The Search for the Holy Grail in Quantum Cryptography

Louis Salvail[1]

BRICS, Basic Research in Computer Science of the Danish National Research Foundation, Department of Computer Science,University of Århus, Ny Munkegade, building 540,DK-8000 Århus C, Denmark.
salvail@daimi.aau.dk

Abstract. In 1982, Bennett and Brassard suggested a new way to provide privacy in long distance communications with security based on the correctness of the basic principles of quantum mechanics. The scheme allows two parties, Alice and Bob, sharing no secret information in the first place, to exchange messages that nobody else can figure out. The only requirement is a quantum channel and a normal phone line connecting the two parties. The fact that quantum mechanics provides unconditional secure communications is a remarkable result that cannot be achieved by classical techniques alone. Apart from secure communication, cryptography is also interested in tasks that aim at protecting one party against a potentially dishonest peer. This scenario, called secure two-party computation, is usually modelled by a function $f(x_A, x_B)$ where x_A and x_B are Alice's and Bob's secret input respectively. They would like to execute a protocol that produces $z = f(x_A, x_B)$ to both parties without disclosing their secret input to the other party. The only information about a secret input that can be leaked toward the other party is what the output z itself discloses about it. Unlike secure communication, secure two-party computation does not assume that Alice and Bob are honest. One honest party's input should remain secret whatever the other party's behaviour. It is well-known that in order to find a protocol for secure two-party computation, one must have access to a secure bit commitment scheme. Unfortunately, in 1996 Mayers showed that no secure quantum bit commitment scheme exists. Similarly to the classical case (where trapdoor one-way functions are needed) quantum cryptography does not provide secure two-party computation for free. In this paper, we discuss the possibilities and limits of quantum cryptography for two-party computation. We describe the essential distinctions between classical and quantum cryptography in this scenario.

1 Introduction

Quantum cryptography aims at designing cryptographic protocols with security guaranteed by the fundamental laws of quantum mechanics. In 1982, Bennett and Brassard [1] proposed two quantum protocols: Quantum key distribution (QKD), and quantum coin tossing. Quantum key distribution allows two parties, Alice and Bob, who share no information to agree on a common secret key

$\mathbf{k} \in \{0,1\}^l$ for some $l > 0$. Typically, once Alice and Bob share $\mathbf{k}$, Alice can encrypt any message $\mathbf{m} \in \{0,1\}^l$ as $\mathbf{c} = \mathbf{m} \oplus \mathbf{k}$. The ciphertext $\mathbf{c}$ is then sent to Bob over a normal channel that can be eavesdropped at will. It is well-known that this encryption method (called the one-time pad) does not leak information about $\mathbf{m}$ to an eavesdropper as long as $\mathbf{k}$ is unknown. This means that whenever a new message $\mathbf{m}$ has to be sent secretly, Alice and Bob first use QKD in order to get a fresh secret key $\mathbf{k}$ that is used for encrypting $\mathbf{m}$. The point here is that no classical method whatsoever can achieve this without relying upon some assumptions [42]. Classically, the security of secret-key exchange can be based upon a computing time limitation an attacker can spend in order to find the key [19]. However, it is very unlikely that one could prove that a secure classical cryptosystem would guarantee absolute security against eavesdroppers limited to spend only polynomial time. A proven security statement like this would imply that $\mathbf{P} \neq \mathbf{NP}$. On the other hand, if secret-key distribution is implemented quantumly then security can be achieved under the only assumption that the basic axioms of quantum mechanics are correct. This offers advantages compared to the classical cryptosystems since the notion of security is independent of the model of computation. This is important since it is possible that all practical public-key cryptosystems are secure against attackers modelled by Turing machines but not against attackers modelled by quantum Turing machines. As an example, RSA [39] and Diffie-Hellmann [19] cryptosystems are breakable by *quantum attackers* since the quantum computer can factorize and extract discrete logs in polynomial time [41].

The idea behind the Bennett-Brassard scheme for QKD [1, 2] is that, any eavesdropper trying to get information by intercepting the communication on the quantum channel will be detected. This is because unknown quantum states cannot be observed without disturbing the state irreversibly. The disturbance can be detected by Alice and Bob by exchanging information over the public channel. The scheme ensures them that if they don't find too many errors it is because no threatening eavesdropping occurred during the quantum transmission. The key they are going to agree on should therefore be secret. Several papers have been written about the security of the Bennett-Brassard scheme. In [2], the scheme was shown secure against an attacker performing the so called *intercept-resend* attack. Intercept-resend attacks are the ones where the attacker keeps the original particles and resends others according to the outcome of a complete test (complete tests will be defined in section 3.1). The security of the scheme was shown against much stronger but still limited attackers in [6]. Very recently, the proof of security has been extended to cover all possible cases sound with quantum mechanics axioms [35]. It follows that quantum mechanics allows to achieve one of the most important cryptographic task without any assumption. Moreover, experimental implementations have demonstrated that quantum cryptography is also practical [2, 37, 43, 24].

What about the other protocol introduced by Bennett and Brassard in 1982 [1]: Quantum coin tossing? A coin tossing protocol takes place between Alice and Bob and guarantees that a random bit $r \in \{0,1\}$ is generated [7]. Even when one party is dishonest the outcome of the coin toss is random. This means that no dishonest party can influence the outcome. Unlike the protocol for QKD, it was already known by the authors that the proposal could be broken by a dishonest party able to produce and manipulate *entangled quantum states.* Loosely speaking, an entangled quantum state is the state of several particles such that:

- Observing one part of the system produces a random outcome and
- once the outcome is known, the state or the rest of the system is also known.

In other words, the state of each particle is correlated with the others. These states are rather difficult to prepare and were out of reach back in 1982. Today however, the entanglement needed in order to break the scheme can easily be produced in laboratory. From the beginning, coin tossing already appeared more difficult to achieve than QKD whereas classically, coin tossing is easier than secret-key distribution [23].

The coin tossing protocol proposed by Bennett and Brassard was in fact implementing a more powerful primitive called *bit commitment.* A bit commitment scheme allows Alice to commit to the value of a bit in a way that prevents Bob to learn it but also in a way that prevents Alice from changing her mind. A coin tossing is easily achieved using a bit commitment scheme:

- Alice commits on a random $r_A \in \{0,1\}$,
- Bob announces a random $r_B \in \{0,1\}$,
- Alice unveils r_A,
- Alice and Bob set $r = r_A \oplus r_B$.

The advantage of considering bit commitment is that it allows to prove knowledge of a statement without divulging it [10, 20]. This kind of cryptographic task is important for solving natural cryptographic problems like identification, Zero-Knowledge proofs of Knowledge, etc... However there are tasks that even bit commitment cannot help to solve.

An *oblivious transfer* is a protocol that allows Alice to send Bob $x \in \{0,1\}$ in such a way that:

- Bob receives x with probability $\frac{1}{2}$ and knows it. When x is not received, Bob gets no information on x.
- Alice has no information on whether or not Bob received x.

Classically, it would be a major breakthrough if one could show that bit commitment and oblivious transfer can be based on the same computational assumptions [23]. Oblivious transfer seems strictly more powerful than bit commitment in the classical world. It allows to build bit commitment quite easily but the opposite will turn out to be true only if the existence of one-way functions implies the existence of trapdoor one-way functions. Coin tossing, bit commitment and oblivious transfer are all protocols involving two parties who want to cooperate while respecting their privacy. The most general task one can imagine in this model is the so called *secure two-party computation* (S2PC). A protocol for S2PC is a generic protocol between Alice and Bob taking as input the description of a function $f : \{0,1\}^N \times \{0,1\}^N \to \{0,1\}^M$ and secret strings $x_A, x_B \in \{0,1\}^N$ for Alice and Bob respectively. The output is the value $f(x_A, x_B)$ that is made available to both parties. The protocol is secure if

1. it computes the correct output and
2. it leaks, to each player, no more information than $f(x_A, x_B)$ about the input of the other party.

Although S2PC seems quite general, an oblivious transfer is sufficient in order for a secure protocol to exists [26, 18]. It follows that the most general primitive for solving any secure two-party computation is oblivious transfer.

From the above, it is natural to ask if oblivious transfer can be implemented quantumly. A positive answer would allow to base almost all modern cryptography upon the correctness of quantum mechanics, that is upon the laws of physics as we observe them. Oblivious transfer can therefore be seem as the Holy Grail of quantum cryptography.

1.1 Overview

Basically, quantum mechanics allows to transmit information in a way that is similar to a transmission through a binary symmetric channel. Quantum mechanics, by virtue of the uncertainty principle, allows to encode information in such a way that the receiver cannot decode it all the time. Measuring an arbitrary quantum state destroys it and does not extract all the information. Measurements are therefore not repeatable so the uncertainty about the measured state always remains. This inherent noisiness is at the basis of all quantum protocols including the one for secret-key distribution. Noisy channels, at least some of them, are powerful cryptographic primitives since they allow to build secure protocols for oblivious transfer [16]. In 1991, Bennett, Brassard, Crépeau and Skubiszewska proposed a quantum protocol for oblivious transfer [5]. Their protocol assume that Alice and Bob have access, as a black-box primitive, to a secure bit commitment scheme. Under this assumption, several results about the security of the scheme were shown [5, 15, 36, 46]. The result of Yao [46], showed that the scheme is secure according to the laws of quantum mechanics and given bit commitment as a black-box. The result showed that bit commitment is sufficient to build a quantum oblivious transfer whereas classically this seems impossible.

There were reasons to be optimistic in 1995; the Holy Grail was in sight. Not for long though! In 1995, Mayers [32] broke the most serious candidate for quantum bit commitment [12] (although at that time it was even not considered as a candidate but as a genuine bit commitment scheme). Then, things got worse. In 1996, Mayers [33] and independently Lo and Chau [27] have given a general attack that can be applied on general quantum protocols for bit commitment. Mayers' construction [33, 34] turns out to be so general that the existence of quantum bit commitment, with security relying merely upon the correctness of quantum mechanics, was ruled out. Quantum bit commitment as its classical counterpart, needs extra assumption in order to be implemented. However, the classical and quantum assumptions can be of very different and independent nature [40]. It is of interest to have different sets of independent and realistic assumptions under which bit commitment and, more generally, oblivious transfer are possible. This allows to choose the model (classical or quantum) that suited the best the requirements of a particular application.

This paper describe the main steps in the search for secure quantum oblivious transfer. We shall see how quantum mechanics principles help in implementing a flavour of noisy channel as a primitive. We describe how to use this primitive to implement oblivious transfer given a black-box for bit commitment. We then describe Mayers' attack that breaks any quantum bit commitment. The description of the attack is a good starting point for getting accustomed to the weirdness of quantum information. It exhibits highly non classical behaviour and more importantly, it suggests how to look at quantum protocols in order not to *over classicize* their behaviour. It has been demonstrated many times, that thinking classically about the security of a quantum protocol can lead to false conclusions.

1.2 Content

In section 2, we introduce the mathematical concepts that are used throughout the paper. In section 3, we define quantum states and measurements using the standard physical representation. In section 4 we describe the standard way to encode obliviously classical information in quantum states. In section 5, we show how to reduce quantum oblivious transfer to the oblivious quantum encoding given a bit commitment scheme. In section 6 we describe Mayers' attack against any quantum bit commitment scheme. We conclude in section 7.

2 Mathematical Background

Here, we introduce a suitable vector space for the representation of quantum objects. We then introduce the definitions and basic properties of linear operators relevant to our discussion. More complete information can be found in almost any book about the basic of linear algebra.

2.1 Vectors and Vector Spaces

In quantum mechanics, states, system evolutions and measurements are all represented by objects in a complex vector space. An appropriate vector space is called Hilbert space which is, for our purposes, not different from the complex vector space with the scalar or inner product defined. In the following we denote by α^* the complex conjugate of any number $\alpha \in \mathbb{C}$. Let $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} =$

$(v_1, \ldots, v_n) \in \mathcal{H}$ be two arbitrary vectors which belong in the same arbitrary Hilbert space $\mathcal{H}$. The inner product $\langle \mathbf{u}, \mathbf{v} \rangle \in \mathbb{C}$ between $\mathbf{u}$ and $\mathbf{v}$ is defined as

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i^* v_i.$$

From the inner product (or scalar product) we define the norm (or length) $\|\mathbf{v}\|$ of vector $\mathbf{v} \in \mathcal{H}$ by $\|\mathbf{v}\|^2 = \langle \mathbf{v}, \mathbf{v} \rangle \in \mathbb{R}$. Two vectors $\mathbf{v}$ and $\mathbf{w}$ are orthogonal if $\langle \mathbf{u}, \mathbf{v} \rangle = 0$. We say that a vector is *normalized* if its norm is 1. As usual, any vector $\mathbf{v} \in \mathcal{H}$ can be written as a linear combination of an infinite number of possible basis. In the following, $\mathcal{H}_n$ stands for the n-dimensional Hilbert space. A basis $\mathbf{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ for $\mathcal{H}_n$ is said to be *orthonormal* if for all $1 \leq i \neq j \leq n$, we have that $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0$ and $\|\mathbf{e}_i\| = 1$.

2.2 Dirac's Notation

A very popular notation for vectors and operators in an Hilbert space is the Dirac's notation. In Dirac's notation, vectors representing states are denoted by a *ket*. For any vector $\mathbf{v} = (v_1, \ldots, v_m) \in \mathcal{H}$, we write the state of a quantum attribute by $|\mathbf{v}\rangle$. One can see $|\mathbf{v}\rangle$ as the column vector:

$$|\mathbf{v}\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix}.$$

The *ket* notation allows to simplify expressions. In particular, it is often convenient to drop the description of vector $\mathbf{v}$ using only symbolic notations. One possible orthonormal basis for $\mathcal{H}_2$ is $+ = \{(1,0),(0,1)\}$. Basis $+$ is called the *standard* or *computational* or *rectilinear basis*. The orthonormal vectors for the standard basis are $+ = \{|\mathbf{0}\rangle, |\mathbf{1}\rangle\} = \{|\mathbf{0}\rangle_+, |\mathbf{1}\rangle_+\}$. Another important orthonormal basis in $\mathcal{H}_2$ is the *diagonal basis* $\times = \{(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}), (\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}) = \{|\mathbf{0}\rangle_\times, |\mathbf{1}\rangle_\times\}$.

Together with the *ket* comes the *bra* notation. If $\mathbf{v} = (v_1, \ldots, v_m) \in \mathcal{H}_m$ then the *bra* of $\mathbf{v}$ is noted $\langle \mathbf{v}|$ and is defined as $\langle \mathbf{v}| = (v_1^*, v_2^*, \ldots, v_m^*)$.

*Bra*s and *ket*s can be combined in order to denote operations. For $\mathbf{u} = (u_1, \ldots, u_m), \mathbf{v} = (v_1, \ldots, v_m) \in \mathcal{H}_m$ we have that $\langle \mathbf{v}|\mathbf{u}\rangle = \sum_{i=1}^{m} u_i^* v_i$ is the inner product between $\mathbf{u}$ and $\mathbf{v}$. Another operation sometime called the *dyadic* is denoted by $|\mathbf{u}\rangle\langle\mathbf{v}|$ and is such that

$$|\mathbf{u}\rangle\langle\mathbf{v}| = \begin{pmatrix} u_1 v_1^* & u_1 v_2^* & \ldots & u_1 v_m^* \\ u_2 v_1^* & u_2 v_2^* & \ldots & u_2 v_m^* \\ \vdots & \vdots & \vdots & \vdots \\ u_m v_1^* & u_m v_2^* & \ldots & u_m v_m^* \end{pmatrix}.$$

For any $\mathbf{v} \in \mathcal{H}_m$, $|\mathbf{v}\rangle\langle\mathbf{v}|$ is a matrix $V = \{v_{ij}\}_{1 \leq i,j \leq m}$ such that for all $i \neq j$ we have $v_{ij} = v_{ji}^*$ and $v_{ii} \in \mathbb{R}$. In the following and except when stated otherwise we shall use vectors with only real components. In this case, the *bra* and the *ket* of vector $\mathbf{v}$ have the same components, the first one being $\mathbf{v}$ as a row vector and the later being $\mathbf{v}$ as a column vector. The inner product between $\mathbf{u} = (u_1, \ldots, u_m) \in \mathbb{R}^m$ and $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{R}^m$ is simply $\sum_{i=1}^{m} u_i v_i$.

2.3 Unitary Evolution

We shall see in next section that vectors in a Hilbert space represent quantum states. The possible evolution of a quantum state can always be described by a *unitary transformation*. We say that a transformation in a m-dimensional Hilbert space is *unitary* if it can be written as a bijective mapping between two orthonormal bases. The following transformation is unitary and acts in a 2-dimensional Hilbert space:

$$\begin{aligned} H : |\mathbf{0}\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle) \\ |\mathbf{1}\rangle &\mapsto \tfrac{-1}{\sqrt{2}}(|\mathbf{0}\rangle - |\mathbf{1}\rangle) \end{aligned}$$

Any unitary transformation acting in a m-dimensional Hilbert space can easily be written as a $m \times m$ matrix. We only have to label each column and each row by one vector of the basis $\mathbf{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ we start with. The matrix entry labelled $(\mathbf{e}_i, \mathbf{e}_j)$ contains the complex number $\alpha_{i,j}$ that appears in front of vector $\mathbf{e}_j$ when the input state is $\mathbf{e}_i$. For example, the matrix form for H is:

$$H = \begin{array}{c|cc} & |\mathbf{0}\rangle & |\mathbf{1}\rangle \\ \hline |\mathbf{0}\rangle & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ |\mathbf{1}\rangle & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{array} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

In the following we will also use the *sign shift operator* S acting on vectors in $\mathcal{H}_2$ and defined as

$$\begin{aligned} S : |\mathbf{0}\rangle &\mapsto |\mathbf{0}\rangle \\ |\mathbf{1}\rangle &\mapsto -|\mathbf{1}\rangle \end{aligned}$$

For any vector $\mathbf{v} = (v_1, v_2) \in \mathcal{H}_2$, S applied on $\mathbf{v}$ produces the vector $\mathbf{v}' = (v_1, -v_2)$. The matrix representation of S is

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Any unitary transformation U has an inverse $U^{-1} = U^{\dagger}$ where $U^{\dagger}$ is the transposed conjugate of U (also called the Hermitian conjugate). One important property of unitary transforms is that they always preserved the inner product namely (i.e. for all $\mathbf{u}, \mathbf{v} \in \mathcal{H}$ we have that $\langle \mathbf{u} | \mathbf{v} \rangle = \langle U\mathbf{u} | U\mathbf{v} \rangle$).

Throughout this paper, we shall denote operators by capital letters. When we write $A \in \mathcal{H}$, we mean that A is an operator acting on vectors in $\mathcal{H}$.

2.4 Relevant Operators

A special case of operators, called Hermitians, will be useful in order to define what is a measurement of a quantum state. An operator $A \in \mathcal{H}_n$ is Hermitian if when A is expressed by $n \times n$ matrix $\{a_{ij}\}_{1 \leq i,j \leq n}$ we have that

1. for all $i \in \{1, \ldots, n\}$ the element $a_{ii} \in \mathbb{R}$. This means that all principal diagonal elements are real.
2. for all $i \neq j$, $a_{ij} = a^*_{ji}$.

An Hermitian operator A is always such that $A = A^\dagger$. When A contains only real elements, then A is Hermitian if and only if A is symmetric. Projections are special cases of Hermitian operators:

Definition 1. *An Hermitian operator P that satisfies $P = PP$ is called a* projection.

The condition $P = PP$ translates what we intuitively consider a projection, namely that a projection does not transform vectors that are parallel to the rays on which it projects. One can show that A is Hermitian in $\mathcal{H}_m$ if and only if it can be written for some $l \leq m$ as,

$$A = \sum_{i=1}^{l} a_i P_i \tag{1}$$

where the P_i's are projection operators projecting on mutually orthogonal rays. We say that $\mathbf{v}$ is an *eigenvector* with *eigenvalue* $a \in \mathbb{C}$ if A is such that $a\mathbf{v} = A\mathbf{v}$. The zero vector $\mathbf{0}$ is not an eigenvector but $a = 0$ is a possible eigenvalue. The set $E_A = \{a_i\}_{i=1}^{l}$ is the set of eigenvalues of A and the decomposition appearing in equation 1 is called the *spectral decomposition* of A. If $\#E_A = m$ then the spectral decomposition is unique and all projections are into orthogonal subspaces of dimension 1 (i.e. they project on rays). One can verify that all Hermitian operators have only real eigenvalues. The following projection operators are relevant to our discussion:

$$\mathbb{P}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \mathbb{P}_{\frac{\pi}{4}} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \mathbb{P}_{\frac{\pi}{2}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \mathbb{P}_{\frac{3\pi}{4}} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

In the above, projection $\mathbb{P}_\alpha$ for $\alpha \in \{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}\}$ is the projection on the ray (i.e. one dimensional subspace) at angle α with vector $(1, 0)$. The projection operator $P_{\mathbf{v}}$ on the ray parallel to the normalized vector $\mathbf{v} \in \mathcal{H}$ is $P_{\mathbf{v}} = |\mathbf{v}\rangle\langle\mathbf{v}|$. For instance, the above projections $\mathbb{P}_0 = |\mathbf{0}\rangle\langle\mathbf{0}|$, $\mathbb{P}_{\frac{\pi}{4}} = |\mathbf{0}\rangle_\times\langle\mathbf{0}|$, $\mathbb{P}_{\frac{\pi}{2}} = |\mathbf{1}\rangle\langle\mathbf{1}|$, and $\mathbb{P}_{\frac{3\pi}{4}} = |\mathbf{1}\rangle_\times\langle\mathbf{1}|$.

The *trace* $\mathrm{Tr}(A)$ of an operator $A \in \mathcal{H}$, is the sum of its principal diagonal elements. More formally, we write

$$\mathrm{Tr}(A) = \sum_{\mathbf{e} \in \mathbf{E}} \langle \mathbf{e} | A\mathbf{e} \rangle \tag{2}$$

for any basis $\mathbf{E}$ for $\mathcal{H}$. It is easy to verify that any projection P is such that $\mathrm{Tr}(P) = 1$. The trace has the following properties:

1. $\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$,
2. $\mathrm{Tr}(cA) = c\mathrm{Tr}(A)$ for $c \in \mathbb{C}$ and
3. $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

It follows from equation 1 that if A has eigenvalues E_A then

$$\mathrm{Tr}(A) = \sum_{a \in E_A} a\mathrm{Tr}(P_a) = \sum_{a \in E_A} a. \tag{3}$$

We shall see in section 3.4 that general quantum states are modelled by a special class of operators characterized by their traces:

Definition 2. *An operator D is a* density operator *if $Tr(D) = 1$.*

2.5 Space Extension

Two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ can be merged together in order to get a larger one $\mathcal{H}$ containing both of them. Let m_1 and m_2 the dimension of $\mathcal{H}_1$ and $\mathcal{H}_2$ and let $\mathbf{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_{m_1}\}$ and $\mathbf{F} = \{\mathbf{f}_1, \ldots, \mathbf{f}_{m_2}\}$ be orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. We define the *tensor product* operation "$\otimes$" that allows, given $\mathbf{E}$ and $\mathbf{F}$, to get a new orthonormal basis $\mathbf{H}$ for the $m_1 m_2$ dimensional Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. The tensor product is dyadic operation acting upon vectors. If vector $\mathbf{e} = (e_1, \ldots, e_{m_1})$ and $\mathbf{f} = (f_1, \ldots, f_{m_2})$ then we define:

$$\mathbf{e} \otimes \mathbf{f} = \begin{pmatrix} e_1 f_1 \\ e_1 f_2 \\ \vdots \\ e_1 f_{m_2} \\ e_2 f_1 \\ \vdots \\ e_{m_1} f_{m_2} \end{pmatrix}. \tag{4}$$

It is now possible to define $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ as the Hilbert space generated by the orthonormal basis $\mathbf{H} = \{\mathbf{e}_1 \otimes \mathbf{f}_1, \mathbf{e}_1 \otimes \mathbf{f}_2, \ldots, \mathbf{e}_{m_1} \otimes \mathbf{f}_{m_2}\}$. The tensor product operation can also be generalized in order to deal with operators as well. Assume A is an operator in the m_1 dimensional Hilbert space $\mathcal{H}_1$ and A' is an operator in the m_2 dimensional Hilbert space $\mathcal{H}_2$. Assume $A = \{a_{ij}\}_{1 \le i,j \le m_1}$ and $A' = \{a'_{ij}\}_{1 \le i,j \le m_2}$ are expressed as $m_1 \times m_1$ and $m_2 \times m_2$ squares matrices respectively. The composite operator $A \otimes A' \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as

$$A \otimes A' = \begin{pmatrix} a_{11}A' & a_{12}A' & \ldots & a_{1m_1}A' \\ a_{21}A' & a_{22}A' & \ldots & a_{2m_1}A' \\ \vdots & \vdots & \vdots & \vdots \\ a_{m_1 1}A' & a_{m_1 2}A' & \ldots & a_{m_1 m_1}A' \end{pmatrix}.$$

3 Quantum States

In quantum cryptography, classical information is encoded in the state of a quantum system. In this section, we describe what is meant by a quantum state. We shall define *pure states* as a special case of all quantum states. Complete measurements of quantum states are also discussed. Finally, we introduce the most general quantum states allowed by the theory: *quantum mixture*.

3.1 Maximal Tests

Before giving the definition of a quantum state, it is convenient to introduce *maximal quantum tests* [38]. Suppose you want to observe the property of a quantum system that can possibly take N different values. If the test you devise allows to distinguish between all N possibilities, we say that it is a *maximal quantum test*. A N-outcome measurement of this property implements a maximal quantum test. A test that gives only partial information about the measured property is said to be a *partial test*.

3.2 Pure States

If a quantum system is prepared in such a way that one can devise a maximal quantum test that yields with certainty a particular outcome then we say that the quantum system is in *pure state*. It follows that measuring several times a pure state yields always the same outcome [38].

In quantum mechanics, pure states are described by normalized vectors in some Hilbert space. If the maximal test for a pure state has n possible outcomes then the state is described by a vector $|\phi\rangle \in \mathcal{H}_n$. The polarization state of a photon is the usual way to encode information in quantum cryptography. Pure states for the polarization of a photon can be tested by a 2-outcome maximal test. It follows that the polarization state (i.e. here we drop the word *pure* adopting the convention that unless stated otherwise a state is pure) is described by a normalized vector in $\mathcal{H}_2$. As an example, $|\mathbf{0}\rangle, |\mathbf{1}\rangle, \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle) = H|\mathbf{0}\rangle$ and $\frac{1}{\sqrt{2}}(-|\mathbf{0}\rangle + |\mathbf{1}\rangle) = H|\mathbf{1}\rangle$ are all possible states for the polarization of a photon. The pure state $|\mathbf{0}\rangle_\times = \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle_+ + |\mathbf{1}\rangle_+)$ is said to be in *superposition* of pure states $|\mathbf{0}\rangle_+$ and $|\mathbf{1}\rangle_+$.

It is easy to verify that the tensor product operation $|\phi\rangle \otimes |\phi'\rangle$ for $\phi \in \mathcal{H}$ and $\phi' \in \mathcal{H}'$ preserves the purity of the two quantum states $|\phi\rangle$ and $|\phi'\rangle$. That means that whenever $|\phi\rangle \in \mathcal{H}$ and $|\phi'\rangle \in \mathcal{H}'$ are brought together then the new composite system remains in pure state. This must be the case since the maximal test in $\mathcal{H}$ for $|\phi\rangle$ followed by the maximal test in $\mathcal{H}'$ for $|\phi'\rangle$ defined one maximal test in $\mathcal{H} \otimes \mathcal{H}'$ for $|\phi\rangle \otimes |\phi'\rangle$.

The time evolution of a pure state (and also for mixture as defined in section 3.4) is always unitary and any unitary transformation is a possible evolution of a quantum state. Let $U \in \mathcal{H}_{2^l}$ be any unitary transformation acting on vectors in Hilbert space $\mathcal{H}_{2^l} = \bigotimes_{i=1}^{l} \mathcal{H}_2$. Let $\mathbf{E} = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{2^l}\}$ be a basis for $\mathcal{H}_{2^l}$ and let $|\phi\rangle \in \mathcal{H}_{2^l}$ be any pure state in $\mathcal{H}_{2^l}$. We have that

$$U|\phi\rangle = U \sum_{j=1}^{2^l} \alpha_j |\mathbf{e}_j\rangle = \sum_{j=1}^{2^l} \alpha_j U |\mathbf{e}_j\rangle$$

for $\alpha_j \in \mathbb{C}$ and $\sum_j |\alpha_j|^2 = 1$. This means that U is in fact applied simultaneously to each element appearing in the superposition $|\phi\rangle$. This kind of parallel computation is very important for speeding up classical algorithms using quantum phenomena. As we shall see in section 6, it has also important consequences in cryptography.

3.3 Complete Measurements

We have seen that pure states are quantum states for which there exists a maximal test giving a predictable outcome (thus repeatable). Measurements are implementations of the testing procedures. Quantum mechanics define complete measurements as measurements implementing a maximal test for some quantum states. Formally,

Definition 3. *A* complete *or* Von Neumann *measurement of a quantum state in $\mathcal{H}_n$ is described by an Hermitian operator $M \in \mathcal{H}_n$ with n distinct eigenvalues $E_M = \{a_1, \ldots, a_n\}$. Each eigenvalue $a \in E_M$ is a possible outcome for the measurement.*

From definition 3, the outcomes of a complete measurement M are in one to one correspondence with the set of orthogonal projections $\mathbf{P}_M$ appearing in M's spectral decomposition, since the decomposition is unique when all eigenvalues are distinct. Let $P_a \in \mathbf{P}_M$ be the projection associated with eigenvalue $a \in E_M$. It is always possible to write $P_a = |\psi_a\rangle\langle\psi_a|$ for a normalized vector $|\psi_a\rangle$ that is an eigenvector of M. Definition 3 does not describe the behaviour of complete measurements but just the way they are modelled. In order to understand what is a complete measurement, we have to specify what is the probability to observe the outcome corresponding to any eigenvalues in E_M and what happens to the system once the outcome has been observed. This is where quantum measurements and consequently quantum states differ from the classical ones. When a system Φ in quantum state $|\phi\rangle \in \mathcal{H}_n$ is measured by a complete measurement M, the following is always satisfied:

- The outcome corresponding to $a \in E_M$ is obtained with probability $p_\phi(a) = \langle\phi|P_a|\phi\rangle$.
- If $a \in E_M$ is the outcome then the state of Φ after the measurement is $|\psi_a\rangle$.

Any normalized vector $|\phi\rangle \in \mathcal{H}_n$ can be tested maximally by a complete measurement M having projection $P_a = |\phi\rangle\langle\phi|$ in its spectral decomposition. The outcome of M applied upon $|\phi\rangle$ is predictable since the eigenvalue a satisfies $p_\phi(a) = \langle\phi|P_a|\phi\rangle = \langle\phi|\phi\rangle\langle\phi|\phi\rangle = 1$. It is always possible to find such an M so that normalized vectors really describe pure states. Since projections and normalized vectors are in one to one correspondence, one can describe a pure state by a projection as well. It follows that a pure state $|\phi\rangle$ can always be written as the projection operator $P_\phi = |\phi\rangle\langle\phi|$. From definition 2 and equation 1 we have that any pure state P_ϕ is represented by a density operator but not all density operators represent pure states, as we shall see in next section.

We have seen that complete measurements in $\mathcal{H}_n$ are modelled by Hermitian operators $M \in \mathcal{H}_n$ having n distinct eigenvalues. The set of eigenvectors E_M for M defines a basis for $\mathcal{H}_n$. It follows that a complete measurement can also be described by a orthonormal basis $\mathbf{F}$ for $\mathcal{H}_n$ where each $\mathbf{v} \in \mathbf{F}$ is a possible outcome of M. Another equivalent way to specify a complete measurement is a set of the n orthogonal projections $\mathbf{P}_M$ in $\mathcal{H}_n$ appearing in M's spectral decomposition. Each projection $P \in \mathbf{P}_M$ is one of the possible orthogonal rays on which M projects the initial state. Using this representation of complete measurements, the following two complete measurements

$$\mathbb{M}_+ = \{\mathbb{P}_0, \mathbb{P}_{\frac{\pi}{2}}\} \text{ and } \mathbb{M}_\times = \{\mathbb{P}_{\frac{\pi}{4}}, \mathbb{P}_{\frac{3\pi}{4}}\}$$

will be used extensively in the following.

3.4 Mixed States

Suppose an observer is sitting next to a source of photons S. The dynamic of S is such that with probability $\frac{1}{2}$ a photon in state $|\mathbf{0}\rangle$ is sent and with probability $\frac{1}{2}$ a photon in state $|\mathbf{1}\rangle$ is sent. The behaviour of S can be described by a probability distribution $\mathcal{D}_S = \{(\frac{1}{2}, |\mathbf{0}\rangle), (\frac{1}{2}, |\mathbf{1}\rangle)\}$ over pure states in $\mathcal{H}_2$. Clearly, the next photon π that is going to be transmitted by S is not in pure state since no complete measurement can be defined such that the outcome will be predictable by the observer. To verify this, observe that if M represents a maximal test on $\mathcal{D}_S$ then we have that $p_{|\mathbf{0}\rangle}(a_0) = p_{|\mathbf{1}\rangle}(a_1) = 1$ where $a_0 \neq a_1$ are two eigenvalues of M. Let $p(a_0)$ and $p(a_1)$ be the probability to observe a_0 and a_1 respectively when the next photon transmitted by S is measured. We have that

$$p(a_0) = \frac{1}{2} p_{|\mathbf{0}\rangle}(a_0) = \frac{1}{2} p_{|\mathbf{1}\rangle}(a_1) = p(a_1) = \frac{1}{2}.$$

We conclude that no implementation of a maximal test is predictable when applied on the next particle produced by S. The quantum state transmitted by S is therefore not in pure state.

Definition 4. *A* quantum mixture *is a probability distribution over pure states in some Hilbert space $\mathcal{H}$. Moreover, any quantum state is a quantum mixture. In general we say that a quantum system is in a* mixed state *if it is not in pure state.*

Definition 4 does not say how a measurement behave when a mixed state is observed. Let $\mathcal{D} = \{(p_i, |\mathbf{s}_i\rangle)\}_{i=1}^{l}$ be an arbitrary quantum mixture in Hilbert space $\mathcal{H}$. We define the operator $\rho_{\mathcal{D}} \in \mathcal{H}$ as

$$\rho_{\mathcal{D}} = \sum_{i=1}^{l} p_i |\mathbf{s}_i\rangle\langle\mathbf{s}_i|. \tag{5}$$

By definition, $\rho_{\mathcal{D}}$ is a density operator since each $|\mathbf{s}_i\rangle\langle\mathbf{s}_i|$ has trace 1. Equation 5 reminds us of the spectral decomposition except for the pure states $|\mathbf{s}_i\rangle$'s that are not necessarily orthogonal. Since $\rho_{\mathcal{D}}$ is Hermitian, it is always possible to write

$$\rho_{\mathcal{D}} = \sum_{i=1}^{l} p_i |\mathbf{s}_i\rangle\langle\mathbf{s}_i| = \sum_{i=1}^{m} \tilde{p}_i P_i \tag{6}$$

where for all $i \neq j$, P_i and P_j are orthogonal and $\sum_{i=1}^{m} \tilde{p}_i = 1$. One consequence of equation 6 is that two different mixtures $\mathcal{D}$ and $\mathcal{D}'$ may share the same density matrix. Let $P_{\mathbf{s}_i} = |\mathbf{s}_i\rangle\langle\mathbf{s}_i|$ be the projection operator associated with the pure state $|\mathbf{s}_i\rangle$. We have that

$$\rho_{\mathcal{D}} = \sum_{i=1}^{l} p_i P_{\mathbf{s}_i} = \sum_{i=1}^{m} \tilde{p}_i P_i = \rho_{\mathcal{D}'}$$

where $\mathcal{D}' = \{(\tilde{p}_i, P_i)\}_{i=1}^{m}$. The physical interpretation is that several and different physical preparations can produce the same physical state.

If we return to our interpretation of a quantum mixture as a probability distribution over pure states, it becomes clear how behave a complete measurement on it. Each time an observer performs a measurement on a quantum mixture $\mathcal{D}$, the measurement is applied on a random pure state $|\phi\rangle \in \mathcal{H}$ picked according to $\mathcal{D}$. Let $\rho_{\mathcal{D}}$ be the density operator for mixture $\mathcal{D} = \{(p_i, |\mathbf{s}_i\rangle)\}_i$. Let $M = \sum_i a_i P_i \in \mathcal{H}$ be a complete measurement with outcomes (or eigenvalues) $E_M = \{a_i\}_i$ and such that all P_i's are orthogonal. The behaviour of M when applied upon $\mathcal{D}$ satisfies the following:

- The probability $p_{\mathcal{D}}(a)$ that the complete measurement M gives the outcome $a \in E_M$ is

  $$p_{\mathcal{D}}(a) = \sum_{(p,|\mathbf{s}\rangle)\in\mathcal{D}} p\langle\mathbf{s}|P_a|\mathbf{s}\rangle = \mathrm{Tr}(P_a \rho_{\mathcal{D}}) \tag{7}$$

  where P_a is the projection associated to the eigenvalue a in the spectral decomposition of M.
- After the outcome a has been observed,the state of the system becomes in pure state P_a.

Since the statistics of a measurement are completely specified by the density operator $\rho_{\mathcal{D}}$, it follows that two mixtures $\mathcal{D}$ and $\mathcal{D}'$ having the same density operator $\rho_{\mathcal{D}}$ behave the same when they are measured. We conclude that two mixtures sharing the same density operator are indistinguishable by any physical process.

As an example, consider the mixture $\mathcal{D}$ produces by the source S and the new mixture $\mathcal{D}' = \{(\frac{1}{4}, |\mathbf{0}\rangle), (\frac{1}{4}, |\mathbf{1}\rangle), (\frac{1}{4}, |\mathbf{0}\rangle_\times), (\frac{1}{4}, |\mathbf{1}\rangle_\times)\}$ produces by the source S'. One can verify that

$$\begin{aligned}
\rho_{\mathcal{D}'} &= \frac{1}{4}(|\mathbf{0}\rangle\langle\mathbf{0}| + |\mathbf{1}\rangle\langle\mathbf{1}| + |\mathbf{0}\rangle_\times\langle\mathbf{0}| + |\mathbf{1}\rangle_\times\langle\mathbf{1}|) \\
&= \frac{1}{4}\left(\begin{pmatrix} 1\,0 \\ 0\,0 \end{pmatrix} + \begin{pmatrix} 0\,0 \\ 0\,1 \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & \frac{-1}{2} \\ \frac{-1}{2} & \frac{1}{2} \end{pmatrix}\right) \\
&= \frac{1}{2}\begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix} \\
&= \frac{1}{2}\mathbb{1} = \rho_{\mathcal{D}}.
\end{aligned}$$

It follows that no physical process can distinguish between sources S and S'. These two preparation methods are equivalent.

In the following we sometime denote quantum systems in $\mathcal{H}_2$ by *qubits*. As we have seen, a qubit cannot store more than 1 classical bit of information since any complete test on it has only two possible outcomes. This explains the analogy between “qubits” and “bits”.

Henceforth, we shall write $\rho \in \mathcal{H}$, for a density operator ρ, if it acts on vectors in $\mathcal{H}$.

4 Oblivious Encoding of Information

In this section we shall see that the indistinguishability between quantum mixed states sharing the same density matrix leads to an encoding of classical information that cannot be recovered with 100% reliability by the receiver. This kind of encoding scheme is relevant to cryptography since it allows to perform non trivial cryptographic tasks. For instance consider the classical binary symmetric channel (BSC) that allows to send bits with error probability $0 < \epsilon < \frac{1}{2}$. The transmission of a classical bit through a BSC does not disclose all information to the receiver since the communication is noisy. The sender does not have all the information neither since (s)he does not know whether the receiver got the bit or its complement. Crépeau and Kilian [16] have shown that a BSC allows to build a secure oblivious transfer protocol and thus provides all the power needed for secure two-party computation. Noisy channels can also be used to implement secure secret-key distribution protocols as, for example, Wyner’s wire-tap channel [45] or Maurer’s secret-key agreement from common information [30]. This *oblivious* encoding of information is what we would like to achieve based on quantum mechanics. It would allow to see the quantum channel like a noisy channel thus providing the power needed for secure two-party computation.

4.1 The BB84 Coding Scheme

The BB84 coding scheme has been introduced by Bennett and Brassard [1] in order to achieve quantum secret-key distribution. As we shall see, the coding scheme can also be used in order to implement a wide variety of cryptographic tasks using the same quantum transmission procedure. The coding implements some kind of noisy transfer of a classical bit.

The idea behind the BB84 coding scheme is that classical bits 0 and 1 are encoded by non-orthogonal states and therefore cannot be distinguished perfectly by any measurement. For, we define the two following basis in $\mathcal{H}_2$:

- The *rectilinear basis* $+ = \{|\mathbf{0}\rangle_+, |\mathbf{1}\rangle_+\}$
- The *diagonal basis* $\times = \{|\mathbf{0}\rangle_\times, |\mathbf{1}\rangle_\times\}$.

Each vector in the rectilinear and diagonal basis will be the encoding of a classical bit. The following quantum transmission scheme is the main tool used in almost all quantum protocols. It is the standard quantum transmission between a sender $\mathcal{S}$ and a receiver $\mathcal{R}$:

`BB84 Quantum Transmission`

1. $\mathcal{S}$ picks a random $b \in_R \{0,1\}$ and a random $\theta \in_R \{+,\times\}$,
2. $\mathcal{R}$ picks a random $\widehat{\theta} \in_R \{+,\times\}$,
3. $\mathcal{S}$ sends a photon π in quantum state $|b\rangle_\theta$ through the quantum channel,
4. $\mathcal{R}$ measures π with the complete measurement $\mathbb{M}_{\widehat{\theta}}$ and records the outcome

$$\widehat{b} = \begin{cases} 0 \text{ if } |\mathbf{0}\rangle_{\widehat{\theta}} \text{ is observed,} \\ 1 \text{ if } |\mathbf{1}\rangle_{\widehat{\theta}} \text{ is observed.} \end{cases}$$

One BB84 quantum transmission produces a photon π with polarization in mixed state $\mathcal{D}_{BB84} = \{(\frac{1}{4}, |\mathbf{0}\rangle_+), (\frac{1}{4}, |\mathbf{1}\rangle_+), (\frac{1}{4}, |\mathbf{0}\rangle_\times), (\frac{1}{4}, |\mathbf{1}\rangle_\times)\}$. From equation 6, the mixture $\mathcal{D}_{BB84}$ is described by the density operator

$$\begin{aligned} \rho_{BB84} &= \frac{1}{4}\left(|\mathbf{0}\rangle_+\langle\mathbf{0}| + |\mathbf{1}\rangle_+\langle 1| + |\mathbf{0}\rangle_\times\langle\mathbf{0}| + |\mathbf{1}\rangle_\times\langle 1|\right) \\ &= \frac{1}{2}\mathbb{1}. \end{aligned}$$

On the receiving end, $\mathcal{R}$ measures π either with the complete measurement $\mathbb{M}_+$ or with $\mathbb{M}_\times$, each being chosen with probability $\frac{1}{2}$. For any $\widehat{\theta} \in \{+,\times\}$ the Hermitian operator $\mathbb{M}_{\widehat{\theta}}$ with eigenvalues $E_{\widehat{\theta}} = \{0,1\}$ can be written as

$$\mathbb{M}_+ = \mathbb{P}_0 = |\mathbf{0}\rangle_+\langle\mathbf{0}| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \mathbb{M}_\times = \mathbb{P}_{\frac{\pi}{4}} = |\mathbf{0}\rangle_\times\langle\mathbf{0}| = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Suppose $\mathcal{S}$ sends π in state $|\mathbf{0}\rangle$ (i.e. when $\mathcal{S}$ chooses $b=0$ and $\theta = +$) and $\mathcal{R}$ measures in basis $\widehat{\theta} = +$. The probability $p_+(0)$ that $\mathcal{R}$ gets the outcome 0 thus setting $\widehat{b} = 0 = b$ is

$$p_+(0) = \langle \mathbf{0} | \mathbb{P}_0 | \mathbf{0} \rangle = \langle \mathbf{0} | \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} | \mathbf{0} \rangle = \langle \mathbf{0} | \mathbf{0} \rangle = 1. \tag{8}$$

If $\mathcal{R}$ would have chosen measurement $\mathbb{M}_\times$ instead then the probability $p_\times(0)$ for $\mathcal{R}$ to decode correctly would be

$$p_\times(0) = \langle \mathbf{0} | \mathbb{P}_{\frac{\pi}{4}} | \mathbf{0} \rangle = \langle \mathbf{0} | \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} | \mathbf{0} \rangle = \langle \mathbf{0} | (\frac{1}{2}, \frac{1}{2}) \rangle = \frac{1}{2}. \tag{9}$$

Equations 8 and 9 show the property of *obliviousness* of the BB84 quantum transmission. If $\mathcal{R}$ chooses $\widehat{\theta} = \theta$ then the decoded bit $\widehat{b} = b$ with probability 1. However, if $\mathcal{R}$ chooses $\widehat{\theta} \neq \theta$ then the decoded bit $\widehat{b}$ is completely random. The BB84 coding scheme is symmetric and behaves the same way if the basis θ is $\times$ instead of $+$ and if the bit $b = 1$ instead of 0. It follows that the probability p_s that $\widehat{b} = b$ is

$$p_s = \mathrm{P}\left(\widehat{\theta} = \theta\right) + \frac{1}{2}\mathrm{P}\left(\widehat{\theta} \neq \theta\right) = \frac{3}{4}. \tag{10}$$

From equation 10 we conclude that if $\mathcal{S}$ and $\mathcal{R}$ follow the protocol honestly then the BB84 quantum transmission implements a BSC with error probability $\frac{1}{4}$.

4.2 BB84 is Oblivious

We now look at what happens when one party involved in a BB84 quantum transmission does not behave according the rules. We shall see what advantage a dishonest receiver $\mathcal{R}^*$ gets by choosing complete measurements different from $\mathbb{M}_+$ and $\mathbb{M}_\times$.

The goal for $\mathcal{R}^*$ is to figure out the bit b with better probability than $\frac{3}{4}$. In other words, $\mathcal{R}^*$ is looking for a complete measurement that allows to distinguish between $\mathcal{D}_0 = \{(\frac{1}{2}, |\mathbf{0}\rangle_+), (\frac{1}{2}, |\mathbf{0}\rangle_\times)\}$ and $\mathcal{D}_1 = \{(\frac{1}{2}, |\mathbf{1}\rangle_+), (\frac{1}{2}, |\mathbf{1}\rangle_\times)\}$ more accurately than measurements $\mathbb{M}_+$ and $\mathbb{M}_\times$. Let ρ_0 and ρ_1 be the density operators for $\mathcal{D}_0$ and $\mathcal{D}_1$ respectively. We have that

$$\rho_0 = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} \text{ and } \rho_1 = \begin{pmatrix} \frac{1}{4} & \frac{-1}{4} \\ \frac{-1}{4} & \frac{3}{4} \end{pmatrix} \tag{11}$$

Using equation 7, one can verify that

$$p_s = \mathrm{P}\left(\widehat{b} \neq b\right) = \frac{1}{4}\left(\mathrm{Tr}(\mathbb{P}_0\rho_0) + \mathrm{Tr}(\mathbb{P}_{\frac{\pi}{4}}\rho_0) + \mathrm{Tr}(\mathbb{P}_{\frac{\pi}{2}}\rho_1) + \mathrm{Tr}(\mathbb{P}_{\frac{3\pi}{4}}\rho_1)\right) = \frac{3}{4}.$$

Let $M_{\mathrm{B}} = \{\mathbb{P}_{\frac{\pi}{8}}, \mathbb{P}_{\frac{5\pi}{8}}\}$ be the complete measurement with possible outcomes $\mathbb{P}_{\frac{\pi}{8}} = |\mathbf{b_0}\rangle\langle\mathbf{b_0}|$ and $\mathbb{P}_{\frac{5\pi}{8}} = \mathbb{1}_2 - \mathbb{P}_{\frac{\pi}{8}} = |\mathbf{b_1}\rangle\langle\mathbf{b_1}|$ where $\mathbf{b_0} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8})$ and $\mathbf{b_1} =$

$(-\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$. Assume $\mathcal{R}^*$ measures π with $M_{\mathtt{B}}$ and let $\tilde{p}_s(b)$ be the probability to get $\widehat{b} = b$ when ρ_b is sent. We have that

$$\tilde{p}_s(0) = \mathrm{Tr}(\mathbb{P}_{\frac{\pi}{8}}\rho_0) = \cos^2\frac{\pi}{8} \tag{12}$$

$$\tilde{p}_s(1) = \mathrm{Tr}(\mathbb{P}_{\frac{5\pi}{8}}\rho_1) = \cos^2\frac{\pi}{8}. \tag{13}$$

Equations 12 and 13 show that if $\mathcal{R}^*$ wants to maximize its information about b, he has advantage to apply measurement $M_{\mathtt{B}}$ on π. In this case, the probability to decode b correctly is about 85% instead of $\frac{3}{4}$ when $\mathbb{M}_+$ or $\mathbb{M}_\times$ is applied. We can show that $M_{\mathtt{B}}$ is in fact the measurement that maximizes the probability to decode b correctly. The spectral decomposition of density operators ρ_0 and ρ_1 is,

$$\rho_0 = \cos^2\frac{\pi}{8}|\mathbf{b_0}\rangle\langle\mathbf{b_0}| + \sin^2\frac{\pi}{8}|\mathbf{b_1}\rangle\langle\mathbf{b_1}| \text{ and } \rho_1 = \sin^2\frac{\pi}{8}|\mathbf{b_0}\rangle\langle\mathbf{b_0}| + \cos^2\frac{\pi}{8}|\mathbf{b_1}\rangle\langle\mathbf{b_1}|.$$

This means that $\mathcal{D}_0 = \{(\cos^2\frac{\pi}{8}, |\mathbf{b_0}\rangle), (\sin^2\frac{\pi}{8}, |\mathbf{b_1}\rangle)\}$ and $\mathcal{D}_1 = \{(\sin^2\frac{\pi}{8}, |\mathbf{b_0}\rangle), (\cos^2\frac{\pi}{8}, |\mathbf{b_1}\rangle)\}$. Therefore, sending b using the BB84 coding scheme behaves like if it was sent through a BSC with error probability $\sin^2\frac{\pi}{8}$ whatever measurement $\mathcal{R}$ performs. It follows that the quantum state ρ_b for any $b \in \{0,1\}$ does not carry more information than $\mathbf{H}(\cos^2\frac{\pi}{8}, \sin^2\frac{\pi}{8})$ about b. The BB84 coding scheme is therefore inherently oblivious.

The BB84 coding scheme hides completely $\mathcal{S}$'s basis $\theta \in \{+, \times\}$. To see this, consider the mixed state $\mathcal{D}_\theta$ corresponding to a photon π polarized in basis θ. We have that $\mathcal{D}_\theta = \{(\frac{1}{2}, |\mathbf{0}\rangle_\theta), (\frac{1}{2}, |\mathbf{1}\rangle_\theta)\}$. Let ρ_+ and $\rho_\times$ be the density operators corresponding to $\mathcal{D}_+$ and $\mathcal{D}_\times$ respectively. One can easily verify that,

$$\begin{aligned}\rho_+ &= \frac{1}{2}(|\mathbf{0}\rangle_+\langle\mathbf{0}| + |\mathbf{1}\rangle_+\langle\mathbf{1}|)\\ &= \frac{1}{2}(|\mathbf{0}\rangle_\times\langle\mathbf{0}| + |\mathbf{1}\rangle_\times\langle\mathbf{1}|)\\ &= \rho_\times.\end{aligned}$$

This implies that, given a BB84 photon π, it is impossible to figure out what basis θ has been used by $\mathcal{S}$. This holds for any quantum measurement $\mathcal{R}$ could perform on π. The basis θ is perfectly concealed by the BB84 coding scheme.

4.3 BB84 as a Quantum Primitive

The BB84 coding scheme is the quantum ingredient of most quantum protocols [1, 2, 12, 17]. The difference between all these protocols is the classical communication taking place after the quantum transmission. The BB84 coding scheme is a kind of *universal* cryptographic primitive. Typically, a quantum protocol requires many BB84 transmissions upon which the classical part of the protocol is based. The parties involved in the classical part communicate only via the public channel. The classical phase is very often the only task dependent part of a quantum protocol.

In the following, we write $\langle(b,\theta),(\widehat{b},\widehat{\theta})\rangle \leftarrow \text{BB84}_N$ to denote N independent BB84 quantum transmissions of photons $\pi_1,\pi_2,\ldots,\pi_N$. $\mathcal{S}$'s random bits are $b = b_1,b_2,\ldots,b_N$ and the N choices for the polarization bases are $\theta = \theta_1,\theta_2,\ldots,\theta_N \in \{+,\times\}^N$. The N particles $\pi_1,\pi_2,\ldots,\pi_N$ that are sent through the quantum channel are therefore in composite state $|b_1\rangle_{\theta_1} \otimes |b_2\rangle_{\theta_2} \otimes \ldots \otimes |b_N\rangle_{\theta_N} \in \mathcal{H}_{2^N}$. On each received particle π_i, $\mathcal{R}$ performs the measurement $\mathbb{M}_{\widehat{\theta}_i}$ for $\widehat{\theta}_i \in \{+,\times\}$ providing the outcome $\widehat{b}_i$.

5 From BB84 to Quantum Oblivious Transfer

The BB84 coding scheme shows similarities with the description of an oblivious transfer. In BB84, the receiver gets the bit b with probability $\frac{1}{2}$ (i.e. when $\widehat{\theta} = \theta$). The only difference between a BB84 transmission and an oblivious transfer is that in the BB84 case, $\mathcal{R}$ does not know if he receives the bit or not.

One way to tell $\mathcal{R}$ whether or not he gets b, would be for $\mathcal{S}$ to announce the basis θ used to transmit b. If the receiver finds out that $\widehat{\theta} = \theta$ then $\widehat{b} = b$. Otherwise, the bit received $\widehat{b}$ is not correlated with the bit sent. However, this method allows $\mathcal{R}$ to cheat and receive $\widehat{b} = b$ all the time! $\mathcal{R}$ just stores the photon he receives and waits (without disturbing it) for $\mathcal{S}$ to announce θ. Once $\mathcal{R}$ knows θ, he measures the photon with measurement $\mathbb{M}_\theta$ thus recovering b perfectly. One way to overcome this problem would be to require $\mathcal{R}$ to commit on $\widehat{\theta}$ and $\widehat{b}$ before $\mathcal{S}$ announces θ. With probability $\kappa > 0$, $\mathcal{S}$ asks $\mathcal{R}$ to open the commitment. $\mathcal{S}$ then verifies that whenever $\widehat{\theta} = \theta$ $\mathcal{R}$ obtained the outcome $\widehat{b} = b$. If it is not the case then $\mathcal{S}$ stops the execution. With probability $1-\kappa$, $\mathcal{S}$ announces θ allowing $\mathcal{R}$ to find out if he receives b. We have made a step forward but the method does not implement an oblivious transfer yet. $\mathcal{R}$ has still a probability $1-\kappa$ not to be asked to open the commitment. This allows him to take a chance and to commit on random values allowing him not to measure the received particle. The probability of not being caught remains better than $1-\kappa$ (i.e. in fact the probability of being caught is $\frac{\kappa}{4}$).

The above construction is the idea behind the quantum oblivious transfer protocol of Bennett, Brassard, Crépeau and Skuwbiszewska [5] called the BBCS protocol. Below, we present a slight modification of the BBCS protocol allowing Alice to send to Bob the bit x by oblivious transfer. N BB84 transmissions are performed out of which about one half have been received perfectly. One subset S_c, for $c \in \{0,1\}$, contains the positions i such that $\theta_i = \widehat{\theta}_i$ whilst the set S_{1-c} contains the positions i such that $\widehat{\theta}_i \neq \theta_i$. The two sets S_0 and S_1 are announced to Alice without telling her the bit c. Alice encodes the bit x she wants to transmit by OT using the bits in positions in S_q for a random $q \in \{0,1\}$. The encoding allows Bob to recover x if and only if $q = c$ which happens with probability exactly $\frac{1}{2}$. The protocol needs a bit commitment scheme in order to be implemented securely. Let us assume that $\texttt{BC}(w)$, for $w \in \{0,1\}$, is a secure commitment of bit w.

`BBCS QOT Scheme`(x)

1. Alice and Bob execute $\langle(b,\theta),(\widehat{b},\widehat{\theta})\rangle \leftarrow \mathrm{BB84}_N$ where Alice is $\mathcal{S}$ and Bob is $\mathcal{R}$,
2. Bob sends to Alice the commitments $\{(\mathtt{BC}(\widehat{b}_i),\mathtt{BC}(\widehat{\theta}_i))\}_{i=1}^N$,
3. Alice selects a random subset of positions $I \subset \{1,\ldots,N\}$ that she announces to Bob,
4. Bob opens $\{(\mathtt{BC}(\widehat{b}_i),\mathtt{BC}(\widehat{\theta}_i))\}_{i\in I}$ allowing Alice to verify that for all $i \in I$ such that $\widehat{\theta}_i = \theta_i$ it is the case that $\widehat{b}_i = b_i$. If Alice finds errors she stops the execution else let $J = \{1,\ldots,N\} \setminus I$ be the set of untested positions,
5. Alice announces $\theta_J = \{\theta_i | i \in J\}$, Bob picks a random $c \in \{0,1\}$ and sets $S_c = \{i \in J | \theta_i = \widehat{\theta}_i\}$, $S_{1-c} = J \setminus S_c$,
6. Bob announces (S_0, S_1) to Alice (he keeps c secret),
7. Alice picks $q \in_R \{0,1\}$ and announces q together with $r = x \oplus \bigoplus_{i\in S_q} b_i$ to Bob,
8. If $q = c$ then Bob computes $x = r \oplus \bigoplus_{i\in S_c} \widehat{b}_i = r \oplus \bigoplus_{i\in S_c} b_i$ else Bob does not receive x.

The security of the scheme is based upon the inability for Bob to decode reliably the b_i's for all transmissions. Intuitively, the commitments ensure Alice that Bob measured completely the particles he received before she announces $\theta = \theta_1,\ldots,\theta_N$. Therefore, it should be the case that there exists a $z \in \{0,1\}$ such that the subset of positions S_z satisfies

$$|\mathrm{P}\left(\bigoplus_{i\in S_z} b_i = \bigoplus_{i\in S_z} \widehat{b}_i\right) - \frac{1}{2}| \leq 2^{-\alpha N}$$

for some $\alpha > 0$. If Bob follows the protocol then for each photon π_i we have that $\widehat{\theta}_i \neq \theta_i$ with probability $\frac{1}{2}$. We have seen that in this case, $\mathrm{P}\left(\widehat{b}_i = b_i | \widehat{\theta}_i \neq \theta_i\right) = \frac{1}{2}$. It follows that there exists $z \in \{0,1\}$ such that $\#\{i \in S_z | \widehat{\theta}_i \neq \theta_i\} \geq \frac{(1-\mu)\#S_z}{2}$ for any $\mu > 0$ as long as N is large enough. In that case, the bit $\bigoplus_{i\in S_z} b_i$ cannot be approximated by Bob. Since Alice encodes x in the XOR of all bits in S_q, for a random $q \in \{0,1\}$, with probability $\frac{1}{2}$ we have that $q = z$ and Bob is unable to obtain information about x.

5.1 Security and Generalized Measurements

In this section we quickly review what is known about the security of the BBCS protocol against dishonest parties that would take advantage of more elaborate quantum processes. Complete measurements as described in section 3.3, are not the only way an attacker can try to get extra information. Quantum mechanics allows generalized measurements to be performed. General measurements can extract information from a quantum state in such a way that the disturbance caused by the measurement process is minimized. In particular, if one is willing to get less information than what is achievable through a complete measurement, then a generalized measurement (also incomplete) of the the original quantum state can be done with no complete destruction of the initial state. One example of an incomplete measurement is the measurement that does nothing. This is formally written as the identity operator $\mathbb{1}$ which has only one eigenvalue $a = 1$ and therefore is not a complete measurement (of course!). In general, incomplete measurements are modelled by Hermitian operators with fewer distinct eigenvalues than the dimension of the Hilbert space in which they operate. They cannot give more information than complete measurements do but can nevertheless be completed later in order to get a complete measurement. For example, it is always possible to apply the useless measurement $\mathbb{1}$ on a quantum state $|\phi\rangle$ and later measures the untouched state $|\phi\rangle$ with a complete measurement. The result is simply the same as if $|\phi\rangle$ would have been measured completely the first time. Or is it? One can see that even the useless measurement $\mathbb{1}$ allows to break BBCS if no commitment was used. An incomplete measurement that gives information about the observed state $|\phi\rangle$ must destroy a part of the initial state. In general, more distinct eigenvalues your measurement has, more destructive it is (an example of a non-trivial incomplete measurement is given in section 6.4). Incomplete measurements can be useful to an attacker involved in a quantum protocol (as we have seen with BBCS using no commitment). The reason is that between the time the attacker performs the incomplete measurement and the time the measurement is completed, some extra information is obtained (i.e. the bases θ in the case of BBCS). With this extra information, the completion of the measurement can be chosen more cleverly than before whilst giving more information than if a complete measurement would have been chosen regardless of the extra information.

We can already verify that Alice has no way to learn whether or not the bit x has been received by Bob, as long as the commitments are concealing. This, because Bob chooses randomly how to measure each photon π_i and never gives information that would allow Alice to figure out what measurements were performed (if the commitments were not concealing Alice could easily find out!). Therefore, given S_0 and S_1, Alice has no information about $c \in \{0,1\}$ such that S_c contains the positions i where $\theta_i = \widehat{\theta}_i$. It follows that no matter what Alice tries, it is always the case that $\mathrm{P}\,(q = c) = \frac{1}{2}$. Only Bob could cheat the protocol by measuring photons $\pi_1, \ldots, \pi_N$ using measurements of its choice.

If we make the extra assumption that Bob only performs complete measurements then the security of the scheme can be shown. To see how, assume that Bob returns a commitment $\mathtt{BC}(\widehat{\theta}, \widehat{b})$ with the property that if $\theta = \widehat{\theta}$ then $\widehat{b} = b$ with probability 1. It follows that Bob's measurement is the complete measurement $\mathbb{M}_\theta$. Clearly, Bob cannot get b more than half the time even once he gets to know θ since after $\mathbb{M}_\theta$ has been performed, the state of the original photon is irreversibly destroyed. Another strategy for Bob would be to return a commitment that has a small but nonzero probability of being caught (i.e. $\widehat{\theta} = \theta$ but $\widehat{b} \neq b$) by applying complete measurements different than $\mathbb{M}_+$ and $\mathbb{M}_\times$. This strategy does not help Bob in increasing its chance to receive the bit x as shown in [15].

In [36], Bob was allowed to perform generalized measurements on single BB84 qubits. These measurements are strictly more powerful than complete measurements but were shown not to allow Bob to cheat the protocol neither. The final piece was provided by Yao [46] who showed that, given a perfectly secure bit commitment scheme, QOT is secure against any strategy allowed by quantum mechanics. The BBCS scheme can also be modified to deal with imperfect apparatus whilst remaining secure.

5.2 Classical vs Quantum Cryptography

Yao's proof of security for the BBCS scheme holds relative to the existence of a secure bit commitment scheme. It follows that the scheme described above does not provide security for free (as it is for quantum key distribution) but rather, reduce the security of QOT to the security of bit commitment. Nevertheless, we achieved something classical cryptography does not: secure oblivious transfer based on bit commitment. Classically, bit commitment can be built from any one-way function but oblivious transfer requires trapdoor one-way functions. It is very unlikely that one can find a proof that one-way functions and trapdoor one-way functions are in fact the same thing [23]. In the classical world, bit commitment is a weaker primitive than oblivious transfer. On the other hand, Yao's proof has shown that quantumly, oblivious transfer is reducible to bit commitment. It follows that oblivious transfer can be based on a weaker assumption in the quantum world (i.e. the existence of one-way functions) than in the classical world.

6 Quantum Bit Commitment

The next important question is whether or not QOT can be shown secure under the only assumption that quantum mechanics is correct. This would allow to base any secure two-party computation upon the same principles than quantum key distribution [31, 35, 6]. The first attempt to find a secure quantum bit commitment scheme is as old as the first protocol for quantum key distribution [1]. This first scheme was known to be insecure but it was believed that a secure one could be found. Several attempts were made in order to fix the original scheme [11, 12]. The last one was even claimed to be unbreakable [12]. Unfortunately, two years later Mayers found a subtle flaw in the last proposal [32]. Afterward, Mayers realized that the flaw he found was not only due to the particular broken protocol but could be applied to a large class of quantum protocol for bit commitment [33]. This has also been observed independently by Lo and Chau [27]. It is now known that no quantum bit commitment exists with security based only on the correctness of quantum mechanics axioms [33, 34].

In this section, we shall look at the general idea behind Mayers' proof and see why quantum mechanics completely forbids the existence of bit commitment. Apart from being used in the proof of [33], concepts introduce here are of independent interest. In particular, they show the striking difference between classical and quantum information. Quantum information will appear much more elusive than its classical counterpart.

6.1 Purification

In this section we shall discuss the main tool needed in order to prove Mayers' theorem. It is shown how a quantum mixture can be embedded in a pure state. This process is called *purification* of a mixed state.

We start by considering an example taken from the BB84 coding scheme. Let BB84(0) be the possible BB84 transmissions of classical bit $b = 0$:

`BB84`(0)

1. $\mathcal{S}$ picks a random $\theta \in_R \{+, \times\}$,
2. $\mathcal{S}$ sends a photon π in quantum state $|0\rangle_\theta$ through the quantum channel.

Clearly, the mixture associated with one transmission through BB84(0) is $\mathcal{D}_0 = \{(\frac{1}{2}, |0\rangle_+), (\frac{1}{2}, |0\rangle_\times)\}$ which has density operator ρ_0, as described in section 4.2. Now let us introduce a similar way to send one of the random state $|0\rangle_+$ and $|0\rangle_\times$ without requiring $\mathcal{S}$ to pick a random basis as in step 1 of BB84(0):

`BB84`*(0)

1. $\mathcal{S}$ prepares $|\Psi\rangle = \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle \otimes |0\rangle_+ + |\mathbf{1}\rangle \otimes |0\rangle_\times) \in \mathcal{H}_4$,
2. $\mathcal{S}$ keeps the first (the left one) particle and sends the other (the right one).
3. $\mathcal{S}$ measures in the standard basis "+" the particle he has kept. If the outcome is 0 then he sets $\theta = +$ otherwise he sets $\theta = \times$.

In BB84*(0), $\mathcal{S}$ never uses coin flips in order to determine which one of the two possible states $|0\rangle_+$ or $|0\rangle_\times$ is going to be sent. The coin is provided by adding an extra particle, called the auxiliary system (or ancilla), that is in superposition of the two possible outcomes of the coin toss. The auxiliary system is entangled with the particle that stores the qubit to be sent. When the the state of the auxiliary system is measured then the state of the qubit can be determined. Before the measurement, the states of the qubit and the auxiliary system were unknown. To see this, consider the standard complete measurement that $\mathcal{S}$ applies on $|\Psi\rangle$. The pure state $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\\frac{1}{2}\\\frac{1}{2}\end{pmatrix}\right) = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{2}\\\frac{1}{2}\end{pmatrix}.$$

When $\mathcal{S}$ executes $\mathbb{M}_+$, he will observe the outcome $\mathbb{P}_0$ (i.e. which is the projection on $|\mathbf{0}\rangle$) with probability

$$p(0) = \langle\Psi||(\mathbb{P}_0 \otimes \mathbb{1}_2)\Psi\rangle = \langle\Psi| \begin{pmatrix}1\ 0\\0\ 0\end{pmatrix} \otimes \mathbb{1}_2|\Psi\rangle = \frac{1}{2}.$$

This means that with probability $\frac{1}{2}$, $\mathcal{S}$ observes 0 and $|\Psi\rangle$ is projected in the state

$$|\Psi_0\rangle = |\mathbf{0}\rangle \otimes |0\rangle_+. \tag{14}$$

With probability also $p(1) = 1 - p(0) = \frac{1}{2}$, the standard measurement produces the outcome 1 that projects the original state $|\Psi\rangle$ into $|\Psi_1\rangle$ defined as

$$|\Psi_1\rangle = |\mathbf{1}\rangle \otimes |0\rangle_\times. \tag{15}$$

Equations 14 and 15 imply that the receiver $\mathcal{R}$ is going to receive $|0\rangle_+$ with probability $p(0) = \frac{1}{2}$ and $|0\rangle_\times$ with probability $p(1) = \frac{1}{2}$. On $\mathcal{R}$'s point of view, the mixed state he receives is $\mathcal{D}_0$ as it is for BB84(0). Since the density operators of BB84(0) and BB84*(0) are the same, $\mathcal{R}$ has no way to tell what preparation $\mathcal{S}$ is using to send the qubit.

Now, consider the mixed state $\mathcal{D}_\mathtt{B} = \{(\cos^2\frac{\pi}{8}, |\mathbf{b_0}\rangle), (\sin^2\frac{\pi}{8}, |\mathbf{b_1}\rangle)\}$, and its purification

$$|\Psi_\mathtt{B}\rangle = \cos\frac{\pi}{8}|\mathbf{0}\rangle \otimes |\mathbf{b_0}\rangle + \sin\frac{\pi}{8}|\mathbf{1}\rangle \otimes |\mathbf{b_1}\rangle.$$

If the leftmost particle is measured with the standard measurement $\mathbb{M}_+$ then with probability $p_\mathtt{B}(0) = \cos^2\frac{\pi}{8}$ the outcome 0 will be observed. We see that $p_\mathtt{B}(0)$ and $p(0)$ (defined above) are not the same but, as we have seen in section 4.2, $\mathcal{D}_\mathtt{B}$ and $\mathcal{D}_0$ share the same density operator ρ_0. The two purifications $|\Psi\rangle$ and $|\Psi_\mathtt{B}\rangle$ are therefore two different purifications for the same mixed state.

It is always possible to replace a probabilistic procedure as BB84(0) by an equivalent one where no coin toss is necessary. Consider an arbitrary mixture $\mathcal{D} = \{(p_i, |\mathbf{s_i}\rangle)\}_{i=1}^{l}$ where each $|\mathbf{s_i}\rangle$ belongs to the Hilbert space $\mathcal{H}$. Let $\mathcal{H}_\mathtt{1}$ be an Hilbert space of dimension $\mathtt{1} = 2^{\lceil \lg_2 l \rceil}$. A system $\Psi_\mathcal{D} \in \mathcal{H}_\mathtt{1} \otimes \mathcal{H}$ in pure state

$$|\Psi_\mathcal{D}\rangle = \sum_{i=1}^{l} \sqrt{p_i}|\mathbf{i}\rangle \otimes |\mathbf{s_i}\rangle \tag{16}$$

is called a *purification* of $\mathcal{D}$. The auxiliary system (the leftmost register) is used to store indices of all possible coin toss outcomes. Let $w \in \{1, \ldots, l\}$ be written in binary as $\text{Binary}(w) = w_0, w_1, \ldots, w_\mathtt{1}$. A value for w is encoded in pure state $|\mathbf{w}\rangle = |\mathbf{w_0}\rangle \otimes |\mathbf{w_1}\rangle \otimes \ldots \otimes |\mathbf{w_1}\rangle \in \mathcal{H}_\mathtt{1}$. The state of equation 16 is guaranteed, when the leftmost particle is measured with $\mathbb{M}_+$, to give the outcome w with probability p_w in which case the rightmost particle is projected in state $|\mathbf{s_w}\rangle$. This is exactly the behaviour of mixed state $\mathcal{D}$ that is provided by the entanglement of an auxiliary system with the pure states in $\mathcal{D}$.

One strange thing about purifications is that it allows to perform operations upon the result of a coin toss without knowing the outcome of the coin toss. For instance, in BB84*(0) it is not necessary for $\mathcal{S}$ to measure the register he keeps. Not measuring it changes nothing to what $\mathcal{R}$ will receive, it is still the mixed state $\mathcal{D}_0$ that is sent. But if $\mathcal{S}$ does not measure the kept register then he does not know what state has actually been transmitted although he knows that it has been chosen according to $\mathcal{D}_0$. The only way of doing this classically would be to require the sender to forget what he had done.

6.2 Purifying a Coin Toss

The most simple case of purification is probably the coin toss. Suppose that one instruction in a quantum protocol requires to flip a biased coin $\mathtt{C}(p)$ as follows

$$\mathtt{C}(p) = \begin{cases} 1 \text{ with probability } p, \\ 0 \text{ with probability } 1-p. \end{cases}$$

Unlike classically, it is possible to store a coin toss in a quantum memory without forcing the outcome. This is straightforward to achieve by preparing a quantum register $\Psi_{\mathtt{C}(p)}$ in state

$$|\Psi_{\mathtt{C}(p)}\rangle = \sqrt{p}\,|\mathbf{1}\rangle + \sqrt{1-p}\,|\mathbf{0}\rangle.$$

By measuring $|\Psi_{\mathtt{C}(p)}\rangle$ with measurement $\mathbb{M}_{+}$ one gets the outcome $\mathbb{P}_0$ with probability $1-p$ and the outcome $\mathbb{P}_{\frac{\pi}{2}}$ with probability p. As long as the measurement is not performed, the register $|\Psi_{\mathtt{C}(p)}\rangle$ keeps both possibilities in superposition. The coin toss itself is a quantum object. Classically, a coins toss does not exist until the outcome is known.

Assume that a quantum register is in mixed state $\rho \in \mathcal{H}$ and V_0 and V_1 are two unitary transforms acting on states in $\mathcal{H}$. One application of quantum coin toss is the purification of the sequence of instructions:

1. Pick $r \in \{0,1\}$ such that $\mathrm{P}\,(r=1) = p$,
2. Apply V_r to ρ for some arbitrary density operator $\rho \in \mathcal{H}$.

Let us define an unitary transformation $V \in \mathcal{H}_2 \otimes \mathcal{H}$ acting on a one qubit register $\Psi_{\mathtt{C}(p)}$ in addition to the register in state ρ. Transformation V simply applies V_0 to ρ if register $|\Psi_{\mathtt{C}(p)}\rangle = |\mathbf{0}\rangle$ and applies V_1 to ρ if $|\Psi_{\mathtt{C}(p)}\rangle = |\mathbf{1}\rangle$. Let $\mathbf{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ be an orthonormal basis for $\mathcal{H}$. Transformation V is defined as

$$\begin{aligned} V : |\mathbf{0}\rangle \otimes |\mathbf{e}_1\rangle &\mapsto |\mathbf{0}\rangle \otimes V_0\,|\mathbf{e}_1\rangle \\ |\mathbf{0}\rangle \otimes |\mathbf{e}_2\rangle &\mapsto |\mathbf{0}\rangle \otimes V_0\,|\mathbf{e}_2\rangle \\ \vdots \qquad &\;\;\vdots\;\;\vdots \\ |\mathbf{0}\rangle \otimes |\mathbf{e}_m\rangle &\mapsto |\mathbf{0}\rangle \otimes V_0\,|\mathbf{e}_m\rangle \\ |\mathbf{1}\rangle \otimes |\mathbf{e}_1\rangle &\mapsto |\mathbf{1}\rangle \otimes V_1\,|\mathbf{e}_1\rangle \\ \vdots \qquad &\;\;\vdots\;\;\vdots \\ |\mathbf{1}\rangle \otimes |\mathbf{e}_m\rangle &\mapsto |\mathbf{1}\rangle \otimes V_1\,|\mathbf{e}_m\rangle. \end{aligned}$$

The fact that both V_0 and V_1 are unitary ensures that V is also unitary. Using a quantum coin toss and transformation V, one can purify the above instructions as follows:

1. Prepare a register in state $|\Psi_{\mathtt{C}(p)}\rangle$
2. Apply $V|\Psi_{\mathtt{C}(p)}\rangle \otimes \rho$.

It can easily be shown that both procedures generate the same mixture. Measuring the leftmost register allows to select the coin toss outcome and consequently which of V_0 or V_1 has been applied on the rightmost register.

In the above construction, the number of outcomes for the coin toss is irrelevant. Any coin toss distribution $D = \{(p_i, i)\}_i$ can be purified the same way.

6.3 Purifying a Measurement

The purification process is not only possible on $\mathcal{S}$'s side of the quantum channel. It can also be done on the receiving end. Typically, $\mathcal{R}$ is supposed to measure a particle π with some measurement M picked according to a distribution $D_M = \{(p_1, M_1), (p_2, M_2), \ldots, (p_l, M_l)\}$. A purification of such a process would allow to perform all possible measurements in superposition until $\mathcal{R}$ wants to know what measurement and what outcome he gets. When he does so, $\mathcal{R}$ gets the outcome of a measurement picked according distribution D_M.

Without loss of generality, let us assume that $D_M = \{(p_+, \mathbb{M}_+), (p_\times, \mathbb{M}_\times)\}$. The BB84 coding scheme corresponds to the special case $p_+ = p_\times = \frac{1}{2}$. Assume that a quantum register $\Psi_{\mathtt{C}(p_+)}$ in state $|\Psi_{\mathtt{C}(p_+)}\rangle \in \mathcal{H}_2$ contains a purification of the coin toss $\mathtt{C}(p_+)$ as described in the previous section. Let π be a qubit that $\mathcal{R}$ is supposed to measure according to D_M. We now define the unitary transformation $U_M \in \mathcal{H}_2 \otimes \mathcal{H}_2$ that perform the required purification:

$$
\begin{aligned}
U_M : \overbrace{|\mathbf{0}\rangle}^{\text{coin}} \otimes \overbrace{|\mathbf{0}\rangle}^{\pi} &\mapsto |\mathbf{0}\rangle \otimes |\mathbf{0}\rangle \\
|\mathbf{1}\rangle \otimes |\mathbf{0}\rangle &\mapsto \tfrac{1}{\sqrt{2}}|\mathbf{1}\rangle \otimes (|\mathbf{0}\rangle + |\mathbf{1}\rangle) \\
|\mathbf{0}\rangle \otimes |\mathbf{1}\rangle &\mapsto |\mathbf{0}\rangle \otimes |\mathbf{1}\rangle \\
|\mathbf{1}\rangle \otimes |\mathbf{1}\rangle &\mapsto \tfrac{1}{\sqrt{2}}|\mathbf{1}\rangle \otimes (|\mathbf{0}\rangle - |\mathbf{1}\rangle).
\end{aligned}
$$

The register containing the coin toss is the auxiliary system of the purification. Transformation U_M stores the measurement in the auxiliary system and stores the outcome in the system that encoded particle π initially. Let $|b\rangle_\theta$ be a BB84 qubit and let $|\Psi_{\mathtt{C}(p_+)}\rangle$ be the purification of an arbitrary coin toss. One can verify that

$$
\begin{aligned}
U_M(|\Psi_{\mathtt{C}(p_+)}\rangle \otimes |b\rangle_\theta) = \sqrt{p_+}|\mathbf{0}\rangle \otimes \left(\sqrt{p_+(0)}|\mathbf{0}\rangle \pm \sqrt{p_+(1)}|\mathbf{1}\rangle\right) \\
+\sqrt{p_\times}|\mathbf{1}\rangle \otimes \left(\sqrt{p_\times(0)}|\mathbf{0}\rangle \pm \sqrt{p_\times(1)}|\mathbf{1}\rangle\right)
\end{aligned}
$$

where $p_{\widehat{\theta}}(\widehat{b})$ is the probability of the outcome $\widehat{b}$ whenever the initial state is $|b\rangle_\theta$ and the measurement is $\mathbb{M}_{\widehat{\theta}}$. If the leftmost register is measured with $\mathbb{M}_+$ then the outcome $\mathbb{P}_0$ is obtained with probability p_+ and the rightmost register contains the possible outcomes of measurement $\mathbb{M}_+$ when applied to the BB84 state $|b\rangle_\theta$. Similarly, the outcome $\mathbb{P}_{\frac{\pi}{2}}$ is obtained with probability $p_\times$ and the rightmost register contains the possible outcomes of measurements $\mathbb{M}_\times$ when applied on $|b\rangle_\theta$. If measurement $\mathbb{M}_+$ is applied on the rightmost particle first, an outcome $\widehat{b}$ is obtained without the measurement being completely specified. The leftmost register is in superposition of all possible measurements that can produce outcome $\widehat{b}$ when the initial state is $|b\rangle_\theta$. Purifying a random measurement and measuring the rightmost register (the outcome register) allows to get the outcome of an unknown measurement!

Suppose $\mathcal{R}$ is asked to perform a measurement $M \in \{\mathbb{M}_+, \mathbb{M}_\times\}$ according to distribution D_M on the particle π. Let $|b\rangle_\theta \in \mathcal{H}_2$ be an unknown BB84 state for π that is received by $\mathcal{R}$ through the quantum channel. The following implements a purification of this procedure given a register containing the coin toss $|\Psi_{\mathtt{C}(p_\times)}\rangle$ for choosing according to D_M:

1. $\mathcal{R}$ applies $|\Psi_M\rangle = U_M |\Psi_{\mathtt{C}(p_\times)}\rangle \otimes |b\rangle_\theta$.

The state $|\Psi_M\rangle$ contains a superposition of both possible measurements. If at some point after the BB84 transmission, $\mathcal{R}$ must announce the outcome of a random measurement $\mathbb{M}_{\widehat{\theta}}$ for $\widehat{\theta} \in \{+, \times\}$ according to D_M, then the measurement $\mathbb{M}_+$ applied to the rightmost register gives a possible outcome. To fix the measurement M, $\mathcal{R}$ only measures with $\mathbb{M}_+$ the leftmost register. If $\mathbb{P}_0$ is obtained then the selected measurement was $M = \mathbb{M}_+$ otherwise $M = \mathbb{M}_\times$ was selected. Applying U_M to a coin toss $\mathtt{C}(\frac{1}{2})$ register and a BB84 particle π purifies $\mathcal{R}$'s part of the BB84 transmission. The same technique can be used for sets of any N possible measurements by using a N-outcome quantum coin toss.

The measurement $\mathbb{M}_+$ performed by $\mathcal{R}$ on the leftmost register does nothing to the leftmost register and is formally defined as $M = \mathbb{M}_+ \otimes \mathbb{1}_2$. It is an incomplete measurement since it has only 2 distinct eigenvalues but acts in $\mathcal{H}_4$.

6.4 From One Purification to Another

In this section we shall argue that two purifications of the same mixed state are in fact equivalent. By equivalent we mean that one can transform a purification to another purification of the same mixture by acting only on the auxiliary part of the purification. This is a result of Hughston, Jozsa and Wootters [22].

Let us consider the unitary transformation $U^* = SH$ (see section 2.3) acting in $\mathcal{H}_2$ when applied on the auxiliary part of $|\Psi\rangle$:

$$\begin{aligned}
(U^* \otimes \mathbb{1}_2)|\Psi\rangle &= (SH \otimes \mathbb{1}_2)\frac{1}{\sqrt{2}}(|\mathbf{0}\rangle \otimes |0\rangle_+ + |\mathbf{1}\rangle \otimes |0\rangle_\times) \\
&= \frac{1}{2}((|\mathbf{0}\rangle - |\mathbf{1}\rangle) \otimes |0\rangle_+ + (|\mathbf{0}\rangle + |\mathbf{1}\rangle) \otimes |0\rangle_\times) \\
&= \frac{1}{2}((|\mathbf{0}\rangle - |\mathbf{1}\rangle) \otimes (\cos\frac{\pi}{8}|\mathbf{b_0}\rangle - \sin\frac{\pi}{8}|\mathbf{b_1}\rangle) + \\
&\qquad (|\mathbf{0}\rangle + |\mathbf{1}\rangle) \otimes (\cos\frac{\pi}{8}|\mathbf{b_0}\rangle + \sin\frac{\pi}{8}|\mathbf{b_1}\rangle)) \\
&= \cos\frac{\pi}{8}|\mathbf{0}\rangle \otimes |\mathbf{b_0}\rangle + \sin\frac{\pi}{8}|\mathbf{1}\rangle \otimes |\mathbf{b_1}\rangle \\
&= |\Psi_{\mathtt{B}}\rangle.
\end{aligned}$$

Applying U^* on the auxiliary part of $|\Psi\rangle$ transforms purification $|\Psi\rangle$ into purification $|\Psi_{\mathtt{B}}\rangle$. This allows $\mathcal{S}$ to decide which preparation $\mathcal{D}_0$ or $\mathcal{D}_{\mathtt{B}}$ he wants to use even after the particle is gone! $\mathcal{S}$ just prepares the purification of $\mathcal{D}_0$ and sends to $\mathcal{R}$ the leftmost particle keeping the auxiliary system. If at some point $\mathcal{S}$ wants to change his mind and wants to prepare the photon already sent using preparation $\mathcal{D}_{\mathtt{B}}$ instead, then he just applies U^* upon the auxiliary part.

The above construction is not a coincidence. Any pair of purifications $|\Psi\rangle$ and $|\Psi'\rangle$ for the same density operator is always related by an unitary transformation acting only on the auxiliary part of the purifications [22]. Let $\Psi \in \mathcal{H}_m \otimes \mathcal{H}_n$ be a purification of the density operator $\rho \in \mathcal{H}_n$. The Schmidt decomposition [22, 38] allows to write $|\Psi\rangle$ as a sum of *bi-orthogonal* terms. This means that there exists $r \leq \min(m,n)$ (depending only on ρ) and two sets of orthonormal vectors $\mathbf{E} = \{\mathbf{e}_i\}_{i=1}^r$ and $\mathbf{F} = \{\mathbf{f}_i\}_{i=1}^r$ in $\mathcal{H}_m$ and $\mathcal{H}_n$ respectively, such that[1]

$$|\Psi\rangle = \sum_{i=1}^{r} \sqrt{\alpha_i} |\mathbf{e}_i\rangle \otimes |\mathbf{f}_i\rangle \tag{17}$$

where as usual $\sum_i |\alpha_i|^2 = 1$. In equation 17, the set $\{\alpha_i\}_{i=1}^r$ is the set of eigenvalues of $\rho \in \mathcal{H}_n$. Let $|\Psi'\rangle \in \mathcal{H}_m \otimes \mathcal{H}_n$ be another purification of density operator $\rho \in \mathcal{H}_n$. We make the assumption that the auxiliary system in Ψ' belongs to the same Hilbert space $\mathcal{H}_m$ than the auxiliary system for Ψ. This can be done without loss of generality by taking the larger Hilbert space whenever the auxiliary systems for Ψ and Ψ' are defined in different Hilbert spaces. From the Schmidt decomposition, there exists two sets of orthonormal vectors $\mathbf{E}' = \{\mathbf{e}'_i\}_{i=1}^r$ and $\mathbf{F}' = \{\mathbf{f}'_i\}_{i=1}^r$ such that

$$|\Psi'\rangle = \sum_{i=1}^{r} \sqrt{\alpha_i} |\mathbf{e}'_i\rangle \otimes |\mathbf{f}'_i\rangle. \tag{18}$$

Clearly, the unitary transformation $W \in \mathcal{H}_m$ defined for all $i \in \{1, \ldots, r\}$ as

$$W : |\mathbf{e}_i\rangle \mapsto |\mathbf{e}'_i\rangle$$

is such that

$$(W \otimes \mathbb{1}_n)|\Psi\rangle = |\Psi'\rangle$$

since the subsystem in $\mathcal{H}_n$ is the same mixed state ρ in both purifications. In this case, it can be shown that $\mathbf{F} = \mathbf{F}'$.

[1] More precisely, let $|\Psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ be an arbitrary pure state and let $\rho = |\Psi\rangle\langle\Psi|$ be the associated projection. Let $\rho_1 = \mathrm{Tr}_{\mathcal{H}_1}(\rho)$ and $\rho_2 = \mathrm{Tr}_{\mathcal{H}_2}(\rho)$ be the partial trace of ρ over $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. It is always the case that ρ_0 and ρ_1 share the same nonzero eigenvalues (with the same multiplicity) $\{\alpha_i\}_{i=1}^r$ for $r \leq \min(\mathrm{Dim}(\mathcal{H}_1), \mathrm{Dim}(\mathcal{H}_2))$. The Schmidt polar form of $|\Psi\rangle$ is described in equation 17 and is such that vectors in $\{\mathbf{e}_i\}_{i=1}^r$ and vectors in $\{\mathbf{f}_i\}_{i=1}^r$ are orthogonal. This is why we call this a decomposition as a sum of *bi-orthogonal* terms.

6.5 Purifying a Quantum Protocol

The main idea behind Mayers' proof is that purifications can be applied not only to the cases we have seen previously but to any sequence of instructions that might occur in a protocol. One party can, without having any chance of being caught, execute his part of the protocol at the quantum level, meaning that every action is purified.

Let us first review what set of instructions one party involved in a quantum protocol should be able to perform. The instructions should be enough to execute what we considered intuitively a quantum protocol (that is basically a pair of algorithms usually not quantum connected by a classical and a quantum channels). The algorithm of party $\mathcal{P}$ defines, at each step, a transition function from the actual view $\mathcal{V} \in \mathbb{V}$ to the new view $\mathcal{V}' \in \mathbb{V}$ for an arbitrary set of possible views $\mathbb{V}$. The view $\mathcal{V}$ can be seen as the memory a player needs in order to complete the execution of the protocol. The following describes what $\mathcal{P}$ should be able to execute at step $h > 0$ given the view $\mathcal{V}_{h-1}$ after step $h-1$ (i.e. $\mathcal{V}_0$ is the initial secret input if needed):

1. Picks a random bit r such that $\mathrm{P}(r = 1) = p$ and sets $\mathcal{V}_h = \mathcal{V}_{h-1} \cup \{(h, r)\}$,
2. Computes a function $f : \mathbb{V} \to \mathbb{V}$ and sets $\mathcal{V}_h = \mathcal{V}_{h-1} \cup \{(h, f(\mathcal{V}))\}$,
3. Announces, through the classical channel, the value $v \in \{0, 1\}$ of some memory register and sets $\mathcal{V}_h = \mathcal{V}_{h-1} \cup \{(h, v)\}$,
4. Sends a qubit in state depending on the view $\mathcal{V}$ through the quantum channel,
5. Stores in memory a classical bit received through the classical channel,
6. Measures a qubit received through the quantum channel using measurement M chosen according the view $\mathcal{V}$. The outcome O_M is added to the actual view $\mathcal{V}_h = \mathcal{V}_{h-1} \cup \{(h, O_M)\}$ (note that not measuring the received qubit is also covered by this case since it is equivalent to apply measurement $\mathbb{1}$).

Intuitively, if one party $\mathcal{P}$ can execute all these instructions then $\mathcal{P}$ can execute any quantum protocol. As we have seen in sections 6.1,6.2, and 6.3, most of the above instructions can be purified if they are considered isolated. The only missing piece is how to compose them in a such a way that the properties of purification remain. Suppose $\mathcal{P}$ has a quantum memory $\mathtt{QM} \in \mathcal{H}$ where $\mathcal{H}$ is large enough for storing all possible states in $\mathbb{V}$. Suppose that initially $\mathcal{P}$'s quantum memory $\mathtt{QM} \in \mathcal{H}$ is in state $|\mathtt{QM}_0\rangle$ where $\mathtt{QM}_0$ is state V_0 encoded in quantum registers. During the course of actions, $\mathtt{QM}$ will evolve to a quantum mixture since mixed states will be received through the quantum channel and entangled registers will be sent. We denote by $\rho_{\mathtt{QM}}(h)$ the mixed state of $\mathtt{QM}$ after step $h > 0$. $\mathcal{P}$ purifies each of the above instructions as follows:

1. $\mathcal{P}$ prepares a new quantum register in state $|\Psi_{\mathtt{C}(p)}\rangle$. The quantum memory is now in state $\rho_{\mathtt{QM}}(h) = \rho_{\mathtt{QM}}(h-1) \otimes |\Psi_{\mathtt{C}(p)}\rangle$.
2. Let $U_f \in \mathcal{H}$ be an unitary transformation implementing f. It might be the case that $\mathcal{P}$ has to append few quantum registers in some pure state $|\phi\rangle$ in order to satisfy the requirement that U_f is unitary. The new state of $\mathtt{QM}$ is $\rho_{\mathtt{QM}}(h) = U_f(\rho_{\mathtt{QM}}(h-1) \otimes |\phi\rangle)$.

3. $\mathcal{P}$ applies the standard measurement $\mathbb{M}_+$ on the quantum register $R_{\mathbf{v}}$ containing $\mathbf{v}$. He announces 0 if the outcome is $\mathbb{P}_0$ and announces 1 if the outcome is $\mathbb{P}_{\frac{\pi}{2}}$. The new state $\rho_{\mathtt{QM}}(h)$ for QM can be computed in terms of $\rho_{\mathtt{QM}}(h-1)$ as described in equation 7.
4. $\mathcal{P}$ simply sends away the quantum register containing the qubit to be sent. This operation mixes the state of QM. The new state $\rho_{\mathtt{QM}}(h)$ is $\rho_{\mathtt{QM}}(h-1)$ without register $R_{\mathbf{v}}$ (formally speaking $\rho_{\mathtt{QM}}(h)$ is the partial trace of $\rho_{\mathtt{QM}}(h-1)$ with respect to register $R_{\mathbf{v}}$). The state of the qubit can be determined by a sequence of coin tosses previously generated and other quantum registers. The purification is performed by an easy generalization of the method described in section 6.1.
5. $\mathcal{P}$ adds a new register in state $|b\rangle$ to QM where $b \in \{0,1\}$ is the bit received through the classical channel. The new state is $\rho_{\mathtt{QM}}(h) = \rho_{\mathtt{QM}}(h-1) \otimes |b\rangle$.
6. In this case, $\mathcal{P}$ does not store the outcome but all possible outcomes of all possible measurements as we have seen in section 6.3. It is always possible to determine an unitary transformation U_M which applies each measurement specified by the state of some registers in QM. This is because the set of registers involved in the choice of the measurement behaves like a set of quantum coin tosses.

Suppose a protocol performed between $\mathcal{P}$ and $\mathcal{P}'$ has the property that the final view of $\mathcal{P}'$ corresponds to the mixed state $\rho' \in \mathcal{H}$. If $\mathcal{P}$ purifies each step then the state of the system Ψ that contains $\mathcal{P}$'s quantum memory QM plus all what $\mathcal{P}'$ has generated and received during the execution, is in pure state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ where $\mathcal{H}'$ is the Hilbert space for $\mathcal{P}'$'s part of the system. Moreover, since $\mathcal{P}$'s behaviour is indistinguishable from the non-purified execution of the protocol (that is the main property of the purification process) we have that $|\Psi\rangle$ is a purification of ρ'.

To get to know more about how to purify a quantum protocol, consult [33] and [34].

6.6 Quantum Bit Commitment is Impossible

We are now ready to conclude the impossibility of quantum bit commitment. Suppose BC is a candidate for a secure quantum bit commitment scheme between Alice, the sender, and Bob, the receiver. A secure protocol for bit commitment must be

Concealing: Let $\rho_{\mathtt{BC}}(0) \in \mathcal{H}'$ and $\rho_{\mathtt{BC}}(1) \in \mathcal{H}'$ be the density operator corresponding to the mixed state received by Bob when Alice commits 0 and 1 respectively. In order for the commitment to be concealing, it must be the case that $\rho_{\mathtt{BC}}(0) \approx \rho_{\mathtt{BC}}(1)$.

Binding: Once the committing phase completed, Alice can open with success only one bit b.

We show that if the concealing condition holds then necessarily the binding condition does not. First, if $\rho_{\mathtt{BC}}(0)$ and $\rho_{\mathtt{BC}}(1)$ are sensibly different then they can be distinguished with good probability by a quantum measurement. For more information about how distinguishable are different density operators, consult [21]. In the following, we assume that $\rho_{\mathtt{BC}}(0) = \rho_{\mathtt{BC}}(1)$ instead of being approximatively the same. To see how to address the case where $\rho_{\mathtt{BC}}(0)$ and $\rho_{\mathtt{BC}}(1)$ are *close* but not identical, consult [32]. Alice's attack, that is described next, is the same in both cases.

Assume that Alice purifies the commitment of $b = 0$ using the technique describes in the last section. The resulting quantum system $\Psi_0 \in \mathcal{H} \otimes \mathcal{H}'$ that contains Alice's QM and what has been generated and received by Bob, is a purification of $\rho_{\mathtt{BC}}(0)$. At revelation, Alice can open $b = 0$ since all information that was needed in order to commit honestly to $b = 0$, is still accessible in QM. After the revelation phase, Bob accepts the opening of $b = 0$ exactly as it is in the honest case (this is what purification is all about).

Alice could have purified the commitment of $b = 1$ instead. This would result in a quantum purification $\Psi_1 \in \mathcal{H} \otimes \mathcal{H}'$ for the mixed state $\rho_{\mathtt{BC}}(1)$ corresponding to the commitment of $b = 1$. When Ψ_1 is created, QM contains all the necessary information to open $b = 1$. Since $\rho_{\mathtt{BC}}(1) = \rho_{\mathtt{BC}}(0)$ it follows that $|\Psi_1\rangle$ is a purification of $\rho_{\mathtt{BC}}(0)$ as well.

Assume Alice wants to open $b = 1$. We now take full advantage of the purification of $\rho_{\mathtt{BC}}(0)$. In last section, we have seen that for any pair of purifications Ψ_0 and Ψ_1 for the same density operator $\rho_{\mathtt{BC}}(0)$ there exists an unitary transformation $W \in \mathcal{H}$ such that

$$|\Psi_1\rangle = (W \otimes \mathbb{1}_{\mathcal{H}'})|\Psi_0\rangle.$$

Moreover, the transformation W depends only upon the protocol specification and is independent on what Bob does. Alice can therefore open $b = 1$ after having applied W on her part of the system (i.e. which is QM) just by following the revelation protocol honestly.

In conclusion, here is the always successful attack against the quantum bit commitment scheme BC:

1. Alice purifies the commitment of $b = 0$,
2. If Alice wants to open $b = 0$, she executes the revelation protocol from her part of the purification stored in QM,
3. If Alice wants to open $b = 1$, she applies W on QM and follows the revelation protocol for $b = 1$.

This strategy is indistinguishable from the honest one and therefore can be applied to any candidate for a quantum bit commitment scheme. We conclude that no quantum bit commitment exists.

7 Conclusion

It is now clear that in quantum cryptography, security in two-party games is much more difficult to achieve than the security of Alice and Bob against the world. Security against the world is what is needed in order to achieve secret-key distribution and that, quantum cryptography can do for free. However, two-party games involve two parties that, although collaborative, do not trust the integrity of the other. In this model, we discussed the fact that quantum oblivious transfer is reducible to bit commitment which is not known/expected to be true in the classical world. We have also seen that the security conditions for bit commitment cannot be met by any purely quantum process. After Mayers' had shown that no quantum bit commitment exists, the spontaneous attitude was to try taking advantage of subtle assumptions appearing in the theorem statement. Most of those approaches use classical assumptions that have to hold only temporarily. The goal being to build from such assumptions a commitment scheme that is both concealing and binding even after the assumption is withdrawn. Unfortunately, none of these attempts provided more than what classical cryptography alone provides [13]. Mayers' attack is now known to apply in scenarios lying beyond the original statement of the no-go theorem. It can also be shown that perfect quantum coin tossing is also impossible [28]. However, quantum bit commitment is possible under physical (not computational assumptions). In [40], it has been shown that if one party is restricted to perform a subset of all possible generalized quantum measurements then quantum bit commitment is possible. The subset of possible measurements can be chosen in such a way that the assumption is likely to hold in any practical situation that will occur in a foreseeable future. In other words, the existence of an unitary process that breaks a quantum protocol does not necessarily imply that it can be implemented in real life. There is an inherent asymmetry between the complexity of physical processes involved in the execution of quantum protocols and those involved in quantum algorithms breaking them. It is not clear if Mayers' attack will be implementable in real life for all practical quantum bit commitment protocols. It would be interesting to characterize the *physical complexity* of the attack against protocols designed to make it difficult to implement.

Although they aim at solving the same kind of problems, the structure of quantum and classical cryptography differ. In a particular situation, one may offer advantages over the other. One thing we did not talked about yet is the possibility to use hybrid systems. Quantum encoding of information, like the BB84 coding scheme, allows to send classical information in an oblivious way. The receiver does not know for sure what was the original classical bit, and the sender does not know whether or not the receiver got the bit sent. But the sender, by announcing the transmission basis θ, allows the receiver to determine whether or not he received the bit perfectly. This simple primitive, although not powerful enough to provide bit commitment, cannot be done classically using no assumptions. It would be interesting to see if it can be used in a purely classical setting in order to weakened the classical assumptions required for a particular task. We have already seen that it is the case for oblivious transfer based on bit commitment; what about other cases?

In conclusion, quantum information is more elusive than its classical counterpart. One must always take care when analyzing and reasoning about quantum protocols. Although the Holy Grail is not achievable quantumly (nor classically), quantum cryptography offers a good alternative to classical cryptography. Quantum cryptography provides an independent framework to complexity-based cryptography and several open questions remain in order to get a better understanding of its possibilities and limits.

8 Acknowledgements

I thank Jan Camenisch, Ivan Damgård, and Stefan Dziembowski for comments on earlier drafts. I would like to express my gratitude to the organizing committee and, in particular, to Ivan Damgård for having brought to life such a successful event.

References

1. Bennett, C. H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175 – 179.
2. Bennett, C. H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, Vol. 5, no. 1, 1992, pp. 3 – 28.
3. Bennett, C. H., G. Brassard, S. Breidbart and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens", *Advances in Cryptology: Proceedings of Crypto 82*, August 1982, Plenum Press, pp. 267 – 275.
4. Bennett, C. H., G. Brassard, C. Crépeau and U. Maurer,"Generalized Privacy Amplification",IEEE Transaction on Information Theory, vol. 41, no. 6, november 1995, pp. 1915–1923.
5. Bennett, C. H., G. Brassard, C. Crépeau and M.–H. Skubiszewska, "Practical quantum oblivious transfer", Advances in Cryptology, Lecture Notes in Computer Sciences, Springer-Verlag, vol. 576, 1991, pp. 351–366. *Advances in Cryptology — Proceedings of Crypto '91*, August 1991, Springer – Verlag, pp. 351 – 366.
6. Biham, E, G. Brassard,M. Boyer,J. van de Graaf and T. Mor, "Security of Quantum Key Distribution Against All Collective Attacks", Los Alamos preprint archive `quant-ph/9801022`, January 1998.
7. Blum, M.,"Coin Tossing by Telephone: A Protocol for Solving Impossible Problems", Proceeding of the 24th IEEE Computer Conference, 1982, pp. 133–137; reprint in SIGACT News, vol.15, no.1, 1983,pp.23–27.
8. Buttler, W.T., R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson and C.M. Simmons, "Free-space quantum key distribution",available at `http://xxx.lanl.gov/ps/quant-ph/9801006`, january 1998.
9. Brassard, G., "Recent developments in quantum cryptography", *Proceedings of Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology*, Prague, October 1996.
10. Brassard, G., D. Chaum and C. Crépeau, "Minimum Disclosure Proofs of Knowledge", Journal of Computing and System Science, vol.37 , 1988, pp. 156–189.

11. Brassard, G., C. Crépeau, "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology — Proceedings of Crypto '90*, August 1990, Springer – Verlag, pp. 49 – 61.
12. Brassard, G., C. Crépeau, R. Jozsa and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 34th Annual IEEE Symposium on the Foundations of Computer Science*, November 1993, pp. 362 – 371.
13. Brassard, G., C. Crépeau, D. Mayers and L. Salvail, "Defeating Classical Bit Commitments with a Quantum Computer", Los Alamos preprint archive `quant-ph/9806031`, June 1998.
14. Carter, J.L. and M.N. Wegman, "Universal Class of Hash Functions", Journal of Computer and System Sciences, vol. 18, 1979, pp.143–154.
15. Crépeau, C., "Quantum oblivious transfer", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2445 – 2454.
16. Crépeau, C. and Kilian, J., "Achieving oblivious transfer using weakened security assumptions", *Proceedings of 29th Annual IEEE Symposium on Foundations of Computer Science*, 1988, pp. 42 – 52.
17. Crépeau, C. and L. Salvail, "Quantum oblivious mutual identification", Advances in Cryptology, proceedings of EUROCRYPT'95, Lecture Notes in Computer Sciences, Springer-Verlag, vol. 921, 1995, pp.133–146.
18. Crépeau, C., J. van de Graaf, and A. Tapp, "Committed Oblivious Transfer and Private Multi-Party Computation", Adavances in Cryptology, proceedings of Crypto'95, Lecture Notes in Computer Sciences, Springer-Verlag, Vol. 963, 1995, pp. 110 – 123.
19. Diffie, W. and M.E., Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, vol. IT-22, 1976, pp. 644–654.
20. Goldreich, O., S. Micali, and A. Wigderson, "Proofs That Yield Nothing but Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems", Journal Assoc. Comput. Mach., vol. 38, 1991, pp. 691–729.
21. Fuchs, C.A. and J. van de Graaf, "Cryptographic Distinguishability Measures for Quantum Mechanical States", Los Alamos preprint archive `quant-ph/9712042`, December 1997.
22. Hughston, L. P., R. Jozsa, and W. K. Wootters, "A complete classification of quantum ensembles having a given density matrix", *Physics Letters A*, vol. 183, pp. 14 – 18, 1993.
23. Impagliazzo, R and S. Rudich, "Limits on Provable Consequences of One-Way Permutations", in the 24th ACM conference on the theory of computing, 1989.
24. Jacobs, B.C. and J.D. Franson, "Quantum cryptography in free space", Optics Letters, vol. 21, no. 22, November 15, 1996.
25. Jozsa, J., "Fidelity for mixed quantum states", *Journal of Modern Optics*, vol. 41(12), pp. 2315 – 2323, 1994.
26. Kilian, J., "Founding Cryptography on Oblivious Transfer", Proceedings of the 20th Annual ACM Symposium on the Theory of Computing, Chicago, 1988, pp. 20 – 31.
27. Lo, H.–K. and H. F. Chau, "Is quantum bit commitment really possible?", *Physical Review Letters*, vol 78, pp. 3410 – 3413 (1997).
28. Lo, H.–K. and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible." Available at `http://xxx.lanl.gov/ps/quant-ph/9711065`.
29. Lo, H.–K. and H. F. Chau, "Security of Quantum Key Distribution", available at `http://xx.lanl.gov/list/quant-ph/9803006`, March 1998.

30. Maurer, U.M.,"Protocols for Secret Key Agreement by Public Discussion Based on Common Information",Advances in Cryptology, proceedings of CRYPTO'92, Lecture Notes in Computer Sciences vol. 740, Springer-Verlag, 1993, pp. 461–470.
31. Mayers, D., On the security of the quantum oblivious transfer and key distribution protocols, Advances in Cryptology, proceedings of Crypto'95, Lecture Notes in Computer Sciences, Springer-Verlag, vol. 963, 1995, pp.124–135.
32. Mayers, D., "The trouble with quantum bit commitment", LANL Report No. quant-ph/9603015 (to be published). The author first discussed the result in Montréal at a workshop on quantum information theory held in October 1995.
33. Mayers, D., "Unconditionally secure quantum bit commitment is impossible", submitted to *Fourth Workshop on Physics and Computation — PhysComp '96*, Boston, November 1996.
34. Mayers, D., "Unconditionally secure quantum bit commitment is impossible", *Physical Review Letters*, vol 78, pp. 3414 – 3417 (1997). Note that this paper has the same title as [33] even though it uses a different approach.
35. Mayers, D.,"Unconditional security in Quantum Cryptography", available at `http://xx.lanl.gov/list/quant-ph/9802025`, february 1998.
36. Mayers, D. and L. Salvail, "Quantum oblivious transfer is secure against all individual measurements", *Proceedings of the Third Workshop on Physics and Computation — PhysComp '94*, Dallas, November 1994, IEEE Computer Society Press, pp. 69 – 77.
37. Muller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin, "Plug and Play systems for quantum cryptography", available at `http://xx.lanl.gov/list/quant-ph/9611042`, november 1996.
38. Peres, P., "Quantum Theory:Concepts and Methods", Fundamental Theories of Physics seriesm, Kluwer Academic Publishers,vol. 72, 1995.
39. Rivest, R.L., A., Shamir and L.M, Adleman,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, vol.21, 1978,pp.120–126.
40. Salvail, L., "Quantum Bit Commitment from a Physical Assumption", Advances in Cryptology, proceedings of CRYPTO'98, Lecture Notes in Computer Sciences, Springer-Verlag, vol. 1462, 1998, pp. 338–353.
41. Shor, P.,"Algorithms for Quantum Computation:Discrete Logarithms and Factoring", Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, 1994, pp. 124–134.
42. Shannon, C.E.,"A Mathematical Theory of Communication", Bell System Technical Journal, vol.27, 1948,pp.379–423 and pp.623–656.
43. Townsend, P., J. Rarity and P. Tapster,"Single photon interference in a 10km long optical fibre interferometer", electronic Letters, 29, 1993, pp.634–635.
44. Wiesner, S., "Conjugate coding", *Sigact News*, Vol. 15, no. 1, 1983, pp. 78 – 88; original manuscript written *circa* 1969.
45. Wyner, A.D.,"The wire-tap channel", Bell System Technical Journal,vol. 54, no. 8, 1975, pp. 1355–1387.
46. Yao, A. C.–C., "Security of quantum protocols against coherent measurements", Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 1995, pp. 67 – 75.