{2}\left\{2 - H\left[\frac{1}{2}\left(1+\frac{\sin^2 2x}{4}\right)\right] - H\left[\frac{1}{2}\left(1+\sin^2 x\right)\right]\right\}.$$

Also this function can be inverted by means of Eq.(5.39) and reported, as a function of d, in Fig.5.4. It is apparent that the condition $\mathcal{I}_{AB} \geq \mathcal{I}_{BE}$ is fullfilled for every value of d, i.e. Alice and Bob can always establish a secret key, *regardless of the noise in the channel*. This is resembling of what happens with *reverse reconciliation* in continuous variables [78]. On the contrary $\mathcal{I}_{AB} \geq \mathcal{I}_{AE}$ when $d \lesssim 23\%$. Yet, the analysis of $\mathcal{I}_{AE}$ can still be useful to upper-bound Eve's information when a *general individual attack* is undertook. In this case it turns out that the communication is secure until $d \lesssim 18\%$. We notice that the maxima of $\mathcal{I}_{AE}$ and $\mathcal{I}_{BE}$ correspond to a detection probability of $37.5\% = 3/8$, which is the least disturbance Eve can introduce on the channel when she eavesdrops a full amount of information.

Double-CNOT attack

Let us study the evolution of the states prepared by Bob under the action of a double CNOT gate by Eve.

Eve appends an ancilla in the state $|0\rangle_e$ to the initial states (5.3), and then performs a first CNOT gate before Alice's station. The states become:

$$\begin{aligned} |0\rangle_b |0\rangle_e &\xrightarrow{CNOT} |0\rangle_b |0\rangle_e \\ |1\rangle_b |0\rangle_e &\xrightarrow{CNOT} |1\rangle_b |1\rangle_e \\ |+\rangle_b |0\rangle_e &\xrightarrow{CNOT} \frac{|0\rangle_b |0\rangle_e + |1\rangle_b |1\rangle_e}{\sqrt{2}} \\ |-\rangle_b |0\rangle_e &\xrightarrow{CNOT} \frac{|0\rangle_b |0\rangle_e - |1\rangle_b |1\rangle_e}{\sqrt{2}}. \end{aligned} \tag{5.46}$$

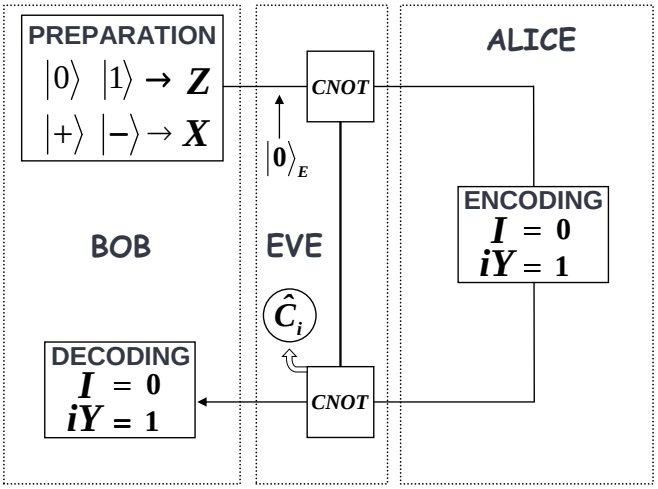

Figure 5.5: The CNOT strategy

We can notice that when Bob prepares states in the basis $\hat{S}_x$ the CNOT gate creates an entangled state with the travelling qubit and Eve's ancilla. After that Eve forwards the qubit indicated with subscript 'b' (for 'Bob') to Alice, who performs her encoding $\hat{C}_i$ on it and, after that, sends it back to Bob. Eve, on the backward path, executes a second CNOT gate on the whole system. We report Alice's and Eve's actions as:

$$
\begin{aligned}
&|0\rangle|0\rangle_e \xrightarrow{\hat{C}_i} \left(\hat{C}_i|0\rangle\right)|0\rangle_e \xrightarrow{CNOT} \left(\hat{C}_i|0\rangle\right)|i\rangle_e \\
&|1\rangle|1\rangle_e \xrightarrow{\hat{C}_i} \left(\hat{C}_i|1\rangle\right)|1\rangle_e \xrightarrow{CNOT} \left(\hat{C}_i|1\rangle\right)|i\rangle_e \\
&\frac{|0\rangle|0\rangle_e + |1\rangle|1\rangle_e}{\sqrt{2}} \xrightarrow{\hat{C}_i} \frac{\left(\hat{C}_i|0\rangle\right)|0\rangle_e + \left(\hat{C}_i|1\rangle\right)|1\rangle_e}{\sqrt{2}} \xrightarrow{CNOT} \left(\hat{C}_i|+\rangle\right)|i\rangle_e \\
&\frac{|0\rangle|0\rangle_e - |1\rangle|1\rangle_e}{\sqrt{2}} \xrightarrow{\hat{C}_i} \frac{\left(\hat{C}_i|0\rangle\right)|0\rangle_e - \left(\hat{C}_i|1\rangle\right)|1\rangle_e}{\sqrt{2}} \xrightarrow{CNOT} -\left(\hat{C}_i|-\rangle\right)|i\rangle_e
\end{aligned}
\tag{5.47}
$$

Writing explicitly transformations (5.47) we can recognize that entanglement created in the first step disappears in the second step:

$$
\begin{aligned}
&\mathbb{1}|0\rangle|0\rangle_e \xrightarrow{CNOT} |0\rangle|0\rangle_e \qquad iY|0\rangle|0\rangle_e \xrightarrow{CNOT} |1\rangle|1\rangle_e \\
&\mathbb{1}|1\rangle|1\rangle_e \xrightarrow{CNOT} |1\rangle|0\rangle_e \qquad iY|1\rangle|1\rangle_e \xrightarrow{CNOT} |0\rangle|1\rangle_e \\
&\mathbb{1}\frac{|0\rangle|0\rangle_e+|1\rangle|1\rangle_e}{\sqrt{2}} \xrightarrow{CNOT} |+\rangle|0\rangle_e \qquad iY\frac{|0\rangle|0\rangle_e+|1\rangle|1\rangle_e}{\sqrt{2}} \xrightarrow{CNOT} |-\rangle|1\rangle_e \\
&\mathbb{1}\frac{|0\rangle|0\rangle_e-|1\rangle|1\rangle_e}{\sqrt{2}} \xrightarrow{CNOT} |-\rangle|0\rangle_e \qquad iY\frac{|0\rangle|0\rangle_e+|1\rangle|1\rangle_e}{\sqrt{2}} \xrightarrow{CNOT} -|+\rangle|1\rangle_e .
\end{aligned}
\tag{5.48}
$$

For Eve is sufficient to measure her ancilla in the basis $\hat{S}_z$ to find out Alice's encoding since the subscript of $\hat{C}_i$, containing the information by Alice, has been transferred to the ancilla state: $|0\rangle_e$ indicates Alice performed the identity while $|1\rangle_e$ indicates the spin-flip operation. Moreover, from

Eqs.(5.48) is apparent that after the second CNOT, the state arriving to Bob is just the right state Alice expected him to receive! This entails that if they were going to use only a *message authentication* as a security strategy, they would never detect this kind of attack by Eve. This is the reason why a control on the single line is necessary too.

With the control mode envisaged before Alice and Bob can reveal Eve. From Eqs.(5.46) we can see that if the qubit is prepared in the basis $\hat{S}_z$ Eve does not perturb the state at all; hence in this case

$$d_1^z = 0,$$

where z indicate the preparation basis and d_1^z is detection probability on the forward line. Instead, when the qubit is prepared in the basis $\hat{S}_x$ Eve's ancilla gets entangled with it, and can be revealed:

$$d_1^x = \frac{1}{2}.$$

Of course the preparation basis and the basis chosen by Eve to perform the CNOT gate are arbitrary, and the argument on the "labels" z and x can be totally reversed.

The argument for the backward path is slightly more complex. In control mode Alice measures the incoming state in the same basis as Bob prepared it (in the other case the run is rejected), projecting out (and thus preparing) a single particle state from those in Eqs.(5.46); then she sends on the backward path this new state. This entails that during control mode the second CNOT executed by Eve does not have the same effect as in message mode, described by Eqs. (5.47) and (5.48), but rather an effect similar to the first CNOT, because the control qubit (that prepared by Alice) and the target qubit (Eve's ancilla) have been disentangled by Alice's projective measurement. Thus we can at once affirm that:

$$\begin{aligned} d_2^z &= 0 \Rightarrow d^z = 0 \\ d_2^x &= \frac{1}{2} \Rightarrow d^x = \frac{3}{4}, \end{aligned}$$

where $d_2^{z,x}$ is the detection probability on the backward line and $d^{z,x}$ is the probability to detect Eve *either* on one path *or* on the other. Thus the average detection probability for CNOT attack results to be:

$$\overline{d} = \frac{3}{8},$$

as in *measure-and-resend* attacks.

Lossy channel

Losses are very dangerous to PP84 and to two-ways protocols in general, as we saw studying Ping-Pong and Cai-Li protocols. The reason is that the forward and backward paths are suitable to represent the two arms of a Mach-Zender interferometer built by Eve to eavesdrop information (see Fig.5.6). This sort of device reveals powerful because conceals its presence behind losses. Under normal conditions losses are due to imperfect channels or to ineffective apparatuses of measure. Alice and Bob can thus attribute them to natural problems related to the communication. Instead Eve, endowed with a perfect technology, can substitute these inefficient means with her hyper-fine ones, and let her strategy cause losses without being revealed. Let us envisage an Eve's general attack based on losses.

In the following we indicate as $\left\{ |1\rangle_{\uparrow b}, |1\rangle_{\downarrow b} \right\}$ respectively the states $\{|\uparrow\rangle_b, |\downarrow\rangle_b\}$ of the qubit prepared by Bob and traveling towards Alice and back; $|0\rangle_b$, eventually with a subscript containing

the polarization-arrow, is the vacuum state. The labels "b" nd "e" stand for states prepared by Bob and Eve.

The most general transformation Eve can do hiding herself behind losses, and supposing Bob never sends out the vacuum state, is:

$$\begin{aligned} E\left|1\right\rangle_{\uparrow b}\left|A\right\rangle_{e} &= \alpha\left|1\right\rangle_{\uparrow b}\left|A\right\rangle_{e} + \beta\left|0\right\rangle_{\uparrow b}\left|B\right\rangle_{e} \\ E\left|1\right\rangle_{\downarrow b}\left|A\right\rangle_{e} &= \gamma\left|1\right\rangle_{\downarrow b}\left|C\right\rangle_{e} + \delta\left|0\right\rangle_{\downarrow b}\left|D\right\rangle_{e}, \end{aligned} \tag{5.49}$$

where we can assume ancillary states to be mutually orthogonal in a Hilbert space of arbitrary dimension. We notice that Eve's intervention does not change polarization of the traveling photon. This means that during control mode Alice and Bob can find the vacuum state but they can not find uncorrelated results: the disturbance consists in losses rather than in noise.

From Eq.(5.49) we obtain by linearity the disturbance Eve creates when Bob prepares X eigenstates:

$$\begin{aligned} E\left|1\right\rangle_{\rightarrow b}\left|A\right\rangle_{e} &= \frac{1}{\sqrt{2}}\left[\left|1\right\rangle_{\rightarrow b}\left(\frac{\gamma\left|C\right\rangle_{e} + \alpha\left|A\right\rangle_{e}}{\sqrt{2}}\right) + \left|1\right\rangle_{\leftarrow b}\left(\frac{\gamma\left|C\right\rangle_{e} - \alpha\left|A\right\rangle_{e}}{\sqrt{2}}\right) + \right. \\ &+ \left. \beta\left|0\right\rangle_{\uparrow b}\left|B\right\rangle_{e} + \delta\left|0\right\rangle_{\downarrow b}\left|D\right\rangle_{e}\right] \end{aligned} \tag{5.50}$$

In this basis things are slightly different: the second term in squared brackets leads Eve to be detected with probability $\frac{1}{4}\left(\left|\gamma\right|^2 + \left|\alpha\right|^2\right)$ by Alice and Bob's control mode, because she changes the polarization of the state. This is true because control mode is performed in a symmetric fashion, with a *random* measure along either axis X or Z. The third and fourth terms are not revealed by Alice and Bob because they represent the vacuum. If Eve wants to hide herself also in this case she must put

$$\alpha\left|A\right\rangle_{e} = \gamma\left|C\right\rangle_{e}. \tag{5.51}$$

In this way the new transformations are:

$$\begin{aligned} E'\left|1\right\rangle_{\uparrow b}\left|A\right\rangle_{e} &= \alpha\left|1\right\rangle_{\uparrow b}\left|A\right\rangle_{e} + \beta\left|0\right\rangle_{\uparrow b}\left|B\right\rangle_{e} \\ E'\left|1\right\rangle_{\downarrow b}\left|A\right\rangle_{e} &= \alpha\left|1\right\rangle_{\downarrow b}\left|A\right\rangle_{e} + \beta\left|0\right\rangle_{\downarrow b}\left|D\right\rangle_{e} \\ E'\left|1\right\rangle_{\rightarrow b}\left|A\right\rangle_{e} &= \alpha\left|1\right\rangle_{\rightarrow b}\left|A\right\rangle_{e} + \beta\left(\frac{\left|0\right\rangle_{\downarrow b}\left|D\right\rangle_{e} + \left|0\right\rangle_{\uparrow b}\left|B\right\rangle_{e}}{\sqrt{2}}\right) \\ E'\left|1\right\rangle_{\leftarrow b}\left|A\right\rangle_{e} &= \alpha\left|1\right\rangle_{\leftarrow b}\left|A\right\rangle_{e} - \beta\left(\frac{\left|0\right\rangle_{\downarrow b}\left|D\right\rangle_{e} - \left|0\right\rangle_{\uparrow b}\left|B\right\rangle_{e}}{\sqrt{2}}\right) \end{aligned} \tag{5.52}$$

where we have also explicitly reported what happens to the state $\left|1\right\rangle_{\leftarrow b}$, and we have used the identity $\left|\alpha\right|^2 + \left|\beta\right|^2 = \left|\alpha\right|^2 + \left|\delta\right|^2$ (orthonormal states) together with reality of coefficients. We notice that if the symmetry request is not fulfilled then Eve must not be afraid to be revealed since, for instance, Alice and Bob never measure along X; hence the condition (5.51) must not be satisfied. This underlines once again the importance of *symmetry* in preparation and control when dealing with losses. What comes out from calculations is that if Eve remains hidden behind losses then the state $\left|A\right\rangle_{e}$ takes no information at all because it is equal for all the four states. The information about the traveling qubit is transferred to the ancillae related to the vacuum state, and can not be used by Eve with a second attack analogous to Eq.(5.52) performed by means of fresh ancillae. To clarify this point we write below the states after such a strategy by Eve, restricting ourselves to the case in which Bob prepares states in the Z basis; the X basis is analogous. After

Eve's first attack and Alice encoding, the state $|1\rangle_{\uparrow b}$ becomes:

$$\begin{array}{l}\alpha\,|1\rangle_{\uparrow b}\,|A\rangle_e+\beta\,|0\rangle_{\uparrow b}\,|B\rangle_e \quad \text{if Alice performed } \mathbb{1}\\ -\alpha\,|1\rangle_{\downarrow b}\,|A\rangle_e-\beta\,|0\rangle_{\downarrow b}\,|B\rangle_e \quad \text{if Alice performed } iY.\end{array}$$

After Eve's second attack (indicated with primed letters) with fresh ancillae it becomes:

$$\alpha\alpha'\,|1\rangle_{\uparrow b}\,|A\rangle_e\,|A'\rangle_e+|0\rangle_{\uparrow b}\,(\alpha\beta'\,|A\rangle_e\,|B'\rangle_e+\beta\,|B\rangle_e\,|A'\rangle_e) \quad \text{if Alice performed } \mathbb{1} \tag{5.53}$$

$$-\alpha\alpha'\,|1\rangle_{\downarrow b}\,|A\rangle_e\,|A'\rangle_e-|0\rangle_{\downarrow b}\,(\alpha\beta'\,|A\rangle_e\,|D'\rangle_e-\beta\,|B\rangle_e\,|A'\rangle_e) \quad \text{if Alice performed } iY \tag{5.54}$$

By the same token when Bob prepares the state $|1\rangle_{\downarrow b}$ we obtain:

$$\alpha\alpha'\,|1\rangle_{\downarrow b}\,|A\rangle_e\,|A'\rangle_e+|0\rangle_{\downarrow b}\,(\alpha\beta'\,|A\rangle_e\,|D'\rangle_e+\beta\,|D\rangle_e\,|A'\rangle_e) \tag{5.55}$$

$$\alpha\alpha'\,|1\rangle_{\uparrow b}\,|A\rangle_e\,|A'\rangle_e+|0\rangle_{\uparrow b}\,(\alpha\beta'\,|A\rangle_e\,|B'\rangle_e+\beta\,|D\rangle_e\,|A'\rangle_e) \tag{5.56}$$

It is evident from above equations that Eve can not distinguish between Alice operations by measuring her ancillae. We must then conclude that the only way to extrapolate information from Eqs.(5.52), where the vacuum is involved, is by means of an interferometric pattern.

INTERFEROMETRIC SCHEME

We describe the attack with reference to Fig.5.6, considering only $50 \div 50$ beam-splitters for simplicity; the argument can be complicated at will by adjusting coefficients of reflection and transmission of the beam-splitters involved.

At point E_1 Eve intercepts the qubit with the first beam-splitter ($\mathbf{BS}_1$), and at point E_2 she put a second beam-splitter ($\mathbf{BS}_2$) to realize a Mach-Zender interferometer (**M-Z**). In order to calibrate perfectly the interferometer Eve put also a delay line between $\mathbf{BS}_1$ and $\mathbf{BS}_2$, so that the two arms of the **M-Z** result of equal length.

Now suppose Alice is going to perform the identity operation on the state she receives. The state of the qubit remains the same and when it reaches $\mathbf{BS}_2$ a temporal inversion of the transformation occurred at $\mathbf{BS}_1$ comes about on the state; this entails that the photon will certainly escape $\mathbf{BS}_2$ on the path 'b'. On the contrary, when Alice performs the flip operation on the state she changes the polarization, and interference does not occur anymore at $\mathbf{BS}_2$; this means that the photon can escape $\mathbf{BS}_2$ both on path 'a' and on path 'b'. Then it is straightforward that when Eve detects a photon on path 'a' she can infer with certainty that Alice carried out a flip operation on the qubit. We remark that the above photo-detection can be made by Eve without destroying the state. After her guess, Eve forwards the state to Bob by recollecting the two paths 'a' and 'b' into $\mathbf{BS}_3$. This operation can be made perfect by means of an optical fiber circulator. Eve adds some "artificial losses" to the backward path in order to make the transmittance equal to that of the line going from Bob to Alice; else, the legitimate users could notice a suspicious difference. As a matter of fact , $\mathbf{BS}_3$ plays exactly this role: in fact the losses on the forward channel are determined by $\mathbf{BS}_1$, and amount to 50%, and the same is true for $\mathbf{BS}_3$ on the backward path.

It is not a difficult task to determine Eve's information. When the photon is on path 'a' then Eve knows the information is 1 (Alice made iY) with certainty. When the photon is revealed on path 'b' then, by using Bayes theorem, we can establish that with probability 1/3 information is 1, and with probability 2/3 information is 0. Then Eve will guess that information in the former case is 1, while it is 0 in the latter case. Only in the second case she will commit an error with

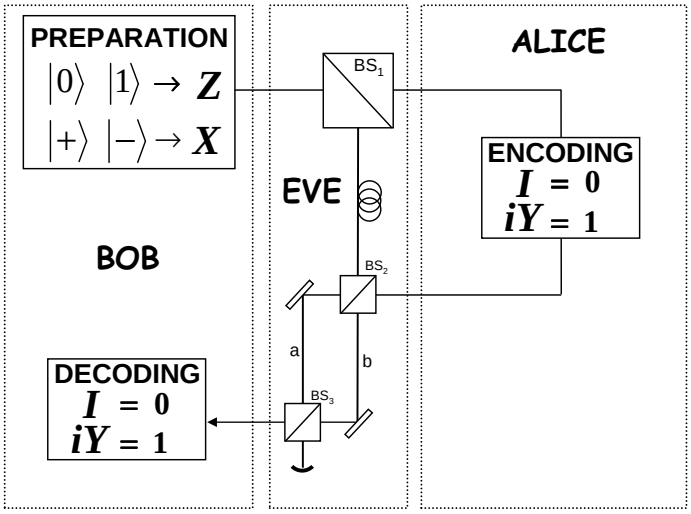

Figure 5.6: Interferometric scheme Eve uses to eavesdrop information by means of a losses-based attack. Note the two ideal Mach-Zender interferometers arranged by Eve by means of beam-splitters and delay lines.

probability $P_{wrong} = 1/3$. So the information is the average between the two cases and amounts to:

$$\begin{aligned} \overline{I}_{AE} &= \frac{1}{2}\left(I_{AE}^{(1)} + I_{AE}^{(0)}\right) \\ &\simeq \frac{1}{2}\left(1 + 0.08\right) = 0.54. \end{aligned}$$

Now the question is whether Alice and Bob can detect this strategy somehow. It turns out that PP84 is already secure against this kind of attack, but it can be further improved.

The first thing to notice is that the usual control can not be used to detect Eve, since results remain always correlated in polarization. In fact beam-splitters can not change the qubit polarization. Nevertheless the following scenario could occur: Alice in control mode detects no photon (vacuum state); so she forwards no photon to Bob. Nonetheless the photon is traveling through Eve's arm of the **M-Z**, and has a probability of 50% to reach Bob. If this happen Alice and Bob detect Eve because it is impossible that a photon reaches Bob's station and not Alice's, if an eavesdropper is not in the line. This scenario verifies in 1/4 of the control runs, hence it allows to detect Eve with a 25% probability.

This is the only protection strategy the two legitimate parties can use in PP84. However it can be improved by adding security procedures.

As a first additional protection procedure we mention the *message authentication* already described above. During the message mode it happens that when Alice performs identity Bob receives the correct state with certainty. On the contrary when Alice performs the flip Bob can receive a wrong state. In particular each time a flipped photon arrives at Bob's site it is wrong with probability 1/2. This entails that the average mutual information $\overline{I}_{AB}$ between Alice and Bob amounts to

$$\overline{I}_{AB} = \frac{1}{2}\left(1 + 0\right) = 0.50$$

i.e. it is less than $\overline{I}_{AE}$. And it can be further decreased by Eve by means of a DoS attack (see Sec.4.2.1). As we will see, this is a dangerous situation for the users, because Eve has more information than they have, thus preventing them from sharing a secure key by means of one-way protocols [4]. However, every time $\overline{I}_{AB} \neq 1$ the *message authentication* procedure results effective. By revealing a part of the encoded operations Alice and Bob find out an anticorrelation of results, i.e. an evidence of Eve's presence, 1/4 of the times, as for the previous strategy. It could be objected that Alice should reveal only a part of the iY encoding operations, because only the flipped qubits can result in an error. Yet this is not true; symmetry of the revelation is important, because Eve could put a polarization rotator in the middle of her arm of **M-Z**, and reversing all the argument above, making the identity the only operation to cause an error.

As a final protection strategy we consider a physical solution: the *phase randomization*. Eve aims at stealing information by means of an interferometer. Then Alice could simply add, beside the encoding operation on qubit's polarization, a random phase $\varphi^{\mathrm{RANDOM}}$ in her arm. In this way the interference at $\mathbf{BS}_2$ would become random too, and would not be informative for Eve anymore. Nevertheless Bob would decode Alice's sequence without problems, as his decoding is polarization-based. This strategy has the advantage that no qubit must be sacrificed to implement it. It immediately implies that $\overline{I}_{AE} = \overline{I}_{AB} = 0$, that is Eve acquires no information, and is detected with probability 1/2 by means of a *message authentication* stage.

5.2.2 Variants and implementation

Hyper-secure PP84

During the discussion about eavesdropping we encountered several types of attacks with related solutions to them. Now we want to gather all the described security procedures, in order to design a more reliable version of PP84.

i) Symmetry condition. We remarked the importance of symmetry in the preparation of the initial states by Bob and during the control procedure in order to guarantee security. The original version of PP84 already accomplish this requirement: it establishes that Alice must, with a certain probability $c_{xz} = c - c_{enc}$, measure the traveling qubit in one of the two bases $\hat{S}_x$ or $\hat{S}_z$, chosen randomly. c is the total probability to perform a control run.

ii) Message authentication. Alice must, in analogy with BB84, reveal a part of the encoding in order to verify the quality of Bob's information. So with probability c_{enc}, she performs some random operations $\hat{C}_i$ on the qubit and sends it back to Bob. Bob's measurement does not change. Afterwords, either run-by-run or at the end of the transmission, a public discussion is settled from which Alice and Bob are able to estimate Bob's error rate, i.e. the QBER Q. Hence they can value their mutual information I_{AB}, that is a function of the only parameter Q. In turn, Q is of course related to detection probabilities d_1 and d_2 along the lines B-A and A-B, but this connection is in most cases far from simple. We will return on this argument in the section devoted to unconditional security.

iii) Phase randomization. Alice must, together with her encoding procedure, change randomly the phase of the travelling qubit. Bob's measurement does not change. This prevents attacks based on losses.

We stress that all the security operations described above can be accomplished at the end of the whole transmission because entanglement is not involved in the protocol. In this way Alice's decision does not influence Bob's decoding operation.

Completely-deterministic PP84

Thus far we have been dealing with a PP84 control procedure that results effective only when Alice guesses the basis used by Bob to prepare the initial states; this happens about one half of the times Alice decides for a control mode. This entails that one half of the control qubits are discarded because of a wrong choice of the bases. We propose here a variant of PP84 that can make deterministic also the control procedure beside the message one. This feature determines a higher total transmission rate; the price is a lower security of the communication.

In PP84's control mode Alice measures the traveling qubit in one of the two bases X or Z, chosen randomly. Then she forwards the projected qubit to Bob without further modifying it. The qubit arrives to Bob in the same basis Alice measured it in. Bob measures the qubit in the same basis he prepared it in.

Rather than follow this procedure Alice can forward the qubit to Bob after making a rotation of $\frac{\pi}{2}$ to the qubit itself around $\hat{y}$ axis. This can be achieved by an operator $e^{i\frac{\pi}{2}Y}$, and causes a change of basis of the qubit. In this way it is secure that Alice and Bob's bases coincide either on the forward path or on the backward one. This feature makes the protocol completely deterministic, both in its message mode and in its control mode. However, the control mode is less effective in this scheme, because it works only the path for which the bases coincide. As an example, the detection probability $d = 3/8$ against the CNOT attack obtained in Sec.5.2.1, is decreased to the value of $1/4$.

Phase-encoded PP84

There are already different working realizations of BB84 [4]. Some of them exploit entanglement in polarization to encode a random string of bits in two unbiased polarization bases of a single photon, thus following the original proposal. These implementations adopt optical fibers as quantum channels for photons' states. However, polarization is not the most suitable degree of freedom for communication with fibers, because birefringence usually fluctuates randomly in a fiber, making the encoded information impossible to decode. The most appealing setup for real telecom communications is based on the phase degree of freedom.

As an example we consider the setup shown in the upper part of Fig.5.7, that has been used for a QKD up to 30 km [79]. In this arrangement a relative phase $\Phi_A \equiv \{0, \pi/2, \pi, 3\pi/2\}$ between two time-bins of a photon state is realized by the sender (Alice) with an unbalanced interferometer and a phase modulator. The receiver (Bob) measures incoming bins by means of a second interferometer, matched to the sender's one, set to $\Phi_B \equiv \{0, \pi/2\}$. With a probability of 50% the phase difference between Alice and Bob's interferometers will be 0 or π, and their measures will be correlated; in the other half of cases measures will be discarded by the two users.

Another realization of phase encoded QKD is reported in the lower part of Fig.5.7, and it has been used for QKD up to a distance of 67 km [80]. Using an intense pulse, Bob populates two time-bins with relative phase $\Phi_B = 0$, and sends them to Alice. Alice applies a relative phase $\Phi_A \equiv \{0, \pi/2, \pi, 3\pi/2\}$, reflects the pulses on a Faraday mirror, let them pass through an attenuator, and sends them back to Bob. The two pulses retrace in their backward path all the fluctuations they suffered in the forward path, thus arriving at Bob's interferometer ready for being revealed. As in the previous scheme Bob sets at random $\Phi_B \equiv \{0, \pi/2\}$, and measures the outcomes, completing the *non-deterministic* QKD pertaining to BB84. This mechanism of automatic compensation of noise earned this setup the name of "Plug-and-Play" [4].

PP84 with phase encoding We propose here the phase-encoded version of PP84 [81]. The receiving user, Bob, prepares a photon in a superposition of two time-bins with a relative phase

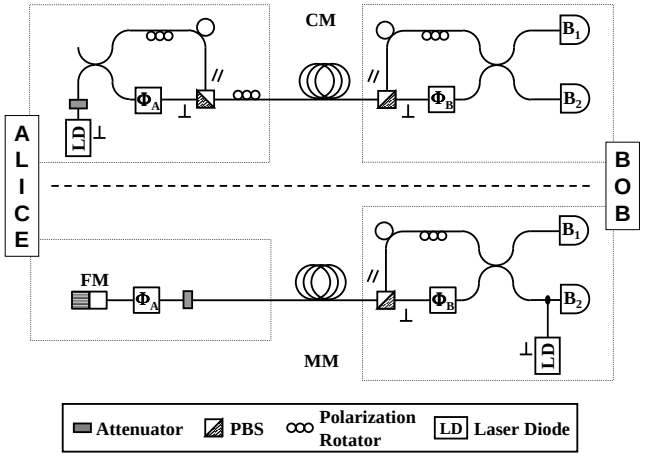

Figure 5.7: Schematics of two interferometers for BB84. The upper one, termed CM, has been used for QKD up to 30 km; the lower one, termed MM, is the Plug-and-Play setup used for QKD up to 67 km.

Φ_B randomly chosen between the values $\{0, \pi/2, \pi, 3\pi/2\}$. He sends the photon to Alice, the transmitting user, who chooses one of two possible tasks, *control mode* (CM) or *message mode* (MM), with probability (c) and $(1-c)$ respectively; the former realizes a control on the security of the channel, the latter the deterministic communication between the users.

MM: Alice encodes a bit of information with an unitary operation on the two time-bins: she can either apply the identity operation, choosing $\Phi_A = 0$ and encoding a '0', or introduce a 'phase-flip', by applying a phase $\Phi_A = \pi$ between the time-bins and encoding a '1'. The photon is sent back to Bob who measures it with his apparatus set with the same phase Φ_B he prepared initially. In this way Bob's measurement is *deterministic*, because the initial phase of the state (that he does know) is changed by an amount of 0 or π; he can thus guess Alice's operation without any needs of a classical channel.

CM: Alice detects the photon with her interferometer randomly set to $\Phi_A = 0$ or $\Phi_A = \pi/2$. After that Alice prepares a *new photon state* with a phase $\Phi'_A = \Phi_A + \pi/2$, and sends it back to Bob who, analogously to what he did in MM, measures it with the same phase Φ_B he prepared initially. We notice that if phase difference between Bob's interferometer and Alice's one is 0 or π then the two users share correlated information, while in the other two cases they do not. It is straightforward to realize that Alice procedure in preparing the new photon let the two users' interferometers to be necessarily correlated either in the forward path or in the backward one. This entails that none of the qubit states destined to the control procedure is discarded because of a wrong choice of the basis. As a consequence, both the CM and the MM of our protocol are performed in a deterministic fashion, thus achieving the doubling of the whole rate transmission mentioned before.

We remark that the *phase randomization* security procedure added to the original version of PP84 to make it more safe is not necessary in this case, since the encoding itself is done in phase, and the control mode has just the role of detecting eavesdroppings realized in this degree of freedom.

Implementation Given un unjammable public channel two users can exchange information in a secure manner by means of the above protocol. Eve can try to gain information by inquiring the phase of the photon both on the forward and on the backward path; alternatively, she can prevent Bob from gaining information (DoS attack [68]) by randomly measuring the state of the traveling photon; finally, on a lossy channel, she can conceal her presence behind losses [69]. Nevertheless no attack can remain undetected by the control procedure since it is akin to a BB84 check test, performed either on the forward path or on the backward one. This guarantees the protocol is unconditionally secure, as BB84 is, even if the security threshold may be different. Our protocol gives a probability of 25% to detect DoS attack as well as a general attack providing Eve with full information.

The practical implementation requires to gather the two interferometers of Fig.5.7. The resulting scheme is shown in Fig.5.8: the upper interferometer is devoted to CM, the lower to MM, and they are connected by a 1x2 fiber-coupler. The signal prepared by Bob goes at random into CM or into MM with probability c and $1-c$, respectively. Later on, when the photon is on the backward path, this device redirects it to Bob.

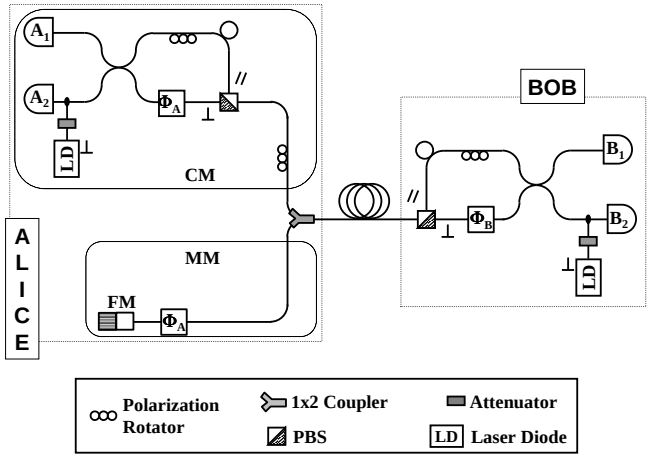

Figure 5.8: Final setup for deterministic Plug-and-Play cryptography. It merges the two interferometers of Fig.5.7, the upper one (CM) and the lower one (MM). An automatic switch between MM and CM is performed by a 1x2 coupler.

The MM-interferometer resembles the one used for testing BB84 up to 67 km [80]. It is a typical Plug-and-Play scheme, with the unique difference that the attenuator is inserted just after the laser-diode (LD), at Bob's side. A laser pulse with a mean photon number much lower than unity goes through Bob's interferometer and comes out into two time-bins with a relative phase Φ_B and opposite polarizations. In the Plug-and-Play setup an intense pulse is sent to Alice to provide a trigger signal for Alice's electronics. In our case, as the pulse is already attenuated at Bob's side, a further synchronization system, like the one usually adopted in other practical QKD setup [4, **?**, 79], is necessary. After reflection on the Faraday mirror, the photon travels back to Bob, retracing exactly those paths that compensate any undesired phase: this makes unnecessary the stabilization of the polarization. Eventually, Raileigh backscattering is not a problem in this case because of the low value of the average photon number from the beginning of the protocol.

The CM-interferometer resembles the one used for BB84 QKD up to a distance of 30 km [79]. As a time-polarization division technique is implemented, this task is sensible to random phase changes, and needs adjustments during the protocol runs. A value of ~ 0.6 rad/min for slow thermal drift in the interferometer was estimated, thus requiring a compensation step every $\sim 5s$ [79]. Also in this case Alice must synchronize her electronics with detectors, phase-modulator, and laser-diode using a suitable synchronization system.

Chapter 6

DQC specific features

Hitherto we described deterministic quantum cryptosystems, with or without entanglement, paying a special attention to the question of their security against *individual attacks*. We saw how PP and CL protocols turned out to be not secure in this sense, eventually arriving at PP84 that, on the contrary, allows for a safe communication between Alice and Bob.

However this kind of security is not the only feature that deserves to be studied in detail; other features are important as well. For instance we must remember that all the schemes described so far are "communication protocols" besides "cryptosystems" . Hence quantities like *efficiency* in delivering a message, i.e. the transmission rate, are significant. Actually it comes out that theoretical efficiency establishes the superiority of deterministic protocols over non-deterministic ones, while practical efficiency proves that non-entanglement-based schemes are preferable to entanglement-based ones.

In this chapter we deal with peculiar features of DQC, and establish a comparison with their analogues in NDQC. The discussion gives particular emphasis to PP84 scheme.

6.1 Asymptotical security

We begin by addressing the following question: GIVEN AN AMOUNT OF INFORMATION I_0 EAVESDROPPED BY EVE IN A SINGLE RUN, AND THE CORRESPONDING DETECTION PROBABILITY d, WHICH IS THE PROBABILITY EVE GAINS AN INFORMATION $I > I_0$ IN SEVERAL RUNS WITHOUT BEING REVEALED? The answer to this question leads to estimate the "asymptotical security" of a communication protocol. Nonetheless before covering this task some remarks are in order.

All the protocols described so far work in a run-by-run fashion. This means that the public discussion on the classical channel, usually settled down at the end of the whole communication, like in BB84, is performed at the end of each single run. In protocols exploiting entanglement, like PP and its variants, a classical channel's use in each run is mandatory, because the measurement Bob performs in order to decode the message depends on Alice's choice between control mode and message mode, and must be broadcast to Bob through the classical channel. Instead in protocols without entanglement there is no need for using the classical channel in each run, because Bob's measurement is always the same regardless the modality of that specific run. Hence in these types of protocols THE PUBLIC DISCUSSION CAN ALWAYS BE DEFERRED AT THE END OF THE WHOLE TRANSMISSION. However we point out that when the transmitted sequence is represented by a meaningful message the public discussion on security must be necessarily addressed run-by-run

(cf. Sec.6.3). In order to give a homogeneous scenario about all the possible situations we keep the run-by-run picture henceforth.

An important implicit statement encountered up to now in deterministic protocols is the *noiseless communication*: we assumed all the quantum channels to be immune from noise, as well as detectors and experimental apparatuses in general. As a consequence, any single error revealed by Alice and Bob could only be attributed to the presence of Eve, thus causing the arrest of the whole communication. This supposition can, of course, be removed from all the protocols examined above, at least as QKD is concerned, otherwise deterministic cryptography would result completely unpractical. Notwithstanding we will keep it in the following, postponing the generalization to noisy channels until the section on "unconditional security" .

Now we can answer the initial question. In all deterministic protocols envisaged and in all eavesdropping strategies considered, two parameters were always present: the probability per single run to detect Eve, d, and the probability for Alice and Bob to switch to control mode, c. Now suppose Eve is going to eavesdrop the whole information I_0 contained in a single message run; she adopts one of the attacks seen in the previous chapters that allow her to gain a full amount of information. The probability Eve's strategy is successful depends only on the "frequency" of *control modes*. If for example the first run is just a *message run* then her attempt is immediately successful, because no control is executed; the probability for this event is $(1-c)$. Yet if the first run is a *control run*, and the second is a *message* one, then Eve must at first survive the control run and only then she can complete her task, during the second run. The probability for this event is $c\,(1-d)\,(1-c)$, i.e. the probability the first run is a *control run*, multiplied the probability for Eve to survive one control, multiplied the probability the second run is a *message* one. By the same token, the whole probability Eve steals the information I_0 of a single run without being revealed is [63]:

$$\begin{aligned} s(c,d) &= (1-c)\left[1 + c\,(1-d) + c^2\,(1-d)^2 + ...\right] \\ &= (1-c)\sum_{i=0}^{\infty} x^i = \frac{(1-c)}{1-x} = \frac{(1-c)}{1-c\,(1-d)} \end{aligned} \tag{6.1}$$

when $x = c\,(1-d) < 1$; when $x = \{0,1\}$ we have the trivial cases $c = \{0,1\}$ or $d = \{0,1\}$.

If Eve wants to steal an information $I = nI_0$ pertaining to n message runs, by repeating the above argument we realize that she has a probability

$$[s(n,c,d)]^n = \left[\frac{(1-c)}{1-c\,(1-d)}\right]^n \tag{6.2}$$

to be successful. The expression (6.2) quantifies the concept of *asymptotical security* mentioned above. We notice that the fraction between square brackets is less than one, thus entailing a decrease of the probability $s(n,c,d)$ *exponential* with n.

Let us make an example. Suppose Alice and Bob are using PP84 for QKD. They set the probability for a control run to $c = 1/2$. Eve tries to steal the whole information by means of the Double-CNOT attack (Sec.(5.2.1)). In this case the detection probability amounts to $d = 3/8$. Thus the probability Eve gains one bit of information without being revealed is

$$s(c = 1/2, d = 3/8) = \frac{8}{11} \simeq 73\%.$$

This value can be decreased at will by increasing the value of c. However it is worth remarking that one bit of information is a small quantity. In order to increase the stolen information to

a considerable extent Eve aims at eavesdropping at least one or two bytes (1 byte = 8 bits) of information. In this case we obtain:

$$s_{\mathbf{1}byte}(n = 8, c = 1/2, d = 3/8) = \left(\frac{8}{11}\right)^8 \simeq 7.83\%$$
$$s_{\mathbf{2}bytes}(n = 16, c = 1/2, d = 3/8) = \left(\frac{8}{11}\right)^{16} \simeq 0.61\%.$$

The values above show the rapid decrease of Eve's chances to survive to repeated control runs.

We remark that we were dealing with the transmission of a meaningless sequence, since a QKD protocol was at issue. If a meaningful sequence is given, as in a QDC protocol, the correlations among words and letters inside it complicate the argument, because it is difficult to quantify information when correlations are present.

6.2 Efficiency

The efficiency in transmitting information given a fixed set of resources is a crucial problem of communications, both theoretical and practical. An important theorem of classical information theory states that if a (classical) communication channel has mutual information $I(X : Y)$ between the input signal X and the received output Y, then that channel can be used to send up to, but no more than, $I(X : Y)$ bits [45]. This entails that one is allowed to send up to *one bit* of classical information when a binary system is used.

All the same, for quantum mutual information we have [82]:

$$I(A : B) \leq S(\rho) - \sum_i p_i S(\rho_i), \tag{6.3}$$

where S is the von Neumann entropy, ρ_i are the states prepared and sent by Alice and $\rho = \sum_i \rho_i$. The equality holds if, and only if, all the transmitted states ρ_i commute. Eq.(6.3) in turn implies that the upper bound for the allowed quantum bit rate is again *one bit*. Nevertheless, to reach this limit is far from simple: the equality in Eq.(6.3) must hold, and the states involved must be pure; yet we can not permit the terms ρ_i commute, because in this case Eve would realize a perfect eavesdropping: by means of an orthogonal measurement she could steal all the information without being detected, with the strategy we already described in Sec.3.3.1. In the next, we are going to show that DQC allows us to reach the upper limit of one bit, widely surpassing NDQC's performances.

As far as efficiency of transmission is concerned we refer to the work of Cabello [83], in which a precise definition is given. The *theoretical efficiency* of a quantum communication protocol is defined by the formula

$$\mathcal{E} = \frac{b_s}{(q_t + b_t)}. \tag{6.4}$$

b_s is the expected number of secret bits received by Bob in each run of the protocol, q_t is the number of qubits transmitted in each run on the quantum channel, and b_t is the average number of bits transmitted in each run on the classical channel in order to complete the communication. In this definition the potential classical bits required to authenticate the channel are not taken into account, as they are a constant, negligible when compared with the number of transmitted secret bits. Furthermore it is important to remark that the fraction of bits devoted to test the quantum channel for eavesdropping does not enter Eq.(6.4): we can imagine that Alice and Bob transmit

Nb_s bits of secret information, and then decide to publicly reveal a part of these bits for control purposes. But the amount of revealed information does not change the value neither of b_s nor of $\mathcal{E}$.

To show how formula (6.4) applies we report the case of BB84 (for which we slightly disagree with Cabello [1]). In BB84 each qubit prepared and sent by Alice ($q_t = 1$) has a probability of 1/2 to be correctly measured (i.e. Alice and Bob's bases coincide). This entails that the expected number of secret bits received by Bob is: $b_s = 1/2$. In order to transform the results of their measurements into the final key *both Alice and Bob* have to publicly transmit the bits of information concerning the bases they used, hence $b_t = 2$. The theoretical efficiency of BB84 is then:

$$\mathcal{E}_{BB84} = \frac{1/2}{1+2} = \frac{1}{6}. \tag{6.5}$$

Cabello finds the different value $\mathcal{E}_{BB84} = 1/4$, but the only way to obtain it is by setting $b_t = 1$, and this poses the problem of how can Alice and Bob find a bilateral agreement on the bases used, eventually arriving at the final key. If only Alice, for example, communicates her basis, how can she apprehend when it is equal to Bob's one?

Scheme	b_s	q_t	b_t	$\mathcal{E}$
Bennett, 1992	<0.5	1	1	<0.25
Bennett and Brassard, 1984	0.5	1	1	0.25
Goldenberg and Vaidman, 1995	1	2	≥1	≤0.33
Ekert, 1991	1	1	1	0.5
Koashi and Imoto, 1997	1	2	0	0.5
Cabello, 2000	2	2	1	0.67
PP84, 2004	1	1	0	1

Figure 6.1: Theorethical efficiencies of several non-deterministic protocols according to Table I of [83]. The result of an unitary efficiency pertaining to PP84 is dramatic.

Eq.(6.5) tells us that BB84 allows to send on average $\sim$ 0.167 bits per run. Let us now discuss PP84's efficiency.

In PP84 no classical information is needed to encode and decode a string of bits. This means that we have $b_t = 0$. Moreover, the deterministic nature of the protocol allows that for each qubit ($q_t = 1$) we correspondingly obtain one bit of information ($b_s = 1$), since no qubits are discarded because of a wrong choice of the bases. Then the theoretical efficiency of PP84 is:

$$\mathcal{E}_{PP84} = 1. \tag{6.6}$$

We notice that the value in (6.6) leads just to the upper bound of *one bit* mentioned above! The main reason for this important value is the fact that $b_t = 0$, since classical communication is not needed. From Fig.6.1 we can see that only the protocol by Koashi and Imoto [84], among the six cited, has $b_t = 0$ as well, but in that case $q_t = 2$, hence more quantum resources are involved in it and the whole efficiency can not reach the unity.

We also point out that not all deterministic protocols have an unitary efficiency. For example the protocol by Ekert in Fig.6.1 is deterministic, but its efficiency is half the unit. Another interesting example of deterministic protocol is PP [63], studied in Sec.4.2. In this case we have $q_t = 1$ and $b_t = 1$ as well, because Alice has to tell Bob, by means of the classical channel, whether she is in control mode of message one. We remember that this bit of information is *necessary* to Bob to

[1] In Table I of his work ([83]) one can read the value 0.25 for BB84, while we find the value 1/6.

decode Alice's operation; without it Bob does not know which kind of measure he must perform. Finally, the expected number of secret bits transmitted is $b_s = 1$ in the original version of PP [63], while is $b_s = 2$ in the improved version by Cai and Li [71]. By consequence the theoretical efficiency is $\mathcal{E}_{PP} = 1/2$ in the former case and $\mathcal{E}_{PP} = 1$ in the latter case.

Let us study now the *practical efficiency* of a quantum communication scheme. As far as this quantity is concerned we refer to the definition given in [70].

In PP84 a qubit, represented for instance by the polarization of a photon, is traveling for a distance $2L$, being L the separation, in free space or in an optical fiber, between Alice and Bob. To take into account the natural losses occurring among photons covering this distance, we introduce the coefficient of transmission $\mathcal{T}$ for a photon that travels over a distance L. Hence in PP84 we have a total transmittance $\mathcal{T}^2$ over a distance $2L$. The practical efficiency can then be evaluated as the product of this value versus the theoretical efficiency found above:

$$\mathcal{E}'_{PP84} = \mathcal{E}_{PP84}\mathcal{T}^2 = \mathcal{T}^2. \tag{6.7}$$

On the contrary in BB84 the photon only travel for a distance L, thus the practical efficiency results:

$$\mathcal{E}'_{BB84} = \mathcal{E}_{BB84}\mathcal{T} = \frac{1}{6}\mathcal{T}. \tag{6.8}$$

Comparing Eq.(6.8) with Eq.(6.7), we can see that if $\mathcal{T} \geq \frac{1}{6} \simeq 16.7\%$ (a condition that is easily fulfilled even with a very defective technology) then PP84 turns out to be more efficient, also from a practical point of view, than BB84.

Let us calculate the practical efficiency of the improved version of PP protocol [71]. As seen before its theoretical efficiency amounts to one. Nonetheless its practical efficiency is lower, because it makes use of entanglement. We have two photons in an EPR pair: one travels over a distance 2L, the other is stored by Bob for a time 2L/c (c is the speed of light in the quantum channel) in a fiber ring of length 2L. Thus in PP we have two photons that should be protected from losses for a time $2L/c$ each. This brings a factor $\mathcal{T}^4$ in the practical efficiency (cf. [70]):

$$\mathcal{E}'_{PP} = \mathcal{E}_{PP}\mathcal{T}^4 = \mathcal{T}^4, \tag{6.9}$$

where we have taken into account the unitary theoretical efficiency of the improved version of PP. A comparison between Eqs. (6.9) and (6.7) shows that PP is always less efficient than PP84, because $\mathcal{T} \leq 1$; only for ideal channels ($\mathcal{T} = 1$) their efficiencies become equal. This result is due to the presence of entanglement in PP: as a matter of fact entanglement represents a hindrance to practicality. Hence, from the point of view of practical efficiency, cryptosystems that do not make use of entanglement are preferable.

6.3 Meaningful communication

We have seen how a meaningless string of bits, a *random key*, can be distributed in a secure way by using quantum mechanics, with the aim of successively using it in a OTP algorithm. This task takes the acronym of QKD and both NDQC and DQC are suitable to issue it. In the former case the two users do not know the random key until the very moment the protocol is completed; in this sense often the term "key generation" rather than "key distribution" is used to indicate this situation. On the contrary in the latter case we can speak about a real *key distribution*, because Alice already has with her the random string of bits she wants to send Bob, and she uses the photons prepared by Bob to transmit this sequence.

This represents a relevant difference from a logical point of view between the two approaches to QC. The most dramatic manifestation of this assertion is that the sequence transmitted from Alice to Bob *can be meaningful*, i.e. it can be the very *plain-text* that Alice aimed at sending Bob in a secure manner. In fact nobody prevents Alice from sending out a meaningful sequence rather than a random key because the way to do it is exactly the same seen for QKD in deterministic protocols. This kind of meaningful communication takes the name of "Quantum Direct Communication" , and the acronym of QDC. We point out that QDC is a peculiar feature of deterministic QC; it is easy to realize that there is no way to achieve it with non-deterministic QC.

We remark also that the term QDC usually refers to the transmission both of the *plain-text* and of the *scrambled-text*, i.e. of the plain-text XOR-ed with a random key (cf. Chapter 3). In this last case the random key used for encryption is revealed afterwards on the public channel to permit decryption; we prefer to call this form of QDC "scrambled-QDC" , to distinguish it from raw QDC. In general scrambled-QDC results more secure than QDC, because the encrypting key is revealed only after a successful security test of the quantum channel; if the test fails the key, and hence the message, is not given at all. Nevertheless scrambled-QDC uses more classical resources than QDC, as many as OTP. In fact to give the scrambled-text and then the key is *analogous* to give the key (by a normal QKD) and then the scrambled-text (by means of OTP). We said "analogous" and not "equivalent" because the former process is less secure than the latter[2]. So there is no explicit advantage in performing a scrambled-QDC rather than the couple of protocols QKD $\bigoplus$ OTP. On the contrary simple QDC, although less secure, ensues in a communication faster and less demanding on classical resources.

6.3.1 Direct communication

All the protocols described above, from PP to PP84, allow for QDC, because of their deterministic transmission of information. None of the message qubits is discarded and there is no wrong choice of the bases: the transformation executed by Alice is deterministically decoded by Bob if no noise or eavesdroppers are in the line. So all that is necessary for QDC is a meaningful message in the hands of Alice; she traduces the bits in quantum operations and performs these operations on the qubits prepared by Bob, in analogy with the mechanism of deterministic QKD described above. The only requirement is that the protocol *must be executed run-by-run*. The reason is that if the control procedure was held back to the end of transmission, a potential adversary would be revealed only after he stole the whole, meaningful, message. For this reason QDC is more demanding on security than QKD. In a run-by-run execution of deterministic protocols the form of security is the *asymptotical security* treated in Sec.6.1. Notwithstanding the notion of information used there is precise, while it is not so in this case, because we are speaking about meaningful messages. Information is a concept strictly related to the one of "randomicity" ; it can be defined in a rigorous manner only when the source of symbols we are interested in is a random source. A message, as every meaningful sequence, is not a random source: it contains correlations among its bits, since in every language there are preferred combinations of letters; the words by whom it is composed represent a kind of "codewords" that allow quick identification among millions of similar sounds; the very argument of any discussion makes some words more probable than others. So it is a difficult task to say how much information is contained in a meaningful message. Hence it is difficult to estimate how much information is necessary to an adversary to steal the whole message. In the following sentence we have replaced half of the letters (a huge amount of information!) with points:

[2]Privacy Amplification, mentioned in Sec.6.4, can not be performed neither in scrambled-QDC nor in any other type of QDC.

N.l .e.z. d.l .a.m.n .i .o.t.a .i.a
.i .i.r.v.i .e. u.a .e.v. o.c.r.,
c.é .a .i.i.t. v.a .r. s.a.r.t.

Yet, some skilled reader, specially if Italian, could recognize the meaning without going to see the bibliographic reference [85]. It could be sufficient for Eve to steal one third of the bits, or one fourth, to arrive at the whole message. For this reason is impossible to precisely quantify the stolen information and the disturbance in QDC, because *they depends on the knowledge about correlations given to the adversary*.

Nonetheless QDC could be an important tool when the noise level on the quantum channel is very low. In this case QDC results to be as secure as QKD (Sec.6.4), and twice faster because what is broadcasted is directly the message. One can envisage a situation in which the time available for the communication is limited (for instance when a satellite is used) and the users are disposed to sacrifice some security in favor of velocity. In such a situation QDC represents a fine compromise between the two requirements.

6.3.2 Quantum dialogue

A common feature to all deterministic protocols is the use of two ways. One could object that the usage of two ways reduces to one half the rate of transmission, but it is not so. The relevant information flows from Alice to Bob, and is this quantity to determine the transmission rate; the photons traveling from Bob to Alice must not be included. This allows deterministic protocols to outperform non-deterministic ones as far as efficiency is concerned. However, there exists a scheme that makes even greater the difference between deterministic and non-deterministic approach. It takes the name of "Quantum Dialogue" (QD) because of its peculiar "question-answer" structure [86, 87].

The scheme of QD proposed in [86] is not involved, but it is closely related to the use of entanglement and to Ping-Pong protocol (Sec.4.2). Yet it is not compulsory to require entanglement to perform QD. In order to extend QD also to protocols without entanglement we propose here a simplified version of it equivalent to the original in all respects.

In a first step Alice and Bob execute a QDC in which Alice sends out a message $\mathcal{M}_1$. If the transmission and control modes are successful then the two users are authorized to think that Eve acquired only an exponentially small amount of information about the delivered message. This entails that the message $\mathcal{M}_1$ itself, known by both the users, can be used by Bob as a key for encrypting his answer $\mathcal{M}_2$ and sending it out on the classical channel in a *One Time Pad* fashion:

$$\mathcal{M}'_2 = \mathcal{M}_2 \oplus \mathcal{M}_1. \tag{6.10}$$

The security of QD resides in the fact that the XOR operation in Eq.(6.10) between the two meaningful strings $\mathcal{M}_1$ and $\mathcal{M}_2$ makes the string $\mathcal{M}'_2$ meaningless. Nonetheless such an assumption is not completely true. The immediate counterexample is provided by the XOR between two strings maximally non-random like $\mathcal{M}_1 = \{00...0\}$ and $\mathcal{M}_2 = \{11...1\}$. Moreover the explicit declaration on the public channel of the XOR between two meaningful messages is considered a serious weakness [4].

Despite of these drawbacks QD explicitly shows that, at least in principle, it is possible to further increase the transmission rate of non-deterministic protocols by means of deterministic cryptography. Furthermore the possibility of a bidirectional exchange of information remains an appealing logical task impossible to accomplish without deterministic approach.

6.4 PP84 unconditional security

The question of security is crucial in the frame of quantum cryptography. Usually it comes in two main classes: security against practical attacks and general security proofs against every kind of conceivable attack. This latter argument, restricted to deterministic protocols, and without any claim to be exhaustive, is the matter treated in the present section.

We begin the discussion by reporting the security criterium for a cryptographic protocol [25]:

SECURITY CRITERION: A QKD protocol is defined as being *SECURE* if, for any security parameters $l > 0$ and $s > 0$ chosen by Alice and Bob, and for any eavesdropping strategy, either the scheme aborts, or it succeeds with probability at least $1 - O(2^{-l})$, and guarantees that Eve's mutual information with the final key is less than 2^{-s}. The key string must also be essentially random.

From this definition we can immediately deduce that QDC and QD can not be *secure*, because they convey a meaningful, and hence non-random, string of bits. This quite restrictive view can be avoided, as we will see, but it is a very delicate point. In analogy with demonstration of BB84's unconditional security by Lo and Chau [51] we begin by restricting ourselves to the study of PP84 on a noiseless channel.

Step 1: PP84 as a Quantum OTP.

The first step to acknowledge unconditional security of PP84 is to realize that PP84 is a kind of "Quantum OTP" [88]. In the forward path Bob sends the *quantum key* to Alice, represented by the sequence of initial states (5.30). If Alice measured it, she and Bob would follow the procedure of BB84, creating a random key to use in a future execution of a "classical" OTP. On the contrary in PP84 Alice does not measure the *quantum key* but rather uses it to encode the sequence by means of either identity or spin-flip operations. These operations realize a kind of "quantum XOR" : identity is like Alice XOR-ed the received bit with 0, and spin-flip is like a XOR with 1. To clarify this point let us take the following example:

(i) Bob prepares the *key* $K = 0110001010$. He decides to translate it into quantum language by associating to the bit 0 the qubits $\uparrow$ or $\rightarrow$, and to the bit 1 the qubits $\downarrow$ or $\leftarrow$ in a random choice. He thus obtains the sequence (*quantum key*):

$$QK = \{\uparrow, \downarrow, \leftarrow, \rightarrow, \uparrow, \rightarrow, \downarrow, \uparrow, \leftarrow, \rightarrow\} \tag{6.11}$$

(ii) Alice prepares the *message* $M = 1011001001$ and translates univocally it in quantum operations (*quantum message*):

$$QM = \{F, I, F, F, I, I, F, I, I, F\} \tag{6.12}$$

where F stands for Flip operation, given by iY, and I for Identity.

(iii) Alice performs operations (6.12) on the *quantum key* (6.11) thus creating the quantum sequence:

$$QK' = \{\downarrow, \downarrow, \rightarrow, \leftarrow, \uparrow, \rightarrow, \uparrow, \uparrow, \leftarrow, \leftarrow\}\,. \tag{6.13}$$

By reversing Bob's initial process we associate one bit to each qubit of the sequence (6.13) and obtain deterministically the sequence $S = 1101000011$. Now it is an easy task to verify that the sequence S is effectively the XOR between K and M:

$$S = K \oplus M$$

where addition is intended to be modulo two. This shows that PP84 is a kind of quantum version of OTP. We notice that, once this interpretation is given, is sufficient for Bob to calculate the XOR between his sequence and that received by Alice to recover Alice's message:

$$S \oplus K = (K \oplus M) \oplus K = M \tag{6.14}$$

and this is exactly what happens in PP84.

As the security of the message in OTP depends strictly on the security of the key, the second step in PP84's unconditional security proof consists in showing the unconditional security of the quantum key's transmission. This step is easy because it resembles BB84's unconditional security proof.

Step 2: PP84's forward path as a QKD with EPR scheme.

The argument is similar to the one envisaged in Sec.3.3.2. One way to prepare the initial random states (5.30) is that Bob creates the Bell state (4.4)

$$\left|\Phi^{(+)}\right\rangle = \sqrt{\frac{1}{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right) = \sqrt{\frac{1}{2}}\left(|+_A +_B\rangle + |-_A -_B\rangle\right).$$

Then he measures photon B along $\hat{S}_z$ basis if he wants to filter out one of the states $|0_A\rangle$ or $|1_A\rangle$, and along $\hat{S}_x$ basis for the states $|+_A\rangle$ or $|-_A\rangle$. Then he sends photon A to Alice. This procedure is conceptually equivalent to that in which Bob sends photon A to Alice and *after that* measures his photon. If it was not so, superluminal signal could be sent. To verify that Eve is not in the line Alice and Bob measure their photons along random bases, and compare results during a public discussion, estimating the fidelity of the transmitted information. This is exactly the control procedure we saw for Ping-Pong protocol, and it is easy to realize it is completely equivalent to what happens in BB84 and PP84. This equivalence can be exploited by means of the lemma by Lo and Chau [51] introduced in Sec.3.3 and here restated for the problem at issue:

LO-CHAU LEMMA: Information gain (on the quantum key) implies disturbance (on the forward path).

The worst situation we can imagine for Alice and Bob is when Eve has the complete control of the quantum channel or, even worse, when is Eve herself to distribute the state $|\Phi^+\rangle$ to the users. Let us suppose that Eve distributes a state ρ different from the state she declared ($|\Phi^+\rangle$). Alice and Bob verify during control mode how much the state in their possession resembles the declared state $|\Phi^+\rangle$. So they estimate the fidelity

$$F^2\left(\rho, \left|\Phi^+\right\rangle\left\langle\Phi^+\right|\right) = \left\langle\Phi^+\right|\rho\left|\Phi^+\right\rangle = 1-\gamma \tag{6.15}$$

by means of local measurements and classical communication only. The probability they find out by these means a state different from $|\Phi^+\rangle\langle\Phi^+|$ is:

$$\begin{aligned} tr\left[\rho\left(\mathbb{1} - \left|\Phi^+\right\rangle\left\langle\Phi^+\right|\right)\right] &= tr\left(\rho\right) - tr\left(\rho\left|\Phi^+\right\rangle\left\langle\Phi^+\right|\right) \\ &= 1 - \left\langle\Phi^+\right|\rho\left|\Phi^+\right\rangle = 1-(1-\gamma) = \gamma. \end{aligned}$$

Since entropy is an upper bound to mutual information [25] the maximal information gain between Alice and Eve is given by the entropy of the density matrix ρ. In turn the maximal entropy is obtained from a matrix like

$$\rho_{\max} = \frac{1}{4} diag\left(1-\gamma, \gamma/3, \gamma/3, \gamma/3\right),$$

which has the first term equal to the fidelity (6.15) and the other equally distributed among the other three Bell states to give $Tr(\rho_{\max}) = 1$. A bound to the entropy Eve gains in a single run when the fidelity is γ is represented by $S(\rho_{\max})$:

$$S(\rho_{\max}) = -(1-\gamma)\log_2(1-\gamma) - \gamma\log_2\frac{\gamma}{3}.$$

Similarly a bound to the entropy Eve gains in n runs when the fidelity is still γ is :

$$S(\rho_{\max}) = -(1-\gamma)\log_2(1-\gamma) - \gamma\log_2\frac{\gamma}{2^{2n}-1}.$$

The unconditional security criterium requires that after all the n control runs $S(\rho_{\max})$ must be exponentially small. If we set $\gamma = 2^{-s}$ we can see that when Alice and Bob find $F^2\left[\rho, \left(|\Phi^+\rangle^{\otimes n}\langle\Phi^+|\right)\right] > 1-\gamma$ then the transmission is secure. In fact in that case we obtain for the bounding entropy:

$$\begin{aligned} S(\rho_{\max}) &= -\left(1-2^{-s}\right)\log_2\left(1-2^{-s}\right) - 2^{-s}\log_2\frac{2^{-s}}{2^{2n}-1} \\ &= H\left(2^{-s}\right) + 2^{-s}\log_2\left(2^{2n}-1\right) \\ &< H\left(2^{-s}\right) + (2n)\,2^{-s} \\ &= -\left(1-2^{-s}\right)\log_2\left(1-2^{-s}\right) + (s+2n)\,2^{-s} \\ &= \left(s+2n+\frac{1}{\ln 2}\right)2^{-s} + O(2^{-2s}) \end{aligned}$$

i.e. we are sure that Eve's information is bounded from above by a quantity exponentially small, according to the security criterium (6.4). In the above relations we used the identity $-(1-x)\log_2(1-x) = \frac{1}{\ln 2}x + O(x^2)$, true for small values of x. We notice here that from the argument above it is easily seen that the probability to detect Eve amounts to $\frac{2}{3}\gamma$, and not to $\frac{1}{2}\gamma$, as reported in [71]. This leads to the value $d = \frac{1}{2}$ of the footnote 4 in Sec.4.2.2.

One can observe that the CNOT strategy depicted in Sec.5.2.1 appears to contradict the argument above: in fact one could object that during CNOT attack Eve does not gain any information about the quantum key, so the L-C Lemma seems to be not valid in that case. Furthermore the accessible information $\chi(\rho)$[3] [82] decreases under quantum operations [25] like the CNOT gate performed by Eve. But the states of the whole system involved in transformations (5.46) are all pure states, so this quantity is always zero. What changes is the entropy of the subsystems. Eve begins with the pure state $|0\rangle_e$ that has a zero content of information and ends up with a mixed state given by $\rho_E = Tr_B(|\Omega\rangle_{be})$, where $|\Omega\rangle_{be}$ is the bipartite state shared between Eve and Bob after first CNOT, containing information about the *quantum key*. Bob in his turn ends up with $\rho_B = Tr_E(|\Omega\rangle_{be})$. Since run by run $|\Omega\rangle_{be}$ is a pure state, then the reduced density matrices ρ_E and ρ_B have the same non-zero eigenvalues, and thus the same entropies $S(\rho_E)$, $S(\rho_B)$ respectively. This shows that after first CNOT Eve's information about the quantum key is equal to Bob's one, and has increased from zero to $S(\rho_E)$ that, in general, is a quantity greater than zero because ρ_E is a mixed state.

As a final comment to the paragraph we notice that in a run-by-run execution of the protocol on a noiseless channel (in which a single error stops the transmission) the *unconditional security* reported in the Security Criterium must be necessarily substituted with the concept of *asymptotical security* (see Sec.6.1). Anyhow the two criteria are equivalent. In fact, in a run-by-run procedure either the transmission succeeds and Eve has an exponentially small asymptotical probability to

[3] $\chi(\rho)$ is defined to be $S(\rho) - \sum_k p_k S(\rho_k)$, where $\rho = \sum_k p_k\rho_k$, and S is the von Neumann entropy.

collect an amount of information greater than zero, or the transmission aborts. So all the above argumentations remain valid for run-by-run protocols; then from this point of view QDC, for which a run-by-run execution is compulsory, results as secure as QKD, for which it is not. Moreover the last sentence of the Security Criterium "THE KEY STRING MUST ALSO BE ESSENTIALLY RANDOM" can be avoided in QDC by using the *scrambled-QDC* discussed in Sec.6.3: the meaningful sequence is XOR-ed with a temporary random key that is revealed on the classical channel only after security of the quantum channel has been properly verified. Then at this stage *QDC and QKD are equally secure.*

Step 3: PP84 on a Noisy Channel.

So far we considered noiseless channel. In this case the transmission stops as soon as a single error occur during control mode. Notwithstanding in practice noise plagues any conceivable communication. In this case a communication protocol that aborts at the first error results very unpractical. Thus when noise is present we need a "tolerance" on detected errors, but the risk is that Eve exploits this tolerance to perform powerful attacks. Nevertheless a theorem by classical information theory [89] helps to solve the problem [4]:

C-K THEOREM: FOR A GIVEN $P(\alpha, \beta, \epsilon)$, ALICE AND BOB CAN ESTABLISH A SECRET KEY (USING ONLY ERROR CORRECTION AND CLASSICAL PRIVACY AMPLIFICATION) IF AND ONLY IF $I(\alpha, \beta) \geq I(\alpha, \epsilon)$ OR $I(\alpha, \beta) \geq I(\beta, \epsilon)$, WHERE $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$ DENOTES THE MUTUAL INFORMATION AND H IS THE SHANNON ENTROPY.

In the theorem above $I(\alpha, \beta) = I_{AB}$, $I(\alpha, \epsilon) = I_{AE}$ and $I(\beta, \epsilon) = I_{BE}$. One can immagine that at some point of the protocol Alice, Bob and Eve measure their quantum systems; the outcomes provide them with classical random variables α, β and ϵ respectively, and with $P(\alpha, \beta, \epsilon)$, joint probability distribution. Given this joint probability distribution it is possible to distill a random key from the noise by means of two classical algorithms, viz. Error Correction (EC) and Privacy Amplification (PA), both accomplished by a public discussion on the classical channel. The details of such algorithms are beyond the scope of this work. We only say that by means of EC Alice and Bob can correct the errors due to noise in their respective keys, thus achieving a mutual information $I_{AB} = 1$. During Alice and Bob's public execution of EC Eve is listening to their communication, and uses it to improve her mutual information with the two users; then the algorithm PA is used by Alice and Bob to reduce Eve's information to zero. The necessary and sufficient condition to do this is that, very intuitive, given by C-K theorem: the mutual information between legitimate users must be greater than the mutual information between Eve and one of the two users.

The argument above has two immediate important consequences:

(i) In order to apply C-K theorem is necessary for Alice and Bob to have the possibility of estimating the quantity I_{AB}. This issue can be performed in PP84 (and also in the other deterministic protocols) only by means of a MESSAGE AUTHENTICATION STRATEGY, already described in Sec.5.2.2. In fact, except for special situations like that encountered in Sec.5.2.1 (see Fig.5.4), in which Eve's strategy is given, it is not possible to know how much information reaches Bob only by means of statistical analysis of the errors detected on the two paths. To get persuaded about this fact it is sufficient to compare the *measure-and-resend* attack with the *double-CNOT* attack: they are detected by Alice and Bob with the same probabilities $\overline{d_1} = \overline{d_2} = 1/4$, $\overline{d} = 3/8$ but in the former case $I_{AB} = 1/2$ (Sec.**??**) while in the latter it is $I_{AB} = 1$. So only a message authentication is effective to find out I_{AB}, and this quantity results to be a function of the only QBER Q. On the contrary the mutual informations I_{AE} and I_{BE} are functions of the forward and backward detection probabilities d_F and d_B. Of course the three parameters Q, d_F and d_B are not independent, but their explicit dependance is very complicate. What can be obtained in

general is a plot in three dimensions of the mutual informations, as that reported in Fig.6.2: the line defined by the intersection of the two graphics corresponds to the condition $I_{AB} = I_{AE}$, and so it determines the security area of the protocol.

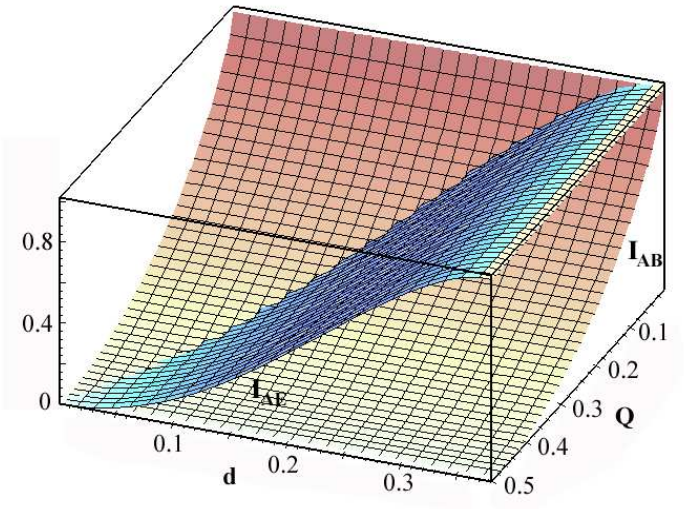

Figure 6.2: Example of security graphics in deterministic cryptography. The red curve represents I_{AB} as a function of the only parameter Q (QBER). The blue curve I_{AE} is a function of detection probability d. The intersection between the two graphics determines the "security line" . We point out that the above graphic has not been plotted from a real physical situation.

(ii) Quantum direct communication stops being as secure as quantum key distribution. The problem with QDC is that although EC can be performed on a meaningful message (indeed the meaning of the message represents a kind of error correcting code), PA can not. The reason is apparent: PA takes the strings in possession of Alice and Bob to a higher level of randomness in order to decrease Eve's information about them. If the string is meaningful this procedure looses evidently of significance.

As a conclusive remark we want to return on the interpretation of PP84 as a Quantum OTP. Now that such a view has been clarified we can recognize that also entanglement-based protocols, like Ping-Pong, share the same interpretation, even if it results less transparent in that case. Then our final task will be to show how entanglement present in those protocols can be employed to realize unconditional security also for Direct Communication in presence of noise. The scheme is completely theoretical.

The key ingredient to fulfil this task is the creation of m perfect EPR pairs. This can be carried out by means of an even imperfect distribution of EPR pairs, like in Ping-Pong, followed by an operation of *entanglement distillation* (ED). This last procedure permits to create m perfect EPR pairs from $M > m$ imperfect EPR pairs by means of local operations and classical communication. At the beginning Alice and Bob use a fraction of M to test the channel; then, according to the result of this test they distill m perfect EPR couples from M. It can be shown that ED gathers EC and PA in a single quantum algorithm [25]. So once ED is performed Alice and Bob share m perfect EPR pairs and has no information in common with Eve; citing again the Quantum

OTP interpretation we could also say that Alice and Bob share a secure *quantum key*. Now it is sufficient for Alice to execute encoding operations (meaningful or not) on her m halves of EPR pairs and send them to Bob, who will decode them by means of Bell measurements. The safety of the *quantum key* implies the safety of the meaningful communication as well.

Conclusion

The present dissertation is divided in two parts, for reasons related to the course of author's Ph.D at Rome's university "La Sapienza" .

In Part I we addressed the problem of *Quantum Decoherence* and *Disentanglement* of two-levels quantum systems dipped in a large symmetry-breakable fermionic environment, below the critical temperature T_c. In the frame of mean field theory analytical results are provided for coherence of system's density matrix ρ_s (Chapter 1) and for time behaviour of entanglement between two qubits (Chapter 2), measured by means of *concurrence* of the bipartite system. Hamiltonians involved in the discussion are those typical of *Ising* and *transverse Ising models* (shortened respectively with "IM" and "TIM" in the text) capable of magnetic ordering under suitable conditions. To assign them a physical meaning we notice that, upon addition of a transverse field in the system hamiltonian $\mathcal{H}_s$, our model resembles an array of Rydberg atoms interacting with a cavity mode of the radiation field [22]. Nevertheless such an assumption for $\mathcal{H}_s$ makes the problem unsolvable by analytical techniques, and requires numerical investigation. Beside that, it would be worthy to overcome mean field approximations adopted in the calculations, for instance by including the effect of fluctuations, or by applying the *spin wave* approach [90] to the bath, to gain a deeper insight into the physics of the model.

My personal contribution in the above scenario concerned for the most part the problem of entanglement. What came out from calculations is quite a counterintuitive conservation of entanglement in a bath with strong interactions: the bigger the coupling strength (or the lower the ratio $\frac{T}{T_c}$) the longer the time qubits remain entangled (cf. Eq.(2.22) and Fig.(2.1)). In some cases entangled qubits do not perceive environment at all, and the system state is a *decoherence free* one (Eq.(2.16)). Several connections with results from the field of entanglement decoherence are provided.

Part II contains description and discussion of protocols related to the topic of *Quantum Cryptography* (QC). In Chapter 3 we provided a short introduction to *non-deterministic* QC (NDQC), explaining reasons and motivations that led some physicists to think about it. As a matter of fact, limitative theorems from quantum mechanics, like the famous "No-Cloning" theorem, can be used to render secure operations, e.g. that of the distribution of a random key (QKD), that could not be so by only means of classical solutions.

The remaining chapters are devoted to the study of *deterministic* QC (DQC). In Chapter 4 we introduce the subject through the examples of *Dense Coding* and *Ping-Pong* protocol, a deterministic entanglement-based cryptosystem. We furnished a complete analysis of this protocol specially as far as its "claimed" security is concerned, discussing a variety of possible eavesdropping strategies to tamper with it. In chapters 5 and 6 we described deterministic cryptosystems that *do not make use of entanglement*. Among them we cite that named "PP84" because it has been suggested and developed by the author himself. Chapter 5 analyzes particularly the question of security of these protocols. The safety of communication in this case is guaranteed by

non-orthogonality of the quantum states involved, rather than by entanglement. We showed the complete security of PP84 against a wide variety of *individual attacks*, included, of course, those which afflict the other protocols. Eventually in Chapter 6 a number of other relevant features are studied. First of all *efficiency* both of DQC and NDQC is examined: it turned out that DQC is far more efficient than NDQC, and hence preferable for many purposes. Besides, practical efficiency of non-orthogonality-based cryptosystems proved to be higher than that of entanglement-based ones. In addition to that we showed how deterministic quantum ciphers allow for a real distribution of a random key, as well as for cryptographic applications different from QKD, e.g. *Quantum Direct Communication* (QDC) and *Quantum Dialogue* (QD), in which users communicate directly the plain-text rather than the cipher-text. Despite they are not completely secure, QDC and QD are suitable for a fast transmission of information. These new kinds of crypto-communication are impossible to address with non-deterministic schemes. As a final exercise we reported three steps to discuss unconditional security of PP84 protocol.

Four appendices at the end of the manuscript contain the most involved calculations and the complete lists of the cryptosystems cited in the text.

Appendix A

Exponentiation of suitable matrices

Let us define a 2×2 traceless matrix $\mathcal{A}$ as

$$\mathcal{A} = (a\hat{\sigma}_x + b\hat{\sigma}_z) = \begin{pmatrix} b & a \\ a & -b \end{pmatrix}, \tag{A.1}$$

with a, b real coefficients. The exponentiation of A gives:

$$e^{\mathcal{A}} = (\cosh q)\, I + \left(\frac{\sinh q}{q}\right)\mathcal{A}\,; e^{i\mathcal{A}} = (\cos q)\, I + i\left(\frac{\sin q}{q}\right)\mathcal{A} \tag{A.2}$$

with $q = \sqrt{(a^2 + b^2)}$. Therefore:

$$tr\left(e^{\mathcal{A}}\right) = 2\,(\cosh q)\;; tr\left(e^{i\mathcal{A}}\right) = 2\,(\cos q) \tag{A.3}$$

Let us extend these arguments to three matrices $\mathcal{I}$, $\mathcal{R}$, and $\mathcal{I}'$ of the same form of $\mathcal{A}$:

$$\begin{aligned} tr\left[e^{i\mathcal{I}} e^{\mathcal{R}} e^{i\mathcal{I}'}\right] &= tr\left\{\left[(\cos x)\, I + i\left(\frac{\sin x}{x}\right)\mathcal{I}\right]\left[(\cosh y)\, I + \left(\frac{\sinh y}{y}\right)\mathcal{R}\right]\left[(\cos z)\, I + i\left(\frac{\sin z}{z}\right)\mathcal{I}'\right]\right\} \\ &= (\cosh y)\left[2\,(\cos x)\,(\cos z) + i\,(\cos z)\left(\frac{\sin x}{x}\right)\left(\frac{\tanh y}{y}\right) tr\,(\mathcal{I}\mathcal{R})\right. \\ &\qquad \left. + i\,(\cos x)\left(\frac{\tanh y}{y}\right)\left(\frac{\sin z}{z}\right) tr\,(\mathcal{R}\mathcal{I}') - \left(\frac{\sin x}{x}\right)\left(\frac{\sin z}{z}\right) tr\,(\mathcal{I}\mathcal{I}')\right], \end{aligned} \tag{A.4}$$

where x, y, z are respectively related to the elements of $\mathcal{I}$, $\mathcal{R}$, $\mathcal{I}'$ as q was related to A.

Appendix B

Coherence Expression for TIM

As an example of calculation we report the steps that lead to Eq.(1.51). All other calculations are easier than this one and can be performed following the same line.

The time evolution of the total density matrix is:

$$\begin{aligned}\rho(t) &= \frac{e^{-m^2JN/T}}{Z}\left\{\exp\left\{it\sum_k\left[\left(\frac{J_0}{\sqrt{N}}\hat{S}_0^z+2mJ\right)\hat{S}_k^z+w\hat{S}_k^x\right]\right\}\rho_s \right. \\ &\left.\times\exp\left\{(1/T)\sum_k\left(w\hat{S}_k^x+2mJ\hat{S}_k^z\right)\right\}\exp\left\{-it\sum_k\left[\left(\frac{J_0}{\sqrt{N}}\hat{S}_0^z+2mJ\right)\hat{S}_k^z+w\hat{S}_k^x\right]\right\}\right\}. \end{aligned} \tag{B.1}$$

First, the partition function results:

$$Z=e^{-m^2JN/T}tr\left\{\exp\left[(1/T)\sum_k\left(w\hat{S}_k^x+2mJ\hat{S}_k^z\right)\right]\right\}=e^{-m^2JN/T}\prod_k tr\left[e^{\left(w\hat{S}_k^x+2mJ\hat{S}_k^z\right)/T}\right]. \tag{B.2}$$

By virtue of equation (A.3) we find

$$Z=e^{-m^2JN/T}\ 2^N\ \left\{\cosh\left[\frac{\Theta}{2T}\right]^N\right\}. \tag{B.3}$$

Notice that the constant $e^{-m^2JN/T}$ in the partition function simplifies with that present in Eq.(B.1).

Let us now study the time evolution of the operator $\hat{S}_0^- = |0\rangle\langle 1|$ that represents the off diagonal part of the density matrix:

$$\begin{aligned}\hat{S}_0^-(t) &= \left[2\cosh\left(\frac{\Theta}{2T}\right)\right]^{-N} tr_B\{\prod_k e^{it[(\frac{J_0}{\sqrt{N}}\hat{S}_0^z+2mJ)\hat{S}_k^z+w\hat{S}_k^x]} \\ &\qquad e^{(w\hat{S}_k^x+2mJ\hat{S}_k^z)/T}\,|0\rangle\langle 1|\prod_k e^{-it[(\frac{J_0}{\sqrt{N}}\hat{S}_0^z+2mJ)\hat{S}_k^z+w\hat{S}_k^x]}\} \\ &= \hat{S}_0^-(0)\left[2\cosh\left(\frac{\Theta}{2T}\right)\right]^{-N}\prod_k tr_B\left\{e^{i\mathcal{I}}e^{\mathcal{R}}e^{i\mathcal{I}'}\right\}, \end{aligned} \tag{B.4}$$

where:

$$\mathcal{I} = t\left[\left(\frac{J_0}{2\sqrt{N}} + 2mJ\right)\hat{S}_k^z + w\hat{S}_k^x\right], \tag{B.5}$$

$$\mathcal{R} = \left(w\hat{S}_k^x + 2mJ\hat{S}_k^z\right)/T, \tag{B.6}$$

$$\mathcal{I}' = -t\left[\left(-\frac{J_0}{2\sqrt{N}} + 2mJ\right)\hat{S}_k^z + w\hat{S}_k^x\right]. \tag{B.7}$$

In order to use Eq.(A.4) we evaluate the following quantities:

$$x = \frac{t}{2}\sqrt{\Theta^2 + 2\frac{mJJ_0}{\sqrt{N}} + O\left(\frac{1}{N}\right)} \tag{B.8}$$

$$y = \frac{\Theta}{2T} \Longrightarrow \left(\frac{\tanh y}{y}\right) = \frac{2T}{J} \tag{B.9}$$

$$z = \frac{t}{2}\sqrt{\Theta^2 - 2\frac{mJJ_0}{\sqrt{N}} + O\left(\frac{1}{N}\right)} \tag{B.10}$$

and

$$tr\left(\mathcal{I}\mathcal{R}\right) = \frac{t}{2T}\left(\frac{mJJ_0}{\sqrt{N}} + \Theta^2\right), \tag{B.11}$$

$$tr\left(\mathcal{R}\mathcal{I}'\right) = \frac{t}{2T}\left(\frac{mJJ_0}{\sqrt{N}} - \Theta^2\right), \tag{B.12}$$

$$tr\left(\mathcal{I}\mathcal{I}'\right) = -\frac{t^2}{2}\left(\Theta^2 - \frac{1}{4}\frac{J_0^2}{N}\right) = -\frac{t^2\Theta^2}{2} + O\left(\frac{1}{N}\right). \tag{B.13}$$

Then, substituting these into Eq.(A.4) and performing the product we obtain:

$$\prod_k tr\left\{e^{i\mathcal{I}}e^{\mathcal{R}}e^{i\mathcal{I}'}\right\} = 2^N\left(\cosh\frac{\Theta}{2T}\right)^N\left[\cos\left(\frac{tmJJ_0}{\Theta\sqrt{N}}\right) + i\frac{\Theta}{J}\sin\left(\frac{tmJJ_0}{\Theta\sqrt{N}}\right)\right]^N. \tag{B.14}$$

We can recognize in the second member of Eq.(B.14) the constant $r_{TIM}(t)$ defined in Eq.(1.50); the absolute value of it, in the limit of large N, gives the result of Eq.(1.51). The other quantities of the article come out with similar calculations.

Appendix C

Complete R matrix for TIM

Let's begin with time dependent density matrix expression for TIM hamiltonians (2.1). After mean field approximation (1.46) we obtain:

$$\begin{aligned}
\rho\left(t\right) &= \frac{1}{Z}\left[e^{-it\left(\mathcal{H}_s+\mathcal{H}_{sB}+\mathcal{H}_B^{mf}\right)}\rho_s e^{-\mathcal{H}_B^{mf}/T}e^{it\left(\mathcal{H}_s+\mathcal{H}_{sB}+\mathcal{H}_B^{mf}\right)}\right] \\
&= \frac{1}{Z}\exp\left\{it\left[\sum_k\left(\frac{J_0}{\sqrt{N}}\left(\hat{S}_{01}^z+\hat{S}_{02}^z\right)+2mJ\right)\hat{S}_k^z+\sum_k w\hat{S}_k^x\right]\right\} \\
&\qquad \rho_s'\exp\left\{(1/T)\sum_k\left(w\hat{S}_k^x+2mJ\hat{S}_k^z\right)\right\} \\
&\qquad\qquad \exp\left\{-it\left[\sum_k\left(\frac{J_0}{\sqrt{N}}\left(\hat{S}_{01}^z+\hat{S}_{02}^z\right)+2mJ\right)\hat{S}_k^z+\sum_k w\hat{S}_k^x\right]\right\}\ ,
\end{aligned} \tag{C.1}$$

where we set $\rho_s' = e^{it\xi_0\hat{S}_{01}^z\hat{S}_{02}^z}\rho_s e^{-it\xi_0\hat{S}_{01}^z\hat{S}_{02}^z}$.

The constants present in Eqs. (2.9) and (2.10) are found by complex conjugation of the following quantities, evaluated in a similar manner as the one seen in Appendix B:

$$\begin{aligned}
A^* &= \frac{1}{Z}\prod_k tr_B\left\{e^{it[2mJ\hat{S}_k^z+w\hat{S}_k^x]}e^{(w\hat{S}_k^x+2mJ\hat{S}_k^z)/T}e^{-it[(\frac{J_0}{\sqrt{N}}+2mJ)\hat{S}_k^z+w\hat{S}_k^x]}\right\} \\
B^* &= \frac{1}{Z}\prod_k tr_B\left\{e^{it[(-\frac{J_0}{\sqrt{N}}+2mJ)\hat{S}_k^z+w\hat{S}_k^x]}e^{(w\hat{S}_k^x+2mJ\hat{S}_k^z)/T}e^{-it[(\frac{J_0}{\sqrt{N}}+2mJ)\hat{S}_k^z+w\hat{S}_k^x]}\right\} \\
D^* &= \frac{1}{Z}\prod_k tr_B\left\{e^{it[(-\frac{J_0}{\sqrt{N}}+2mJ)\hat{S}_k^z+w\hat{S}_k^x]}e^{(w\hat{S}_k^x+2mJ\hat{S}_k^z)/T}e^{-it[2mJ\hat{S}_k^z+w\hat{S}_k^x]}\right\}
\end{aligned}$$

After calculations it's an easy task to verify that $A^* = D^*$, and for this reason the constant D doesn't appear in Eqs.(2.9-2.10).

The matrix $R(t)$ for TIM is:

$$R(t) = \begin{pmatrix} R_1 & R_2 \\ R_3 & R_4 \end{pmatrix} \tag{C.2}$$

where:

$$R_1 = \begin{pmatrix} |\alpha|^2 |\delta|^2 \left(1+|B|^2\right) - 2\alpha^*\beta\gamma\delta^* |A|^2 e^{-it\xi_0} & 2\alpha^*\beta |\gamma|^2 A^* e^{-\frac{1}{2}it\xi_0} - |\alpha|^2 \gamma^*\delta \left(A^* + AB^*\right) e^{\frac{1}{2}it\xi_0} \\ \alpha\beta^* |\delta|^2 \left(A + A^*B\right) e^{\frac{1}{2}it\xi_0} - 2|\beta|^2 \gamma\delta^* A e^{-\frac{1}{2}it\xi_0} & -2\alpha\beta^*\gamma^*\delta |A|^2 e^{it\xi_0} + 2|\beta|^2 |\gamma|^2 \end{pmatrix}$$

$$R_2 = \begin{pmatrix} 2\alpha^* |\beta|^2 \gamma A^* e^{-\frac{1}{2}it\xi_0} - |\alpha|^2 \beta^*\delta \left(A^* + AB^*\right) e^{\frac{1}{2}it\xi_0} & 2\alpha^* |\alpha|^2 \delta B^* - 2\left(\alpha^*\right)^2 \beta\gamma \left(A^*\right)^2 e^{-it\xi_0} \\ -2\alpha \left(\beta^*\right)^2 \delta |A|^2 e^{it\xi_0} + 2\beta^* |\beta|^2 \gamma & |\alpha|^2 \beta^*\delta \left(A^* + AB^*\right) e^{\frac{1}{2}it\xi_0} - 2\alpha^* |\beta|^2 \gamma A^* e^{-\frac{1}{2}it\xi_0} \end{pmatrix}$$

$$R_3 = \begin{pmatrix} \alpha\gamma^* |\delta|^2 \left(A + A^*B^*\right) e^{\frac{1}{2}it\xi_0} - 2\beta |\gamma|^2 \delta^* A e^{-\frac{1}{2}it\xi_0} & -2\alpha \left(\gamma^*\right)^2 \delta |A|^2 e^{it\xi_0} + 2\beta\gamma^* |\gamma|^2 \\ 2\alpha\delta^* |\delta|^2 B - 2\beta\gamma \left(\delta^*\right)^2 A^2 e^{-it\xi_0} & 2\beta |\gamma|^2 \delta^* A e^{-\frac{1}{2}it\xi_0} - \alpha\gamma^* |\delta|^2 \left(A + A^*B\right) e^{\frac{1}{2}it\xi_0} \end{pmatrix}$$

$$R_4 = \begin{pmatrix} -2\alpha\beta^*\gamma^*\delta |A|^2 e^{it\xi_0} + 2|\beta|^2 |\gamma|^2 & |\alpha|^2 \gamma^*\delta \left(A^* + AB^*\right) e^{\frac{1}{2}it\xi_0} - 2\alpha^*\beta |\gamma|^2 A^* e^{-\frac{1}{2}it\xi_0} \\ 2|\beta|^2 \gamma\delta A e^{-\frac{1}{2}it\xi_0} - \alpha\beta^* |\delta|^2 \left(A + A^*B\right) e^{\frac{1}{2}it\xi_0} & |\alpha|^2 |\delta|^2 \left(1+|B|^2\right) - 2\alpha^*\beta\gamma\delta^* |A|^2 e^{-it\xi_0} \end{pmatrix}$$

From Eq.(C.2) we have extracted all particular cases treated in the text.

Appendix D

Detailed protocols

We report here the detailed versions of the main deterministic protocols present in the text. We notice that all of them are reported in a run-by-run fashion, in which a public discussion is established for every run assigned to be a control run. Nevertheless none of the following protocols are obliged, by security matters, to follow this fashion when a nonsense key has to be transmitted. In this case all the public discussions can be deferred at the end of the transmission. This is not completely true for EPR-based deterministic protocols, as explained in Sec.6.1, because a classical run-by-run communication is always needed to tell Bob the right measurement to do. In this sense EPR-based protocol are more demanding on classical channel's use. On the opposite non-EPR protocols are more similar to BB84, with QBERs and unconditional security estimated in a statistical fashion, at least as far as a key distribution is concerned.

Ping-Pong [63]

(p.0) Protocol is initialized: $n = 0$. The message to be transmitted is a sequence $x^N = (x_1, ..., x_N)$, where $x_n \in \{0, 1\}$.

(p.1) $n = n + 1$. Alice and Bob are set to message mode. Bob prepares two qubits in the Bell state $|\Psi^+\rangle = 1/\sqrt{2}\,(|01\rangle + |10\rangle)$.

(p.2) He stores one qubit, the home qubit, and sends the other one, the travel qubit, to Alice through the quantum channel.

(p.3) Alice receives the travel qubit. With probability c she switches to control mode and proceeds with $(c.1)$, else she proceeds with $(m.1)$.

(c.1) Alice measures the travel qubit in the basis B_z and obtains the result $i \in \{0, 1\}$ with equal probability.

(c.2) She sends i through the public channel to Bob.

(c.3) Bob receives i from the public channel, switches to control mode, and measures the home qubit in the basis B_z, resulting in the value j.

(c.4) $(i = j)$: Eve is detected: Abort transmission. $(i \neq j)$: Set $n = n - 1$ and Goto $(p.1)$.

(m.1) Define $\hat{C}_0 := \mathbf{1}$ and $\hat{C}_1 := \hat{\sigma}_z$. Alice performs the coding operation $\hat{C}_{x_n}$ on the travel qubit and sends it back to Bob.

(m.2) Bob receives the travel qubit and performs a Bell measurement on both qubits resulting in the final state $|\Psi'\rangle \in \{|\Psi^+\rangle, |\Psi^-\rangle\}$. He decodes the message as

$$|\Psi'\rangle = \left\{ \begin{array}{l} |\Psi^+\rangle \Rightarrow x_n = 0 \\ |\Psi^-\rangle \Rightarrow x_n = 1 \end{array} \right\}$$

(m.3) $(n < N)$: Goto $(p.1)$. $(n < N)$: Goto $(p.4)$.

(p.4) Message x^N is transmitted from Alice to Bob. Communication successfully terminated.

Now let us modify the above protocol according to Cai and Li suggestion [71].

(c.1)' Alice measures randomly in the basis B_z or $\mathsf{B}_x = \{|+\rangle, |-\rangle\}$ ($z : a = 0$, $x : a = 1$) and obtains the result $i \in \{0, 1\}$ with equal probability.

(c.2)' She sends the pair (a, i) through the public channel to Bob.

(c.3)' Bob receives (a, i) from the public channel, switches to control mode, and measures the home qubit in the basis B_a, resulting in the value j.

These points make the original PP protocol secure.

Cai-Li [76]

(1) Bob prepares one qubit in state $|0\rangle$ or $|+\rangle$ randomly with record.

(2) Bob sends the qubit to Alice.

(3) Alice receives the travel qubit. She decides on the message mode $(4m)$ or the control mode $(4c)$ by chance.

(4c) *Control mode.* Alice replaces the qubit she received from Bob with a qubit that she randomly prepares in a state among $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, and sends it to Bob. Bob performs his decoding measurement. After Bob announces his receipt of the qubit, Alice announces that it was a control run, and tells Bob which state she prepared. If Bob used the same basis as Alice and if he found a state different from the one prepared by Alice, then Eve is detected and the communication stops; otherwise, Alice sends next qubit to Bob.

(4m) *Message mode.* Alice performs an operation on the travel qubit to encode information. She encodes the bit '0' using the operation 1 and the bit '1' using the operation iY. Then Alice sends the qubit back to Bob. Bob measures the qubit to gain the message Alice encoded, and sends her the receipt through the public channel.

(5) When all of Alice's information is transmitted the communication is successfully terminated.

PP84 [77]

(p.0) *Initialization*: $n = 0$. The sequence to be transmitted is $x^N = (x_1, ..., x_N)$, where $x_n \in \{0, 1\}$; it is in any case determined by Alice, but it is *randomly determined* if it must represent a nonsense key or *accordingly, properly, determined* if it must represent a meaningful message. The operations necessary to encode the sequence are defined as $\hat{C}_0 := 1$ and $\hat{C}_1 := iY$. Alice has at her disposal a random N bit string a. Bob has two random N bit strings b and j.

(p.1) $n = n + 1$. Bob prepares the n^{th} qubit according to the following rules:

$$\begin{aligned} |\Psi\rangle_B &= |0\rangle \text{ if } (b_n, j_n) = (0, 0) \\ |\Psi\rangle_B &= |1\rangle \text{ if } (b_n, j_n) = (0, 1) \\ |\Psi\rangle_B &= |+\rangle \text{ if } (b_n, j_n) = (1, 0) \\ |\Psi\rangle_B &= |-\rangle \text{ if } (b_n, j_n) = (1, 1) \end{aligned}$$

He then sends it to Alice through the quantum channel.

(p.2) *CM or MM: decision.* Alice receives the qubit.

With probability c she goes to control mode $(c.1)$.

With probability $(1 - c)$ she goes to message mode $(m.1)$.

(c.1) Alice measures the n-th qubit in $\hat{S}_z$ basis if $a_n = 0$ or in $\hat{S}_x$ basis if $a_n = 1$. She finds the value $i_n = 0$ for $|0\rangle$ or $|+\rangle$, $i_n = 1$ for $|1\rangle$ or $|-\rangle$. He registers i_n. After that she will send the projected qubit to Bob. $(p.3)$.

(m.1) Alice performs the coding operation $\hat{C}_{x_n}$ on the qubit and sends it to Bob. $(p.3)$.

(p.3) Bob receives the qubit and announces publicly this event[1]. He measures the qubit along the same basis used for the preparation (determined by the value of b_n), resulting in the value $j'_n = 0$ for $|0\rangle$ or $|+\rangle$, $j'_n = 1$ for $|1\rangle$ or $|-\rangle$. He registers j'_n.

(p.4) *CM or MM: announcement.* Alice announces whether she performed a control $(c.2)$ or an encoding $(m.2)$.

(c.2) Alice announces publicly the couple $\{a_n, i_n\}$. Bob announces publicly the values $\{b_n, j_n, j'_n\}$. If $a_n = b_n$ then $(c.3)$. Else Alice and Bob discard this run: $n = n - 1$, $(p.1)$.

(c.3) *Double control.* If $j_n = i_n = j'_n$ then transmission goes on: $n = n - 1$, $(p.1)$. Else abort transmission and start all over.

(m.2) Bob can easily decode the sequence as $x_n = j_k \oplus j'_k$. $(p.5)$.

(p.5) If $(n < N)$ then $(p.1)$. If $(n = N)$ then the transmission is successfully terminated.

Hyper-secure PP84

(p.0) Protocol is initialized: $n = 0$. The key to be transmitted is a sequence $x^N = (x_1, ..., x_N)$, where $x_n \in \{0, 1\}$. The operations to transmit the key are defined as $\hat{C}_0 := \mathbf{1}$ and $\hat{C}_1 := i\hat{\sigma}_y$.

(p.1) $n = n+1$. Bob has two random N bit string b and j. He prepares the n^{th} qubit according to the following rules:

$$\begin{aligned} b_n &= 0, j_n = 0 \rightarrow |\Psi\rangle_B = |0\rangle \\ b_n &= 0, j_n = 1 \rightarrow |\Psi\rangle_B = |1\rangle \\ b_n &= 1, j_n = 0 \rightarrow |\Psi\rangle_B = |+\rangle \\ b_n &= 1, j_n = 1 \rightarrow |\Psi\rangle_B = |-\rangle \end{aligned}$$

He then sends it to Alice through the quantum channel.

(p.2) Alice receives the qubit.

With probability $(1 - c)$ she goes to message mode $(m.1)$.

With probability $c_{enc} \leq c$ she goes to control mode $(c.1)$.

With probability $c_{xz} = c - c_{enc}$ she goes to control mode $(c.2)$

(m.1) Alice performs the coding operation $\hat{C}_{x_n}$ on the qubit; moreover she will change randomly the phase of the qubit letting it pass through one of two paths of different length; eventually she sends it back to Bob; $(p.3)$.

(c.1) Alice encodes randomly the operation $\hat{C}_{i_n}$ on the qubit and sends it back to Bob. $i_n \in \{0, 1\}$ with equal probability. $(p.3)$

(c.2) Alice measures the qubit along X or Z chosen randomly. She finds the value i_n. After that

1) she will send the projected qubit to Bob. $(p.3)$

2) she will rotate the qubit of $\frac{\pi}{2}$, thus changing its basis, and send it to Bob. $(p.3)$

(p.3) Bob receives the qubit and measures it along the same basis used for the preparation (determined by the value of b_n), resulting in the value j'_n. He registers j'_n.

(p.4) $(n < N)$: Goto $(p.1)$. $(n = N)$: Transmission ended.

[1]This is necessary to establish the completion of the transmission run. After this signal the data of the classical discussion can be revealed publicly.

(p.5) Alice reveals which qubits are control qubits, and in which cases she used the first strategy or the second one. A public discussion is settled by Alice and Bob to value the security of the key distributed. In a noiseless and lossless channel if Alice and Bob find even only one error they abort the protocol:

$$\begin{aligned} \text{First Strat } (c_{enc}) \quad &: \quad j_k \oplus j'_k = i_k \text{ else } ABORT \\ \text{Second Strat } (c_{xz}) \quad &: \quad j_k = i_k = j'_k \text{ else } ABORT \end{aligned}$$

If all the controls go right then the key x^N is safely transmitted from Alice to Bob and Bob can easily decode the message qubits as:

$$x_n = j_k \oplus j'_k$$

Bibliography

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[2] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature **390**, 575 (1997); D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[3] S. Wiesner, SIGACT News **15**, 23 (1983).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935); A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[6] A. M. Steane, Rep. Prog. Phys. **61**, 117 (1998); E. G. Rieffel and W. Polak, arXiv: quant-ph/9809016, submitted to ACM Computing Surveys.

[7] W. H. Zurek, Phys. Rev. D **24**, 1516 (1981).

[8] W. H. Zurek, Phys. Rev. D **26**, 1862 (1982).

[9] W. H. Zurek, Phys. Today **44**, 36 (1991).

[10] C. W. Gardiner, *Quantum Noise*, Springer-Verlag, Berlin, 1991.

[11] D.Giulini, E. Joos, C. Kiefer, J. Kupsch, I. Stamatescu, and H. D. Zeh, *Decoherence and the appearance of a classical world in quantum theory*, Springer-Verlag, Berlin, 1996.

[12] D. Vitali, P. Tombesi, and G. J. Milburn, J. Mod. Opt. **44**, 2033 (1997).

[13] L.-M. Duan, and G.-C. Guo, Phys. Rev. A 57, 737 (1998).

[14] L. Viola and S. Lloyd, Phys. Rev. A 58, 2733 (1998).

[15] D. Vitali and P. Tombesi, Phys. Rev. A **59**, 4178 (1999).

[16] P. W. Shor, Phys. Rev. A **52**, 2493 (1995); P. W. Shor, Proc. of the 37h Annual Symp. on the Foundations of Computer Science (1994), arXiv: quant-ph/9605011.

[17] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996); A. M. Steane, Phys. Rev. A **54**, 4741 (1996).

[18] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098-1105 (1996).

[19] G.M. Palma, K.-A. Suominen, and A.K. Eckert, Proc. R. Soc. London, Ser. A 452, 557 (1996).

[20] P.Zanardi and M.Rasetti, Phys.Rev.Lett. **79**, 3306 (1997); L.M.Duan and G.C.Guo, *ibid.* **79**, 1953 (1997); D. A. Lidar, I. L. Chuang, and K. B. Whaley, *ibid.* **81**, 2594 (1998).

[21] L.Viola, E. Knill, and S. Lloyd, Phys.Rev.Lett. **82**, 2417 (1999); L.Viola, S. Lloyd, and E. Knill, Phys.Rev.Lett. **83**, 4888 (1999); L.Viola, E. Knill, and S. Lloyd, Phys.Rev.Lett. **85**, 3520 (2000).

[22] S. Paganelli, F. de Pasquale, and S. M. Giampaolo, Phys. Rev. A **66**, 052317 (2002).

[23] S. Paganelli, degree thesis, 2002.

[24] M. Lucamarini, S. Paganelli, and S. Mancini, Phys. Rev. A **69**, 062308 (2004).

[25] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[26] W. H. Zurek, S. Habib, and J, P. Paz, Phys. Rev. Lett. **70**, 1187 (1993).

[27] W. H. Zurek, Progr. Theor. Phys. **89**, 281 (1993).

[28] W. H. Zurek, arXiv: quant-ph/9708022 (2001).

[29] J. Preskill, *Lecture notes for the course on quantum information and computation*, Caltech, Pasadena, California, 1999; www.theory.caltech.edu/people/preskill/ph229.

[30] D. F. Walls and G. J. Milburn, *Quantum optics*, Springer, 1^{st} edition, 1995.

[31] H. Bohr, *Almost periodic functions*, Chelsea, New York, 1951.

[32] K. Huang, *Statistical Mechanics*, Zanichelli, 1987.

[33] B. Misra, and E. C. G. Sudarshan, J. Math. Phys. **18**, 756 (1977).

[34] C. B. Chiu, E. C. G. Sudarshan, and B. Misra, Phys. Rev. D **16**, 520 (1977).

[35] A. Peres, Am. J. Phys. **48**, 931 (1980).

[36] J. W. Negele and H. Orland, *Quantum many-particle systems*, Addison-Wesley, 1988.

[37] S. Sachdev, *Quantum Phase Transition* (Cambridge University Press, Cambridge, 1999).

[38] G. Jona-Lasinio, C. Presilla, and C. Toninelli, Phys. Rev. Lett. **88**, 123001 (2002).

[39] D. Gunlycke, V. M. Kendon, V. Vedral and S. Bose, Phys. Rev. A **64** 042302 (2001); T. Osborne and M. Nielsen, Phys. Rev. A **66**, 032110 (2002).

[40] T. Yu and J.H. Eberly, Phys. Rev. B **66**, 193306 (2002); T. Yu and J.H. Eberly, *ibid.* **68**, 165322 (2003).

[41] D.R. Terno, Phys. Rev. A **59**, 3320 (1999); T. Mor, Phys. Rev. Lett. **83**, 1451 (1999).

[42] P. Blanchard, L. Jakóbczyk, and R. Olkiewicz, J. Phys. A: Math. Gen. **34**, 8501 (2001).

[43] L. Tessieri and J. Wilkie, J. Phys. A: Math. Gen. **36**, 12305 (2003).

[44] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[45] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[46] C. A. Fuchs, and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[47] W. Diffie and M. E. Hellman, IEEE Tran. Info. Theor. **22**, 644 (1976).

[48] R. L. Rivest, A. Shamir and L. Adleman, Comm. ACM 21, 120 (1978).

[49] C. H. Bennett, and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York), pp. 175179, (1984).

[50] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[51] H.-K. Lo and H. F. Chau, Science **283**, 2050-2056 (1999)

[52] D. Mayers, J. ACM **48**, 351 (2001); quant-ph/9802025. Preliminary version: D. Mayers, in N. Koblitz (ed.), *Advances in Cryptology*, Proceedings of Crypto 96, Springer-Verlag, New York, 1996, p. 343-357.

[53] P. W. Shor, and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); quant-ph/0003004.

[54] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Crypt. **5**, 3 (1992).

[55] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theor. **41**, 1915 (1995).

[56] D. Deutsch, Proc. R. Soc. Lond. A **420**, 97 (1985).

[57] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[58] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[59] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[60] S. Pirandola, M. Lucamarini, and S. Mancini, in preparation, (2004).

[61] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[62] K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[63] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[64] L. Vaidman, and N. Yoran, Phys. Rev. A **59**, 116 (1999). 5501. N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[65] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).

[66] M. A. Neumark, Izv. Akad. Nauk SSSR, Ser. Mat. **4**, 277 (1940).

[67] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, The Nederlands).

[68] Qing-Yu Cai, Phys. Rev. Lett. **91**, 109801 (2003).

[69] A. Wojcik, Phys. Rev. Lett. **90**, 157901 (2003).

[70] I. P. Degiovanni, I. Ruo Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, Phys. Rev. A **69**, 032310 (2004).

[71] Qing-Yu Cai and Bai-Wen Li, Phys. Rev. A **69**, 054301 (2004).

[72] F.-G. Deng, G. L. Long, and X.-S. Liu, Phys. Rev. A **68**, 042317 (2003).

[73] X. Li, arXiv: quant-ph/0209050 (2002).

[74] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).

[75] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).

[76] Qing-Yu Cai and Bai-Wen Li, Chin.Phys. Lett. **21**, 601 (2004).

[77] M. Lucamarini and S. Mancini, arXiv: quant-ph/0405083 (2004). Submitted to Phys. Rev. Lett. on May 15$^{\text{th}}$ 2004, not yet rejected.

[78] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, quant-ph/0306141 (2003).

[79] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995); P. D. Townsend, Nature (London) **385**, 47 (1997).

[80] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, New J. Phys. **4**, 41 (2002).

[81] M. Lucamarini, and G. Di Giuseppe, special issue of Int. J. Quant. Inf. for the proceedings of Camerino, meeting April 16-19, 2004. ArXiv: quant-ph/0407256.

[82] A. S. Holevo, Probl. Peredachi. Inf. **9**, 3 (1973). [Probl. Inf. Transm. (USSR) **9**, 177 (1973)].

[83] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).

[84] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).

[85] "*Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura, ché la diritta via era smarrita.*" - Dante Alighieri, Divina Commedia, Canto I.

[86] Z. J. Zhang, arXiv: quant-ph/0403186 (2004).

[87] B. A. Nguyen, arXiv: quant-ph/0406130 (2004).

[88] F.-G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[89] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **IT-24**, 339 (1978).

[90] M. Sparks, *Ferromagnetic Relaxation Theory* (Mc Graw-Hill, New York, 1964)

Acknowledgements

I acknowledge personal responsibilities in the quite unfortunate course of my Ph.D: I was not prepared to tackle the hard struggle it represents. I followed for a couple of years vague ideas on the possibility of a "Ferromagnetic Ensemble Quantum Computer" , and several months within these years attempting to demonstrate a phantom "No-Go theorem" for Quantum Computation, very far from being factual. Later on I understood that my efforts to invalidate the whole Quantum Computation because of the failure of my little model were quite naive, and I abandoned the enterprise (fundamental in this sense was the reading of the book "La scomparsa di Majorana" by the Italian writer Leonardo Sciascia, in which is reported that Quirino Majorana, Ettore's uncle, spent all his life trying to demonstrate the fallacy of the theory of Relativity...) However I must also thank the lack of incentives, both economic and scientific, that everyday, with infinite patience, helped me in the issue of such a disappointing undertaken.

On the opposite, I would like to underline that it is not my fault I am still a member of the scientific community rather than a seller of videotapes. Anyone who wants to express his complaint about such a fact can ask me the address of the following people:

My parents, and my whole family
The ex-director of Doctorate prof. Guido Martinelli, and Doctorate's secretary Mrs. Cannillo
My supervisor in Rome prof. F. de Pasquale
My supervisor in Camerino and friend dr. S. Mancini
The whole group of Quantum Optics in Camerino
My friends Giannetto and Stefano "Cobbra" Pirandola, along with Giannetto's family.

All these people, for different reasons, believed in my skills more than I did: THANK YOU !!! , this thesis is partly yours.

Eventually, moved thanks are for all my male and, most importantly, female friends, who so nicely sweetly pleasantly delayed my scientific career. Sincerely CHEERS.