Université Libre de Bruxelles
Faculté des Sciences Appliquées
Service de Théorie de l'information et des communications

ASPECTS OF QUANTUM CRYPTOGRAPHIC PROTOCOLS

Louis-Philippe Lamoureux

Thèse présentée en vue de l'obtention
du grade de Docteur en Sciences

Promoteur: Nicolas Cerf

Année académique: 2005-2006

Remerciements

Je souhaite tout d'abord remercier Nicolas Cerf et Serge Massar qui ont encadré cette these. Les quatre années passées avec eux ont été extraordinaires et pour cela je leur en serai toujours profondément reconnaissant. Leur savoir-faire et leurs aptidudes multi-disciplinaires m'auront fait connaître plusieurs aspects de la physique et m'auront laissé avec une vision encore plus globale que j'aurais osé esperer. Je les remercie pour tout ce qu'ils m'ont appris. Je tiens aussi à remercier chaleureusement Philippe Emplit pour son soutien et tous les conseils qu'il m'a donnés. Je le remercie particulièrement de m'avoir integré dans son laboratoire dès mon arrivée à l'ULB : l'environment de recherche que j'y ai trouvé et les contacts avec les autres membres de son groupe m'ont fortement inspiré et encouragé.

Merci à Edouard Brainis avec qui j'ai eu la chance de collaborer, pour tout ce que nos discussions m'ont apporté. Merci à tous les chercheurs que j'ai eu la chance de cottoyer durant mes quatre années dans le service de Théorie de l'information et des Communications, en particulier Julien Niset, Stefano Pironio et Jérémie Roland qui sont devenus de vrais amis. Merci aussi aux membres du service Optique et Acoustique pour l'aide qu'ils m'ont chacun fournie, particulièrement Pascal Kockaert, Xavier Hutsebaut, David Amans et Cyril Cambournac.

Merci à ma famille car sans elle je ne serais jamais devenu la personne que je suis aujourd'hui. Je leur en serai toujours reconaissant. Merci aussi à tous mes amis que j'ai laissé derrière moi au Canada. En particulier, je remercie Eric Lanoue qui sans le savoir a toujours été une source d'inspiration pour moi. Merci à Julie Mingueza qui a su me supporter pendant ces dernières années.

Merci à toi Manu, le seul photon que j'ai réussis à capturer durant mon séjour ici.

Contents

Chapter 1

Introduction

Quantum mechanics is, without a doubt, the most completely confirmed physical theory that has ever been created in terms of being verified by experiment. Ever since the validity of Planck's constant was accurately measured by Millikan in 1916 [Mil16], experiment has never contradicted the theory. As we look back today, we observe that a century of quantum mechanical theory has not only given rise to new interpretations of the physical world but is also responsible for revolutionnary technological offsprings. Its ramifications are incredibly broad as quantum theory is accountable for many phenomena such as superconductivity, Bose-Einstein condensation, lasers and scanning tunneling microscopy just to name a few.

Another remarkable theory has distinguished the twentieth century for its important technological consequences. In 1948 Shannon published his seminal work on source coding and channel coding therefore mathematically defining the concept of information [Sha48]. More specifically, Shannon's theory set an upper bound to the error correction rate that can be achieved (and thus the level of noise that can be tolerated) when sending information on a given channel. The result of this great intellectual triumph led to the modern theory of information and communication and is greatly responsible for dominating our economy and knitting together the global community in which we live in today.

It was quickly observed by Landauer [Lan61] that the concept of information alone is incomplete. More precisely, he concluded that information cannot be separated from its physical representation: it is always stored in some physical system, manipulated by some physical process. This interesting observation has a number of consequences for information theory. The most important concerns the laws governing the dynam-

ics of an information carrier. Indeed, Shannon's theory of information relies on the fact that information is stored and processed in classical systems. All applications that can be drawn from this theory are ultimately limited by the laws of classical mechanics.

The arrival of the modern computer brought along Moore's law [Moo65] which concludes that the decreasing transistor size, and increasing computer performance per cost will slow down (or perhaps even halt) within the next few decades. The possible impacts on an information society such as ours are non-negligible and should be taken seriously. It is important to envision an alternative knowing that as transistors get smaller, the laws which govern the information carriers will change shifting from classical to quantum mechanical.

This leads to the natural merger of quantum theory and information theory which occured gradually during the last few decades. Wiesner was among the first to recognize that information can be encoded in systems obeying the laws of quantum mechanics. This discovery enventually led to the field of "quantum information theory". Today, the theory has greatly matured and contains many analoguous concepts present in Shannon's classical theory [NC00] such that we now have many tools to understand the achievable limits of information processing when evolving according to the laws of quantum mechanics. Furthermore, although still in its infancy, experimental implementation of quantum informational tasks have made milestone progress over the last 30 years but still offer monumental challenges for the future. The main problem being decoherence: the fact that quantum information is lost in the environment surrounding the quantum mechanical process. These processes are now being implemented, at a very low scale, with ion-traps, nuclear-magnetic resonance, semiconductors and optical photons to name a few.

Just as classical information theory, quantum information theory is divided in three major branches: quantum computation, quantum communication and the study of quantum ressources. The first can be described as the science of solving abstract mathematical problems using quantum carriers subjected to a complete set of logical quantum gates. Several difficult problems such as factoring large integers [Sho95], sorting databases [Gro97] or simulating large quantum systems [Fey82] have been found to be solved more efficiently using quantum computation. For example, we can prove the exsistence of quantum algorithms for which a large number N can be factored in $\mathcal{O}(\log N)^3$ in time whereas the best classical algorithms achieve only $\sim \mathcal{O}(a^N)$ in time. Although this result is of great intellectual interest it more importantly has profound

implications in the field cryptography. Indeed, the security of the most widely used classical cryptographic protocols are based on the fact it is difficult to factor large numbers using classical computation. Thus, in the advent of quantum computing, these protocols would automatically breakdown.

The second branch of quantum information, quantum communication, provides an adequate solution to the above problem and is the core subject of this dissertation. The main idea in quantum communication is to exploit the laws of quantum mechanics in order to achieve secure cryptographic tasks. In contrast to classical communication protocols where the security is based on computational hypotheses [GRTZ02] (such as the difficulty of factoring large numbers), the security of quantum communication protocols is guaranteed by the laws of physics. We shall see that certain tasks such as perfect quantum cloning, prohibited by the laws of quantum mechanics, can cleverly be used to the advantage of parties wishing to implement communication protocols. We will also describe how it is possible to implement these protocols using photons in optical fibers. Before giving any more detail about the outline of the thesis however, we briefly recall some basic notions of quantum mechanics.

1.1 Quantum information

Classical information theory is based on the concept of the *bit*, a dichotomic variable which can assume the values 0 or 1. The quantum analogue of the bit, the *qubit*, is defined in a two-dimensional Hilbert space spanned by the basis $\{|0\rangle, |1\rangle\}$. It can be interpreted as the superposition quantum state of a spin-1/2 particle. An arbitrary qubit $|\psi\rangle$ in a pure state can then be written as

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{1.1}$$

where α_0 and α_1 are complex numbers and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The basis $\{|0\rangle, |1\rangle\}$, is usually called the *computational* basis.

Generally a qubit is not in a pure state but a mixed one. In this case the system is completely described by its density operator ρ, which is a positive operator with trace one, acting on the state space of the system. The general mixed state is expressed as

$$\rho = \sum_i p_i |i\rangle\langle i| \tag{1.2}$$

in terms of any complete set of pure states $|i\rangle$ realized in the mixture with probability p_i.

1.1.1 Multipartite systems

In many situations we will need to describe the evolution and the properties of the subsystem of a composite system. The quantum state of a bipartite system composed of the systems A and B is described by the density operator ρ_{AB}. The system A alone is fully expressed by the reduced density operator defined as

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) \tag{1.3}$$

where Tr_B is a map of operators known as the partial trace over system B. The partial trace is defined by

$$\mathrm{Tr}_B\big(|a_i\rangle_A\langle a_i| \otimes |b_i\rangle_B\langle b_i|\big) = |a_i\rangle_A\langle a_i|\mathrm{Tr}_B(|b_i\rangle_B\langle b_i|) \tag{1.4}$$

An example of a composite system is the so-called entangled state. The word "entanglement" was first introduced by Schröedinger in 1935 to explain the unique quantum correlations existing among different subsystems after an adequate "preparation". Quantum entanglement, expressing the counter intuitive, most intriguing condition of the quantum world, i.e. the quantum "non-locality", lies at the heart of many quantum information tasks as, for instance, quantum cryptography.

When is a multipartite system "separable", i.e., expressible by a mere "product state", or entangled? Let us consider the simplest case, a system of two qubits A and B in a pure state $|\phi\rangle_{AB}$. $|\phi\rangle_{AB}$ is separable if and only if it can be written as the product state:

$$|\phi\rangle_{AB} = |a\rangle_A|b\rangle_B \tag{1.5}$$

in some basis, otherwise it is entangled. For instance, a separable pure state is $|0\rangle_A|0\rangle_B$, while the "singlet" state of two qubits

$$|\Psi^-\rangle_{AB} = \frac{1}{2}\big[|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\big] \tag{1.6}$$

is entangled and usually called a maximally entangled (ME) state [EPR35]. The density matrices of the subsystems A and B, obtained by applying the partial trace operator $\mathrm{Tr}_B(\rho_{AB}) = \mathrm{Tr}_A(\rho_{AB}) = \frac{1}{2}\mathbb{1}$, are completely mixed states. A feature of the singlet state is that under any geometrical "rotation" R, i.e. $SU(2)$; transformation affecting simultaneously the systems A and B, it keeps its typical formal expression.

Note that the definition of entanglement can be extended to the case of mixed states [HHH96]. Also note that the ME state $|\Psi^-\rangle$ is an element of the Bell basis consisting of four orthogonal states spanning 4-dimensional Hilbert space:

$$\begin{aligned} |\Phi^\pm\rangle &= \big[|00\rangle \pm |11\rangle\big]/\sqrt{2}, \\ |\Psi^\pm\rangle &= \big[|01\rangle \pm |10\rangle\big]/\sqrt{2} \end{aligned} \tag{1.7}$$

and will be widely used throughout the thesis.

1.1.2 Quantum dynamics

The "completely positive" map, also called CP-map, is the only operation which can be realized on any quantum mechanical system and determines the evolution of a general quantum open system. A map $\Omega : \rho \in \mathcal{H} \rightarrow \rho \in \mathcal{K}$ is a CP-map if it satifies the following properties [NC00]:

[1] Tr $\Omega(\rho) = 1$ if Tr$\rho = 1$.

[2] Ω must be convex and linear.

[3] Ω is completely positive.

1.1.3 Positive operator valued measures

A projective measurement of the qubit $|\psi\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$ leads as result to the state $|0\rangle$ with probability $|\alpha_0|^2$ and state $|1\rangle$ with probability $|\alpha_1|^2$. Generally quantum measurements are described by a collection $\{M_k\}$ of positive measurement operators, satisfying the completeness equation $\sum_k M_k^\dagger M_k = \mathbb{1}$. These operators act on the state space of the system being measured. The index k refers to the measurement outcomes that may occur in the experiment. If the initial state of the quantum system is ρ, the probability of obtaining outcome k over ρ is $\rho(k) = \mathrm{Tr}\big[M_k^\dagger M_k \rho\big]$ and the state after measurement can be expressed as

$$\rho_k = \frac{M_k^\dagger \rho M_k}{\mathrm{Tr}\big[M_k^\dagger M_k \rho\big]}. \tag{1.8}$$

If the result of the measurement is unknown, the output state is

$$\rho_{\mathrm{out}} = \sum_k M_k^\dagger \rho M_k. \tag{1.9}$$

1.2 Outline of the thesis

The contents of this thesis mainly concerns experimental implementations of quantum communication protocols (also called quantum cryptographic protocols) in optical fibers. These implementations are all accompanied by thourough theoretical demonstrations proving their validity. The first part of this thesis will therefore describe these experiments and their validity. In a second, shorter part, we will be concerned with the concept of quantum cloning and study the achievable limits that are imposed by quantum mechanics for specific cases.

In **chapter 2**, we introduce the first and most famous quantum cryptographic protocol where two separated parties aim at generating a common secret key without having a third malicious party gain any information. This is called quantum key distribution (QKD). In particular, the description of this protocol will introduce many tools and concepts in quantum and classical information theory which will be necessary throughout the rest of this dissertation. We will conclude by describing the intimate link between QKD and quantum cloning and introduce a simple quantum cloning formalism which will be used in subsequent chapters. In **chapter 3**, we lay down the general framework of a clever experimental technique, called "plug and play", which enables one to encode, process and measure quantum information using optical photons and passive, linear optical components. We will conclude that chapter by illustrating the power of this technique by describing an original experimental implementation of the first quantum algorithm introduced by Deutsch and Jozsa in 1992. We will show how it was possible to implement this algorithm for three qubits, a task that has never before been accomplished.

In **chapter 4**, we will turn to the implementation of a QKD protocol over highly noisy channels. We introduce the concept of *error filtration* discovered by Gisin *et al* [GLMP05] and argue that this method is efficient in order to surpress the effects of noise in long distance communication. We are the first to realize an experimental demonstration of this method. We illustrate its potentialities by carrying out the optical part of a QKD scheme over a line whose phase noise is too high for a standard implementation of a QKD scheme to be secure.

In **chapter 5**, we present new theoretical results concerning the rate at which a secret key can be generated during QKD. Our result is of great importance for practical quantum cryptosystems because it reduces the need for high-speed random number

generation (an absolute requirement in QKD). Surprisingly, our conclusions do not impair on the security against the most widely considered type of eavesdropping attack.

In **chapters 6** and **7**, we will introduce two new quantum cryptographic protocols: quantum coin tossing and quantum identification. In coin tossing, two distant parties who do not trust each other aim at generating a random bit without the need for a third-trusted party. Because the security of classical coin-tossing is based on computational hypotheses, a party can not leave out the possibility that his adversary has the capability of performing quantum computational tasks and therfore perfectly bias the outcome of the toss. We implement a quantum bit-string generation protocol (a generalisation of coin tossing) using the experimental technique described in chapter 3 and argue that the randomness we generate relies only on the laws of physics. Furthermore, we are the first to prove that our experimental implementation generates a higher level of randomness than what is achievable with classical bit-string protocols. As we have mentionned before, the security of quantum cryptography relies on no-go theorems, that is, tasks which are prohibited by quantum mechanics. In **chapter 7**, we devise and implement a new quatum cryptographic protocol based on a no-go theorem that has never been exploited to realise a cryptographic task. The task we perform is that of short distance identification where a claimant must prove her/his identity to a verifier by demonstrating knowledge of a secret known to be shared between the two parties.

The remaining two chapters of this thesis will be dedicated to specific problems in quantum cloning. In **chapter 8**, we study for the first time the problem of entanglement cloning. In particular, we show that any quantum operation that perfectly clones the entanglement of all ME qubit pairs cannot preserve separability. We will investigate a separability-preserving optimal "cloning machine" that duplicates all ME states of two qubits with the same quality.

The penultimate chapter will show how it is possible to exploit the cloning formalism introduced in chapter 2 in order to optimally clone an important class of quantum states. Our results are important because they emphasize the simplicity of the cloning formalism we use as opposed to other, more tideous methods. The last chapter of this thesis summarizes our results and looks upon future directions.

Chapter 2

Quantum Key Distribution

2.1 Introduction

Quantum Key Distribution is the most advanced field in quantum information science. In contrast to quantum computation or other quantum cryptographic protocols, QKD has made major progress not only within its theoretical realm but as well on experimental aspects to such an extent that implementations of QKD protocols are now commercially available (i.d. quantique, MagiQ). To understand the illustrious path which the field has taken so far we must head back to 1970 when a paper by Wiesner entitled "Conjugate Coding" [Wie83] (note that the paper was published much later) introduced the first ideas which would forge their way to become what we now refer as to QKD. In his seminal paper, Wiesner introduced the concept of "quantum money": unforgeable bank notes based on the laws of quantum mechanics. He suggested that during fabrication a series of two-level quantum systems be added on the bank note. Each system would be in a well defined state chosen among a finite set of non-orthogonal states in such a way that to measure a state correctly would require the extra information concerning the basis in which the state belonged to. Assuming that the mint be the sole keeper of this extra information, a counterfeiter (who would have no choice but to measure each state using a random basis) would have very little chances of perfectly forging the note without disturbing the original and thus having the mint authorities notice quickly. For the first time in the history of cryptology, someone had raised the possibility of cryptographic security relying on the fundamental laws of Nature rather than some mathematical proof or computational hypothesis. A decade later, another interesting paper authored by Herbert entitled "FLASH - A superluminal communicator based upon a new kind of measurement" was submitted to Foundations of Physics [Her82]. In his paper, Herbert raised the notion of super-

luminal signalling - a flagrant violation of the theory of special relativity. He claimed that an idealized laser cavity could have macroscopically distinguishable outputs when the input was a single arbitrarily polarized photon. He argued that the noise in this process would, in principle, not prevent perfectly identifying the polarization state of the photon. This process, he claimed, would lead the way to superluminal methods of broadcasting information. The paper, who was reviewed by two referees, was aproved by only one of them but nevertheless was accepted. The story behind why such a fundamentally wrong idea still managed to be published is an interesting one. The referee who recommended its publication, now known to be the late Asher Peres, justified his choice by expecting "that it would elicit considerable interest and that finding the error would lead to significant progress in our understanding of physics." A year later, his expectations came true. Almost simultaneously, Wooters and Zurek [WZ82] and Dieks [Die82], published their version of the no-cloning theorem and therefore the answer to Herbert's mistake: the proof that an unknown quantum state cannot be perfectly cloned. The no-cloning theorem marked a new milestone in the History of quantum mechanics and, one could argue, inevitably gave birth to the field of quantum information science. This led to a significant number of discoveries, not only in quantum mechanics but also in computer science, information theory and other fields of physics expanding the pluridisciplinary character of quantum information science. The first offspring of these mergers (and one of the most important) turned out to be a provably secure QKD protocol by Bennett and Brassard in 1984. It tackled the problem of distributing a secret key by using information carriers evolving according to the laws of quantum mechanics. The impact has been overwhelming as we now possess the tools which could potentially revolutionalize the way we process and transmit information. Although this chapter is devoted to a review of this protocol it is nevertheless important because it introduces the building blocks which will be necessary in the subsequent chapters. This chapter provides a theoretical introduction to the protocol whereas chapter 3 will introduce a practical method of implementing both QKD protocols and quantum algorithms.

2.2 Main Ingredients

The security of QKD relies on two fundamental concepts: true random numbers and the linearity of quantum mechanics. The former is true for many cryptographic systems whether classical or quantum mechanical the reason being that many encryption transformations need to be generated in a manner which is unpredictable to an adversary. Regardless, one must be extremely cautious in his/her method of generating

unpredictable quantities. Computer generated random numbers for example, are not truely random because computers are deterministic systems[1]. This implies that the adversary could predict the output of a generated sequence by optimizing a search strategy based on a biased probability distribution provided by such a deterministic system. In order to be sure that the generating process is really random, one should exploit the only true random process in Nature: quantum randomness. Examples of such natural phenomena include:

- elapsed time between emission of particles during radioactive decay;
- a single photon impinging on a beamsplitter;

The second fundamental concept lies at the heart of quantum theory. The quantum evolution of a closed quantum system is described by a unitary transformation. For a given system, such a transformation is generated by the Schrodinger equation $i\hbar\frac{\partial\psi}{\partial t} = H\psi$, a linear partial differential equation where H corresponds to the Hamiltonian of the system. The linearity of the Schrodinger equation forbids certain tasks of being perfectly fulfilled. In particular, it prohibits the perfect duplication of an unknown quantum state. At first glance, this impossibility can discourage the more pessimistic but with a little insight can be transformed into a most powerful tool. We now demonstrate this impossibility which happens to be the second ingredient for a secure realization of QKD.

2.2.1 The no-cloning theorem

The no-cloning theorem states that for any quantum state $|\psi\rangle$ there does not exist a unitary transformation $\mathcal{U}$ which will yield two perfect copies of $|\psi\rangle$. More specifically, given an unknown, pure input state $|\psi\rangle \in \mathcal{H}$ of which we would like to make two perfect copies, a "blank" state $|0\rangle \in \mathcal{H}$ (which will serve as one of the copies) and an ancillary system $|M_{\text{ini}}\rangle \in \mathcal{H}_{\text{QCM}}$ in some initial state, we show that the transformation

$$|\psi\rangle|0\rangle|M_{\text{ini}}\rangle \xrightarrow{\mathcal{U}} |\psi\rangle|\psi\rangle|M_{\text{fin}}(\psi)\rangle,\ \forall\ \psi \tag{2.1}$$

where $|M_{\text{fin}}(\psi)\rangle$ is the final state of the ancillary system does not satisfy the linear constraint imposed by quantum mechanical evolution and therefore cannot exist. Indeed, suppose that the unitary operation $\mathcal{U}$ allowed the following transformations:

$$|0\rangle|0\rangle|M_{\text{ini}}\rangle \xrightarrow{\mathcal{U}} |0\rangle|0\rangle|M_{\text{fin}}(0)\rangle$$
$$|1\rangle|0\rangle|M_{\text{ini}}\rangle \xrightarrow{\mathcal{U}} |1\rangle|1\rangle|M_{\text{fin}}(1)\rangle.$$

[1]Except maybe when using Windows.

Then the transformation $\mathcal{U}\big[|0\rangle + |1\rangle\big]|0\rangle|M_{\text{ini}}\rangle$ (neglecting the normalization factor) which by linearity of $\mathcal{U}$ can be rewritten as

$$\mathcal{U}|0\rangle|0\rangle|M_{\text{ini}}\rangle + \mathcal{U}|1\rangle|0\rangle|M_{\text{ini}}\rangle = \big[|0\rangle|0\rangle + |1\rangle|1\rangle\big]|M_{\text{fin}}\rangle$$

clearly does not lead to the desired result

$$\big[|0\rangle + |1\rangle\big]^{\otimes 2}\,|M_{\text{fin}}\rangle = \big[|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\big]|M_{\text{fin}}\rangle. \tag{2.2}$$

We therefore conclude that given a unitary transformation $\mathcal{U}$, no perfect cloning of an unknown, arbitrary quantum state is possible $\square$.

The no-cloning theorem is intricatelly related to the Heisenberg uncertainty principle. If one could perfectly clone an arbitrary quantum state then one could, in principle, make as many copies as one wished. These copies could then be measured such that every dynamical variable of the state could be known with arbitrary precision and therefore violate the uncertainty principle. Furthermore, the no-cloning theorem prevents absurdities such as superluminal signalling, and therefore reinforces the peaceful coexistence between quantum mechanics and special relativity [Gis98]. Finally, note that this conclusion can be easilly extended to higher dimensional systems and mixed states [BCF+96]. Now that the necessary ingredients have been laid out, we move on to the main section of this chapter where we describe the first and most studied QKD protocol.

2.3 The BB84 protocol

The BB84 protocol was devised by Charles Bennett of IBM and Gilles Brassard of the University of Montreal in 1984 [BB84]. The idea is the following. Suppose Alice and Bob, two widely separated parties[2], would like to generate a secret key known only to them with no or little prior common information. To accomplish this task, they must be absolutely certain of the identity of the other party. Also, they must be certain that they share an authenticated classical communication channel (a link that guarantees you're communicating with the intended party). These two requirements, alone, form a basis of extensive study. We shall not leap into details of how these two requirements are fulfilled but rather only mention that adequate techniques exist that satisfy them.

[2]We assume from now on that both parties are isolated from the outside world in their respective laboratory.

Once Alice and Bob have been convinced that the above requirements are satisfied, they can move on to the distribution of the quantum states which will eventually generate the secret key. This first phase of the protocol generates the so-called "raw" key, which contains N bits, and as we shall see, will eventually shrink to half its size to form the "sifted" key. It begins by Alice preparing strings $\overrightarrow{s}$ and $\overrightarrow{t}$ of N truly random classical bits. With these two strings, she goes on to prepare quantum states in 2-dimensional Hilbert space chosen among two mutually-unbiased (MU) bases. Two bases A and B for a d-dimensional system are said to be MU [LBZ02] if a state prepared in any element of A (such as $|A, \alpha\rangle$) has a uniform probability distribution of being found in any element of B, namely

$$|\langle A, \alpha | B, \beta \rangle| = \frac{1}{\sqrt{d}} \, . \tag{2.3}$$

In our description, we introduce a reference (computational) basis, which we label basis $B_Z = \{|0\rangle, |1\rangle\}$ from which we construct a second basis B_X (often referred as the "dual" basis), MU to B_Z:

$$B_X = \big\{|+\rangle, |-\rangle\big\}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}[|0\rangle \pm |1\rangle]$. We associate a classical bit value to each of these four states:

$$\begin{aligned} |0\rangle &= \text{"0"} \qquad |+\rangle = \text{"0"} \\ |1\rangle &= \text{"1"} \qquad |-\rangle = \text{"1"}. \end{aligned} \tag{2.4}$$

We stress that the quantum states and most importantly the reference frame in which Alice and Bob are working in are assumed to be publicly known. This assumption also applies to the above bit association. To select the i^{th} state she will prepare and send to Bob, Alice randomly picks a basis using s_i (the two possible bit values "0" and "1" are associated with B_Z and B_X, respectively) and then ramdomly picks a state contained in the chosen basis using t_i (again, the two possible bit values are associated with a state contained in the chosen basis). Bob, who also has in his possession a truly random bit-string $\overrightarrow{r}$ will use string element r_i to select in which basis he will measure the incoming state. The measurement outcome indicates Bob with a possible bit value. Note that, with probability $\frac{1}{2}$, Alice and Bob will use different bases such that sometimes the outcome will contain no information. After performing his measurement and storing the value of the bit, call it b_i, he awaits the $i^{\text{th}} + 1$ state that Alice has prepared in the meantime and proceeds to measure it with the

basis associated to r_{i+1}. This process is repeated until all N states have been sent. Afterwards, Alice and Bob begin a public discussion which aims at eliminating the incompatible measurements. This public discussion, accessible to an eavesdropper is called $sifting$. In the sifting phase, only information about the bases is revealed. That is, Bob informs Alice on the basis he has measured in for a given state, while Alice informs Bob on the basis in which she has encoded the corresponding state. This procedure generates the $sifted$ key which, in the absence of an eavesdropper, should be the same for both parties. Note that all we have shown so far is that Alice and Bob can arrive at a shared secret key without publicly announcing any of the bits. Also note that neither Alice nor Bob chooses the outcome of the key; it is the conjunction of both their random strings $\overrightarrow{r}$, $\overrightarrow{s}$ and $\overrightarrow{t}$ that produces the secret key. However, the presence of an eavedropper complicates the protocol. Indeed, because the information carriers are governed by the laws of quantum mechanics, an eavesdropper trying to tap the channel will gain information about the incoming states and inadvertantly introduce noise in Alice and Bob's sifted keys. Luckily, their exists methods that can counter the actions of the eavesdropper and still let Alice and Bob generate a secret key. We introduce the subject by describing the simplest attack an eavesdropper - call her Eve - can perpetrate. But before we do so, we quickly summarize important results in information theory which will help us quantify and interpret the information transfer between Alice, Bob and Eve.

2.3.1 Entropy and Information

The central result of classical information theory is the notion of *Shannon* entropy. Given a single binary random variable A with probability distribution $\{p_a, 1-p_a\}$, the entropy of A measures the amount of uncertainty about A before we learn its value (or equivalently how much we gain on average when learning the value of A). The binary Shannon entropy for random variable A is defined as:

$$H(A) \equiv -p_a \log p_a - (1-p_a)\log(1-p_a) \tag{2.5}$$

where the logarithms are assumed to be in base 2 (this assumption is extended to the rest of this thesis unless stated otherwise). We can extend our definition of entropy to a pair of binary random variables, (A, B), which measures the joint uncertainty about the pair (A, B):

$$H(A,B) = -\sum_{a,b=0}^{1} p(a,b)\log p(a,b). \tag{2.6}$$

Furthermore, upon knowing one of the variables (say A), we can define the entropy of B conditional on knowing A:

$$H(B|A) = -\sum_{a,b=0}^{1} p(b,a) \log p(b|a). \tag{2.7}$$

Finally, let us introduce the notion of *mutual information* which measures how much information A and B have in common:

$$I(A:B) = H(A) + H(B) - H(A,B). \tag{2.8}$$

This is the measure that we will use in order to quantify and compare the information shared between Alice and Bob, Alice and Eve, and Bob and Eve. Shannon entropy enjoys the following properties - amongst others - which we state without proof:

(1) $H(A), H(B) \geq 0$
(2) $I(A:B) = I(B:A)$
(3) $H(A) \leq H(A,B)$
(4) $H(A,B) \leq H(A) + H(B)$.

We emphasize that Shannon entropy measures the uncertainty related with a *classical* probability distribution. In the concerned chapters of this thesis, we focus on classical entropic characteristics, that is, the entropy of classical probability distributions arising from measurement outcomes of quantum mechanical systems. There exists an analogue measure of uncertainty related to quantum systems with density operators replacing probability distributions called the Von Neumann entropy.

2.3.2 Quantum-bit-error-rate and fidelity

The quantum-bit-error-rate (QBER) and the fidelity (F) are two other important measures which help quantify the communication between Alice, Bob and Eve. The QBER is the quantum analog of the bit-error-rate (BER) in classical information theory. The QBER - sometimes called the *disturbance* (D) - is defined as the ratio of the number of erroneous bits in the sifted key to the total number of sifted bits. This measure is useful in the context of eavesdropping because it easily quantifies the effects of a given eavesdropping strategy. For example, by perturbing a quantum state, Eve re-emits a mixed state which has a non-zero probability of being detected incorrectly by Bob. Equivalently, Bob can measure how close his received state is to the original one sent by Alice. Generally, he receives a density operator $\rho = \sum_i p_i |i\rangle\langle i|$ which

overlaps with the original pure state sent by Alice, $|\psi\rangle$. We define the fidelity as the distance separating ρ from $|\psi\rangle$:

$$F(\psi, \rho) = \langle\psi|\rho|\psi\rangle \tag{2.9}$$

where $F \in [0, 1]$. As we can see, $F = 1$ occurs only when $\rho = |\psi\rangle\langle\psi|$ while $F = 0$ occurs only when $\rho = |\psi^{\perp}\rangle\langle\psi^{\perp}|$. In between, the fidelity depends on the purity of ρ and/or the overlap with $|\psi\rangle$. Trace preservation imposes a simple relationship between the disturbance and the fidelity:

$$\mathcal{E}\big(|\psi\rangle\big) = \rho = F|\psi\rangle\langle\psi| + D|\psi^{\perp}\rangle\langle\psi^{\perp}| \tag{2.10}$$

for any CP-map $\mathcal{E}$ and where $F + D = 1$.

2.3.3 Intercept-resend attack

The simplest attack Eve could attempt is quite simple and intuitive but not very effective. The intercept resend attack consists in intercepting each incoming qubit individually and measuring it in a random basis. Each measurement outcome provides Eve with a possible bit value. Just as Bob, she is unaware of which basis a given state has been encoded with. In order to remain unnoticed, Eve prepares a quantum state corresponding to the outcome of her measurement and sends it on to Bob. At the end of the distribution, Eve, like Alice and Bob, is in possession of a raw key containing N bits. Alice and Bob then perform the sifting thus generating Bob's, Alice's, and Eve's respective sifted keys. Alice and Bob's sifted keys should, in principle, be perfectly corrolated. However, the fact that Eve has tampered with the states introduces errors thus inducing a non-zero QBER. Altogether, if Eve uses this strategy, she gets approximately 50% of the information, while Alice and Bob end up with a QBER of approximately 25%. In other words, once they have eliminated the cases in which Alice and Bob used incompatible bases, there are still about 25% errors. A more subtle strategy could have Eve intercept and resend only a fraction, say p, of the states travelling from Alice to Bob thus minimizing her presence. As we shall see, the information gained by Eve is then directly proportional to p.

An additional and necessary step of the BB84 protocol is for Alice and Bob to compare a small fraction of the sifted key which Alice and Bob choose to publicly reveal. If they indeed notice a 25% difference in their small fractions, they can quickly conclude that Eve has done her work. However, if no discripancies are detected, they can safely conclude that Eve was not present. They go on to discard the small revealed sequence

and keep the rest of the sifted key which they can eventually use in a classical cryptographic task such as the one-time-pad.

Let us calculate the information curves $I(A,B)$ and $I(A,E)$ for a given probability p that Eve will intercept, prepare and resend a given state or otherwise, with probability $1-p$, leave the state undisturbed. We begin with $I(A,E)$ and suppose that the sifted key has been created. Also, assume that Alice has sent a state chosen from basis B_Z (the converse yields the same result). The uncertainty surounding Alice is thus related to the bit value of the sent state which is uniformly distributed: $H(A)=1$. The uncertainty surrounding Eve is twofold. Firstly, there is the uniform probability that she chooses to measure in either bases (B_Z or B_X) and secondly, the uniform probability concerning the outcome of her measurement. Therefore, $H(E)=2$. The joint and conditional probability distributions of Alice sending state $A=|0\rangle$ and Eve measuring one of the four possible outcomes are summarized in table 2.11. (The necessary extension to Alice sending state $|1\rangle$ is omitted but trivial.)

Eve	P$(E\|A)$	P(A,E))
$\|0\rangle$	$\frac{1}{4}(1+p)$	$\frac{1}{8}(1+p)$
$\|1\rangle$	$\frac{1}{4}(1-p)$	$\frac{1}{8}(1-p)$
$\|+\rangle$	$\frac{1}{4}$	$\frac{1}{8}$
$\|-\rangle$	$\frac{1}{4}$	$\frac{1}{8}$

(2.11)

The information between Alice and Eve is therefore

$$I(A,E)=\frac{3}{2}+\frac{1}{4}(1+p)\log(\frac{1}{8}(1+p))+\frac{1}{4}(1-p)\log(\frac{1}{8}(1-p)). \tag{2.12}$$

A similar analysis can be performed for $I(A,B)$. Again, $H(A)=1$. Now, because the reconciliation has been performed, Bob has no uncertainty surrounding the basis of his measurement. The value of the bit (i.e. the quantum state) is the only source of uncertainty and therefore $H(B)=1$. The joint and conditional probability distributions when Alice sends state $|0\rangle$ are summarized in table 2.13. (Again, the extension to state $|1\rangle$ is trivial.)

Bob	P$(B\|A)$	P(A,B))
$\|0\rangle$	$(1-\frac{p}{4})$	$(\frac{1}{2}-\frac{p}{8})$
$\|1\rangle$	$\frac{p}{4}$	$\frac{p}{8}$

(2.13)

The information between Alice and Eve is thus expressed as:

$$I(A,B)=2+(1-\frac{p}{4})\log(\frac{1}{2}-\frac{p}{8})+\frac{p}{4}\log(\frac{p}{8}). \tag{2.14}$$

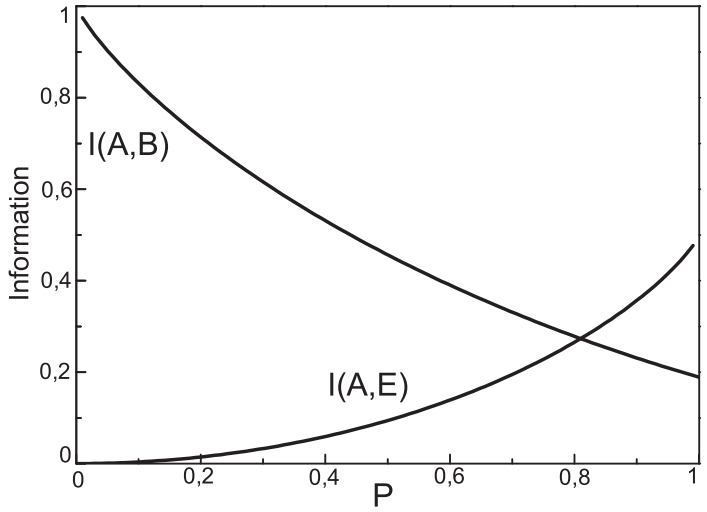

Figure 2.1: Information curves $I(A,B)$ and $I(A,E)$ for a given probability p that Eve will apply the intercept-resend strategy. Note that the QBER induced on Bob's sifted key is related to p as QBER $= \frac{p}{4}$.

Figure (2.1) plots the two information curves $I(A,B)$ and $I(A,E)$ for a given value of p. As expected, for low values of p, Bob's information is larger. But, more errors provide Eve with more information, while Bob's information gets lower. The fact that Eve can gain partial information about a given bit does not necessarily imply that Alice and Bob cannot extract a secret key. Indeed, once Alice has completed sending her states and that the reconciliation has been performed, Alice and Bob can use standard error correction techniques to get a shorter key without errors. Afterwards, Alice and Bob have identical copies of a key, but Eve may still have some information about it. Alice and Bob thus need to lower Eve's information down to an arbitrarily low value using some privacy amplification protocols. Using adequate protocols, it is possible for Alice and Bob to extract a secret key up to a QBER of 25% that is, the QBER corresponding to Eve's maximal information gain in the intercept-resend attack. In fact, for any cryptographic protocol, Csiszár and Körner have shown [CK78] that it is possible to extract a secret key as long as

$$R \geq \max\big[I(A,B) - I(A,E), I(A,B) - I(B,E)\big] \tag{2.15}$$

Although this 25% bound is the absolute upper limit, it is not quite realistic because the privacy amplification protocols that achieve security in this case are difficult to implement since they rely on the interaction of many quantum mechanical systems. This bound is usually not considered in the literature. Such a situation where the legitimate parties share classical information, with high but not 100% correlation and

with possibly some correlation to a third party is common to all quantum cryptosystems.

With the simplest error correction protocol, Alice randomly chooses pairs of bits and announces their XOR value (i.e. their sum modulo 2). Bob replies either "accept" if he has the same XOR value for his corresponding bits, or "reject" if not. In the first case, Alice and Bob keep the first bit of the pair and eliminate the second one, while in the second case they eliminate both bits. In reality, more complex and efficient algorithms are used. To lower the information between $I(A, E)$ Alice and Bob, Alice again randomly choses pairs of bits and computes their XOR value. But, contrary to error correction she does not announce this XOR value. She only announces which bits she chose (e.g. bit number 103 and 537). Alice and Bob then replace the two bits by their XOR value. In this way they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even lower. Consider for example that Eve knows only the value of the first bit, and nothing about the second one. Then she has no information at all on the XOR value.

Apart from performing naive measurements, Eve can be more subtle in her quest to gain information about the secret key. In fact, the only limits imposed on her are the ones imposed by the laws of quantum mechanics. The next section is to be a brief overview of the general eavesdropping strategies that Eve can take advantage of.

2.4 Eavesdropping

In order to be practical and secure, a QKD scheme must be based on existing technology, but its security must be guaranteed against an eavedropper with unlimited computing power whose technology is limited only by the laws of quantum mechanics. Although based on simple principles, the task of proving unconditional security in QKD is a very difficult one. Mayers was first to provide a version [May01] of the proof for the BB84 protocol and was quickly followed by Lo and Chau [LC99] and eventually by Shor and Preskill [SP00]. Although it is not the aim of this chapter to rederive the results of these proofs, we nevertheless dedicate a few paragraphs to illustrate the importance of security in QKD without any claim of mathematical rigor.

As we shall see, different techniques can be exploited by Eve in order to gain information on the true value of the qubits travelling from Alice to Bob. These techniques all have the same definite goal that is to estimate as accurately as possible the sequence

of bits generated by the two protagonists without them being aware of her. Obviously, these techniques must be quantum mechanical in nature because they must interact, at some point, with the aforementionned quantum states. Furthermore, in order to extract a maximum amount of information, Eve must also exploit the classical information exchanged by Alice and Bob. She can also exploit the imperfections arising from the source, the quantum channel and the detection apparatus. These several degrees of freedom can lead to many eavedropping problems which depend on both the given QKD protocol and the assumed fidelity of Alice and Bob's equipment.

The most studied classes of eavesropping fall into two categories: incoherent and coherent attacks. The idea of incoherent eavesdropping is for Eve to address each qubit individually. Furthermore, she can attach a probe of her choice (a quantum mechanical system in a dimension and initial state chosen by herself) to each individual qubit sent by Alice. She is free to choose the interaction between her probe and the qubit as long as it obeys the laws of quantum mechanics i.e. as long as the interaction is unitary. After the interaction is completed, she sends the state to Bob who performs his measurement. Once Alice and Bob have publicly declared their bases, she performs the measurment of her choice on the individual probes thus extracting some information concerning the values of the qubits. A coherent attack assumes that Eve collects a given fraction of the qubits sent by Alice and attaches a probe of her choice which interacts with the sequence of qubits. Again, after Alice and Bob's public discussion, Eve performs the measurement of her choice on the different probes she has accumulated.

It is possible to quantify and place bounds on the information that can be gained by Eve about the value of the qubits sent by Alice for a given eavesdropping strategy. However, we stress that it is still not known which of these two strategies is the most efficient one. Regardless, it still remains possible for Alice and Bob to extract a secret key with the appropriate privacy amplification protocols. We will now explore in further detail the implication of incoherent eavesdropping which is the simplest and most intuitive strategy and conclude by commenting on the other strategy.

2.4.1 Generalized incoherent attacks

We describe a general theory of incoherent eavesdropping attacks for the BB84 protocol. The idea is that Eve can attach individual probes to each qubit travelling from Alice to Bob. We suppose that the four possible states encountered by Eve are those

belonging to the B_Z and B_X bases. When intercepting a state, Eve attaches a probe $|\phi_E\rangle \in \mathcal{H}^{\otimes d}$ for which she is free to choose the dimension and the initial state. She then applies a unitary operation on the composite system consisting in the qubit and her probe:

$$\rho_{B,E}(\psi) = \mathcal{U}|\psi\rangle|\phi_E\rangle. \tag{2.16}$$

Finally, she sends the modified qubit state $\rho_B(\psi)$ to Bob while keeping the modified probe $\rho_E(\psi)$. Once the information concerning the basis has been made public, Eve will perhaps discard the state because it has been rejected by the protagonists and will therefore no longer be used. Otherwise she measures $\rho_E(\psi)$ in a basis which should yield the maximum information about $|\psi\rangle$. Her task is thus to optimize her choice of $|\phi_E\rangle$ and $\mathcal{U}$. Because she is unaware of the state of the qubit upon its receipt, Eve should require that its interaction with the probe be independent of its state[3]. By tracing off Eve's or Bob's respective subspaces, whe can examine in more detail what the other remains with. The density operator received by Bob can be expressed as:

$$\begin{aligned}\rho_B &= \mathrm{Tr}_E\ \rho_{B,E}(\psi) \\ &= \frac{\mathbb{1}}{2} + \frac{\eta_B}{2}(|\psi\rangle\langle\psi| - |\psi^\perp\rangle\langle\psi^\perp|) \\ &= F_B\ |\psi\rangle\langle\psi| + D_B\ |\psi^\perp\rangle\langle\psi^\perp|\end{aligned} \tag{2.17}$$

where $\eta_B \in [0,1]$ is the so-called "shrinking" factor. As we can see, the unitary operator $\mathcal{U}$ maps $|\psi\rangle$ onto a mixture of $|\psi\rangle$ and $|\psi^\perp\rangle$ such that with probability $F_B = \frac{1+\eta_B}{2}$ Bob will measure outcome $|\psi\rangle$ and with probability $D_B = \frac{1-\eta_B}{2}$ he will measure outcome $|\psi^\perp\rangle$. The shrinking factor is a constant and implies that all four states are shrunk the same amount. Conversely, after the interaction, Eve's probe $|\phi_E\rangle$ will be described in a similar way:

$$\begin{aligned}\rho_E &= \mathrm{Tr}_B\ \rho_{B,E}(\psi) \\ &= \frac{\mathbb{1}}{d} + \frac{\eta_E}{d}\left[|\phi(\psi)\rangle\langle\phi(\psi)| - \sum_{i=1}^{d-1} D_i|\phi_i^\perp(\psi)\rangle\langle\phi_i^\perp(\psi)|\right] \\ &= F_E\ \theta(\psi) + D_E\ \Gamma(\psi).\end{aligned} \tag{2.18}$$

Note that Eve's and Bob's density operators are completely characterized by their shrinking factor. Furthermore, it can be easily shown that the two shrinking factors η_B and η_E can be expressed as a function of the other but submitted to certain constraints imposed by the unitarity of $\mathcal{U}$. This relationship is intricately related to the

[3]This is a natural requirement given that all four states of the BB84 protocol are sent with equal probability.

no-cloning theorem which imposes a tradeoff between the values of η_B and η_E. In particular, both shrinking factors cannot simultaneously equal to 1 because Eve would gain all information concerning $|\psi\rangle$ (i.e. $F_E = 1$) while keeping Bob's QBER nul (i.e. $D_B = 0$).

Since Eve knows the basis in which $|\psi\rangle$ belongs to (assume it is B_X), she consequently knows her probe is in one of the following two mixed states:

$$\rho_E(+) = F_E\ \theta(+) + D_E\ \Gamma(+) \tag{2.19}$$
$$\rho_E(-) = F_E\ \theta(-) + D_E\ \Gamma(-). \tag{2.20}$$

It can be shown [GRTZ02] that the θ's generate a subspace orthogonal to the Γ's. Eve's optimum measurement in order to distinguish $\rho_E(+)$ from $\rho_E(-)$ thus consists in first distinguishing whether her state is in the subspace generated by $\theta_E(+)$ and $\theta_E(-)$ or the one generated by $\Gamma_E(+)$ and $\Gamma_E(-)$. This is possible since the two subspaces are mutually orthogonal. The former occurs with probability F_E while the latter with probability D_E. Once this discripancy has been made, Eve must then distinguish between the pure states $\theta_E(+)$ and $\theta_E(-)$ or $\Gamma_E(+)$ and $\Gamma_E(-)$ characterized by the following overlaps:

$$\theta_E^\dagger(+)\ \theta_E(-) = \cos x \tag{2.21}$$
$$\Gamma_E^\dagger(+)\ \Gamma_E(-) = \cos y. \tag{2.22}$$

The optimal measurement distinguishing two states with a given overlap $\cos x$ provides Eve with the correct guess with probability $\frac{1+\sin x}{2}$. We can now compute the mutual information between Alice and Eve knowing that the only *a priori* uncertainty surrounding $|\psi\rangle$ is its value, $H(E) = 1$. Therefore

$$I(A,E) = F_E[1 - H\Big(\frac{1+\sin x}{2}\Big)] + D_E[1 - H\Big(\frac{1+\sin y}{2}\Big)]. \tag{2.23}$$

Equation (2.23) is maximal when $x = y$. For a fixed QBER $D_E(\eta_E)$, the maximal information that can be gained is thus:

$$I_{\max}(A,E) = 1 - H\Big(\frac{1+\sin x}{2}\Big). \tag{2.24}$$

Bob's information depends only on the QBER induced by Eve's probing:

$$\begin{aligned} I(A,B) &= 1 - H(D_B) \\ &= 1 + F_B \log F_B + D_B \log D_B \end{aligned} \tag{2.25}$$

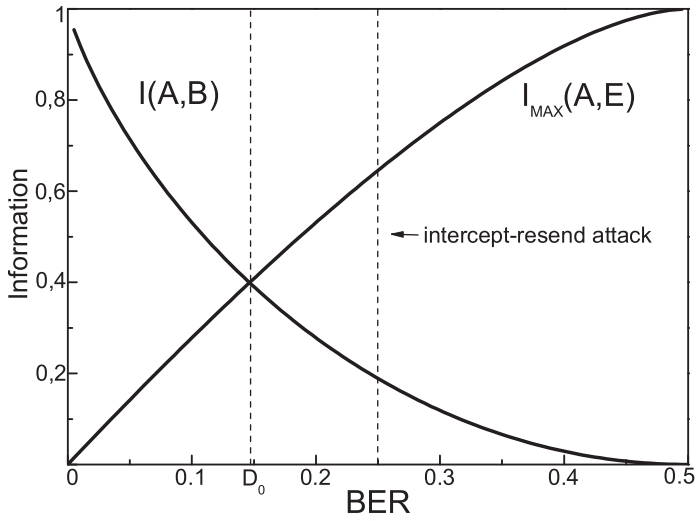

Figure 2.2: Incoherent eavesdropping for the BB84 protocol as function of Bob's BER.

Bob's and Eve's information curve are plotted on Fig. (2.2) as a function of Bob's error rate D_B. As expected, for low error rates, Bob's information is larger whereas more errors will provide Eve with more information at the expense of Bob's information. The information curves cross at the specific point $D_0 = \frac{1}{2}(1-\sqrt{2}) \simeq 15\%$. This bound is considered the critical limit at which Alice and Bob can extract a secret key because the necessary privacy amplification protocols are easy to implement. Furthermore, this bound happens to be the limit achievable by quantum cloning. That is, if Eve chooses to produce two clones of the incoming state (knowing the possible values it can take) with the highest achievable fidelity, it happens that the QBER she introduces is D_0 such that Bob receives:

$$|\psi\rangle \overset{\text{cloning}}{\longrightarrow} \rho_B = F_0\ |\psi\rangle\langle\psi| + D_0\ |\psi^{\perp}\rangle\langle\psi^{\perp}|. \tag{2.26}$$

Furthermore, the optimal information Eve gains for a QBER of D_0 is extracted from the probe (the second clone) which is described by exactly the same density operator, ρ_B. Such a cloning transformation where both clones have the same fidelity is called symmetric. It has been shown that such approximate cloning yields the security bounds for many QKD protocols. The concluding section of this chapter describes a simple cloning formalism that yields these optimal fidelities. This formalism will be used in other chapters of this thesis.

Another bound achieved through coherent attacks can be derived which is compatible with incoherent eavesdropping. This bound, $D_C = 11\%$, is precisely that obtained in the proof of Mayers and others. However, it is only valid if the key is much longer than

the number of qubits that Eve attacks coherently. The D_0 bound is a necessary one since, as we have seen, an explicit eavesdropping strategy exists contrary to coherent attacks. It is not known what happens in the intermediate range $11\% < D_0$.

2.4.2 Photon number splitting attacks

The implementation of a QKD protocol relies on technology available at present day. Consequently, this gives rise to imperfections which cannot be ignored when considering unconditional security. Every component exploited by Alice and Bob in order to perform secure QKD must be thouroughly examined and studied in order to avoid undetected eavesdropping.

As will become clearer in the next chapter, today's practical QKD relies on photon encoded qubits. In accordance with the theory described above, a qubit should be encoded in two-dimensional Hilbert space. There exist several photon degrees of freedom which support two-dimensional Hilbert space such as the polarization of the electric field. However, single photon sources are at present day not available commercially although quasi-deterministic sources exist in many laboratories [SFV+02]. As a temporary solution a photonic qubit is produced from an attenuated laser pulse. The problem with this solution is that the light-beam produced by a laser actually consists in a mixture of photon number states called Fock states. Such a quantum system is referred to as a *coherent state* and is expressed as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.27}$$

where $|\alpha|^2$ is the average photon number and $|n\rangle$ is a n-photon energy eigenstate . A direct consequence of this state is the impossibility to prepare a light pulse containing exactly one photon. Indeed, if the average photon number $|\alpha|^2 = 1$, we readily see that the probability of the state containing more than one photon is non-zero. In fact, the probability distribution is Poissonian:

$$P(n) = e^{-<n>} \frac{< n >^n}{n}. \tag{2.28}$$

Therefore if Alice encodes a qubit using an attenuated coherent state (which itself is just a weaker coherent state), mimicking a single photon, she will have a non-zero probability of sending two or more replicas of the same qubit. More importantly, Eve can exploit this flaw by performing a so-called non-demolition measurement (possible with linear optics and ancillary photons) which descriminates the number of photons

contained within the pulse without destroying the photons. If she concludes that the state contains more than one photon, she keeps one and sends the others on to Bob otherwise she does nothing. One can easily conclude that if the average photon number is too high, Eve can gain complete information on the secret key without having Alice nor Bob notice.

Without getting further into details, we state that this attack poses no threat as long as the average photon number is low , that is, as long as the probability of having more than one photon per pulse is negligible and that the distance seperating Alice and Bob is short. Specifically, if the average photon number is of the order of $0,1$ photon, one can prove that Alice and Bob can still generate a secret key. Note however that this low average reduces the generation rate since it increases the probability that the pulse contains no photon at all.

2.4.3 Beyond the BB84 paradigm: the six-state protocol

There exist many other QKD protocols. For example, an obvious extension of the BB84 protocol can be constructed once it has been understood that two-dimensional Hilbert space contains *three* M.U. bases [BM02]. Indeed, recall that the security of the BB84 protocol relies partly on the incompatibility of two M.U. bases. That is, the linearity of quantum mechanics does not allow one to distinguish between states belonging to two M.U. bases. This linearity also applies to three M.U. bases. In fact, it is an even harder task for Eve to distinguish three M.U. bases from two. Therefore Alice choosing to communicate with Bob using states belonging to the following three M.U. bases: B_Z, B_X and $B_Y = \{\frac{1}{\sqrt{2}}\big(|0\rangle \pm i|1\rangle\big)\}$ (to which we also associate binary values) will render Eve substantially more visible because she will introduce a higher QBER [BPG99]. Indeed, a similar analysis as the one performed for the BB84 protocol in the case of incoherent eavesdropping yields a lower fidelity of $F_6 = \frac{5}{6} < F_4$. However, the a priori probability distribution that Alice and Bob use the same basis is reduced to $1/3$, which means that they have to discard $2/3$ of the transmitted qubits before they can extract a cryptographic key thus slowing the rate at which it is created.

Although the six-state protocol is the only other QKD protocol that will be considered in this thesis, we nevertheless mention that other interesting and practical variants exist. The B92 [Ben92] is arguably the simplest QKD protocol because it

requires only two non-orthogonal (and therefore partly indistinguishable) states. The Ekert protocol [Eke91] exploits the non-local correlations that exist within so-called *entangled* quantum states. Finally, let us also mention the continuous variable protocol [] which exploits the incompatibility of two continuous observables such as the quadratures of the electromagnetic field.

2.5 Pauli Cloning Machines

A direct consequence of the seminal papers by Wooters, Zurek and Dieks was the introduction to the notion of approximate quantum cloning. By proving the no-cloning theorem, they opened a whole new facet as to how quantum information can be transfered and manipulated. Indeed, more than 10 years after the discovery of the no-cloning theorem, Buzek and Hillary became the first to ask the simple but very relevant question: "If quantum mechanics prohibits perfect quantum cloning then how close does it allow us to get?" They answered their question by showing the existence of a "universal quantum cloning machine" (UQCM) -i.e., a transformation which approximately copies arbitrary quantum states such that the fidelity of the output clones does not depend on the input state. It was in fact later shown to be optimal by Bruss *et al* in [] and Gisin and Massar in [GM97].

Approximate quantum cloning machines have since been thouroughly studied especially in the context of QKD. A typical feature of quantum cloning is that the optimal cloning transformation depend on the considered set of input states. The greater the set, the lower the fidelity. This is reflected in the performance of different QKD schemes. For example, the six-state protocol allows a much higher BER than the BB84 protocol. The reason is that the optimal quantum cloning machine (QCM) Eve could use for the latter is in fact less performing than the optimal QCM for the former since the set of states for the six-state protocol is bigger.

In this thesis we will study different aspects of quantum cloning thus relating the subject to QKD, entanglement and information transfer . More specifically, in Chapter 5 we will be interested in modified versions of the BB84 and six-state protocols which reduce the need for random numbers. As we shall see, this will be done by encoding successive states chosen in the same basis. We will show that the optimal cloning strategy for Eve still remains the cloning strategies of the standard BB84 and six-state protocols and conclude that Eve can not gain more information than in these standard counterparts. Chapter 10 will be devoted to the cloning of entanglement.

We will raise the question of whether quantum entanglement itself can be cloned or not. More specifically, we will show that it is possible to clone part of the original entanglement, much in the same way that quantum states can be cloned imperfectly. Finally, in Chapter 11, we will analyze QCMs that duplicate with an equal fidelity all uniform d-dimensional superposition states with arbitrary phases. We will apply our results to asymmetric cloners and analyze the balance between the fidelity of the two clones.

Although many methods exist in order to derive the optimal cloners, they are often quite complicated and not very intuitive. However, in chapters 5, 10 and 11 we will use a convenient cloning formalism (derived in [Cer98, Cer00] and summarized below) such that after aplying the cloning transformation, the clones are left in a mixture of the input state itself and states resulting from applying operators of the discrete Weyl group (also called "error" operators) on an input state. This formalism is designed for the special case of $1 \rightarrow 2$ quantum cloning. Specifically, if we consider a 2-dimensional[4] input state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ then after the cloning transformation the two output clones A and B are given in a mixture of the states $|\psi_{m,n}\rangle = U_{m,n}|\psi\rangle$:

$$\begin{aligned} \rho_A &= \sum_{m,n=0}^{1} |a_{m,n}|^2 \ |\psi_{m,n}\rangle\langle\psi_{m,n}| \\ \rho_B &= \sum_{m,n=0}^{1} |b_{m,n}|^2 \ |\psi_{m,n}\rangle\langle\psi_{m,n}|. \end{aligned} \tag{2.29}$$

The unitary $U_{m,n}$ operator can be viewed as an *error* operator that alters state $|\psi\rangle$ as:

$$U_{m,n} = \sum_{k=0}^{1} e^{2\pi i(\frac{kn}{2})}|k + m \bmod 2\rangle\langle k|. \tag{2.30}$$

In other words, $U_{m,n}$ shifts $|\psi\rangle$ by m units modulo 2 in the computational basis, and multiplies it by a phase so as to shift its Fourier transform by n units modulo 2. In 2-dimensional Hilbert space the error operators corespond to the identity and the Pauli matrices: three Pauli matrices:

$$\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{2.31}$$

$$\begin{aligned} U_{0,0} &= \mathbb{1} \qquad & U_{0,1} &= \sigma_Z \\ U_{1,0} &= \sigma_X \qquad & U_{1,1} &= \sigma_Z\sigma_X = -i\sigma_Y. \end{aligned} \tag{2.32}$$

[4]Note that, this formalism can easily be extended to $d > 2$ dimensional Hilbert space.

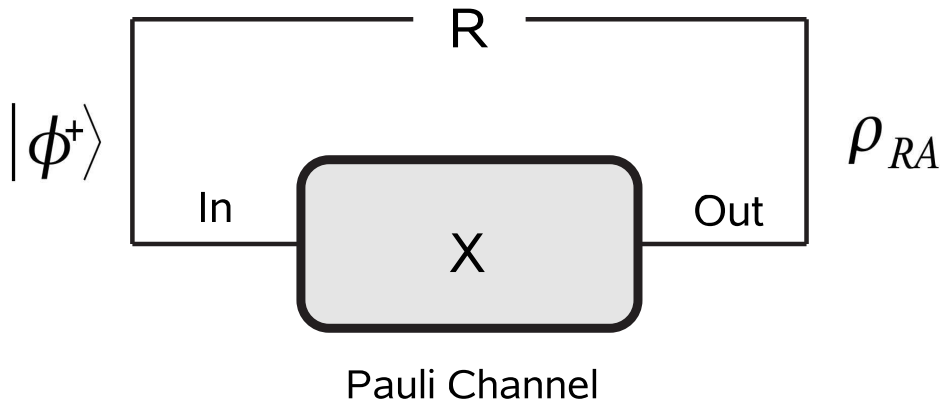

Figure 2.3: A Pauli channel processing subsystem X of the ME pair $|\phi^+\rangle$.

In other words, this class of transformation will map a qubit onto two clones each in a mixture of the unchanged qubit, the qubit having underwent a phase flip, the qubit having underwent a bit flip, or a combination of both. Since the no-cloning theorem prohibits perfect cloning, it implies that the weights $|a_{0,0}|^2$ and $|b_{0,0}|^2$ cannot simultaneously equal 1 because in that would imply perfect cloning. To understand the duality that exists between the $a_{m,n}$ and $b_{m,n}$ amplitude functions at the limit of what the no-cloning theorem allows and to measure the optimal fidelities that can be achieved, we now describe the class of cloning transformations which actually produce the clones characterized by Eq. (2.29)

We start off by considering a normalized arbitrary qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ with complex coefficients which we process through a Pauli channel. A Pauli channel has the particularity that at its output A, $|\psi\rangle$ will be described by a mixture of the four error operators $\{\mathbb{1}, \sigma_Z, \sigma_X, -i\sigma_Y\}$ acting on $|\psi\rangle$ to which we associate weights $\{(1-p), p_Z, p_X, p_Y\}$ respectively and where $p = 1 - p_Z - p_X - p_Y$:

$$|\psi\rangle \rightarrow \rho_A = (1-p)|\psi\rangle\langle\psi| + p_Z\sigma_Z|\psi\rangle\langle\psi|\sigma_Z + p_X\sigma_X|\psi\rangle\langle\psi|\sigma_X + p_Y\sigma_Y|\psi\rangle\langle\psi|\sigma_Y. \quad (2.33)$$

Another way to describe the transformation of state $|\psi\rangle$ after its passing through the Pauli channel is to suppose that an input qubit X, ME with a reference qubit R, is processed through the channel while $|R\rangle$ remains unchanged, see Fig. 2.3. Let X and R together form the ME Bell state $|\phi^+\rangle = 2^{-1/2}(|0\rangle_R|0\rangle_X + |1\rangle_R|1\rangle_X)$. A remarkable feature of entanglement is that any local operation on a subsystem of a ME state (e.g. the pauli channel operating locally on X) will map it onto another ME state. Furthermore, if this local operation turns out to be one of the three Pauli matrices,

$|\phi^+\rangle$ is mapped onto one of its three ME orthogonal Bell states:

$$\mathbb{1}_R \otimes \sigma_Z^X |\phi^+\rangle = |\phi^-\rangle_{RA} \tag{2.34}$$

$$\mathbb{1}_R \otimes \sigma_X^X |\phi^+\rangle = |\psi^+\rangle_{RA} \tag{2.35}$$

$$\mathbb{1}_R \otimes -i\sigma_Y^X |\phi^+\rangle = |\psi^-\rangle_{RA}. \tag{2.36}$$

Consequently, once the Pauli channel has operated on X, $|\phi^+\rangle$ ends up in a mixture of the four Bell states:

$$\rho_{RA} = \left[(1-p)|\phi^+\rangle\langle\phi^+| + p_Z|\phi^-\rangle\langle\phi^-| + p_X|\psi^+\rangle\langle\psi^+| + p_Z|\psi^-\rangle\langle\psi^-|\right]_{RA}. \tag{2.37}$$

Note that this mixture uniquely characterizes the Pauli channel since the four weights are simply those associated to the four error operators. Therefore, in order to describe the action of the Pauli channel on the arbitrary qubit $|\psi\rangle$, one must simply project the reference system $|R\rangle$ onto $|\psi^*\rangle = \alpha_0^*|0\rangle + \alpha_1^*|1\rangle$:

$$\begin{aligned} |\psi\rangle \rightarrow \rho_A &= (\langle\psi_R^*| \otimes \mathbb{1}_A)\rho_{RA}(\mathbb{1}_A \otimes |\psi_R^*\rangle) \\ &= (1-p)|\psi\rangle\langle\psi| + \sum_{i=1}^{3} p_i\sigma_i|\psi\rangle\langle\psi|\sigma_i \end{aligned} \tag{2.38}$$

where σ_i represents the three pauli operators with their associated weights p_i. A special case arises when $p_Z = p_X = p_Y = p/3$ which describes a *depolarizing* channel:

$$|\psi\rangle \rightarrow \rho_A = (1-4p/3)|\psi\rangle\langle\psi| + 4p/3\frac{\mathbb{1}}{2}. \tag{2.39}$$

The fidelity of $|\psi\rangle$ which has been acted by such a channel is

$$\begin{aligned} f &= \langle\psi|\rho_A|\psi\rangle \\ &= 1 - \frac{2p}{3}. \end{aligned} \tag{2.40}$$

Note how this particular channel is state independent: the fidelity of the output density matrix is constant for all values of α_0 and α_1. Take another channel, this time state dependent where $p_Z = p$ and $p_X = p_Y = 0$. In this case, $|\psi\rangle$ is mapped onto

$$|\psi\rangle \rightarrow \rho_A = (1-p)|\psi\rangle\langle\psi| + p\sigma_Z|\psi\rangle\langle\psi|\sigma_Z. \tag{2.41}$$

We label this channel a *dephasing* channel because with probability p the state is rotated along the z axis and with probability $(1-p)$ it remains unchanged. In comparaison to the previous, depolarizing channel, this channel is state dependent which implies that different states will exit with different fidelities:

$$\begin{aligned} f &= \langle\psi|\rho_A|\psi\rangle \\ &= |\alpha_0|^2. \end{aligned} \tag{2.42}$$

For example, we see that states $|0\rangle$ and $|1\rangle$ are left unchanged while states $2^{-1/2}(|0\rangle \pm |1\rangle)$ exit completely mixed. As we shall see, the main concept behind Pauli cloning is to use Pauli channels with weights p_i adapted for the set of states we would like to clone. The universal cloner - the cloner that optimally clones all states on the Bloch sphere - for example will be implemented with depolarizing Pauli channels because all states are affected the same way.

The idea is the following. We begin with the ME state $|\phi^+\rangle$ again consisting of subsystems R and X. We define our Pauli cloner as a cloner which outputs three density matrices, ρ_{RA}, ρ_{RB} and, ρ_{RC} where output subsystems A, B and, C are entangled with reference subsystem R. More specifically, we will construct the cloner in such a way that all three outputs ρ_{RA}, ρ_{RB} and, ρ_{RC} be mixtures of Bell states each with their own respective set of weights. Systems A and B will consist in the two clones whilst qubit C will consist in an extra ancillary system which, as we shall see, is necessary in the construction of the cloner but is discarded in the end.

To achieve such a cloner we first remark that in order to purify the 4-dimensional systems ρ_{RA} or ρ_{RB} it is necessary to attach a system which has the same state space as these two density matrices, that is, a system spanning 4-dimensional Hilbert space. We can define a 16-dimensional pure state for the combined system $|\psi_{RABC}\rangle$ such that tracing over subsystems B and C, A and C or A and B reduces to either ρ_{RA}, ρ_{RB} or ρ_{RC}, respectively. Indeed, suppose ρ_{RA} has orthonormal decomposition $\rho_{RA} = \sum_{i=0}^{3} p_i |i_{RA}\rangle\langle i_{RA}|$. To purify ρ_{RA} we introduce a system ρ_{BC} which has the same dimension as system RA, with orthonormal basis states $|i_{BC}\rangle$, and define a pure state for the combined system

$$|\psi\rangle_{RABC} = \sum_{i=0}^{3} \sqrt{p_i}|i\rangle_{RA}|i\rangle_{BC}. \tag{2.43}$$

We can now calculate the density operator for system RA corresponding to the state $|\psi\rangle_{RABC}$:

$$\begin{aligned} \mathrm{Tr}_{BC}|\psi\rangle_{RABC}\langle\psi| &= \sum_{i,j=0}^{3} \sqrt{p_i p_j}|i_{RA}\rangle\langle j_{RA}|\mathrm{Tr}\big(|i_{BC}\rangle\langle j_{BC}|\big) \\ &= \sum_{i,j=0}^{3} \sqrt{p_i p_j}|i_{RA}\rangle\langle j_{RA}|\delta_{i,j} \\ &= \rho_{RA}. \end{aligned} \tag{2.44}$$

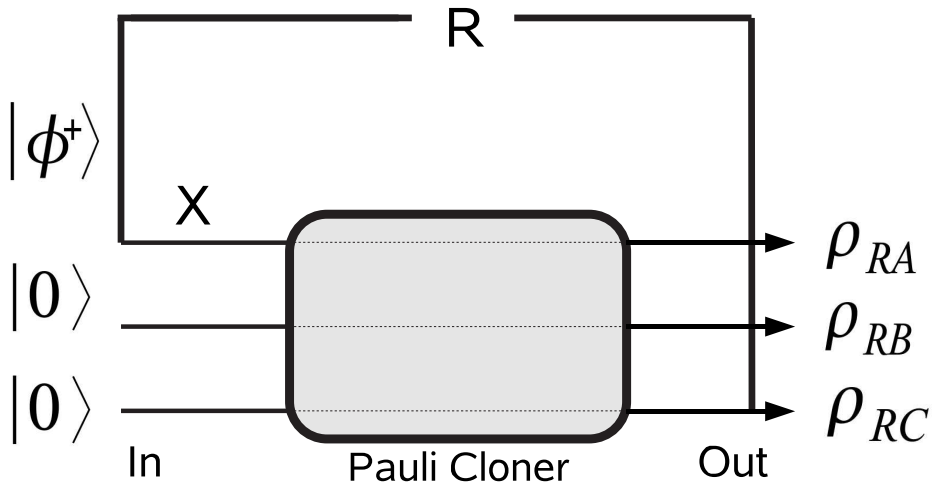

Figure 2.4: A Pauli cloner with output subsystems RA, RB and RC. Outputs A and B consist in the two clones whilst C consists of an ancillary system that can be discarded.

Thus, $|\psi\rangle_{RABC}$ is a purification of ρ_{RA} [NC00]. A similar procedure can be done for ρ_{RB} by introducing the 4-dimensional system ρ_{AC}. As we can see, subsystem C is solely needed in order to purify ρ_{RA} and ρ_{RB}. Now, instead of specifying a Pauli cloning machine by a particular unitary transformation acting on input state $|\psi\rangle$ (the state we would like to clone) we rather characterize the Pauli cloner by the wave function $|\psi_{RABC}\rangle$ underlying the entanglement of the outputs A and B with R. To do so, we introduce the 16-dimensional input system $|\phi^+\rangle_{RX}|0\rangle_B|0\rangle_C$ of which subsystems X, $|0\rangle_B$ and $|0\rangle_C$ are processed in a Pauli cloner which in fact consists of three distinct Pauli channels (see Fig. 2.4). Therefore $|\phi^+\rangle_{RX}|0\rangle_B|0\rangle_C$ is mapped to $|\psi_{RABC}\rangle$ where

$$|\psi\rangle_{RABC} = \frac{1}{\sqrt{2}}|0\rangle_R \sum_{i,j,k=0}^{3} \Omega_{ijk}\sigma_i|0\rangle_A\sigma_j|0\rangle_B\sigma_k|0\rangle_C + \frac{1}{\sqrt{2}}|1\rangle_R \sum_{i,j,k=0}^{3} \Omega_{ijk}\sigma_i|1\rangle_A\sigma_j|0\rangle_B\sigma_k|0\rangle_C$$

which can conveniently be rewritten in the form of equation Eq. (2.43) by using the Schmidt decomposition [Sch06]:

$$|\psi_{RABC}\rangle = \{a_{0,0}|\phi^+\rangle|\phi^+\rangle + a_{0,1}|\phi^-\rangle|\phi^-\rangle + a_{1,0}|\psi^+\rangle|\psi^+\rangle + a_{1,1}|\psi^-\rangle|\psi^-\rangle\}_{RA;BC}. \quad (2.45)$$

The requirement that the qubit pairs RA and BC are Bell mixtures is thus satisfied, that is, $\rho_{RA} = \rho_{BC}$ is of the form of Eq. (2.37) with $p_Z = |\alpha_{0,1}|^2$, $p_X = |\alpha_{1,0}|^2$,

$p_Y = |\alpha_{1,1}|^2$ and, $(1-p) = |\alpha_{0,0}|^2$. A remarkable feature of these double Bell states is that they transform into superpositions of double Bell states for the two remaining partitions of the four qubits $RABC$ into two pairs (RB vs. AC, RC vs. AB). This implies that $|\psi\rangle_{RABC}$ is also a superposition of double Bell states (albeit with different amplitudes) for these two partitions, which, threfore, also yield mixtures of Bell states when tracing over half of the system. Specifically, for the partition RB vs. AC, we obtain

$$|\psi_{RABC}\rangle = \{b_{0,0}|\phi^+\rangle|\phi^+\rangle + b_{0,1}|\phi^-\rangle|\phi^-\rangle + b_{1,0}|\psi^+\rangle|\psi^+\rangle + b_{1,1}|\psi^-\rangle|\psi^-\rangle\}_{RB;AC} \quad (2.46)$$

where

$$\begin{aligned} b_{0,0} &= \tfrac{1}{2}(a_{0,0} + a_{0,1} + a_{1,0} + a_{1,1}) \\ b_{0,1} &= \tfrac{1}{2}(a_{0,0} + a_{0,1} - a_{1,0} - a_{1,1}) \\ b_{1,0} &= \tfrac{1}{2}(a_{0,0} - a_{0,1} + a_{1,0} - a_{1,1}) \\ b_{1,1} &= \tfrac{1}{2}(a_{0,0} - a_{0,1} - a_{1,0} + a_{1,1}). \end{aligned} \quad (2.47)$$

Similarly, the third output C is described by considering partitions RC vs. AB,

$$|\psi_{RABC}\rangle = \{c_{0,0}|\phi^+\rangle|\phi^+\rangle + c_{0,1}|\phi^-\rangle|\phi^-\rangle + c_{1,0}|\psi^+\rangle|\psi^+\rangle + c_{1,1}|\psi^-\rangle|\psi^-\rangle\}_{RC;AB} \quad (2.48)$$

where

$$\begin{aligned} c_{0,0} &= \tfrac{1}{2}(a_{0,0} + a_{0,1} + a_{1,0} - a_{1,1}) \\ c_{0,1} &= \tfrac{1}{2}(a_{0,0} + a_{0,1} - a_{1,0} + a_{1,1}) \\ c_{1,0} &= \tfrac{1}{2}(a_{0,0} - a_{0,1} + a_{1,0} + a_{1,1}) \\ c_{1,1} &= \tfrac{1}{2}(a_{0,0} - a_{0,1} - a_{1,0} - a_{1,1}). \end{aligned} \quad (2.49)$$

Thus Eqs. (2.47) and (2.49) relate the amplitudes of the double Bell states for the three possible partitions of the four qubits into two pairs, and thereby specify the entire set of asymmetric Pauli cloners considered here. Of particular interest, is the relation that exists between the amplitude coefficients of output clones A and B. A closer look at Eq. (2.48) enables one to conclude that the amplitudes are simply related by a 2-dimensional Fourier transform:

$$b_{m,n} = \frac{1}{2}\sum_{x,y=0}^{1}(-1)^{nx+my}a_{x,y}. \quad (2.50)$$

It is clear from Eq. (2.50) that when output A is perfect ($a_{0,0} = 1$) output B becomes completely mixed ($b_{m,n} = \frac{1}{2}$) and vice versa. Consequently, the probability distributions characterizing the channels leading to outputs A and B cannot have a variance

simultaneously tending to zero, giving rise to an uncertainty principle governing the trade-off between the quality of the copies.

The construction we have developed is very useful because one can easily express the output state resulting from cloning an arbitrary input state $|\psi\rangle$ simply by projecting the reference system R onto an appropriate state. Indeed, before cloning, projecting R onto state $|\psi^*\rangle$ amounts to project the input system onto $|\psi\rangle$ since these two systems are in state $|\phi^+\rangle$. Therefore, as this projection of R onto $|\psi^*\rangle$ can as well be performed after cloning, it is easy to write the restulting joint state of the two clones and the ancillary system C when the input state is $|\psi\rangle$:

$$\begin{aligned} |\phi^+\rangle_{RX}|0\rangle_B|0\rangle_C &\rightarrow \langle\psi_R^*||\psi_{RABC}\rangle \\ &= \sum_{m,n=0}^{1} a_{m,n}U_{m,n}|\psi\rangle_A|B_{m,n}\rangle_{BC} \\ &= \sum_{m,n=0}^{1} b_{m,n}U_{m,n}|\psi\rangle_A|B_{m,n}\rangle_{AC} \end{aligned} \tag{2.51}$$

It is easy to check that tracing over systems B and C or A and C yields the expected final states of clone A or B, in accordance with Eq. (2.29). Thus, the four amplitudes $a_{m,n}$ completely define the state after cloning, Eq. (9.4), so they completely characterize the class of cloning transformations of interest here.

The cloning fidelity can be calculated based on the amplitude coefficients $a_{m,n}$ (and $b_{m,n}$). The fidelity of the clone A when copying state $|\psi\rangle$ can be written, in general, as

$$\begin{aligned} F_A &= \langle\psi|\rho_A|\psi\rangle \\ &= \sum_{m,n=0}^{1} |a_{m,n}|^2|\langle\psi|\psi_{m,n}\rangle|^2 \end{aligned} \tag{2.52}$$

and similarly for the second clone B. In order to find the optimal fidelity for a given set of input states, one simply needs to calculate the value of the fidelity for each input state of the set and maximize under the constraint of normalization and, if symmetry is imposed, the constraint that both output clones yield the same fidelity. As mentionned above, this double-Bell state ansatz has been shown to yield the optimal fidelity in many cases [CDPC05]. However, only recently has a general proof been provided thus sheding light on the appearance of the double-Bell states in the optimal $1 \rightarrow 2$ cloning machines [].

2.6 Conclusion

This concludes our introduction to the BB84 protocol and the necessary tools which will be needed in the rest of this thesis. Because this thesis is just as much oriented towards experimental quantum cryptographic protocols, we will now introduce a convenient method to implement certain quantum information tasks such as QKD. The idea is to encode quantum information in a single photon using linear optical components. We will convince the reader that this method is robust and stable by illustrating the original implementation of a quantum algorithm.

Chapter 3

Experimental Quantum Information Processing

3.1 Introduction

Now that the concept of QKD has been introduced and that its building blocks have been laid out, we can proceed to describe the more practical aspects of QKD. There exist numerous methods that implement QKD protocols and quantum algorithms. In principle, one is limited only by the notion that quantum information carriers should obey the laws of quantum mechanics. In practise however, the choice should meet certain criterions that limit the number of possible alternatives. In particular, the carriers should be implemented by robust physical systems that can retain their quantum properties over long distances. The system should also be chosen for its capability to prepare a specified set of states and to perform a specified unitary transformations. This requirement is much more difficult to fulfill when one wants to carry out quantum computational tasks because a universal set of states and a universal familly of unitary transformations are required. In contrast, only the preparation of a small set of states is necesseray in order to perform QKD. Finally, measuring the output result should be easy and efficient.

Many physical systems partially meet the above requirements but it seems that optical photons be a natural choice for QKD. The main motivations being that photons can propagate over (relatively) long distances, interact very ligthly with their environment, and that today's telecommunications community provides a wide range of inexpensive devices that can address all photon degrees of freedom.

Once the medium is fixed, there remain the questions of the source and detectors. Since they have to be compatible, the crucial choice is the wavelength. Two alternatives are possible. The first implies using a source around 800 nm for which there exist very efficient detectors ($\sim$ 80% quantum efficiency[1]). The second alternative implies using a source at 1,55 μm for which less efficient detectors exist ($\sim$ 10% quantum efficiency) but compatible with today's telecommunication optical fibers. The reason why today's telecommunication technology relies on infrared sources is because the attenuation in optical fibers is lowest at this wavelength. At 800 nm, the best fibers attenuate about 2 dB/km. This implies that in 1.5 km a photon travelling in such a fiber will have 50% chances of being lost. Conversely, at 1,55 μm, the best fibers attenuate on the order of 0.2 dB/km meaning that a photon can travel 15 km before having 50% chances of being lost. These losses are nearly entirely due to Rayleigh scattering such that the above bounds are imposed by the laws of physics, not technological limitations.

The next consideration concerns the degree of freedom in which the quantum information should be encoded. A photon contains a few candidates such as polarization, phase, position and momentum. In this chapter, we introduce an encoding method in time. The method is dubbed "plug and play" [GHM+97]. This method is, at present day, an excellent method for encoding quantum information for cryptographic purposes because it requires very little alignment - it relies on guided optics components - and can remain stable for days. We first explain this method and then illustrate its potential by describing an original implementation of a simple quantum algorithm.

3.2 The plug and play method

3.2.1 Time bin encoding

One of the central ideas behind plug and play quantum processing is to encode information in time bins by splitting a single photon in an unbalanced Mach-Zehnder (MZ) interferometer. Such a device consists in a semi-transparent mirror (i.e. beam-splitter or, in terms of optical fibers, a coupler) of transmittivity $|t|^2 = \frac{1}{2}$ connected to both input arms (A_0 and A_1) of the interferometer of path length difference $d = t_0 - t_1$. Typically this length is of the order of a few meters in accordance with the temporal

[1] By quantum efficiency, we mean the fraction of photons hitting the photoreactive surface of the detector and subsequently being recognized by it.

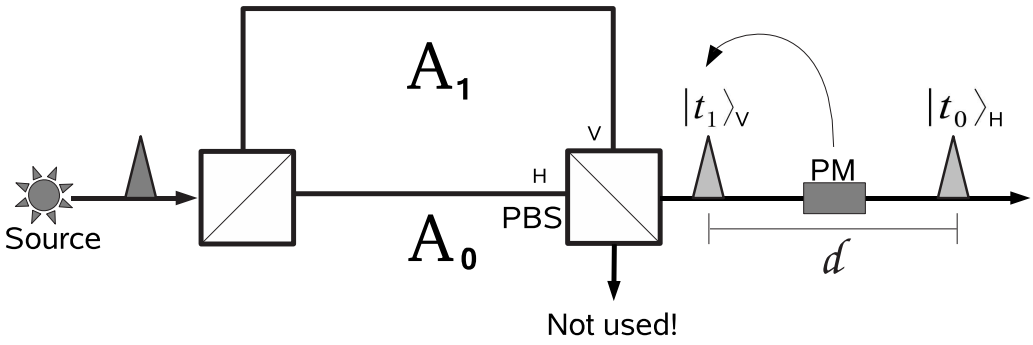

Figure 3.1: An unbalanced MZ interferometer that prepares a time bin encoded quantum state. The single photon impinges on the first beam-splitter and propagates with equal amplitudes $\frac{1}{\sqrt{2}}$ through the two arms A_0 and A_1. The wave packets then exit through the same output port of the PBS by turning the respective polarization. Finally, the qubit is encoded by addressing the phase of the second wave packet $|t_1\rangle_V$ with the phase modulator PM.

resolution of the optical apparatus (note that 20 cm $\simeq$ 1 ns in silica[2]). The single photon is thus divided in two wave packets each travelling down its own respective path. The two arms eventually recombine at a second beam-splitter where the two wave packets arrive seperated by d nanoseconds (i.e. they impinge on the beam-splitter at different times and therefore do not interfere). Either by using a polarization sensitive beam-splitter (PBS) or an optical switch, it is possible to deterministically direct both wave packets in the same output port of the beam-splitter. The first solution is easy to implement. One must simply tune the polarization of each wave packet in the two arms of the interferometer such that when impinging on the PBS, the wavepackets exit through the same output port, see Fig. 3.1. The second alternative is not possible because present day technology delivers only high insertion loss optical switches not suitable for the single photon regime. One could also use a simple beam-splitter exactly like the one at the entrance of the MZ interferometer. However, this method induces a systematic loss of $\frac{1}{2}$. For the sake of completeness, we will assume that the second beam-splitter is in fact a PBS whose eigenstates are horizontal (H) and vertical (V) polarization. In order to exit through the same output port the wavepacket travelling through A_0 should impinge on the PBS with H polarization and the wave packet travelling through A_1 sould impinge with V polarization.

[2]Here and throughout this thesis we express distance in terms of time units rather than length units for its correspondance with optical apparatus. The two quantities are simply related by the speed of light, c_s, in optical fibers.

Thus, at the output of the MZ interferometer we have two orthogonal wavepackets which we label $|t_0\rangle_H$ and $|t_1\rangle_V$ for their association to the two arms of the interferometer and their respective polarization. The output state, which we label $|-\rangle$, can be seen as an eigenstate of the interferometer and expresses the uniform superposition of the photon having taken both paths:

$$|-\rangle = \frac{1}{\sqrt{2}}\big[|t_0\rangle_H - |t_1\rangle_V\big]. \tag{3.1}$$

The minus sign results from the two reflections that $|t_1\rangle_V$ has been subjected to. Each reflection is responsible for the accumulation of an $e^{i\frac{\pi}{2}} = i$ phase. A closer inspection of beam-splitter dynamics shows that this convention is necessary to satisfy energy conservation[3]. The plug-and-play method enables one to encode quantum information through the relative phase contained between the two time bins. The phase difference that appears at the output of the interferometer fixes the reference frame and should be taken into consideration for all successive operations and measurements. To encode information it is necessary to introduce a parameter, $\phi \in [0, 2\pi]$, which defines the dephasing between $|t_0\rangle_H$ and $|t_1\rangle_V$ with respect to the reference frame:

$$\begin{aligned} |\psi\rangle &= U_\phi|-\rangle \\ &= \frac{1}{\sqrt{2}}\big[|t_0\rangle_H - e^{i\phi}|t_1\rangle_V\big] \end{aligned} \tag{3.2}$$

where the unitary operator U_ϕ is expressed as:

$$U_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

The set of states prepared by this encoding method is limited because of the fixed value of the beam-splitter transmittance. Only those with a uniform amplitude distribution but with arbitrary phase can be implemented. Using a variable transmittance beam-splitter however, one could in principle prepare all states in 2-dimensional Hilbert space. Nevertheless, we shall see that this limited set of states is sufficient for performing many quantum information tasks including QKD.

In order to achieve the state described by Eq. (3.2) all that is needed is an optical retarder that addresses only one of the two wave packets. Physically, such a retarder,

[3]In fact, Fresnel's law of reflection predicts this phase shift if the dielectric constant n_M of the reflecting medium is higher than the dielectric constant of optical fiber n_s.

commonly called a phase modulator (PM), is any device that can retard a photon on the order of its wavelength. In the experiments described in the subsequent chapters the phase modulator we use is a simple crystal (of length ~ 5 cm) to which is applied a potential typically of the order of a few Volts. The crystal is placed on the fiber optic line and the potential can be switched on and off rapidly enough to address only one wave packet. The applied potential modifies the index of refraction of the crystal and thus retards the wave packet subjected to it. The dephasing is proportional to the crystal length and the crystal's index of refraction which itself is proportional to the applied potential. Because both time bins travel through the crystal, the dephasing occurs only when the potential is applied to the subjected wave packet. This last procedure completes the time bin encoding. It can then be sent for further processing depending on the task it must fulfill.

Measuring a time-encoded quantum state is made by using a MZ interferometer which has the exact same properties as the one described above. The idea is the following. We suppose that the first beam-splitter of the interferometer is in fact a PBS which is configured such that it deterministically directs time bin $|t_0\rangle_H$ into arm A_1 while the late time bin, $|t_1\rangle_V$, into arm A_0 (we show below that this is done automatically with the help of a Faraday mirror). By doing so, each time bin travels a distance that eventually compensates the delay, d, between them. At exactly that moment both time bins impinge together on the second beam-splitter and interfere. The phase difference $e^{i\phi}$ determines which output of the beam-splitter the photon will take. Each output is connected to a single photon detector (M_0 and M_1) thus completing the measurement (see Fig. 3.2). We can compute the probability that the photon exits through either output ports. Because both interferometers have exactly the same properties, the basis in which the photon is measured is the same as the one preparing the state, that is, $\{|\mp\rangle\}$. The probabilities are given by:

$$P(M_0) = \tfrac{1}{2} + \tfrac{1}{2}\cos\phi \qquad P(M_1) = \tfrac{1}{2} - \tfrac{1}{2}\cos\phi. \tag{3.3}$$

We illustrate this useful result in Fig. (3.3). Note that when measuring eigenstates of σ_Y ($\phi = \frac{\pi}{2}$):

$$|+^i\rangle = \tfrac{1}{\sqrt{2}}[|t_0\rangle_H + i|t_1\rangle_V] \qquad |-^i\rangle = \tfrac{1}{\sqrt{2}}[|t_0\rangle_H - i|t_1\rangle_V],$$

the probability of detecting the photon is uniform: $P(M_0) = P(M_1) = \frac{1}{2}$. In other words, these two states are MU to the measurement basis. However, by rotating the measurement basis we can achieve the inverse situation. Indeed, applying the transformation $U_{\phi=\frac{\pi}{2}}$ to the incoming state $|\psi\rangle$ before the measurement (e.g. using another

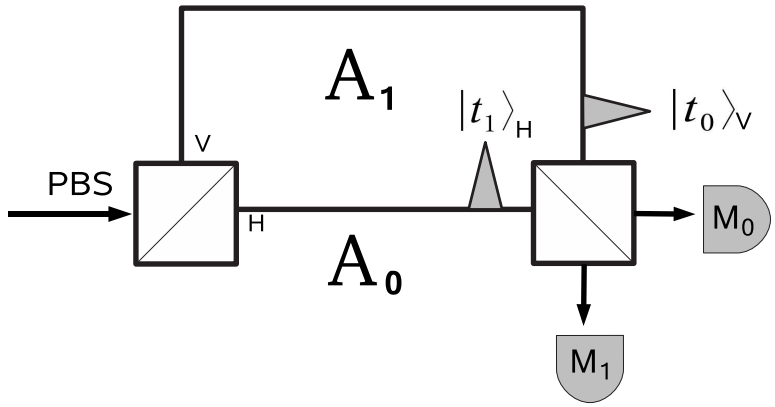

Figure 3.2: Measuring a time bin encoded qubit. The two wave packets impinge on the PBS with polarization turned such that $|t_0\rangle$ goes through A_1 and vice-versa. The wave packets then interfere on the beal-splitter. The photon exists towards detector M_0 or M_1 depending on the phase ϕ.

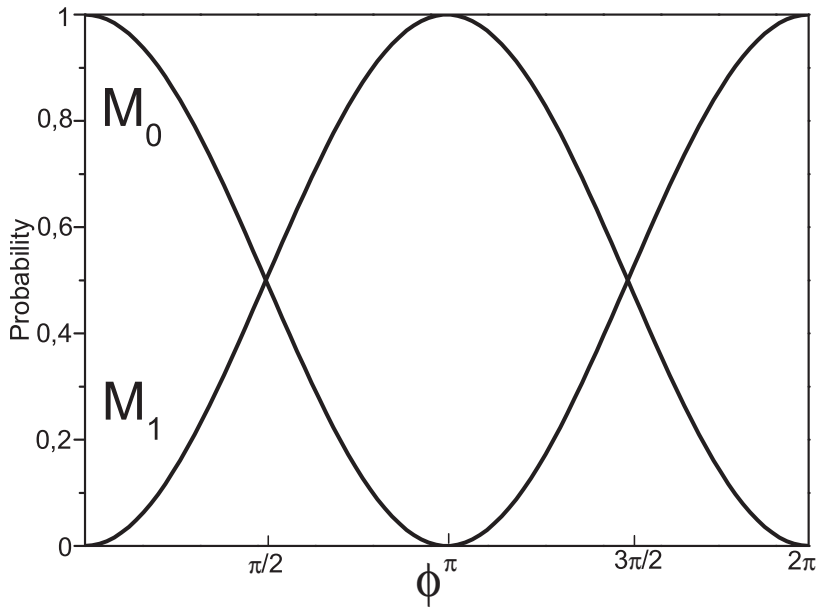

Figure 3.3: Probability of detecting the photon in either detectors M_0 or M_1 as function of the relative phase ϕ.

PM) rotates the state by 45° around the Z axis. In fact, it is more convenient to interpret this rotation as a change of measurement basis by 45°. This interpretation will be quite useful for QKD where Bob must randomly measure the incoming state in one of either two bases. If the measurement basis is now an eigenstate of σ_Y, the probability distribution becomes for states $|\pm^i\rangle$ deterministic again at the expense of completely mixing the probability distributions of states $|\mp\rangle$.

The time bin encoding offers a convenient way of preparing and measuring states expressed as $|\psi\rangle = \frac{1}{\sqrt{2}}[|t_0\rangle + e^{i\phi}|t_1\rangle]$. However, two weaknesses should be addressed before labelling this method practical. The first implies that the two unbalanced interferometers must be kept stable within a fraction of the wavelength of the photon to maintain the correct phase relation. In other words, both interferometers must have exactly the same delay, d. The second issue lies in the vectorial nature of the photon which obliges that the two wave packets have the same polarization in order to manifest interference effects. Asymmetries in the geometry of optical fibers induce the effect of birefringence - the presence of two different phase velocities for two orthogonal polarization states. This effect can be seen as an arbitrary combination of two wave plates, that is, a unitary transformation. If this transformation is constant then it is possible to compensate for it by applying the inverse transformation (e.g. with polarization controllers). However, for long distances in an unpredictable environment, birefringence becomes uncontrolable thus constantly modifying the properties of the fiber therefore randomizing the polarization of the propagating photon. This weakness is particularly unforgiving when sending out qubits on the same channel over a long period of time.

3.2.2 The Faraday mirror

Luckily, a single and simple solution to both of the above problems is available. The idea is to add a Faraday mirror (FM) in replacement of the second (measuring) MZ interferometer. The FM will reflect the photon such that it will travel back to the first MZ interferometer who will now not only serve to encode the state but to measure it as well (in other words the PM will serve to both encode the state and select the measurement basis). All subsequent operations on the qubit after its encoding will be done on the optical fiber before the FM. Since it is the same interferometer that is used to both prepare and measure the state renders the problem of stability obsolete[4].

[4]We assume that the photon round-trip is much faster than any fluctuation in the properties of the fiber, including the interferometer.

Moreover, we will show that the random polarization fluctuations that can limit the visibility of the interference will now be auto-compensated by the FM and thus guarantee that both wave packets interfere with the same polarization.

The FM is a simple, somewhat exotic device consisting of an optical mirror placed behind a Faraday Rotator (FR). A FR is a passive optical device that rotates the polarization (π) of a photon due to the Faraday effect, which in turn is based on a magneto-optical effect. A feature of the FM is its capibility in keeping the π character of a given photon: a linear π is transformed into a linear π' whereas a circular (π) is transformed into a circular π'. Furthermore, for specific values of the FR, it is possible to realize exact orthogonality between π and π'. Without pursueing any physical justification of this phenomena, we briefly describe, the effect of the FM on an arbitrary π state.

The first consideration we must take concerns the *spatial* reference frame in which the photon π will be examined. We therefore introduce the spatial reference frame (x, y, z) where z is the direction of propagation of the photon while x and y belong to the plane of the FM orthogonal to the z. We will assume that the photon's π state is identified according to the right-handed coordinate convention. This implies that after reflection, the π state will be identified on the basis of a new coordinate system $(x' = x, y' = -y, z' = -z)$ obtained by rotating the original frame by 180° around the $\overrightarrow{x}$ axis.

Suppose now that the π state of the photon after being encoded is expressed as $|\chi\rangle = a|H\rangle + b|V\rangle$ where $|a|^2 + |b|^2 = 1$ and H and V form a basis for two-dimensional Hilbert space. This is the Hilbert space of the photon polarization where H corresponds to horizontal polarization and V to vertical polarization. We define three orthogonal axes within this Hilbert space which we label σ_i, $i = \{1, 2, 3\}$. Each is associated to the following eigenstates:

$$\sigma_1 \leftrightarrow \{|H\rangle, |V\rangle\}$$
$$\sigma_2 \leftrightarrow \{\frac{1}{\sqrt{2}}[|H\rangle \pm |V\rangle]\}$$
$$\sigma_3 \leftrightarrow \{\frac{1}{\sqrt{2}}[|H\rangle \pm i|V\rangle]\}.$$

The eigenstates of σ_2 are linear polarization states whereas the eigenstates of σ_3 are circular polarization states. Upon reaching the FM, the photon is first subjected to the FR which acts as a rotation of 90° around the σ_3 axis. The state is then reflected

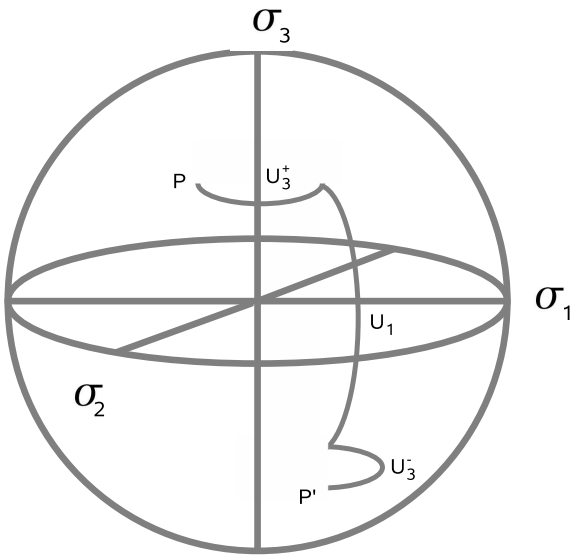

Figure 3.4: FM rotation in state space. A pure state P lying on the surface of the Bloch sphere undergoes a global rotation of 180° around the σ_2 axis to end up in state P'.

by the mirror which induces a 180° rotation around the σ_1 axis. Finally, before leaving the FM, the photon is again subjected to the FR this time in the rotated reference frame. The final state of the photon after leaving the mirror is thus [DMSS04]:

$$\begin{aligned} U_{FM}|\chi\rangle &= U_3^- i\sigma_1 U_3^+ |\chi\rangle \\ &= e^{-i\frac{\pi}{4}\sigma_3} i\sigma_1 e^{i\frac{\pi}{4}\sigma_3} \\ &= i\sigma_2|\chi\rangle. \end{aligned} \tag{3.4}$$

As we can see, the photon's π state is rotated by 180° around the σ_2 axis regardless of its initial state (the global phase i is a consequence of the reflection), see Fig. (3.4).

Let us now show how it is possible to counter the effects of the fluctuating birefringence using the FM. Let the fluctuations affecting the travelling photon from the encoding site to the FM be expressed as the general unitary operator

$$U = e^{i\frac{\theta}{2}(\vec{n}\cdot\vec{\sigma})}. \tag{3.5}$$

where $\vec{\sigma}$ represents the three Pauli matrices and $\vec{n} = \{n_1, n_2, n_3\}$ is a unit vector such that U represents a rotation through θ about the $\vec{n}\cdot\vec{\sigma}$ axis in the π state space. After leaving the FM, the photon is affected by the inverse operator (in the rotated

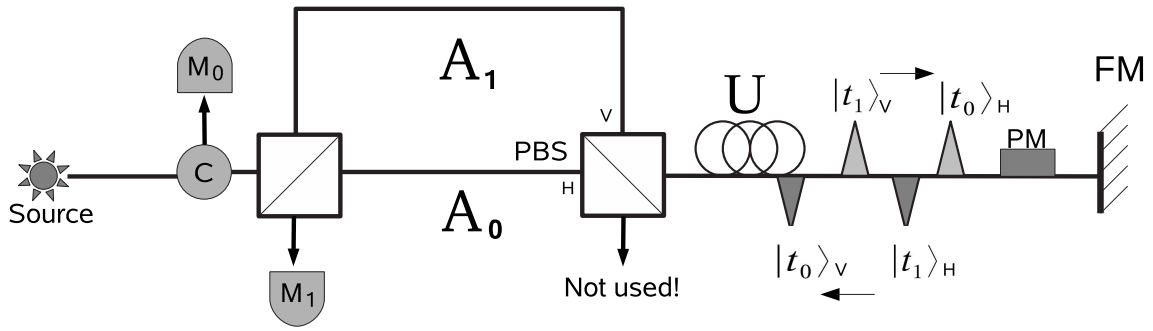

Figure 3.5: A possible plug and play setup. The wave packets propagate to the FM affected by the environment U and come back orthogonally polarized. After interfering the circulator "C" is used to redirect the photon away from the source and towards the detector M_1 if it indeed ended up in that output port.

reference frame) $U' = e^{-i\frac{\theta}{2}(\vec{n'}.\vec{\sigma})}$ where $\{n'_1, n'_2, n'_3\} = \{n_1, -n_2, -n_3\}$. The overall process can be expressed by a round trip through the whole device:

$$U'U_{FM}U|\chi\rangle = i\sigma_3|\chi\rangle \tag{3.6}$$

A possible setup is described in Fig. (3.5) As we can see, the effect of any round trip unitary process is exactly cancelled by the FM. Furthermore, note that a photon described by the initial π state $|H\rangle$ or $|V\rangle$ and subjected to the above operations will come back orthogonally polarized. Therefore a time bin encoded qubit leaving the MZ interferometer in state $|\psi\rangle = \frac{1}{\sqrt{2}}\left[|t_0\rangle_H - e^{i\phi}|t_1\rangle_V\right]$ will return as $|\psi'\rangle = \frac{1}{\sqrt{2}}\left[|t_0\rangle_V - e^{i(\phi+\varphi)}|t_1\rangle_H\right]$ such that upon impinging on the PBS the two time bins will systematically choose their opposite paths and interfere with the same π state at the second beam-splitter. Note that this final automatic directing can only be achieved with one encoding and one measuring PBS. Any other operation on the qubit requiring an interferometer must systematically use a standard beam-splitter or an (hypothetical) optical switch.

With the added Farday mirror, we are now in possesion of a robust and stable technique to prepare, process and measure qubits. Although much more can be said on the plug and play method, the above description will be sufficient to justify the upcoming implementations of quantum processings. We begin by describing an original implementation of the first quantum algorithm ever discovered.

3.3 The Deutsch-Jozsa algorithm

Another appealing field of quantum information is quantum computation, i.e. using quantum mechanical systems to solve mathematical problems. Here, we will be interested in Deutsch's algorithm [Deu85], which was later generalized by Deutsch and Jozsa [DJ92] (DJ). The DJ algorithm discriminates between a constant or a balanced N-point binary function using one single quantum query, while a classical algorithm requires $\mathcal{O}(N)$ classical queries.

3.3.1 The algorithm

Let us start by recalling the principle of the DJ algorithm. At the core of the algorithm is the oracle which computes a function $f(\alpha)$, where $\alpha \in \{0,1\}^N$ is an N bit string, and $f \in \{0,1\}$ is a single bit. The DJ problem is to discriminate whether f is a constant or balanced function, while querying the oracle as few times as possible. A balanced function is such that the number of α's on which $f(\alpha) = 0$ is equal to the number of α's on which $f(\alpha) = 1$. Classically, $2^{N-1} + 1$ queries are necessary in the worst case, whereas the DJ algorithm requires a single query as we shall see. In this algorithm, N qubits are used, and the basis of the Hilbert space is chosen as $|\alpha\rangle = |\alpha_1 \alpha_2 \dots \alpha_N\rangle$ where $\alpha_i \in \{0,1\}$. The quantum oracle carries out the transformation

$$|\alpha\rangle|\beta\rangle \xrightarrow{\text{oracle}} |\alpha\rangle|\beta \oplus f(\alpha)\rangle \ , \tag{3.7}$$

where $|\beta\rangle$ is an ancillary qubit. By choosing $|\beta\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$, the action of the oracle simplifies into

$$|\alpha\rangle \xrightarrow{\text{oracle}} (-1)^{f(\alpha)}|\alpha\rangle \ . \tag{3.8}$$

since $|\beta\rangle$ then remains unchanged. The DJ algorithm starts with the system in the state $|0\rangle = |00\dots0\rangle$. Next, a Hadamard transform H is applied independently on each of the N qubit. Using the definition

$$H|\alpha\rangle = \frac{1}{2^{N/2}} \sum_{\gamma=0}^{2^N-1} (-1)^{\alpha\cdot\gamma}|\gamma\rangle, \tag{3.9}$$

where $\alpha \cdot \gamma = \sum_i \alpha_i \gamma_i \bmod 2$ is the inner product of two N-bit strings, we see that the Hadamard transform acting on the initial state simply yields a uniform superposition of all states:

$$\begin{aligned} |\psi\rangle &= H|0\rangle \\ &= 2^{-N/2} \sum_{\alpha=0}^{2^N-1} |\alpha\rangle. \end{aligned} \tag{3.10}$$

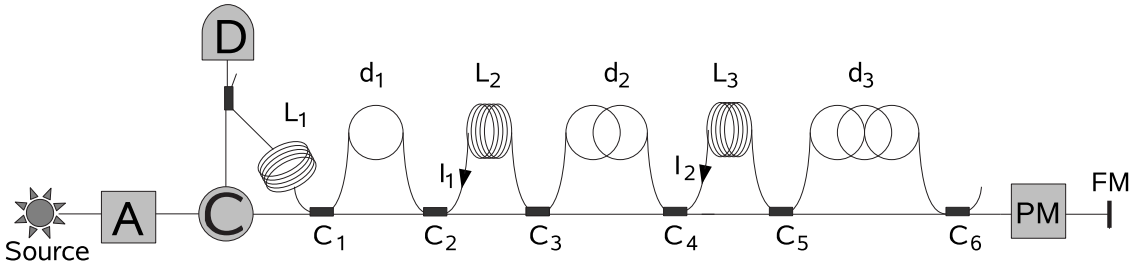

Figure 3.6: Fiber optics setup implementing the 8-dimensional Deutsch-Jozsa.

This state is then sent through the oracle whereupon it becomes

$$|\psi\rangle \xrightarrow{\text{oracle}} \frac{1}{2^{N/2}} \sum_{\alpha=0}^{2^N-1} (-1)^{f(\alpha)} |\alpha\rangle \,. \tag{3.11}$$

The superposition principle allows the oracle to be queried on all input values in parallel. A second Hadamard transform is then carried out to obtain the state

$$|\psi'\rangle = \frac{1}{2^N} \sum_{\alpha,\gamma=0}^{2^N-1} (-1)^{\alpha\cdot\gamma+f(\alpha)} |\gamma\rangle \tag{3.12}$$

which is finally measured in the γ basis. One easily deduces from Eq. (3.12) that when f is constant, the probability of measuring $|0\rangle$ is one. In contrast, when f is balanced, ie. when the number of inputs on which $f = 0$ is equal to the number of inputs on which $f = 1$, this probability is always zero, so the DJ algorithm can distinguish with certainty between these two classes of functions by querying the oracle a single time (whereas classically $2^{N-1} + 1$ queries would be necessary in the worst case).

3.3.2 Experimental setup

Our all optical fiber (standard SMF-28) setup is illustrated in Fig. (**??**) Initially, a 3 ns light pulse is produced by a laser diode at $1,55\ \mu$m, attenuated by an optical attenuator (Agilent 8156A), and then is processed through three unbalanced MZ interferometers with path length differences d_j $(j = 1, 2, 3)$ obeying $d_3 = 2d_2 = 4d_1 = 15$ ns. Each MZ interferometer doubles the number of pulses so that, at the coupler C6, we get eight equally spaced pulses. This corresponds to the action of the Hadamard transform on the three input qubits in state $|0\rangle$. The pulses are then reflected by a Faraday mirror and, on their way back, are modulated by a phase modulator (Trilink) commanded by a pattern generator (Agilent 81110A) which selectively puts a phase shift of 0 or π on each pulse according to the 8-point function [see Eq. (3.11)]. This implements

the oracle. The pulses then pass back through the three MZ interferometers, thereby realizing a second triple Hadamard transform, and are sent via a circulator to a single-photon detector (id Quantique id200), which completes the DJ algorithm.

The additional delay lines L_1, L_2, and L_3, which obey $L_3 > 2L_2 > 4L_1 > 8d_3$, ensure that the different outputs of the DJ algorithm all reach the detector at different times. The delay lines L_2 and L_3 also contain an isolator so that the pulses passing thru L_1, L_2 and L_3 are not transmitted on their way to the mirror. The photodetector was gated during 5 ns around the arrival time of each pulse by the pattern generator. The output of the detector was registered using a time to digital delay converter (ACAM-GP1) connected to a computer. All delays d_j and L_j were chosen to be integer multiples of d_1 within 0,2 ns. All electronic components were triggered by a pulse generator (Standford Research Inc. DG535). In order to maximize the visibility, polarization controllers were introduced in the long arm of each MZ interferometer and in front of the polarization-sensitive phase modulator. Once optimized, the setup was stable for days.

Note that the small number of optical elements in our setup implies that it is relatively easy to increase the number of qubits N while keeping the optical setup stable. As we shall see, a disadvantage of our setup is that the Hadamard transform can only be implemented with a probability of success of $1/2$. Since $2N$ Hadamard transforms are needed for the DJ algorithm with N qubits, the resulting attenuation is 2^{-2N}.

3.3.3 Theoretical correspondance

Let us now prove that our optical setup indeed realizes the DJ algorithm. The quantum state describing the eight pulses at coupler C6 can be written as

$$|\psi\rangle \propto \sum_{\alpha=000}^{111} \exp\left[i\sum_{j=1}^{3}(k\alpha_j d_j + \pi\alpha_j)\right] |\sum_{j=1}^{3}\alpha_j d_j\rangle \tag{3.13}$$

where α stands for $(\alpha_1, \alpha_2, \alpha_3)$ and $|p\rangle$ denotes a pulse located at position p. The three bits $\alpha_1, \alpha_2, \alpha_3 = 0, 1$ label whether the pulse took the short ($\alpha = 0$) or the long ($\alpha = 1$) path through each interferometer. The factor $\exp[ik\sum_j \alpha_j d_j]$ with k being the wave number takes into account the phase difference between a pulse traveling along the short or long paths of the interferometers. The factor $\exp[i\sum_j \pi\alpha_j]$ takes into account the phase accumulated at the couplers: if the pulse takes the short path, it is transmitted at two couplers, whereas, if it takes the long path it is reflected twice.

After reflection at the Faraday mirror and phase modulation, the pulses cross again the three MZ interferometers and reach the photodetector in the state

$$|\psi\rangle \propto \sum_{\alpha,\beta,\gamma=000}^{111} (-1)^{f(\alpha)} \exp\left[i\sum_{j=1}^{3}\left(k(\alpha_j+\beta_j)d_j + \pi(\alpha_j+\beta_j-\beta_j(\gamma_j+\gamma_{j+1}) + \frac{\gamma_j+\gamma_{j+1}}{2})\right)\right] \Big|\sum_{j=1}^{3}((\alpha_j+\beta_j)d_j+\gamma_j L_j)\Big\rangle \tag{3.14}$$

where the bits $\beta_1, \beta_2, \beta_3$ equal 0 or 1 according to whether the pulse passed through the short or the long path of each of the interferometers on its way back, and the bits $\gamma_1, \gamma_2, \gamma_3$ equal 0 or 1 according to whether or not the pulse exited each of the interferometer in the path containing the delay lines L_1, L_2 or L_3. Note that we put $\gamma_4 = 0$. We have again taken into account the phases induced by transmission or reflexion at the couplers C1-C6. The final state contains 120 pulses, but we are only interested in the eight pulses such that $\alpha_1+\beta_1 = \alpha_2+\beta_2 = \alpha_3+\beta_3 = 1$, which are those that exhibit 8-path interference. The other pulses are filtered out in the computer analysis (they correspond to different time bins). The final state then becomes

$$|\psi\rangle \propto \sum_{\gamma=000}^{111} (-i)^{\gamma_1}(-1)^{\gamma_2+\gamma_3}\sum_{\alpha}(-1)^{f(\alpha_1,\alpha_2,\alpha_3)+\alpha_1(\gamma_1+\gamma_2)+\alpha_2(\gamma_2+\gamma_3)+\alpha_3\gamma_3} \Big|d_1+d_2+d_3+\gamma_1 L_1+\gamma_2 L_2+\gamma_3 L_3\Big\rangle \tag{3.15}$$

By relabeling the time bins according to the substitution $\gamma_1 \to \gamma_1+\gamma_2+\gamma_3$ mod 2, $\gamma_2 \to \gamma_2+\gamma_3$ mod 2, and $\gamma_3 \to \gamma_3$, this equation coincides (up to irrelevant phases and an overall normalization factor) with Eq. (3.12) with the 8 logical states $|\gamma\rangle$ identified as specific time bins. The prefactor 2^{-3} takes into account that at the output of each interferometer (couplers C2, C4, and C6) the pulses have a probability amplitude $1/\sqrt{2}$ of exiting by the wrong path and being absorbed.

The setup thus realizes the DJ algorithm, the main difference with an ideal algorithm being an extra attenuation by a factor of 2^{-7}. A factor 2^{-3} originates from the couplers C2, C4, and C6 because each time a pulse passes through these couplers it only has a probability 1/2 of exiting by the right path. Otherwise, it is absorbed by the isolators I1 and I2 or by the unconnected fiber pigtail at coupler C6. Another factor 2^{-3} is due to the filtering out of the 112 pulses produced on the way back that do not correspond to 8-path interferences. The remaining factor 2^{-1} is due to the coupler C7. This overall loss of 21 dB could be remedied by replacing the couplers C2, C4, C6, and C7 by optical switches which would direct the light pulses along the appropriate

path. However, as mentionned above, high speed, low loss optical switches are not available commercially at present, so we had to use couplers in the present experiment.

In order to characterize the performances of our setup, we considered the 2^N oracles of the form $f_k(\alpha) = \alpha \cdot k$ and $\overline{f}_k(\alpha) = \alpha \cdot k + 1 \bmod 2$ (i.e., the oracles in the BV algorithm and their complements). For each oracle f_k (or $\overline{f}_k$), we ran the algorithm 500,000 times and registered the number of counts in time bin γ, denoted as $n_k(\gamma)$ (or $\overline{n}_k(\gamma)$). The algorithm gives constructive interference in the time bin $\gamma = k$ for the oracle f_k or $\overline{f}_k$, and destructive interference elsewhere. We then computed

$$V_j(\gamma) = \frac{1}{2}\left(\frac{n_\gamma(\gamma) - n_k(\gamma)}{n_\gamma(\gamma) + n_k(\gamma)} + \frac{\overline{n}_\gamma(\gamma) - n_k(\gamma)}{\overline{n}_\gamma(\gamma) + n_j(\gamma)}\right) \tag{3.16}$$

for each pair of oracles with $k \neq \gamma$, and calculated the visibility $V(\gamma)$ in time bin γ by taking the average of $V_k(\gamma)$ over all values of k. The measured visibilities $V(\gamma)$ for 2 and 3 qubits are shown in Table I. Remarkably, they remain relatively high when going from 2 to 3 qubits in spite of the fact that 8 path interferences are involved. This is because the path differences are automatically compensated and only $N + 1$ polarizations must be adjusted. It should therefore be relatively easy to go beyond $N = 3$ without significantly decreasing the visibilities.

Because of the attenuation in our setup along with the quantum efficiency ($\simeq 10.5$ %) and the dark count probability ($\simeq 10^{-4}$ ns^{-1}) of our detector, the signal-to-noise ratio was not high enough to perform these visibility measurements in the single-photon regime. For this reason, in our experiment, approximatively 20 photons per pulse entered the phase modulator (oracle) in 4 dimensions, and approximatively 50 in 8 dimensions. However, minimal modifications should allow us to decrease the number of photons while keeping the signal-to-noise ratio constant. In particular, by reducing the pulse length or using two detectors instead of the coupler C7, it should be possible to operate in the single-photon regime in 4 (and possibly 8) dimensions. Moreover, as already mentioned, the Hadamard transform could be rendered deterministic by using fast low-loss optical switches instead of couplers, which would strongly reduce the losses.

3.4 Conclusion

In this chapter, we have introduced a convenient method to prepare and manipulate qubits. We have illustrated this method in the context of quantum computation where

γ	1	2	3	4	5	6	7	8
$V(\gamma)^{N=2}$	98.4	97.4	98.5	98.6				
$V(\gamma)^{N=3}$	96.78	97.99	97.68	97.32	97.33	97.56	97.37	97.28

Table 3.1: Measured average visibility $V(\gamma)$ in the γth time bin for the DJ algorithm with $N = 2$ and $N = 3$ qubits.

we have shown that it is possible to implement the DJ algorithm for 3 qubits. Note that the DJ algorithm has already been implemented using table-top optics [Tak00], NMR [JM98] and ion traps [GRL$^+$03]. However, our setup differs from this realization in several major aspects. First, it based on the plug and play method, which makes it unnecessary to perform a precise alignment. Second, although it relies on linear optics, our realization is relatively efficient in terms of used optical resources compared to [Rec94, CAK98]. The central idea of such implementations consists in representing the basis states of a N-dimensional Hilbert space by N optical paths so that unitary transformations are obtained by chaining linear optics components that make these paths interfere. Such implementations seem, however, to be inherently inefficient since the space requirement (the number of optical components) and the time requirement both grow exponentially with the number N of qubits. In contrast, in our setup, the number of components is kept linear in N, while the time needed still grows exponentially. Note that any implementation of an algorithm involving an arbitrary 2^N-point function does in any case require exponential resources to simulate this function. Therefore, the linear optical implementation of quantum algorithms involving oracles can reasonably be made as efficient as any other implementation in this respect. For all these reasons, our experimental demonstration works with a 8-point (3-qubit) function and might probably be extended even further without fundamental difficulty, while the realisation [Tak00] used a 4-point (2 qubit) function[Tak00].

We now proceed to demonstrate how it is possible to implement QKD with the plug and play technique. Furthermore, we will exploit this method not only to encode the qubits necessary to perform the key distribution but also in order to filter errors than can occur during the exchange of qubits.

Chapter 4

Error Filtration

4.1 Introduction

As introduced in the previous chapter, the plug and play method is, at present, an excellent solution to many problems in quantum information. Unfortunately, this method suffers from a fundamental drawback that is the limiting distance at which sending photons is possible. This leads to two important consequences which result in the breakdown of QKD. The first is the exponential decrease in bit rate which quickly tends to zero, while the second is the violation of the security of QKD because of a constant noise level which eventually overtakes the decreasing signal.

The longest fibre over which any key has been exchanged is currently just over a 100 km [**?**]. In order to circumvent the above problems and to considerably increase the distance at which QKD is feasible, the idea of quantum repeaters has been put forward. This device would tackle the problem of signal loss by temporarily storing the state of each photon. It would allow new photons with the same state to be generated at each repeater, thus transforming the exponential decay into a polynomial one which would be achieved by a number of short steps. To date a variety of schemes have been suggested for photon-atom quantum communication using either trapped atoms in cavity quantum electrodynamics (cavity-QED) setups or atomic ensemble, and very promising experimental progress has been made toward realizing quantum repeaters [DLCZ01, PSBZ01].

However, once high-fidelity quantum repeaters will be available, the main limiting factor will no longer be distance but rather errors due to the accumulation of noise in long distance plug and play QKD. This noise originates from the interaction of

the photon with acoustic phonons caused by thermal excitations of the optical fiber in which it is propagating. This results in a modification of the characteristics of the photon such as phase and polarization. Because plug-and-play QKD is based on phase encoded qubits, acoustic phonons bias the value of qubits propagating through the optical fiber. Since these phonons have frequencies on the order of a few 100 MHz and that time bins for a given qubit are seperated by a few 100 ns, the accumulation is only significant at distances much longer than 100 km. Phase noise accumulated in present day short distance QKD is not a significant problem because the BER remains lower than 11% (the BER at which the BB84 protocol is no longer secure). Beyond the distances achievable today, phase noise will become a significant problem to such an extent that it may render QKD insecure.

Luckily, one of the central results in quantum information is that errors can, in principle, be corrected [Sho97, BBP$^+$96]. Practical realizations of quantum error correcting codes are, however, extremely difficult because they require multiphoton interactions. A first experimental demonstration of quantum error correction has recently been realized [PGU$^+$03], but it is still very far from being usable in practical applications. An alternative method, called *error filtration*, allows errors to be filtered out during quantum communication, and can in contrast be easily implemented using present day technology [GLMP05]. The main idea of error filtration is to encode one qubit in a single photon within a Hilbert space of dimension greater than 2. It is then possible to detect, with high probability, whether a phase error has occurred, and, if so, to discard the state. This quantum error detection scheme is less powerful than full error correction, but, for many applications such as QKD, discarding the state affected by noise is sufficient. The advantage of this method is that the encoding and decoding operations do not require multiphoton interactions, hence they are relatively easy to implement by interferometric techniques. Note that it was previously realized that the use of higher dimensional systems can increase the resistance of QKD to noise [CBKG02]. We will discuss the advantages of error filtration over these previous methods in the concluding remarks of this chapter.

4.2 Basic Principle

The main idea behind error filtration is *multiplexing*, i.e. using more transmission channels than the minimum required to send a given information. To illustrate this concept, suppose Alice would like to send an arbitrary quantum state to Bob via a noisy quantum communication channel such as time bins propagating through an optical

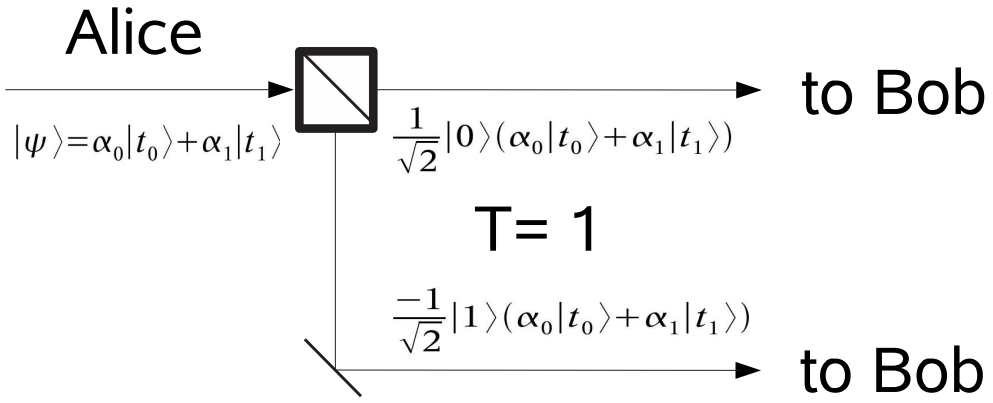

Figure 4.1: After prepraring the state, Alice encodes it for filtration by sending it on a beam-splitter. The state is split in 2^T independent channels (in this case $T = 1$).

fiber. To remain as simple as possible and faithful to the experimental demonstration, we will assume that the information she would like to send is encoded in a single photon in 2-dimensional Hilbert space: $|\psi\rangle = \alpha_0|t_0\rangle + \alpha_1|t_1\rangle$ where $|\alpha_0|^2 + |\alpha_1|^2 = 1$ and $\langle t_0|t_1\rangle = 0$. In other words, $|\psi\rangle$ is a normalized superposition of the computational basis states $|t_0\rangle$ and $|t_1\rangle$ with complex coefficients. Before sending the state to Bob, Alice divides the communication channel (e.g. with beam-splitters) in a series of parallel channels such that the quantum state is uniformally distributed among them. This could be achieved by having Alice send her photon on the input port of an interferometer where the total number of possible paths would be chosen by the number of divisions applied by Alice on the original channel and is illustrated in Fig. (4.1) for the case of a qubit impinging on two parallel channels. As we shall see, this encoding will allow Alice and Bob to discriminate, with high probability, whether the state has been affected by noise during its propagation towards Bob. Thus $|\psi\rangle$ becomes embedded in a 2^{T+1} Hilbert space where T refers to the number of divisions the channel has underwent. Formally, transfering the state to 2^T parallel channels (described by some unitary operation U_e) transforms it as:

$$U_e|\psi\rangle = \sum_{\overline{k}=0}^{2^T-1} \frac{(-1)^m}{\sqrt{2^T}} |\overline{k}\rangle \big[\alpha_0|t_0\rangle + \alpha_1|t_1\rangle\big] \tag{4.1}$$

where the channel is labeled $\overline{k} \Leftrightarrow \{k_T \cdots k_1\}$, $k_i \in \{0, 1\}$ and, $m = \sum_{i=0}^{T} k_i \bmod 2$. The additional $(-1)^m$ phase affects the wave packets which are reflected either by beam-splitters or mirrors and, as mentionned in the previous chapter, is a consequence of energy conservation. This encoding transformation has been shown to be optimal

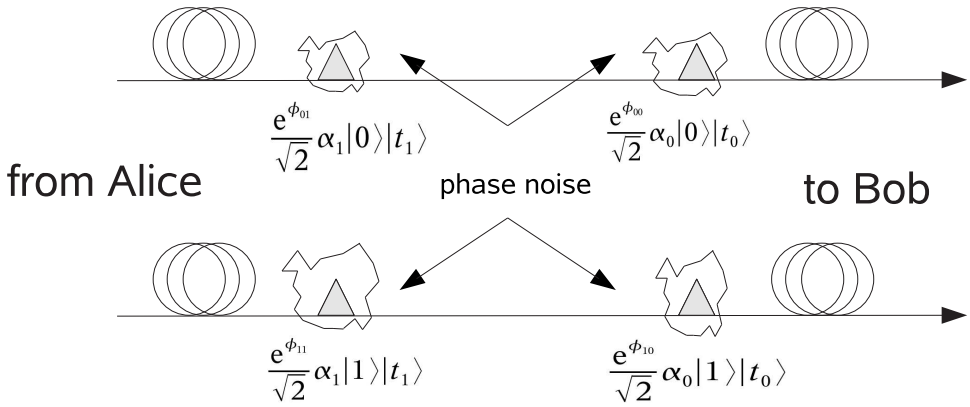

Figure 4.2: The propagation of the four pulses towards Bob. Each pulse is associated to independent phase noise.

[GLMP05] and, as we shall see, is chosen for its correspondance with our experimental setup. State $|\psi\rangle$ propagates to Bob in a superposition of the 2^T parallel channels which we assume to be affected by independent phase noise[1]. Indeed to remain as close as possible to the context of our experiment, we consider that the noise affecting the different wave packets is phase noise. That is, we suppose unlikely the event of a flip error where wave packet $|t_0\rangle \rightarrow |t_1\rangle$ and vice versa. The phase noise however implies that an additional 2^{T+1} independent random variables $e^{i\varphi_{\overline{k}t_j}}$ with $\varphi_{\overline{k}t_j} \in [0, 2\pi]$ be associated to each channel and each wave packet $|t_j\rangle$ propagating in one of the given channels, see Fig. (4.2):

$$U_e|\psi\rangle \rightarrow |\psi'\rangle = \sum_{\overline{k}=0}^{2^T-1} \frac{(-1)^m}{\sqrt{2^T}} |\overline{k}\rangle \left[\alpha_0 e^{i\varphi_{\overline{k}0}}|t_0\rangle + \alpha_1 e^{i\varphi_{\overline{k}1}}|t_1\rangle\right]$$

where $\varphi_{\overline{k}t_j}$ is drawn from a gaussian probability distribution

$$P(\varphi_{\overline{k}j}) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\varphi_{\overline{k}j}^2/(2\sigma^2)\right) \tag{4.2}$$

of average zero. Upon recieving $|\psi'\rangle$, Bob completes the filtration before processing it any further. To decode it, he performs the inverse operation carried out by Alice. More precisely, he combines the channels such that each wave packet $e^{i\varphi_{\overline{k}j}}|\overline{k}j\rangle$ interferes with its neighbour and gradually recombines to one channel thus projecting $|\psi'\rangle$ back onto the original two-dimensional Hilbert space. Each interference can be interpreted as a

[1]This experimental constraint could easilly be fulfilled by spatially separating the channels far away from each other.

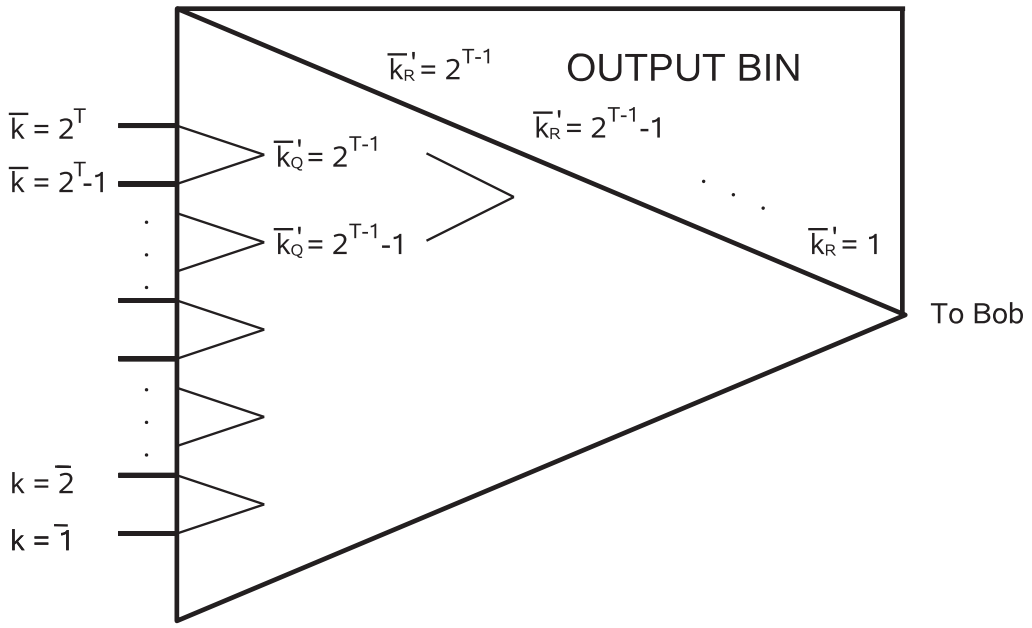

Figure 4.3: Error filtration for a given wavepacket $|t_j\rangle$. The figure illustrates the first recombination of the last two channels. The signal is either discarted ($|\overline{k'_R}\rangle$) or interferes again at the next level of filtration ($|\overline{k'_Q}\rangle$). This process is repeated until reaching Bob.

filtration. Consider, as an example, state $|t_j\rangle$ having travelled through neighbouring channels $2^T = \overline{k}$ and $2^T - 1 = \overline{k} - 1$: $e^{i\varphi_{\overline{k}j}}|\overline{k}t_j\rangle$ and $e^{i\varphi_{(\overline{k}-1)j}}|(\overline{k}-1)t_j\rangle$. (Note that $|t_j\rangle$ has also travelled through $2^T - 2$ other channels which recombine in pairs and interfere.) As a result, the recombination of these two states induces the following superposition (up to a normalization factor):

$$\alpha_j\left[e^{i\varphi_{\overline{k}j}}|\overline{k}\rangle + e^{i\varphi_{(\overline{k}+1)j}}|\overline{k}+1\rangle\right]|t_j\rangle \rightarrow$$
$$\frac{\alpha_j e^{i\varphi_{\overline{k}j}}}{2}\left[(1+e^{i(\varphi_{(\overline{k}+1)}-\varphi_{\overline{k}j})})|\overline{k'_Q}t_j\rangle + (1-e^{i(\varphi_{(\overline{k}+1)}-\varphi_{\overline{k}j})})|\overline{k'_R}t_j\rangle\right] \quad (4.3)$$

where $\overline{k'_Q} = 2^{T-1}$ labels the output channel of the interferometer which carries on to the next interference and eventually to Bob while $\overline{k'_R}$ labels the output channel of the interferometer which leads to an output bin, see Fig. (4.3). If the photon emerges in channel $\overline{k'_Q}$ it will again interfere, this time with neighbouring channel $\overline{k'_Q} = 2^{T-1} - 1$. This process will repeat until only two channels $\overline{k'_Q} = 0$ and $\overline{k'_Q} = 1$ remain and that the photon interferes one last time. The interferometers are tuned in such a way that when no error occurs, the state emerges with certainty in channel

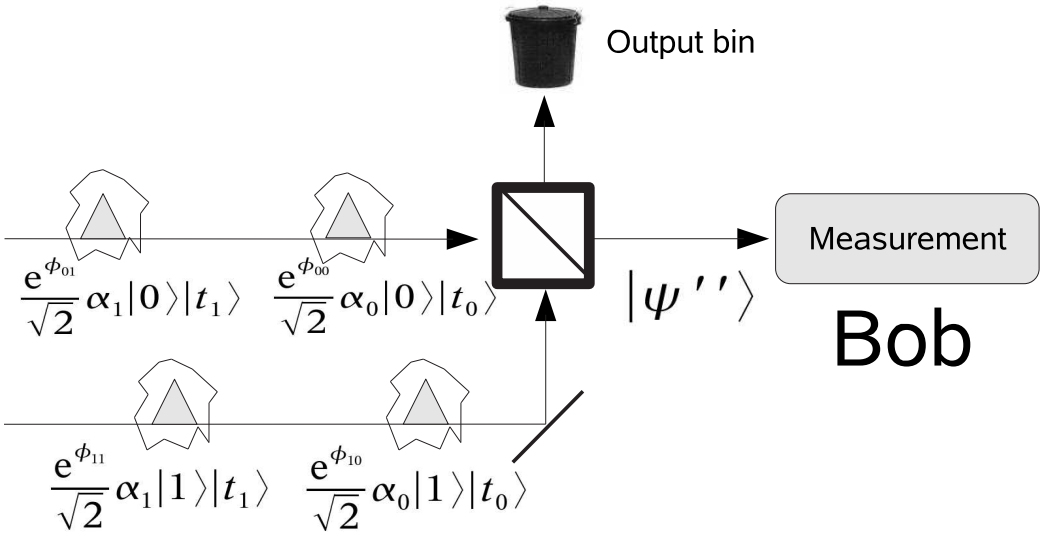

Figure 4.4: The propagation of the four pulses towards Bob. Each pulse is associated to independent phase noise.

$|\overline{k'_Q}t_j\rangle$. That is, we arrange the interferometers so that, in the absence of errors, there is complete constructive interference in the output channels $|\overline{k'_Q}t_j\rangle$ and complete destructive interference in the other output channels $|\overline{k'_R}t_j\rangle$. The probability of either outcome depends on the phase difference $\varphi_{\overline{k}j} - \varphi_{(\overline{k}+1)j}$. The bigger this difference, the higher the probability that state $|t_j\rangle$ will be directed to the output bin. In that case we know that an error has occurred - otherwise the state would not have ended up there - so we discard it. Therefore, a noisy channel and a disturbed state will have a higher probability of being identified with error filtration. The higher the degree of multiplexing, the higher the probability. The wave packet that exits the last beam splitter and travels to Bob is written as

$$|\psi''\rangle = \frac{(-1)^T}{2^T} \sum_{\overline{k}=0}^{2^T-1} \left[\alpha_0 e^{i\varphi_{\overline{k}_0}}|t_0\rangle + \alpha_1 e^{i\varphi_{\overline{k}_1}}|t_1\rangle\right]. \tag{4.4}$$

Bob then completes the protocol by measuring the state of the photon. Although there is a probability that the photon will be affected by noise and discarded by error filtration, there is still the probability that it will reach Bob who will measure in the $\{|\psi\rangle, |\psi^\perp\rangle\}$ basis. Therefore, the probability for Bob to measure the photon in output

$|\psi\rangle$ is obtained by projecting $|\psi''\rangle$ onto $|\psi\rangle$:

$$\begin{aligned}\mathrm{P}(\psi) = |\langle\psi|\psi''\rangle|^2 = \frac{1}{2^{2T}}\Big[|\alpha_0|^4\big(2^T + 2\sum_{\overline{k},\overline{k}'=0}^{2^T-1}\cos\left(\phi_{\overline{k}0} - \phi_{\overline{k}'0}\right)\delta_{\overline{k},\overline{k}'}\big) \\ + 2|\alpha_0\alpha_1|^2\sum_{\overline{k},\overline{k}'=0}^{2^T-1}\cos\left(\phi_{\overline{k}1} - \phi_{\overline{k}'0}\right) \\ + |\alpha_1|^4\big(2^T + 2\sum_{\overline{k},\overline{k}'=0}^{2^T-1}\cos\left(\phi_{\overline{k}1} - \phi_{\overline{k}'1}\right)\delta_{\overline{k},\overline{k}'}\big)\Big]. \qquad (4.5)\end{aligned}$$

Similarly, the probability that he measures the photon in output $|\psi^\perp\rangle$ is given by:

$$\begin{aligned}\mathrm{P}(\psi^\perp) = |\langle\psi^\perp|\psi''\rangle|^2 = \frac{|\alpha_0\alpha_1|^2}{2^{2T}}\Big[2^T + 2\sum_{\overline{k},\overline{k}'=0}^{2^T-1}\cos\left(\phi_{\overline{k}0} - \phi_{\overline{k}'0}\right)\delta_{\overline{k},\overline{k}'} \\ - 2\sum_{\overline{k},\overline{k}'=0}^{2^T-1}\cos\left(\phi_{\overline{k}1} - \phi_{\overline{k}'0}\right) \\ + (2^T + 2\sum_{\overline{k},\overline{k}'=0}^{2^T-1}\cos\left(\phi_{\overline{k}1} - \phi_{\overline{k}'1}\right)\delta_{\overline{k},\overline{k}'})\Big]. \qquad (4.6)\end{aligned}$$

In order to characterize the performance of error filtration as a function of T, the level of multiplexing, we can calculate the visibility of the setup (by averaging over the noise) which describes the quality of the interference fringes as measured by Bob:

$$\begin{aligned}\mathrm{V}_T &= \frac{< I_\psi > - < I_{\psi^\perp} >}{< I_\psi > + < I_{\psi^\perp} >} \\ &= \frac{T}{T - 1 + e^{\sigma^2}} \\ &= 1 - 2\ \mathrm{BER}. \qquad (4.7)\end{aligned}$$

$< I_\psi >$ is the average number of correct detections (Bob measures outcome $|\psi\rangle$) and $< I_{\psi^\perp} >$ is the average number of incorrect detections (Bob measures outcome $|\psi^\perp\rangle$). They are defined as

$$< I_\psi >=< \tfrac{1}{N}\textstyle\sum_{i=1}^{N}|\langle\psi|\psi_i'\rangle|^2 > \qquad \text{and} \qquad < I_{\psi^\perp} >=< \tfrac{1}{N}\textstyle\sum_{i=1}^{N}|\langle\psi^\perp|\psi_i'\rangle|^2 > .$$

The visibility enables us to calculate the density matrix as measured by Bob:

$$\rho = \mathrm{V}_T|\psi\rangle\langle\psi| + (1 - \mathrm{V}_T)\mathbb{1}/2, \qquad (4.8)$$

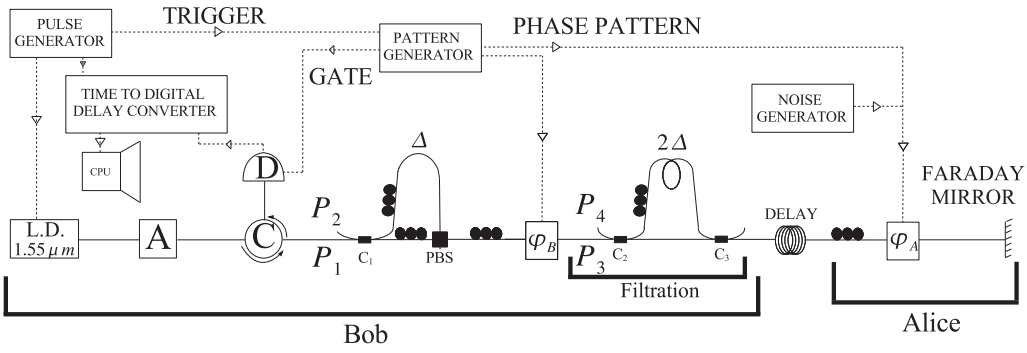

Figure 4.5: Fiber optics QKD setup with error filtration. A Attenuator, C Circulator, D Single Photon Detector.

where we conclude that phase noise amounts to the admixture of isotropic noise. It is clear from Eq. (4.7) that in the limit where the degree of multiplexing is infinite the visibility attains 1. That is, all states affected by noise are discarded by error filtration such that the BER reaches zero at the expense of having a lower bit rate.

4.3 Experiment

This section is devoted to the experimental demonstration of error filtration based on plug and play quantum cryptosystem. We motivate the interest for error filtration by performing the optical part of a QKD scheme over a noisy quantum communication channel with so much noise that a secure BB84 protocol cannot be realized. As explained in Chapter 1, if the BER exceeds 14.6%, then a simple cloning attack makes the BB84 protocol insecure. On the other hand, if the BER is lower than 11.0%, then the BB84 protocol is provably secure. Between the two boundaries lies a gray zone where the security of BB84 is unknown[2]. In our experiment, we consider an error prone QKD scheme with a BER = 15.3% ± 0.1%, which is therefore insecure. Using error filtration, the BER is brought down to 10.6% ± 0.1% so that QKD is rendered secure.

Before discussing error filtration let us first introduce a setup which realizes the optical part of a plug and play BB84 protocol. This setup works with attenuated coherent states traveling in localized time bins in standard SMF-28 optical fibers, see Fig. 4.5. In plug and play QKD, Bob initiates the protocol by preparing a classical light pulse. In our experiment, he uses a laser diode at 1.55 μm to produce a 3-ns

[2]These bounds refer to BB84 with one way classical post-processing.

light pulse. The pulse is attenuated by an optical attenuator (Agilent 8156A), and then split by a first 50/50 coupler (C_1) to produce two pulses. These pulses impinge on the input ports of a polarization beamsplitter (PBS) with a time delay $\Delta = 60$ ns. Their polarizations are rotated, using polarization controllers, so that the two pulses exit by the same port of the PBS. This produces two emerging pulses traveling down a 900-ns delay line (representing the noisy communication channel). Then, at Alice's site, the pulses are reflected back by a Faraday mirror. Recall that the use of a Faraday mirror makes the setup insensitive to birefringence in the delay line. Alice may modify the phases of the two pulses using a phase modulator (ϕ_A) (Trilink) controlled by a pattern generator (Agilent 81110A). Upon reaching Bob's site, the two pulses travel through Bob's phase modulator (ϕ_B) (Trilink) and the PBS to the coupler C_1, where they interfere and are sent to a single-photon detector (id Quantique id200) via a circulator. The detector was gated by a pattern generator during a 5-ns window around the arrival time of the central pulse. Its output was registered by a time-to-digital delay converter (ACAM-GP1) connected to a computer. All electronic components were triggered by a pulse generator (Standford Research Inc. DG355). In order to maximize the interference visibilities, polarization controllers were introduced in the long arm of the MZ interferometer and in front of the polarization-sensitive phase modulators. Once optimized, the setup was stable for days.

The classical pulse emerging from the laser is attenuated in such a way that upon leaving Alice's site, the combination of the two pulses contains, on average, less than one photon. Therefore, after Alice encodes her phase ϕ_A the wavefunction describing the two pulses (making the approximation that a single photon fock state is contained in the 2 pulses) can be written as $\frac{1}{\sqrt{2}}(|t_0\rangle_H - e^{i\phi_A}|t_1\rangle_V)$, where the subscripts H and V represent the polarization states while the subscripts 0 and 1 represent the relative delay of time bin i, i.e. $t_i = i \cdot \Delta$. The (-1) phase in front of $|t_1\rangle_V$ takes into account the conventional relative phase of $\pi/2$ between the reflected and transmitted light at coupler C_1 and at the PBS. In the BB84 protocol, Alice must randomly choose among two maximally unbiased bases and again randomly choose among the states contained therein. In the plug and play version, these two bases are:

$$\begin{array}{c|c} \frac{1}{\sqrt{2}}(|t_0\rangle_H + |t_1\rangle_V) & \frac{1}{\sqrt{2}}(|t_0\rangle_H + i|t_1\rangle_V) \\ \frac{1}{\sqrt{2}}(|t_0\rangle_H - |t_1\rangle_V) & \frac{1}{\sqrt{2}}(|t_0\rangle_H - i|t_1\rangle_V). \end{array}$$

That is, the phase ϕ_A must be chosen randomly in $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. The state leaving Alice's site thus reads

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|t_0\rangle_V - e^{i\phi_A}|t_1\rangle_H\right] \tag{4.9}$$

where the polarizations have been interchanged because of the Faraday mirror.

Due to the short distance over which the time bins traveled, intrinsic noise in our plug-and-play QKD scheme was actually very low so that in our experiment we had to simulate the noisy channel by making Alice's phase modulator imperfect. This was achieved by electronically combining the signal from the pattern generator with the output of a function generator (Agilent 33250A) producing gaussian electronic noise with an adjustable amplitude and a 50-MHz 3dB-bandwidth. Since the time bins are separated by 60 ns, the phase noise in the successive time bins can be considered as independent. The state which is sent to Bob is thus

$$|\psi'\rangle = \frac{1}{\sqrt{2}}\left[e^{i\varphi_0}|t_0\rangle_V - e^{i(\phi_A+\varphi_1)}|t_1\rangle_H\right] \tag{4.10}$$

where the φ_i's are independent random phases drawn from a gaussian probability distribution defined in Eq. (4.2) with tunable variance σ^2. In terms of BER, this noise level corresponds to

$$\mathrm{BER} = \frac{(1-e^{-\sigma^2})}{2}.$$

The two pulses travel back to Bob, who performs a measurement in the $\frac{1}{\sqrt{2}}(|t_0\rangle_V \mp e^{-i\phi_B}|t_1\rangle_H)$ basis by applying the phase $\phi_B \in \{0, \frac{\pi}{2}\}$. Bob's detector is connected to either output port P_1 or P_2. The probability for Bob to detect a count (assuming a perfect detector) is $\frac{1}{2} \pm \frac{1}{2}\cos(\varphi_1 - \varphi_0 + \phi_A + \phi_B)$ where the sign depends on which output port is used. The measured values of V_0 for various levels of σ^2 (after subtracting dark counts) agree well with this prediction, see lower curve in Fig. 9.2.

In order to carry out error filtration, an additional unbalanced MZ interferometer is placed after the PBS (T=1) identified by couplers C_2 and C_3 with path length difference equivalent to 2Δ, see Fig 4.5. This second interferometer produces four emerging pulses which travel down the 900-ns delay line and, as we shall show, realizes error filtration. Formally, each pulse exiting from the PBS is split into two pulses by the MZ interferometer according to

$$|t_0\rangle_H \rightarrow \tfrac{1}{2}(|0\rangle|t_0\rangle_H - |1\rangle|t_0\rangle_H) \qquad |t_1\rangle_V \rightarrow \tfrac{1}{2}(|0\rangle|t_1\rangle_V - |1\rangle|t_1\rangle_V).$$

The factor 1/2 takes into account that half of the intensity is lost at coupler C_3. After Alice has encoded her phase ϕ_A and the pulses have been reflected by the Faraday mirror, the state becomes

$$|\psi\rangle = \frac{1}{2\sqrt{2}}\left[|0\rangle|t_0\rangle_V - |1\rangle|t_0\rangle_V - e^{i\phi_A}(|0\rangle|t_1\rangle_H - |1\rangle|t_1\rangle_H)\right]. \tag{4.11}$$

This is formally identical to the BB84 protocol since Alice effectively uses the 2-dimensional space spanned by $(|0\rangle|t_0\rangle_V - |1\rangle|t_0\rangle_V)$ and $(|0\rangle|t_1\rangle_H - |1\rangle|t_1\rangle_H)$. Then, because of the noise, the four pulses get random phases φ_{00}, φ_{10}, φ_{01} and φ_{11}, respectively. The state that Alice sends back to Bob is thus

$$|\psi'\rangle = \frac{1}{2\sqrt{2}}\left[e^{i\varphi_{00}}|0\rangle|t_0\rangle_V - e^{i\varphi_{10}}|1\rangle|t_0\rangle_V - e^{i\phi_A}(e^{i\varphi_{01}}|0\rangle|t_1\rangle_H - e^{i\varphi_{11}}|1\rangle|t_1\rangle_H)\right]. \quad (4.12)$$

It now belongs to the full space spanned by $|0\rangle|t_0\rangle_V$, $|0\rangle|t_1\rangle_V$, $|1\rangle|t_0\rangle_H$ and $|1\rangle|t_1\rangle_H$, since the phase noise has taken it out of the 2-dimensional Hilbert space. With error filtration Bob projects the state back onto the 2-dimensional Hilbert space in order to selectively enhance the visibility. This projection is realized by the MZ interferometer. At coupler C_3 each time bin has amplitude $1/\sqrt{2}$ of following the long path and amplitude $1/\sqrt{2}$ to follow the short path. This gives rise to eight new time bins of which four can be considered as parasites because they do not interfere at coupler C_1 where Bob performs his measurement. In the theoretical analysis above, these additional time bins were not considered. As we discuss later their appearance is due to the specific implementation we use and gives rise to a loss which is not intrinsic to the method. These four time bins, which we label $|ss\rangle_0$, $|ss\rangle_1$, $|ll\rangle_0$ and, $|ll\rangle_1$ arise from state $|j\rangle$ having travelled twice through the short arm or the long arm of the MZ interferometer. The resulting state after C_2 (ignoring the parasite wave packets) is

$$|\psi''\rangle = \frac{1}{4\sqrt{2}}\left[-(e^{i\varphi_{00}} + e^{i\varphi_{10}})|0\rangle_V + e^{i\phi_A}(e^{i\varphi_{01}} + e^{i\varphi_{11}})|1\rangle_H\right]. \quad (4.13)$$

Bob now realises his measurement by putting his phase ϕ_B on time bin 1: $|t_1\rangle \rightarrow e^{i\phi_B}|t_1\rangle$. At the PBS wave packet $|0\rangle_V$ takes the long path whereas wave packet $|1\rangle_H$ takes the short path and interfere at coupler C_1. The probability to detect the photon is

$$\frac{1}{16}\Big[(1+\cos(\varphi_{00}-\varphi_{10})) + (1+\cos(\varphi_{00}-\varphi_{10}))(1+\cos(\varphi_A-\varphi_B)) \pm \Big(\sum_{k,k'=0}^{1}\cos(\varphi_{k0}-\varphi_{k1}-\phi_A) + \cos(\varphi_{k0}-\varphi_{k1}-\phi_B)\Big)\Big]$$

where the $\pm$ sign depends on which output port (P_1 or P_2) the state exits. When the photon emerges in the time bin corresponding to the interference of $|0\rangle_V$ and $|1\rangle_H$ the visibility is

$$V_1 = 2/(1+e^{\sigma^2}). \quad (4.14)$$

Comparing with Eq. (4.11) we see that filtration effects an increase of visibility.

There are two sources of loss in the above implementation. The first is not intrinsic to the method and is due to the photons ending up in time bins $|ss\rangle$ and $|ll\rangle$ after Bob's measurement which do not have improved visibility and are therefore discarded. In principle this could be remedied by replacing coupler C_3 by a switch that deterministically sends pulses $|s\rangle_0$ and $|s\rangle_1$ along the long path and pulses $|l\rangle_1$ and $|l\rangle_1$ along the short path. We did not implement this because high speed, low loss switches do not exist commercially at present. The second source of loss is intrinsic to the method of error filtration: visibility is enhanced by separating the signal into two components, a noisy one which is discarded and a good one which is kept. This intrinsic loss occurs in our experiment at coupler C_2 where $|0\rangle|t_0\rangle$ and $|1\rangle|t_0\rangle$ interfere and similarly for $|0\rangle|t_1\rangle$ and $|1\rangle|t_1\rangle$. The light which emerges from the unused output port (P_4) is completely noisy and is simply discarded.

The measured average visibilities (after substracting detector dark counts) are plotted in Fig. 9.2 as a function of the phase noise standard deviation in the case where Alice applies $\phi_A = 0$ and Bob measures the output port P_1. In this case, without noise, the maximal visibilities exceeded 99%. With unfiltered noise (lower curve), the visibility decreases exponentially with the amount of noise in accordance with Eq. (4.11). The filtration achieved by our setup (upper curve) is also very close to the theoretical prediction of Eq. (4.14). Visibilities in the range from 65% to 78% are enhanced, by filtration, to the range from 78% to 85%, see inset of Fig. 9.2. Noting that the security threshold BER $< 11.0\%$ translates into $V > 78.0\%$ while the insecurity threshold BER $\geq 14.6\%$ corresponds to $V \leq 70.7\%$, we conclude that our setup transforms a BB84 protocol which is insecure (or of unknown security) into a provably secure one. Note that the visibilities were also tested for the other possible values of $\phi_A = \pi/2, \pi, 3\pi/2$ used in the BB84 protocol and for both ports P_1 and P_2. The visibilities all exceeded 97.2% in the case where no noise is added. The lowest visibilities are associated with the cases where Alice and Bob choose the $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ basis since then both parties must apply a potential to their polarization-sensitive phase modulator which makes the setup noisier.

In Figure 9.2, the visibilities were measured in a regime where the overall number of photons in all time bins when they leave Alice's site is approximately 120 photons. In this way, the dark counts of the detector are negligible. To consider a realistic QKD implementation, we also ran the experiment in the single-photon regime, where the quantum state sent by Alice back to Bob contains approximately 0.8 photons in total. The difficulty in this case is that dark counts become very important (they give a raw

error rate of about 30%) because we use 3-ns pulses [3]. Nevertheless, we were able to show in this regime that a visibility of 69.4% ±0.2% in the absence of filtration can be turned into 78.8% ±0.2% by filtration (where the statistical error due to subtracting the dark counts was calculated for a 95% confidence level), see open circles in Fig. 9.2. These visibilities are averaged over all four choices of ϕ_A and for the two output ports P_1 and P_2, so they are the relevant quantities for characterizing a QKD scheme. This averaging explains why these points lie slightly off the curves in Fig. 9.2. Note that in QKD the errors due to the dark counts can in principle be removed using error correction codes without altering the security, although in practice this is probably impossible for the high level of dark counts we have here.

We conclude by comparing this method with other QKD schemes that use higher dimensional systems [CBKG02]. The noise model in both cases is the same: a d-dimensional state $|\psi\rangle$ entering the communication channel exits as $\rho = e^{-\sigma^2}|\psi\rangle\langle\psi| + (1 - e^{-\sigma^2})I/d$. This makes the comparison meaningful. The QKD schemes based on sets of mutually unbiased bases considered in [CBKG02] can only tolerate a noise level up to $e^{-\sigma^2} < 1/2$. This is because when $e^{-\sigma^2} = 1/2$, there is a simple attack in which the eavesdropper (Eve) does not modify the state with probability 1/2, while, with probability 1/2, she keeps the state and sends a random one instead. In contrast, error filtration can tolerate arbitrarily high levels of noise if the dimensionality d of the Hilbert space is sufficiently large since the visibility V_d tends to 1 for large d and fixed $e^{-\sigma^2}$. The reason why the above attack no longer works in the case of error filtration is that when Eve replaces the quantum state by a random one, the filtration preferentially removes the corresponding noisy term. In other words, the noise is replaced by a higher effective loss. Nevertheless, this also means that a QKD scheme using error filtration can be vulnerable to attacks which exploit loss. For instance, if Alice sends attenuated coherent states, Eve could use a photon-number splitting attack, see [GRTZ02] and references therein. In fact, our setup would probably be insecure against such attacks since we used attenuated coherent states with 0.8 photons on average and were very close to the limit of provably secure QKD. This is not a fundamental problem and could be remedied by further attenuating the states or by using better approximations of single-photon sources.

[3] By using shorter laser pulses, we should be able to decrease the dark count rate by at least a factor of 10.

4.4 Conclusion

The present experiment demonstrates the optical part of a quantum key distribution scheme which can operate with a phase-noise level that is too high for a standard implementation of the BB84 to be secure. This demonstrates the power and simplicity of error filtration as a practical method for circumventing phase noise in quantum communication. In the next chapter, we will tackle yet another problem in QKD which is more of a technological inconvience rather than a fundamental drawback but is nevertheless very important for practical QKD. This is the problem of generating random numbers which, with present day technology, is responsible for the slow rate at which a secret key is created. We present a solution that greatly reduces the need for random numbers which implies encoding successive qubits drawn from the same basis. We show that Eve cannot gain more information than what is possible with traditional QKD protocols.

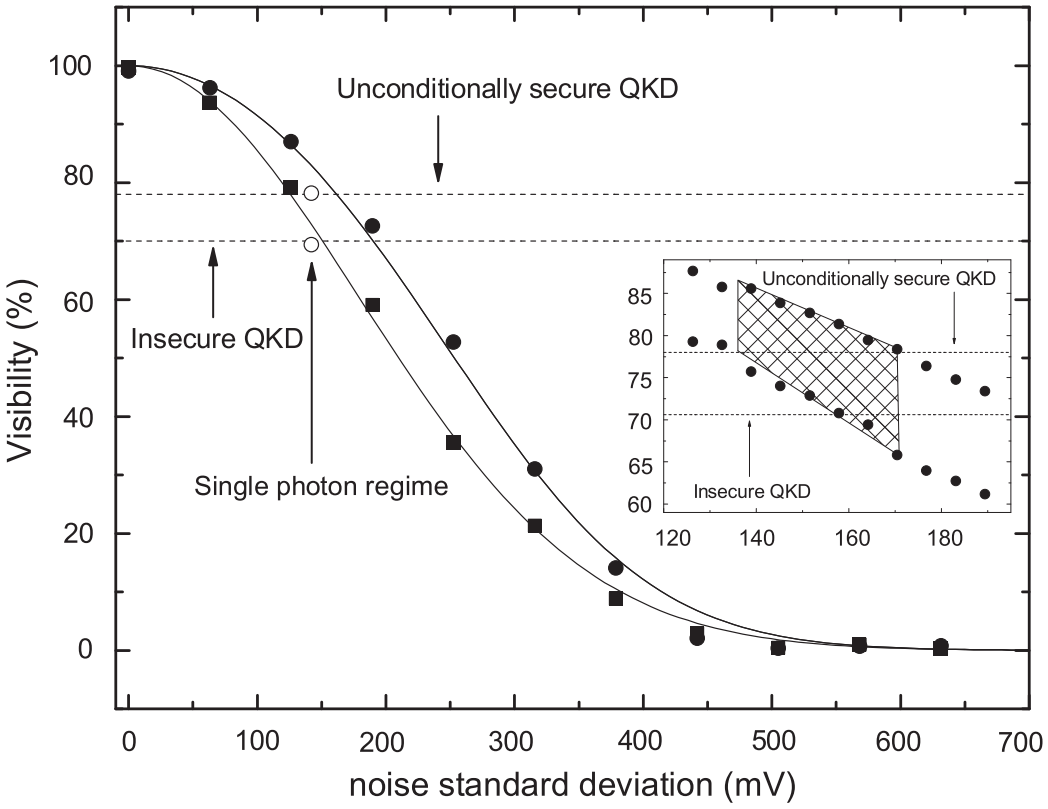

Figure 4.6: Visibility (detector dark counts subtracted) as a function of the standard deviation of the noise signal produced by the function generator. The proportionality factor between the x-axis and σ was determined by fitting the experimental data without filtration with Eq. (4.11). The squares (full circles) represent the measured visibilities without (with) filtration, while the curves are the theoretical predictions of Eqs. (4.11) and (4.14). The open circles show filtration in the single-photon regime. The inset magnifies the data in the region where one passes from an insecure ($V \leq 70.7\%$) to a secure ($V > 78.0\%$) QKD protocol. The criss-crossed area shows that a visibility that is either insecure or of unknown security can be increased to a provably secure one. By making the statistics over 200,000 runs, the error bars were made smaller than the plotting points.

Chapter 5

Reduced Randomness in Quantum Key Distribution

5.1 Introduction

As we have seen in the introductory chaper, the security of QKD is based on two main ingredients. The first refers to the impossibility of perfectly cloning some unknown quantum state selected from a nonorthogonal set. As a result, Eve cannot clone the quantum state transmitted by Alice and re-transmit it undisturbed to the receiver Bob. The second ingredient, although often mentioned only implicitly in the litterature, is also an absolute requirement: truly random numbers must be available on both Alice's and Bob's sides. Indeed, with pseudo-random number generators, the sequence of choices made by Alice and Bob could in principle be predicted by Eve if the seed is known to her. Clearly, quantum cryptography should use quantum randomness. But, in practice, this is a severe constraint because a complete protocol requires a huge amount of random numbers, from Alice's state choices to Bob's basis choices, as well as for the random choices and random permutations needed in error correction and privacy amplification. Making high-speed quantum random-number generators is a big technological challenge, so that most realizations of quantum cryptography today rely on an active [1] choice that uses a standard random-number generator. It is therefore of a great importance to investigate whether this requirement of high-rate

[1]Note that if the choice is passive, based on quantum effects (e.g. the photon being detected at one or the other output port of a beam splitter at Bob's station), then it is still not completely equivalent to using a quantum random-number generator. Indeed, in the latter case, the photon involved in the random-number generation is generated locally, and has not been transmitted over the line and potentially tapped by Eve.

random number generation can be relaxed, at least in part.

In this chapter, we consider a variant of the BB84 or six-state protocols in which the basis chosen for encoding is kept unchanged over long sequences of qubits instead of being drawn at random for each qubit. Quite surprisingly, we show that, if the sequences are much shorter than the key, the security is unaffected by this modification of the protocol although the random number generation rate is significantly reduced. The BB84 and six-state protocols are amongst the cryptographic schemes for which the security has exhaustively been studied. Since it has been shown that the optimal eavesdropping strategy for these two protocols coincide with approximate cloning [CBKG02], we restrict our analysis to cloning-based attacks.

We consider the cloning of sequences of N qubits. In each sequence the qubits are prepared in the same basis, but the state is chosen at random among the basis states. This is viewed as the optimal avesdropping attack against a quantum cryptographic protocol in which we do not restrict Alice and Bob to make random choices of bases for every qubit, but allow them to use the same basis for the entire length-N sequence (N is assumed to be publicly known and much smaller than the size of the key). That is, for each sequence, Alice and Bob make new and independent random choices of bases. At first sight, one could imagine that this encoding would increase Eve's knowledge about the secret key, but we shall see that for the class of cloning transformations we have studied, this is not the case: Eve's optimal cloning attack provides her with no more Shannon information, for a given quantum bit error rate, than in the usual case where Alice and Bob make random basis-choices for each qubit and Eve applies a cloning attack on each qubit. Under the assumption that this class of approximate cloning transformations corresponds to the optimal eavesdropping strategy, we have thus proven that the requirement for random number generation can be reduced without impairing on the security against finite-size attacks.

5.2 General quantum cloning formalism

We refer to the double-Bell state ansatz as defined in Chapter 1 which we adapt here for this new scenario. Considering an arbitrary state $|\psi\rangle$ in a 2^N-dimensional Hilbert space (the Hilbert space of N consecutive qubits), we wish to produce two (approximate) clones. The class of cloning transformations we will analyze implies

that if the input state is $|\psi\rangle$ (in what follows this state will be the composite state of N qubits), then the resulting joint state of the two output clones (noted E for Eve and B for Bob) and the ancillary system (noted C) is:

$$\begin{aligned} |\psi\rangle \rightarrow & \sum_{\overline{m},\overline{n}=0}^{2^N-1} a_{\overline{m},\overline{n}} U_{\overline{m},\overline{n}} |\psi\rangle_E |B_{\overline{m},\overline{n}}\rangle_{B,C} \\ = & \sum_{\overline{m},\overline{n}=0}^{2^N-1} b_{\overline{m},\overline{n}} U_{\overline{m},\overline{n}} |\psi\rangle_B |B_{\overline{m},\overline{n}}\rangle_{E,C} \end{aligned} \tag{5.1}$$

where the couple $\{\overline{m},\overline{n}\} \Leftrightarrow \{m_1 \dots m_N, n_1 \dots n_N\}$ and $m_i, n_i \in \{0,1\}$. Here, E, B and C are 2^N-dimensional systems and $U_{\overline{m},\overline{n}}$ is defined as

$$U_{\overline{m},\overline{n}} = \bigotimes_{i=1}^{N} X^{m_i} Z^{n_i}, \tag{5.2}$$

where $X^{m_i} Z^{n_i}$ represents the identity and the three Pauli matrices

$$\begin{aligned} X^0 Z^0 &= I \\ X^1 Z^0 &= \sigma_X \\ X^0 Z^1 &= \sigma_Z \\ X^1 Z^1 &= -i\sigma_Y. \end{aligned}$$

Here, $|B_{\overline{m},\overline{n}}\rangle$ is defined as

$$|B_{\overline{m},\overline{n}}\rangle = \sum_{\overline{k}=0}^{2^N-1} (-1)^{(\overline{k}\cdot\overline{n})} |\overline{k}\rangle |\overline{k}+\overline{m}\rangle \tag{5.3}$$

where $\overline{k}\cdot\overline{n}$ represents the bitwise scalar product, i.e. $\overline{k}\cdot\overline{n} = \sum_i k_i n_i$. Thus, $U_{\overline{m},\overline{n}}$ is the tensor product of N Pauli matrices each acting on a two-dimensional subsystem. An error operator U_{m_i,n_i} is associated to each subsystem. Such an operator shifts the state by m_i units (modulo 2) in the computational basis, and multiplies it by a phase so as to shift its Fourier transform by n_i units (modulo 2). Eq. (9.3) defines the d^2 generalized Bell states for a pair of 2^N-dimensional systems with $|B_{\overline{m},\overline{n}}\rangle = \left(U_{\overline{m},\overline{n}} \otimes \mathbb{1}\right) |B_{\overline{0},\overline{0}}\rangle$. Tracing over systems B and C (or E and C) yields the final states of clone E (or clone B): if the input state is $|\psi\rangle$, the clones E and B are in a mixture of the states $|\psi_{\overline{m},\overline{n}}\rangle = U_{\overline{m},\overline{n}}|\psi\rangle$ with respective weights $p_{\overline{m},\overline{n}}$ and $q_{\overline{m},\overline{n}}$:

$$\begin{aligned} \rho_E &= \sum_{\overline{m},\overline{n}=0}^{2^N-1} p_{\overline{m},\overline{n}} |\psi_{\overline{m},\overline{n}}\rangle\langle\psi_{\overline{m},\overline{n}}| \\ \rho_B &= \sum_{\overline{m},\overline{n}=0}^{2^N-1} q_{\overline{m},\overline{n}} |\psi_{\overline{m},\overline{n}}\rangle\langle\psi_{\overline{m},\overline{n}}| \end{aligned} \tag{5.4}$$

In addition, the weight functions of the two clones ($p_{\overline{m},\overline{n}}$ and $q_{\overline{m},\overline{n}}$) are related by

$$p_{\overline{m},\overline{n}} = |a_{\overline{m},\overline{n}}|^2, \quad q_{\overline{m},\overline{n}} = |b_{\overline{m},\overline{n}}|^2, \tag{5.5}$$

where $a_{\overline{m},\overline{n}}$ and $b_{\overline{m},\overline{n}}$ are two (complex) amplitude functions that are dual under N two-dimensional Fourier transforms:

$$b_{\overline{m},\overline{n}} = \frac{1}{2^N} \sum_{\overline{x},\overline{y}=0}^{2^N-1} (-1)^{\overline{n}\cdot\overline{x}-\overline{m}\cdot\overline{y}} a_{\overline{x},\overline{y}}. \tag{5.6}$$

The fidelity of a clone, say E, is given by

$$F_E = \langle\psi|\rho_E|\psi\rangle = \sum_{\overline{m},\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 |\langle\psi|U_{\overline{m},\overline{n}}|\psi\rangle|^2 \tag{5.7}$$

and similarly for the B clone (replace the $|a_{\overline{m},\overline{n}}|^2$ term by $|b_{\overline{m},\overline{n}}|^2$).

5.3 BB84 protocol with 2-qubit correlated bases

In this section we compare the amount of information that can be gained by Eve when performing a cloning attack on individual qubits (two-dimensional) and on pairs of qubits (four-dimensional) which may have been chosen from correlated bases. We study here how this affects the BB84 protocol and in the next section we move on to the six-state protocol.

Recall that in the BB84 protocol, Alice chooses from states belonging to two mutually unbiased bases. Alice and Bob choose the first basis as the computational basis (eigenstates of σ_Z) $\{|0\rangle, |1\rangle\}$ and the second as the dual basis (eigenstates of σ_X) $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$.

5.3.1 BB84 - single qubit attack - no basis correlation

If Eve chooses to clone the qubits individually, she must use a cloning strategy which is optimal for this set of states. When using the double-Bell ansatz described in Sec. 5.2, one can easily verify that the expression of the fidelity for all states of a given basis is the same. Here and throughout the rest of this chapter, we consider fidelities as expressed by Eq. (9.6). Particularly for Eve's clone one finds that the fidelity for the computational basis is $F_E = |a_{0,0}|^2 + |a_{0,1}|^2$ and the dual basis is $F_E = |a_{0,0}|^2 + |a_{1,0}|^2$. A cloning machine that acts equally well for this set of states

implies $|a_{0,0}|^2 + |a_{0,1}|^2 = |a_{0,0}|^2 + |a_{1,0}|^2$. Since there is *a priori* no reason why the optimal values of these elements be different from each other, we make the hypothesis that they should all be equal and real. Furthermore, we extend our hypothesis to the remaining element, $|a_{1,1}|^2$ such that the form of the amplitude matrix reduces to:

$$a_{\overline{m},\overline{n}} = \begin{pmatrix} v & x \\ x & y \end{pmatrix}. \tag{5.8}$$

Eve's fidelity is now expressed as $F_E = v^2 + x^2$ and normalization requires $v^2 + 2x^2 + y^2 = 1$. Bob's clone can be characterized by a similar amplitude matrix by making the same hypotheses:

$$b_{\overline{m},\overline{n}} = \begin{pmatrix} v' & x' \\ x' & y' \end{pmatrix}, \tag{5.9}$$

where the different matrix elements are related to the $a_{m,n}$ coefficients by Eq. (9.5). Thus, Bob's fidelity is $F_B = v'^2 + x'^2$ in both bases and the corresponding mutual information between Alice and Bob (if the latter measures his clone in the good basis) is given by

$$I(A,B) = 1 + F_B \log_2 F_B + (1 - F_B) \log_2 (1 - F_B). \tag{5.10}$$

Maximizing Eve's fidelity F_E for a given value of Bob's fidelity F_B under the normalization constraint yields

$$\begin{aligned} v &= \frac{1}{2} + \sqrt{F_B(1 - F_B)} \\ x &= F_B - \frac{1}{2} \\ y &= \frac{1}{2} - \sqrt{F_B(1 - F_B)} \end{aligned}$$

such that the corresponding optimal fidelity for Eve is

$$F_E = \frac{F_B}{2} + \frac{1 - F_B}{2} + \sqrt{F_B(1 - F_B)}. \tag{5.11}$$

Under the assumption that Alice and Bob exchange many sequences which are short in comparison to the size of the total key, Alice and Bob can rely on the randomness of the sequence basis distribution to guaranty the security of their exchange. As we have seen, Csiszár and Körner's theorem provides a lower bound on the rate R at which Alice and Bob can generate secret key bits using privacy amplification:

$$R \geq \max\big[I(A,B) - I(A,E), I(A,B) - I(B,E)\big]. \tag{5.12}$$

It is therefore a sufficient condition that $I(A,B) > I(A,E)$ in order to establish a secret key with non-zero rate for one way communication channels. It has been shown in [CBKG02] that Bob and Eve's information curves intersect exactly where the fidelities coincide because, in this particular case, the mutual information shared between Alice and Eve is also expressed by Eq. (5.10). This yields the optimal symmetric fidelity of phase covariant cloning [BCdM00]

$$F_E = F_B = \frac{1}{2} + \frac{1}{\sqrt{8}} \simeq 0.8536. \tag{5.13}$$

Note that this result is independent of the fact that Alice may have chosen to encode sequences of consecutive qubits in the same basis since Eve is intercepting them individually.

5.3.2 BB84 - two qubit attack - no correlation

Suppose now that Eve intercepts the qubits in sequences of two and clones them. We make the same assumption as before, namely that Alice has randomly chosen the basis she has encoded her qubit with. We would like to know if Eve can gain more information per qubit using this cloning approach as opposed to cloning them individually. Our first task is to determine the set of states that she will have to clone. If Alice chooses among the computational and dual bases, the possible sequences Eve might encounter are products of eigenstates of $\sigma_Z^{\otimes 2}$: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, products of eigenstates of $\sigma_X^{\otimes 2}$:

$$\begin{aligned}
&\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle),\\
&\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle),\\
&\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle),\\
&\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle),
\end{aligned}$$

and products between eigenstates of these two bases ($\sigma_Z \otimes \sigma_X$ and $\sigma_X \otimes \sigma_Z$):

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(|00\rangle \pm |01\rangle) \quad , \quad \frac{1}{\sqrt{2}}(|10\rangle \pm |11\rangle)\\
&\frac{1}{\sqrt{2}}(|00\rangle \pm |10\rangle) \quad , \quad \frac{1}{\sqrt{2}}(|01\rangle \pm |11\rangle).
\end{aligned}$$

Because we are now dealing with a *four*-dimensional Hilbert space ($N = 2$) with tensor product structure, the $U_{\overline{m},\overline{n}}$ operators take the following form:

$$U_{m_1m_2;n_1n_2} = \begin{pmatrix} I & Z \\ X & Y \end{pmatrix} \otimes \begin{pmatrix} I & Z \\ X & Y \end{pmatrix}$$

Each of these matrix elements consists in a tensor product of two Pauli operators each acting on an associated qubit. Eve is interested in the information she can gain from a single qubit when she clones them in sequences of two. In other words, Eve is interested in the optimal *four*-dimensional cloning map where the figure of merit is not the single-clone *four*-dimensional fidelity but rather the single-clone, single-qubit *two*-dimensional fidelity averaged over the two qubits. To obtain this fidelity, we must trace over the second qubit subsystem and compute the fidelity of the first qubit, repeat this operation for the second qubit by tracing out the first qubit subsystem and finally average over the two fidelities. For example, the reduced density matrix of the first qubit for Eve's clone is expressed as:

$$\begin{aligned} \rho_E^1 &= \mathrm{Tr}_2\big[\sum_{\overline{m},\overline{n}} |a_{\overline{m},\overline{n}}|^2 X^{m_1} Z^{n_1} |\phi_1\rangle\langle\phi_1| Z^{n_1} X^{m_1} \\ &\quad \otimes X^{m_2} Z^{n_2} |\phi_2\rangle\langle\phi_2| Z^{n_2} X^{m_2} \big] \\ &= \sum_{\overline{m},\overline{n}} |a_{\overline{m},\overline{n}}|^2 X^{m_1} Z^{n_1} |\phi_1\rangle\langle\phi_1| Z^{n_1} X^{m_1} \end{aligned}$$

where $|\phi_i\rangle$ is a two-dimensional system. For sequences of qubits both drawn from eigenstates of σ_Z the fidelity is

$$\begin{aligned} F_{E,zz}^1 &= \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 |\langle\phi_1| X^{m_1} Z^{n_1} |\phi_1\rangle|^2 \\ &= \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{m_1,0} \end{aligned} \tag{5.14}$$

for the first qubit and

$$\begin{aligned} F_{E,zz}^2 &= \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 |\langle\phi_2| X^{m_2} Z^{n_2} |\phi_2\rangle|^2 \\ &= \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{m_2,0} \end{aligned} \tag{5.15}$$

for the second qubit. For clusters of qubits both drawn from eigenstates of σ_X the fidelity is

$$F^1_{E,xx} = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{n_1,0} \tag{5.16}$$

for the first qubit and

$$F^2_{E,xx} = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{n_2,0} \tag{5.17}$$

for the second qubit. To be complete, we must also compute the fidelity for clusters expressed as tensor products drawn from eigenstates of $\sigma_Z \otimes \sigma_X$ and $\sigma_X \otimes \sigma_Z$. The former yields $F^1_{E,zx} = F^1_{E,zz}$ for the first qubit and $F^2_{E,zx} = F^2_{E,xx}$ for the second qubit. The latter yields a fidelity of $F^1_{E,xz} = F^1_{E,xx}$ for the first qubit and $F^2_{E,xz} = F^2_{E,zz}$ for the second qubit. The expressions for these fidelities F^i_E can easily be interpreted as follows. Every single-qubit fidelity consists in a sum of eight terms for which the first four express the fidelity of the $four$-dimensional system in question (in other words the contribution from the $a_{\overline{m},\overline{n}}$ coefficients where no errors occur on either qubits) while the remaining four terms correspond to the $a_{\overline{m},\overline{n}}$ coefficients for which the i^{th} qubit is not affected by an error but the remaining one is. Generally, the fidelity of the i^{th} qubit is expressed as

$$F^i_E = F_{4E} + D^i_E \tag{5.18}$$

where F_{4E} is the fidelity of the $four$-dimensional system and D^i_E is the disturbance of the i^{th} qubit and is expressed as

$$D^i_E = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{m_i,1}\, \delta_{m_{\neg i},0} \tag{5.19}$$

for qubits drawn from the computational basis and

$$D^i_E = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{n_i,1}\, \delta_{n_{\neg i},0} \tag{5.20}$$

for qubits drawn from the dual basis. Here, the qubit of the pair which is not the i^{th} qubit is given the index $\neg i$. The average qubit fidelity of Eve's clone is therefore:

$$F_E = F_{4E} + \frac{1}{2}(D^1_E + D^2_E). \tag{5.21}$$

A similar analysis can be made for Bob's clone from which we obtain a single-qubit fidelity

$$F_B = F_{4B} + \frac{1}{2}(D_B^1 + D_B^2) \tag{5.22}$$

which is function of the $b_{\overline{m},\overline{n}}$ coefficients. We are again interested in the mutual information shared between Alice and Bob and Alice and Eve. To do this, let us first compute Eve's optimal fidelity F_E for a fixed value of Bob's fidelity F_B under the normalization constraint

$$\sum_{\overline{m}=0,\overline{n}=0}^{3} |a_{\overline{m},\overline{n}}|^2 = 1 \tag{5.23}$$

and the constraint that the single-qubit fidelity be the same for all 16 considered input states. The optimization yields the following $a_{\overline{m},\overline{n}}$ matrix:

$$a_{\overline{m},\overline{n}} = \begin{pmatrix} v_1 & x_1 \\ x_1 & y_1 \end{pmatrix} \otimes \begin{pmatrix} v_2 & x_2 \\ x_2 & y_2 \end{pmatrix} \tag{5.24}$$

where

$$\begin{aligned} v_1 = v_2 &= \frac{1}{2} + \sqrt{F_B(1-F_B)} \\ x_1 = x_2 &= F_B - \frac{1}{2} \\ y_1 = y_2 &= \frac{1}{2} - \sqrt{F_B(1-F_B)} \end{aligned}$$

such that

$$F_E = \frac{F_B}{2} + \frac{1-F_B}{2} + \sqrt{F_B(1-F_B)}. \tag{5.25}$$

From the previous subsection we know that Bob and Eve's information curves intersect exactly where the fidelities coincide. This implies that Alice and Bob can share secret bits via privacy amplification as long as $F_B > F_E$, that is

$$F_B > \frac{1}{2} + \frac{1}{\sqrt{8}}. \tag{5.26}$$

This optimal symmetric fidelity turns out to be the same as the optimal fidelity obtained when the cloner is designed for *two*-dimensional systems meaning that the optimal *four*-dimensional cloning map for single-qubit single-clone fidelity boils down to the tensor product of the *two*-dimensional optimal cloners.

5.3.3 BB84 - two qubit attack - correlated bases

Now consider the situation where Alice is limited by her random number generator and must therefore send two consecutive states drawn from the same basis in order to keep a decent cadence [qua]. Of course if Eve intercepts every qubit individually, the fidelity she obtains after cloning is just the same as before, namely $F = \frac{1}{2} + \frac{1}{\sqrt{8}}$. If she intercepts them in sequences of two qubits she will necessarily find that they are correlated: either she expects to find two qubits drawn from the computational basis σ_Z (equivalently, a four dimensional state drawn from the eigenstates of $\sigma_Z \otimes \sigma_Z$) or two qubits drawn from the dual basis σ_X (equivalently, a four dimensional state drawn from the eigenstates of $\sigma_X \otimes \sigma_X$). Compared to the previous situation where no correlation was present, the set of input states Eve has to consider has now decreased. Intuitively we should expect that the optimal single-qubit cloner would give rise to a higher fidelity. We shall see that this is not the case.

The cloner we consider is again characterized by the double-Bell ansatz (5.1) such that the single-qubit fidelity for this set of input states is defined exactly like Eqs. (5.14) and (5.15) for eigenstates of σ_Z and like Eqs. (5.16) and (5.17) for eigenstates of σ_X. These are the four expressions of the fidelity for which the $a_{\overline{m},\overline{n}}$ (and consequently the $b_{\overline{m},\overline{n}}$) coefficients must be optimized for. The constraints we must consider here are the normalization constraint and the constraint that these four expressions be equal. Of course, these fidelities are again characterized by Eq. (5.21). Interestingly, the constrained optimization yields $a_{\overline{m},\overline{n}}$ coefficients which have exactly the same form as Eq. (5.24) and therefore the same expressions for Eve's fidelity as a function of Bob's. Once again, the lower bound on the mutual information Alice and Bob must share in order to generate a secret key is given by

$$F > \frac{1}{2} + \frac{1}{\sqrt{8}}. \tag{5.27}$$

We conclude that even if Alice chooses to encode two consecutive states in the same basis, Eve's optimal cloning strategy does not permit her to gain more information than complete random choices. In Section V we will generalize this idea for sequences of N qubits, but first let us examine how these cloning strategies apply to the six-state protocol.

5.4 Six-state protocol with 2-qubit correlated bases

The six-state protocol is very similar to the BB84 protocol, the only difference being that Alice now has the choice to pick up states from a third basis MU to the other two. Again, let us choose the first two bases as the computational basis and the dual basis and let the third basis be the eigenstates of σ_Y: $\{\frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)\}$.

5.4.1 six-state - single qubit attack - no correlation

The cloner that must be used for the six-state protocol is an asymmetric *two*-dimensional universal cloner [CBKG02] characterized by the same amplitude matrix as Eq. (5.8) except that we make the change $y = x$:

$$a_{\overline{m},\overline{n}} = \begin{pmatrix} v & x \\ x & x \end{pmatrix}.$$

Eve's fidelity is expressed as $F_E = v^2 + x^2$ and normalization requires $v^2 + 3x^2 = 1$. Maximizing her fidelity for a fixed value of Bob's fidelity yields the optimal cloner:

$$v = \sqrt{\frac{3F_B - 1}{2}}$$
$$x = \sqrt{\frac{1 - F_B}{2}}.$$

Bob's clone is characterized by a similar amplitude matrix:

$$b_{\overline{m},\overline{n}} = \begin{pmatrix} v' & x' \\ x' & x' \end{pmatrix}, \tag{5.28}$$

where as before, v' and x' are given by Eq. (9.5) while the mutual information he shares with Alice by Eq. (5.10). It has been shown in [CBKG02] that the mutual information shared between Alice and Eve for the six-state protocol is given by

$$\begin{aligned} I(A,E) = 1 &+ (F_B + F_E - 1)\log_2\left(\frac{F_B + F_E - 1}{F_B}\right) \\ &+ (1 - F_E)\log_2\left(\frac{1 - F_E}{F_B}\right) \end{aligned} \tag{5.29}$$

such that for a given F_B, $I(A,E)$ is lower than for the BB84 protocol which is consistent with the stronger requirement we put on that cloner. This implies that the fidelity F_B for which $I(A,E) = I(A,B)$ is slightly lower, and equal to $F_B \simeq 0,8436$.

5.4.2 six-state - two qubit attack - no basis correlation

If Eve chooses to clone the incoming states in sequences of two, the set of four-dimensional states she has to clone consists of tensor products of states belonging to the three maximally unbiased bases above. The single-qubit fidelity is computed as above, with the exception that there are extra constraints, namely that the fidelity should also clone equally well eigenstates of σ_Y:

$$F^1_{E,yy} = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{m_1,n_1}$$

for the first qubit and

$$F^2_{E,yy} = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{m_2,n_2}$$

for the second qubit. The other constraints come from tensor products of $\sigma_Y \otimes \sigma_Z$, $\sigma_Y \otimes \sigma_X$ and vice-versa. The expression for the fidelity of the i^{th} qubit can be expressed as:

$$F^i_E = F_{4E} + D^i_E \tag{5.30}$$

where, for eigenstates of σ_Y,

$$D^i_E = \sum_{\overline{m}=0,\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 \delta_{m_i,n_i+1}\, \delta_{m_{\neg i},n_{\neg i}}. \tag{5.31}$$

The average qubit fidelity is again:

$$F_E = F_{4E} + \frac{1}{2}(D^1_E + D^2_E). \tag{5.32}$$

As before a similar analysis can be made for Bob's clone from which we obtain a single-qubit fidelity

$$F_B = F_{4B} + \frac{1}{2}(D^1_B + D^2_B). \tag{5.33}$$

We are again interested in the mutual information shared between Alice and Bob, and Alice and Eve. We compute Eve's optimal fidelity F_E for a fixed value of Bob's fidelity F_B under the normalization constraint Eq.(9.18) and the constraint that the single-qubit fidelity be the same for all input states. The optimization yields the following $a_{\overline{m},\overline{n}}$ matrix:

$$a_{\overline{m},\overline{n}} = \begin{pmatrix} v_1 & x_1 \\ x_1 & x_1 \end{pmatrix} \otimes \begin{pmatrix} v_2 & x_2 \\ x_2 & x_2 \end{pmatrix} \tag{5.34}$$

where

$$v_1 = v_2 = \sqrt{\frac{3F_B - 1}{2}}$$
$$x_1 = x_2 = \sqrt{\frac{1 - F_B}{2}}$$

such that

$$F_E = 1 - \frac{F_B}{2} + \frac{1}{4}\sqrt{6F_B - 2}\sqrt{2 - 2F_B}. \tag{5.35}$$

In the previous subsection, we have seen how to express $I(A, B)$ and $I(A, E)$. Again in this case the lower bound on Bob's fidelity needed for $I(A, B) > I(A, E)$ is given by $F_B > 0.8436$ which is the same fidelity for individual attacks. Thus, so far, we arrive to the same conclusions as for the BB84 protocol.

5.4.3 six-state - two qubit attack - correlated bases

If Alice is again limited by her random number generator and must encode two consecutive qubits in the same basis, Eve can clone the incoming states by sequences of two expecting to find four-dimensional states expressed as eigenstates of $\sigma_Z \otimes \sigma_Z$, $\sigma_X \otimes \sigma_X$ or $\sigma_Y \otimes \sigma_Y$. By making a similar reasoning as in the previous subsection we arrive to the same conclusions as before, namely that the information Eve can gain when cloning a $four$-dimensional system boils down to the optimal single qubit information.

5.5 Cloning of N-qubit sequences

We now proceed to generalize the cloning strategies considered in the previous sections. We suppose that Alice encodes her qubits using the same basis for sequences of N qubits. We also suppose that N is much smaller than the total size of the raw key she will be exchanging with Bob. We also suppose that Eve is aware of when a new sequence begins and ends. Generally, for a sequence of N qubits, the reduced density matrix of the i^{th} qubit for a given clone (say E) is written as

$$\begin{aligned}\rho_E^i &= \mathrm{Tr}_{j\neq i} \sum_{\overline{m},\overline{n}} |a_{\overline{m},\overline{n}}|^2 \bigotimes_{j=1}^{N} X^{m_j} Z^{n_j} |\phi_j\rangle\langle\phi_j| Z^{n_j} X^{m_j} \\ &= \sum_{\overline{m},\overline{n}} |a_{\overline{m},\overline{n}}|^2 X^{m_i} Z^{n_i} |\phi_i\rangle\langle\phi_i| Z^{n_i} X^{m_i},\end{aligned} \tag{5.36}$$

such that fidelity of the j^{th} qubit is written as

$$F_E^j = F_{E2^N} + D_E^j \tag{5.37}$$

and similarly for qubits of Bob's clone. The average qubit fidelity is therefore expressed as:

$$F_E = F_{E2^N} + \frac{1}{N}\sum_{i=1}^{N} D_E^i. \tag{5.38}$$

If we assume that the optimal $a_{\overline{m},\overline{n}}$ amplitude matrices are expressed as

$$a_{\overline{m},\overline{n}} = \begin{pmatrix} v & x \\ x & y \end{pmatrix}^{\otimes N} \tag{5.39}$$

for the BB84 protocol and

$$a_{\overline{m},\overline{n}} = \begin{pmatrix} v & x \\ x & x \end{pmatrix}^{\otimes N} \tag{5.40}$$

for the six-state protocol, we can check that they indeed satisfy a constrained optimization. Since the information curves are both monotonically increasing functions of the fidelities, we use the Lagrange multiplier method to optimize Eve's fidelity for a fixed value of Bob's.

The constraint that the fidelity for different qubits in the sequence be the same is already satisfied by the hypothesized $a_{\overline{m},\overline{n}}$ matrix. The function is:

$$\begin{aligned}
\mathcal{L} &= F_E + \lambda_1 F_B + \lambda_2\Big(\sum_{\overline{m},\overline{n}=0}^{2^N-1} |a_{\overline{m},\overline{n}}|^2 - 1\Big) \\
&= \frac{1}{N}\sum_{\overline{m}=0}^{N}(N - \sum_{i=1}^{N} m_i)\prod_{i=1}^{N}(v^2+x^2)^{m_i\oplus 1}(x^2+y^2)^{m_i} \\
&+ \lambda_1\Big[\frac{1}{N}\sum_{\overline{m}=0}^{N}(N - \sum_{i=1}^{N} m_i)\prod_{i=1}^{N}(\frac{1}{2}+vx+xy)^{m_i\oplus 1}(\frac{1}{2}-vx-xy)^{m_i}\Big] \\
&+ \lambda_2\Big[(v^2+2x^2+y^2)^N - 1\Big]
\end{aligned} \tag{5.41}$$

where the modular sum is in base 2. The equivalent expression of Eq. (5.41) for the six-state protocol is very similar except that one should exchange y^2 for x^2.

We have checked, using a symbolic calculator, that the hypothesized amplitude matrices satisfy the constrained optimization and yield the optimal fidelities (Eqs. (5.25) and (5.35)) for $N = 2$ and $N = 3$.

5.6 Conclusion

We have considered the cloning of sequences of N qubits, where all the qubits in each sequence are prepared in the same basis while each state is chosen at random. This situation is very different from the usual scenario of cloning multiple copies, where all the copies are prepared in the same state. Our investigation was motivated by the situation in quantum cryptography where the legitimate users are required to make truly random choices for each single qubit. From a practical point of view, this requirement on high-rate random-number generation is a severe constraint. Indeed, high-rate quantum random number generators on the market today produce much lower rates than the anticipated high-rate (e.g. 100Mb/s) quantum key distribution of the future.

However, under the assumption that the class of cloning transformations we considered here provides the optimal eavesdropping strategy, we have shown that this requirement can be relaxed, so that Alice can prepare long sequences of qubits in the same basis without compromising the security. Surprisingly, Eve cannot exploit her knowledge that the used basis is fixed for the entire sequence, regardless of its length provided it is much shorter that the total key size. The constraint on the sequence size is necessary because even though we assume Alice and Bob to exchange qubits encoded by a single photon source (i.e. Eve cannot exploit photon number splitting attacks), Eve could still make a naive attack where she randomly guesses the value of the basis for each sequence. For example in the extreme case where the sequence is the same size as the key, i.e. when the variance of the information gain is high, Eve would, with probability $\frac{1}{2}$, completely guess the secret key. Conversely, when $N = 1$ (i.e. the standard BB84 or six-state protocol) the variance will be lower and implies that the optimal eavesdropping strategy is achieved through cloning. In order to avoid this security threat, Alice and Bob should choose N in such a way that the variance of the information gain implies that the optimal strategy Eve should use remains the single-qubit cloning strategies utilized in the original BB84 and six-state protocols. We leave as an open question as to which bounds can be achieved. Nevertheless, even with reasonably low values of the sequence size, such as $N = 10$, the saving of the random bits is already significant (in this case, 45%). This result is quite important for practical applications of quantum cryptography as it implies that higher secret-key rates may be obtained using the same random number generator but with this new modified protocol.

Chapter 6

Experimental quantum bit string generation

6.1 Introduction

Let us now turn to another kind of cryptographic task which has recently gained much attention in the field of quantum communication. In contrast to key distribution where two parties wish to generate a secret key without having a third party intrude, there exist another branch of cryptography which arise when $mistrutful$ parties need to generate, process or exchange information within a given degree of security. This is an especially difficult task to fulfill when the two parties are seperated because of the lack of confidence they have in the actions of their adversary. In this chapter, we solve this problem by introducing the concept of quantum *coin tossing* or, more specifically, quantum *bit-string generation* and describe an original experimental implementation of the latter which is greatly inspired from the plug and play method.

Coin tossing was introduced by Manuel Blum in 1981 [Blu81]. The aim is for two parties who do not trust each other to generate a common random bit. Coin tossing is an important primitive with many applications in more complicated tasks. In particular, it is important in the design of other two-party protocols such as mental poker (i.e. performing a set of cryptographic problems over distance without the need for a trusted third party) and remote user authentication. Classically, coin tossing is impossible without computational assumptions: at least one of the parties can in principle always cheat and fix the outcome. Nevertheless, using quantum communication, non-trivial coin tossing is possible [SR02a, SR02b, Amb02]. In many applications however, the parties do not want to generate a single coin, but many. This is called bit-string

generation [Ken03, BM04a, BM04b]. Here we introduce a bit-string generation protocol and report on an experimental implementation based on the plug and play scheme. Using the theoretical analysis of [BM04b] we are able to show that the bit strings generated in our experiment achieve a high level of randomness. This demonstrates a fundamental new concept: namely the possibility of generating a string of random coins with an adversary who is limited only by the laws of physics.

Because losses is the principal type of noise in long distance quantum communication, it seems to preclude tossing of a single coin with a high level of randomness. That is, a malicious party can always bias the outcome of a single coin toss with the help of simple cheating strategies. For this reason this work focuses on bit string generation rather than the tossing of a single coin. This difficulty is illustrated by another experiment [**?**] which was simultaneously realized with our implementation for which incomplete and hand waving arguments were provided with regards to the generated randomness. This implementation used very different experimental techniques based on entanglement swapping.

6.2 The protocol

We begin by reviewing security conditions for the generation of n random bits. The outcome of the protocol is either a string of bits $\vec{x} \in \{0,1\}^n$ or one of the parties aborts, in which case we write $\vec{x} = \perp$. The protocol is *correct* if when both parties are honest, the probability of aborting is small and all the coins are fair. Mathematically we express this as

$$\begin{aligned} \forall \vec{c} \in \{0,1\}^n \quad & \mathrm{P}(\vec{x} = \vec{c}) = (1-\delta_n)/2^n, \\ & \mathrm{P}(\vec{x} = \perp) = \delta_n. \end{aligned} \tag{6.1}$$

It is necessary to include the parameter δ_n because of experimental imperfections which induce a non-zero probability of the protocol aborting even if both parties are honest. In the protocol we use, δ_n decreases to zero exponentially fast with n and can be neglected.

We shall use two security conditions. The first, called the "average bias", describes the degree of randomness of individual bits of the string. Formally we define the upper bound $\bar{\epsilon}_{A(B)}$ on the average bias when Alice (Bob) is dishonest and the other party is

honest as:

$$\begin{aligned} \forall S_A \forall \vec{c} \in \{0,1\}^n \quad & \frac{1}{n}\sum_{i=1}^{n} \mathrm{P}^{S_A H_B}(x_i = c_i) \leq \frac{1}{2} + \bar{\epsilon}_A, \\ \forall S_B \forall \vec{c} \in \{0,1\}^n \quad & \frac{1}{n}\sum_{i=1}^{n} \mathrm{P}^{H_A S_B}(x_i = c_i) \leq \frac{1}{2} + \bar{\epsilon}_B, \end{aligned} \tag{6.2}$$

where we denote a general strategy of Alice (Bob) by S_A (S_B), and the honest strategy defined by the protocol as H_A (H_B). The average bias is a simple measure of security but it is not very satisfactory. Consider, for example, the case in which Alice can cheat so that Bob's output is either the string composed of all zeros or the string composed of all ones, with equal probabilities: $\mathrm{P}(\vec{c} = 0^n) = \mathrm{P}(\vec{c} = 1^n) = 1/2$. The average bias $\bar{\epsilon}_{A(B)}$ is zero, although the security is clearly very bad.

For this reason we introduce another security condition based on the *Shannon entropy* of the string which measures the degree of randomness of the string taken as a whole. We define $H_{A(B)}$ as the entropy[1] of the string if Alice (Bob) is dishonest and the other party is honest. We define

$$H_A = H\left(\mathrm{P}^{S_A, H_B}(\vec{c})\right), \tag{6.3}$$

$$H_B = H\left(\mathrm{P}^{H_A, S_B}(\vec{c})\right), \tag{6.4}$$

where H is the usual Shannon entropy of a probability distribution as defined in chapter 2. Now we say that a bit-string generation protocol is *arbitrarily secure* if $(n - H_A)/n \to 0$ and $(n - H_B)/n \to 0$ as $n \to \infty$. Roughly speaking, this means that a cheater may be able to fix the values of some of the coins, but that the fraction of coins thus affected must become small as n increases. It is *partially secure* if $H_A, H_B > 0$. We refer to [BM04b] for a more detailed discussion of security conditions where it is shown that our quantum protocol is relatively secure in the absence of noise and partially secure in the presence of noise, with security depending quantitatively on the amount of noise.

The protocol we shall use, inspired by that of [BM04a, BM04b] is as follows. Choose a security parameter $0 < \kappa < 1$.

1. For $i = 1$ to n.

[1]The symbols H_A and H_B defined here are identical to those used to denote Alice's and Bob's honest strategies. However, it will always be clear which is meant.

2. Alice chooses a random bit a_i. If $a_i = 0$, she prepares a coherent state of the electromagnetic field with amplitude α: $\psi_0 = |\alpha\rangle$. If $a_i = 1$, she prepares a coherent state with amplitude $-\alpha$: $\psi_1 = |-\alpha\rangle$. She sends the coherent state ψ_{a_i} to Bob. After receiving the quantum state from Alice, Bob chooses a random bit b_i. Bob tells Alice the value of b_i.

3. After learning the value of b_i, Alice reveals the value of a_i to Bob.

4. Bob now verifies whether the state Alice sent him is indeed the coherent state $|(-1)^{a_i}\alpha\rangle$. He does this by using a Local Oscillator (LO) to carry out the displacement $\mathcal{D}(-(-1)^{a_i}\alpha)$. If Alice was honest, the displaced state should be the vacuum state $|\text{vac}\rangle$. Bob checks that this is the case by sending the state onto a single photon detector. If the detector clicks, Bob sets $k_i = 1$. If the detector does not click, Bob sets $k_i = 0$.

5. Next i.

6. If $\frac{1}{n}\sum_i k_i > \kappa$, Bob aborts. Otherwise the output of the protocol is the bit string $x_i = (a_i + b_i) \bmod 2$.

6.2.1 Bob's cheating strategy

When Bob is dishonest his best strategy is to measure the state sent to him by Alice as soon as he receives it (i.e., before carrying out step 3 above). One easily shows, see [BM04b], that

$$\overline{\epsilon_B} \leq \frac{\sin\theta}{2}, \quad \text{where} \quad \cos\theta = |\langle\psi_0|\psi_1\rangle| = e^{-2|\alpha|^2} \ . \tag{6.5}$$

In other words, the bigger the overlap between the two states, the higher the probability that Bob can bias the outcome due to his improved ability to discriminate between the two states.

6.2.2 Alice's cheating strategy

If Alice is dishonest she may not send Bob the state ψ_{a_i} but an arbitrary state ρ. In general she may prepare an entangled state, keeping half of it and sending the other half to Bob. Furthermore, she may correlate and even entangle her strategy over different runs. In [BM04b], however, it is shown that strategies correlated over different runs cannot help Alice for large n. A bound on $\overline{\epsilon}_A$ is proven that depends on the average value of the fidelity $f_i = \langle\psi_{a_i}|\rho|\psi_{a_i}\rangle$, as estimated by Bob. Since the probability

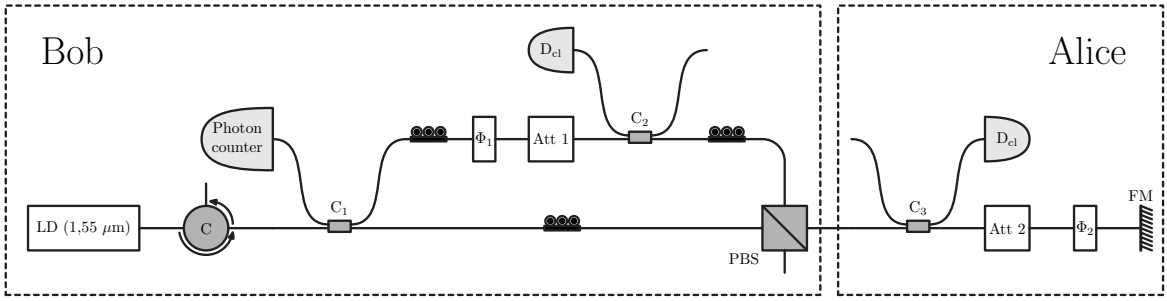

Figure 6.1: Optical setup. LD: Laser Diode, C_i (i=1,2,3): Coupler, Att: Attenuator, Φ: phase modulator, FM: Faraday Mirror, D_{cl}: classical detector.

that Bob's detector clicks (assuming his detector is perfect) is related to the fidelity by $P(k_i = 1) \geq 1 - f_i$, the result of [BM04b] then implies that, assuming large n, the bias if Alice is dishonest is bounded by $\overline{\epsilon_A} \leq \mathcal{F}(\kappa)$, where $\mathcal{F}(x) = \frac{\sqrt{x}}{\sqrt{2}\sin^2\theta} + \frac{x}{\sin^2\theta}$. Below we show how this relation must be modified to take into account imperfections in Bob's measuring apparatus.

Note that due to such imperfections, Bob's detector may click even if Alice is honest. Alice and Bob should choose κ such that it is larger than the expected number of clicks if both parties are honest. When this is the case, the probability δ_n that the protocol aborts if both parties are honest decreases exponentially fast to zero and the protocol is correct.

6.3 Experimental implementation

Our experimental setup, depicted in Fig. 9.1, is based on the plug and play method introduced in the previous chapters. However the plug and play method has a number of specific features which must be carefully taken into account in order that neither Alice nor Bob have the possibility to completely bias the outcome. Each round of the protocol begins with Bob producing a short (20ns) intense (25mW) laser pulse at $\lambda = 1.55\mu$m. The pulse is split in two by the 50/50 coupler C_1. The two pulses acquire a relative time delay of 100ns and then impinge with orthogonal polarization on a PBS whereupon they are sent to Alice. Between C_1 and the PBS, along the long path, are an attenuator, a 99/1 coupler C_2 and a phase modulator. The role of these elements will be explained later. The relative attenuation of the two pulses is $A \simeq 45$dB. The first pulse to reach Alice is intense and contains $N_0 \simeq 10^9$ photons. This pulse will play the role of LO. The second pulse to reach Alice is attenuated and contains AN_0

photons. The second pulse will play the role of signal.

Upon receiving the pulses, Alice measures the intensity of the signal pulse (using the 80/20 coupler C_3 and a classical detector D_{cl}) and attenuates both pulses. The two pulses are reflected by the Faraday mirror and travel back to Bob. The total attenuation at Alice's site is $A' \simeq 50$dB. Thus the two pulses now contain $A'N_0$ and $AA'N_0$ photons respectively. In particular the signal pulse now contains only a few photons ($AA'N_0 = |\alpha|^2 = O(1)$). Alice also adds a phase $\phi_A = a_i\pi$ to the signal pulse, thereby encoding the value of her bit a_i.

6.3.1 Bob's cheating strategy revisited

The fact that Bob provides Alice with the signal state seems to provide him with some simple cheating strategies. For instance he could provide Alice with a signal state that is squeezed in phase in order to decrease the overlap between $|\psi_0\rangle$ and $|\psi_1\rangle$. This apparently allows him to discriminate much better $|\psi_0\rangle$ from $|\psi_1\rangle$ and hence the value of a_i. The role of the attenuation is to prevent this kind of cheating. Indeed under strong attenuation any quantum state tends towards a mixture of coherent states. For a proof, please refer to the original article [LBA+05].

Another simple cheating strategy is for Bob to increase the intensity of the signal state since it is then much easier for him to estimate the phase ϕ_A. The role of the classical intensity measurement is to ensure that the signal state Alice sends back is not too intense. In fact it is impossible for Bob to exploit the fact that he provides Alice with the light pulse which will become the signal state, since by measuring the intensity of the pulse Bob sends her and then attenuating it, Alice ensures that she sends back to Bob a coherent state of known intensity.

Note that the classical intensity measurement of Alice will be affected by noise because AN_0 is close to the sensitivity limit of Alice's detector. We circumvent this technical problem by letting Alice carry out statistical tests on the n intensity measurements (one for each round of the protocol). More precisely she checks whether the distribution of measured intensities is consistent with the Gaussian distribution she expects from instrumental noise. If it is she has a precise estimate of $|\alpha|^2$, and hence of $P^{S_B H_A}(\vec{c})$ through eq. (6.5). If it is not she aborts.

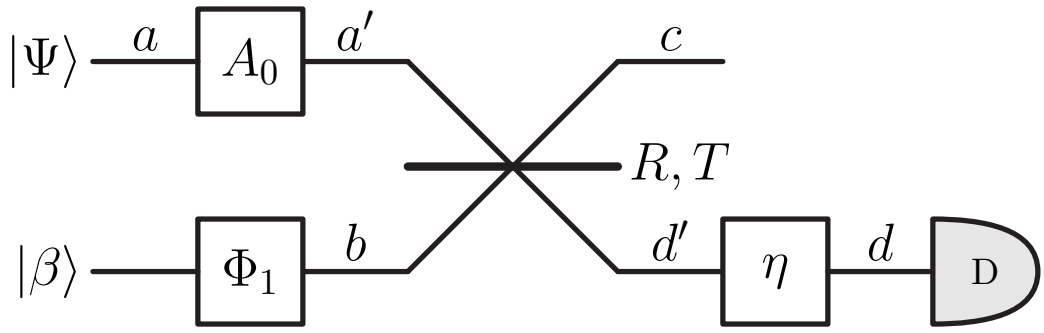

Figure 6.2: Optical setup equivalent to Bob's measurement, including its imperfections.

6.3.2 Alice's cheating strategy revisited

Upon receiving the two pulses from Alice, Bob uses coupler C_2 to measure the intensity of the LO, attenuates it by A, and adds a phase $e^{i\phi_B}$, with $\phi_B = a_i\pi$. Note that by measuring the intensity of the LO state provided by Alice and then attenuating it, Bob ensures that the LO he uses is a coherent state (or a mixture of coherent states) of known intensity $|\beta|^2$. (The argument is exactly the same as that given above in the case of Alice).

Let us consider the two states that interfere at coupler C_1. On the one hand there is the LO which as we have just argued is a coherent state of known intensity $|\beta|^2$. On the other hand there is the signal state. The signal state travels through the PBS where it gets attenuated by A_0. It then interferes with the LO at coupler C_1. This coupler has transmission and reflection coefficients $|t|^2$ and $|r|^2$ (both are approximately 50%). Finally one of the outputs of the coupler is sent to a single photon detector (id Quantique) with efficiency η. In our experiment $A_0T = 4.3$dB and $\eta = 10.5\%$. We can therefore model the whole of Bob's detection system by the scheme depicted in Fig. 9.2. It is composed of the LO (a coherent state of amplitude β), the signal state Ψ, the attenuator A_0, a beam splitter with transmission and reflection coefficients T and R. The imperfect detector is modeled by an attenuation of η followed by a perfect detector. Let us denote by α the amplitude of the coherent state that would give rise to destructive interference at the single photon detector. It satisfies $\alpha\sqrt{A_0T} + i\beta\sqrt{R} = 0$. When $a_i = 0$, the state Alice should send if she is honest is the coherent state $|\alpha\rangle$. (If $a_i = 1$ she should send the state $|-\alpha\rangle$. By using the phase modulator Bob can cancel this phase). But if Alice is dishonest she will send another state $|\Psi\rangle$. We expand $|\Psi\rangle$ in the basis of displaced Fock states $|\Psi\rangle = D_a(\alpha)\sum_n c_n|n\rangle$ where

$D_a(\alpha)$ is the displacement operator acting on mode a, i.e. $D_a(\alpha)aD_a(\alpha)^\dagger = a - \alpha$, and $|n\rangle = (a^\dagger)^n/\sqrt{n!}|\text{vac}\rangle$ are the Fock states. The fidelity of the state sent by Alice is thus $f = |\langle\alpha|\Psi\rangle|^2 = |c_0|^2$.

We model the effect of the attenuation by the transformation $a \to \sqrt{A_0}a' + \sqrt{1-A_0}e_1$ where e_1 is a mode of the environment; the effect of the BS by the transformations $a' \to \sqrt{T}d' - i\sqrt{R}c$, $b \to \sqrt{T}c - i\sqrt{R}d'$; and the effect of the detector inefficiency by $d' \to \sqrt{\eta}d + \sqrt{1-\eta}e_2$ where e_2 is another mode of the environment (the modes a, a', b, c, d', d are all described in the figure). One then finds that the state just before entering the single photon detector is

$$D_c(\gamma)\sum_n \frac{c_n}{\sqrt{n!}}[\sqrt{A_0T\eta}d^\dagger + i\sqrt{A_0R}c^\dagger + \sqrt{1-A_0}e_1^\dagger + \sqrt{(1-\eta)TA_0}e_2^\dagger]^n|\text{vac}\rangle$$

where $\gamma = \beta\sqrt{T} + i\alpha\sqrt{A_0R}$. From this one easily computes that the probability that the detector does not register a single click is

$$P(\text{no click}) = \sum_{n=0}^{\infty}|c_n|^2(1-A_0T\eta)^n. \tag{6.6}$$

The probability of registering a click is thus bounded by $P(\text{click}) \geq (1-|c_0|^2)A_0T\eta$. Thus the number of clicks on Bob's detector divided by $A_0T\eta$ gives a bound on the fidelity $|c_0|^2$.

A final inefficiency that must be taken into account is that Bob's detector will have a non-zero dark count rate $\kappa_{dark} = 9 \times 10^{-4}$. Putting all this together we deduce the bound on the average bias if Alice is dishonest:

$$\overline{\epsilon_A} \leq \mathcal{F}(\frac{\kappa - \kappa_{dark}}{A_0T\eta}) \tag{6.7}$$

Note that this bound on $\bar{\epsilon}_A$ is given entirely by parameters which can be measured by Bob. Using this protocol, and taking into account experimental imperfections as described below, a typical run of our experiment generates 10^7 coins. Some results for different values of $|\alpha|^2$ are presented in Fig. 9.3.

6.4 Conclusion

The main goal of this work was to provide a bit-string generation protocol where an adversary is limited only by the laws of physics. Furthermore, it was originally

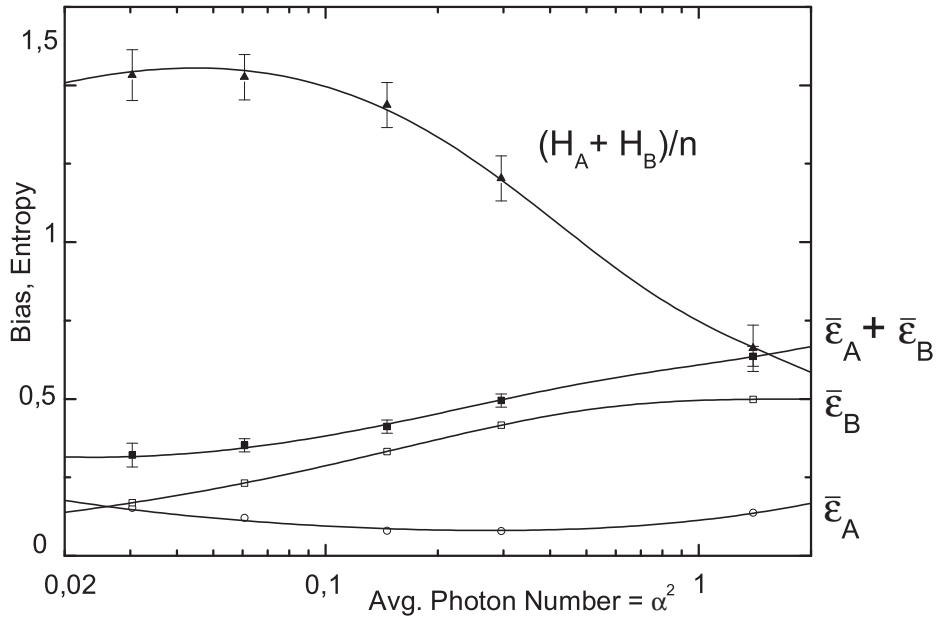

Figure 6.3: Measured bounds on average bias and on entropy of bit strings for different values of the average photon number α^2. Open squares: bounds on $\overline{\epsilon}_B$ obtained using eq. (6.5); open circles: bounds on $\overline{\epsilon}_A$ obtained using eq. (6.7): filled squares: bounds on $\overline{\epsilon}_A + \overline{\epsilon}_B$. The same expressions which give bounds on $\overline{\epsilon}_A$, $\overline{\epsilon}_B$ also give lower bounds on the entropies $H_{A(B)}$ of the bit string if Alice (Bob) is dishonest (see [BM04b]). Filled triangles: bounds on the entropy per bit $(H_A + H_B)/n$. The error bars for $\overline{\epsilon}_A + \overline{\epsilon}_B$ and $(H_A + H_B)/n$ describe systematic errors arising from incorrect callibration of detector efficiency η and incorrect estimation of α^2. The plotted curves are theoretical predictions based on the observed optical visibility of 96.5%. For $\overline{\epsilon}_B$ the curve is given by eq. (6.5) and for $\overline{\epsilon}_A$ it is given by eq. (6.7) using the fact that for small α^2, $(\kappa - \kappa_{dark})/A_0 T\eta \simeq (1 - V)\alpha^2/2$.

our intention to show that the bit-strings generated in our experiment achieve a level of randomness impossible classicaly. However, after our work was published, it was realized that classical protocols exist which produce strings with high randomness. The question of whether our experiment produced strings more random than what is achievable classicaly is still an open one. Using another security criteria however might answer this question affirmatively.

The two security criteria used to describe how random the strings our in our experiment were the average bias and the entropy. For both these criteria classical protocols can also produce strings with high randomness. Unpublished work by Barrett and Massar introduces a new security criteria, the "min-entropy" condition $H^{\infty}_{A(B)}$ which measures the maximal probability of occurrence of a specific string. They show that if a cheater wants to keep the probability of being caught small, then the min-entropy must be larger than the classical bound. It is conjectured that in the presence of noise, this criteria is still valid such that our experiment produces coins more random than possible classicaly. Figure (6.4) plots our experimental data for the "min-entropy" condition. The classical bound is shown to be 1 and is clearly exceeded by our quantum protocol.

An important property of our protocol and of its experimental implementation is that we do not have to make any hypothesis about the Hilbert space Alice or Bob use if they are dishonest - for instance it is not necessary to restrict them to the single photon subspace -, nor do we have to make any hypothesis about the kind of technology they can use if they are dishonest. Thus the randomness of the bit string when one of the parties is dishonest is guaranteed by the laws of physics.

Let us now move on to report the last experiment described in this dissertation. The protocol we implement is that of short-distance identification. As we shall see, the experimental implementation will exploit another photon degree of freedom in order to encode quantum information and therefore exit the realm of plug and play.

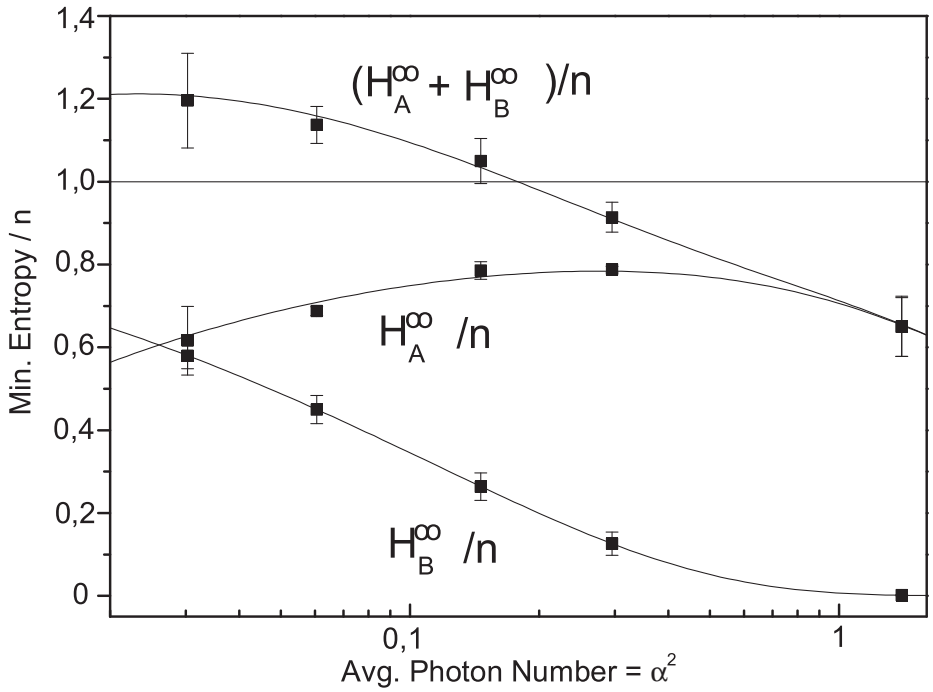

Figure 6.4: Conjectured values of the min-entropy, if a cheater want to keep the probability that she/he is caught small, for our experimental data. The graph plots the value of the min entropy H_A^∞ if Alice keeps the probability that she is caught small and uses the same cheating strategy at each round (The values of the min-entropy H_B^∞ if Bob is dishonest do not depend on any hypothesis). The sum $H_A^\infty + H_B^\infty$ is clearly above the value of 1, which is the maximum attainable for classical strategies.

Chapter 7

Beyond the plug and play paradigm: quantum identification

7.1 Introduction

The previous chapters have described how it is possible to implement quantum cryptographic protocols using the plug and play technique. However, this technique limits the quantum tasks that can be performed because it does not allow the preparation of a universal set of states. As we have seen, this is due to the fixed transimittivity of the beam-splitter. In this chapter, we will be interested in the cryptographic task of short distance identification and propose a solution that requires the preparation of a set of states larger than what is achievable with plug and play. We emphasize at this point that the work contained in this chapter is still in progress and not yet published at the time of writting.

The security of QKD relies on the physical principle that it is impossible to perfecly clone an arbitrary quantum state. This is a direct consequence of the unitarity of the quantum evolution operator. This unitarity also prevents other quantum mechanical tasks from being perfectly carried out. One such example is the so-called universal inverser or UNOT gate. The UNOT gate (if it indeed existed) would take some arbitrary quantum state and transform it to an orthogonal state. In two-dimensional Hilbert space, this would take qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and send it to its antipode $|\psi\rangle^{\perp} = \alpha_0^*|0\rangle - \alpha_1^*|1\rangle$ where $\langle\psi^{\perp}|\psi\rangle = 0$. The UNOT gate is an anti-unitary operation which by definition is not completely positive and therefore cannot exist in Nature [BP99]. Anti-unitary operations can be expressed by the so-called time-reversal map $T = i\sigma_Y K$ times any unitary operation where K is the conjugation operation,

$K|\psi\rangle = |\psi^*\rangle$. For qubits the time-reversal map is equivalent to the UNOT gate.

Since quantum mechanics does not allow antiunitary operations and therefore the UNOT gate, one can ask the following question: "What is the largest set of quantum states which can be perfectly flipped by using the laws of quantum mechanics?" For two-dimensional Hilbert space, this subset happens to be a great circle on the Bloch sphere. More precisely, for any unitary operator described by a 90◦ rotation around a given axis $Q = \overrightarrow{n} \cdot \overrightarrow{\sigma}$ on the Bloch sphere:

$$U_R = e^{i\frac{\pi}{2}(\overrightarrow{n}\cdot\overrightarrow{\sigma})}$$

it is possible to define a set of states who will be mapped to their antipode upon applying this operator. This set of states lies on the great circle orthogonal to Q. The Pauli matrices are well known examples of such operators.

Interestingly so far, no quantum cryptographic task has emerged which relies on the impossibility to perform a time reversal map. Although, in comparaison to standard quantum cryptography based on the no-cloning principle, we expect a malicious party intending to bypass a protocol based on the impossibility to perform a UNOT gate would have much more difficulty. This is because the optimal fidelity of the transformation which best approximates the UNOT gate is much lower than the fidelity achieved by the optimal cloning transformation. Thus, a direct consequence of this lower fidelity is that it can be exploited to design protocols with a higher noise tolerance.

In this chapter we report on a proof of principle experimental demonstration of a novel quantum cryptographic protocol that exploits this impossibility. The cryptographic task to be fulfilled is the task of *short distance identification* where a claimant, Alice, must prove her identity to a verifier, CPU by demonstrating knowledge of a secret known to be shared between the two parties. This is done by providing a response to a time-variant challenge, where the response depends on both the secret and the challenge. In today's modern society, short distance identification has become a daily task which people are confronted to, thereby making it as important as QKD or cointossing. Whether it's to withdraw money from a cash machine, cross into a secure area or log onto a computer, identification is omnipresent in our everyday life.

7.2 Preliminaries

The theory behind approximating unphysical transformations has been extensively studied, in particular in the case of the UNOT [**?**, BHW99]. The best achievable transformation allowed by quantum mechanics for an arbitrary qubit was shown to yield a fidelity of $\frac{2}{3}$ [BP99]. This means that when measured in the $\{|\psi\rangle\ , |\psi^{\perp}\rangle\}$ basis one should expect to see $|\psi^{\perp}\rangle$ two times out of three. A well known example of a transformation which reaches this upper bound is given by the universal cloning machine which produces, in addition to the clones, an anti-clone (which can be interpreted as the final state of the cloning machine itself) having this fidelity. From a physical point of view, this corresponds intuitively to assuming a "conservation law" in the cloning process, where the ancilla undergoes a time-reversed transformation in order to balance the corresponding transformation of the clones.

In what follows, we illustrate a quantum cryptographic protocol which exploits the impossibility of time reversal. More specifically, in this protocol, the two parties exchange a set of six quantum states spanning a two-dimensional Hilbert space. These six states form three maximally unbiased bases and can be seen as eigenstates of the three Pauli operators σ_Z, σ_X and σ_Y,:

$$\begin{array}{lll} |0\rangle & |+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle] & |+^i\rangle = \frac{1}{\sqrt{2}}[|0\rangle + i|1\rangle] \\ |1\rangle & |-\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] & |-^i\rangle = \frac{1}{\sqrt{2}}[|0\rangle - i|1\rangle] \end{array}$$

respectively. The six states are extremal (or cardinal) points on the surface of the Bloch sphere. Indeed, they have conveniently been chosen in such a way that two out of three of the Pauli matrices invert a given state while the third matrix leaves it unchanged. In other words each Pauli operator flips perfectly 4 out of the 6 states while leaving the remaining two states unchanged. The optimal fidelity that can be achieved when considering these six states is the same as when considering all states in two-dimensional Hilbert space, that is[1] $F = \frac{2}{3}$. A simple method to achieve this upper bound is in fact a classical one: by randomly choosing one of the three Pauli operators, we are sure to map any of the six states with probability 2/3, hence achieving

$$|\psi\rangle \xrightarrow{\mathrm{U}} \frac{1}{3}\big[|\mathbb{1} + |\psi^{\perp}\rangle\langle\psi^{\perp}|\big]. \tag{7.1}$$

Another method achieving the same fidelity consists in cloning the state. Indeed, by duplicating the state (say with the optimal pauli cloning machine) the output of the

[1] This is analoguous to optimal universal quantum cloning; the optimal fidelity when considering only the six cardinal states is the same as when considering the whole Bloch sphere [CDPC05].

transformation yields the following entangled state:

$$|\Psi\rangle = \frac{1}{\sqrt{3}}\left[|\psi\rangle_A|\psi^-\rangle_{BC} + |\psi\rangle_B|\psi^-\rangle_{AC}\right] \tag{7.2}$$

where A, B and C refer to the two clones and the ancilla, respectively and $|\psi^-\rangle = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]$ is the anti-symmetric Bell state. The ancillary system can be seen as an "anti-clone" described exactly by Eq. (7.1). This transformation not only yields the optimal fidelity for universal cloning but as well for the approximate universal inverser. We now go on to describe our identification protocol.

7.3 Identification protocol

Our simple identification protocol is described in the following way: Alice and the CPU share a secret string of "trits" $\overrightarrow{s}$ (call it a password) represented by one of the three great circles crossing the six states (assumed to be publicly known):

$$\begin{aligned} \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} &= \text{"0"} \\ \{|0\rangle, |1\rangle, |+^i\rangle, |-^i\rangle\} &= \text{"1"} \\ \{|+\rangle, |-\rangle, |+^i\rangle, |-^i\rangle\} &= \text{"2"} \end{aligned} \tag{7.3}$$

Each trit is associated to one of the Pauli operators which correctly flips its four states. The idea is that for every trit of the string, the CPU sends one of its 4 states to Alice. Her non-trivial task is to flip the state and send it back to the CPU who can then verify that the operation has been performed successfully. Note that this task can only be perfectly achieved if Alice knows the value of each trit, i.e. which Pauli operator she should use for every state sent to her. Also note that the CPU answers "YES" or "NO" only after the exchange of qubits has been completed thus indicating Alice whether the CPU acknowledges or denies her claim of identity. Because we only take into account short-distance identification, we do not consider man in the middle type of attacks where a malicious adversary could eavesdrop in between the two parties to try and gain information on the password. That is, we suppose that the adversary, call him Percy, has only the capacity to perform *personification* type of attacks where he tries to convince the CPU that he is Alice.

One can easily conclude that the above protocol is indeed a valid one because in the absence of the correct password Percy has a non-zero probability of introducing errors as he flips the incoming states. This is a consequence of the absence of a UNOT transformation. Thus for a given threshold acknowledged by both Alice and the CPU,

the latter can abort if the BER exceeds this limit[2]. However, in order to gain more insight on the performance of our protocol, we must compare it to a classical analog.

We choose to compare our protocol to a very well known classical analog, namely the password. In this classical counterpart a claimant is challenged in entering a series of classical trits[3]: a password which she/he suposedly shares with the CPU. Demonstrating knowledge of this password convinces the CPU on the identity of the claimant. For a password consisting in N successive trits, there exists 3^N different possibilities. Therefore a malicious claimant who aims in personifying someonelse (e.g. Alice) has probability

$$P(\text{YES}|\text{NO}^{\otimes M}) = \frac{1}{3^N - M} \tag{7.4}$$

of being answered "YES" by the CPU after M consecutive "NO"s and take a maximum of 3^N successive tries in order to convince the CPU. Once she is in possession of the password Percy can log in and out of the CPU as long as neither Alice nor the CPU have knowledge of her intervention. In our quantum analog, Alice and the CPU share an N trit string $\overrightarrow{s}$. Each trit is represented by four states as defined above. For each trit in the string the CPU will send a state belonging to the corresonping great circle. The challenge in order to identify herself is for Alice to flip the state and send it back to the CPU. Formally, for each trit Alice needs to perform the following operation:

$$\sigma_i|\psi\rangle = |\psi^{\perp}\rangle \tag{7.5}$$

where i corresponds to the Pauli matrix which correctly flips any of the four corresponding states.

We have performed a series of preliminary calculations (which are not exposed here) aimed at characterizing the performance of our protocol and compare them to the classical analog. Our results are unfortunately not very interesting because the probability of entering the CPU, for both protocols, scales exponentially, even giving a slight edge to the classical analog. The probability to succeed after M tries is given by

$$P(\text{YES}|\text{NO}^{\otimes M}) = \frac{2^N}{3^N - M} \tag{7.6}$$

[2]Even though the password is encoded in terms of a ternary alphabet, the CPU concludes the protocol by measuring *binary* obervables indicating whether Alice has correctly flipped the states. This is the reason why the threshold is expressed in terms on *bit* error rate rather than *trit* error rate.

[3]we choose a terneray alphabet for an easier comparaison to the quantum protocol.

for the quantum protocol (for large N). Nevertheless, we can show that the probability of re-entering the CPU after a successful try is unity for the classical protocol and is exponentially low in the string length for the quantum protocol.

To reach these conclusions, we have studied two personification scenarios. The first, which we call *random basis attack* consists in Percy randomly choosing a Pauli operator and applying it to the incoming state and repeats for all N states. One can see that this strategy is in fact similar to the classical one. Percy's second strategy is slightly more complicated. It involves performing a cloning transformation to each incoming state as described in the previous section. For each cloning operation, Percy will keep the clones A and B and send the anti-clone (the ancilla) C back to the CPU. Both of the above strategies yield the same probability of success because all N states sent back to the CPU have a probability $\frac{2}{3}$ of being correctly flipped. However, the information that Percy can gain following the CPU's answer differs for the two strategies. For example, in the cloning attack, Percy can measure his clones once the CPU has given an answer. For large N however, Percy should choose the random basis attack. The reason being that cloning provides (asymptotically) no information on the value of the given candidate string that Percy has tested in contrast to the random basis attack which provides some (but not all) information. Finally, note that if Percy uses the random basis attack, he has a non-zero probability of entering the CPU even if he applies the wrong sequence of operations (although quite improbable for large N). However, contrary to the classical protocol, the probability that Percy personifies Alice following a successive entry is small.

7.4 Experimental quantum identification

Because our protocol relies on six MU qubits, it cannot be implemented with the plug and play technique. We have nevertheless chosen to encode our quantum information in infrared photons therefore exploiting the technological baggage available. However, instead of encoding information in time bins we encode information in the polarization (π) of a single photon expressed in the horizontal and vertical basis, $\{|H\rangle, |V\rangle\}$ also spaning two-dimensional Hilbert space. We associate the three Pauli matrices to the

three MU bases formed from the $\{|H\rangle, |V\rangle\}$ basis:

$$\sigma_Z \leftrightarrow \{|H\rangle, |V\rangle\}$$
$$\sigma_X \leftrightarrow \{\frac{1}{\sqrt{2}}[|H\rangle \pm |V\rangle]\}$$
$$\sigma_Y \leftrightarrow \{\frac{1}{\sqrt{2}}[|H\rangle \pm i|V\rangle]\}.$$

Our experimental identification setup works with attenuated coherent states traveling in localized time bins partly in optical fibers and partly on a table-top; see Fig. 7.1. The CPU uses a laser diode at 1,55 μm to produce a 10 ns light pulse. The pulse is attenuated by an optical attenuator (Agilent 8156A) and then impinges on a 50/50 polarizing beam-splitter (PBS). The π of the pulse is rotated, using π controllers such that it exits port H (horizontal π port) rather than the orthogonal V port of the PBS. Immediately afterwards, the pulse exits the optical fiber and is focused on a quarter waveplate and a half waveplate which are used by the CPU in order to prepare one of the 6 possible states which will be sent down to Alice. The pulse then travels down a 2 ns line towards Alice. At Alice's site, the pulse crosses a quarter-wave plate, is reflected by a mirror, crosses again the wave plate and is sent back to the CPU. The pulse is then reinjected in the optical fiber. Depending on whether Alice has performed the correct operation or not, the pulse will either exit through the H port (which consequently leads to a circulator and a single photon detector - id Quantique id200) or the V port (which leads to a single photon detector - id Quantique id200). The detector was gated during a 20 ns window around the arrival time of the pulse. Its output was registered using a time-to-digital delay converter (ACAM-GP1) connected to a computer. All electronic components were triggered by a pulse generator (Standford Research Inc). Note that the requirement that a single photon be sent is primordial because as the photon number increases a better estimation of the qubit value is achieved thus leading to the realization of a higher fidelity flipping transformation [**?**, BHW99]. The fact that the CPU is limited to sending attenuated coherent states should be taken into account in the tolerated BER.

Let us now prove that our setup indeed performs the quantum identification protocol described in the previous section. The first consideration we must take concerns the *spatial* reference frame in which the photon π evolves. We therefore introduce the spatial reference frame (x, y, z) where z is the direction of propagation of the photon while x and y belong to the plane of the mirror orthogonal to z. (These coordinates should not be confused with the capital characters associated to the Pauli matrices defined above.) We will assume that the photon's π state is identified according to

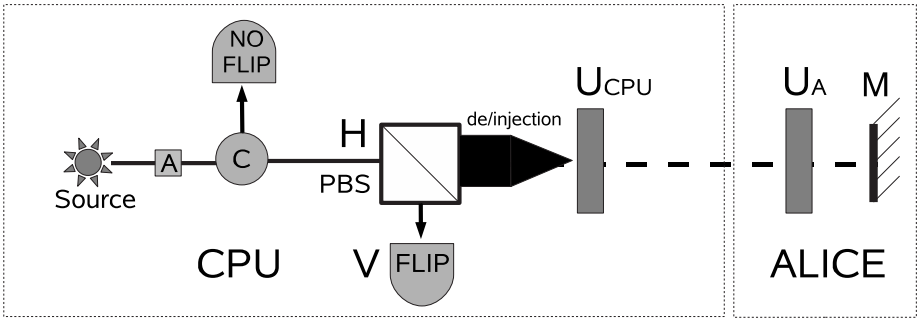

Figure 7.1: Optical setup. The CPU prepares an attenuated coherent state with the source and the attenuator "A". Afterwards, the photon is polarized in the $|H\rangle$ state (selected by the PBS) and exits the optical fiber through the dejection. The CPU then encodes the state with U_{CPU} and sends it on to Alice who leaves the state unchanged with the help of U_{A} and the mirror "M". The photon then travels back to the CPU where it is reinjected in the optical fiber and impinges on the PBS. The two outputs are connected to detectors "FLIP" and, via a circulator "C", "NO FLIP".

the right-handed coordinate convention. This implies that after reflection, the π state will be identified on the basis of a new coordinate system $(x' = x, y' = -y, z' = -z)$ obtained by rotating the original frame by 180° around the $\overrightarrow{x}$ axis.

The experiment we have performed is designed up to a unitary transformation; rather than asking Alice to send back the flipped state $|\psi^{\perp}\rangle$ the CPU can equivalently ask her to return the state $U|\psi^{\perp}\rangle$, where U is an arbitrary unitary operation, and measure the returned state in the $\{U|\psi\rangle, U|\psi^{\perp}\rangle\}$ basis. The reason is the following. After reflecting on the mirror, linear π states will remain unchanged whereas circular π states will become orthogonal (in the new reference frame): $|H\rangle \to |H\rangle$, $|V\rangle \to |V\rangle$, $|\pm\rangle \to |\pm\rangle$, $|\pm^i\rangle \to |\mp^i\rangle$. Because we use waveplates in our experiment, it was impossible to flip all states corresponding to trit "0" because waveplates cannot flip states around the Y axis (i.e. waveplates cannot perform the σ_Y operation). For this reason, we redefine the protocol up to the unitary operation $U = \sigma_Y$. Therefore, the operation that Alice will apply on the incoming states will be the following:

$$
\begin{aligned}
&\text{"0"} \to \sigma_Y\sigma_Y = \mathbb{1} \\
&\text{"1"} \to \sigma_Y\sigma_X = \sigma_Z \\
&\text{"2"} \to \sigma_Y\sigma_Z = \sigma_X.
\end{aligned}
$$

As we can see, the corresponding challenge is thus for Alice to return the state unchanged.

To create the six states, the CPU begins by preparing state $|H\rangle$ with the PBS oriented in the σ_Z basis. After exiting the optical fiber, the CPU completes the preparation by turning the π state with the appropriate series of waveplates (U_{CPU}):

$$|H\rangle = \mathbb{1}|H\rangle \qquad |D\rangle = U(\tfrac{\lambda_X}{4})\, U(\tfrac{\lambda_Z}{4})\, |H\rangle \qquad |R\rangle = U(-\tfrac{\lambda_X}{4})\, |H\rangle$$
$$|V\rangle = U(\tfrac{\lambda_X}{2})\, |H\rangle \qquad |A\rangle = U(\tfrac{\lambda_X}{4})\, U(-\tfrac{\lambda_Z}{4})\, |H\rangle \qquad |L\rangle = U(\tfrac{\lambda_X}{4})\, |H\rangle$$

where

$$U(\tfrac{\lambda_X}{2}) = \sigma_X, \qquad U(\tfrac{\lambda_X}{4}) = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \quad \text{and} \quad U(\tfrac{\lambda_Z}{4}) = \tfrac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ i & -1 \end{pmatrix}.$$

Having prepared the necessary state, the CPU sends it to Alice who's task is to return it unchanged. To do so, she uses a waveplate U_A and a silver mirror. The action of the mirror on the π state can be seen as a rotation around the Z axis and an additional 180° phase shift: $i\sigma_Z$.

After the CPU prepares the state ($U_{CPU}|H\rangle$) it travels twice through Alice's waveplate. Thus for a given state sent by the CPU, Alice must use a waveplate designed in such a way that it will perform the correct operation after two passes through it. For trit "0" the correct operation in order to leave any of the four states representing this trit unchanged is the identity $\mathbb{1}$, for trit "1" the correct operation is $\sigma_Z = U(\frac{\lambda_Z}{4})\, U(\frac{\lambda_Z}{4})$ and for trit "2" the correct operation is $\sigma_X = U(\frac{\lambda_X}{4})\, U(\frac{\lambda_X}{4})$. Note that in the rotated reference frame the U_{CPU} and U_A are changed into the transposition of their original counterpart. Furtermore, note that $U(\frac{\lambda_Z}{4}) = U(\frac{\lambda_Z}{4})^T$ and $U(\frac{\lambda_X}{4}) = U(\frac{\lambda_X}{4})^T$ such that passing twice through the waveplate indeed performs the desired operation. Upon reaching the CPU's site, the state travels again through the waveplate U_{CPU} which was used to prepare the initial state. As a consequence, one can easily verify that the state

$$U_{CPU}^T\, U_A^T\, U_A\, U_{CPU}|H\rangle \tag{7.7}$$

left unchanged by Alice will end up in state $|H\rangle$ and be detected at the NO FLIP detector. Conversely a state which has been flipped by Alice (or a malicious party) will end up in the vertical state and be detected by the FLIP detector. Thus, the CPU can discriminate between Alice performing the correct or the wrong operation.

Trit	CPU	BER_A (%)	BER_E (%)
0	H,V,L,R	0.31	32.42
1	H,V,A,D	0.3	32.4
2	A,D,L,R	0.36	32.45

Table 7.1: Table 1: Experimental BER for Alice and Percy. Note

In order to characterize our setup, we have measured a series of visitibilities corresponding to different states prepared by the CPU and different actions performed by Alice. For each of the six states prepared by the CPU we have calculated the BER associated with the two possible outcomes $\mathrm{BER_N}$ (NO FLIP) and $\mathrm{BER_F}$ (FLIP). Recall that the BER is related to the visibility V by $\mathrm{BER} = \frac{1-V}{2}$. From these we have extracted the expected BERs for all three trits in the case of an honest Alice and a malicious Percy. More precisely, in the case of Alice, the expected BER for trit i is given by

$$\mathrm{BER_A}(i) = \frac{1}{4}\sum_{|\psi\rangle\in i} \mathrm{BER_N}(|\psi\rangle) = 0 \tag{7.8}$$

and

$$\mathrm{BER_P}(i) = \frac{1}{4}\sum_{|\psi\rangle\in i} \frac{1}{3}\big[2\ \mathrm{BER_N}(|\psi\rangle) + (1 - \mathrm{BER_F}(|\psi\rangle))\big] = \frac{1}{3} \tag{7.9}$$

for Percy. Table 1 summarizes our results. As we can see the values are closely related to the theoretical predictions. This is not surprising since the potential noise (i.e. birefringence) which could affect the photon $|\pi\rangle$ is minimal the reason being that it travels through air.

7.5 Conclusion

In this chapter we have implemented the optimal approximate flipping transformation for a set of three maximally unbiased bases in two-dimensional Hilbert space. We have shown that approximate flipping can be exploited to perform secure short distance identification and implemented an experimental demonstration with photon polarization. We ran the experiment in the single photon regime where the quantum state, when it left the CPU, contained less than 1 photon. As we have seen above, the $\mathrm{BER_A}$ in the case where Alice is the one identifying herself is theoretically zero. Because of experimental imperfections, errors occured but the BER_A remained below 0.5%. In the case of Percy, we expected a BER_E of $\frac{1}{3}$ and measured a value above 32%. As we can see, even in the presence of high levels of noise, the CPU can easily

discriminate between an honest claim or a false one. Note that because nearly all optical components are located in the CPU part of the circuit, losses can be solely attributed to it. Fortunately, because the CPU can control this characteristic, it cannot be exploited by a malicious party to gain information and cheat the CPU, and therefore only contributes to a reduction in the identification rate.

Finally, let us mention that although our identification protocol does not have any significant advantages over its classical counterpart it still shows for the first time that other quantum impossibilities such as the UNOT can be used to accomplish quantum cryptographic tasks. Hopefully this will open the door towards novel quantum protocols that clearly outperform their classical analogs and take full advantage of the low fidelity of the optimal approximate UNOT gate.

Chapter 8

Entanglement cloning

8.1 Introduction

We conclude this dissertation by discussing in further detail some interesting problems in quantum cloning. We begin by studying the cloning of entanglement and finish with the cloning of d-dimensional phase-covariant states. Although we present analytical solutions for both problems (symetric and asymetric) we verify our results with a numerical technique based on semidefinite programming.

Quantum entanglement is known to be a resource that is central to many quantum information processes such as quantum teleportation, quantum cryptography, or quantum computing [NC00]. In view of this, much work has been devoted to defining measures of entanglement or to investigating the best information-theoretical use of entanglement. Despite the fact that entanglement is a very fragile resource, extremely sensitive to decoherence, several techniques have been developed in order to overcome decoherence, namely quantum error correction or entanglement purification (see [BDSW96]). Out of these many studies of entanglement, none has so far addressed the issue of whether (and how well) entanglement can be cloned.

In this chapter, we raise the question of whether quantum entanglement itself can be cloned or not. In order to simplify our analysis, we restrict ourselves to qubit pairs (dimension 2×2). We show that the requirement of perfectly cloning the entanglement carried by a qubit pair in an arbitrary (ME) state is incompatible with the requirement that separable qubit pairs remain unentangled via cloning. Of course, if we restrict ourselves to four orthogonal ME states such as the Bell states

$$|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}, \;\; |\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}, \tag{8.1}$$

then we can very well make a Bell measurement of the original pair and subsequently prepare an arbitrary number of clones in the measured ME state. However, this procedure does not work properly on the linear combinations of Bell states that are separable states. Even if the clones are not required to be close to the original ME 2-qubit state but solely to be entangled, it remains impossible to fully preserve entanglement.

Here we show that it is nevertheless possible to clone part of the original entanglement, much in the same way quantum states can be cloned imperfectly. We define the optimal entanglement cloner as a machine that preserves separability while, for maximally-entangled input states, it produces two qubit pairs with the same and highest amount of entanglement regardless of their actual state. We construct a QCM that is universal over the set of ME 2-qubit states and argue that it effects an optimal cloning of entanglement. For this purpose, we exploit the property that the set of ME 2-qubit states is isomorphic to the set of *real* states in 4 dimensions [BDSW96], from which we construct an optimal symmetric cloner that is covariant under local unitaries. Finally, we consider asymmetric QCMs and investigate how entanglement is distributed among the clones by these transformations.

8.2 Entanglement no-cloning principle

Entanglement cannot be cloned perfectly, that is, if a quantum operation can be found that perfectly duplicates the entanglement of all ME states, then it necessarily does not preserve separability (some separable states become entangled after cloning).

Proof: We restrict ourselves to 2 qubits and consider two orthogonal ME states, e.g., $|\Phi^{\pm}\rangle$. Assume that the entanglement of these states is perfectly cloned, i.e., the output states of the clones remain ME even though they may differ from the input state. The most general cloning transformation U preserving the entanglement of these two states can be written as

$$|\Phi^{\pm}\rangle|A\rangle \xrightarrow{U} |e_a^{\pm}\rangle|e_b^{\pm}\rangle|A^{\pm}\rangle \ , \tag{8.2}$$

where $|A\rangle$ denotes the initial state of the ancilla and the blank copy, while $|A^{\pm}\rangle$ is the ancilla state after cloning. Thus, the states of the two clones $|e_a^{\pm}\rangle$ and $|e_b^{\pm}\rangle$ are some ME states. Now, the linear combination $|\tilde{\Phi}\rangle = (|\Phi^{+}\rangle + i|\Phi^{-}\rangle)/\sqrt{2} = (e^{i\pi/4}|00\rangle + e^{-i\pi/4}|11\rangle)/\sqrt{2}$ is still a ME state. By linearity, the above transformation yields the following output state

$$|\tilde{\Phi}\rangle|A\rangle \xrightarrow{U} (|e_a^{+}\rangle|e_b^{+}\rangle|A^{+}\rangle + i|e_a^{-}\rangle|e_b^{-}\rangle|A^{-}\rangle)/\sqrt{2} \ . \tag{8.3}$$

In order to preserve the full entanglement within each clone, a necessary condition is that either $|e_a^+\rangle = |e_a^-\rangle$ or $|e_b^+\rangle = |e_b^-\rangle$. However, in each of these two cases, at least one of the clones is left in a ME state that is independent of the input state (within the space spanned by $|\Phi^\pm\rangle$) regardless of it being separable or not. For example, in the first case, if the input is the separable state obtained as the linear combination $|s\rangle = (|\Phi^+\rangle + |\Phi^-\rangle)/\sqrt{2} = |00\rangle$, then the transformation gives

$$|s\rangle|A\rangle \xrightarrow{U} |e_a\rangle(|e_b^+\rangle|A^+\rangle + |e_b^-\rangle|A^-\rangle)/\sqrt{2}\ . \tag{8.4}$$

Clearly, the separability is not preserved here since the first clone is maximally entangled. We therefore conclude that no perfect cloning of entanglement is possible. □

As a consequence, only imperfect QCMs that approximately reproduce the entanglement while preserving separability can be implemented. In the rest of this chapter, we will be interested in separability-preserving QCMs that yield clones with the highest achievable entanglement for all ME input states. As shown later on, finding these QCMs is strongly related to finding transformations that clone optimally and equally well the set of 2-qubit ME states.

8.3 Cloning formalism

Consider an arbitrary 2-qubit pure state

$$|\Phi\rangle = \sum_{i=0}^{3} n_i |e_i\rangle \tag{8.5}$$

written in the orthonormal basis made of the Bell states with particular phases (sometimes referred to as the magic basis [BDSW96]):

$$|e_0\rangle = |\Phi^+\rangle,\ |e_1\rangle = i|\Phi^-\rangle,\ |e_2\rangle = i|\Psi^+\rangle,\ |e_3\rangle = |\Psi^-\rangle, \tag{8.6}$$

where the amplitudes n_i are normalized as $\sum_{i=0}^{3} |n_i|^2 = 1$. In this basis, the entanglement of formation E of the state $|\Phi\rangle$ can be expressed in a very simple way as

$$E(\mathcal{C}(\Phi)) = H\left(\frac{1}{2} + \frac{1}{2}\sqrt{1 - \mathcal{C}(\Phi)^2}\right)\ , \tag{8.7}$$

where H is the binary entropy function (as introduced in chapter 2) and

$$\mathcal{C}(\Phi) = |\sum_i n_i^2| \tag{8.8}$$

is called the concurrence [BDSW96, HW97]. Clearly, any *real* linear combination (up to an irrelevant global phase) of the magic basis elements is a ME state since $\mathcal{C}$ (and therefore E) is then equal to one. Furthermore, *every* ME state can be expressed as a real linear combination of the magic basis elements. For this reason, the problem of cloning the set of ME 2-qubit states boils down to constructing a transformation that optimally clones all real 4-dimensional states in the magic basis.

This particular transformation we will use is based on the Pauli cloning introduced in chapter 2: the qubit pair to be cloned is itself maximally entangled with a reference qubit pair. The most general joint state describing the reference R, the output clones A and B, and an ancilla C after the cloning transformation reads

$$|\mathcal{S}\rangle_{R,A,B,C} = \sum_{i,j,k,l=0}^{3} s_{ijkl}\ |l\rangle_R|i\rangle_A|j\rangle_B|k\rangle_C\ . \tag{8.9}$$

(The reference, the two clones, and the ancilla are all 4-dimensional systems here.) This state serves to completely define the cloning transformation: the result of cloning the ME state $|\Phi\rangle = \sum_i n_i|e_i\rangle$ (with real n_i's) is obtained by projecting R onto the complex conjugate $|\Phi^*\rangle$ (which is equal to $|\Phi\rangle$ here). Thus, the most general cloning transformation is defined as

$$|\Phi\rangle \to \sum_{i,j,k,l=0}^{3} s_{ijkl}\ n_l\ |i\rangle_A|j\rangle_B|k\rangle_C\ . \tag{8.10}$$

At this point, we impose the additional condition that the QCM is covariant under $SU(2)\times SU(2)$ in the computational basis (or, equivalently, under $SO(4)$ in the magic basis). This means that the QCM acts similarly in all bases connected by local unitaries to the computational basis. This restriction is natural since it guarantees that all states equivalent up to local unitaries (thereby having the same entanglement) result in equally entangled clones. A sufficient condition for covariance is [NC03]

$$|\mathcal{S}\rangle_{R,A,B,C} = R^{\otimes 4}\ |\mathcal{S}\rangle_{R,A,B,C}\ , \tag{8.11}$$

where R is any real rotation matrix in $SO(4)$. This requirement implies that s_{ijkl} is an invariant tensor of rank four, that is, $s_{ijkl} = R_{ii'}R_{jj'}R_{kk'}R_{ll'}\,s_{i'j'k'l'}$. A main simplification here results from the fact that the generic form of such a tensor is

$$s_{ijkl} = a\ \delta_{il}\delta_{jk} + b\ \delta_{jl}\delta_{ik} + c\ \delta_{kl}\delta_{ij}\ , \tag{8.12}$$

with the normalization condition on (8.10) imposing that

$$4(|a|^2 + |b|^2 + |c|^2) + 2\,\mathrm{Re}(ab^* + ac^* + bc^*) = 1\ . \tag{8.13}$$

For a symmetric cloner, the permutation symmetry between the two clones imposes furthermore that $a = b$, so that we are left with a transformation depending on two parameters, a and c. If we use the cloning fidelity as a figure of merit, Eqs. (8.10) and (8.12) result in

$$F = \langle\Phi|\rho_{A,B}|\Phi\rangle = 7|a|^2 + |c|^2 + 4\,\mathrm{Re}(ac^*) \;, \tag{8.14}$$

where $\rho_{A(B)}$ denotes the reduced density matrix of clone $A(B)$. This expression can be maximized under the normalization constraint Eq. (8.13), giving

$$a = \frac{1}{3}\left(\frac{1}{2} + \frac{1}{\sqrt{13}}\right)^{1/2}, \quad c = \frac{A}{2}(\sqrt{13} - 3) \;, \tag{8.15}$$

with the corresponding fidelity

$$F = \frac{5 + \sqrt{13}}{12} \simeq 0.7171 \;. \tag{8.16}$$

Interestingly, this maximization procedure yields a fidelity that saturates the upper bound derived from the no-signaling condition in [NC03]. We therefore conclude that the optimal covariant cloner of ME 2-qubit states is characterized by Eq. (8.15) and yields the fidelity (9.6). This is slightly higher than the fidelity of the universal 4-dimensional cloner, namely $F = 7/10$ [Wer98, Cer98], as expected since the ME states form a subset of the 2-qubit states.

We now generalize Eq. (8.14) to asymmetric cloning transformations ($A \neq B$). The cloning fidelities become

$$\begin{aligned} F_a &= 4|a|^2 + |b|^2 + |c|^2 + 2\,\mathrm{Re}(ab^* + ac^* + bc^*) \;, \\ F_b &= 4|b|^2 + |a|^2 + |c|^2 + 2\,\mathrm{Re}(ab^* + ac^* + bc^*) \;. \end{aligned} \tag{8.17}$$

Assuming a, b, and c to be real, we eliminate a and c from Eqs. (8.13) and (8.17), to get

$$\begin{aligned} F_A(b, F_B) = -3b^2 + \frac{F_B + 1}{2} + \frac{\sqrt{-3b^2 + F_B} - b}{2} \\ \times\sqrt{18b^2 + 18b\sqrt{-3b^2 + F_B} - 15F_B + 6} \;. \end{aligned} \tag{8.18}$$

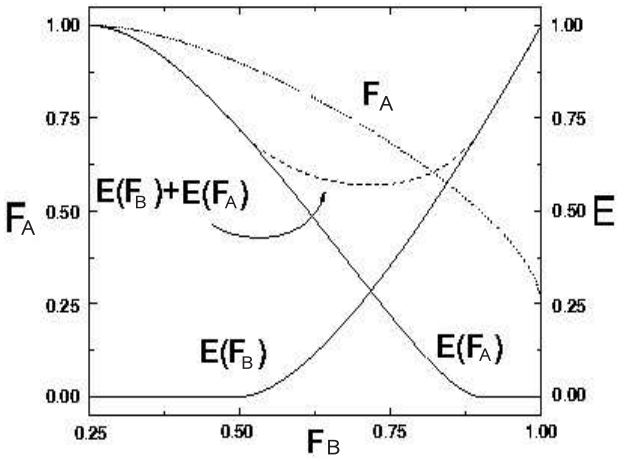

Figure 8.1: Fidelity (dotted line) of clone A as a function of that of clone B for the optimal 2-qubit entanglement cloner. The two fidelities coincide at $F_A = F_B = (5 + \sqrt{13})/12$. Entanglement of formation of clones A and B (solid line) and their sum (dashed line) as a function of the fidelity of clone B. The two curves intersect at $E_A = E_B = 0.2847$.

We then maximize F_A over b as a function of F_B. Figure 9.1 displays the resulting F_A as a function of F_B. The mid-point value of this curve lies at $F_A = F_B = F$, as expected. We also confirm that the fidelity of a clone is equal to one when the other one is in a completely mixed state, i.e., when its fidelity equals 1/4.

8.4 Semidefinite programming

We have numerically confirmed the optimality of this class of asymmetric cloners with the use of a technique based on semidefinite programming [Fiu01, Fiu03]. This technique enables one to obtain the maximal (mean) fidelity that can be attained by the optimal CP-map which most closely approximates a given transformation between pure states. Before applying this method to entanglement cloning, we briefly describe its foundation.

Suppose we would like to implement a transformation between pure states $|\psi_{\text{in}}\rangle \in \mathcal{H}$ and $|\psi_{\text{out}}\rangle \in \mathcal{K}$

$$|\psi_{\text{in}}(\vec{x})\rangle \rightarrow |\psi_{\text{out}}(\vec{x})\rangle. \tag{8.19}$$

Here $\vec{x}$ denotes a set of numbers parametrizing all pure states in Hilbert space of input states $\mathcal{H}$. Note that the dimensions of input and output Hilbert spaces may differ in

general, $\dim\mathcal{H} \neq \dim\mathcal{K}$. It may happen that the desired transformation (8.19) cannot be implemented exactly because (8.19) is not a linear CP-map (e.g. perfect cloning of non-orthogonal states) and we thus want to find a CP-map which most closely approximates the transformation (8.19).

Let us begin by introducing a convenient representation of the CP-maps. We say that map $\rho \to \mathcal{E}(\rho)$ is positive if it preserves the positivity of operators ρ. The map $\mathcal{E}$ is completely positive if and only if the extension $\mathcal{E}_{\mathcal{H}} \otimes \mathcal{I}_{\mathcal{H}'}$ is a positive map for any Hilbert space $\mathcal{H}'$, where $\mathcal{I}$ is an identity map. Any CP-map can be represented by a positive operator [**?**]. Consider the maximally entangled state on $\mathcal{H}^{\otimes 2}$,

$$|\varphi\rangle = \sum_{j=1}^{\dim\mathcal{H}} |j\rangle_1 |j\rangle_2 \tag{8.20}$$

and define the operator

$$\chi = \mathcal{E}_{\mathcal{H}} \otimes \mathcal{I}_{\mathcal{H}}(|\varphi\rangle\langle\varphi|). \tag{8.21}$$

Note that χ acts on a Hilbert space $\mathcal{H} \otimes \mathcal{K}$. It is easy to show that the CP-map $\rho_{\text{out}} = \mathcal{E}(\rho_{\text{in}})$ can be written as

$$\rho_{\text{out}} = \text{Tr}_{\mathcal{H}}[\chi\, \rho_{\text{in}}^{\text{T}} \otimes \hat{1}_{\mathcal{K}}], \tag{8.22}$$

where T stands for the transposition and $\hat{1}_{\mathcal{K}}$ denotes the identity operator on $\mathcal{K}$. The requirement that the CP-map $\mathcal{E}$ should preserve the trace imposes the following constraint on χ,

$$\text{Tr}_{\mathcal{K}}[\chi] = \hat{1}_{\mathcal{H}}. \tag{8.23}$$

We would like to quantify how well the CP-map χ approximates the desired transformation (8.19). To this end we define the mean fidelity as

$$F = \int d\vec{x} \langle\psi_{\text{out}}(\vec{x})|\mathcal{E}\left(|\psi_{\text{in}}(\vec{x})\rangle\langle\psi_{\text{in}}(\vec{x})|\right)|\psi_{\text{out}}(\vec{x})\rangle, \tag{8.24}$$

where $d\vec{x}$ denotes the proper measure on space of pure states $|\psi_{\text{in}}(\vec{x})\rangle$. With the help of Eq. (8.22) we may rewrite the expression (8.24) as

$$F = \text{Tr}[\chi R], \tag{8.25}$$

where the positive operator R acting on $\mathcal{H} \otimes \mathcal{K}$ is given by

$$R = \int d\vec{x} \left(|\psi_{\text{in}}(\vec{x})\rangle\langle\psi_{\text{in}}(\vec{x})|\right)^{\text{T}} \otimes |\psi_{\text{out}}(\vec{x})\rangle\langle\psi_{\text{out}}(\vec{x})|. \tag{8.26}$$

Our task is to find a trace-preserving CP-map χ which maximizes the fidelity (9.6). We take into account the constraint (8.23) by introducing an operator Lagrange multiplier $\Lambda = \hat{\lambda} \otimes \hat{1}_{\mathcal{K}}$ and we look for the maximum of the functional

$$\tilde{F}[\chi] = \mathrm{Tr}[\chi R] - \mathrm{Tr}[\chi \Lambda]. \tag{8.27}$$

We expand χ in eigenstate basis

$$\chi = \sum_j r_j |\pi_j\rangle\langle\pi_j|, \tag{8.28}$$

and rewrite the functional (8.27) as

$$\tilde{F}[\chi] = \sum_j r_j \langle\pi_j| R - \Lambda |\pi_j\rangle.$$

A variation of $\tilde{F}[\chi]$ with respect to $\langle\pi_j|$ yields the extremal equations,

$$(R - \Lambda) r_j |\pi_j\rangle = 0. \tag{8.29}$$

We multiply Eq. (8.29) by $\langle\pi_j|$ and sum over j. After some manipulations we obtain

$$\chi = \Lambda^{-1} R \chi. \tag{8.30}$$

Further we take Hermitian conjugate of this formula, $\chi = \chi R \Lambda^{-1}$, and insert it back to the right-hand side of Eq. (8.30). Thus we arrive at a symmetrized extremal equation

$$\chi = \Lambda^{-1} R \chi R \Lambda^{-1}. \tag{8.31}$$

The Lagrange multiplier $\Lambda = \hat{\lambda} \otimes \hat{1}_{\mathcal{K}}$ can be determined from the constraint (8.23) which provides expression for $\hat{\lambda}$,

$$\hat{\lambda} = \left(\mathrm{Tr}_{\mathcal{K}}[R \chi R]\right)^{1/2}. \tag{8.32}$$

We fix the square root by postulating that $\hat{\lambda}$ is positive Hermitian operator. The system of coupled nonlinear extremal equations (8.31) and (8.32) can be conveniently solved by means of repeated iterations, starting from some initial 'unbiased' CP-map, for example a map which transforms every input density matrix to the maximally mixed state on $\mathcal{K}$, $\rho_{\mathrm{in}} \to \hat{1}_{\mathcal{K}}/\mathrm{dim}\mathcal{K}$. Note that the iterations preserve the positivity of χ and the constraint (8.23) is exactly satisfied at each iteration step.

From the formula (9.6) we can obtain an upper bound on the optimal fidelity F,

$$F \leq \mathrm{Tr}[\chi] R_{\max} = \mathrm{dim}\mathcal{H} R_{\max}, \tag{8.33}$$

where $R_{\max}$ is the largest eigenvalue of the operator R. If we find a CP-map which reaches the upper bound on fidelity (8.33) then such transformation is, by definition, optimal one. (8.18)

In our case, the cloning transformation is a linear trace-preserving CP-map that can be represented by the positive semidefinite operator Ω on the tensor-product space of the input and output states. The cloning fidelities can be expressed as $F_{A(B)} = \mathrm{Tr}[\Omega S_{A(B)}]$, where

$$S_{A(B)} = \mathrm{Tr}_{B(A)} \int d\vec{x} \left(|\Phi_{\mathrm{in}}(\vec{x})\rangle\langle\Phi_{\mathrm{in}}(\vec{x})|\right)^{\mathrm{T}} \otimes \left(|\Phi_{\mathrm{out}}(\vec{x})\rangle\langle\Phi_{\mathrm{out}}(\vec{x})|\right) \tag{8.34}$$

and

$$|\Phi_{\mathrm{out}}(\vec{x})\rangle\langle\Phi_{\mathrm{out}}(\vec{x})| = |\Phi_{\mathrm{in}}(\vec{x})\rangle_A\langle\Phi_{\mathrm{in}}(\vec{x})| \otimes |\Phi_{\mathrm{in}}(\vec{x})\rangle_B\langle\Phi_{\mathrm{in}}(\vec{x})|.$$

The optimal asymmetric cloner can be obtained by maximizing $F = pF_A + (1-p)F_B$, where $p \in [0,1]$ is the asymmetry parameter. The resulting fidelities coincide with those obtained from Eq. (8.18) up to the machine precision.

8.5 Discussion

Let us now investigate the entanglement properties of this cloning transformation and show that it is also optimal with respect to our original goal, namely cloning the amount of entanglement. Let us start by checking that it preserves separability. For the ansatz (8.9), we have $\Omega = \mathrm{Tr}_C(|\mathcal{S}\rangle\langle\mathcal{S}|)$, and the CP-map that describes the relationship between the input and the clone A (B) can be characterized by $\Omega_{A(B)} = \mathrm{Tr}_{B(A)}[\Omega] \geq 0$. Since the positive partial transpose (PPT) criterion is a necessary and sufficient separability condition for a qubit pair, a sufficient condition for these two maps to preserve separability is that Ω_A and Ω_B represent PPT operations [Rai01]. The map $\Omega_{A(B)}$ is PPT if $\Omega_{A(B)}^{T_{1,1'}} \geq 0$, where $T_{1,1'}$ denotes partial transposition with respect to the first qubit of the original and the clone $A(B)$. An explicit analytical calculation shows that if s_{ijkl} is an invariant rank-4 tensor (8.12), then $\Omega_{A(B)}^{T_{1,1'}} = \Omega_{A(B)} \geq 0$, hence a covariant cloner necessarily preserves separability.

It is therefore natural to maximize the output entanglement for the other extreme case, namely when the original qubit pair is maximally entangled. The amount of entanglement left in the clones will be measured here by the entanglement of formation E, which can be evaluated by using the extended definition of the concurrence $\mathcal{C}$ for mixtures [HW97]. The entanglement of formation of an arbitrary 2-qubit state ρ is

given by $E(\rho) = E(\mathcal{C}(\rho))$, where $\mathcal{C}(\rho) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4)$ and the λ_i's are the eigenvalues, in decreasing order, of the Hermitian matrix $\tilde{\rho} \equiv \sqrt{\sqrt{\rho}\rho^*\sqrt{\rho}}$. Here ρ^* denotes the complex conjugate of ρ when expressed in the magic basis [HW97]. For a generic covariant cloner, Eq. (8.12), the reduced density matrices of the clones of an input ME state $|e_i\rangle$ can always be written as

$$\rho_{A,B} = F_{A,B} \, |e_i\rangle\langle e_i| + \frac{1 - F_{A,B}}{3} \sum_{j \neq i} |e_j\rangle\langle e_j| \ , \tag{8.35}$$

so the clones are left in a mixture of (generalized) Bell states. This is consistent with the fact that $\rho_{A,B}$ are real density matrices in the magic basis because the input state is real [HW97]. Hence, $\tilde{\rho}_{A,B} = \rho_{A,B}$ so the concurrence of the clones simply reduces to $\mathcal{C}_{A,B} = \max(0, 2F_{A,B} - 1)$. Therefore, for a covariant cloner, maximizing E reduces to maximizing F. Consequently, the cloner characterized by Eq. (8.15) is the entanglement cloner we were looking for, provided that covariance is taken for granted.

The corresponding entanglement of formation of the clones, E_A and E_B, is shown in Fig. 9.1 for different values of F_A. As expected, the entanglement of formation of clone B vanishes for $F_B \leq 1/2$. Conversely, the entanglement of formation of clone A vanishes when $F_B \geq 0.8984$ (that is, when $F_A \leq 1/2$). Note that the entanglement of formation of a clone is equal to one only when its fidelity is one, thus confirming that a fully asymmetric cloner (a trivial cloner which outputs the original and a random clone) is the only solution if we want to fully conserve the original entanglement of 1 ebit. Finally, note that the sum of the entanglement of formation of the two clones (also shown in Fig. 9.1) never exceeds one, meaning that the entanglement cloner does not create more entanglement than that contained in the original ME state.

For the symmetric cloner, the entanglement of formation of both clones is equal to $E_A = E_B = 0.2847$ bits. The optimality of this result has been verified using numerical optimization where the structure of the cloning transformation was based on the Pauli cloning formalism and the maximized quantity was the concurrence instead of the fidelity. The optimization was carried out without imposing the covariance of the cloning machine. Up to irrelevant local unitaries (which decrease F while keeping $\mathcal{C}$ and E constant), we recovered the same cloning transformation. This strongly suggests that restricting ourselves to covariant QCMs is justified, so the cloner of ME states also optimally clones the amount of entanglement.

Finally, the properties of our entanglement cloner can be analyzed in the intermediate

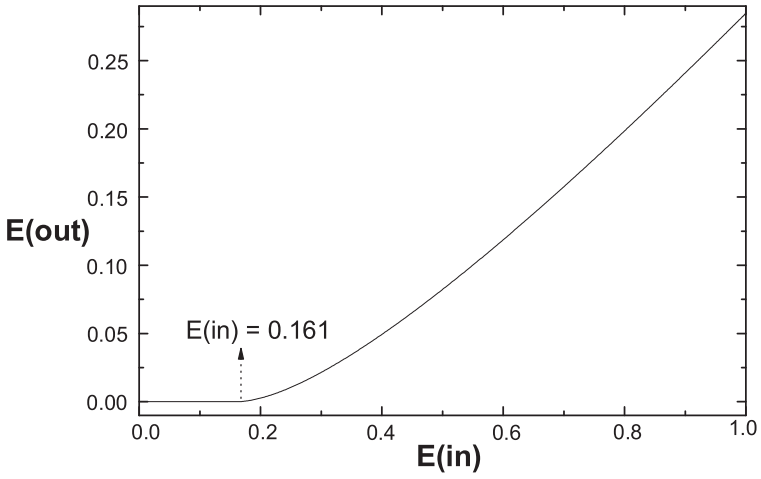

Figure 8.2: Entanglement of the clones versus the entanglement of the input state for the symmetric cloner.

case of non-maximally entangled input states. In Figure 9.2, we plot the entanglement of formation of the clones as a function of that of the original state $\alpha|00\rangle + \sqrt{1-\alpha^2}|11\rangle$ $(0 \leq \alpha \leq 1)$ for the symmetric cloner. No entanglement is cloned below a critical value $E_{\text{in}} = 0.161$ bits. Then, the output entanglement increases monotonically to reach its maximum $E_{\text{out}} = 0.2847$ bits at $E_{\text{in}} = 1$ bit.

8.6 Conclusion

In conclusion, we have shown that the quantum entanglement of an unknown ME qubit pair cannot be perfectly cloned if, at the same time, product states are required to be cloned into unentangled qubit pairs. In other words, a separability-preserving QCM cannot perfectly duplicate the entanglement of the set of ME states. Only imperfect QCMs do exist. As a first step, we have constructed an optimal symmetric entanglement cloner which is universal over the set of ME states, and whose fidelity saturates the no-signaling upper bound [NC03]. This cloner yields imperfect clones with 0.285 ebits if the original qubit pair contains 1 ebit, while unentangled pairs are cloned into separable states. The distribution of entanglement among the clones has also been investigated using an asymmetric cloner. Similarly to the situation that prevails when cloning quantum states, this no-go theorem for entanglement cloning might be exploited in order to imagine new quantum key distribution schemes. For example, one could imagine a protocol where the eavesdropper is only able to apply a *local* cloning on a ME state instead of the above global cloning. One can check that

applying the optimal universal qubit cloner [HW97] locally on each qubit of a ME state reduces the fidelity of the clones to 7/12. We obtain $\mathcal{C} = 1/6$ leading to only about 0.060 ebits per clone. Thus, the fact that independent local operations on each qubit are less efficient than joint operations could be used to give an advantage to the authorized parties.

Chapter 9

Asymmetric phase-covariant d-dimensional cloning

9.1 Introduction

A typical feature of quantum cloning is that the optimal cloning transformation depends on the considered set of input states. The greater the set, the lower the fidelity. More precisely, if the set of input states is the orbit of a given state under the action of a group of unitary transformations the smaller is the group, the higher is the fidelity.

In this chapter, we analyze quantum cloning machines that duplicate with an equal fidelity all uniform d-dimensional superposition states with arbitrary phases. These so-called phase-covariant cloners have been found initially for qubits ($d = 2$) [BBP$^+$96, CDG02] (and considered in chapter 5 in the context of the BB84 protocol) and qutrits ($d = 3$) [dP01, CDG02, dM03], and we shall investigate their d-dimensional extension here. We will use the Pauli cloning formalism introduced in chapter 2 which we generalize here. As we shall see, our approach will automatically lead to the optimal covariant cloning under the Abelian group $U(1)^{\otimes(d-1)}$ of phase rotations – the phase-covariant d-dimensional cloning. Although we give no analytical proof that our transformation is optimal, it has been shown very recently to be the case for symmetric cloners by Fan *et al.* in [FIMW03]. In their paper, Fan *et al.* calculate the optimal $1 \to 2$ cloning map for the set of d-dimensional input states $e^{i\phi_0}|0\rangle + e^{i\phi_1}|1\rangle + ... + e^{i\phi_{d-1}}|d-1\rangle$ by considering the most general cloning transformation where the only assumption made is that the cloner is symmetric, *i.e.*, one has identical cloning maps for both clones. The drawback is that the calculation of the reduced density matrices of the clones and maximization of the fidelity is somewhat tedious. The Pauli cloning method allows to

recover the same result in a much simpler way, as well as extending it very naturally to the asymmetric case. In the latter case, we have checked the optimality of our construction by numerically computing (with the help of semidefinite programming) the best asymmetric cloning transformation (for several asymmetry parameters), and verifying that the results coincide up to the machine precision. We conclude this chapter by comparing of the performance of the optimal d-dimensional phase covariant cloner with the other known cloners in d dimensions, namely the universal cloner [Wer98, Cer98, BH98], the cloner of real states [NC03], and the cloner of two mutually unbiased bases [CBKG02].

9.2 Optimal phase-covariant cloning

We begin by briefly generalizing the Pauli cloning formalism. The state we consider lies in d-dimensional Hilbert space and is expressed as $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{i\phi_k} |k\rangle$. The output of the cloning machine is such that if the input state is $|\psi\rangle$, then the resulting joint state of the two output clones (noted A and B) and the cloning machine (noted C) is:

$$\begin{aligned} |\psi\rangle \rightarrow & \sum_{m,n=0}^{d-1} a_{m,n} U_{m,n} |\psi\rangle_A |B_{m,-n}\rangle_{B,C} \\ = & \sum_{m,n=0}^{d-1} b_{m,n} U_{m,n} |\psi\rangle_B |B_{m,-n}\rangle_{A,C} \end{aligned} \tag{9.1}$$

where

$$U_{m,n} = \sum_{k=0}^{d-1} e^{2i\pi(kn/d)} |k+m\rangle\langle k| \tag{9.2}$$

and

$$|B_{m,n}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2i\pi(kn/d)} |k\rangle|k+m\rangle \tag{9.3}$$

with $0 \leq m, n \leq d-1$. Here, $U_{m,n}$ is a generalized error operator that acts on a d-dimensional system (in contrast to chapter 5 where we considered an error operator as $\log_2 d$ tensor products of the Pauli matrices each acting on a 2-dimensional system). More precisely, the error operator $U_{m,n}$ acting on state $|\psi\rangle$ shifts the state by m units (modulo d) in the computational basis, and multiplies it by a phase so as to shift its Fourier transform by n units (modulo d). Equation (9.3) defines the d^2 generalized Bell states for a pair of d-dimensional systems. Tracing over systems B and C (or A and C) yields the final state of clone A (or clone B): if the input state is $|\psi\rangle$, then the

clones A and B are left in a mixture of the states $|\psi_{m,n}\rangle = U_{m,n}|\psi\rangle$ with respective weights $|a_{m,n}|^2$ and $|b_{m,n}|^2$:

$$\rho_A = \sum_{m,n=0}^{d-1} |a_{m,n}|^2 \, |\psi_{m,n}\rangle\langle\psi_{m,n}|$$
$$\rho_B = \sum_{m,n=0}^{d-1} |b_{m,n}|^2 \, |\psi_{m,n}\rangle\langle\psi_{m,n}|. \tag{9.4}$$

In addition, the weights of the two clones are related through the fact that the amplitude functions $a_{m,n}$ and $b_{m,n}$ are dual under a Fourier transform [Cer98, Cer00]:

$$b_{m,n} = \frac{1}{d} \sum_{x,y=0}^{d-1} e^{2i\pi(nx-my)/d} a_{x,y}. \tag{9.5}$$

The fidelity of a clone, say A, is given by

$$F_A = \langle\psi|\rho_A|\psi\rangle = \sum_{m,n=0}^{d-1} |a_{m,n}|^2 |\langle\psi|\psi_{m,n}\rangle|^2 \tag{9.6}$$

and similarly for the clone B (replace the $|a_{m,n}|^2$ term by $|b_{m,n}|^2$). Inserting this state $|\psi\rangle$ in Eq. (9.6) yields the expression for the fidelity F_A with

$$\langle\psi|\psi_{m,n}\rangle = \frac{1}{d} \sum_{k=0}^{d-1} e^{i(\phi_k - \phi_{k+m})} \, e^{2i\pi(nk)/d}. \tag{9.7}$$

Note that if $m = 0$, then the identity $\sum_{k=0}^{d-1} e^{2i\pi(nk)/d} = d\,\delta_{n,0}$ implies that $\langle\psi|\psi_{m,n}\rangle = \delta_{n,0}$, so that all the elements of the $a_{m,n}$ matrix with $m = 0$ and $n \neq 0$ do not contribute to the fidelity F_A. We are interested in a cloning machine that yields the same fidelity for all possible values of the ϕ_j's. This imposes strong contraints on the amplitudes $a_{m,n}$ characterizing the cloner. A form which does satisfy these constraints is expressed by the following amplitude matrix

$$a_{m,n} = \begin{pmatrix} v & y & \cdots & y \\ x & x & \cdots & x \\ \vdots & & & \vdots \\ x & x & \cdots & x \end{pmatrix} \tag{9.8}$$

where v, x, and y are arbitrary constants satisfying the normalization constraint

$$v^2 + (d-1)y^2 + d(d-1)x^2 = 1. \tag{9.9}$$

Replacing these $a_{m,n}$ values in Eq. (9.7) yields for the fidelity

$$F_A = v^2 + (d-1)x^2 \tag{9.10}$$

which is indeed independent of y. Note that for a universal cloner (a cloning machine which optimally clones all states in d-dimensional Hilbert space with the same fidelity), one has $x = y$ [Cer98, Cer00]. The main idea here is that we can have $x > y$, implying that the cloning fidelity for the states (**??**) can be higher than that of the universal cloner, at the expense of a lower fidelity for the states of the computational basis $\{|k\rangle\}$.

The second clone is characterized by a similar amplitude matrix

$$b_{m,n} = \begin{pmatrix} v' & y' & \cdots & y' \\ x' & x' & \cdots & x' \\ \vdots & & & \vdots \\ x' & x' & \cdots & x' \end{pmatrix}. \tag{9.11}$$

where the different matrix elements are related to the $a_{m,n}$ coefficients by Eq. (9.5):

$$v' = \frac{1}{d}[v + (d-1)y + d(d-1)x] \tag{9.12}$$

$$y' = \frac{1}{d}[v + (d-1)y - dx] \tag{9.13}$$

$$x' = \frac{1}{d}(v - y). \tag{9.14}$$

Since we seek a symmetric cloner, the amplitude coefficients for the two clones must be equal, that is

$$v = v' = \frac{V + (d-1)X}{\sqrt{d}} \tag{9.15}$$

$$y = y' = \frac{V - X}{\sqrt{d}} \tag{9.16}$$

$$x = x' = \frac{X}{\sqrt{d}}. \tag{9.17}$$

where we have introduced two new parameters V and X (the third parameter has been eliminated by the symmetry constraint). In addition, as a result of the normalization condition

$$V^2 + 2(d-1)X^2 = 1, \tag{9.18}$$

only one free parameter remains. In this new parametrization, the expression of the fidelity (for both clones) reduces to

$$F = \frac{1 + (d-1)(d-2)X^2 + 2(d-1)VX}{d}. \tag{9.19}$$

We are interested in finding the values of V and X that maximize Eq. (9.19) under the normalization constraint (9.18). A simple maximization by use of Lagrange multipliers yields

$$F_{opt} = \frac{1}{d}\left[1 + \frac{d-2+\sqrt{(d-2)^2+8(d-1)}}{4}\right], \tag{9.20}$$

which coincides with the fidelity of the optimal $1 \to 2$ phase-covariant QCM for any dimension as found in [FIMW03]. The corresponding solutions of V and X are

$$V^2 = \frac{d-1}{d}\frac{1}{1+(d-2)F_{opt}} \tag{9.21}$$

$$X^2 = \frac{1}{2(d-1)} - \frac{1}{2d}\frac{1}{1+(d-2)F_{opt}}. \tag{9.22}$$

In Figure 1, we plot the fidelity of the clones as a function of the dimension. Note that the cloning fidelity F_{opt} tends to $1/2 + O(1/d)$ in the high-dimensional limit. Indeed, in this limit, the cloner operates simply by moving the input state into one of the clones, chosen at random, while preparing the other clone in the fully mixed state. As the latter has a vanishing contribution to the fidelity in the high-dimensional limit, we get a fidelity of $\frac{1}{2}$. In the special case where $d = 2$, we recover the optimal phase-covariant qubit cloner of fidelity [BCdM00, CDG02]

$$F_{d=2} = \frac{1}{2}(1 + 1/\sqrt{2}) \simeq 0.854 \tag{9.23}$$

while, when $d = 3$, we recover the optimal two-phase-covariant qutrit cloner [dP01, CDG02]

$$F_{d=3} = \frac{5+\sqrt{17}}{12} \simeq 0.760 \tag{9.24}$$

9.3 Asymmetric cloning

We now generalize Eq. (9.20) to asymmetric cloning transformations ($F_A \neq F_B$). The cloning fidelity of the first clone can be expressed as a function of the fidelity of the second clone (again using the same forms of the $a_{m,n}$ and $b_{m,n}$ matrices) as

$$F_A(F_B, v, y) = v^2 + \Delta \tag{9.25}$$

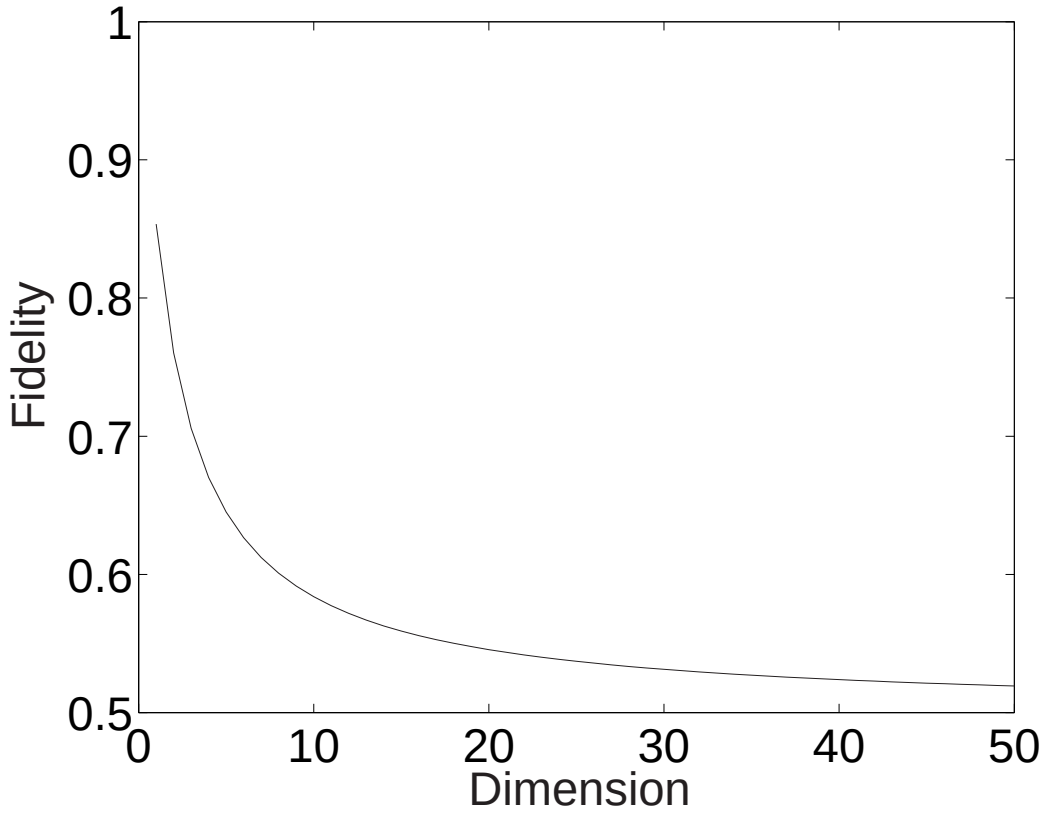

Figure 9.1: Fidelity of the clones versus the dimension for the symmetric phase-covariant cloner. The continuous line is there for visual purposes only.

and the normalization as

$$v^2 + (d-1)y^2 + \Delta = 1 \tag{9.26}$$

where

$$\Delta = \frac{\left(-2yd - 2v + 2y + 2\sqrt{2ydv - y^2d + v^2 - 2vy + y^2 + F_B d^2 - dv^2}\right)^2}{4(d-1)d^2}. \tag{9.27}$$

We then maximize F_A over v and y while keeping d and F_B constant, yielding the best possible balance between the fidelities F_A and F_B. Figure 2 displays the resulting

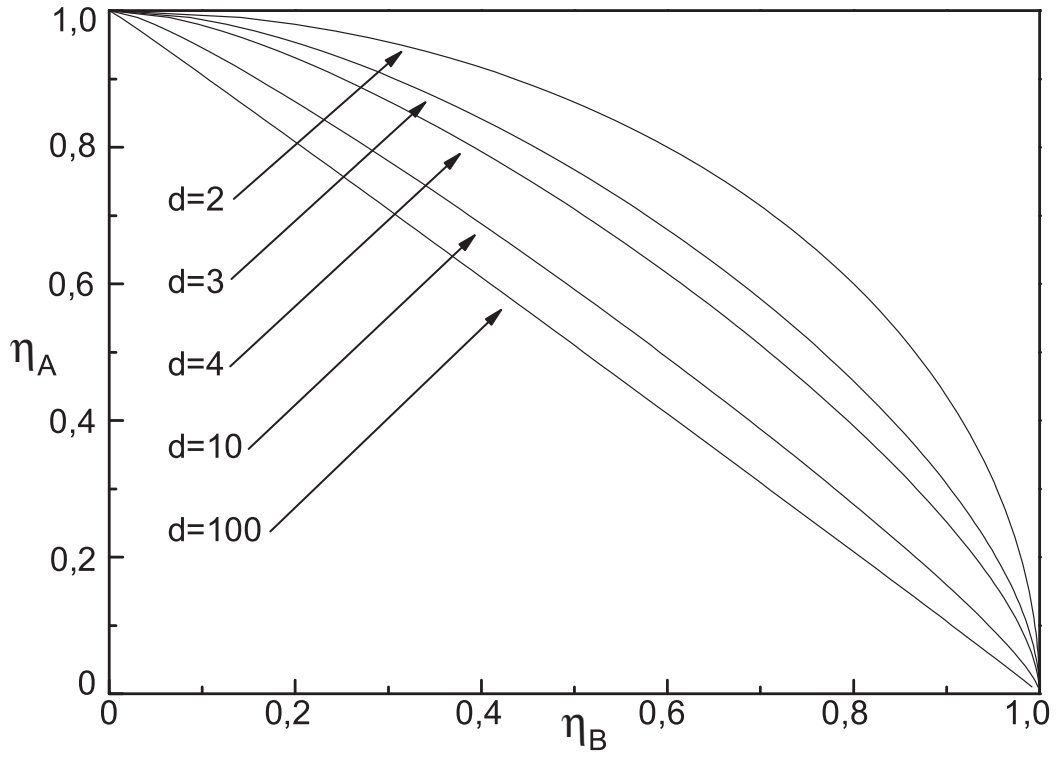

Figure 9.2: Shrinking factor of clone A as function of the shrinking factor of clone B for d = 2,3,4,10 and 100.

shrinking factor η_A of the first clone as a function of the shrinking factor of the second clone η_B. The shrinking factor η is defined here as the probability for the input state not to be depolarized, that is, $F = \eta + (1-\eta)/d$. We see that the fidelity of a clone is equal to one (or $\eta = 1$) when the fidelity of the second clone is equal to $1/d$ (or $\eta = 0$), i.e., when it is completely mixed. We also confirm that the quality of the

clones diminishes as a function of the dimension.

We have numerically confirmed the optimality of this class of asymmetric (and therefore symmetric) cloners with the use of a technique based on semidefinite programming introduced in the previous chapter. The cloning transformation is a linear trace-preserving completely positive (CP) map that can be represented by a positive semidefinite operator Ω on the tensor-product space of the input state ($|\psi\rangle$) and output states ($|\psi\rangle\langle\psi|^{\otimes 2}$). The fidelities can be expressed as $F_{A(B)} = \mathrm{Tr}[\Omega S_{A(B)}]$ with an appropriately defined operator $S_{A(B)} \geq 0$ (see chapter 9). The optimal asymmetric cloner can be obtained by maximizing $F = pF_A + (1-p)F_B$, where $p \in [0,1]$ is the asymmetry parameter. The resulting fidelities coincide with those obtained when maximizing Eq. (9.25) up to the machine precision.

9.4 Conclusion

We have found the class of optimal $1 \to 2$ phase-covariant QCMs in any dimension d along with their corresponding fidelities, Eq. (9.20). Although it was not demonstrated analytically but only checked numerically, this cloner has been proved to be optimal in [FIMW03] in the symmetric case. In the special case where $d = 2$ and $d = 3$, we recover the optimal phase-covariant qubit and qutrit cloners. Furthermore, we have extended our investigation to the class of asymmetric QCMs, and concluded that the relative fidelity between two clones decreases with the dimension.

In Figure 3, we have plotted, for comparaison, the fidelity as a function of the dimension d for the universal cloner [Wer98, Cer98, BH98], the real cloner [NC03], the optimal cloner of two mutually unbiased bases [CBKG02], and the optimal phase-covariant cloner. As expected, the universal d-dimensional cloner has a lower fidelity

$$F_U = (d+3)/(2(d+1)) \tag{9.28}$$

than the other cloners since they span smaller sets of states. The cloner of two mutually unbiased bases is the one which spans the smaller set and therefore has the highest fidelity

$$F_{MU} = \frac{1}{2}(1 + \frac{1}{\sqrt{d}}). \tag{9.29}$$

In between lies the real cloner

$$F_R = \frac{1}{2} + \frac{\sqrt{d^2+4d+20} - d + 2}{4(d+2)} \tag{9.30}$$

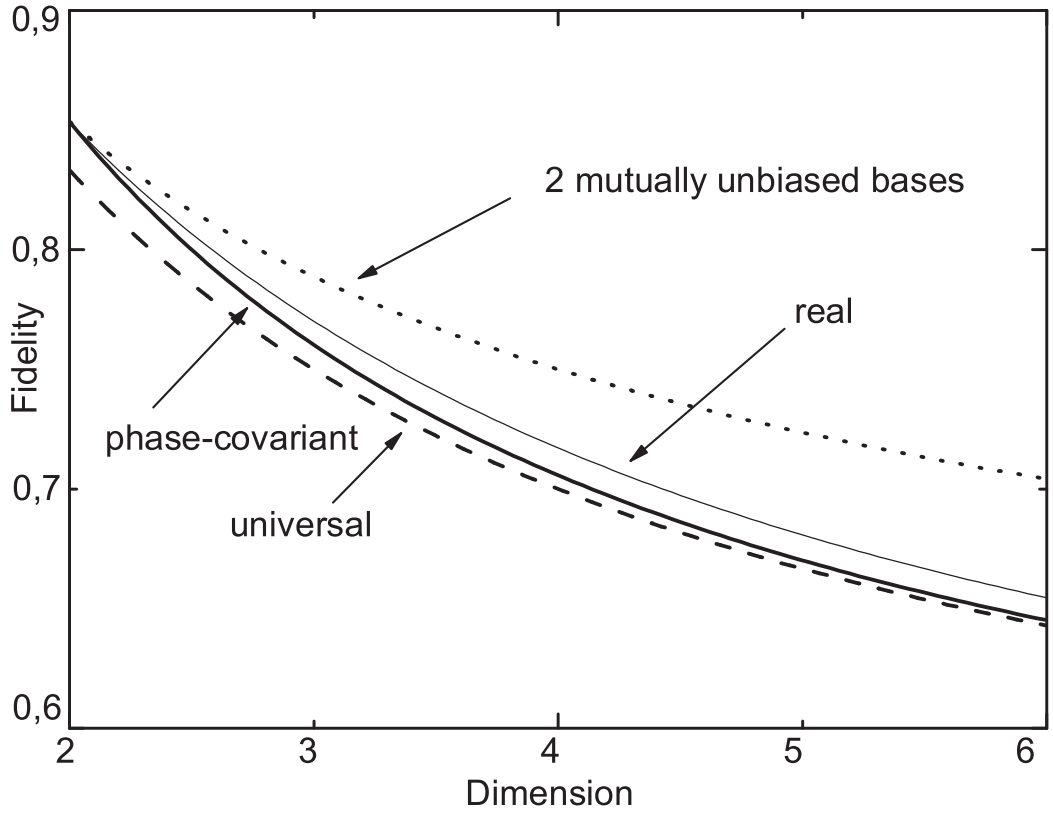

Figure 9.3: Fidelity F as a function of the dimension d for the universal cloner (dash) [Wer98, BH98], the real cloner [NC03], the phase-covariant cloner derived in this paper and the cloner of two mutually unbiased bases (dot) [CBKG02]. The lines are there for visual purposes.

and phase-covariant cloner. Except when $d = 2$ where the fidelities of the latter two cloners are equal to that of the cloner of two mutually unbiased bases, the fidelity of the d-dimensional phase-covariant cloner remains close to the universal cloner and slightly below the real cloner.

Chapter 10

Summary

It is interesting to see how, in a little over 10 years, quantum information has grown from being an intellectual game to a mature field of physics which not only is yielding important results within its own realm but also offering insight in other fields of science as well. This has been illustrated throughout the chapters of this thesis as our results impact not only quantum computation and communication but also quantum optics and classical communication. It is this pluridisciplinary character that not only renders the field exciting and interesting but also draws adepts from every branch of science. The global attention that the field is gaining is perhaps the reason why it is advancing so quickly.

This thesis mainly fused cryptography with quantum optics. The major goal being to exploit the linear dynammics of individual photons in order to perform serure cryptographic tasks. In our opinion, this goal has been fulfilled as we have described the implementation of three protocols which at the least achieve a level of security equal to their classical analog. In chapter 4, we have shown how it is possible to supress the effect of noise in QKD using error filtration. The plug and play technique was perfectly suited for error filtration as extending the dimension of time-bin encoded photons was simply done with the help of passive linear optical components. In chapter 6, we explored the level of randomness in bit-string generation that can be achieved. Based on strong conjectures, we have shown that our experiment not only produced randomness based only on the laws of physics but that this randomness was higher than what is achievable by classical protocols. In chapter 7, we implemented a secure identification protocol. Although this protocol does not seem to offer more advantages than its classical counterpart, it is nevertheless the first time that a quantum cryptographic protocol is implement which relies on a different no-go theorem.

The second part of the thesis dealt on various issues of cloning but relied on common methods in order to achieve the optimal maps. The Pauli cloning formalism we used in chapters 5, 8 and 9 all seem to yield the optimal supported by the semi-definite programming approach as a verification.

References

This thesis is partly based on the following papers.

[1] *Fiber-Optics Implementation of the Deutsch-Jozsa and Bernstein- Vazirani Quantum Algorithms with Three Qubits*,
E. Brainis *et al*
Physical Review Letters 90, 157902 (2003).

[2] *Cloning the entanglement of a pair of quantum bits*,
L.-P. Lamoureux *et al*
Physical Review A 69, 040301(R) (2004).

[3] *Experimental quantum key distribution over highly noisy channels*,
L.-P. Lamoureux *et al*
Physical Review Letters 94, 230501 (2005).

[4] *Provably secure experimental quantum bit-string generation*,
L.-P. Lamoureux *et al*
Physical Review Letters 94, 050503 (2005).

[5] *Asymmetric phase-covariant d-dimensional cloning*
L.-P. Lamoureux and Nicolas Cerf
Quantum Information and Communication Vol.5 No.1 (2005).

[6] *Reduced randomness in quantum cryptography with sequences of qubits encoded in the same basis*
L.-P. Lamoureux *et al*
Physical Review A 73, 032304 (2006).

[7] *Non-linear parametric processes in quantum information*
F. De Martini and F. Sciarrino
Progress in Quantum Electronics 29 (2005) pp. 165-256.

[8] *Quantum cryptography*
N. Gisin *et al*
Review of Modern Physics 74, 145 (2002)

[9] *Extremal equation for optimal completely positive maps*
J. Fiurasek
Physical Review A, 64, 062310 (2001).

[10] *Asymmetric quantum cloning machines*
N. Cerf
Acta Phys. Slovaca 48 (1998), pp. 115-132.

Bibliography

[Amb02] A. Ambainis (2002), pp. 134–142.

[BB84] C. Bennett and G. Brassard, in *Systems and Signal Processing*, edited by in Proceedings of the IEEE International (Conference on Computers, Bangalore, 1984), pp. 175–179.

[BBP+96] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[BCdM00] D. Bruss, M. Cinchetti, G. d'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).

[BCF+96] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[BDSW96] C. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[Ben92] C. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[BH98] V. Buzek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).

[BHW99] V. Buzek, M. Hillery, and R. Werner, Phys. Rev. A **60**, R2626 (1999).

[Blu81] M. Blum, Advances in Cryptology: A Report on CRYPTO 81 pp. 11–15 (1981).

[BM02] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).

[BM04a] J. Barrett and S. Massar, Phys. Rev. A **69**, 022322 (2004a).

[BM04b] J. Barrett and S. Massar, Phys. Rev. A **70**, 052310 (2004b).

[BP99] N. Bechmann-Pasquinucci, H.and Gisin, Phys. Rev. A **59**, 4238 (1999).

[BPG99] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[CAK98] N. J. Cerf, C. Adami, and P. Kwiat, Phys. Rev. A **57**, R1477 (1998).

[CBKG02] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[CDG02] N. J. Cerf, T. Durt, and N. Gisin, J. Mod. Opt. **49**, 1355 (2002).

[CDPC05] G. Chiribella, M. D'Ariano, P. Perinotti, and N. Cerf, Phys. Rev. A **72**, 042336 (2005).

[Cer98] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998).

[Cer00] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).

[CK78] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[Deu85] D. Deutsch (London, 1985), vol. 400, p. 97.

[Die82] D. Dieks, Phys. Lett. **92A**, 271 (1982).

[DJ92] D. Deutsch and R. Jozsa, in *Proc. R. Soc.* (Ser. A, London, 1992), vol. 439, p. 553.

[DLCZ01] L. Duan, M. Lukin, J. Cirac, and P. Zoller, Nature **414**, 413 (2001).

[dM03] G. M. d'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).

[DMSS04] F. De Martini, F. Sciarrino, and V. Secondi, Phys. Rev. A **70**, 040301 (R) (2004).

[dP01] G. d'Ariano and L. Presti, Phys. Rev. A **64**, 042308 (2001).

[Eke91] A. Ekert, Phys. Rev. Lett. **678**, 661 (1991).

[EPR35] A. Einstein, B. Podolsky, and N. Rose, Phys. Rev. **47**, 777 (1935).

[Fey82] R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[FIMW03] H. Fan, H. Imai, K. Matsumoto, and X.-B. Wang, Phys. Rev. A **67**, 022317 (2003).

[Fiu01] J. FiurÃ¡Å¡ek, Phys. Rev. A **64**, 062310 (2001).

[Fiu03] J. FiurÃ¡Å¡ek, Phys. Rev. A **67**, 052314 (2003).

[GHM+97] N. Gisin, B. Huttner, A. Muller, B. Perny, and H. Zbinden, Applied Physcics Letters **70**, 793 (1997).

[Gis98] N. Gisin, Phys. Lett. A **242**, 1 (1998).

[GLMP05] N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. A **72**, 012338 (2005).

[GM97] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[GRL+03] S. Gulde, M. Riebe, G. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. Chuang, and R. Blatt, Nature **421**, 48 (2003).

[Gro97] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[GRTZ02] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys **74**, 145 (2002).

[Her82] N. Herbert, Found. Phys. **12**, 1171 (1982).

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki, Physics Letters A **210(1-2)**, 1 (1996).

[HW97] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[JM98] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).

[Ken03] A. Kent, *Quantum Communication, Measurement and Computing* (Rinton Press, 2003).

[Lan61] R. Landauer, IBM J. Res. Dev. **5**, 183 (1961).

[LBA+05] L.-P. Lamoureux, E. Brainis, D. Amans, J. Barrett, and S. Massar, Phys. Rev. Lett. **94**, 050503 (2005).

[LBZ02] J. Lawrence, C. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).

[LC99] H.-K. Lo and H. Chau, Science **283**, 2050 (1999).

[May01] D. Mayers, Journal of the ACM **48**, 351 (2001).

[Mil16] R. Millikan, Phys. Rev. **7**, 355 (1916).

[Moo65] G. Moore, Electronics **38(8)**, 114 (1965).

[NC00] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[NC03] P. Navez and N. J. Cerf, Phys. Rev. A **68**, 032313 (2003).

[PGU+03] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature **423**, 417 (2003).

[PSBZ01] J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Nature **410**, 1067 (2001).

[qua] quant-ph/0303052.

[Rai01] E. M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).

[Rec94] M. e. a. Reck, Phys. Rev. Lett. **73**, 58 (1994).

[Sch06] E. Schmidt, Math Annalen **63**, 433 (1906).

[SFV+02] C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, Nature **419**, 594 (2002).

[Sha48] C. Shannon, Bell System Tech. J. **27**, 379 (1948).

[Sho95] P. Shor, Phys. Rev. A **52**, R2493 (1995).

[Sho97] P. Shor, SIAM J. Comput. **26**, 1484 (1997).

[SP00] P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[SR02a] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2002a).

[SR02b] R. W. Spekkens and T. Rudolph, Phys. Rev. Lett. **89**, 227901 (2002b).

[Tak00] S. Takeuchi, Phys. Rev. A **62**, 032301 (2000).

[Wer98] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).

[Wie83] S. Wiesner, SIGACT News **15**, 77 (1983).

[WZ82] W. K. Wootters and V. Zurek, Nature **299**, 802 (1982).