Security and implementation of advanced quantum cryptography : quantum money and quantum weak coin flipping

Mathieu Bozzio

université PARIS-SACLAY

NNT : 2019SACLT045

Thèse de doctorat

Sécurité et implémentation en cryptographie quantique avancée:

monnaie quantique et tirage à pile ou face faible

Thèse de doctorat de l'Université Paris-Saclay
préparée à Télécom Paris

École doctorale n°572 Ondes et Matière (EDOM)
Spécialité de doctorat : physique

Thèse présentée et soutenue à Paris, le 10 décembre 2019, par

MATHIEU BOZZIO

Composition du Jury :

Mme. Rosa TUALLE-BROURI Professeur, IOGS, France.	Présidente
Mr. Anthony LEVERRIER Chercheur, INRIA Paris, France.	Rapporteur
Mr. Nicolas SANGOUARD Professeur, Université de Bâle, Suisse.	Rapporteur
Mr. Hugo ZBINDEN Professeur, Université de Genève, Suisse.	Examinateur
Mr. Charles Ci Wen LIM Professeur assistant, NUS, Singapour.	Examinateur
Mme. Isabelle ZAQUINE Professeur, Télécom Paris, France.	Directrice de thèse
Mme. Eleni DIAMANTI Directrice de recherche, CNRS, Sorbonne Université, France.	Directrice de thèse

Abstract (Français)

Les lois de la mécanique quantique présentent un fort potentiel d'amélioration pour la sécurité des réseaux de communication, du cryptage à clé publique au vote électronique, en passant par la banque en ligne. Cette thèse porte sur la sécurité pratique et l'implémentation de deux tâches cryptographiques quantiques : la monnaie quantique et le tirage à pile-ou-face faible.

La monnaie quantique exploite le théorème de non-clonage quantique pour générer des jetons, billets ou cartes de crédit strictement infalsifiables. Nous réalisons la première démonstration expérimentale de cette fonctionnalité sur une plateforme photonique aux longueurs d'onde télécom. Nous développons ensuite une analyse de sécurité pratique pour les cartes de crédit quantiques. La banque peut ainsi vérifier l'authenticité de la carte à distance, même en présence d'un terminal de paiement malhonnête. Enfin, nous proposons une expérience permettant le stockage sécurisé d'une carte de crédit quantique en utilisant la transparence électromagnétiquement induite au sein d'un nuage d'atomes refroidis.

Le tirage à pile-ou-face faible est une primitive cryptographique fondamentale: elle permet en effet la construction de tâches plus complexes telles que la mise en gage de bit et le calcul multipartite sécurisé. Lors d'un tirage à pile ou face, deux entités distantes et méfiantes jettent une pièce. Grâce à l'intrication quantique, il est possible de limiter la probabilité que l'entité malhonnête biaise la pièce. Dans ce projet, nous proposons la première implémentation du pile-ou-face faible. Celle-ci requiert un photon unique et une plateforme d'optique linéaire. Nous présentons l'analyse de sécurité en présence d'erreurs et de pertes, et démontrons que le protocole est réalisable à l'échelle d'une ville. Enfin, nous proposons de réduire davantage la probabilité du biais du protocole.

Abstract (English)

Harnessing the laws of quantum theory can drastically boost the security of modern communication networks, from public key encryption to electronic voting and online banking. In this thesis, we bridge the gap between theory and experiment regarding two quantum-cryptographic tasks: quantum money and quantum weak coin flipping.

Quantum money exploits the no-cloning property of quantum physics to generate unforgeable tokens, banknotes, and credit cards. We provide the first proof-of-principle implementation of this task, using photonic systems at telecom wavelengths. We then develop a practical security proof for quantum credit card schemes, in which the bank can remotely verify a card even in the presence of a malicious payment terminal. We finally propose a setup for secure quantum storage of the credit card, using electromagnetically-induced transparency in a cloud of cold cesium atoms.

Quantum weak coin flipping is a fundamental cryptographic primitive, which helps construct more complex tasks such as bit commitment and multiparty computation. It allows two distant parties to flip a coin when they both desire opposite outcomes. Using quantum entanglement then prevents any party from biasing the outcome of the flip beyond a certain probability. We propose the first implementation for quantum weak coin flipping, which requires a single photon and linear optics only. We provide the complete security analysis in the presence of noise and losses, and show that the protocol is implementable on the scale of a small city with current technology. We finally propose a linear-optical extension of the protocol to lower the coin bias.

Dedication and acknowledgements

First, I would sincerely like to thank my supervisors, Isabelle and Eleni, as well as Iordanis, for their wise guidance, motivating scientific discussions, constant availability, and for providing me with the most interactive, comfortable and friendly work environment I could ever dream of. Many thanks to the other great leaders of the quantum information team, who contribute to this amazing atmosphere: Damian, Elham and Fred.

To my highly inspirational LIP6 colleagues with whom I have shared countless *coffee and whiteboard* discussions, giving birth to many ideas in this thesis: Ulysse, Fred (once again), Shouvik, Simon, Leo, Dominik, Luka, Niraj, Luis and Federico. To the fantastic rest of the LIP6 team, which I treat as a large, cheeky family: Nathan, Francesco, Victor, Rawad, Adrien, Luka, Pierre, Raja, Shane, Andrea, Clément, Matteo, Rhea, Gözde, Natansh and Shraddha. To my other highly motivated collaborators outside LIP6: Atul, Damian and Felix, and to my friendly colleagues from Télécom: Adeline, Martin, Julien, and Alex.

To my fantastic and loving girlfriend, Anu, for making these the happiest years of my life. Thanks for the love, the support, the fun, the countless adventures, trips, food and memories. To our post-PhD life, in this mysterious country that only the future knows about!

I must then thank my long-term high school friends, along with other Paris friends, for always providing balance in my life. To Vidipt, William and Sonia for the endless friendship and support. To Anneka, Sara, Claire and Josh for patiently listening to my quantum monologues, and showing me that people out there actually care about what we do! To my dearest friends and fellow musicians, Pierre, Turmize, Viet, Gil, Ferron, Clément, and Gus, for sharing these trips and musical adventures. To Pierre, Gab and Claire for pursuing the physics thesis experience with me, and for the many fun trips and evenings.

To Yves for introducing me to the fascinating world of science when I was 11 years old, and for giving me the motivation to pursue until now.

Finally, I would like to thank my whole family, especially Monique and Caroline, along with the most important person in my life: my Mum. I am so grateful for your hard work and struggle that have brought me here. This thesis is entirely dedicated to your love, care, guidance and intense will to make the craziest things happen.

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Context

1.1.1 Quantum networks

Modern communication networks are continuously expanding, with the increase in the number of users and available online resources. On a daily basis, users must inevitably trust local network nodes and transmission channels in order to perform sensitive tasks such as private data transmission, online banking, electronic voting, anonymous messaging, digital signatures, delegated computing and many more. In general, such complex networks are secured by relying on a collection of simpler cryptographic primitives, or building blocks, which are put together to guarantee overall security.

Let us illustrate this by considering a simple primitive, known as *bit commitment*. In this two-party protocol, we refer to Alice as the message sender, and Bob as the message receiver. Alice chooses a bit x, encrypts it according to some specific function, and sends it to Bob. The desired security property is two-way: Bob must not learn the value of x until Alice decides to reveal it, while Alice must not be able to change x once she has committed to it. Once this bit commitment primitive is acquired and provided as a black box, it may be used to construct a new primitive known as *strong coin flipping*. This primitive allows two parties to toss a fair coin from a distance without trusting each other. In a secure version of this task, none of the two parties should be able to bias the coin towards their preferred outcome. Assuming the parties use bit commitment as a

secure resource, they may each commit to a bit, choose to reveal it at any given time, and take the sum of the two revealed bits as the outcome of the coin toss. Treating this new primitive as a black box in turn allows to construct more complex tasks relating to online gaming, multiparty computing [1], and randomized consensus protocols [2].

Cryptography often involves rigorously defining the notion of security for a given task, and constructing a protocol which achieves this security. Using classical resources only, the security of many primitives relies on *computational assumptions*. This type of security stems from the complexity of the encryption function used, and the time it takes for an adversary to reverse it. Essentially, a scheme is considered unbreakable when the time it takes for an adversary to computationally reverse the encryption function is much larger than the time over which the protocol must remain secure. A widely used public key encryption scheme, which relies on the computational difficulty in factoring large numbers, is the RSA method [3]. It allows for two parties to exchange a secret key over a public channel, such that no eavesdropper can recover the secret key over the timescale of interest.

Strikingly, it turns out that encoding secret information onto quantum systems instead of classical ones can provide a much stronger level of security for public-key encryption, as well as for many other tasks. At the heart of quantum theory lie the uncertainty principle and the no-cloning theorem [4]. The first property states that, given two conjugate physical observables, decreasing the uncertainty on the value of one increases the uncertainty on the other. The second property states that it is physically impossible to perfectly clone an unknown quantum system, that is, to generate two identical copies of the system starting from a single copy. This contrasts with the classical world, in which measuring the properties of an unknown system allows to recreate many identical copies of it.

In the early seventies, Wiesner brought up an outrageously novel concept [5]: encoding information onto quantum observables instead of classical observables allows to exploit these fundamental properties to achieve *information-theoretic security*, i.e. security which does not rely on any computational assumption. This form of security already exists in the classical world for some tasks, such as the one-time-pad [6], which serves to encrypt a message with a pre-shared secret key of the same length. However, Wiesner's ground-breaking proposal allows to achieve information-theoretic security for many primitives which previously based their security on computational assumptions. These strong implications effectively gave birth to the field of quantum cryptography [7–9]. Of course, claiming information-theoretic security with the laws of quantum mechanics

presents an implicit assumption: quantum theory must be an accurate description of the physical world. If this does not hold, the adversary could potentially exploit more general physical theories [10, 11].

Wiesner illustrated his original paper with two potential applications, of which one was the fabrication of unforgeable quantum money. Simply speaking, quantum money involves a mint, a client, and a bank. The mint encodes a secret classical key into a sequence of two-level quantum states, known as qubits. These are stored in a quantum memory and handed to a client. The sequence of qubit states, along with the quantum storage device, constitute the physical money state, which the client may choose to spend wherever. The secret key specifies the quantum observable in which each qubit is encoded, and is known to the mint and the bank only. In an adversarial scenario, the client may attempt to counterfeit the money (i.e. produce several copies of it) in order to spend more than the initial amount. Thanks to the uncertainty principle and the no-cloning theorem, this is impossible to achieve without disturbing and modifying some of the quantum states in the money state. When a branch of the bank, in possession of the secret key, later verifies the authenticity of the money, inconsistencies with the key will be detected, and the payment will be rejected. Note that, in the classical world, it is always possible for a powerful adversary to duplicate banknotes, passports, signatures, keys and other objects, provided that they have enough time and computational power to reverse-engineer the complex design of such documents. A more formal introduction to quantum money will be provided in Chapter 3.

Wiesner's idea was subsequently used to boost the security of many quantum cryptographic schemes such as key distribution, coin flipping and bit commitment [12]. In particular, the BB84 quantum key distribution protocol from [7], along with its many variants, has since thrived as one of the most studied and successfully implemented quantum information applications [9, 13, 14]. Just like RSA, it allows for two parties to securely establish a secret key over a public, eavesdropped (this time quantum) channel. However, it exhibits the crucial advantage of achieving information-theoretic security, provided the required classical communication is performed over an authenticated channel.

A year only after quantum key distribution was invented, Deutsch defined and formalized the universal quantum computer, namely a device which uses quantum objects to perform computations [15]. Noticeably, exploiting quantum resources such as *superposition* enables quasi-exponential computation speedup over the best known classical algorithms for specific tasks, such as factoring large numbers. When Shor showed how such a hypothetical quantum computer could break specific schemes based on compu-

tational assumptions in a very short time [16], scientists gradually entered a new era: that of constructing schemes which are secure against *quantum adversaries*. Quantum key distribution, along with most previously mentioned quantum-cryptographic tasks, provide this new, crucial form of security.

We note that, on top of quantum superposition, quantum theory provides a second significant resource for cryptography: *entanglement*, which Einstein originally qualified as "spooky action at a distance". This phenomenon effectively correlates the properties of two quantum systems at an arbitrary distance, in a way that cannot be explained by classical deterministic models [17]. It helps achieve quantum advantage in tasks involving weak coin flipping [18], anonymous message transmission [19] and alternative forms of quantum key distribution [20]. Crucially, it also provides us with quantum teleportation [21, 22], which greatly benefits quantum communication networks [23].

Since 2017, a large and collaborative network of European research teams has started to lay the foundations of a quantum internet [23], which would enable any two points on Earth to communicate efficiently and securely thanks to quantum technologies. This ambitious research effort gathers physicists, mathematicians and computer scientists to develop full stack quantum networks, from hardware implementation to compilers and user interface. In order to help such diverse scientists understand each other, an open-access quantum protocol zoo has also been developed [24]. This serves as an open-access repository, in which a comprehensive set of quantum primitives and tasks are compactly explained, and the links between them are made explicit.

This thesis fits well within the quantum internet framework, as it develops practical security proofs for two pillars of quantum cryptography: quantum money, which protects against the forgery of physical money, and quantum weak coin flipping, which is involved in the construction of many tasks, such as quantum bit commitment and quantum strong coin flipping [25, 26]. We rigorously show how information-theoretic security can be achieved with current technology for these two tasks, propose the first implementation for quantum weak coin flipping, and experimentally demonstrate a quantum money protocol for the first time. This is done using practical photonic systems.

1.1.2 Security in practice

Using quantum resources can drastically boost the performance and security parameters of cryptographic tasks, such as secret key rate in key distribution protocols and bias in coin flipping tasks. However, while information-theoretic security is guaranteed in theory through quantum properties, real-world implementation opens a whole new spectrum of

attacks and loopholes which must be characterized and fixed. This is exactly the focus of this thesis, as it aims to implement quantum money and quantum weak coin flipping protocols in such a way that information-theoretic security is preserved. In general, these practical attacks make use of two major experimental imperfections, *noise* and *losses*, which allow the adversary to exploit vulnerabilities in state generation, quantum channels and measurement devices. The performance and security of a quantum protocol with respect to its classical counterpart will therefore crucially depend on the parameters associated with a given experimental setup. In order to highlight this key point, we briefly describe three powerful attacks which may occur in the presence of losses for different quantum-cryptographic tasks. The first attack, which we label the *50/50 card split*, relates to practical quantum money schemes, and actually arises from the results in this thesis. The second attack refers to *dishonest aborts* in protocols such as quantum weak coin flipping, which are also studied in this thesis. The third attack, *unambiguous state discrimination*, is already well documented [27], and may occur in quantum key distribution protocols, as well as quantum money schemes.

- *The 50/50 Card Split.* As previously mentioned, quantum money is a task which guarantees the unforgeability of physical money. We recall that the mint encodes a secret key into a sequence of quantum states, which physically embody the money state, stores it in a quantum memory, and hands it to a client. A dishonest client will be unable to copy the quantum object without partially altering the initial state, since the secret key is unknown to them. Upon verification, a bank will detect changes in the quantum states and conclude whether the money state is authentic or not. Thus, in theory, information-theoretic security is guaranteed by quantum-mechanical properties. In a lossy implementation, however, the dishonest client may successfully extract twice the amount of money in two different banks without getting caught. This may occur when the honest quantum channel, or the quantum storage device, exhibits 50% losses or more. In this scenario, the client may simply replace the channel with a perfect one, and split the money state in two. They may then send the first half to one bank, and the second to another bank. Since cloning attacks have not been attempted, both banks will validate the money state, as the quantum states have not been altered. The client will then be able to spend twice the amount of money associated with the original state. It is therefore crucial to upper bound and monitor the losses in any quantum money implementation.

- *The Dishonest Abort.* Quantum weak coin flipping is a task in which two parties wish to toss a fair coin from a distance without trusting each other. It effectively designates a

winner and a loser. One of the parties is therefore very likely to cheat, by attempting to bias the coin in their favor. In a perfect implementation, quantum entanglement allows both parties to agree on an outcome without needing to simultaneously broadcast their respective bits. A clever protocol structure then prevents the dishonest party from biasing the outcome of the flip above a certain threshold. In the presence of losses, however, this security property may very quickly break down: in order to account for the potential loss of the quantum state, the notion of *abort* must be introduced in the protocol. When both parties are honest, this gives a third possible outcome to the coin flip, in which no one wins or loses. When one of the parties is dishonest, however, they can choose to falsely declare the loss of their quantum state, and hence force an abort, whenever the outcome of the coin flip designates them as the loser. In this case, it may be claimed that the protocol performs strictly better than classically *provided* that the losses do not exceed a specific threshold. When these become too important, a classical coin flipping protocol may actually perform better than the quantum protocol.

- *Unambiguous State Discrimination (USD).* This attack was originally studied in the context of quantum key distribution [27], in which two parties wish to establish a common secret key by communicating through a public quantum channel. An eavesdropper may intercept and measure each transmitted quantum state, in such a way that they can unambiguously discriminate a fraction of the states sent. An extra measurement "don't know" outcome is output for the remaining states that were not discriminated. In an ideal world, this attack can be detected by the two communicating parties since the "don't know" outcome limits to the amount of information that the adversary may retrieve about the key. In a lossy implementation however, the two honest parties will expect and tolerate a specific amount of losses due to their imperfect setup. The eavesdropper may then replace the lossy channel by a perfect one, perform a USD attack, and replace all states which they didn't manage to discriminate with losses [27]. In this way, the two parties do not record any errors, but simply losses which they discard from the final secret key. This attack also applies to quantum money, as described in this thesis.

When transitioning from ideal to practical protocols, these three examples highlight the need for new security proofs which are specifically targeted towards imperfect experimental setups. The core work in this thesis deals with such types of security analyses for quantum money schemes and quantum weak coin flipping schemes.

1.2 Thesis results

1.2.1 Outline

This thesis is split into two introductory chapters, four original research chapters, and one conclusion chapter. Two of the four research chapters are devoted to theoretical results, while the two others are devoted to experimental results.

Chapter 2 introduces the main technical tools required in this thesis. We first describe the mathematical framework and quantum resources which enable the construction of quantum protocols. We then introduce the basic concepts of semidefinite programming, which allow to derive both analytical and numerical results throughout the thesis. We finally explore the areas of quantum optics which are relevant to the implementation of both quantum money and quantum weak coin flipping protocols.

Chapter 3 introduces the foundations of quantum cryptography. We first explain how fundamental quantum properties can drastically improve the security of some cryptographic tasks. We then illustrate this with three protocol sections: quantum money, quantum key distribution and quantum coin flipping. The first and third sections provide functionality classifications which are crucial to the understanding of this thesis.

Chapter 4 describes the practical security analysis and proof-of-principle implementation of an unforgeable quantum credit card scheme, assuming a trusted payment terminal. We first show how to transition from the abstract two-dimensional security framework to a practical, infinite-dimensional one. We then provide a fibered experimental demonstration, using polarization-encoded weak coherent states of light at telecom wavelengths. The implementation is labeled "proof-of-concept" as it does not involve a quantum storage device, which is a key requirement in quantum credit card schemes.

Chapter 5 derives a practical and rigorous security analysis which deals with both trusted and untrusted terminals in quantum credit card schemes. We first highlight that the work from Chapter 4 does not account for all loss-dependent attacks, and that it assumes a trusted payment terminal. We then derive a new framework which allows to derive a more general security proof without requiring such assumptions. We do this by incorporating experimental parameters directly into a convex optimization framework. By using the duality of semidefinite programs, we finally show that an adversary cannot better cheat by correlating the states in the credit card.

Chapter 6 builds upon the theoretical results from Chapter 5 to propose a secure demonstration of a credit card scheme with genuine quantum storage. We first de-

scribe the experimental setup for the trusted terminal scheme. This involves storing polarization-encoded weak coherent states of light in a cold atomic cloud, through the creation of electromagnetically-induced transparency (EIT). We then expose the new security issues which arise from the use of such an imperfect storage device, and clearly state the post-selection assumptions which are made.

Chapter 7 provides the first implementation proposal for quantum weak coin flipping. We start by introducing the primitive and explaining why proposing an experimental setup for such a protocol is non-trivial. We then present a linear-optical implementation consisting of a single photon and three beamsplitters only. We derive the corresponding security proof in the presence of noise and losses, and show that protocol is implementable over a few kilometers of lossy optical fiber. Finally, we investigate a possible extension to lower both parties' cheating probabilities.

Chapter 8 provides a general discussion of the main thesis results and future perspectives. We sum up the key ideas from each research chapter, and describe how they fit within the larger quantum internet framework. We finally discuss major unsolved challenges.

1.2.2 Publications

The results from Chapters 4 and 5 were respectively published in the following articles:

- [28] *Experimental investigation of practical unforgeable quantum money,*
  M. Bozzio, A. Orieux, L.T. Vidarte, I. Zaquine, I. Kerenidis and E. Diamanti,
  npj Quantum Information, 4, 5 (2018).

- [29] *Semi-device-independent quantum money with coherent states,*
  M. Bozzio, E. Diamanti and F. Grosshans,
  Physical Review A, 99, 022336 (2019).

Some theoretical results from Chapter 6 were also published in [29], although most of this work is currently in progress. The manuscript associated with Chapter 7 is in preparation:

- *Quantum weak coin flipping with a single photon.*
  This is joint work with E. Diamanti, I. Kerenidis and U. Chabaud.

The results in this thesis have also been presented as contributed talks in international conferences such as QCrypt 2017, AQIS 2018, CEWQO 2018, EQTC 2019, and disseminated in newspapers and scientific magazines including *Le Monde*, *Science et Vie* and *La Recherche*.

CHAPTER 2

PRELIMINARIES

2.1 Mathematical framework

2.1.1 First resource: quantum coherence

The physical state of a quantum system may be described by a single vector, or wavefunction $|\psi\rangle$, living in a complex Hilbert space $\mathscr{H}$. The Hermitian conjugate of such a vector is denoted by $\langle\psi|$. When all the information about the physical system can be contained in such vector form, the system is said to lie in a *pure* quantum state, which may be expressed as:

$$|\psi\rangle = \sum_{k=1}^{N} c_k |\psi_k\rangle , \tag{2.1}$$

where $\{c_k\}$ are complex coefficients and the vectors $\{|\psi_k\rangle\}$ form an orthonormal basis for the N-dimensional Hilbert space $\mathscr{H}$. Pure quantum states may always be expressed as a linear superposition, referred to as *quantum superposition*. When a measurement is performed on the system, the state is said to *collapse* to one of the $|\psi_k\rangle$ states with probability $|c_k|^2$. The state $|\psi\rangle$ must therefore be normalized to ensure $\sum_{k=1}^{N} |c_k|^2 = 1$. One pure quantum state of interest is the two-dimensional *qubit* state, which allows to encode a classical information bit into a physical system, and takes the following general form:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \tag{2.2}$$

with $(\alpha, \beta) \in \mathbb{C}^2$ and $\{|0\rangle, |1\rangle\}$ spanning a 2-dimensional Hilbert space.

An observer may sometimes lack some information about the state of a system, in which case the vector representation becomes insufficient. This usually occurs when the system of interest is a subsystem of a larger system with unknown degrees of freedom. Since the probabilistic behaviour of the state which arises from the observer's lack of knowledge cannot be distinguished from the inherent probabilistic nature of quantum superposition described in (2.1), a new formalism is required to describe such *mixed* quantum states : the density matrix. Given a collection of pure quantum states $\{|\psi_k\rangle\}$, one possible expression for a mixed state's density matrix ρ is given by:

$$\rho = \sum_{k=1}^{N} p_k |\psi_k\rangle \langle\psi_k|, \tag{2.3}$$

where p_k is the probability, arising from classical statistics, that the system lies in pure state $|\psi_k\rangle$. The density matrix is positive semidefinite, and satisfies $Tr(\rho) = 1$ to ensure that $\sum_{k=1}^{N} p_k = 1$, as well as $Tr(\rho^2) = 1$ if the quantum state is pure. For general mixed states, $0 \leqslant Tr(\rho^2) < 1$. Let us now write the density matrix for the general qubit state presented in (2.2) in the $\{|0\rangle, |1\rangle\}$ basis:

$$\rho = |\psi\rangle \langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha^* \beta \\ \beta^* \alpha & |\beta|^2 \end{bmatrix}. \tag{2.4}$$

This explicit expression for the qubit density matrix allows to identify $Tr(\rho) = 1$, and interpret the diagonal terms $|\alpha|^2$ and $|\beta|^2$ as the probabilities of measuring the system in pure states $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, respectively. Other terms of interest are the off-diagonal terms, which play a crucial role in quantum information theory as they identify the *quantum coherence* of the state. This property is the first essential resource in quantum cryptography and computing, as it is an inherently quantum feature. We will detail its applications in further sections. When the coherent terms are zero, the state becomes an entirely classical state in the studied basis. For real a and b, the state given by:

$$\sigma = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \tag{2.5}$$

may indeed not be written in the coherent superposition form of (2.1) in the $\{|0\rangle, |1\rangle\}$ basis, which implies no quantum feature. Such a density matrix may correspond to the output of an uncharacterized source for instance, which produces the states $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$ with probabilities a and b respectively. We note, however, that this state may present quantum features when expressed in another basis.

It is worth noting that the density matrix of any mixed qubit state may be expanded in a specifically convenient basis as:

$$\rho = \frac{1}{2}\left(\mathbb{1} + b_x\sigma_x + b_y\sigma_y + b_z\sigma_z\right), \tag{2.6}$$

where $\{b_x, b_y, b_z\}$ are known as the coordinates of the *Bloch vector* $\vec{b}$, $\mathbb{1}$ denotes the identity over the 2-dimensional Hilbert space, and the three traceless Hermitian Pauli matrices read:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.7}$$

2.1.2 Second resource: quantum entanglement

The second crucial resource of quantum information is *quantum entanglement*, which arises when considering composite Hilbert spaces and multi-partite quantum states (shared between different parties). This property is a fundamental resource of quantum communication in that it allows to engineer and exploit correlations between distant states that cannot occur in the classical world. This enables to teleport quantum states across networks for instance, in which case classical communication and local quantum operations only are required to retrieve the state at the given destination [21]. This avoids the problem of sending quantum information through quantum channels to distant parties, where losses and errors inevitably occur as the quantum state interacts with its environment. It also provides the foundation of security for some quantum-cryptographic protocols such as quantum key distribution (Section 3.3) and quantum coin flipping (Section 3.4).

More formally, let us consider a general pure quantum state $|\psi^{(N)}\rangle$ living in Hilbert space $\mathscr{H} = \bigotimes_{i=1}^{N} \mathscr{H}_i$, composed of N subsystems. The state is said to be a *product state* if it can be expressed in the following factorizable form:

$$|\psi^{(N)}\rangle = \bigotimes_{i=1}^{N} |\psi_i\rangle, \tag{2.8}$$

where $\{|\psi_i\rangle\}$ is a pure state living in $\mathscr{H}_i$. When $|\psi^{(N)}\rangle$ may not be expressed in such a form, the state is said to be *entangled*. In this case, it may only be expressed as a coherent superposition of product states, and the partial trace over one subsystem is a mixed state. Similarly, a mixed quantum state $\rho^{(N)}$, living in Hilbert space $\mathscr{H} = \bigotimes_{i=1}^{N} \mathscr{H}_i$

and composed of N subsystems $\{\rho_i\}$, is said to be *separable* if it can be expressed as the following classical mixture of product states:

$$\rho^{(N)} = \sum_{k=1}^{L} m_k \bigotimes_{i=1}^{N} \rho_{i,k}, \tag{2.9}$$

where $\sum_{k=1}^{L} |m_k|^2 = 1$. When it cannot be expressed in such a form, the mixed state is said to be *entangled*.

In order to gain insight into why quantum entanglement is a resource that cannot be retrieved with classical physics alone, we briefly introduce a famous thought experiment, linked to the Bell inequalities [17]. Setting aside quantum theory for a moment, let us consider a party Charlie, who can repeatedly (and identically) produce two particles: the first is sent to Alice, while the second is sent to Bob. At a pre-agreed time, both parties measure a property of their particle: Alice flips a coin to decide whether she measures observable A_1 or A_2, while Bob flips a coin to decide whether he measures B_1 or B_2. The set of observables $\{A_1, A_2, B_1, B_2\}$ can take values ± 1. They repeat the experiment a large number of times, and, at the end, compute the value of the following sum of expectation values: $E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2)$.

Classical mechanics is a *realist* theory, in which physical properties have definite values independently of whether they are observed or not. It is also a *local* theory, in that the measurement that Alice makes on her particle should not influence the measurement that Bob makes on his particle. Under such assumptions, it can be shown that [17, 30]:

$$E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2) \leqslant 2. \tag{2.10}$$

Let us now attempt this experiment with quantum particles. Strikingly, if Charlie sends pairs of particles described by the following entangled quantum state:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B), \tag{2.11}$$

and Alice and Bob perform measurements in two different bases such that:

$$\begin{aligned} A_1 &= \sigma_z & A_2 &= \sigma_x \\ B_1 &= -\frac{1}{\sqrt{2}}(\sigma_z + \sigma_x) & B_2 &= \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x), \end{aligned} \tag{2.12}$$

then it is possible to violate the upper bound from Eq. (2.10) [30]:

$$E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2) = 2\sqrt{2}. \tag{2.13}$$

This surprising result shows that either one or both assumptions of *realism* and *locality* must be dropped if quantum mechanics is correct. The violation of this inequality, and hence the confirmation that quantum mechanics is complete without local realism, was experimentally demonstrated in [31].

In quantum information, the maximally-entangled Bell states, composed of two subsystems A and B, play a significant role:

$$\begin{aligned}
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \\
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B).
\end{aligned} \tag{2.14}$$

For such bipartite states, the reduced state of each subsystem is the maximally mixed state $\mathbb{1}/2$. This means that the joint system has a well-defined state, but no information can be gained by looking at each subsystem on its own. This can be mathematically derived by considering the *partial trace* over one system. Considering Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$, where $\{|a_i\rangle\}$ is the basis for the first space and $\{|b_i\rangle\}$ for the second space, any bipartite quantum state $\rho^{(AB)}$ may be expressed as:

$$\rho^{(AB)} = \sum_{ijkl} c_{ijkl} \, |a_i\rangle \langle a_j| \otimes |b_k\rangle \langle b_l| \, . \tag{2.15}$$

The partial trace over system A and over system B are then respectively defined as:

$$\begin{aligned}
\mathrm{Tr}_A(\rho^{(AB)}) &= \sum_{ijkl} c_{ijkl} \, |b_k\rangle \langle b_l| \langle a_j|a_i\rangle \, , \\
\mathrm{Tr}_B(\rho^{(AB)}) &= \sum_{ijkl} c_{ijkl} \, |a_i\rangle \langle a_j| \langle b_l|b_k\rangle \, .
\end{aligned} \tag{2.16}$$

For bipartite entangled states, this operation allows to derive the reduced density matrix of one subsystem by tracing over the other subsystem. We may then confirm that:

$$\begin{aligned}
Tr_A\left(|\psi^+\rangle\langle\psi^+|\right) = Tr_A\left(|\psi^-\rangle\langle\psi^-|\right) = Tr_A\left(|\phi^+\rangle\langle\phi^+|\right) = Tr_A\left(|\phi^-\rangle\langle\phi^-|\right) = \frac{\mathbb{1}_B}{2}. \\
Tr_B\left(|\psi^+\rangle\langle\psi^+|\right) = Tr_B\left(|\psi^-\rangle\langle\psi^-|\right) = Tr_B\left(|\phi^+\rangle\langle\phi^+|\right) = Tr_B\left(|\phi^-\rangle\langle\phi^-|\right) = \frac{\mathbb{1}_A}{2}.
\end{aligned} \tag{2.17}$$

2.1.3 Quantum measurements

Any quantum observable is described by a Hermitian operator A, whose set of real eigenvalues describes the set of possible measurement outcomes. For each eigenvalue, the associated eigenstate gives the quantum state onto which the system collapses after it is measured. As the outcome of the measurement is probabilistic, the expectation value $< A >$ of the measurement of observable A repeated over infinite identical copies of state ρ can be computed using:

$$< A >= Tr(\rho A). \tag{2.18}$$

As an example, the Pauli matrices introduced in (2.7) may be used to describe observables such as photon polarization and particle spin. The expectation values for the measurement of the x, y or z-components of a polarization or spin state ρ are then given by $Tr(\sigma_x \rho)$, $Tr(\sigma_y \rho)$ and $Tr(\sigma_z \rho)$ respectively.

One specific type of measurement is the *projective measurement*. It is described by a set of operators $P = \{P_m\}_{m=1...n}$, whose number of elements n is smaller or equal to the dimension of the Hilbert space. The projectors satisfy the following conditions:

$$\begin{cases} (i) & P_m P_{m'} = \delta_{mm'} P_m \quad \text{projectivity} \\ (ii) & \sum_m P_m = \mathbb{1} \quad \text{completeness} \\ (iii) & P_m \geqslant 0 \quad \text{semidefinite positivity} \end{cases} \tag{2.19}$$

Note that, when the projectors are rank 1, diagonalizing observable A allows to decompose it into the projectors on the different subspaces:

$$A = \sum_m e_m P_m, \tag{2.20}$$

where P_m is the projector onto the subspace associated with eigenvalue e_m, and the probability $p(m)$ of measuring outcome m given state $|\psi\rangle$ is given by:

$$p(m) = \langle \psi | P_m | \psi \rangle, \tag{2.21}$$

while the post-measurement state then simply reads:

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{2.22}$$

Such projective measurements are interesting, since their outcome may be determined with a single measurement on a pure state. However, a transition towards a more

general type of measurement is needed, just like in the transitioning from pure states to mixed states. This applies to cases where the measuring party does not care about the post-measurement state, and is more interested in the statistics of the outcome over several rounds of measurements. These generalized measurements are known as POVMs *(Positive Operator-Valued Measurements)*. Unlike projectors, if $E = \{E_m\}$ is a POVM, then its elements need not satisfy $E_m^2 = E_m$, and the number of elements needs not be limited to the dimension of the Hilbert space. Conditions (ii) and (iii) of Eq. (7.73), however, are still satisfied.

Finally, we define the *commutator* associated with two quantum observables A_1 and A_2:

$$[A_1, A_2] = A_1 A_2 - A_2 A_1. \tag{2.23}$$

As we shall see in Chapter 3, one founding principle of quantum security is based on the fact that some quantum observables do not commute: A_1 and A_2 cannot be measured simultaneously when their commutator $[A_1, A_2] \neq 0$.

2.1.4 Quantum operations

A quantum operation is a linear map Λ which takes a quantum state ρ_1 living in Hilbert space $\mathscr{H}_1$ to another quantum state ρ_2 living in $\mathscr{H}_2$. In order for such a map to be physical (i.e. mapping a quantum state to another quantum state), it must satisfy the following conditions:

- **Complete positivity:** from Section 2.1.1, a density matrix ρ is positive semidefinite, and this must remain true when map Λ is only applied to a subsystem of this density matrix.
- **Trace preservation (or trace decrease):** from Section 2.1.1, a density matrix has unit trace, and this must be preserved (or decreased) at the output of the map.

Quantum operations may be expressed in matrix form. Kraus' theorem states that any such quantum operation may be decomposed in terms of Kraus operators $\{K_i\}$, satisfying $\sum_i K_i^\dagger K_i \leqslant \mathbb{1}$, as:

$$\Lambda(\rho) = \sum_i K_i \rho_1 K_i^\dagger. \tag{2.24}$$

A *unitary operation* on Hilbert space $\mathscr{H}$ is an operation which preserves the inner product, i.e. an operation which admits a single Kraus operator U in its decomposition, and for which:

$$U^\dagger U = UU^\dagger = \mathbb{1}. \tag{2.25}$$

In general, completely positive trace-preserving (CPTP) maps are crucial to describing any physical transformation applied to a quantum state. It is often possible to work with a density-matrix equivalent representation of CPTP maps, as will be required in Chapter 5 for instance. For this purpose, let us consider a tensor product of two d-dimensional Hilbert spaces $\mathscr{H} = \mathscr{H}_1^d \otimes \mathscr{H}_2^d$, and define the (unnormalized) maximally entangled state $|\Phi^+\rangle\langle\Phi^+|$ on $\mathscr{H}$ as:

$$|\Phi^+\rangle\langle\Phi^+| = \sum_{i,j=1}^{d} |i\rangle\langle j| \otimes |i\rangle\langle j|. \tag{2.26}$$

We introduce a completely positive linear map $\Lambda : \mathscr{H}_1^d \to \mathscr{H}_3^{d'}$, and define the Choi–Jamiołkowski operator $J(\Lambda) : \mathscr{H}_1^d \otimes \mathscr{H}_2^d \to \mathscr{H}_3^{d'} \otimes \mathscr{H}_2^d$ as the operator which applies Λ to the first half of the maximally entangled state $|\Phi^+\rangle\langle\Phi^+|$:

$$J(\Lambda) = \sum_{i,j=1}^{d} \Lambda(|i\rangle\langle j|) \otimes |i\rangle\langle j|. \tag{2.27}$$

Choi's theorem then states that Λ is completely positive if and only if $J(\Lambda)$ is positive semidefinite. This is obvious for the $\Lambda \to J(\Lambda)$ way of the equivalence, since Λ is applied only to a subsystem of $|\Phi^+\rangle\langle\Phi^+|$, and we want the output state to remain a density matrix.

We also have that Λ is a trace-preserving map if and only if $\mathrm{Tr}_{\mathscr{H}_3^{d'}}(J(\Lambda)) = \mathbb{1}_{\mathscr{H}_2^d}$ [32–34]. A physical interpretation of this equivalence arises from the fact that $|\Phi^+\rangle$ is a maximally entangled state. Then, from Section 2.1.2, the partial trace over one subystem must yield the maximally mixed state on the other. These properties are implemented as constraints in the optimization problems from Chapter 5.

2.2 Semidefinite programming

In this section, we briefly introduce the terminology and field of semidefinite programming from a quantum-information perspective. The techniques presented here will be extensively used in Chapters 5 and 7, for the derivation of both analytical and numerical

bounds. For a more complete study, the lecture notes from [33] provide a simple introduction to the field, while the book from [34] allows a deeper understanding of general convex optimization.

2.2.1 Convex cone

As emphasized in Section 2.1.1, quantum theory heavily relies on linear algebra. In quantum cryptography, security analyses often involve optimizing over semidefinite positive objects to find the adversary's optimal cheating strategy. Most of the time, these objects are density matrices, measurement operators, or more general CPTP maps. Semidefinite programming provides a suitable framework for this, as it allows to optimize over semidefinite positive variables, given linear constraints.

More formally, positive semidefinite matrices belong to the *convex cone* $\mathscr{C}$. This is a subset, closed under linear operations with positive ordered coefficients, of a larger vector space $\mathscr{V}$. In other words, any operators X and Y in $\mathscr{C}$ satisfy:

$$X, Y \in \mathscr{C} \Rightarrow \alpha X + \beta Y \in \mathscr{C}, \tag{2.28}$$

for positive scalars α and β. Note that $\mathscr{C}$ is not bounded due to the scaling of α and β. We now define an *affine slice* $\mathscr{A}$, which is the subset of matrices Z of a general vector space $\mathscr{V}$ which satisfy:

$$Z \in \mathscr{A} \Rightarrow \Lambda(Z) = C, \tag{2.29}$$

given a linear map Λ and operator $C \in \mathscr{V}$. Semidefinite programming optimizes convex functions over all operators which lie in the intersection of an affine slice (i.e. satisfying a specific linear constraint) with the convex cone (i.e. the set of positive semidefinite matrices).

2.2.2 Primal problem

A semidefinite program may be defined as a triple (Λ, F, C) where Λ is a Hermitian-preserving CPTP map, and F and C are Hermitian operators living in complex Hilbert spaces $\mathscr{H}_F$ and $\mathscr{H}_C$, respectively.

We start by defining a maximization problem, which will serve as our *primal problem*. The primal problem maximizes a *primal objective function*, $\mathrm{Tr}\left(F^\dagger X\right)$, over all positive semidefinite variables X, given a set of linear constraints expressed as a function of C:

$$\begin{aligned} \text{maximize} \quad & \text{Tr}\left(F^\dagger X\right) \\ \text{s.t.} \quad & \Lambda(X) = C \\ & X \geqslant 0. \end{aligned} \tag{2.30}$$

Any operator X which satisfies these constraints is said to be *primal feasible*, and thus belongs to the following primal feasible set :

$$\mathscr{S}_p = \left\{ X \in \mathscr{H}_F \mid X \geqslant 0,\ \Lambda(X) = C \right\}. \tag{2.31}$$

We define the *primal optimal value* s_p as the supremum over all values taken by the objective function for $X \in \mathscr{S}_p$:

$$s_p = sup\left\{ \text{Tr}\left(F^\dagger X\right) \mid X \in \mathscr{S}_p \right\}, \tag{2.32}$$

Note that when there is no feasible solution, the optimal value may be $+\infty$. If the optimal value can be reached, the *primal optimal solution* is the operator X_p for which the objective function achieves this optimal value.

2.2.3 Dual problem

Semidefinite programs present an elegant dual structure, which associates a dual minimization problem to each primal maximization problem. Effectively, the new variable(s) of the dual problem may be understood as the Lagrange multipliers associated with the constraints of the primal problem (one for each constraint).

Let us start by re-writing problem (2.30) in the following standard form, where *max* and *min* are short for *maximize* and *minimize* (i.e. search for a supremum or infimum over the set, respectively):

$$\begin{aligned} \max_{X \geqslant 0} \quad & \text{Tr}\left(F^\dagger X\right) \\ \text{s.t.} \quad & \Lambda(X) - C = 0. \end{aligned} \tag{2.33}$$

Problem (2.33) presents a single constraint. We therefore introduce a new variable Y, which will serve as the Lagrange multiplier associated with this single constraint. The following step is to minimize the Lagrangian function associated with (2.33) over all Hermitian Y:

$$\begin{aligned} \max_{X \geqslant 0} \min_{Y} \quad & \mathrm{Tr}\left(F^\dagger X\right) - \mathrm{Tr}\left((\Lambda(X) - C)^\dagger Y\right) \\ \text{s.t.} \quad & Y = Y^\dagger. \end{aligned} \tag{2.34}$$

We now re-order this expression in order to isolate a term which depends on Y only:

$$\begin{aligned} \mathrm{Tr}\left(F^\dagger X\right) - \mathrm{Tr}\left((\Lambda(X) - C)^\dagger Y\right) &= \mathrm{Tr}\left(F^\dagger X\right) - \mathrm{Tr}\left(\Lambda^\dagger(X) Y\right) + \mathrm{Tr}\left(C^\dagger Y\right) \\ &= \mathrm{Tr}\left(F^\dagger X\right) - \mathrm{Tr}\left(X^\dagger \Lambda^*(Y)\right) + \mathrm{Tr}\left(C^\dagger Y\right) \\ &= \mathrm{Tr}\left(\left(F - \Lambda^*(Y)\right)^\dagger X\right) + \mathrm{Tr}\left(C^\dagger Y\right), \end{aligned} \tag{2.35}$$

where Λ^* is the unique adjoint map of Λ, i.e. the map which satisfies:

$$\mathrm{Tr}\left(\Lambda^\dagger(X) Y\right) = \mathrm{Tr}\left(X^\dagger \Lambda^*(Y)\right). \tag{2.36}$$

From Eq. (2.35), we see that the second term, $\mathrm{Tr}\left(C^\dagger Y\right)$, depends on Y only. Problem (2.34) is then equivalent to minimizing this term over all Hermitian Y, such that the first term from Eq. (2.35), which depends on both X and Y, does not tend to $+\infty$, i.e. $(F - \Lambda^*(Y)) \leqslant 0$. Without this constraint, the maximization would become trivial, as one could always make $\mathrm{Tr}\left(\left(F - \Lambda^*(Y)\right)^\dagger X\right)$ tend to infinity by picking X large enough, which would always yield an optimal value of $+\infty$. We may finally write the dual problem associated with (2.30) as:

$$\begin{aligned} \text{minimize} \quad & \mathrm{Tr}\left(C^\dagger Y\right) \\ \text{s.t.} \quad & \Lambda^*(Y) - F \geqslant 0 \\ & Y = Y^\dagger. \end{aligned} \tag{2.37}$$

Similarly to the primal problem, we have that any Hermitian operator Y which satisfies these constraints is said to be *dual feasible*, and thus belongs to the following dual feasible set:

$$\mathscr{S}_d = \left\{ Y \in \mathscr{H}_C \mid Y = Y^\dagger,\ \Lambda^*(Y) - F^\dagger \geqslant 0 \right\}. \tag{2.38}$$

We define the *dual optimal value* s_d as:

$$s_p = inf \left\{ \mathrm{Tr}\left(C^\dagger Y\right) | Y \in \mathscr{S}_d \right\}, \tag{2.39}$$

and the *optimal solution* is the operator X_s which allows to achieve this solution. Note that there may be no feasible solution, and in that case, the optimal value can be $-\infty$.

2.2.4 Weak and strong duality

The Lagrange multiplier method allows to find the local extremum of a constrained function. The optimal value s_p of the primal problem therefore upper bounds the optimal value s_d of the dual problem, while the optimal value of the dual lower bounds that of the primal. This property is known as *weak duality*, and may be simply expressed as:

$$s_p \leqslant s_d. \tag{2.40}$$

In many quantum-cryptographic applications however, we wish to ensure that the upper bound derived in the primal problem is *tight*, i.e. that the local maximum is in fact a global maximum for the objective function. The dual problem will help to prove this when there exists *strong duality*:

$$s_p = s_d. \tag{2.41}$$

We will encounter concrete examples of how to apply theses methods in Chapters 5 and 7.

2.3 Quantum optics

2.3.1 Quantum states of light

In quantum cryptography, information is often encoded onto single photon states and other weak-intensity states of light, which cannot be simply described by the wavelike picture: the electromagnetic field must be quantized. For this purpose, we introduce the creation operator $a^\dagger$ and annihilation operator a, which express the creation and destruction of a photon in the electromagnetic field, respectively. Their action can be explicited by considering the *Fock states* (or photon number states), labeled $\{|n\rangle\}_{n=0\to\infty}$. These are eigenstates of the quantum harmonic oscillator of frequency ω, whose energy levels are described by the following Hamiltonian:

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right). \tag{2.42}$$

In this picture, the action of $a^\dagger$ and a can be interpreted as increasing and lowering the number of photons in the quantum field:

$$\begin{aligned} a^\dagger |n\rangle &= \sqrt{n+1}\,|n+1\rangle \\ a\,|n\rangle &= \sqrt{n}\,|n-1\rangle \end{aligned} \tag{2.43}$$

Note that the action of the annihilation operator on the vacuum state $|0\rangle$ gives the zero vector in the given Hilbert space. While the vacuum state should definitely not be confused with the zero vector, applying the annihilation operator on such a state yields the zero vector since no photon can be subtracted from the quantum vacuum. The vacuum state materializes the lowest possible non-zero energy state of the quantum field, which interestingly still presents a fundamental constant energy of value $\frac{\hbar\omega}{2}$:

$$H\,|0\rangle = \frac{\hbar\omega}{2}\,|0\rangle \tag{2.44}$$

We now have a framework which allows the description of single photon states. For practical reasons however (see Chapters 4 and 6), we may also want to encode quantum information onto *coherent states*, which can be easily produced by laser sources. Such states may be expressed in the infinite Fock state basis as as a function of their amplitude α:

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} e^{\alpha a^\dagger}\,|0\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{2.45}$$

It is important to note that this expression describes classical states very well: increasing the amplitude α shifts the peak of the probability distribution to higher number Fock states. At very low amplitudes, however, coherent states are a good candidate to encode quantum information, as they can be reduced to mostly the 0 and 1-photon components, thus mimicking a qubit and a third vacuum dimension.

2.3.2 Linear optics

A linear optical circuit consists of a sequence of unitary operations which preserve the input photon number. The protocols that we implement in this thesis heavily rely on linear optical elements. Here, we introduce the beam-splitter (BS) and polarizing beam-splitter (PBS) transformations, as the well as the phase shift (PS), half wave-plate (HWP) and quarter wave-plate (QWP) transformations.

The BS transformation is the basic component of interferometers, and may also be used to create the two fundamental resources from Section 2.1: superposition and entanglement. It is applied thanks to a partially reflective mirror of transmission probability t and reflection probability r. Its action is best described in terms of creation operators,

in order to avoid the infinite-dimensional representation in the Fock basis from Section 2.3.1. The input creation operators $a_1^\dagger$ and $a_2^\dagger$, corresponding to the incoming spatial modes, in terms of the output operators $a_3^\dagger$ and $a_4^\dagger$, corresponding to the output spatial modes, transform as:

$$\begin{aligned} a_1^\dagger &\to \sqrt{r}\, a_3^\dagger + \sqrt{t}\, a_4^\dagger, \\ a_2^\dagger &\to \sqrt{t}\, a_3^\dagger - \sqrt{r}\, a_4^\dagger. \end{aligned} \tag{2.46}$$

The PBS operation allows to perform a projective polarization measurement: in a given $\{|0\rangle, |1\rangle\}$ polarization basis, a $|0\rangle$-polarized photon will be transmitted, while the orthogonally $|1\rangle$-polarized photon will be reflected.

The PS operation simply introduces a ϕ phase-shift on one of the components of the incoming photonic state. Its action on the creation operators $a_1^\dagger$ and $a_2^\dagger$, associated with two orthogonal components of the input optical mode, reads:

$$\begin{aligned} a_1^\dagger &\to a_1^\dagger, \\ a_2^\dagger &\to e^{i\phi} a_2^\dagger. \end{aligned} \tag{2.47}$$

The HWP operation transforms any linear polarization state (a superposition of $|0\rangle$ and $|1\rangle$ with real coefficients, up to global complex phase) into another linear polarization state. This operation may be realized by sending the photon through an anisotropic crystal, which essentially produces a $\pm\pi$ phase shift on one of the polarization components. This will change the input linear polarization vector to its symmetric with respect to one of the crystal's axes. In terms of creation operators for the two polarization modes $a_H^\dagger$ and $a_V^\dagger$, its action on an input polarization state rotated by an angle θ from the main crystal axis reads:

$$\begin{aligned} a_H^\dagger &\to \cos 2\theta\, a_H^\dagger + \sin 2\theta\, a_V^\dagger, \\ a_V^\dagger &\to \sin 2\theta\, a_H^\dagger - \cos 2\theta\, a_V^\dagger. \end{aligned} \tag{2.48}$$

The QWP operation transforms linear polarization states into circularly-polarized states (a $\pm\pi/2$ relative phase between the $|0\rangle$ and $|1\rangle$ components, up to global complex phase). In terms of creation operators $a_H^\dagger$ and $a_V^\dagger$, its action on the input polarization state, rotated by an angle θ from the main crystal axis, then reads:

$$\begin{aligned} a_H^\dagger &\to \left(\cos^2\theta - i\sin^2\theta\right) a_H^\dagger + (1+i)\cos\theta\sin\theta\, a_V^\dagger, \\ a_V^\dagger &\to (1+i)\cos\theta\sin\theta\, a_H^\dagger + \left(\sin^2\theta - i\cos^2\theta\right) a_V^\dagger. \end{aligned} \tag{2.49}$$

Note that the action of HWP and QWP on the input polarization vector, along with any arbitrary waveplate transformation, may be derived by:

- Expressing the input polarization in the basis described by the crystal's axes.
- Applying the desired phase-shift to one of the components.
- Re-expressing the transformed state back into the original polarization basis.

2.3.3 EIT and slow light

In order to fully demonstrate the quantum money scheme in Chapter 6, we use Electromagnetically Induced Transparency (EIT). This scheme creates and exploits the destructive interference process that occurs between two transitions in a Λ-type atomic system, such as the one presented in Fig. 2.1. The quantum information is effectively stored in the collective excitation of a cloud of cold atoms: the group velocity of the incident light in the cloud is considerably reduced, whilst a transparency window is created which results in no photon absorption. While there exist other mechanisms for light storage in atomic ensembles, such as photon echo schemes [35], or using other platforms like single emitters [36, 37], here we simply provide theoretical intuition for how to create EIT in a cloud of atoms. Note that a more complete derivation of the dark state phenomenon may be found in [38], while a thorough interpretation of slow light can be found in [39].

We provide a semi-classical treatment of the dynamics of the Λ-system, displayed in Fig.2.1: the three-level atomic system is treated as a fully quantum system, while the incident electromagnetic fields are treated as classical waves. We assume that the $|1\rangle \rightarrow |2\rangle$ transition is forbidden. For simplicity, we neglect the decay rates from the upper level to the lower levels caused by spontaneous decays and dephasing, as well as the decays in the two ground levels.

The total Hamiltonian describing the time evolution of the driven system may be written as a sum of the constant unperturbed atomic Hamiltonian H_a, and the interaction Hamiltonian $H_i(t)$, which describes the dynamics due to the interaction with the electromagnetic fields:

$$H(t) = H_a + H_i(t) \tag{2.50}$$

Considering the eigenbasis $\{|1\rangle, |2\rangle, |3\rangle\}$, with energy eigenvalues $\hbar\omega_1$, $\hbar\omega_2$, and $\hbar\omega_3$, respectively, allows to express the unperturbed atomic Hamiltonian as:

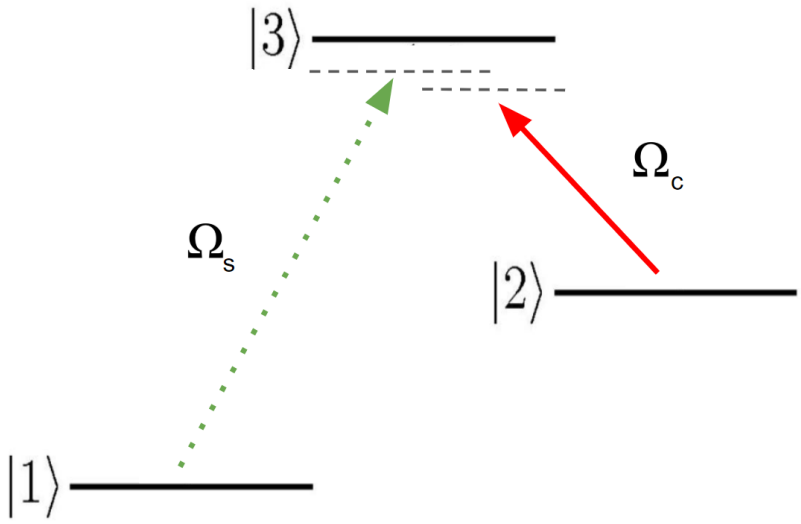


Figure 2.1: **Schematic configuration of the atomic Λ-system.** Level $|3\rangle$ is considered as the excited state, while levels $|1\rangle$ and $|2\rangle$ are the two ground states, which are not coupled to one another. A weak signal field with Rabi frequency Ω_s drives the $|1\rangle \rightarrow |3\rangle$ transition, whilst a stronger control field with Rabi frequency Ω_c drives the $|2\rangle \rightarrow |3\rangle$ transition.

$$H_a = \hbar\omega_1 |1\rangle\langle 1| + \hbar\omega_2 |2\rangle\langle 2| + \hbar\omega_3 |3\rangle\langle 3|. \tag{2.51}$$

Let us now derive a simple expression for the interaction Hamiltonian. In order to store and retrieve quantum information from a Λ-type system, the presence of two electromagnetic fields is required. The first one, which we call the *signal field*, is a weak electromagnetic field which drives the $|1\rangle \rightarrow |3\rangle$ transition. In our experiment, this field actually contains the quantum information that we wish to store. The second one is labelled the *control field*, and drives the $|2\rangle \rightarrow |3\rangle$ transition. It is a much stronger field which allows to steer the Λ system such that the quantum information from the signal field is mapped onto the atomic state, and then retrieved.

We first assume that the wavelength λ of the incident light is much larger than the radius of the atom. This assumption, known as the dipole approximation, allows us to discard the spatial part of the incident electric fields. The total electric field applied on the atom is then the sum of the signal and control fields, which oscillate with angular frequency ω_s and ω_c and amplitudes E_s and E_c, respectively:

$$\vec{E}(t) = \vec{E}_s \cos(\omega_s t) + \vec{E}_c \cos(\omega_c t). \tag{2.52}$$

We now define the *dipole moment*, which occurs when the center of the total positive charge and the center of the total negative charge do not spatially overlap. Assuming that the total atomic dipole moment $\vec{D}$ is aligned with the electric field $\vec{E}$ allows to write the interaction Hamiltonian, defined as $H_i(t) = -\vec{D} \cdot \vec{E}(t)$, in the following way:

$$H_i(t) = -e\hat{r}E(t), \tag{2.53}$$

where $E(t) = E_s \cos(\omega_s t) + E_c \cos(\omega_c t)$. The larger the distance between the center of the positive and negative charges, described by $\hat{r}$, the higher the dipole moment. As in many three-level systems, an interesting feature is that the dipole transition $|1\rangle \rightarrow |2\rangle$ is forbidden due to the specific selection rules of the physical system. This will be of use to create EIT, and implies that the elements of $\hat{r}$ associated with this transition satisfy $r_{12} = r_{21} = 0$. Furthermore, we assume no permanent dipole on the atom, which is true for atoms such as Rubidium, and implies $r_{11} = r_{22} = r_{33} = 0$. This allows a simple expression of the interaction Hamiltonian from Eq. (2.53):

$$H_i(t) = -eE(t)(r_{13} |1\rangle \langle 3| + r_{23} |2\rangle \langle 3| + cc.) \tag{2.54}$$

We now apply a unitary transformation $U_i(t)$ to $H_i(t)$, which allows to work in the interaction picture:

$$U_i(t) = e^{i\omega_1 t} |1\rangle \langle 1| + e^{i\omega_2 t} |2\rangle \langle 2| + e^{i\omega_3 t} |3\rangle \langle 3| \tag{2.55}$$

This picture allows both the states and the operators to carry a time-dependence. We may then express the cosines from $E(t)$ in their exponential form and expand out all terms from $U_i H_i U_i^\dagger(t)$, which can be gathered in fast and slow-rotating terms. Since the signal field drives the $|1\rangle \rightarrow |3\rangle$ transition, the fast-rotating terms are those which contain the expression $e^{-i(\omega_1 - \omega_3 + \omega_s)t}$, since $\omega_1 - \omega_3 + \omega_s \approx 2\omega_s$. One the other hand, the terms which contain the expression $e^{-i(\omega_1 - \omega_3 - \omega_s)t}$ rotate very slowly since, $\omega_1 - \omega_3 - \omega_s \approx 0$. So we may use the rotating wave approximation to discard the fast-rotating terms, as these evolve much faster than the dynamics we are interested in. Applying a similar reasoning to the control field and the $|2\rangle \rightarrow |3\rangle$ transition allows to drop the other fast-rotating terms containing the expression $e^{-i(\omega_2 - \omega_3 + \omega_c)t}$. We then apply the unitary $U_i(t)$ again to transform back to the original picture. The new interaction Hamiltonian may then be written:

$$H_i(t) = -\frac{1}{2} e \left(r_{13} E_s e^{i\omega_s t} |1\rangle \langle 3| + r_{23} E_c e^{i\omega_c t} |2\rangle \langle 3| + cc. \right) \tag{2.56}$$

We now recall the general expression for the oscillations' Rabi frequency Ω_d in terms of the dipole magnitude $|\vec{D}|$ and the driving electric field amplitude E_d:

$$\Omega = \frac{1}{\hbar} E_d |\vec{D}|. \tag{2.57}$$

We substitute the two Rabi frequencies Ω_s and Ω_c in Eq. (2.56) and add this contribution to the unperturbed Hamiltonian H_a to get the following expression for the total Hamiltonian:

$$H(t) = \hbar\omega_1 |1\rangle\langle 1| + \hbar\omega_2 |2\rangle\langle 2| + \hbar\omega_3 |3\rangle\langle 3| - \frac{\hbar\Omega_s}{2} e^{i\phi_s} e^{i\omega_s t} |1\rangle\langle 3| - \frac{\hbar\Omega_c}{2} e^{i\phi_c} e^{i\omega_c t} |2\rangle\langle 3| + cc. \tag{2.58}$$

where ϕ_s and ϕ_c are the phases of the dipoles driven by the signal and control fields, respectively. Finally, we attempt to remove all time-dependence by applying a unitary $\widetilde{U}(t)$ which transforms to the so-called co-rotating basis, which we label $\{|\widetilde{1}\rangle, |\widetilde{2}\rangle, |\widetilde{3}\rangle\}$. This unitary may be expressed as:

$$\widetilde{U}(t) = e^{-i\phi_s} e^{-i\omega_s t} |\widetilde{1}\rangle\langle 1| + e^{-i\phi_c} e^{-i\omega_c t} |\widetilde{2}\rangle\langle 2| + |\widetilde{3}\rangle\langle 3|. \tag{2.59}$$

The transformed Hamiltonian $\widetilde{H}(t)$ must still satisfy the Schrödinger equation, which governs the dynamics of all quantum systems:

$$\widetilde{H}|\widetilde{k}\rangle = i\hbar\frac{\partial}{\partial t}|\widetilde{k}\rangle = \left(i\hbar\frac{\partial\widetilde{U}}{\partial t}\widetilde{U}^\dagger + \widetilde{U}\widetilde{H}\widetilde{U}^\dagger\right)|\widetilde{k}\rangle. \tag{2.60}$$

where $|\widetilde{k}\rangle \in \{|\widetilde{1}\rangle, |\widetilde{2}\rangle, |\widetilde{3}\rangle\}$. Solving Eq. (2.60) for $\widetilde{H}$ allows to derive the final time-independent expression for $\widetilde{H}$ in the co-rotating basis. We express this in matrix form so that the significance of each matrix element is clear:

$$\widetilde{H} = \frac{\hbar}{2}\begin{bmatrix} 2(\omega_1+\omega_s) & 0 & -\Omega_s \\ 0 & 2(\omega_2+\omega_c) & -\Omega_c \\ -\Omega_s & -\Omega_c & 2\omega_3 \end{bmatrix} \tag{2.61}$$

In order to explain the EIT process, we now give the energy eigenvalues and their corresponding eigenvectors for the interaction component of this full Hamiltonian (the unperturbed Hamiltonian only shifts the eigenvalues by the intrinsic energy of the atomic levels):

$$E_\pm = \pm\hbar\Omega_0 \qquad\qquad |\Psi^\pm\rangle = \frac{\Omega_s|\widetilde{1}\rangle + \Omega_c|\widetilde{2}\rangle \mp \Omega_0|\widetilde{3}\rangle}{\sqrt{2}\Omega_0} \tag{2.62}$$

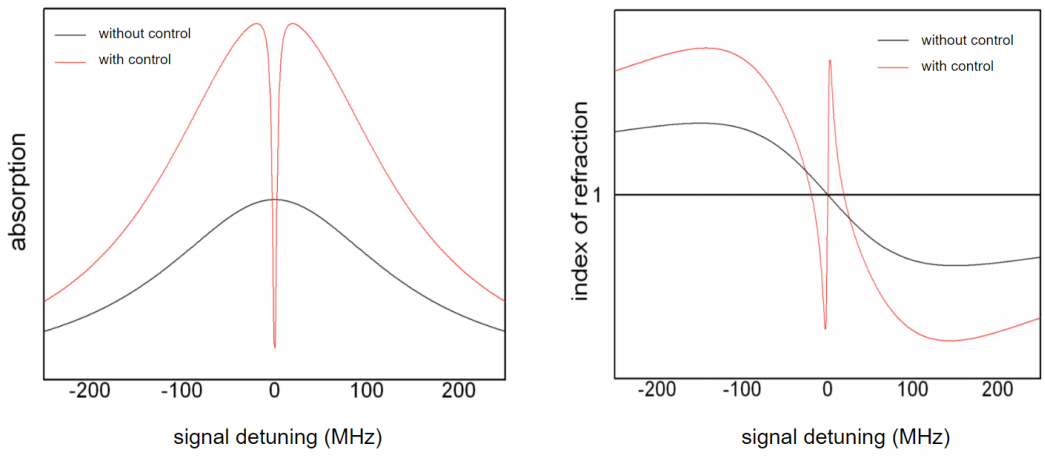


Figure 2.2: **Real and imaginary parts of first-order susceptibility $\chi^{(1)}$.** These are plotted as a function of signal detuning Δ. The real part of $\chi^{(1)}$ corresponds to the dispersion profile of the medium, while the imaginary part corresponds to the absorption profile. The red dotted lines indicate the profiles without the presence of a control field, and the solid black lines indicate the new profiles when the control beam is applied. All units are arbitrary.

$$E_d = 0 \qquad |\Psi^d\rangle = \frac{\Omega_s |\widetilde{1}\rangle - \Omega_c |\widetilde{2}\rangle}{\Omega_0} \tag{2.63}$$

where we define $\Omega_0 = \sqrt{\Omega_s^2 + \Omega_c^2}$. Eq. (2.63) shows that one of the interaction Hamiltonian's eigenstates, which we label $|\Psi^d\rangle$, is not coupled to the third state by the incident field. Any population decaying from the excited state to the $|\Psi^d\rangle$ state will therefore remain trapped, without ever getting excited back to the third state. Such a state is known as a dark state, as it cannot interact with light and so does not present any photon absorption: transparency has effectively been induced by applying two near-resonant fields to the three-level system. From Eq. (2.63), it is also evident that slowly turning off the control field (i.e. $\Omega_c \to 0$) causes the dark state to slowly evolve towards the $|\widetilde{2}\rangle$ state. When the information must be retrieved, the control field is switched back on such that the state $|\widetilde{3}\rangle$ is coupled to the light field again. This process is responsible for the storage and retrieval of quantum information.

We now turn to a more optical interpretation of EIT in a cloud of N cold atoms, each bearing the same Λ-type structure. Here, the response of the atomic ensemble to the incident electric field can be characterized by its first-order susceptibility $\chi^{(1)}$, which is a dimensionless proportionality constant describing the extent to which the medium polarizes due to the presence of an electric field:

$$\chi^{(1)} = \frac{N}{V}\frac{|d_{31}|^2}{\epsilon_0}\frac{i\left(i\Delta+\gamma_{21}\right)}{\left(i\Delta+\gamma_{31}\right)\left(i\Delta+\gamma_{21}\right)+\Omega_s^2} \tag{2.64}$$

where $\Delta = \omega_1 - \omega_3 - \omega_s$ is the signal detuning, d_{31} is the dipole moment for the $|3\rangle \rightarrow |1\rangle$ transition, γ_{ij} is the decoherence rate for the $|i\rangle \rightarrow |j\rangle$ transition, and V is the volume occupied by the N atoms. As shown in Fig. 2.2, plotting the real part of $\chi^{(1)}$ as a function of Δ provides the dispersion profile of the medium, while the imaginary part provides the absorption profile. The effects of the creation of a dark state are therefore explicited: the absorption can be decreased significantly around zero detuning, which explains the transparency effect. Furthermore, the dispersion is also significantly increased around zero detuning. By relating this quantity to the medium's refractive index $n(\omega)$, and recalling the expression for the light's phase and group velocities v_p and v_g as a function of $n(\omega)$, allows to derive the following expression:

$$v_p \approx c \qquad\qquad v_g \approx \frac{c}{1+\frac{N}{\Omega_s^2}\frac{\omega_{31}|D_{31}|^2}{2\epsilon_0 V}} \tag{2.65}$$

where c is the speed of light in vacuum. The phase velocity of the light is more or less preserved, but it is interesting to see that the group velocity can be significantly decreased by increasing the atomic density N/V and controlling the energy of the fields. The signal light is therefore slowed down, which results in effective storage of the information.

CHAPTER 3

QUANTUM CRYPTOGRAPHY

3.1 Foundations of information-theoretic security

3.1.1 Conjugate coding

In the early 70s, Stephen Wiesner proposed a novel idea in a paper entitled *Conjugate Coding*, which was published 10 years later [5]. He suggested that the laws of quantum mechanics could be used to achieve information-theoretic security in specific cryptographic tasks. One famous example is the unforgeable quantum money application, which this thesis aims to implement, and for which a full introduction is provided in Section 3.2. This idea paved the way to the famous BB84 quantum key distribution protocol [7], which we shall discuss further in Section 3.3.

The concept of conjugate coding is based on the uncertainty principle, which bears no classical analogue. The uncertainty principle states that, for a pair of conjugate variables x_1 and x_2 describing two different properties of a quantum system, decreasing the uncertainty on the value of one observable increases the uncertainty on the other. Recalling Section 2.1.3, this occurs when the variables do not commute, i.e. $[x_1, x_2] \neq 0$. In this way, performing a measurement to learn the exact value of one observable completely destroys the information on the value of the other observable. More formally, the uncertainty principle may be described by the following product:

$$\Delta x_1 \Delta x_2 \geqslant C, \tag{3.1}$$

where Δx_i is the uncertainty (variance) of observable x_i and C is a strictly positive constant, whose value depends on the specific uncertainty product considered. This law applies to position and momentum, or time and energy in quantum mechanics. It also applies to the outcomes of measurements performed in conjugate bases, and this provides the first principle of quantum security. Let us consider the pure quantum states $|0\rangle$ and $|1\rangle$, eigenstates of the Pauli σ_z operator from Eq. (2.7), as well as the following coherent superpositions of $|0\rangle$ and $|1\rangle$:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{3.2}$$

Since $|+\rangle$ and $|-\rangle$ are eigenstates of the Pauli σ_x operator, and σ_z and σ_x do not commute, then the uncertainty on the eigenvalue obtained upon measurement in either basis obeys the uncertainty principle. In this way, a party willing to conceal a bit may decide to randomly encode bit 0 in either the $|0\rangle$ or $|+\rangle$ state, and bit 1 in either the $|1\rangle$ or $|-\rangle$ state. The value of the bit is then partially hidden, provided that the adversary does not know the preparation basis. Performing a projective measurement in one basis will then completely destroy any information encoded in the other basis. This provides a type of security which can never be achieved with computational assumptions: *information-theoretic security*. That is, unlike most classical protocols in which assumptions are made on the computational power of the adversary to perform a hard operation, quantum cryptography can provide a much higher level of security in which none of these assumptions are required. Once again, security in this setting assumes that quantum theory provides a correct description of our physical world.

3.1.2 No-cloning theorem

The no-cloning theorem embodies a fundamental difference between classical and quantum information, and represents the second founding principle of quantum cryptography. In fact, it is a more general and abstract way of stating the uncertainty principle, and also allows for conjugate coding. The theorem states that an unknown quantum system cannot be perfectly copied with unit probability. This is in contrast with the classical world, in which a bit of information may be read or measured without destroying its properties, and hence reproduced an infinite amount of times with no error. This property arises once again from the linearity of quantum mechanics described in Section 2.1.1, and the proof may be derived by contradiction.

Let us consider a two-system Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$ spanned by $\{|0\rangle_A, |1_A\rangle, |0\rangle_B, |1\rangle_B\}$. The pure state $|\psi\rangle$ that we wish to copy lives in $\mathscr{H}_A$, while a qubit is initialized in the $|0\rangle_B$ state on $\mathscr{H}_B$. Perfect cloning implies that there exists a unitary operator U which transforms this initial state to two identical copies of state $|\psi\rangle$:

$$U|\psi\rangle_A \otimes |0\rangle_B = |\psi\rangle_A \otimes |\psi\rangle_B . \tag{3.3}$$

There exists such a cloning unitary for the basis eigenstates, since it is always possible to discriminate them perfectly, and hence create any number of perfect copies. This implies that:

$$\begin{aligned} U|0\rangle_A \otimes |0\rangle_B &= |0\rangle_A \otimes |0\rangle_B , \\ U|1\rangle_A \otimes |0\rangle_B &= |1\rangle_A \otimes |1\rangle_B . \end{aligned} \tag{3.4}$$

Expressing $|\psi\rangle$ as a general qubit state, we may then rewrite the left-hand side of (3.3) as:

$$\begin{aligned} U\left(\alpha|0\rangle_A + \beta|1\rangle_A\right) \otimes |0\rangle_B &= \alpha U|0\rangle_A \otimes |0\rangle_B + \beta U|1\rangle_A \otimes |0\rangle_B \\ &= \alpha|0\rangle_A \otimes |0\rangle_B + \beta|1\rangle_A \otimes |1\rangle_B . \end{aligned} \tag{3.5}$$

Let us now rewrite the right-hand side of (3.3):

$$\begin{aligned} |\psi\rangle_A \otimes |\psi\rangle_B &= \left(\alpha|0\rangle_A + \beta|1\rangle_A\right) \otimes \left(\alpha|0\rangle_B + \beta|1\rangle_B\right) \\ &= \alpha^2|0\rangle_A \otimes |0\rangle_B + \alpha\beta|0\rangle_A \otimes |1\rangle_B + \beta\alpha|1\rangle_A \otimes |0\rangle_B + \beta^2|1\rangle_A \otimes |1\rangle_B . \end{aligned} \tag{3.6}$$

Comparing the results from (3.5) and (3.6) allows to conclude that the cloning operation proposed in (3.3) is not possible for any arbitrary input qubit state $|\psi\rangle_A$. The additional cross terms in (3.6) arise from the non-linear aspect of the cloning operation, which is forbidden in a linear theory such as quantum mechanics.

3.2 Quantum money

3.2.1 Classification

The aim of a quantum money protocol is to protect against forgery of cheques, banknotes or credit cards by associating them with a secret key encoded into quantum-mechanical states. By appropriately using conjugate coding, information-theoretic security is then guaranteed by the uncertainty principle and the no-cloning theorem (Section 3.1). Here,

we briefly define what we mean by cheques, credit cards and banknotes in the quantum setting, and propose a classification of quantum money schemes, summarized in Fig. 3.1. All quantum money schemes involve a mint, which generates the quantum money state, stores it in a quantum memory and hands it to a client. Depending on the type of key and verification, the presence of other parties will vary.

In a *private-key* money scheme, the quantum state is encoded according to a secret classical key, which is known by the mint and the verification bank only. The key contains a sequence of secret information bits, as well as a sequence of secret basis bits, which indicate the random preparation basis of each information bit. This ensures that a dishonest client willing to duplicate the money state will introduce errors in at least one of two states, due to no-cloning (Section 3.1.2). Upon verification, these errors will be detected by the bank, which measures each sub-system of the money state in the correct basis and compares the measurement outcomes with the secret key.

Two types of verification may be used in a private-key scheme: quantum and classical verification. The original scheme, introduced by Wiesner around the mid 70s, and later published in [5], involved *quantum verification*: the client has to send the entire quantum money state to a distant bank for verification. In this thesis, this money state will be called a *cheque*, since the state must physically reach the bank for it to be declared authentic. Such quantum money schemes are described in Section 3.2.2. We note that, in [40], the term *cheque* is also used for private-key money schemes with quantum verification, but with the extra property that the issuer of the cheque should be identified. This requires the combination of quantum money with digital signature schemes.

From an implementation perspective, quantum verification is not practical, as it subjects the money state to unwanted errors and losses due to imperfect, long-distance transmission. This may cause an honest money state to be rejected by the bank. Much later, Gavinsky therefore introduced quantum money with *classical verification* [41], in which the measurements are performed locally by a vendor, and the distant bank verifies the authenticity of the money state through classical communication only. We shall refer to such schemes as *credit card* schemes, since the vendor performs the measurements locally with a payment terminal (measurement setup), and classically transfers the outcomes to a distant bank for verification. Such quantum money schemes are described in Section 3.2.3. As we shall see in Chapter 5, this raises the question of whether the payment terminal should be trusted or not, as it may potentially help the client in double spending.

For completeness, we finally introduce the concept of *public-key* quantum money,

private-key (unconditional security)	quantum verification	 cheque
	classical verification	 credit card
public-key (computational security)	any verification	 banknote

Figure 3.1: **Simple classification of quantum money schemes.** The first column indicates which type of key is used, as well as the level of security it achieves. The second column indicates the corresponding type of verification. The third column indicates the analogy which may be drawn with classical payment methods.

which will not be studied in this thesis. This refers to *banknotes* (i.e. real, physical money): a mint generates a quantum banknote according to a public key, which may then freely circulate amongst clients and vendors. However, any party must be able to verify the authenticity of a banknote without requiring communication with a bank. It has been shown that, unlike private-key schemes, such schemes cannot achieve information-theoretic security, and must therefore rely on computational assumptions. However, they still provide a security advantage over the classical world for physical money, as briefly explained in Section 3.2.4.

3.2.2 Private-key with quantum verification

In Wiesner's original scheme [5], the mint generates a random secret classical key $k^{(s)}$ and encodes it according to a secret classical basis key $b^{(s)}$. The quantum cheque state associated to public serial number s and secret classical keys $k^{(s)}$ and $b^{(s)}$ may then be written:

$$|€^{(k,b)}\rangle = \bigotimes_{j=1}^{n} |\psi_j^{(k,b)}\rangle, \tag{3.7}$$

where $|\psi_j^{(k,b)}\rangle \in \{|+\rangle, |+i\rangle, |-\rangle, |-i\rangle\}$. More specifically, bit $k_j^{(s)}$ is encoded in the σ_x basis when $b_j^{(s)} = 0$, and in the σ_y basis when $b_j^{(s)} = 1$.

The mint stores $|€^{(k,b)}\rangle$ in a quantum memory and hands it to a client. When a transaction must be performed, the client sends all n qubits of the cheque to the bank

for verification. The bank, who shares the secret classical keys with the mint, measures each of the n qubits of $|\in^{(k,b)}\rangle$ in the correct preparation basis, and checks whether all outcomes coincide with $k^{(s)}$. If there are no errors, the cheque is deemed authentic and the transaction can proceed. In the honest scenario, this occurs with probability $p_h = 1$. If there are some errors, the bank rejects the payment. Note that, unlike the original Wiesner proposal, the bank should NOT send the state back to the client in any case, as sending the quantum state back and forth can lead to powerful adaptive attacks [42].

This protocol guarantees information-theoretic security against counterfeiting thanks to the principles of Section 3.1: it is strictly impossible for a counterfeiter to produce two copies of the initial quantum cheque which both pass the verification in two separate branches of the bank. For a cheque consisting of a single state (i.e. $n = 1$), the dishonest strategy only succeeds with probability $p_d \leqslant 3/4$ [5, 32].

This upper bound is reached for a strategy in which the dishonest client measures the unknown state randomly in one of the two conjugate bases. If basis σ_i was picked, and outcome j is measured, the client then encodes bit j into two identical quantum states prepared in the σ_i basis. When σ_i is the correct preparation basis, the client succeeds with probability 1. If it is the incorrect preparation basis, they succeed with probability 1/2 only. Since each basis is picked with probability 1/2, the total winning probability indeed reads $p_d = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$.

For a cheque consisting of n states, the honest success probability remains 1, while the probability that a dishonest client succeeds can be made arbitrarily close to 0. This is because the client cannot succeed any better in performing a general attack on the n states. The best strategy is therefore to perform the same attack on each individual qubit, which leads to $p_d(n) \leqslant \left(\frac{3}{4}\right)^n$. This property arises from the product rule of semidefinite programs [32, 43, 44]. The protocol therefore satisfies the following properties:

$$\begin{aligned} p_h(n) &= 1 && \text{correctness} \\ p_d(n) &\leqslant \left(\frac{3}{4}\right)^n && \text{security} \end{aligned} \tag{3.8}$$

3.2.3 Private-key with classical verification

Classical verification was originally proposed by Gavinsky in [41], and was later extended to simpler quantum states in [45]. As previously highlighted, we shall refer to such schemes as *quantum credit card* schemes, since the verification proceeds through an intermediate payment terminal, which sends classical data to a distant bank. The

	Mint	Client	Terminal	Bank
(i)	H	H	H	H
(ii)	H	D	H	H
(iii)	H	D/H	D	H
(iv)	D	D/H	D	H
(v)	D	D/H	D/H	D

Table 3.1: **Adversarial scenarios for quantum money with classical verification.** Each scenario is expressed in terms of honest (H) and dishonest (D) parties. Cases denoted by D/H are indistinguishable to the bank.

basic idea behind the removal of quantum verification is that the bank can verify the authenticity of the credit card through classical challenge questions only.

In the work from [29], we summarize all possible adversarial scenarios which may occur in such protocols (involving a mint, a client, a payment terminal and a bank). This summary is displayed in Table 3.1. Scenario (i) involves honest parties only. In this case, the property of interest is the correctness c of the protocol: the credit card must always be verified with probability $c = 1$.

Scenario (ii) relates to cases where the credit card is verified through classical communication, but the payment terminal which performs the local quantum measurements follows the protocol honestly. In this thesis, Chapter 4 proposes a proof-of-principle implementation of this scenario.

Scenario (iii) extends the security to cases in which the payment terminal cannot be trusted, and is therefore not constrained to follow the protocol's measurements: it can perform any POVM or quantum operation on the initial quantum credit card state. In Chapter 5, we propose a rigorous and practical security proof for Scenario (iii). Scenario (ii) is also studied again in a semi-device-independent regime, in which the squashing models from [46] are used to strongly limit the assumptions on the terminal detectors, while both *(iii)* and *(iv)* are by definition semi-device-independent. Note that the notion of semi-device-independence will be introduced in Chapter 5.

Scenario *(iv)* treats cases in which all parties are dishonest, except the bank. This will not be treated in this thesis, but was very recently studied in [47], and was shown to be impossible without assumptions on the dimensionality of the quantum states and the type of attacks allowed. Finally, scenario *(v)* is of no cryptographic interest since none of the parties are honest.

3.2.4 Public-key

In the classical world, money schemes are impossible with information-theoretic security and are therefore based on computational assumptions. We have just seen that, provided the key is private, then information-theoretic security may be achieved with quantum mechanics. Regarding quantum banknotes, such public-key schemes cannot base their security solely on the no-cloning theorem, even in the quantum world. They require some computational assumptions, involving knot problems or quantum obfuscation for instance [48–53]. This computational security is still interesting since in the classical world there can be no notion of mathematical security for banknotes; their security is based only on the fact that it is difficult for a counterfeiter to copy a banknote due to its intricate coloring and hologram design. The recent experimental work from [53] has shown how such quantum banknotes can be constructed on-the-fly but also forged.

3.3 Quantum key distribution

3.3.1 BB84 protocol

A year after Wiesner's seminal work was published [5], and after closely working with him on the proposal of unforgeable quantum subway tokens [54], Bennett and Brassard proposed the first idea for quantum key distribution (QKD): the BB84 protocol [7]. This has been the most widely studied and implemented quantum-cryptographic task up to now [13, 14]. Since some of the security tools used in this thesis were originally designed for quantum key distribution, we give here a brief outline of the protocol. Unlike quantum money or quantum coin flipping however, the two parties involved in QKD trust each other: Alice and Bob wish to establish a common secret key over a public channel. However, they want to ensure that the unwanted presence of an eavesdropper, Eve, on the channel is always detected. Information-theoretic security for such a task may be achieved with Wiesner's conjugate coding principle (Section 3.1.1). Once a secret key has successfully been established, Alice and Bob may use it to encrypt a secret message through one-time padding [6]. This encryption technique requires a secret key whose length is at least equal to the message length.

As displayed in Fig. 3.2, Alice starts by encoding the n bits of the secret key she wishes to share into n qubit states (here, photon polarization states). She randomly picks the encoding basis for each qubit (σ_z or σ_x), and stores this classical information. Bit 0 is therefore randomly encoded in either $|0\rangle$ or $|+\rangle$, while bit 1 is randomly encoded in $|1\rangle$ or

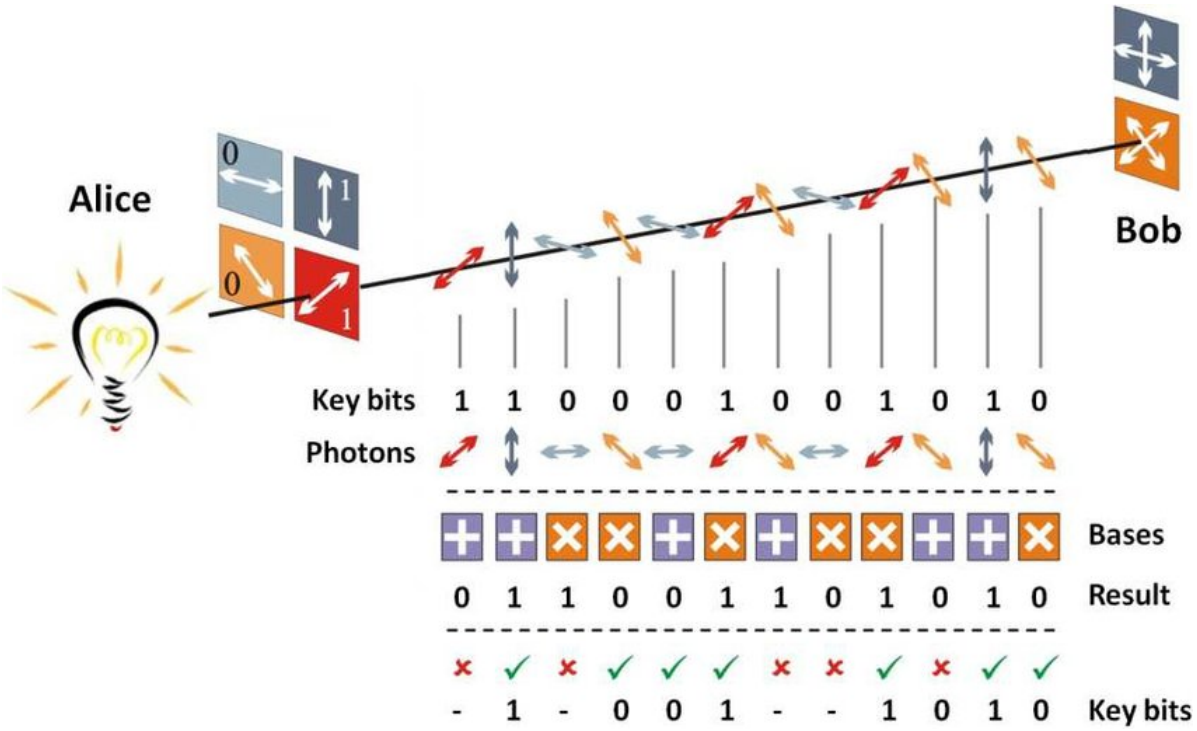


Figure 3.2: **Illustration of the BB84 protocol steps with polarized photons.** Alice encodes her secret key bits into a sequence of polarized photon states, randomly prepared in the σ_z or σ_z basis. She sends the photons to Bob over a quantum channel. Upon reception, Bob picks a measurement basis at random for each photon, and records the measurement results. Over a classical channel, Alice and Bob then dismiss all results for which the basis picked by Bob does not match Alice's initial preparation basis. Such cases are indicated by red crosses. Only the results for which the preparation and measurement bases match (green ticks) will constitute the final secret key. *For the image source, please see [55].*

$|-\rangle$. The states are sent over a quantum channel to distant Bob, who does not know the encoding basis, and thus randomly measures each qubit in either σ_z or σ_x. He records each qubit's measurement basis, along with the associated measurement outcomes.

Once the quantum communication stage is over, Alice and Bob proceed to a classical reconciliation stage: Bob communicates his sequence of measurement bases (without the measurement outcomes) to Alice. After comparing it with her stored sequence, Alice reports to Bob the elements for which her preparation basis does not match Bob's measurement basis. They both agree to dismiss all bits which correspond to a basis mismatch from the final key.

After basis reconciliation, Alice and Bob then compare a pre-agreed random subset of their corrected key to ensure that all bits match. If any of the bits disagree, they may

conclude on the presence of Eve and abort the protocol. If all bits agree, the key has then successfully been established, and they may use it to encrypt a secret message. Note that an additional stage, known as privacy amplification, is required in the noisy setting, in order to decrease the amount of information that Eve acquires from Alice and Bob's classical communication [56].

For the security definition, let us now consider the following tripartite states:

- $\rho_{ABE} = \left(\sum_{k=1}^{N} \frac{1}{N} |k\rangle \langle k|\right)_{AB} \otimes \rho_E$: the secret key state shared by Alice and Bob, described by a mixture over N possible classical keys $|k\rangle$, is totally uncorrelated from Eve's quantum state, labeled ρ_E,
- σ_{ABE}: Alice, Bob and Eve share a (partially) correlated state.

When the three parties share ρ_{ABE}, Eve gains no information about the key. When the three parties share a partially correlated state σ_{ABE}, then Eve gains some information about the key. The security requirement for QKD may be expressed as an upper bound on the trace distance between these two states:

$$\frac{1}{2}||\sigma_{ABE} - \rho_{ABE}||_1 \leqslant \epsilon, \tag{3.9}$$

where ϵ is the security parameter, which should be chosen as small as possible, given a specific protocol and implementation constraints. We note that in practice, losses and noise will allow adversaries to cheat differently in quantum money and in quantum key distribution schemes. Practical attacks in quantum money will be treated rigorously in Chapter 5. For practical attacks in QKD, the works from [14, 57] provide a good overview.

3.3.2 Other variants

While implementations of BB84 have been realized with a multitude of different encodings (polarization, phase, time-bin, etc...), using discrete degrees of freedom of coherent states [58, 59], we note the existence of other types of QKD protocols:

- **Entanglement-based QKD [20]**: Alice and Bob establish a secret key by sharing the Bell states from Eq. (2.14). Checking that the correlations are inherently quantum allow them to detect the presence of Eve.
- **Continuous-variable QKD [60]**: Alice and Bob establish a secret key by sending coherent states (Section 2.3.1) instead of qubit states. The information is encoded

on continuous photonic degrees of freedom (electromagnetic field quadratures), and the measurements are also continuous. Eve's presence will introduce excess noise just like in BB84.

3.4 Quantum coin flipping

3.4.1 Strong coin flipping

From a quantum network perspective, the last task that we introduce, two-party coin flipping, is a fundamental cryptographic primitive: it helps in the construction of more complex security tasks.

Strong coin flipping (SCF) allows two distant parties, Alice and Bob, to generate and agree on a random bit. They do not trust each other and wish to ensure that the bit is truly random. We call the coin flip *fair* when two honest parties each win with probability 1/2. On the other hand, security for this task must guarantee that none of the two parties can force the other to declare outcome $i \in \{0,1\}$ with probability higher than $P = \frac{1}{2} + \epsilon^{(i)}$, where $\epsilon^{(i)}$ is the protocol *bias*. In its most general form, SCF does not necessarily involve equal cheating probabilities for both parties, but when it does, the protocol is labelled *balanced*. We define the following upper bounds on Alice and Bob's probabilities of forcing their opponent to declare outcome i:

$$\begin{aligned} P_A^{(i)} &\leqslant \frac{1}{2} + \epsilon_A^{(i)} \quad \text{Alice forces Bob to declare } i \\ P_B^{(i)} &\leqslant \frac{1}{2} + \epsilon_B^{(i)} \quad \text{Bob forces Alice to declare } i \end{aligned} \tag{3.10}$$

The bias ϵ of a given SCF protocol is then defined as the highest of all four biases:

$$\epsilon = \max\left\{\epsilon_A^{(0)}, \epsilon_A^{(1)}, \epsilon_B^{(0)}, \epsilon_B^{(1)}\right\}. \tag{3.11}$$

In the classical world, a naive way of perform SCF with zero bias would involve Alice and Bob generating two random bits x_A and x_B, respectively. They would then simultaneously broadcast their bits at a pre-agreed time, and calculate the outcome of the flip as $(x_A \oplus x_B)$. However, this property requires perfect clock synchronization, which effectively amounts to trusting a third party, such as a GPS for instance. Trusting a third party defies the very purpose of two-party coin flipping, as it is a much stronger assumption. Classically therefore, two-party SCF may only achieve computational secu-

rity, as it requires some form of bit commitment, whose security is based on hardness assumptions.

In the quantum world, it has been shown by Kitaev that information-theoretically secure SCF is possible, but with a fundamental lower bound on the achievable bias [61]:

$$\epsilon \geqslant \frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.207. \tag{3.12}$$

This fundamental no-go theorem appears quite unfortunate, but it still allows to perform fair protocols in which a dishonest party can bias the flip with probability no higher than ≈ 0.707, without requiring any computational assumption. Quantum SCF has been implemented using a variety of different encodings in [62–64]. However, such implementations present fairly high biases which exceed 0.30.

3.4.2 Weak coin flipping

Two-party weak coin flipping (WCF) allows Alice and Bob to agree on a random bit when they both have known, preferred, opposite outcomes. In other words, the outcome of the flip will designate a winner and a loser. In terms of biases and cheating probabilities, WCF may be seen as a more restricted version of SCF for which:

$$\begin{aligned}
&P_A^{(0)} \leqslant \frac{1}{2} + \epsilon_A^{(0)} \quad \text{Alice forces Bob to declare 0} \\
&P_A^{(1)} = 1 \quad \text{Alice forces Bob to declare 1} \\
&P_A^{(0)} = 1 \quad \text{Bob forces Alice to declare 0} \\
&P_B^{(1)} \leqslant \frac{1}{2} + \epsilon_B^{(i)} \quad \text{Bob forces Alice to declare 1}
\end{aligned} \tag{3.13}$$

Note that a protocol which satisfies these conditions is labelled *weak* as two out of four bias parameters remain unconstrained: $\epsilon_A^{(1)}$ and $\epsilon_B^{(0)}$ are both allowed to reach their trivial $\frac{1}{2}$ values. This means that Alice and Bob can always choose to lose with probability $P_A^{(1)} = P_B^{(0)} = 1$. Interestingly however, quantum WCF schemes are crucial to constructing optimal quantum SCF schemes [25], as well as other useful cryptographic primitives such as bit commitment [26].

3.4.3 Unified framework with abort cases

As we shall see in Chapter 7, constructing loss-tolerant weak coin flipping protocols is very challenging, since it allows any dishonest party to declare an abort whenever they

are not satisfied with the outcome of the flip. Furthermore, allowing for abort cases may enable some classical coin flipping protocols to perform better than quantum protocols. This is because increasing the abort probability effectively decreases Alice and Bob's cheating probabilities. We say that the protocol achieves quantum advantage when it provides strictly better bounds than any classical coin flipping protocol (here, this relates to the bias).

In this section, we highlight the conditions on the protocol parameters which enable quantum advantage. We recall the general coin flipping formalism from [65], in which any classical or quantum coin flipping protocol may be expressed as a:

$$CF\left(P_{00},P_{11},P_A^{(0)},P_A^{(1)},P_B^{(0)},P_B^{(1)}\right), \tag{3.14}$$

where P_{ii} is the probability that two honest players output value $i \in \{0,1\}$, $P_A^{(i)}$ is the probability that Dishonest Alice forces Honest Bob to declare outcome i, and $P_B^{(i)}$ is the probability that Dishonest Bob forces Honest Alice to declare outcome i. Note that this formalism takes into account the abort probability, as the correctness P_{ii} may be rewritten:

$$P_{ii} = f(i,a), \tag{3.15}$$

where a is the probability that the protocol aborts when both parties are honest, and f is some function of a. In this formalism, an ideal SCF protocol can then be expressed as a:

$$CF\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right), \tag{3.16}$$

while an ideal WCF may be expressed as a:

$$CF\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1,\frac{1}{2}\right). \tag{3.17}$$

From [65], the condition for which quantum protocols achieve strictly better bounds than classical protocols (Q>C), reads:

$$Q > C \iff \begin{cases} P_A^{(0)} + P_A^{(1)} > 1 \\ P_B^{(0)} + P_A^{(1)} > 1 \end{cases} \tag{3.18}$$

CHAPTER 4

PROOF-OF-PRINCIPLE IMPLEMENTATION OF A QUANTUM CREDIT CARD

4.1 Motivation

Quantum credit card schemes provide the most practical candidate for experiment, since they allow classical verification: the central bank can verify the authenticity of the quantum credit card through a distant payment terminal, which performs local quantum operations only and communicates classically. This avoids long-distance transmission of quantum states through noisy and lossy quantum channels, which can lead to the rejection of honest credit cards.

Historically, quantum money with classical verification was first proposed in [41]: the distant bank verifies the authenticity of the quantum money state by asking some classical challenge questions and ensuring that the answers match the secret key. This was based on the quantum retrieval game (QRG) formalism from [66], while the information was encoded on hidden-matching states [67]. Several rounds of classical communication between the vendor and the bank were required, and implementing such a scheme implied generating high-dimensional entangled states. These impractical requirements were recently dismissed in [68], by proposing to map this high-dimensional encoding on a separable train of phase-encoded coherent states. Independently, a new encoding for classical verification was proposed in [45], making use of the simple $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ states. The latter scheme is the one we aim to implement in this chapter.

As emphasized in Section 3.2.3, classical communication raises the question of whether the bank can always trust the distant terminal to perform the correct quantum measurements and provide the true measurement outcomes. In this chapter, we focus on the practical security analysis and first proof-of-principle implementation of a quantum credit scheme in which the bank trusts its distant terminal. The untrusted terminal treatment is left for Chapter 5. Furthermore, the security analysis is targeted towards the proof-of-concept experiment in which we post-select on losses. While the noisy security analysis is rigorous, we only consider specific loss-dependent attacks, while the general loss-dependent treatment is also left for Chapter 5.

The protocol presented in this chapter builds upon the work in [45] in conjunction with the techniques developed in [44], and uses only pairs of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ states and a single round of classical communication for verification. The elegant quantum retrieval game formalism from [66] allows the payment terminal to choose the measurement basis at random, and also to formulate conditions for correctness and security that can be experimentally tested. These conditions are satisfied experimentally using a practical photonic setup based on polarization encoding of weak coherent states of light, and secure regimes of operation are derived. The experiment includes the full procedure of credit card state generation, readout and verification without a quantum memory. The full experimental demonstration involving genuine quantum storage of the credit card state is left for Chapter 6. Finally, we provide a comparison of our work from [28] with independent work that appeared in [69].

4.2 Protocol and correctness

For simplicity, we start by describing the honest protocol with a quantum credit card consisting of a single state. The mint generates a unique public serial number s, which will serve to identify the credit card when a transaction occurs. It then generates a random secret classical key $k^{(s)}$ consisting of three bits $\{b, c_0, c_1\}$, which collectively identify one of the states from the following set:

$$S_{\text{pair}} = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle, |+0\rangle, |+1\rangle, |-0\rangle, |-1\rangle\}, \tag{4.1}$$

where $|0\rangle$, $|1\rangle$ and $|+\rangle$, $|-\rangle$ are the Pauli σ_z and σ_x basis eigenstates, respectively. Within the secret classical key, $b = 0$ indicates that the first qubit is encoded in the σ_z basis and the second in the σ_x basis, while $b = 1$ indicates that the first qubit is encoded in the σ_x

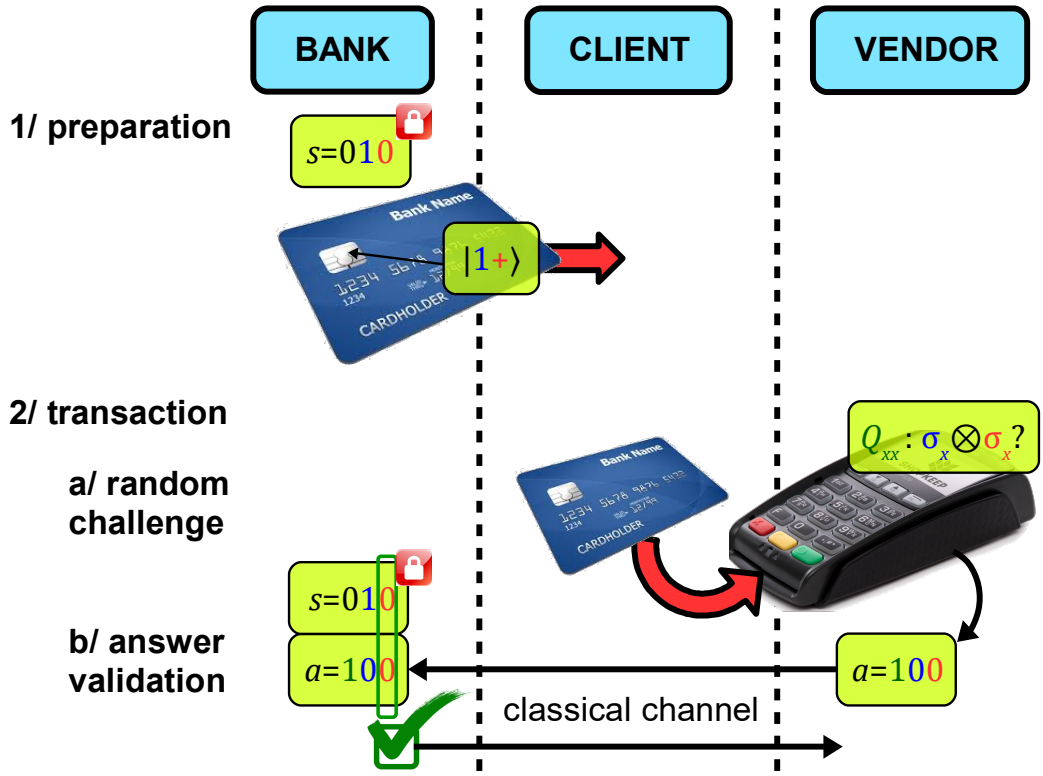


Figure 4.1: **Practical quantum money protocol.** The sequence of interactions between the credit card holder (client), the trusted payment terminal (vendor) and the mint/bank involved in the transaction. In the preparation phase, the mint uses a secret key $k^{(s)}$, associated to public serial number s, to prepare the quantum state loaded on the credit card, which is then handed to the client. In the transaction phase, the vendor randomly selects one out of two challenge questions Q_{zz} or Q_{xx} , measures the qubits accordingly, and sends the classical outcome to the bank, who can then verify the validity of the credit card or detect a forgery attempt.

basis and the second in the σ_z basis. The bits c_0 and c_1 refer to the encoded information, with 0 corresponding to the states $|0\rangle, |+\rangle$ and 1 corresponding to the states $|1\rangle, |-\rangle$.

A transaction consists of three distinct steps, as illustrated in Fig. 4.1. First, the client hands the credit card to the vendor, who chooses at random one of two *challenge questions* and measures the credit card with a trusted payment terminal. The aim here is to perform a measurement on the stored qubit pair in order to provide a correct answer to the randomly selected challenge. As a second step, the vendor sends the measurement outcomes, along with the chosen challenge, to the bank. Finally, the bank verifies the authenticity of the credit card using the secret string $k^{(s)}$ and allows the transaction if and only if the measurement outcomes coincide with the triplet $\{b, c_0, c_1\}$. In the opposite

case, the card is rejected and declared as a counterfeit. The two challenges, which we label Q_{zz} and Q_{xx}, effectively ask the trusted terminal to provide the correct bit c_i for one of the qubits prepared in a specific basis, and a random answer $c_{\bar{i}}$ for the qubit prepared in the other basis:

Q_{zz} = *Provide two bits* c_0 *and* c_1*, such that the bit corresponding to the qubit prepared in the* σ_z *basis is correct.*

Q_{xx} = *Provide two bits* c_0 *and* c_1*, such that the bit corresponding to the qubit prepared in the* σ_x *basis is correct.*

The main idea here is that a valid credit card can always be verified in the ideal case. In order to answer the Q_{zz} challenge, the trusted terminal performs a measurement in the $\sigma_z \otimes \sigma_z$ basis. In order to verify the Q_{xx} challenge, it performs a measurement in the $\sigma_x \otimes \sigma_x$ basis. We denote by c the probability of successfully answering Q_{zz} or Q_{xx}, and name it the *correctness parameter*. In a perfect implementation, c always equals 1 for the above challenges, since measuring both qubits in the σ_z basis always answers the Q_{zz} challenge correctly, and similarly for Q_{xx}. In a realistic implementation, however, c might not be equal to 1 due to system imperfections. It might also take different values, c_{zz} and c_{xx}, depending on whether the Q_{zz} or Q_{xx} challenge is selected by the terminal. In this case, c can be defined as the average of c_{zz} and c_{xx}:

$$c = \frac{c_{zz} + c_{xx}}{2} \tag{4.2}$$

For a fragment of the credit card consisting of n qubit pairs, the vendor's trusted terminal picks only one challenge for the n pairs. It then proceeds to measure the $2n$ qubits in the same basis, before sending the measurement outcomes and the selected challenge to the bank for verification. In an ideal implementation, the probability of accepting an honest credit card fragment remains 1.

4.3 Security

4.3.1 Single qubit pair

Let us now analyze what happens when a dishonest client tries to produce to copies of the single-qubit-pair quantum credit card fragment. The qubit pair is unknown to the client, since the secret key $k^{(s)}$ is private and known by the bank only. The no-cloning theorem (Section 3.1.2) therefore ensures that a dishonest client cannot pass both challenges Q_{zz}

and Q_{xx} at the same time in two separate branches of the bank. This effective cheating challenge, which we label Q_ϵ, may be interpreted as the conjunction of both Q_{zz} and Q_{xx} challenges:

Q_ϵ = *Provide the two correct bits* c_0 *and* c_1.

We denote by ϵ the upper bound on the probability of successfully answering this challenge, and call it the *security parameter*. The value of ϵ was derived in [41, 45] using semidefinite programming techniques, and shown to be 3/4. The set of three challenges Q_{zz}, Q_{xx} and Q_ϵ, which may be answered at best with probability c, c and ϵ, respectively, can be gathered in a 1-out-of-2 (c,ϵ) quantum retrieval game G. Informally, this is a game in which, given a quantum state ρ, one of two possible challenges may be asked. Each challenge may be correctly answered with probability c at most, while the conjunction of both challenges may only be correctly answered with probability ϵ [44].

Two spacelike-separated payment terminals (which cannot communicate with one another) will randomly pick the same challenge with probability 1/2, in which case a dishonest client can apply the honest strategy from Section 4.2 and pass the verification with probability 1. However, these two terminals may also pick different challenges with probability 1/2, in which case a dishonest client cannot pass with probability higher than ϵ. We therefore deduce that the following relation between the correctness and security parameters must hold for game G:

$$c > \frac{\epsilon + 1}{2}. \tag{4.3}$$

4.3.2 Extension to n pairs

A crucial property of game G is that, if one attempts to answer in parallel n such challenges, then one can upper bound the probability that a dishonest client will successfully answer challenge Q_ϵ for all n repetitions by ϵ^n [41]. This bound follows naturally from the product property of semidefinite programs [43, 44]. Such a product bound implies that performing a general attack on the composite Hilbert space of all qubit pairs in the card cannot yield a higher cheating probability than performing an optimal attack on each individual pair.

Starting from a game G for which Eq. (4.3) holds, we may then construct a different game G' that consists of n parallel repetitions of game G. Here again, the vendor chooses at random one of two challenge questions and performs a measurement on all $2n$ qubits accordingly: either $\sigma_z \otimes \sigma_z$ on all n pairs or $\sigma_x \otimes \sigma_x$ on all n pairs. Considering a tolerance parameter $\delta > 0$, we now define the two challenges as: (i) answering the challenge Q_{zz}

correctly for at least a fraction $(c-\delta)$ of the n pairs, and (ii) answering the challenge Q_{xx} for at least a fraction $(c-\delta)$ of the n pairs.

Since the honest strategy for winning game G' can be obtained by performing the same measurement on each of the n pairs individually, then we may use a Chernoff argument [70] to bound the new correctness parameter c'. That is, the number of pairs among the n pairs for which the challenge is answered correctly will be close to its expectation value cn with high probability. In other words, if $X_1,...X_n$ are independent random Bernouilli variables that take the value 1 if the challenge for pair i is passed, then we have that the sum $X=\sum_i X_i$ satisfies:

$$\Pr[X \geq (1-\delta)cn] \geq 1-e^{-\frac{cn}{2}\delta^2}. \tag{4.4}$$

Similarly for the security parameter, the optimal cheating strategy consists in performing the same attack on each pair individually. We may then use the same Chernoff argument to bound the new security parameter ϵ' : for n pairs, with very high probability the number of pairs among these n pairs for which the challenge is answered correctly is very close to its expectation value ϵn. In other words, if $Y_1,...Y_n$ are independent random Bernouilli variables that take the value 1 if the challenge for pair i is passed, then the sum $Y=\sum_i Y_i$ satisfies:

$$\Pr[Y \geq (1+\delta)\epsilon n] \leq e^{-\frac{\epsilon n}{3}\delta^2}. \tag{4.5}$$

We may then label the lower and upper bounds from Eqs. (4.4) and (4.5) in terms of the correctness c' and security ϵ' of game G':

$$c' = 1-e^{-\frac{cn}{2}\delta^2} \text{ and } \epsilon' = e^{-\frac{\epsilon n}{3}\delta^2}. \tag{4.6}$$

This means that, for game G', the correctness is exponentially close to 1 and the security parameter is exponentially close to zero. This is the desired behaviour in a noisy implementation: the probability than an honest noisy card gets accepted should be very close to 1, while the probability that a counterfeit passes the verification should be arbitrarily small. An expression for δ in terms of c and ϵ is derived in Appendix A.1, allowing us to compute c' and ϵ' explicitly:

$$\delta = \frac{2c-\epsilon-1}{3}. \tag{4.7}$$

Enforcing $\delta > 0$ then allows to recover the security condition from Eq. (4.3). Since in our initial game G we have $\epsilon = 3/4$, then we can see from Eq. (4.3) that in any secure implementation of game G we need to achieve $c > 7/8 = 0.875$. The more c exceeds this

bound, the better security (*i.e.*, the lower ϵ') we will get for a game G' with n parallel repetitions.

The above description provides a game with exponentially good security parameters for a quantum credit card fragment, or àmini-scheme [44]. By including quantum states that correspond to many such games in the same credit card as well as a unique classical serial number, one can use theorems from [41, 44, 50] to extend the above scheme into a full quantum prepaid credit card scheme, where the quantum credit card may be re-used multiple times and a dishonest client cannot create a copy of the credit card even if they have in their possession multiple credit cards. Hence, satisfying Eq. (4.3) experimentally is enough to implement a full quantum money scheme with information-theoretic security given by correctness and security parameters from Eq. (4.6).

4.3.3 Weak coherent states with fixed phase

In our discussion up till now, we have assumed that the mint creates true single qubit states and stores them in the credit card. In practice, this assumption would be compatible with an implementation using either a quantum memory based on single emitters [36, 37], which are expected to emit true single photons to be measured by the vendor for verification regardless of the input state used by the bank in the card preparation stage, or a quantum memory based on atomic ensembles [71, 72] when the input state is a true single-photon state. In the following, we shall refer to this case as the "single-photon state" protocol. The correctness and security parameters defined in Section 4.3.2 apply to this case.

In other cases of practical interest, however, we would like to use atomic-ensemble quantum memories and also weak coherent states as an input, as is typically the case in quantum cryptographic applications. In this case, the memory preserves the Poisson photon statistics of the input coherent state and simply introduces attenuation, hence reducing the average photon number per pulse μ that characterizes such states. The security threshold therefore has to be modified. More specifically, the bound that c must exceed has to be a function of μ. In the following, we shall refer to this case as the "weak coherent state" protocol.

Our security analysis first considers specific attacks that may take place in an experiment, and were briefly introduced in Chapter 1: unambiguous state discrimination (USD) attacks. Such attacks are possible only for sets of linearly independent states [27, 73, 74], which is the case for the set of states used in our protocol when physically

realized with the weak coherent state encoding. State discrimination is not possible for sets of linearly dependent states, since the uncertainty principle and no cloning theorem (Section 3.1.2) then come into play.

Using USD, a dishonest client willing to copy the credit card can perform specific POVMs (Section 2.1.3) to unambiguously learn and identify a fraction of the states in the card. The remaining states are left unidentified, since they correspond to the *don't know* outcome of the USD POVM set. The dishonest client may however replace these with vacuum states in ordered to hide their failed discrimination attempts. If the losses are not monitored, this strategy can lead to unit cheating probability. The security condition for losses with respect to this specific attack is presented in Section 4.3.5. Furthermore, successfully identifying one state in a pair allows the successful cloning of the whole pair, since the adversary knows that the other state is prepared in the conjugate basis. Following the analysis from [27] and [74] for our set of states gives the probability for successful USD:

$$P_D = 2e^{-\frac{\mu}{2}}\left(\sinh\frac{\mu}{2} - \sin\frac{\mu}{2}\right). \tag{4.8}$$

By a Chernoff bound argument [70], we then have that for n pulses (in the $2n$-qubit sequence) that are created according to the Poisson distribution with a mean photon number μ, with very high probability the number of pulses among these n pulses for which the USD is successful is very close to its expectation. If $L_1,...L_n$ are random variables that take the value 1 when the pulse leads to successful USD, then we have for the sum $L = \sum_i L_i$ that:

$$\Pr[L \geq (1+\eta)P_D] \leq e^{-\frac{P_D n}{3}\eta^2}, \tag{4.9}$$

where $\eta > 0$ is a parameter accounting for finite number statistics that can be optimized as discussed further on. We may now define a new parameter:

$$\delta = \frac{2c - \epsilon - (1+\eta)P_D - 1}{3} > 0, \tag{4.10}$$

derived in Appendix A.1, and restate the condition of Eq. (4.3) as:

$$c > \frac{\epsilon + (1+\eta)P_D + 1}{2}. \tag{4.11}$$

This leads to the following correctness and security parameters that take into account possible USD attacks:

$$c' = 1 - e^{-\frac{cn}{2}\delta^2} \text{ and } \epsilon' \leq e^{-\frac{\epsilon n}{3}\delta^2} + e^{-\frac{P_D n}{3}\eta^2}. \tag{4.12}$$

Note that the second term in the expression of ϵ' comes from the fact that, in case L is bigger than its expectation, then the dishonest client can perfectly cheat on a larger number of pairs.

4.3.4 Weak coherent states with randomized phase

Although USD leads to some of the most powerful explicit attacks in quantum-cryptographic implementations involving coherent states, considering them does not provide a general security bound against all attacks. In this section, we aim to derive a more pessimistic yet rigorous bound which does not require any assumption on the type of attack. As emphasized previously however, we limit ourselves to attacks which do not exploit losses. A general security analysis which considers the subtle interplay between noise and losses will be derived in Chapter 5. Here, we use the technique of phase-randomization [75] to suppress the coherence between Fock states that the client can exploit. We first explicit the mapping between qubit states and polarized coherent states, which will help us gain insight into the effects of phase randomization:

$$\begin{aligned} |0\rangle &\to |\alpha\rangle \otimes |\text{vac}\rangle \qquad |1\rangle \to |\text{vac}\rangle \otimes |-\alpha\rangle \\ |+\rangle &\to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |\tfrac{\alpha}{\sqrt{2}}\rangle \qquad |-\rangle \to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-\tfrac{\alpha}{\sqrt{2}}\rangle \\ |+i\rangle &\to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |i\tfrac{\alpha}{\sqrt{2}}\rangle \quad |-i\rangle \to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-i\tfrac{\alpha}{\sqrt{2}}\rangle, \end{aligned} \tag{4.13}$$

where α is the coherent state amplitude, $|\text{vac}\rangle$ denotes the vacuum state (Section 2.3.1), and the tensor product is over the two polarization modes. The last four states from Eq. (4.13) may then be expressed more compactly as:

$$\left|e^{i\phi}\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|e^{i(\phi+\theta)}\frac{\alpha}{\sqrt{2}}\right\rangle, \tag{4.14}$$

where the global phase $\phi = 0$ and the relative phase $\theta \in \{0, \frac{\pi}{2}, 2\pi, \frac{3\pi}{2}\}$. This formulation shows that an adversary must access θ to unveil the information encoded in the states. Phase randomization scrambles the global phase reference by allowing ϕ to take values from $[0, 2\pi]$ uniformly at random instead of a single value. Appendix A.2 details how integrating over all possible values of ϕ leads to the adversary seeing a classical mixture of Fock states given by [75]:

$$\frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}e^{i\phi}\rangle\langle\sqrt{\mu}e^{i\phi}| d\phi = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|, \tag{4.15}$$

where $\mu = |\alpha|^2$ is the average photon number, and $|n\rangle$ are the photon number states. As the coherent superposition of number states vanishes in Eq. (4.15), the security proof may simply proceed according to the result of quantum non demolition (QND) photon number measurements, considering three distinct cases:

- **0 photon:** no information content.

- **1 photon:** qubit proof from Section 4.3.1 may be applied.
- **2 photons or more:** perfect cheating is assumed, since the information is effectively cloned within the original pulse, and so one photon can be sent to each of the two terminals and pass the verification test with probability 1.

The photon number content of a coherent state follows Poisson statistics. The probability λ of finding two photons or more in a given pulse may therefore be expressed as:

$$\lambda = 1 - p(0|\mu) - p(1|\mu) = \frac{1-(1+\mu)e^{-\mu}}{1-e^{-\mu}}, \tag{4.16}$$

where $p(i|\mu)$ is the probability of finding i photons in a pulse given average photon number per pulse μ. This allows to adapt the security threshold from Eq. (4.3) in the following way:

$$c > \frac{\epsilon + (1+\eta)\lambda + 1}{2}. \tag{4.17}$$

In fact, this security threshold is slightly overestimated, as one could replace ϵ with $p(1|\mu)\epsilon$, since the qubit security proof applies only in cases which involve only one photon in the pulse, which occurs with probability $p(1|\mu)$. Using the same Chernoff argument as in the two previous subsections, we may then write the general correctness and security parameters for n pairs as:

$$c' = 1 - e^{-\frac{cn}{2}\delta^2} \text{ and } \epsilon' \leq e^{-\frac{\epsilon n}{3}\delta^2} + e^{-\frac{\lambda n}{3}\eta^2}. \tag{4.18}$$

As long as it is possible to satisfy Eq. (4.17) experimentally, then a quantum credit card scheme with information-theoretic security against all attacks performed on uniformly phase randomized weak coherent states, characterized by correctness and security parameters given in Eq. (4.18), can be implemented. Only the loss-dependent attacks are discarded here.

4.3.5 Loss tolerance for USD

A dishonest client may further boost their cheating probability by exploiting the losses present in a realistic implementation. These are identified by the detection and quantum memory efficiences η_d and η_m, respectively. In the presence of losses, the client having used USD to copy the card may indeed replace the states that they have successfully identified with states containing a higher average photon number μ at the input of the

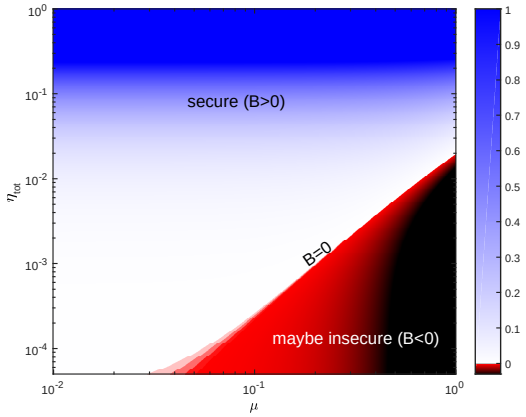


Figure 4.2: **Security regions for weak coherent states.** $B = \eta_{\text{tot}} + \ln(1-P_D)/\mu$ is plotted as a function of the average number of photons per pulse μ and the total efficiency $\eta_{\text{tot}} = \eta_m \eta_d$. The security condition of Eq. (4.19) is fulfilled when $B > 0$.

payment terminal, in order to increase the probability of detection by the vendor, and replace the ones that they failed to identify with vacuum states. Such a strategy will not be detected when a state is measured in the correct basis but it will induce an increase in the number of total clicks on the detectors registered by the card reader when a state is measured in the conjugate basis. Based on [27], in order for this cheating strategy to be detected and thus for the protocol to be secure, the total efficiency must fulfill the condition:

$$\eta_m \eta_d > \frac{-\ln(1-P_D)}{\mu}, \tag{4.19}$$

where η_m is the retrieval efficiency of the quantum memory in the original valid card and η_d is the detection efficiency of the card reader. The corresponding security region is plotted in Fig. 5.6.

Thus, for the "weak coherent state" protocol, as long as it is possible to satisfy Eqs. (4.11) and (4.19) experimentally, then a quantum credit card scheme secure against USD attacks, characterized by correctness and security parameters given in Eq. (4.12), can be implemented.

4.4 Experimental implementation

4.4.1 Proof-of-principle setup

In order to test in practice the security conditions from Eqs. (4.3), (4.11) and (4.19) and identify suitable operation regimes, we have implemented an on-the-fly version of our quantum money protocol in which the qubit pairs of the credit card are sent directly to the vendor's payment terminal, without intermediate storage in a quantum memory. In our experiment we have not performed phase randomization (this can be implemented subsequently in the same manner as [76]), hence the security bound of Eq. (4.17) has not been explicitly considered. The verification test consists in measuring the correctness parameters c_{zz} for the challenge question Q_{zz} and c_{xx} for Q_{xx} on blocks of n qubit pairs, each of which is randomly chosen from the set of Eq. (4.1). This is done by measuring each block in the $\sigma_z \otimes \sigma_z$ basis or in the $\sigma_x \otimes \sigma_x$ basis, respectively. As noted earlier, the correctness parameter is calculated as $c = (c_{zz} + c_{xx})/2$, and must exceed the thresholds from Eqs. (4.3) and (4.11) in order for the credit card to be validated by the bank. This does not compromise the security of the implementation as it is always possible to symmetrize the data by relabeling the bases such that in practice the two parameters become effectively the same. Once c has been measured, the correctness and security of the full protocol can be estimated for the different scenarios from Eqs. (4.6) and (4.12).

The experimental setup is shown in Fig. 4.3. The qubit pairs of the credit card state are encoded in the polarization of weak coherent states of light produced with standard optical communication components. The light emitted at 1564 nm by a continuous-wave laser diode is first modulated using an acousto-optic modulator to produce pulses with a duration of 20 μs and a repetition rate of 20 kHz. A variable optical attenuator is used to reduce the intensity of the pulses and set the average photon number per pulse μ. Then, the light pulses go through a multi-stage polarization controller consisting of an electro-optic modulator, which sets the polarization of each pulse to horizontal, vertical, diagonal or antidiagonal, according to a suitable combination of applied voltages. These polarization states correspond to the qubit states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, respectively. The voltage sequences applied to the controller are generated such that two successive pulses form a pair whose polarization state is randomly chosen from the set S_{pair}, as required by our protocol.

The value of μ is fixed for each experiment at the output of the polarization controller. Finally, the pulses are directed to the credit card reader, where the polarization state of each pulse is measured in either the σ_z or the σ_x basis by the combination of a half-wave

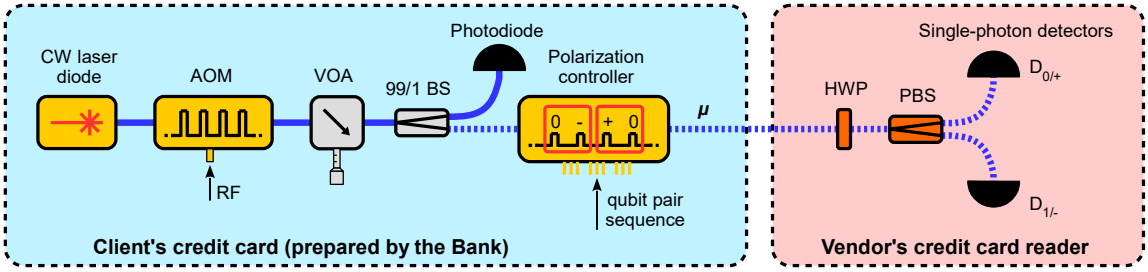


Figure 4.3: **Experimental setup of the quantum money system.** The credit card state preparation is performed using pulses carved from light emitted by a telecommunication wavelength laser diode using an acousto-optic modulator (AOM). A multi-stage polarization controller (EOSPACE) is then used to select the polarization states according to the protocol by applying suitable voltages. The average photon number of pulse μ is set by a variable optical attenuator (VOA) and is calibrated with a 99/1 beam splitter (BS) and a nano powermeter. The credit card reader is materialized by a standard polarization analysis setup including a half-wave plate (HWP), a polarization beam-splitter (PBS) and two InGaAs single-photon avalanche photodiodes (ID201). The entire setup is synchronized using a multi-channel delay generator and is controlled by software incorporating the random state generation and data acquisition and processing.

plate, set at an angle 0° or 22.5° with respect to the horizontal direction, respectively, and a polarization beamsplitter whose outputs are directed to two single-photon detectors labeled $D_{0/+}$ and $D_{1/-}$. At the end of the experiment, the data sets corresponding to the credit card state generated by the bank, the bases selected by the vendor, and the measurement outcomes obtained for the different challenge questions are analyzed to assess the security of our implementation.

4.4.2 Experimental steps

Regarding **pulse chopping**, an acousto-optic modulator is used, driven by an RF signal. The driver generates a 200 MHz RF electrical output signal which, thanks to an electro-acoustic transducer, transforms into a periodic acoustic standing wave inside the modulator. Such a wave triggers a periodic variation of the crystal's refractive index due to the alternating compression and dilation phenomena, which in turn serve as a Bragg reflector for the incident laser beam. For a specific incidence angle θ, part of the beam is deflected by first order diffraction, while the rest of the beam follows its original path (zeroth order diffraction). The deflected beam constitutes the output of the modulator.

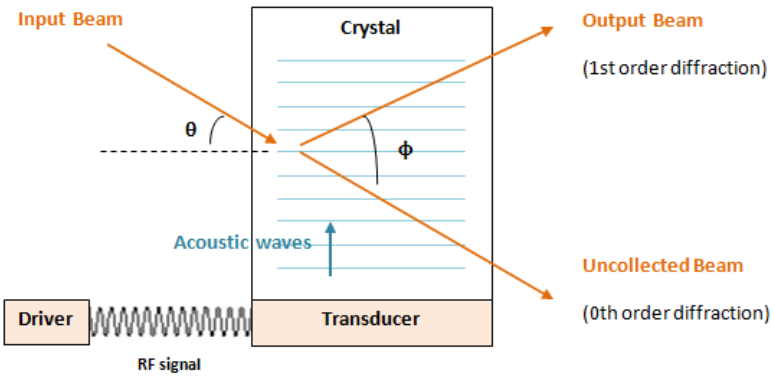


Figure 4.4: **Simplified diagram of the acousto optic modulator's deflection function.**

The pulses are then created by using the arbitrary waveform generator's pulsed input as an envelope for the driver's RF signal. When the envelope goes to zero, there is no deflection and so the entire incident beam is blocked. When the envelope peaks, then the deflected beam is at its maximum, and so a pulse will be created.

The overall response time of the modulator is around 70 ns, and there are some insertion losses due to the only partially deflected beam that serves as the output. Such losses, however, do not have to be considered as they are generated in the mint's honest lab.

Regarding the **attenuation process**, an IDIL variable optical attenuator is used, followed by a 99/1 beam splitter. The 99% arm is coupled to a nano powermeter, while the other arm is coupled to the polarization controller and the detection part of the experiment. Such a setup allows a precise estimation of the power needed to reach the desired value of μ.

Polarization control is performed thanks to an EOspace lithium-niobate crystal containing three stages. A triplet of voltages is applied transversely to each stage (Fig. 4.5) in order to create a polarization rotation via the Pockels effect. Applying a transverse electric field on the crystal triggers a charge reorganization which modifies the birefringence in a proportional manner.

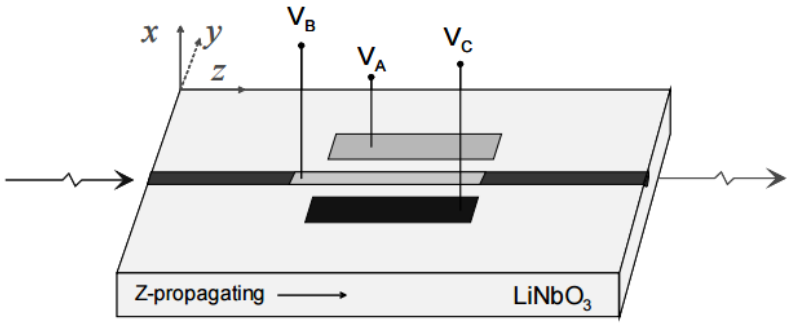


Figure 4.5: **Polarization waveguide and electrode configuration of the EOspace polarization controller.** *For image source, please visit http://www.hanamuraoptics.com.*

The required operating voltages to achieve a δ-wave plate with orientation angle $\alpha/2$ using a single stage are given by the following :

$$\begin{cases} V_A = 2V_0\delta\sin\alpha - V_\pi\delta\cos\alpha + V_{A\,bias} \\ V_B = 0 \\ V_C = 2V_0\delta\sin\alpha + V_\pi\delta\cos\alpha + V_{C\,bias} \end{cases} \tag{4.20}$$

where V_0 rotates all power from the horizontal state to the vertical state and V_π induces a phase shift of π between the two states. $V_{A\,bias}$ and $V_{C\,bias}$ allow zero birefringence between the two modes, and typically $V_{A\,bias} \approx -V_{C\,bias}$.

Single photon detection is realized with the id 201 avalanche single photon detectors from id Quantique. These are based on a reverse-biased InGaAs pn-junction, to which a voltage much higher than the breakdown voltage is applied. This allows a single photon to create an electronic avalanche in the medium, which will induce a macroscopic current. A TTL single will consequently be output by the detector in order to record a detection event. These detectors are typically gated: the strong voltage is applied only periodically, for an effective gate width duration of 500 ps, which implies that the detector cannot detect any photon outside of this region. Due to the finite, non-zero temperature of the pn-junction, some noisy detections, known as *dark counts*, may occur. The measured dark count probability for these detectors is about 5×10^{-5} per gate. These detectors also have a non-unit detection efficiency of 25%.

Data is generated and acquired using PCI-6115 National Instruments data acquisition cards, driven by DAQ-mx and controlled by a C++ program running on Ubuntu.

Generation and acquisition are triggered by the clock produced by the waveform generator.

The voltages applied to the first two stages of the polarization controller are held constant, at bias value, thanks to two standard asymmetrical voltage sources. The desired voltage sequence applied to the third stage to generate the paired states in real time is randomly generated by an Octave program. The corresponding V_A and V_C voltages are then applied through the two NI card output channels, and amplified through a standard op-amp circuit with gain 2.5 (as the NI cards cannot generate over 10V). The photon detection output is a TTL signal, which is acquired by the same card on 4 separate input channels. The results are read as vectors, for which the ith element contains either a $5V$ input if one or more photons have been detected in the ith pulse and a $0V$ input for no detection.

4.4.3 Results

The experimental results for the values of c_{zz}, c_{xx} and c, obtained for weak coherent states with different values of $\mu \leq 1$, are shown in Fig. 4.6 (green symbols). We also display the security thresholds corresponding to Eq. (4.3) for the "single-photon state" protocol (full pink line) and Eqs. (4.11) and (4.17) for the "weak coherent state" protocol, which is plotted for different values of parameter η (dashed red and purple lines respectively). We post-select on events for which at least one of the detectors has clicked.

We have also plotted simulations of the evolution of c with μ (cyan lines) according to a theoretical model that takes into account Poisson statistics of weak coherent states, dark count probability, finite detection efficiency, state purity and post-selection of pulses where at least one detector clicks. The expression for c is derived in Appendix A.3. The best fit of our data points corresponds to a state purity of $p = 93\%$. This reduced purity with respect to the 99.5% purity obtained when all states in a block are, for instance, σ_z eigenstates, is due to the large voltage differences that are required as an input to the polarization controller for different consecutive states in a block of random states. The limited response time of the involved electronics leads to state generation with non-optimal purity.

Note that, even though we are using an attenuated laser in the experiment, our data also gives us a good estimation of the performance we would obtain with true single photons emitted with an efficiency μ. For our regime of parameters, the expected value of the correctness parameter c for single-photon states (blue lines in Fig. 4.6) is extremely

close to those for weak coherent states. Thus, our experimental data can be analyzed for the various input state and quantum memory configurations considered here.

For the "weak coherent state" protocol, the security threshold of Eq. (4.11), taking into account USD attacks only, reaches 1 for $\mu \gtrsim 1$. Hence, for larger values of μ, the protocol is insecure against USD attacks. Note that for the threshold of Eq. (4.17) which ensures security against any non-loss-dependent attack (for phase-randomized states), it can be seen that μ must not exceed 0.40. The simulations in Fig. 4.6 also show that the protocol is insecure when the state purity p drops below 76%, since the value of c then falls below the USD attack security threshold. However, for $0.01 \leq \mu < 1$ and for $p \geq 0.76$, there is a wide region of parameters for which the protocol is secure against such attacks. Indeed, for our experimental results with $p = 0.93$, the protocol is secure against USD attacks for values of μ up to 1. From Fig. 5.6, our experiment with $\eta_m = 1$ and $\eta_d = 0.25$ are situated in the secure region for all values of $\mu \leq 2$.

For the "single-photon state" protocol, the security threshold of Eq. (4.3) is constant and equal to $7/8 = 0.875$ for all values of μ. Our experimental data, interpreted as if resulting from single-photon states with a polarization purity $p = 0.93$ and an efficiency $0.02 \leq \mu \leq 1$, are secure and show a value of c well above the security threshold. We also notice that the protocol can tolerate large attenuations even for relatively low values of purity.

The measured values for c allow us to estimate the number n of qubit pairs required for our prepaid quantum credit card scheme (corresponding to the game G') to reach a high level of security. In Fig. 4.7, we show values for the correctness and security parameters c' and ϵ' defined in Eq. (4.6) for the "single-photon state" protocol, using the experimental values $c = 0.953 \pm 0.011$ for $\mu = 1$ (full red line), $c = 0.966 \pm 0.018$ for $\mu = 0.10$ (dashed red line) and $c = 0.953 \pm 0.014$ for $\mu = 0.025$ (dotted red line). We see that, as ϵ' drops quickly with the number of qubit pairs n, a measured credit card state consisting of a number of pairs comprised between 10^4 and 10^5 is sufficient to reach an arbitrarily small cheating probability in this case, for a wide range of efficiencies $\mu \in [0.025; 1]$. Note that when estimating c' and ϵ', we use the lowest value for the experimental value of c taking into account error bars of 5σ. In this way, there is a probability no higher than 10^{-6} that the true c value actually lies beneath this point.

In Fig. 4.7, we also display values for the correctness and security parameters c' and ϵ' defined in Eq. (4.12) for the "weak coherent state" protocol, using the experimental values $c = 0.953 \pm 0.011$ for $\mu = 1$ (full blue line), $c = 0.965 \pm 0.010$ for $\mu = 0.40$ (mixed blue line), $c = 0.966 \pm 0.018$ for $\mu = 0.10$ (dashed blue line) and $c = 0.953 \pm 0.014$ for

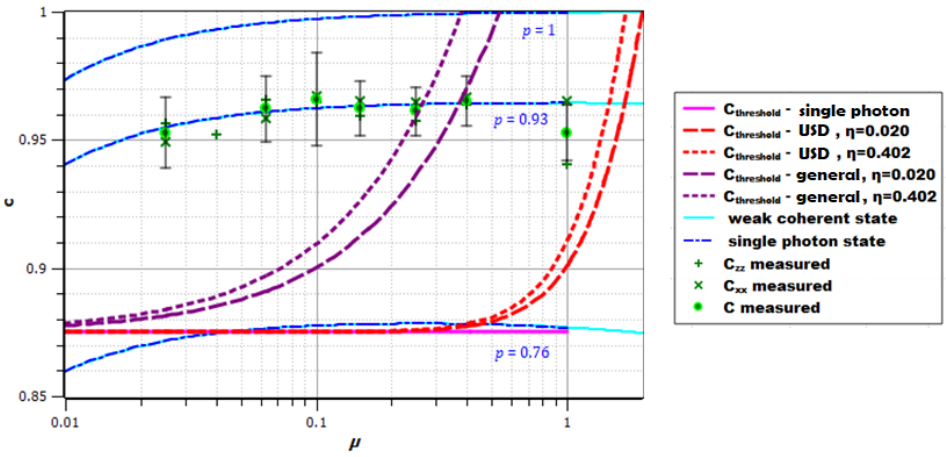


Figure 4.6: **Experimental results for different values of μ.** Measured c_{zz}, c_{xx}, and c values (green symbols) are plotted as a function of the average photon number per pulse μ. Each measured block consists of a number of post-selected pairs ranging from 1.3×10^5 for $\mu = 0.025$ to 2.6×10^5 for $\mu = 0.40$ and 2.0×10^5 for $\mu = 1$. The red lines correspond to the security threshold for the "weak coherent state" protocol encompassing USD attacks for values of $\eta = 0.020$ and $\eta = 0.402$, while the purple line corresponds to the threshold for general attacks on phase-randomized weak coherent states, for the same values of η. The full pink line corresponds to the security threshold for the "single-photon state" protocol. The cyan curves correspond to theoretical simulations for weak coherent states assuming a dark count probability of 7×10^{-5}, detection efficiency of 25%, state purity values of $p = 0.76, 0.93, 1$ and post-selection of pulses with at least one detector clicking (Appendix A.3). The blue curves correspond to the same theoretical simulations, this time for true single-photon states with an emission efficiency μ. The plotted error bars correspond to 5σ.

$\mu = 0.025$ (dotted blue line). The parameter η has an opposite effect in the two terms in the expression of ϵ' and we find that these two terms must be roughly balanced. Values for η have therefore been chosen accordingly, and we see that the optimal values strongly depend on μ : they must be increased as μ decreases. We also notice that, in general, states with large values of μ require a higher number of detected pairs than states with small values of μ in order to reach the same security level. However, as long as μ is not too big, the minimal number of pairs remains of the order of 10^5, and this effect is counter-balanced by the fact that a higher value of μ increases the number of useful detected pulses and hence the number n of detected pairs. Thus, despite this trade-off, in order to optimize the performance of the setup, it is in general preferable to keep μ as high as possible in order to maximize the number of detected pairs. We may therefore conclude that our proof-of-principle experiment for the "weak coherent state" protocol

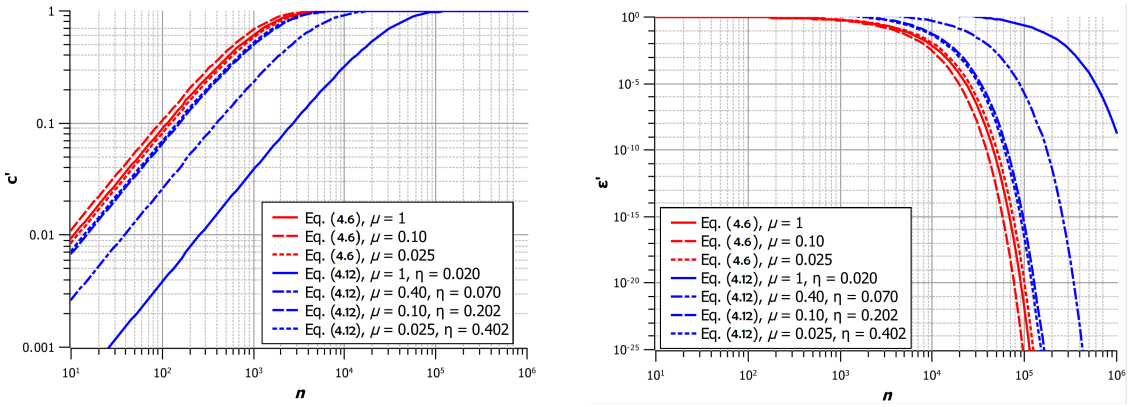


Figure 4.7: **Correctness and security parameters of the full scheme.** Numerical calculations for the correctness parameter c' (left) and security parameter ϵ' (right) as a function of the number n of measured qubit pairs in the credit card, with experimental values of $c = 0.953 \pm 0.011$ for $\mu = 1$ (full red and blue lines), $c = 0.965 \pm 0.010$ for $\mu = 0.40$ (mixed blue line), $c = 0.966 \pm 0.018$ for $\mu = 0.10$ (dashed red and blue lines) and $c = 0.953 \pm 0.014$ for $\mu = 0.025$ (dotted red and blue lines). Note that the lowest values of the 5σ error bars are considered for plotting these bounds. Red lines correspond to the "single-photon state" protocol while blue lines correspond to the "weak coherent state" protocol.

works optimally when $\mu \in [0.10; 0.40]$.

4.5 Independent work

4.5.1 Results outline

Independent work also simultaneously reported a first proof-of-principle implementation of quantum money with classical verification in [69]. Here, the classical verification is also based on quantum retrieval games and also assumes communication with a trusted payment terminal. Instead of encoding the secret key bits into the standard $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ states, however, the mint encodes each secret n-bit string $x = x_1x_2x_3x_4$ into the phase degree of freedom of a hidden matching state:

$$|\phi_x\rangle = \frac{1}{2}\sum_{i=1}^{4}(-1)^{x_i}|i\rangle\,. \tag{4.21}$$

In order to perform the verification, the trusted terminal then randomly picks a pair (i, j) from one of the three possible pairwise-disjoint sets of matchings, in order to output the

correct phase parity $(x_i \oplus x_j)$ to the bank:

$$\begin{aligned} M_1 &= \{(1,2),(3,4)\} \\ M_2 &= \{(1,3),(2,4)\} \\ M_3 &= \{(1,4),(2,3)\} \end{aligned} \tag{4.22}$$

Here, the security of the protocol still arises from conjugate coding (Section 3.1.1) , since a dishonest client willing to duplicate the money does not know which matching will be picked by the terminal for verification: a measurement performed in the basis which outputs the correct phase parity for a chosen matching destroys any information contained in the phase parity of the other matchings.

When it comes to implementation, n-dimensional hidden matching states have never been produced for $n > 2$, and so this experiment also exploits the existence of a mapping to the coherent state framework. The phase of each component of the hidden matching state is encoded into the phase of a weak coherent state from the following train of pulses:

$$\frac{1}{2}\sum_{i=1}^{4}(-1)^{x_i}|i\rangle \;\Rightarrow\; \bigotimes_{i=1}^{4}|(-1)^{x_i}\alpha\rangle \tag{4.23}$$

The terminal's random choice of matching is then implemented by using a 1x3 beam-splitter, followed by an unbalanced Mach-Zehnder interferometer in each output arm to measure the phase parity.

4.5.2 Comparison

In this section, we attempt to provide a theoretical and experimental comparison of both proof-of-principle implementations. The major points are summarized in Table 4.1. Regarding noise tolerance, the encoding used in this thesis allows for 20% (assuming phase-randomization), whereas the implementation from [69] tolerates 16.6%. It is worth noting, however, that increasing the dimension N of the hidden matching state (that is, generating blocks of N coherent states instead of 4) can bring the noise tolerance arbitrarily close to 25% [68], although this implies a drastic increase in experimental complexity, as it increases the number of required Mach-Zehnder interferometers to $(N-1)$. Generally, the experimental setup from [28] is more reproducible and scalable, since it only requires a standard BB84 setup: a polarization controller, a polarization beam-splitter and two single photond detectors. When it comes to the highest average

photon number per pulse and the required number of pairs to reach a given security level, both implementations are similar.

	work from this thesis	**work from [69]**
theoretical encoding	qubit state	hidden matching state
experimental encoding	polarization of weak coherent states	phase parity of pairs of weak coherent states
noise tolerance	20.0%	16.6%
experimental error rate	$\approx 4.5\%$	3.0%
required μ	≈ 0.20	≈ 0.20
required number of detections to reach security 10^{-7}	1.2×10^5	8.3×10^4
required optical components	polarization controller polarization beamsplitter 2 single photon detectors	Mach-Zender interferometers phase and amplitude modulators 3×1 beamsplitters 2 single photon detectors
notable advantage	simple state preparation and measurement	noise tolerance may be increased arbitrarily close to 25% by using more matchings

Table 4.1: **Comparison of the implementations from this thesis and [69]**. Theoretical and experimental aspects of the two independent proof-of-principle quantum money experiments are compared: type of encoding, noise tolerance, average photon number per pulse, required number of states to reach high security, setup simplicity and main advantages.

4.6 Conclusion

This chapter reports the first on-the-fly implementation of unforgeable quantum money, assuming non-loss-dependent attacks (except for USD). The demonstration is performed on a practical photonic setup with requirements close to those of standard quantum key distribution systems, which is used for quantum credit card on-the-fly generation and readout. The validation of the quantum money protocol and the chosen experimental conditions anticipate the future use of state-of-the-art quantum storage devices, based on single emitters or atomic ensembles, for real-world realization of credit card states.

We remark that our implementation has minimal channel losses as the transaction is performed locally, while detection losses are processed through the post-selection procedure. As mentioned previously however, deriving conditions for noise and losses separately protects against some loss-dependent attacks only (namely USD attacks). In Chapter 5, we introduce an optimization framework which treats noise and losses in a unified manner, and makes no assumption on the type of attack. We point out the existence of a practical loss-dependent attack which is specific to quantum money schemes: the 50/50 *card split*. Furthermore, we extend the practical quantum money framework to allow for malicious payment terminals.

CHAPTER 5

PRACTICAL SECURITY FOR TRUSTED AND UNTRUSTED PAYMENT TERMINALS

5.1 Motivation

Practical security analyses for quantum key distribution (QKD) and quantum money require different figures of merit. In QKD, protocols must be optimized to perform over large distances in order to boost the secret key rate [13, 14]. A noisy and lossy quantum channel will therefore decrease this rate. In quantum credit card schemes, distance is not a concern since the quantum states are measured locally by the payment terminal, and the verification is performed over a classical channel. However, security proofs must take into account attacks which do not occur in QKD schemes. Searching for the optimal strategy involves optimizing over all cloning maps, such that the output of the map is accepted by two spacelike-separated branches of the bank. In this scenario, one extremely powerful attack is the *50/50 card split*: when losses are not monitored, an adversary may simply split the original honest credit card state in two, and send the first half to one terminal and the second to the other. Upon verification, both banks will then accept the card with probability 1, and the adversary will effectively extract twice the amount of money associated with the original credit card. This implies that quantum credit card schemes cannot be considered secure in implementations with under 50% transmission efficiency. The conditions will be even more stringent in the presence of a quantum storage device, since the security will become time-dependent. This will mostly

be treated in Chapter 6.

In this chapter, we provide a rigorous and unified security proof which considers all subtle trade-offs between noise and losses that an adversary may exploit, as opposed to the separate treatment of these imperfections in Chapter 4. For this reason, we present a semidefinite programming framework in which either noise or losses is incorporated as the objective function, and the other parameter as the constraint. We then use the dual structure of semidefinite programs, presented in Section 2.2.4, to prove that an adversary does not gain any advantage in correlating the n coherent states in the credit card to better cheat.

Note that the pair formalism, used and extended in Chapter 4, provides an elegant framework to derive security bounds for quantum credit card schemes in ideal conditions. However, when extended to practical scenarios involving coherent states, noise and losses, the security analysis becomes somewhat artificial, and sometimes incomplete. For example, the case where one of the states in the pair is a vacuum state (either due to channel losses or to the intrinsic vacuum component of coherent states) is not explicitly treated, in which case the pair structure becomes less relevant. When most pairs are incomplete, it indeed makes little sense to use this over single coherent states, as the original aim was to allow the terminal to pick a challenge randomly by measuring both states in the pair. In this chapter, we therefore consider the single-state version of the protocol from Chapter 4.

Finally, our security analysis deals with untrusted payment terminals. As emphasized in Section 3.2.3, it is difficult to ensure that the terminal follows the protocol's measurements honestly. When controlled by a malicious party, the terminal may in fact perform any POVM on the original credit card state in order to better clone the card.

In quantum cryptography, semi-device-independent frameworks have been developed in order to limit the needed assumptions to ensure security. While not as stringent as full device independence [77], this approach allows for practical security and performance while making fewer assumptions on the implementation than usual security proofs. This includes assumptions on the detectors [78–81], the dimensionality of the quantum states [82–84] and other parameters [85]. For quantum money, semi-device-independence relates to scenarios where one does not trust the terminal, as in this work and [47, 86], along with scenarios where the state preparation [47] or the terminal is trusted but imperfectly characterized. Note that the former may also be labelled *one-sided device independence*.

In this chapter, we incorporate semi-device-independence to deal with both trusted

and untrusted payment terminals in the presence of experimental imperfections. We extend the semidefinite programming techniques from [32–34] to the coherent state framework and use the squashing model from [46, 87], of which a brief outline is given in Appendix B.1. We remark that recent and concurrent work by Horodecki and Stankiewicz [47] also studies semi-device-independent quantum money, in a stronger threat model than here (scenario *(iv)* of Table 3.1), but without our focus on realistic implementation. A brief description of this work is provided in Section 5.5.

5.2 Protocol and correctness

The protocol here is simplified to a classical verification variant of Wiesner's single state scheme from Section 3.2.2. In this three-party quantum money scheme, the mint generates a random secret classical key $k^{(s)}$ and encodes it according to a secret classical basis key $b^{(s)}$. The quantum credit card state associated to public serial number s and secret classical keys $k^{(s)}$ and $b^{(s)}$ may then be written as:

$$|€^{(k,b)}\rangle = \bigotimes_{j=1}^{n} |\psi_j^{(k,b)}\rangle\,, \tag{5.1}$$

where $|\psi_j^{(k,b)}\rangle \in \{|+\rangle, |+i\rangle, |-\rangle, |-i\rangle\}$. More specifically, bit $k_j^{(s)}$ is encoded in the σ_x basis when $b_j^{(s)} = 0$, and in the σ_y basis when $b_j^{(s)} = 1$. The mint stores $|€^{(k,b)}\rangle$ in a quantum memory and hands it to a client. When a transaction must be performed, the vendor's honest terminal measures each of the n qubits of $|€^{(k,b)}\rangle$ in a basis dictated by a challenge question randomly chosen by the bank. For a single qubit state, the two challenges read:

c_0: *Give the correct measurement outcome if the qubit is encoded in the σ_x basis, and provide any outcome if the qubit is encoded in the σ_y basis.*

c_1: *Give the correct measurement outcome if the qubit is encoded in the σ_y basis, and provide any outcome if the qubit is encoded in the σ_x basis.*

Note that these challenges are simply the single-state version of the qubit pair challenges from Section 4.2. The difference is that the terminal must now actively select a random measurement basis for each state in the credit card, instead of measuring all states in the same basis. The honest terminal measures the qubit in the basis associated with the given challenge, which provides the honest success probability or *correctness* $c = 1$. The answers corresponding to the measurement results are sent in the form of a classical bit string to the bank, which compares it with $k^{(s)}$ and $b^{(s)}$ and accepts the credit

card only if all the measurement outcomes coincide. Bearing in mind the aim to make the protocol practical and implementable, we now consider the same honest protocol in which qubit states are mapped onto two-mode weak coherent states as:

$$\begin{aligned} |0\rangle \to |\alpha\rangle \otimes |\text{vac}\rangle \qquad & |1\rangle \to |\text{vac}\rangle \otimes |-\alpha\rangle \\ |+\rangle \to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |\tfrac{\alpha}{\sqrt{2}}\rangle \qquad & |-\rangle \to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-\tfrac{\alpha}{\sqrt{2}}\rangle \\ |+i\rangle \to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |i\tfrac{\alpha}{\sqrt{2}}\rangle \quad & |-i\rangle \to |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-i\tfrac{\alpha}{\sqrt{2}}\rangle\,, \end{aligned} \tag{5.2}$$

where α is the coherent state amplitude and $|\text{vac}\rangle$ denotes the vacuum state (see Section 2.3.1). Such a mapping is typically used for polarization or time-bin encoding, where the $|0\rangle$ component is mapped onto the first mode and the $|1\rangle$ component is mapped onto the second [58]. When dealing with polarization, the honest terminal measures each of the n credit card states in the basis which answers either c_0 or c_1 by typically rotating a half or quarter waveplate. It then outputs $(1-f_h)n$ measurement outcomes, where

$$f_h \approx e^{-\eta_d \mu} \tag{5.3}$$

represents the honest losses assuming a weak coherent light source with average photon number per pulse $\mu = |\alpha|^2$, unit channel transmission efficiency, and threshold single-photon detectors with detection efficiency η_d. When no detection occurs, the terminal reports a flag, denoted by $\varnothing$. For large sample sizes, the n-state challenge is then satisfied only if the total number of no-detection reports is equal to $f_h n$.

The multi-photon component of coherent states may also trigger clicks on both detectors at the same time. An adversary may actually exploit this property to boost their cheating probability. Following the methods used in [46], clicks on both detectors are randomly mapped to a single click as either a 0 or 1. This allows to use a squashing model to securely map the infinite-dimensional threshold detection POVMs to a finite dimensional Hilbert space. A brief outline of this model is provided in Appendix B.1.

5.3 Security

5.3.1 Principle and proof outline

In Table 5.1, we recall all possible adversarial scenarios for quantum credit card schemes in terms of honest and dishonest parties from Section 3.2.3. A successful forging attack consists in answering two challenges correctly at the same time, corresponding to extracting twice the original amount of money in one's possession. As the last four states

from Eq. (5.2) are identical on the first mode, we may reduce our security analysis to the single state:

$$|\alpha_k\rangle = |i^k \frac{\alpha}{\sqrt{2}}\rangle \tag{5.4}$$

with $k \in \{0,1,2,3\}$, before extending it to n states in Section 5.4.3.

In scenario *(ii)* from Table 5.1, the mint, the bank and the vendor trust each other. The only untrusted party is therefore the client, who brings their credit card state to the vendor's terminal for verification. In this case, a successful attack is materialized by the creation of two copies of the quantum credit card state, both being accepted by the bank when measured by two separate trusted terminals.

	Mint	Client	Terminal	Bank	Parameter
(i)	H	H	H	H	correctness c
(ii)	H	D	H	H	error rate e
(iii)	H	D/H	D	H	error rate e
(iv)	D	D/H	D	H	N/A
(v)	D	D/H	D/H	D	N/A

Table 5.1: **Adversarial scenarios for quantum money with classical verification.** Each scenario is expressed in terms of honest (H) and dishonest (D) parties. Cases denoted by D/H are indistinguishable to the bank. The parameters of interest are also given, where c indicates the correctness and e indicates the error rate upon verification.

In scenario *(iii)*, only the mint and the bank trust each other, which implies that the quantum measurements and classical data sent by the terminal upon verification cannot be trusted. In other words, the dishonest client and the vendor's terminal may cooperate in attempting to forge the credit card. In this case, a successful attack is materialized by the communication of two classical strings by two untrusted terminals to the bank, which accepts both of them.

In a coherent state implementation, the adversary may modify one or both of the following parameters: losses f_d (probability of a projection onto the vacuum state), and error rate e. The bank may detect an attack when $f_d > f_h$ or when the measured error rate e upon verification is larger than expected. Given average photon number μ, we use SDP techniques from Section 2.2 to first minimize the losses that the adversary must introduce in *(ii)* or declare in *(iii)* to succeed with probability $(1-e)$. We can then identify the range of μ for which $f_d > f_h$.

We will use Choi's theorem from Section 2.1.4 to optimize over the best adversarial linear cloning map. For *(ii)*, the figure of merit for the optimization is based on the

measurements of the two trusted terminals. For *(iii)*, the figure of merit becomes the acceptance of classical data by the bank. We then show how this single state analysis gives a bound for the n-state proof. We also note the following useful lemma, proven in Appendix B.2:

Lemma 5.1. *Given* $|\psi_1\rangle \in \mathscr{H}_1^d$, $|\psi_3\rangle \in \mathscr{H}_3^{d'}$, *and Choi–Jamiołkowski operator* $J(\Lambda)$ *associated to map* Λ, *we have:*

$$\mathrm{Tr}\left(|\psi_3\rangle\langle\psi_3| \Lambda(|\psi_1\rangle\langle\psi_1|)\right) = \mathrm{Tr}\left(|\psi_3\rangle\langle\psi_3| \otimes |\overline{\psi_1}\rangle\langle\overline{\psi_1}| J(\Lambda)\right), \tag{5.5}$$

where the overline denotes complex conjugation.

5.3.2 Trusted terminal

We shall first study the trusted terminal scenario *(ii)*. In the single qubit case, the minimum adversarial error probability is the same as in Wiesner's original quantum verification scheme, namely $e = 1/4$ [5, 32]. We recall that an explicit attack to achieve this probability is provided in Section 3.2.2. When dealing with the coherent states from Eq. (5.2), we use the existence of a squashing model for our threshold detector measurement setup, described in Appendix B.1. By imposing a condition on the terminal's postprocessing, consisting of assigning a random measurement outcome to any double click, this model allows to express the infinite-dimensional measurement operators in a 3-dimensional space spanned by $\{|0\rangle, |1\rangle, |\varnothing\rangle\}$, which greatly simplifies the security analysis.

Let Λ be the optimal adversarial map which produces two copies (living in $\mathscr{H}_1 \otimes \mathscr{H}_2$) of the original quantum credit card state ρ_{mint}, living in $\mathscr{H}_{\mathrm{mint}}$:

$$\rho_{\mathrm{mint}} = \frac{1}{4}\sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k|. \tag{5.6}$$

Note that we may write the infinite-dimensional coherent states $|\alpha_k\rangle = |i^k \frac{\alpha}{\sqrt{2}}\rangle$ in a four-dimensional orthonormal basis $\{|\phi_j\rangle\}$, with $j \in \{0,1,2,3\}$, as:

$$|\alpha_k\rangle = \frac{1}{4}\sum_{j=0}^{3} C_j e^{ijk\frac{\pi}{2}} |\phi_j\rangle, \tag{5.7}$$

where

$$C_0 = \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\cosh\frac{\alpha^2}{2}+\cos\frac{\alpha^2}{2}}$$
$$C_1 = \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\sinh\frac{\alpha^2}{2}+\sin\frac{\alpha^2}{2}}$$
$$C_2 = \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\cosh\frac{\alpha^2}{2}-\cos\frac{\alpha^2}{2}}$$
$$C_3 = \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\sinh\frac{\alpha^2}{2}-\sin\frac{\alpha^2}{2}}.$$

In this basis, the probability p_1 (resp. p_2) that a trusted terminal declares an incorrect measurement outcome for credit card 1 (resp. 2) is then given by:

$$\begin{aligned} p_1 &= \mathrm{Tr}\left[\sum_{k=0}^{3}\left(\frac{1}{2}|\beta_k^\perp\rangle\langle\beta_k^\perp|\otimes\mathbb{1}\right)\Lambda(\frac{1}{4}|\alpha_k\rangle\langle\alpha_k|)\right] \\ p_2 &= \mathrm{Tr}\left[\sum_{k=0}^{3}\left(\mathbb{1}\otimes\frac{1}{2}|\beta_k^\perp\rangle\langle\beta_k^\perp|\right)\Lambda(\frac{1}{4}|\alpha_k\rangle\langle\alpha_k|)\right], \end{aligned} \tag{5.8}$$

where $|\beta_k\rangle$ is the squashed qubit associated with the original state $|\alpha_k\rangle$, i.e. $|\beta_0\rangle = |+\rangle$, $|\beta_1\rangle = |+i\rangle$, $|\beta_2\rangle = |-\rangle$, $|\beta_3\rangle = |-i\rangle$, and $|\beta_k^\perp\rangle$ is its orthogonal qubit state. Appendix B.1 provides a more detailed explanation of this squashing model. The factor 1/4 indicates that each $|\alpha_k\rangle$ is equally likely to occur, while 1/2 accounts for the trusted terminal's random measurement basis choice. Using Lemma 5.1, we may then rewrite these expressions as $\mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right)$ and $\mathrm{Tr}\left(E_2(\mu)J(\Lambda)\right)$, where $E_1(\mu)$ and $E_2(\mu)$ are the *error operators*,

$$\begin{aligned} E_1(\mu) &= \frac{1}{4}\sum_{k=0}^{3}\frac{1}{2}|\beta_k^\perp\rangle\langle\beta_k^\perp|\otimes\mathbb{1}\otimes|\overline{\alpha_k}\rangle\langle\overline{\alpha_k}| \\ E_2(\mu) &= \frac{1}{4}\sum_{k=0}^{3}\mathbb{1}\otimes\frac{1}{2}|\beta_k^\perp\rangle\langle\beta_k^\perp|\otimes|\overline{\alpha_k}\rangle\langle\overline{\alpha_k}|, \end{aligned} \tag{5.9}$$

and $\mu = |\alpha|^2$ is the average photon number in a pulse. Following a similar method, the probability that terminal 1 (resp. 2) registers a no-detection event on credit card 1 (resp. 2) reads $\mathrm{Tr}\left(L_1(\mu)J(\Lambda)\right)$ (resp. $\mathrm{Tr}\left(L_2(\mu)J(\Lambda)\right)$), where $L_1(\mu)$ and $L_2(\mu)$ are the *loss operators*, which contain the projection onto the state $|\varnothing\rangle$:

$$\begin{aligned} L_1(\mu) &= \frac{1}{4}\sum_{k=0}^{3}|\varnothing\rangle\langle\varnothing|\otimes\mathbb{1}\otimes|\overline{\alpha_k}\rangle\langle\overline{\alpha_k}| \\ L_2(\mu) &= \frac{1}{4}\sum_{k=0}^{3}\mathbb{1}\otimes|\varnothing\rangle\langle\varnothing|\otimes|\overline{\alpha_k}\rangle\langle\overline{\alpha_k}|. \end{aligned} \tag{5.10}$$

We now search for the optimal cloning map Λ that minimizes the losses that the adversary must introduce on both credit cards for a given error rate e. We cast this problem as the following SDP for a card with a single state:

$$\begin{aligned} \min \quad & \mathrm{Tr}\left(L_1(\mu)J(\Lambda)\right) \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}(J(\Lambda)) = \mathbb{1}_{\mathscr{H}_{\text{mint}}} \\ & \mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right) = e \\ & \mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right) \geqslant \mathrm{Tr}\left(E_2(\mu)J(\Lambda)\right) \\ & \mathrm{Tr}\left(L_1(\mu)J(\Lambda)\right) \geqslant \mathrm{Tr}\left(L_2(\mu)J(\Lambda)\right) \\ & J(\Lambda) \geqslant 0. \end{aligned} \tag{5.11}$$

The first constraint imposes that Λ is trace-preserving, the second imposes error e when card 1 is measured by terminal 1, the third and fourth impose that the error and losses on card 1 are at least equal to those on card 2, and the fifth imposes that Λ is completely positive.

In Section 5.4.3, we derive the dual problem associated with problem (5.11), and provide numerical evidence for strong duality (i.e. we show that the optimal value is a global minimum). We also extend the problem to n states and use strong duality to show that the optimal solution does not change in this case: the adversary cannot decrease f_d by correlating the n states.

5.3.3 Untrusted terminal

In the untrusted terminal scenario *(iii)*, the adversary aims to provide two classical outcome strings from two different untrusted terminals which are both accepted by the bank. The minimum error in the lossless qubit case yields $e = 1/8$ [32]. For a state encoded in basis b, the corresponding simple strategy reads:

$c_i = c_j$: Adopt the honest strategy and duplicate the classical outcome.
Success probability: 1

$c_i \neq c_j$: Pick a basis b (or $\overline{b}$) at random, measure the state in this basis, and send the classical outcome to answer challenge c_b (or $c_{\overline{b}}$). Send a random measurement outcome to the other challenge $c_{\overline{b}}$ (or c_b). If the correct basis b was picked, then the adversary succeeds with probability 1. If the wrong basis $\overline{b}$ was picked, then the success probability is $\frac{1}{2}$.
Success probability : $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$.

Since the bank will ask each of these challenge combinations with probability $\frac{1}{2}$, then we have a total success probability $\frac{7}{8}$, which yields $e = \frac{1}{8}$. When transitioning to the coherent state framework, we recast (5.11) with newly defined error and loss operators:

$$\begin{aligned}
E_1(\mu) &= \frac{1}{16}\sum_{i,j=0}^{1}\sum_{k\in\{i,i+2\}} |a_{ik}^{\perp}\rangle\langle a_{ik}^{\perp}| \otimes \mathbb{1} \otimes |c_i, c_j, \overline{\alpha_k}\rangle\langle c_i, c_j, \overline{\alpha_k}| \\
E_2(\mu) &= \frac{1}{16}\sum_{i,j=0}^{1}\sum_{k\in\{i,i+2\}} \mathbb{1} \otimes |a_{ik}^{\perp}\rangle\langle a_{ik}^{\perp}| \otimes |c_i, c_j, \overline{\alpha_k}\rangle\langle c_i, c_j, \overline{\alpha_k}| \\
L_1(\mu) &= \frac{1}{16}\sum_{i,j=0}^{1}\sum_{k=0}^{3} |\varnothing\rangle\langle\varnothing| \otimes \mathbb{1} \otimes |c_i, c_j, \overline{\alpha_k}\rangle\langle c_i, c_j, \overline{\alpha_k}| \\
L_2(\mu) &= \frac{1}{16}\sum_{i,j=0}^{1}\sum_{k=0}^{3} \mathbb{1} \otimes |\varnothing\rangle\langle\varnothing| \otimes |c_i, c_j, \overline{\alpha_k}\rangle\langle c_i, c_j, \overline{\alpha_k}|.
\end{aligned} \tag{5.12}$$

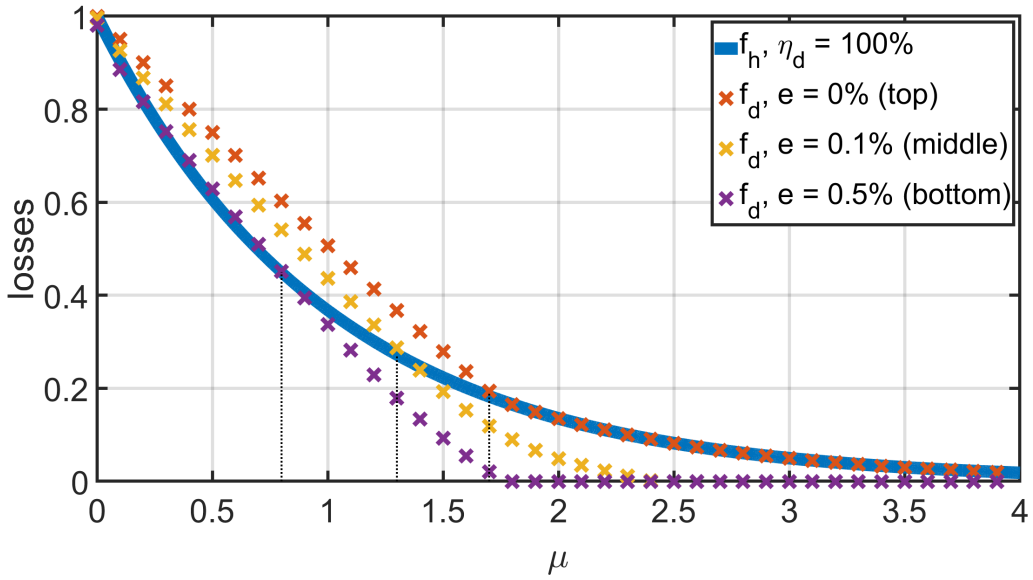
We use *braket* notation to denote the correct classical answer $|a_{ik}\rangle$ to challenge $|c_i\rangle$, given state $|\alpha_k\rangle$. These vectors are all orthogonal to one another, and live in a 3-dimensional space spanned by classical answers $\{|a_0\rangle, |a_1\rangle, |\varnothing\rangle\}$, where the last vector corresponds to a classical no-detection flag. We label the orthogonal (wrong) answer as $|a_{ik}^{\perp}\rangle$.

5.4 Optimization results

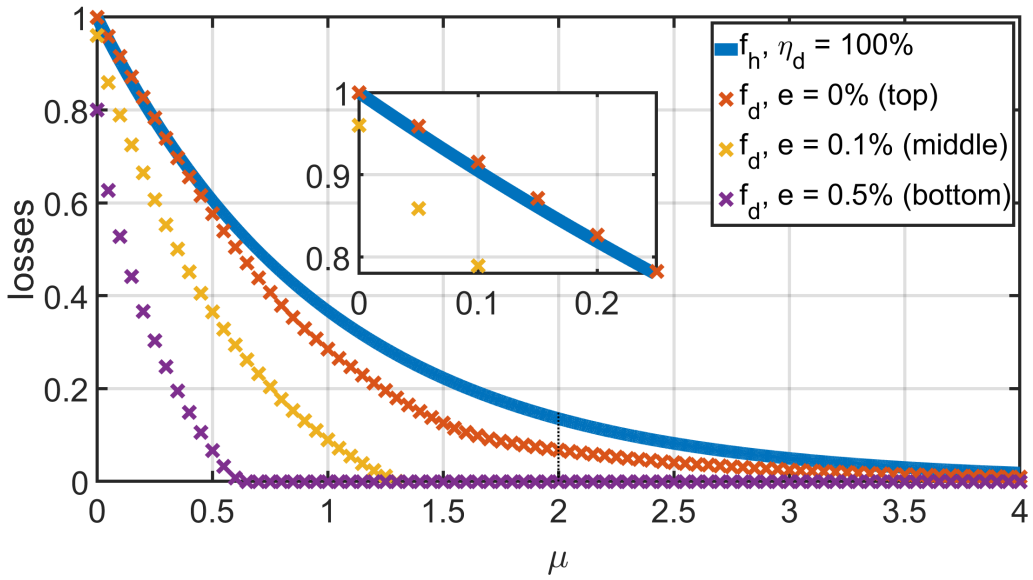
5.4.1 Single state

Solving (5.11) numerically with CVX software [90, 91] provides the results in Fig. 5.1.a for the trusted terminal setting: it is impossible for an adversary to succeed with zero error ($e = 0\%$) without introducing any excess losses ($f_d > f_h$) when $\mu < 1.7$. The protocol may therefore be implemented securely in this range of μ, since the excess losses will allow the bank to detect an attack. Secure regions of operation for other values of error e are also displayed in Fig. 5.1.a. Regarding the untrusted terminal setting, Fig. 5.1.b displays the optimal solutions as a function of μ: an errorless protocol is impossible without increasing the fraction of declared no-detection flags with respect to the honest fraction f_h, although this increase is extremely small compared to the trusted terminal setting (see figure inset).

The small adversarial losses and tight noise tolerance observed in Fig. 5.1.b may be increased by replacing the pure states $\{|\alpha_k\rangle\}$ from Eq. (5.7) with phase-randomized states ρ_k (expressions given in Appendix B.3). Numerical solutions to (5.11) for such states are displayed in Fig. 5.2 for both trusted and untrusted terminals. We observe that the range of μ for which security can be shown in practice is considerably extended in this case.

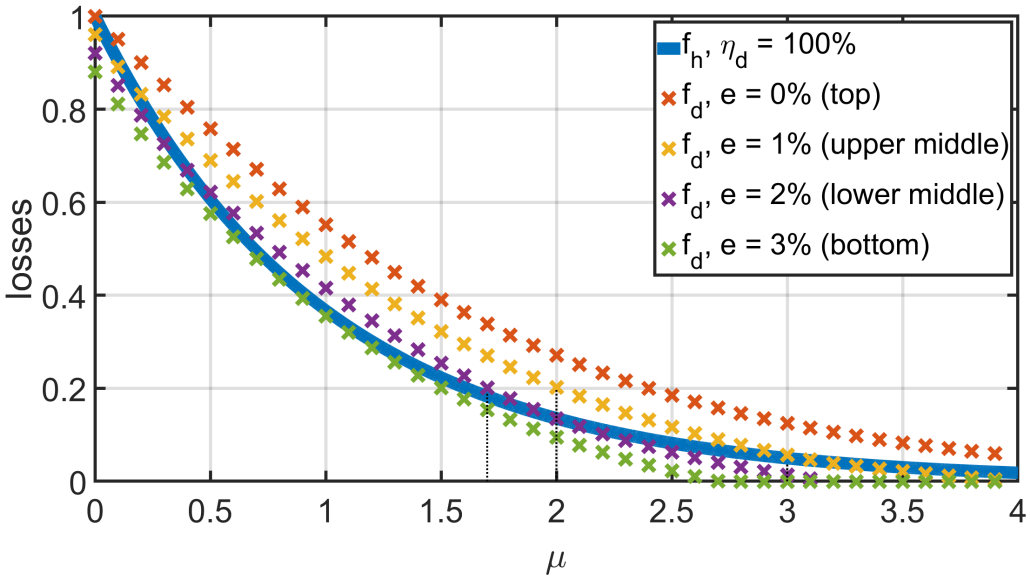


(a) Trusted, fixed phase, $\eta_d = 100\%$

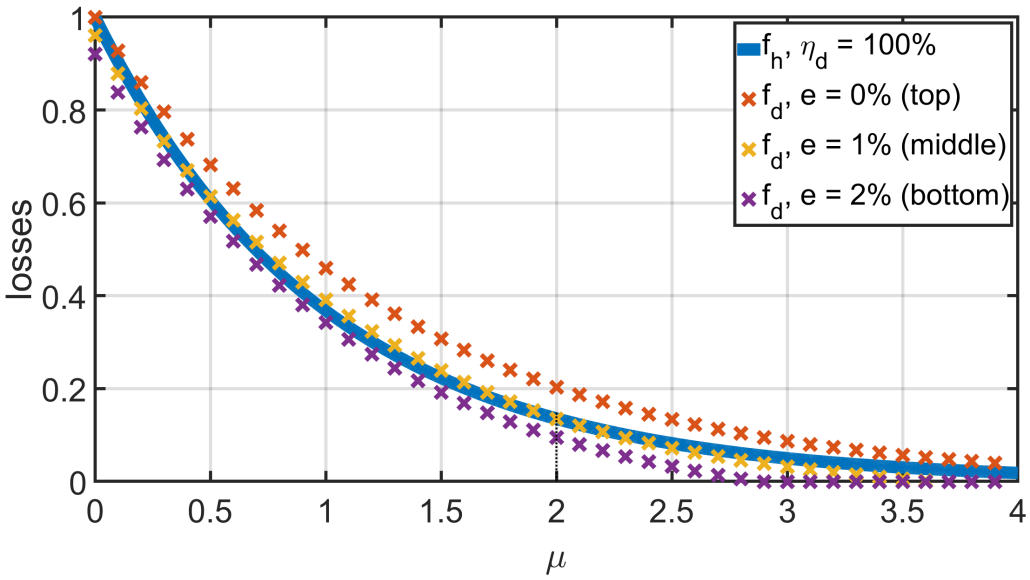


(b) Untrusted, fixed phase, $\eta_d = 100\%$

Figure 5.1: **Optimal numerical values associated with problem (5.11) for fixed-phase states.** These are plotted as a function of average photon number μ for different values of error rate e and detection efficiency $\eta_d = 100\%$, for both trusted and untrusted terminals. Solid lines correspond to the honest losses $f_h = e^{-\eta_d \mu}$. Points indicate the losses f_d that a dishonest party must induce in order to succeed with error e. The protocol is secure in regions where $f_d > f_h$. We used the *SDPT3* solver [88, 89] of the *CVX* [90, 91] software.

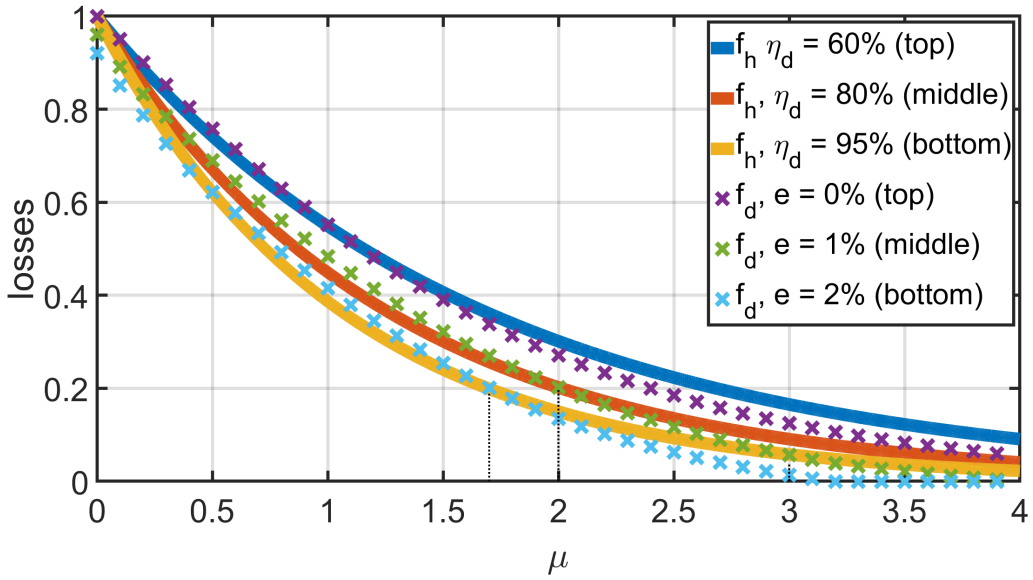


(a) Trusted, randomized phase, $\eta_d = 100\%$

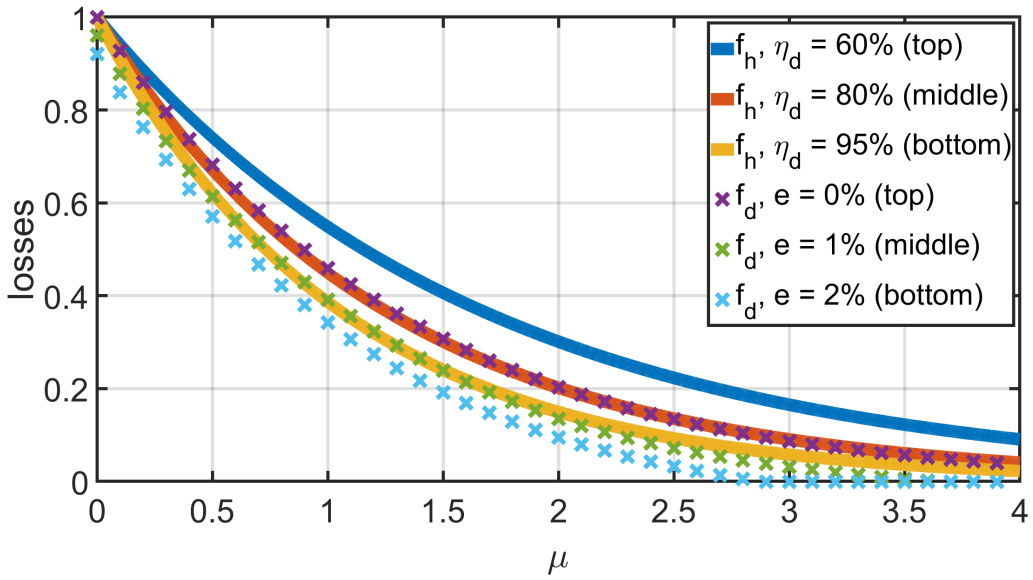


(b) Untrusted, randomized phase, $\eta_d = 100\%$

Figure 5.2: **Optimal numerical values associated with problem (5.11) for phase-randomized states.** These are plotted as a function of average photon number μ for different values of error rate e and detection efficiency $\eta_d = 100\%$, for both trusted and untrusted terminals. Solid lines correspond to the honest losses $f_h = e^{-\eta_d \mu}$. Points indicate the losses f_d that a dishonest party must induce in order to succeed with error e. The protocol is secure in regions where $f_d > f_h$. We used the *SDPT3* solver [88, 89] of the *CVX* [90, 91] software.



(a) Trusted, randomized phase, $\eta_d < 100\%$



(b) Untrusted, randomized phase, $\eta_d < 100\%$

Figure 5.3: **Optimal numerical values associated with problem (5.11) for phase-randomized states and non-unit detection efficiency.** These are plotted as a function of average photon number μ for different values of error rate e and detection efficiencies η_d, for both trusted and untrusted terminals. Solid lines correspond to the honest losses $f_h = e^{-\eta_d \mu}$. Points indicate the losses f_d that a dishonest party must induce in order to succeed with error e. The protocol is secure in regions where $f_d > f_h$. We used the *SDPT3* solver [88, 89] of the *CVX* [90, 91] software.

It is also interesting to analyze our results in this phase-randomized setting for finite detection efficiency η_d, as we will use these bounds to derive secure experimental parameters in the quantum memory setup from Chapter 6. Fig. 5.3 shows that security may be achieved in the trusted terminal scenario using state-of-the-art single-photon detectors [92, 93], depending also on the target error rate, while the untrusted scenario puts much more stringent constraints on the required devices.

5.4.2 Alternative SDP formulation

Here, we provide an alternative SDP to (5.11) which allows to minimize error e given a fixed μ and detection efficiency η_d. This formulation clearly allows to identify the effects of the 50/50 *card split* attack, in which the adversary can simply split the card in two and send half of it to each terminal without introducing any error (see Fig. 5.4). The primal problem may be expressed as:

$$\begin{aligned} \min \quad & \mathrm{Tr}\big(E_1(\mu)J(\Lambda)\big) \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}(J(\Lambda)) = \mathbb{1}_{\mathscr{H}_{\mathrm{mint}}} \\ & \mathrm{Tr}\big(E_1(\mu)J(\Lambda)\big) \geqslant \mathrm{Tr}\big(E_2(\mu)J(\Lambda)\big) \\ & \mathrm{Tr}\big(L_1(\mu)J(\Lambda)\big) \leqslant e^{-\eta_d\mu} \\ & \mathrm{Tr}\big(L_2(\mu)J(\Lambda)\big) \leqslant e^{-\eta_d\mu} \\ & J(\Lambda) \geqslant 0 \end{aligned} \tag{5.13}$$

The first constraint imposes that Λ is trace-preserving, the second imposes that the error on card 1 is greater or equal to that on card 2, the third and fourth impose that the losses on each card are smaller or equal to the honest expected losses f_h, and the fifth imposes that Λ is completely positive.

Numerical results are displayed in Fig. 5.4 for fixed-phase coherent states and Fig. 5.5 for phase-randomized states, in a trusted terminal scenario. We will actually use these results as the basis of our full demonstration of a trusted-terminal quantum credit card scheme in Chapter 6. These allow to find the value of μ for which the noise tolerance is highest given detection efficiency η_d. Roughly, the optimal average photon number lies around $\mu = 0.50$ with fixed phase and $\mu = 1$ for phase-randomized states. In the phase-randomized setting, the maximal noise tolerance is much higher (around 2.5%) than in the fixed-phase setting (around 0.4%). Finally, we notice that allowing for 50% transmission allows the adversary to win without introducing any error.

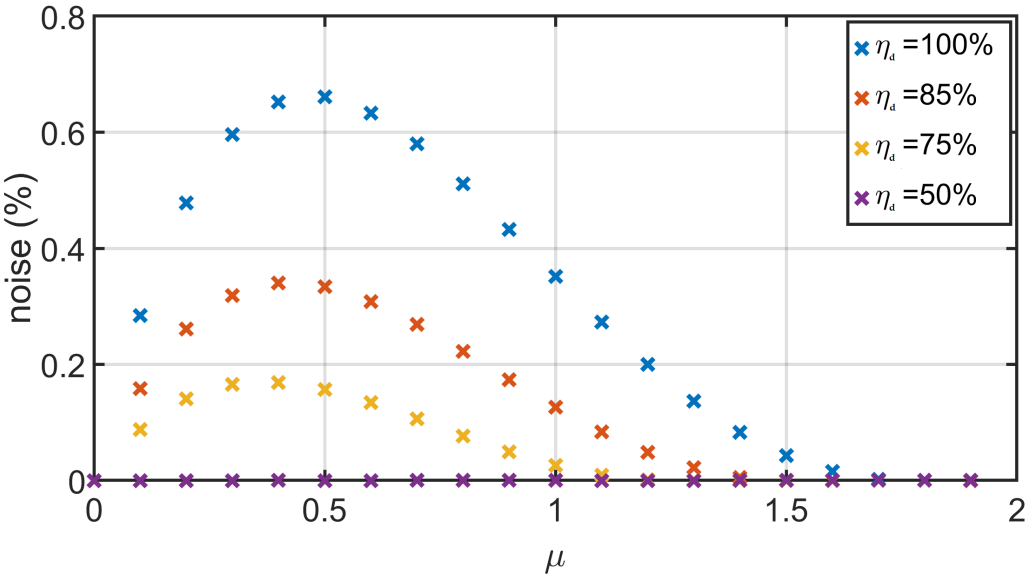


Figure 5.4: **Optimal numerical values of problem (5.13) as a function of average photon number μ for fixed-phase coherent states.** Results are plotted for different values of detection efficiency η_d in the trusted terminal scenario. Points indicate the error e that a dishonest party must induce in order to succeed by introducing less than $e^{-\eta_d \mu}$ losses. We used the *SDPT3* solver [88, 89] of the *CVX* [90, 91] software.

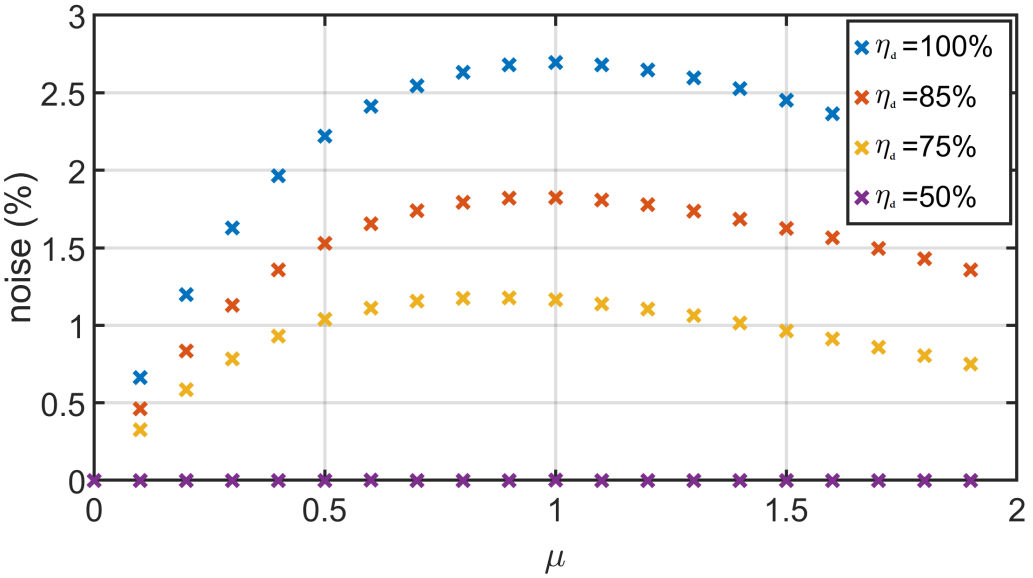


Figure 5.5: **Optimal numerical values of problem (5.13) as a function of average photon number μ for phase-randomized coherent states.** Results are plotted for different values of detection efficiency η_d in the trusted terminal scenario. Points indicate the error e that a dishonest party must induce in order to succeed by introducing less than $e^{-\eta_d \mu}$ losses. We used the *SDPT3* solver [88, 89] of the *CVX* [90, 91] software.

5.4.3 Extension to n parallel repetitions

The aim of this section is to extend SDP (5.11) to a credit card containing n states, and to derive its corresponding dual problem. In order to show that the adversary does not gain any advantage in correlating the n states to better succeed, we will first show that a tensor product of n optimal solutions of (5.11) is a feasible solution to this new n-state primal SDP. We then have to show that there also exists a feasible solution for the associated dual problem which yields the same optimal value as that of the primal. As explained in Section 2.2, such a feature is known as *strong duality*, and implies that these feasible solutions are both the *optimal solutions* to the primal and dual problem, respectively.

To generalize the loss and error operators to the n parallel repetition case, we introduce the projector $\mathscr{P}(n,j,\mathscr{C})$ which, given a collection $\mathscr{C}$ of n quantum states living in Hilbert space $\mathscr{H}^{(n)}$, projects onto $j \leqslant n$ elements of $\mathscr{C}$ and the orthogonal subspace of the $(n-j)$ other elements. More formally, we define this operator as:

$$\mathscr{P}(n,j,\mathscr{C}) = \sum_{s(j)} \bigotimes_{i=0}^{n-1} \left[s_i(j)\mathscr{C}_i + \overline{s_i(j)}(\mathbb{1} - \mathscr{C}_i) \right], \tag{5.14}$$

where $\mathscr{C}_i$ is the i-th quantum state of $\mathscr{C}$ and $s_i(j)$ is the i-th element of a binary string $s(j)$ of length n which contains $(n-j)$ zeros. The summation then runs over all $\binom{n}{j}$ possible $s(j)$ strings. Considering a new adversarial cloning map $\Lambda^{(n)}$ from the original n-state credit card living in $\mathscr{H}^{(n)}_{\text{mint}}$ to a duplicated credit card space $\mathscr{H}^{(n)}_1 \otimes \mathscr{H}^{(n)}_2$, the new loss operators may then be written as:

$$\begin{aligned} L_1^{(n)}(\mu) &= \frac{1}{4^n} \sum_{j=1}^{n} \sum_{k_1 \cdots k_n = 0}^{3} \frac{j}{n} \mathscr{P}\left(n, j, \mathscr{C}^{(\varnothing,n)}\right) \otimes \mathbb{1}_{\mathscr{H}_2^{(n)}} \otimes \left(|\overline{\alpha_{k_1}}\rangle \langle \overline{\alpha_{k_1}}| \otimes \cdots \otimes |\overline{\alpha_{k_n}}\rangle \langle \overline{\alpha_{k_n}}| \right) \\ L_2^{(n)}(\mu) &= \frac{1}{4^n} \sum_{j=1}^{n} \sum_{k_1 \cdots k_n = 0}^{3} \mathbb{1}_{\mathscr{H}_1^{(n)}} \otimes \frac{j}{n} \mathscr{P}\left(n, j, \mathscr{C}^{(\varnothing,n)}\right) \otimes \left(|\overline{\alpha_{k_1}}\rangle \langle \overline{\alpha_{k_1}}| \otimes \cdots \otimes |\overline{\alpha_{k_n}}\rangle \langle \overline{\alpha_{k_n}}| \right), \end{aligned} \tag{5.15}$$

where $\mathscr{C}^{(\varnothing,n)} = \{|\varnothing\rangle\langle\varnothing|\}^n$. The factors $\frac{j}{n}$ ensure that the total sum is normalized, as we are dealing with probabilities and not events. The new error operators read:

$$\begin{aligned} E_1^{(n)}(\mu) &= \frac{1}{4^n} \sum_{j=1}^{n} \sum_{k_1 \cdots k_n = 0}^{3} \frac{j}{n} \mathscr{P}\left(n, j, \mathscr{C}^{(k_1,.,k_n)}\right) \otimes \mathbb{1}_{\mathscr{H}_2^{(n)}} \otimes \left(|\overline{\alpha_{k_1}}\rangle \langle \overline{\alpha_{k_1}}| \otimes \cdots \otimes |\overline{\alpha_{k_n}}\rangle \langle \overline{\alpha_{k_n}}| \right) \\ E_2^{(n)}(\mu) &= \frac{1}{4^n} \sum_{j=1}^{n} \sum_{k_1 \cdots k_n = 0}^{3} \mathbb{1}_{\mathscr{H}_1^{(n)}} \otimes \frac{j}{n} \mathscr{P}\left(n, j, \mathscr{C}^{(k_1,.,k_n)}\right) \otimes \left(|\overline{\alpha_{k_1}}\rangle \langle \overline{\alpha_{k_1}}| \otimes \cdots \otimes |\overline{\alpha_{k_n}}\rangle \langle \overline{\alpha_{k_n}}| \right), \end{aligned} \tag{5.16}$$

e	10^{-6}	10^{-3}	0.01	0.02	0.05	0.10
μ	0.01	0.05	0.10	0.50	1.00	2.00

Table 5.2: Numerical optimal values for dual problem (5.19) were found for all possible combinations of the above e and μ values, using the *SDPT3* solver from the *CVX* software with its default numerical precision (10^{-9}). These solutions obeyed the constraints (5.20) within numerical accuracy and all present a duality gap of order 10^{-9}. We note that, when $e < 10^{-6}$, the solver struggles to find an accurate solution for some low values of μ, as it fails to decrease the duality gap to less than 10^{-7}. The inaccurate optimal dual solutions are nevertheless close to the accurate primal optimal solutions within 10^{-4}.

where $\mathscr{C}^{(k_1,\ldots,k_n)} = \{\frac{1}{2}|\beta^{\perp}_{k_1}\rangle\langle\beta^{\perp}_{k_1}|,\ldots,\frac{1}{2}|\beta^{\perp}_{k_n}\rangle\langle\beta^{\perp}_{k_n}|\}$. For a credit card containing n states, problem (5.11) may then be recast as:

$$\begin{aligned}
&\min \mathrm{Tr}\left(L_1^{(n)}(\mu)J(\Lambda^{(n)})\right)\\
&\text{s.t.}\,\mathrm{Tr}_{\mathscr{H}_1^{(n)}\otimes\mathscr{H}_2^{(n)}}\left(J(\Lambda^{(n)})\right) = \mathbb{1}_{\mathscr{H}_{\mathrm{mint}}^{(n)}}\\
&\quad \mathrm{Tr}\left(E_1^{(n)}(\mu)J(\Lambda^{(n)})\right) = e\\
&\quad \mathrm{Tr}\left(E_1^{(n)}(\mu)J(\Lambda^{(n)})\right) \geqslant \mathrm{Tr}\left(E_2^{(n)}(\mu)J(\Lambda^{(n)})\right)\\
&\quad \mathrm{Tr}\left(L_1^{(n)}(\mu)J(\Lambda^{(n)})\right) \geqslant \mathrm{Tr}\left(L_2^{(n)}(\mu)J(\Lambda^{(n)})\right)\\
&\quad J(\Lambda^{(n)}) \geqslant 0
\end{aligned} \tag{5.17}$$

To derive the dual problem associated with (5.17), we first note that we can replace all inequalities by equalities (except the last semidefinite positive constraint) without loss of generality. This is due to the fact that the adversary can always symmetrize the probabilities by increasing the error rate or losses on card 2 to make them equal to those on card 1. The right hand side elements of the constraints from (5.17) may then be gathered in a $(4^{2n}+3)$-dimensional column vector $\vec{b}^{(n)}$. The first three elements read $(e,e,0)$, and correspond to the value of $\mathrm{Tr}\left(E_1^{(n)}(\mu)J(\Lambda^{(n)})\right)$, $\mathrm{Tr}\left(E_2^{(n)}(\mu)J(\Lambda^{(n)})\right)$ and $\mathrm{Tr}\left(\left(L_1^{(n)}(\mu)-L_2^{(n)}(\mu)\right)J(\Lambda^{(n)})\right)$, respectively. The 4^{2n} other elements, corresponding to the first, trace-preserving constraint of (5.17), may be written as the vector representation of the identity over space $\mathscr{H}_{\mathrm{mint}}^{(n)}$. The vector representation $vec(O)$ of an operator O is obtained through the following isomorphism [94] :

$$\sum_{ij=1}^{d} O_{ij}|i\rangle\langle j| \rightarrow \sum_{ij=1}^{d} O_{ij}|i\rangle\otimes|j\rangle\,. \tag{5.18}$$

The dual problem then maximizes the overlap of variable $\vec{d}^{(n)}$ with constraint vector $\vec{b}^{(n)}$

as:

$$\begin{aligned}&\max\ \vec{b}^{(n)T}\vec{d}^{(n)} = ed_1^{(n)} + ed_2^{(n)} + \mathrm{Tr}(D^{(n)})\\&\text{s.t. } d_1^{(n)}E_1^{(n)}(\mu) + d_2^{(n)}E_2^{(n)}(\mu) + d_3^{(n)}\left(L_1^{(n)}(\mu) - L_2^{(n)}(\mu)\right) + \mathbb{1}_{\mathscr{H}_1^{(n)}\otimes\mathscr{H}_2^{(n)}}\otimes D^{(n)} - L_1^{(n)}(\mu) \leqslant 0,\end{aligned} \tag{5.19}$$

where $D^{(n)}$ is a $4^n \times 4^n$ matrix containing the elements $d_4^{(n)}$ to $d_{4^{2n}+3}^{(n)}$ arranged in order left to right, top to bottom.

We note that a tensor product of optimal solutions $J(\Lambda^{(n)}) = \bigotimes_{j=1}^{n} J(\Lambda)$ represents a feasible solution to primal problem (5.17), as it satisfies all the constraints. We label the associated primal objective function value as $s_p^{(n)}$, and remark that $s_p^{(n)} = s_p^{(1)} = f_d$ for all n. We then search for a feasible solution $\vec{d}^{(1)}$ to the dual problem (5.19) which allows to achieve $s_p^{(1)} = s_d^{(1)}$, where $s_d^{(1)}$ is the dual objective function value. While we were not able to find a generic analytical solution to this problem, we have always found a numerical solution $\vec{d}^{(1)}$ for a representative set of parameters μ and e (specified in Table 5.2), satisfying:

$$\begin{aligned}&d_1^{(1)}, d_2^{(1)} < 0 \qquad D_{ij}^{(1)} = 0 \text{ for } i \neq j\\&d_3^{(1)} = 0.5 \qquad \mathrm{Tr}(D^{(1)}) = s_p^{(1)} - (d_1^{(1)} + d_2^{(1)})e,\end{aligned} \tag{5.20}$$

and presenting a duality gap of order 10^{-9}. Furthermore, adding the last condition as constraint to the SDP does not change the optimal value (within 10^{-4} error, due to the fact the the value of $s_p^{(1)}$ is a numerical primal optimal value which is rounded up when added as a constraint in the dual problem). We now conjecture that these conditions can be enforced for all n. The conditions on $d_1^{(1)}, d_2^{(1)}, d_3^{(1)}$ then allow the following expression of the dual constraint with $\mathrm{Tr}(D^{(n)}) = s_p^{(n)} - (d_1^{(n)} + d_2^{(n)})e$:

$$-|d_1^{(n)}|E_1^{(n)}(\mu) - |d_2^{(n)}|E_2^{(n)}(\mu) - 0.5\left(L_1^{(n)}(\mu) + L_2^{(n)}(\mu)\right) + \mathbb{1}_{\mathscr{H}_1^{(n)}\otimes\mathscr{H}_2^{(n)}}\otimes D^{(n)} \leqslant 0. \tag{5.21}$$

Since the error and loss operators are all positive semidefinite, then it follows that the sum of the first four terms in (5.21) is always a negative semidefinite operator. Numerically, it appears to be possible to satisfy (5.21) by choosing appropriately the diagonal elements of $D^{(n)}$.

In conclusion, we have found two feasible solutions such that $s_p^{(1)} = s_d^{(1)}$, and strong duality seems to hold for problems (5.17) and (5.19), at least up to numerical precision. The optimal solution to the primal problem for n states can therefore be written as a tensor product of optimal solutions to the primal problem for $n = 1$ state. This implies that the adversary does not gain any advantage in correlating the states in the card when performing an attack against a trusted terminal without phase randomization. A

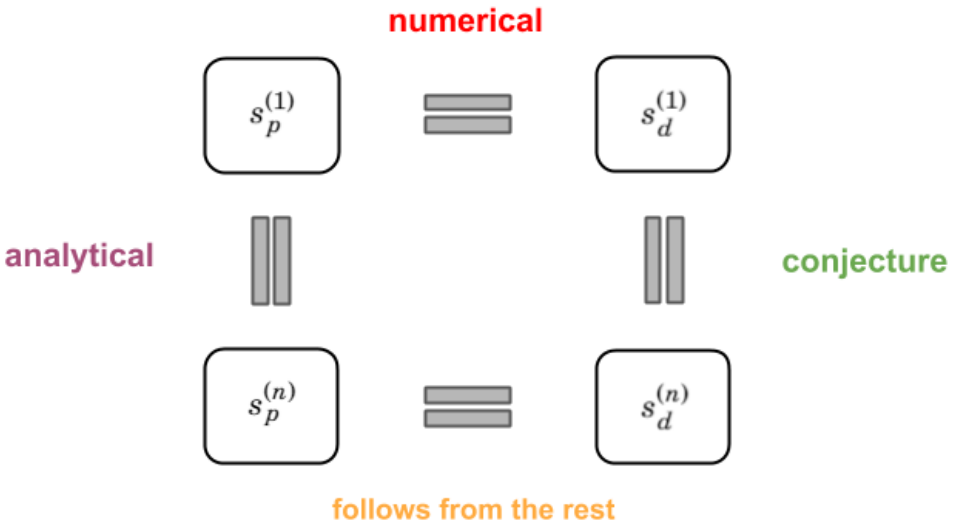


Figure 5.6: **Equalities between optimal values and how they were established.** We have shown numerically that strong duality holds for the 1-state problems: $s_p^{(1)} = s_d^{(n)}$. We have shown analytically that the optimal solution of the 1-state primal problem is a feasible solution for the n-state primal problem, which implies $s_p^{(1)} = s_p^{(n)}$ provided that the conditions from Eq. (5.20) also hold for n states, as conjectured.

similar approach works to prove strong duality for the untrusted terminal case, and we conjecture that this method also works for both scenarios with phase-randomized states.

5.5 Independent work

Independent work also simultaneously reported a semi-device-independent quantum money security proof in [47]. The initial focus, however, differs from ours as it is not targeted towards practical implementation and aims at treating the more extreme scenario of all parties being dishonest but the verification bank: scenario (iv) from Table 5.1. The cost of this stronger threat model is that the quantum states sent by the adversary must be assumed to have bounded dimension (here, 2 dimensions = a qubit), and qubit-by-qubit counterfeiting only is considered. In our case, we do not limit ourselves to such attacks (Section 5.4.3), but part of the proof relies solely on numerical evidence.

The quantum information literature actually initially used the terminology "semi-device-independent" (SDI) from [83] to describe scenarios in which the quantum data has bounded dimension, as in [95]. However, the terminology in our work is used to design other assumptions:

(i) The device is partially uncharacterized. Here, we only make an assumption on the type of device used (threshold detector) in order to reduce our infinite-dimensional security analysis to a 3-dimensional space. This follows the definition from [96], in which SDI can apply to cases where some assumptions are made on the device (of which a dimension constraint is one example, but not the only one): *«a popular relaxation of this approach is called semi-device-independent (SDI), where some assumptions regarding devices are made. The most common assumption is a constraint on the dimension of quantum systems»*. Another example is the talk from [3], in which Pironio defines SDI as simply "based on few assumptions", and gives one-sided quantum cryptography or measurement-device-independence as examples.

(ii) One of the two devices is completely untrusted. This follows the definition from [97]: *«a semi-device-independent certification scenario is one in which at least one party is device-dependent, which is often called trusted, and at least one is device-independent, often called untrusted.»*

5.6 Conclusion

By establishing an optimization framework in the coherent state setting, we have derived secure regions of operation for quantum credit card schemes in both trusted and untrusted terminal scenarios. With phase-randomized states, we have shown that the former case can be secure using a setup with detection efficiency $\eta_d > 80\%$ and noise tolerance around $e = 1$–2%, while the latter case requires tighter parameters: $\eta_d > 95\%$ and noise tolerance lower than $e = 1\%$. The conditions for the trusted terminal are achievable with current nanowire single photon detectors ($\eta_d \approx 85\%$) and the cold atomic quantum memory setup from [98], which presents high state fidelity $\approx 99\%$ and has now been improved to allow 85% storage/retrieval efficiency.

Using the duality of semidefinite programs, we have provided numerical evidence that the adversary cannot increase his/her cheating probability by correlating the n states in the credit card. In such a setting, the uncertainty on the tolerated number of incorrect outcomes en and excess losses $f_d n$ scales as $\sqrt{n}$.

CHAPTER 6

EXPERIMENTAL DEMONSTRATION OF GENUINE CREDIT CARD STORAGE

6.1 Motivation

This chapter focuses on the experimental demonstration of a trusted terminal quantum credit card scheme including the full quantum storage process. Although the setup is currently being optimized and the results are in progress, we describe the experiment in detail and focus on new practical security issues. Following the remarks and results from Chapters 4 and 5, the contributions in this chapter are two-fold.

On the theory side, we propose an implementation which is secure against all loss-dependent attacks, including the previously mentioned USD and 50/50 card splitting attacks, assuming that the quantum storage device *only* is imperfect. For this purpose, we use the general numerical bounds from Chapter 5 to calculate the range of experimental parameters for which the proposed implementation can be information-theoretically secure. We then closely investigate the physical setup, and state under which assumptions these bounds can be satisfied experimentally. We raise new security questions, including the possibility of phase randomization in the presence of electromagnetically-induced transparency, and the need for a time-dependent security proof to account for the decoherence of the quantum memory.

On the experimental side, we change two major components with respect to Chapter 4. First, the polarization-encoded weak coherent states are now generated in free space,

at 894nm instead of 1550nm, in order to fully match the requirements of the quantum storage device. Second, we add the quantum storage device itself, which consists of a laser-cooled, magneto-optically trapped, cloud of cesium atoms, provided by Laboratoire Kastler Brossel [98]. By generating electromagnetically-induced transparency, introduced in Section 2.3.3, the effective polarization qubit contained in each state can be mapped onto a collective atomic excitation, before being retrieved on demand. Furthermore, the cloud is spatially trapped by two pairs of coils only to achieve an elongated, cigar-type shape [98]. This spatial configuration allows for high storage and retrieval efficiency, which is required to satisfy the strict security bounds from Chapter 5.

6.2 Protocol

In this section, we recall the trusted terminal protocol from Chapter 5, and describe it from a more practical perspective:

1) The mint generates an N-bit secret classical key $k^{(s)}$, where s is the unique public serial number of the quantum credit card. For each bit, it picks either the horizontal/vertical $\{H,V\}$ polarization basis or the diagonal/antidiagonal $\{D,A\}$ polarization basis at random. The information is then encoded onto the following coherent states:

$$\begin{aligned} |H(\alpha)\rangle &= |\alpha\rangle \otimes |0\rangle \qquad |V(\alpha)\rangle = |0\rangle \otimes |-\alpha\rangle \\ |D(\alpha)\rangle &= |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |\tfrac{\alpha}{\sqrt{2}}\rangle \quad |A(\alpha)\rangle = |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-\tfrac{\alpha}{\sqrt{2}}\rangle , \end{aligned} \tag{6.1}$$

where the first and second Fock spaces denote the horizontal and vertical polarization modes, respectively. If the $\{H,V\}$ basis was picked, bits 0 and 1 are respectively encoded as $|H(\alpha)\rangle$ and $|V(\alpha)\rangle$. If the $\{D,A\}$ basis was picked, bits 0 and 1 are respectively encoded as $|D(\alpha)\rangle$ and $|A(\alpha)\rangle$.

2) The states are stored in the quantum memory, and handed to a client.

3) When the client wishes to make a payment, the states are retrieved from the quantum memory by a trusted payment terminal (measurement setup), which measures all N of them in either the $\{H,V\}$ or the $\{D,A\}$ basis, picked at random.

4) The measurement outcomes and their basis, along with the serial number s, are sent to the distant bank in the form of classical data. After randomly assigning an outcome to any double-click, the bank checks that at least $(1-e)$ of these outcomes coincide with the secret key $k^{(s)}$, and that the number of no-detection outcomes do not exceed the honest

calibrated losses. Provided that these conditions are satisfied, the credit card is accepted and the payment can proceed. Otherwise, the protocol aborts.

6.3 Experimental principle

6.3.1 Outline

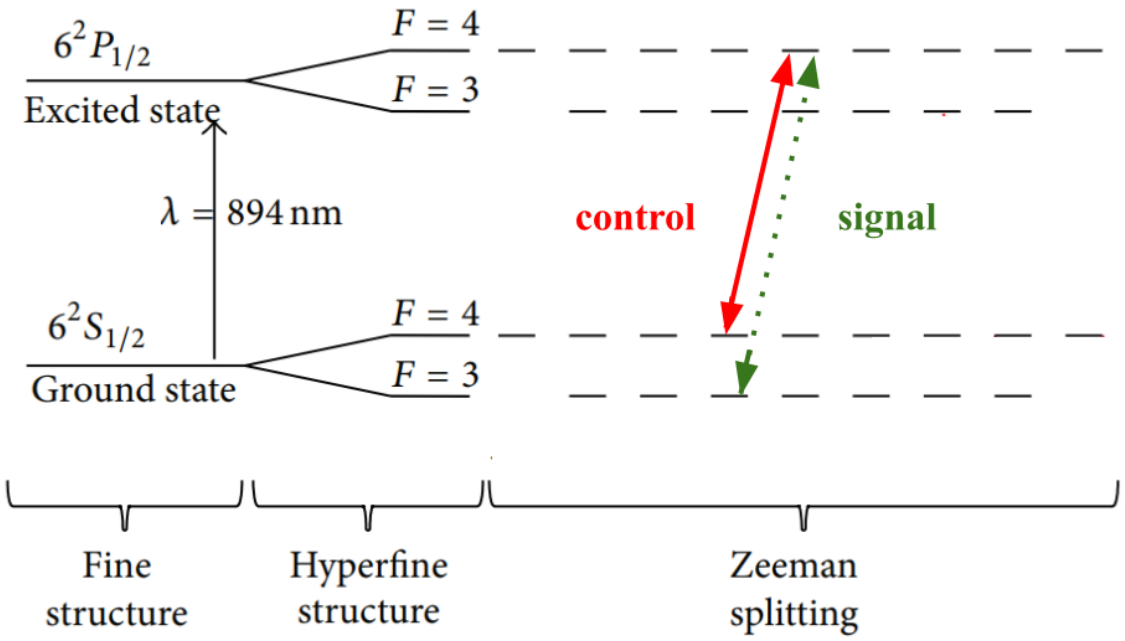


Figure 6.1: **The atomic Λ-system in our experiment.** The signal field is tuned to the D_1 line of cesium (≈ 894 nm). This transition arises from the fine structure splitting, which occurs from the interaction of the electrons' spin with their orbital angular momentum. The Λ-system appears between the hyperfine levels, which are created by the interaction of the nuclear magnetic dipole moment with the magnetic field generated by the electrons. Our signal field is specifically tuned to the $S,F3 \rightarrow P,F4$ transition, while the control field is tuned to the $S,F4 \rightarrow P,F4$ transition. Further unwanted Zeeman splitting occurs due to the magnetic fields which are used to trap the atoms. These are responsible for the main decoherence process in the quantum memory. *The original figure may be found in [99].*

Here, we briefly describe the proposed experimental steps leading to the demonstration of the trusted terminal scheme from Section 6.2:

- **State preparation:** The mint generates an on-the-fly sequence of coherent states thanks to a continuous laser beam chopped up by an acousto-optic modulator.

Each state's polarization is then encoded in real-time using a voltage-driven phase modulator.

- **Quantum storage:** The mint maps the two polarization components of each state onto two spatially-multiplexed collective atomic excitations, in a cloud of cold trapped cesium atoms. This is done using the EIT (presented in Section 2.3.3). The three level system used for EIT is created on the hyperfine levels of the cesium D_1 line, as detailed in Fig. 6.1.

- **Measurement:** The vendor's trusted payment terminal retrieves each state stored in the quantum memory, and performs the measurements dictated by the protocol from Section 6.2, with the help of a half waveplate, a polarization beamsplitter, and two single photon threshold detectors. An additional filtering step is required to eliminate the noise coming from the control pulse used to induce EIT.

- **Data processing:** The vendor's payment terminal transfers the raw classical measurement outcomes to the bank, which performs the required data analysis and accepts or rejects the credit card.

6.3.2 Setup

We now provide a more detailed description of the experimental setup, organized according to the four steps of Section 6.3.1.

State preparation. The signal beam is produced by a continuous Toptica DLpro laser at 894 nm, tuned on the cesium D_1 transition pictured in Fig. 6.1. We chop the light into 300ns pulses using an acousto-optic modulator (AOM), whose operation mode is similar to that from Section 4.4.2. The light is attenuated to the desired average photon number per pulse using density filters. We then encode the pulses' polarization with a Pockels cell, essentially acting as a phase modulator: the incident linear polarization must be input at 45° with respect to the crystal's principal axes, and can then be rotated by changing the refractive index between the two axes through a voltage swing. Note that, unlike the telecom-wavelength implementation from Chapter 4, the shorter wavelength requires a much higher voltage range to rotate the polarization from horizontal to vertical ($\approx 0 - 700V$). This implies the use of a high-voltage power amplifier which allows such a voltage swing at fairly high repetition rates ($\approx 10 - 100$ kHz). We use the PZD350A model from Trek to accomplish this, which preserves the square shape of our voltage steps well enough up to $50 - 100$ kHz. The sequence of voltage steps, corresponding to the randomly

generated states from the protocol, are generated in real-time by the same C++ program and NI acquisition cards similarly to Chapter 4, and fed to the phase modulator.

Quantum storage. We use the phenomenon of electromagnetically-induced transparency (EIT), presented in detail in Section 2.3.3, in a cloud of cold neutral cesium atoms. The exact configuration is a magneto-optical trap (MOT), which involves both laser cooling to around $20\mu K$ and spatial atomic trapping with magnetic coils [98]. The key novelty is the shape of the atomic cloud, which, instead of being spherical, achieves an elongated cigar shape, as depicted in Fig. 6.2. This spatial configuration increases the optical depth of the cloud, which allows to reach high storage/retrieval efficiency, potentially up to 85% [100]. The efficiency is currently being optimized to reach such values, which are required to perform our quantum money scheme (refer to Section 6.4.1 for further detail).

The effective qubit (i.e. the polarization of the weak coherent state), is stored within the cloud by spatially multiplexing its two components: the horizontal and vertical components are first separated with a beam-displacer (BD1), before being focused onto the cloud with a lens such that they both intersect in the center with a 0.4° angular separation. Between the lens and the cloud, a half-wave plate is used to flip the polarization of the vertical mode to horizontal, such that both components have identical polarizations. These are then changed to right-handed circular polarization with a quarter waveplate, in order to interact optimally with the hyperfine atomic levels from Fig. 6.1.

The setup has to be well synchronized by an FPGA, such that the atoms undergo magneto-optical trapping and are released just before the coherent state arrives. This is required because the strong magnetic trapping fields have to be turned off before performing EIT, in order to avoid additional Zeeman splittings. We note that there inevitably remains Zeeman splittings due to Earth's local magnetic field and the Eddy currents generated by the abrupt switching-off of the trapping fields. This is the main source of decoherence in the quantum memory, as it broadens the spectrum of the hyperfine levels. This leads to the need for a time-dependent security analyis, as performed in Section 6.5. In order to limit these splittings, a magnetic field cancellation step must be realized [98].

A strong control beam, detuned by 9.192 GHz and phase-locked with the signal (Section 6.4.3), is then applied to the cloud to produce EIT. It is applied a second time when the state must be retrieved. We refer the reader to [98] for a more detailed description of the synchronization process. Once the collective atomic excitation has been mapped back onto a polarization state, the two components exit the cloud and are rotated and recombined thanks to another quarter waveplate, half waveplate, and beam

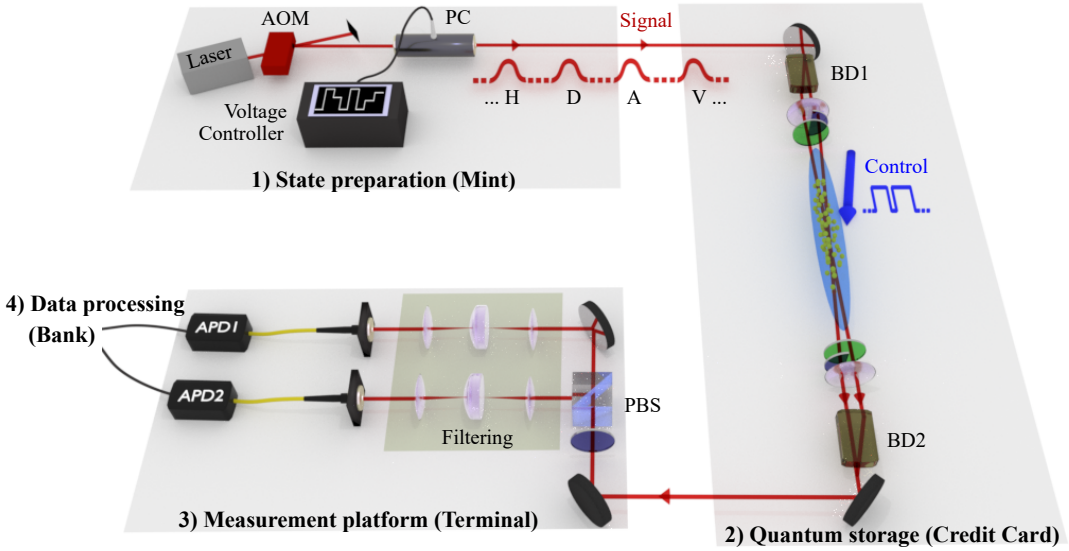


Figure 6.2: **Experimental setup for credit card generation, storage, and measurement.** The signal is produced by a continuous, attenuated laser at 894nm, chopped into pulses using an acousto-optic modulator (AOM). Polarization is encoded in real time using a Pockels cell (PC). Components are then separated on a beam displacer (BD1), and focused onto the cloud with a lens (purple disk). Prior to the cloud, the vertical component is flipped to horizontal using a half waveplate (black half-disk). Both horizontal components are then transformed into right-circular using a quarter waveplate (green disk). These are mapped onto a collective atomic excitation, thanks to a control beam which creates EIT. The control beam is re-applied when the polarization states must be retrieved, and the same set of waveplates and beam displacer (BD2) inverts the previous polarization transformation, and recombines the two components. Measurement consists of another half waveplate (black disk) for basis selection and a polarizing beamsplitter (PBS) for projection. Two Fabry-Pérot cavities are used to filter out the control beam. States are finally detected using two avalanche single photon detectors (APD1 and APD2).

displacer (BD2).

Filtering and measurement. The measurement setup consists of a half waveplate, which selects the measurement basis (oriented at a 0° or 22.5° angle with respect to the horizontal mode), followed by a polarizing beamsplitter (PBS), which splits the horizontal and vertical components of the incoming state. Before measuring the states with two 50% detection efficiency avalanche single photon detectors (one for each polarization mode), we require an extra filtering step, in order to eliminate the control beam contamination. This is realized with two Quantaser FPE001A Fabry-Pérot cavities. The distance between the cavity mirrors can be finely tuned by controlling the temperature inside the cavity. Since the mirrors are highly reflective, the transmission peak corresponding to the cavity's fundamental mode is very narrow: with fine tuning, we may therefore transmit $\approx 75\%$ of the signal and attenuate the control by $50dB$.

Data processing. We register the single photon detectors' TTL signals with the FPGA, allowing precise synchronization with the rest of the setup. A vector of outcomes is then exported as a text file, which, after assigning a random outcome to each double-click, helps to compute the loss and error rates.

6.4 Practical security

6.4.1 Secure parameter range (reminder)

We briefly review the numerical results from Chapter 5 which are of interest to this implementation. Focusing on the trusted terminal scheme, we recall Fig. 5.4 and remark that the required experimental parameters are too tight for our setup: the highest allowed error rate lies around 0.65% for a setup with 100% total transmission efficiency and average photon number per pulse $\mu = 0.5$. Although the quantum memory achieves high fidelity of around 98% with $\mu = 0.5$ [98], this will exceed this small allowed error rate.

In order to increase the noise tolerance, we therefore require phase randomization, and recall the corresponding results from Chapter 5, displayed again here in Fig 6.3. For a reminder of how phase randomization works, and why it increases the noise tolerance, please refer to Section 4.3.4 and Appendix A.2. In this figure, the allowed error rate is increased to almost 3% for 100% total transmission, and to 2% for 85% total transmission with $\mu \approx 1$. Note that, since the state fidelity of our quantum storage device increases with μ, this new range of parameters can allow us to find the optimal trade-off between

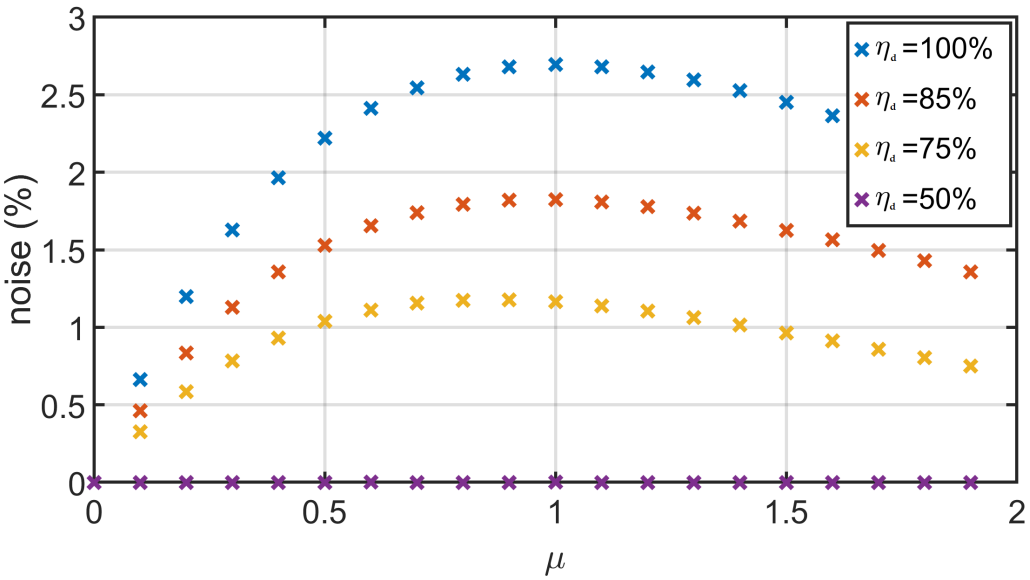


Figure 6.3: **Noise tolerance as a function of average photon number μ.** Points give the allowed error rate e (in %) given a fixed detection efficiency η_d and fixed photon number per pulse μ. These are calculated by solving problem (5.13) numerically.

average photon number and experimental error rate.

6.4.2 Post-selection assumptions

Here, we clearly state the assumptions required to claim a secure demonstration of the quantum money scheme. We start by emphasizing that our single photon detectors exhibit 50% detection efficiency only, which, regardless of the remaining setup losses, is already enough for the 50/50 card split attack to take place. This implies that some form of post-selection *must* be performed. We therefore argue that, although the demonstration cannot be information-theoretically secure with the current setup, we focus on the novel demonstration of a quantum-cryptographic task that is information-theoretically secure in the presence of an imperfect storage device *only*.

Effectively, this amounts to assuming an ideal setup with 100% transmission efficiency (regarding state generation, transmission, filtering and detection), to which we add an imperfect and realistic quantum storage device with 85% storage/retrieval efficiency. This assumption can be justified by noting that the key difficulty in quantum money scheme implementations is the quantum memory. Furthermore, the performance of single photon detectors can always be boosted ($\approx 85\%$ for superconducting nanowire detectors and 95% for transition-edge sensors [93]), and the channel losses are minimal

since the transfer of quantum states is done locally with the payment terminal.

With these assumptions, the detection efficiencies from Fig. 6.3 may now be associated with the storage/retrieval efficiency of the quantum memory, and the secure range of parameters therefore lies along the $\eta_d = 85\%$ curve. As long as our quantum memory setup achieves 85% storage/retrieval efficiency and below 2% error rate for values of $\mu \approx 1$, then we may demonstrate an information-theoretically secure scheme in the presence of a realistic quantum storage device.

6.4.3 Phase locking and randomization

In order to produce successful EIT, the signal and control beams must be *locked in phase*. This allows to finely adjust the small detuning of the control with respect to the signal, which must be equal to 9.192 GHz, i.e. the energy difference between the $S,F3$ and $S,F4$ hyperfine atomic levels of Fig. 6.1.

Before performing such phase-locking, the signal frequency must first be stabilized and locked on the $S,F3 \rightarrow P,F4$ atomic transition. This can be achieved with a warm, room-temperature atomic vapor (as opposed to the cold atomic cloud) through saturated absorption. This technique, which consists of two counter-propagating pump and probe laser beams, allows to finely measure the atomic transition at room-temperature despite the large Doppler broadening which introduces uncertainty on the absorption width. The first intense pump essentially saturates the atomic medium, i.e. brings 1/2 of the population to the excited state while 1/2 remains in the ground state. The counter-propagating probe beam then triggers stimulated emission in the excited atoms that it encounters, which leads to a dip in the absorption ray. From Fig. 6.1, we note that there are four possible hyperfine transitions on the cesium D_1 line, which leads to four absorption dips. The signal can then be locked onto the desired transition, by tracking and minimizing the error signal using an active feedback loop. This is called PID locking: the feedback adjusts the laser frequency by acting on the piezo of the laser cavity mirror.

Once the signal is locked onto the right frequency, the relative phase between the signal and control must now be locked to match the precise 9.192 GHz detuning. This is achieved by interfering the two lasers on a 50/50 beamsplitter, and converting the resulting optical inteference into an electric signal. The beating is then compared to a reference microwave signal with frequency equal to 9.192 GHz, and adjusted with an active feedback loop.

As explained in Section 6.4.1, phase randomization is required to increase the noise and loss tolerance to values which can be reached with our current setup. Generally, this

may be performed by adding a phase modulator, to which we apply a new random voltage for each state, before the Pockels cell polarization encoding. In usual QKD schemes, or in our proof-of-principle experiment from Chapter 4, it is fair to assume that phase randomization has been performed, or to even perform it practice. However, when the encoded states must be phase-locked with another laser, this raises a new problem:

How can signal and control be locked in phase when the signal's global phase is actively scrambled?

We answer this question by proposing two solutions, which can be mentioned as assumptions in our experimental demonstration. Before the generation and storage of each new credit card state:

- The signal and control beams are both phase-randomized in the same way *before* phase-locking is realized. This involves applying the same random voltage to two identical phase modulators, in precise synchronization with the signal pulse chopping. The voltage applied changes before each new pulse.
- The signal laser is switched on and off, causing the global phase to be effectively randomized. Signal frequency-locking and phase-locking between the two lasers must then be performed again.

Since both signal frequency locking and signal/control phase-locking are corrected in real-time using active feedback loops, implementing the first solution seems feasible, as the adaptation of the locking after each global phase jump is performed automatically. The second solution, on the other hand, does not seem practical with our current setup, as this would require an automatic way of controlling the lasers *and* of performing the initial signal locking by saturated absorption, fast enough such that the process ends by the time a new state is generated.

6.5 Time-dependent security

The need for a time-dependent security analysis stems from the decohering nature of our quantum storage device. Generally, a lot of the current experimental effort aims at increasing the storage/retrieval efficiency, storage fidelity, and storage time of optical quantum memories. However, the achieved values reported for a given setup always decrease in time due to decoherence processes, some of which actually preserve quantum information even though they cannot be retrieved by an honest experimentalist.

Quantum cryptography usually assumes that the adversary has access to ideal quantum devices, measurements, and setups. In a quantum credit card scheme, they may therefore transfer all states to an ideal quantum memory which does not decohere in time. Upon verification, the bank (who is aware of the imperfect characteristics of the original quantum memory) will increase the noise and loss tolerance over time, in order to account for these time-dependent imperfections. However, the adversary's credit card is not subjected to such imperfections. They may therefore boost their cheating probability in time by hiding the consequences of their attack in the extra noise and losses tolerated by the bank.

In our implementation, the mint hands the stored quantum state to the client at time $t = 0$. When $t > 0$, the retrieval efficiency $\eta_m(t)$ starts decreasing with time, thus increasing the losses to $e^{-\mu\eta_d\eta_m(t)}$. The initial retrieval efficiency $\eta_m(0)$ of the quantum memory limits the fraction of the N states that a dishonest client can retrieve to $\left(1 - e^{-\mu\eta_d\eta_m(0)}\right)$. In order to compute such values, we note that our experimental platform presents three major loss mechanisms [98]:

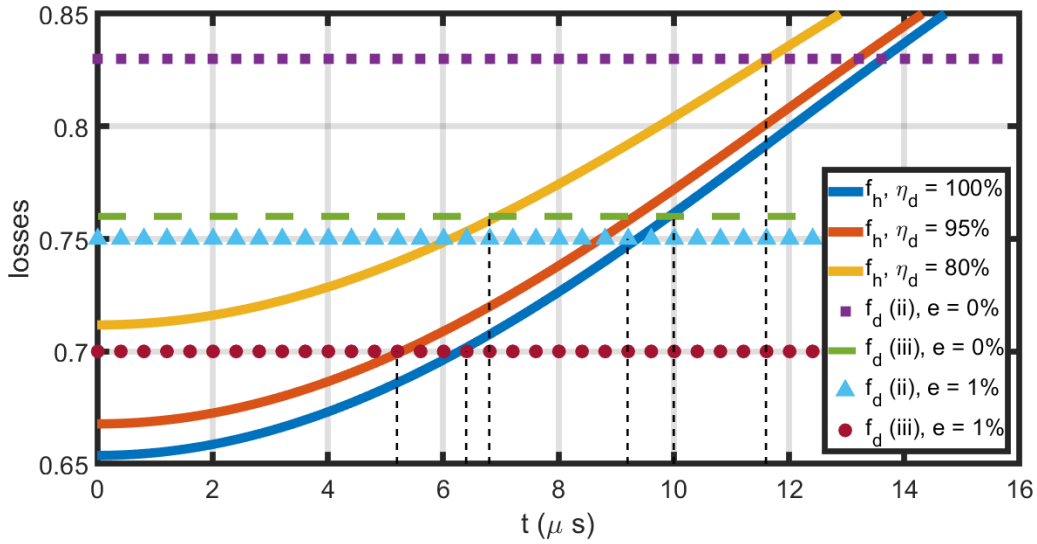
- Dephasing of the collective atomic excitation due to weak residual magnetic fields (from the trapping process): lifetime $\tau_m \approx 15\mu s$.
- Motional dephasing due to the angular dependence of EIT: lifetime $\tau_a \approx 220\mu s$.
- Atomic motion due to finite temperature which decreases the number of atoms in the interaction area: lifetime $\tau_t \approx 7\,\text{ms}$.

Such values show that the retrieval efficiency of the quantum memory is mainly limited by the first mechanism: dephasing of the collective atomic magnetic excitation due to unwanted Zeeman splitting (Fig. 6.1). We indeed have $\tau_m < \tau_a << \tau_t$. This can be combined with the expression for the retrieval efficiency's time-dependence, given in [98]:

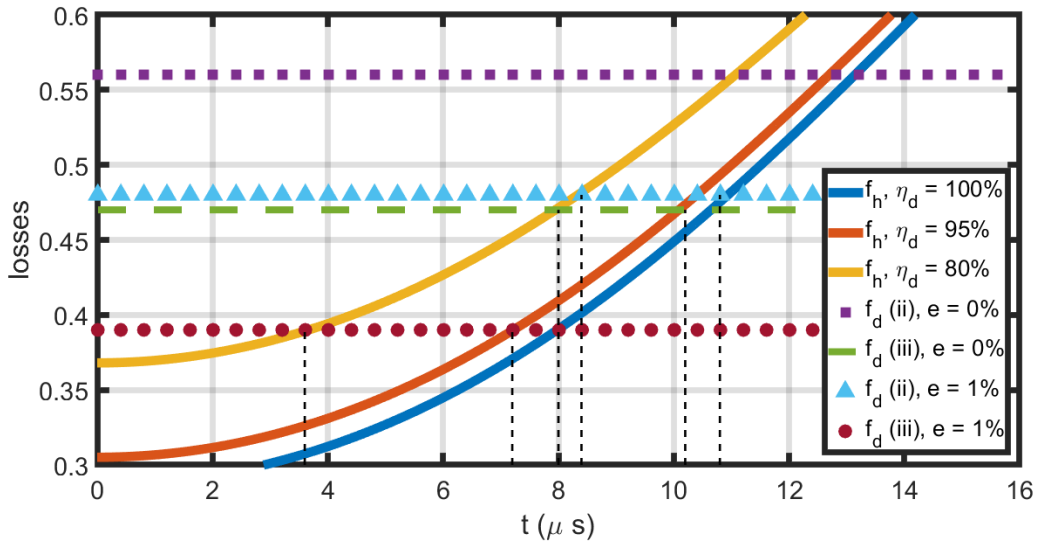
$$\eta_m(t) \approx \eta_m(0) e^{-t^2/\tau^2}, \tag{6.2}$$

where we set $\tau \approx \tau_m$ the lifetime of the dominant loss mechanism, and $\eta_m(0) \approx 85\%$ for our setup. Using this expression, we solve (5.11) with phase-randomized states and derive secure credit card lifetimes of a few μs, as shown in Fig. 6.4 for $\mu = 0.50$ and $\mu = 1.50$.

We now highlight other general security threats which may arise in cold atom-based quantum memories. The first one is caused by fluorescence, which preserves the



(a) $\mu = 0.50$



(b) $\mu = 1.50$

Figure 6.4: **Losses using phase-randomized states as a function of time t.** The solid lines indicate the honest expected setup losses f_h for two values of $\mu = 0.50$ (a) and $\mu = 1.50$ (b), with parameters $\eta_m = 85\%$ and $\eta_d = 100\%$, 95% and 80% from bottom to top. Symbols indicate the dishonest losses f_d induced by the adversary to succeed with error rate $e = 0$ or 1%. The protocol is secure as long as the solid line lies below the symbols.

polarization of the incident light. Although it cannot be retrieved by an experimentalist due to the isotropy of the emission, an adversary with unlimited experimental means can collect all the information that is assumed to be "lost". A second example applies to our quantum setup, since it involves atomic motion due to finite temperature, which causes atoms to gradually escape from the interaction area (where the two spatially multiplexed components meet). The photons emitted by such lost atoms cannot be detected by the honest experimentalist, whereas an adversary can collect all the emission.

The security threat posed by such physical processes may be discarded when their lifetime τ is much larger than the lifetime of other dominant decoherence processes, which is the case in our setup. In the opposite case, these have to be taken into account in the security analysis.

6.6 Conclusion

We have proposed an experimental platform for the near-future implementation of information-theoretically secure quantum money, assuming an ideal setup with an imperfect quantum storage device. In close collaboration with the Laboratoire Kastler Brossel, we are currently building and optimizing the setup, which involves real-time polarization encoding of credit card states, and genuine on-the-fly quantum storage using EIT in a cloud of cold cesium atoms. This aims to provide the first experimental demonstration of a secure quantum-cryptographic task in the presence of a quantum memory.

Assuming that the storage mechanism only is lossy, the memory must achieve 85% storage/retrieval efficiency and we should obtain less than 2% error rate upon verification, given average photon number $\mu \approx 1$. This is within experimental reach, as it has already been demonstrated that using the D_1 line of cesium can provide up to 90% storage/retrieval efficiency [100]. Furthermore, the error rate coming from state preparation can be lowered by decreasing the repetition rate of the experiment (for the voltage amplifier to perform better), and the quantum memory state fidelity can achieve around 99% for $\mu \geqslant 1$ [98].

In the long-term, acquiring superconducting nanowire detectors (which can achieve detection efficiency around 90%), and further optimization of the storage/retrieval efficiency could allow a full demonstration of the trusted-terminal scheme with less post-selection. Furthermore, it would be interesting to attempt the parallel storage of two credit card states at once (as a proof-of-principle step beyond on-the-fly storage), by

adding more spatial multiplexing to the setup for instance.

CHAPTER 7

QUANTUM WEAK COIN FLIPPING WITH A SINGLE PHOTON

7.1 Motivation

Chapter 1 introduced secure coin flipping as one of the building blocks of classical and quantum communication networks. It is a crucial primitive in multiparty computing [1], online gaming and more general randomized consensus protocols [2]. Its importance stems from the fundamentality of the task it accomplishes: generating randomness between two distant parties who do not trust each other. Strong coin flipping (SCF) guarantees that none of the two parties can bias the outcome with probability higher than $(1/2+\epsilon)$, where ϵ is the protocol bias. Weak coin flipping (WCF) performs the same task when both parties have a preferred, opposite outcome: it effectively designates a winner and a loser.

In the classical world, coin flipping is only possible using computational assumptions, or under stringent spacetime constraints [101]: the two parties must each broadcast a random bit simultaneously. Once the broadcast is over, they may both agree on the flip outcome by performing the sum of the two bits. If each party's bit is revealed at exactly the same time, then none of the parties could have influenced the outcome of the flip before the broadcast, since they have no a priori knowledge of the other party's bit. This assumption is very strong however, as it requires precise clock synchronization between both parties, which in turn poses a security flaw: either one of the two parties must

control clock synchronization, or both parties must agree on a trust third party. None of these assumptions are allowed in a secure coin flipping protocol. Using the entanglement property of quantum mechanics allows to bypass this practical issue.

Despite its *weak* name (due to the fact that two out of four biases remain unconstrained, as shown in Section 7.5), quantum WCF allows to construct optimal quantum SCF schemes: combining an unbalanced quantum WCF with cheating probability $(1/2+\epsilon)$ with a classical coin flip yields the optimal SCF with cheating probability $(1\sqrt{2}+\epsilon)$ [25]. WCF schemes also help construct other crucial primitives such as bit commitment [26].

Unlike quantum SCF for which the lowest possible bias is $\epsilon = (1/\sqrt{2} - 1/2)$ [61], quantum WCF may achieve biases arbitrarily close to zero [102, 103]. In 2002, two explicit protocols were proposed, which both allowed to reach small biases: the work from [104] achieved $\epsilon \approx 0.239$, while the work from [18] achieved $\epsilon = (1/\sqrt{2} - 1/2) \approx 0.207$ (which is coincidentally the SCF lower bound). Later, it was shown that the scheme from [18] in fact belonged to a larger family of WCF protocols, of which 1/6 was the lowest bias allowed [105, 106]. Very recently, a new explicit family of protocols achieved $\epsilon = 1/10$ [95].

While quantum SCF protocols have been experimentally demonstrated [62–64], no implementation has ever been proposed for quantum WCF. This may be explained by two reasons. First, it is difficult to find an encoding and implementation which is robust to losses: a dishonest party may always declare an abort when it is not satisfied with the flip's outcome. Second, none of the previously mentioned protocols translate trivially into a simple experimental setup: they all involve performing single-shot POVM measurements [18], generating beyond-qubit states [104] or performing projective measurements on Hilbert spaces which grow with the number of rounds [105].

In this project, we propose a family of quantum WCF protocols, inspired from [18], which allows to reach biases as low as $\epsilon = (1/\sqrt{2} - 1/2) \approx 0.207$. We replace all POVMs by simple projective measurements, and propose an implementation which involves a single photon and linear-optical circuits only. We encode the information by mixing the photon with vacuum on an unbalanced beam splitter, which generates entanglement. Both parties are then able to agree on a random bit, while the entanglement is simultaneously verified. We derive a practical security proof, considering the extension to infinite Hilbert spaces, and show that the fairness and balance of the protocol are preserved through a few kilometers of lossy optical fiber and non-unit detection efficiency. We emphasize that this encoding is very robust to noise, as the single photon needs not be pure or indistinguishable from other photons in any degree of freedom, save photon number. Finally, we investigate a simple extension to n rounds in order to achieve lower biases.

7.2 Protocol and correctness

In the honest protocol, Alice and Bob wish to toss a fair coin, with a priori knowledge that they each favor opposite outcomes. Fig. 7.1 represents the implementation of the honest protocol, which follows five distinct steps. Defining $x \in [0, \frac{1}{2}]$ as a free protocol parameter, these read:

1. Alice mixes a single photon with the vacuum on a beam splitter of reflectivity x.
2. Alice keeps the first half of the state, and sends the second half to Bob.
3. Bob mixes the half he just received with the vacuum on a beam splitter of reflectivity $y = 1 - \frac{1}{2(1-x)}$.
4. Bob measures the second register of his state with a threshold detector, and broadcasts the outcome $c \in \{0, 1\}$.
5. This last step is a verification step, which splits into two cases:
   - $c = 0$: Alice sends her half of the state to Bob, who mixes it with his half on a beam splitter of reflectivity $z = 2x$. He then measures the two output modes with threshold detectors. If the outcome is $(1, 0)$, Alice is declared winner.
   - $c = 1$: Bob discards his half, and Alice measures her half with threshold detectors. If the outcome is 0, Bob is declared winner.

We now derive the correctness of the protocol: we show that the protocol is fair, i.e. that the probability of winning is $\frac{1}{2}$ when both parties are honest. Throughout this chapter, operators with a tilde indicate an action on creation operators (framework from Section 2.3.1), while the operator without the tilde indicates the action in Fock space.

The action of a beam splitter of reflectivity r acting on modes k and l is given by

$$\begin{pmatrix} \hat{b}_k^\dagger \\ \hat{b}_l^\dagger \end{pmatrix} = \tilde{H}^{(r)} \begin{pmatrix} \hat{a}_k^\dagger \\ \hat{a}_l^\dagger \end{pmatrix}, \tag{7.1}$$

where $a_k^\dagger, \hat{a}_l^\dagger$ are the creation operators of the input spatial modes k and l, respectively, $\hat{b}_k^\dagger, \hat{b}_l^\dagger$ are the creation operators of the output spatial modes k and l, respectively, and the beam splitter transformation is given by:

$$\tilde{H}^{(r)} = \begin{pmatrix} \sqrt{r} & \sqrt{1-r} \\ \sqrt{1-r} & -\sqrt{r} \end{pmatrix}. \tag{7.2}$$

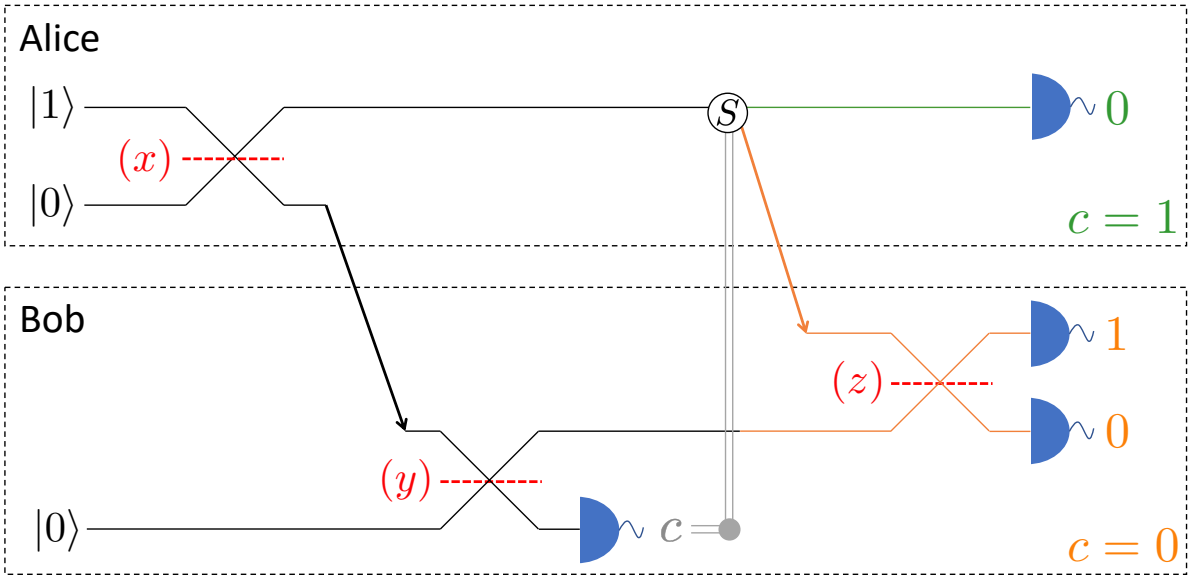


Figure 7.1: **Representation of the honest protocol.** The dashed black lines indicate Alice and Bob's laboratories, respectively, while the dashed red lines represent beam splitters with reflectivity indicated in red. $|0\rangle$ and $|1\rangle$ are the vacuum and single photon Fock states, respectively. Arrows represent quantum communication. Bob broadcasts the classical outcome c, which controls the optical switch S on Alice's side. The protocol when Bob declares $c = 0/1$ is represented in orange/green. The final outcomes are the expected outcomes for an honest protocol.

The evolution of the quantum state over the three modes up to Bob's measurement may then be written as:

$$\begin{aligned} |100\rangle &\underset{(x),12}{\rightarrow} \sqrt{x}\,|100\rangle + \sqrt{1-x}\,|010\rangle \\ &\underset{(y),23}{\rightarrow} \sqrt{x}\,|100\rangle + \sqrt{(1-x)y}\,|010\rangle + \sqrt{(1-x)(1-y)}\,|001\rangle\,, \end{aligned} \tag{7.3}$$

where the notation $(r),kl$ indicates the reflectivity of the beam splitter and the corresponding modes. Hence, the probability that Bob obtains the outcome $c = 1$ when measuring the third register is:

$$P(1) = (1-x)(1-y), \tag{7.4}$$

and $P(0) = 1 - P(1)$. We have $y = 1 - \frac{1}{2(1-x)}$ to ensure that $P(0) = P(1) = \frac{1}{2}$. When outcome $c = 1$ is obtained, the state post-measurement then reads:

$$|00\rangle\,. \tag{7.5}$$

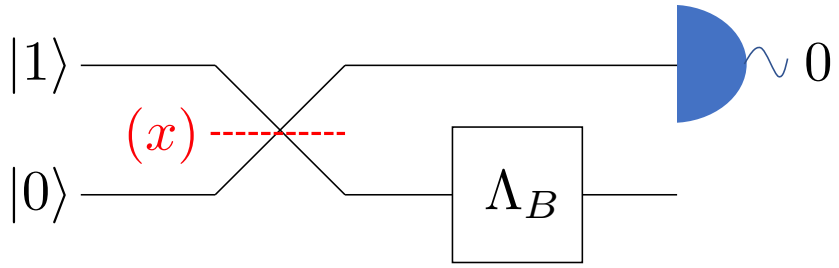


Figure 7.2: **Reduction of the protocol for dishonest Bob.** His most general cheating consists in always broadcasting $c = 1$, and applying a general quantum operation Λ_B to his subsystem. The outcome indicated correspond to Bob winning.

When outcome $c = 0$ is obtained, it reads:

$$\sqrt{2x}\,|10\rangle + \sqrt{1-2x}\,|01\rangle\,, \tag{7.6}$$

In the first case, the measurement performed by Alice outputs 0 with probability 1, while in the second case, the measurement performed by Bob outputs $(1,0)$ with probability 1. Hence, the probability that Alice (resp. Bob) wins is directly given by $P(0)$ (resp. $P(1)$). This shows that the protocol is fair, since $P(0) = P(1) = \frac{1}{2}$.

7.3 Ideal security

We now derive the security of the protocol in the ideal setting, with perfect number-resolving as well as threshold detectors. Namely, we obtain the probabilities of winning when Bob is dishonest and Alice is honest, and when Alice is dishonest and Bob is honest, respectively.

7.3.1 Dishonest Bob

Dishonest Bob should always declare the outcome $c = 1$ in order to maximize his winning probability. The outcome of the coin flip is then confirmed if Alice obtains the outcome 0 upon verification. Bob thus needs to maximize the probability of outcome 0, applying a general quantum operation Λ_B to his half of the state. The reduction of the protocol in this case is given in Fig. 7.2.

However, the probability that the detector clicks is independent of Bob's action. It is given by x, so that Bob's winning probability is upper bounded by $(1-x)$. This upper

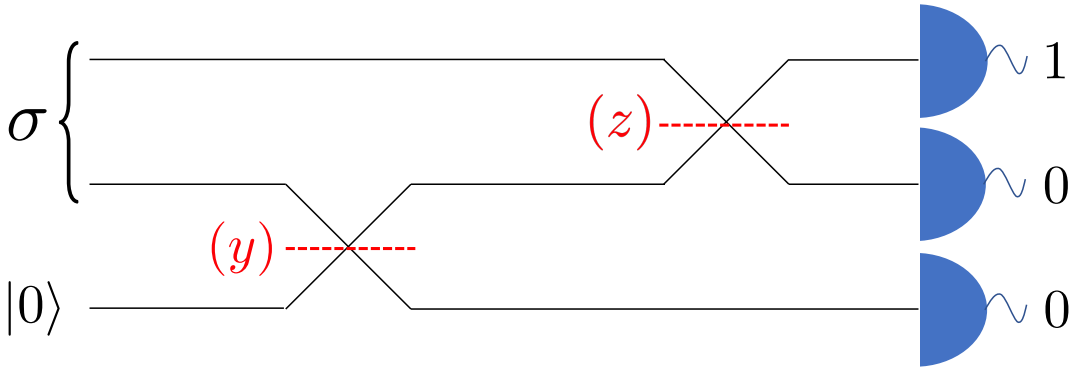


Figure 7.3: **Reduction of the protocol for dishonest Alice.** Her most general strategy is to send a dishonest (mixed) state σ, while Bob performs the rest of the protocol honestly. The outcomes indicated correspond to Alice winning.

bound is reached if Bob discards his half of the state and always broadcasts $c = 1$. Bob's optimal cheating probability is then simply given by:

$$P_d(B) = 1 - x. \tag{7.7}$$

7.3.2 Dishonest Alice with number-resolving detectors

Dishonest Alice wins when Bob declares the outcome $c = 0$ and the outcome of his quantum measurement is $(1,0)$. The reduced protocol is shown in Fig. 7.3. When using number-resolving single-photon detectors, any projection onto the $n > 1$ photon subspace leads to Alice getting chaught cheating. Alice must therefore maximize the overlap with the projective measurement $|100\rangle\langle 100|$ only, as indicated in the honest protocol.

Let σ be the state sent by Alice. Let $U = (H^{(2x)} \otimes \mathbb{1})(\mathbb{1} \otimes H^{(y)})$, with $y = 1 - \frac{1}{2(1-x)}$. Alice needs to maximize the probability of the overall outcome $(1,0,0)$, which is given by

$$P_d(A) = Tr[U(\sigma \otimes |0\rangle\langle 0|)U^\dagger |100\rangle\langle 100|], \tag{7.8}$$

since Bob uses number-resolving detectors. By convexity of the probabilities, we may assume without loss of generality that Alice sends a pure state $\sigma = |\psi\rangle\langle\psi|$, which allows us to write:

$$\begin{aligned} P_d(A) &= Tr[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger |100\rangle\langle 100|] \\ &= Tr[(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger |100\rangle\langle 100|U] \\ &= Tr[\langle\psi| \otimes \langle 0|U^\dagger |100\rangle\langle 100|U|\psi\rangle \otimes |0\rangle]. \end{aligned} \tag{7.9}$$

We have:

$$\begin{aligned} U^\dagger |100\rangle &= (\mathbb{1}\otimes H^{(y)})(H^{(2x)}\otimes\mathbb{1})|100\rangle \\ &= (\mathbb{1}\otimes H^{(y)})(\sqrt{2x}\,|100\rangle + \sqrt{1-2x}\,|010\rangle) \\ &= \sqrt{2x}\,|100\rangle + \sqrt{y(1-2x)}\,|010\rangle + \sqrt{(1-y)(1-2x)}\,|001\rangle\,, \end{aligned} \tag{7.10}$$

and therefore:

$$\begin{aligned} U^\dagger |100\rangle\langle 100| U =& 2x\,|100\rangle\langle 100| + y(1-2x)\,|010\rangle\langle 010| + (1-y)(1-2x)\,|001\rangle\langle 001| \\ &+ \sqrt{2xy(1-2x)}\,(|100\rangle\langle 010| + |010\rangle\langle 100|) \\ &+ \sqrt{2x(1-y)(1-2x)}\,(|100\rangle\langle 001| + |001\rangle\langle 100|) \\ &+ (1-2x)\sqrt{y(1-y)}\,(|010\rangle\langle 001| + |001\rangle\langle 010|)\,. \end{aligned} \tag{7.11}$$

Substituting back into Eq. (7.9) then reduces to:

$$\begin{aligned} P_d(A) &= \langle\psi|\left(2x\,|10\rangle\langle 10| + y(1-2x)\,|01\rangle\langle 01| + \sqrt{2xy(1-2x)}(|10\rangle\langle 01| + |01\rangle\langle 10|)\right)|\psi\rangle \\ &= \langle\psi|\left(\sqrt{2x}\,|10\rangle + \sqrt{y(1-2x)}\,|01\rangle\right)\left(\sqrt{2x}\,\langle 10| + \sqrt{y(1-2x)}\,\langle 01|\right)|\psi\rangle \\ &= \langle\psi|\left(\sqrt{2x}\,|10\rangle + \sqrt{y(1-2x)}\,|01\rangle\right)^2. \end{aligned} \tag{7.12}$$

Using the Cauchy-Schwarz inequality then allows to upper bound $P_d(A)$ as:

$$P_d(A) \leqslant \|\psi\|^2 \left\|\left(\sqrt{2x}\,|10\rangle + \sqrt{y(1-2x)}\,|01\rangle\right)\right\|^2 \leqslant \frac{1}{2(1-x)}\|\psi\|^2, \tag{7.13}$$

which is maximized for $\|\psi\| = 1$. Hence we finally get:

$$P_d(A) \leqslant \frac{1}{2(1-x)}. \tag{7.14}$$

In order to find Alice's optimal cheating strategy (i.e. the optimal pure state $|\psi\rangle$ that she must send to achieve this bound), we remark that the unnormalized state $\sqrt{2x}\,|10\rangle + \sqrt{y(1-2x)}\,|01\rangle$ maximizes the expression in Eq. (7.13). Normalizing this state then provides Alice's optimal strategy, which is to prepare the state:

$$|\phi_x\rangle := 2\sqrt{x(1-x)}\,|10\rangle + (1-2x)|01\rangle\,. \tag{7.15}$$

7.3.3 Dishonest Alice with threshold detectors

Remarkably, the protocol is still secure even if Bob only uses threshold detectors, which is essential to the practicality of the protocol. Moreover, Alice's optimal cheating probability

remains the same in both cases: $P_d(A) = \frac{1}{2(1-x)}$. In particular, for all values of x, we retrieve the property shared by the protocols of [18]: $P_d(A)P_d(B) = \frac{1}{2}$.

Unlike the previous case, incorrect outcomes with higher photon number could still pass the test for $n \geq 1$, since threshold detectors cannot discriminate between a $|100\rangle$ and $|n00\rangle$ projection. We show in the following that this doesn't help a dishonest Alice, and that the strategy described previously for the case of number resolving detectors is still optimal in the case of threshold detectors.

With the same notations as in the previous proof, Alice needs to maximize the probability of the overall outcome $(1,0,0)$, hence the overlap with the projector $\sum_{n=1}^{\infty} |n00\rangle\langle n00| = (\mathbb{1} - |0\rangle\langle 0|) \otimes |00\rangle\langle 00|$. This allows us to write:

$$P_d(A) = Tr[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger((\mathbb{1} - |0\rangle\langle 0|) \otimes |00\rangle\langle 00|)], \tag{7.16}$$

since Bob uses threshold detectors, where $U = (H^{(2x)} \otimes \mathbb{1})(\mathbb{1} \otimes H^{(y)})$ and $y = 1 - \frac{1}{2(1-x)}$.

Linear optical evolution conserves photon number. Hence if Alice sends the vacuum state, the detectors will never click. Removing the two-mode vacuum component of the state prepared by Alice and renormalizing therefore always increases her winning probability. Since we are looking for the maximum winning probability, we can assume without loss of generality that $\langle\psi|00\rangle = 0$, i.e:

$$Tr[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger |000\rangle\langle 000|] = |\langle\psi|00\rangle|^2, \tag{7.17}$$

So maximizing the winning probability in Eq. (7.16) is equivalent to maximizing

$$\tilde{P}_d(A) = Tr[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)], \tag{7.18}$$

given the constraint $\langle\psi|00\rangle = 0$. We have:

$$\begin{aligned} \tilde{P}_d(A) &= Tr[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)] \\ &= Tr[(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)U]. \end{aligned} \tag{7.19}$$

At this point, we use a simple reduction which allows to replace the interferometer U in the above expression by another interferometer V, which will simplify the calculations. This is formalised by the following lemma, proven in Appendix C.1:

Lemma 7.1. *Let $U = (H^{(z)} \otimes \mathbb{1})(\mathbb{1} \otimes H^{(y)})$, with $z > 0$. For any density matrix τ,*

$$Tr[(\tau \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)U] = Tr[(\tau \otimes |0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)V], \tag{7.20}$$

where $V = (\mathbb{1} \otimes H^{(b)})(H^{(a)} \otimes \mathbb{1})(\mathbb{1} \otimes R(\pi) \otimes \mathbb{1})$, with $a = \frac{y(1-z)}{y+z-yz}$ and $b = y + z - yz$, and $R(\pi)$ a phase shift of π acting on mode 2.

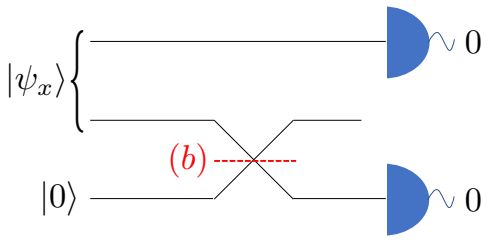


Figure 7.4: **Equivalent picture for dishonest Alice.** In the original dishonest setup of Fig. 7.3, Alice aims to maximize the outcome $(1,0,0)$. This is equivalent to Alice maximizing outcome 0 on spatial modes 1 and 3, independently of what is detected on mode 2. The outcomes indicated correspond to Alice winning. The reflectivity is $b = \frac{1}{2(1-x)}$.

Using Lemma 7.1, Eq. (7.19), and recalling that $(1-x)(1-y) = \frac{1}{2}$ and $z = 2x$, we may thus write:

$$\tilde{P}_d(A) = Tr[(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)V], \tag{7.21}$$

where $V = (\mathbb{1} \otimes H^{(b)})(H^{(a)} \otimes \mathbb{1})(\mathbb{1} \otimes R(\pi) \otimes \mathbb{1})$, $a = (1-2x)^2$ and $b = 1-y = \frac{1}{2(1-x)}$. Let us now define:

$$|\psi_x\rangle := H^{(a)}(\mathbb{1} \otimes R(\pi))|\psi\rangle\,. \tag{7.22}$$

The constraints $\langle\psi|00\rangle = 0$ and $\langle\psi_x|00\rangle = 0$ are equivalent, because the above transformation leaves the total number of photons invariant. With Eq. (7.21) we obtain

$$\tilde{P}_d(A) = Tr[(|\psi_x\rangle\langle\psi_x| \otimes |0\rangle\langle 0|)(\mathbb{1} \otimes H^{(b)})(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)(\mathbb{1} \otimes H^{(b)})], \tag{7.23}$$

with the constraint $\langle\psi_x|00\rangle = 0$. Maximizing this expression thus corresponds to maximizing the probability of the outcome $(0,0)$ when measuring modes 1 and 3 of the state obtained by mixing the second half of $|\psi_x\rangle$ with the vacuum on a beam splitter of reflectivity $b = \frac{1}{2(1-x)}$ (Fig. 7.4).

We now show that an optimal strategy for Alice is to ensure that $|\psi_x\rangle = |01\rangle$. Let us write:

$$|\psi_x\rangle = \sum_{p+q>0} \psi_{pq}\,|pq\rangle, \tag{7.24}$$

where we take into account the constraint $\langle\psi_x|00\rangle = 0$. Then, with Eq. (7.23) we obtain:

$$\begin{aligned}
\tilde{P}_d(A) &= \sum_{p+q>0,p'+q'>0} \psi_{pq}\psi^*_{p'q'} Tr[|pq0\rangle\langle p'q'0|(|0\rangle\langle 0|\otimes H^{(b)}(\mathbb{1}\otimes|0\rangle\langle 0|)H^{(b)})] \\
&= \sum_{q>0,q'>0} \psi_{0q}\psi^*_{0q'} Tr[|q0\rangle\langle q'0|H^{(b)}(\mathbb{1}\otimes|0\rangle\langle 0|)H^{(b)}] \\
&= \sum_{n\geq 0,q>0,q'>0} \psi_{0q}\psi^*_{0q'} Tr[|q0\rangle\langle q'0|H^{(b)}|n0\rangle\langle n0|)H^{(b)}] \\
&= \sum_{n>0} |\psi_{0n}|^2 |\langle n0|H^{(b)}|n0\rangle|^2 \\
&= \sum_{n>0} |\psi_{0n}|^2 b^n,
\end{aligned} \tag{7.25}$$

where we used in the fourth line the fact that $H^{(b)}$ doesn't change the number of photons. We have $b \in [0,1]$, which shows that:

$$\begin{aligned}
\tilde{P}_d(A) &\leqslant b \sum_{n>0} |\psi_{0n}|^2 \\
&= b,
\end{aligned} \tag{7.26}$$

since $|\psi_x\rangle$ is normalized, and this bound is reached for $|\psi_{01}|^2 = 1$, i.e. $|\psi_x\rangle = |01\rangle$. With Eq. (7.22), this implies that an optimal strategy for Alice is to prepare the state

$$\begin{aligned}
|\psi\rangle &= (\mathbb{1}\otimes R(\pi))H^{(a)}|01\rangle \\
&= \sqrt{1-a}\,|10\rangle + \sqrt{a}\,|01\rangle \\
&= 2\sqrt{x(1-x)}\,|10\rangle + (1-2x)|01\rangle \\
&= |\phi_x\rangle\,,
\end{aligned} \tag{7.27}$$

and her winning probability is then $b = 1 - y = \frac{1}{2(1-x)}$. We therefore recover the same result as for number-resolving detectors.

7.4 Noise tolerance

The vacuum/single-photon encoding is very robust to noise, in comparison to polarization or phase encoding for instance: the only property which must be generated and preserved through propagation is photon number. This implies that photon indistinguishability and purity are not required in any degree of freedom other than photon number. In this case, Alice may simply produce a heralded single photon via spontaneous parametric down-conversion (SDPC) [107], which generates a photon pair: one may be used for the flip, while the other may herald the presence of the first one. Given photon-pair-emission

probability p, accidentally emitting two pairs at the same time using SPDC occurs with probability p^2. Since p may be arbitrarily tuned by changing the pump power, p^2 (and therefore the probability of 2 photons being accidentally generated by Alice at once) may then be decreased to negligible values.

We note that, in the case where Alice's single photon source is probabilistic but heralded (as in SPDC), she may always inform Bob of a successful state generation prior to his announcement of c without compromising security. In what follows, we may therefore assume that both parties have agreed on the presence of an initial state, and hence know when the protocol occurs.

Noise will therefore stem from the non-ideal reflectivities of the beam splitters, and the non-zero detector dark count probability p_{dc}. For each party, these may affect the protocol correctness in two ways: an undesired bias of the flip, and an added abort probability during the verification process.

Regarding the flip bias, a change from x to x' in the first beam splitter's reflectivity will cause Honest Alice to generate a slightly different initial entangled state, which will change the correctness from $P(0) = P(1) = 1/2$ to:

$$P(1) = (1-x')(1-y) \qquad P(0) = 1 - P(1). \tag{7.28}$$

Similarly for Bob, a change from y to y' will yield

$$P(1) = (1-x)(1-y') \qquad P(0) = 1 - P(1). \tag{7.29}$$

Regarding the verification process, Alice will call Honest Bob a liar only if she detects a photon. Noisy detectors on Alice's side will therefore cause an unwanted abort with probability p_{dc}, since she always expects the $(0,0)$ vacuum outcome when Bob is honest. With nanowire single photon detectors, this probability is typically very low, of the order of $p_{dc} < 10^{-6}$. Hence the probability that Honest Bob is called a liar is simply $p_{dc} < 10^{-6}$.

For modes 1 and 2, outcome $(0,0)$ is therefore the most problematic case, as it crucially depends on the losses in the setup. We consider this case in Section 7.5.

7.5 Loss tolerance

7.5.1 Correctness

We have just shown that any source of noise in the protocol (which flips a $|0\rangle$ to $|1\rangle$) may be incorporated in the security analysis by simply replacing parameters x, y, and z

with x', y', and z'. Furthermore, this source of error will most likely be negligible with current technology. We therefore solely focus on the more consequential effects of channel losses, as well as non-unit fiber transmission and detection efficiencies, which will be responsible for any flip from $|1\rangle$ to $|0\rangle$. We label η_t the transmission efficiency of Alice and Bob's quantum channel. We then define $\eta_f^{(i)}$ as the transmission efficiency of party i's fiber delay, while $\eta_d^{(i)}$ denotes the detection efficiency of party i's measurement.

We assume that each party introduces a fiber delay whenever they are waiting for the other party's communication. The delay time therefore depends on the distance between the two parties. When both parties are honest, the outcome of the flip may be reduced to the value of the declared outcome c, provided that the quantum verification step yields the awaited outcome: $(1,0)$ for Alice and 0 for Bob.

The correctness on Bob's side is directly given by his chance of detecting the photon (the photon gets to his detector and doesn't get lost):

$$P_h(B) = \eta_t \eta_d^{(B)} (1-x)(1-y). \tag{7.30}$$

On the other hand, Alice wins if the photon, starting from her first input mode, is detected by Bob in the last step. The evolution of the creation operator of the first mode during the lossy honest protocol is given in Appendix C.2. In particular, the photon reaches Bob's first detector with probability:

$$\begin{aligned} P_h(A) &= \left(\sqrt{x \eta_f^{(A)} \eta_t z \eta_d^{(B)}} + \sqrt{(1-x)\eta_t y \eta_f^{(B)} (1-z) \eta_d^{(B)}} \right)^2 \\ &= \eta_t \eta_d^{(B)} \left(\sqrt{xz\eta_f^{(A)}} + \sqrt{(1-x)y(1-z)\eta_f^{(B)}} \right)^2 . \end{aligned} \tag{7.31}$$

Finally, the protocol aborts for all other detection events:

$$P_h(X) = 1 - P_h(A) - P_h(B). \tag{7.32}$$

We may now gather the expressions which give us the correctness and abort probability for the lossy protocol:

$$\begin{aligned} P_h(A) &= \eta_t \eta_d^{(B)} \left(\sqrt{xz\eta_f^{(A)}} + \sqrt{(1-x)y(1-z)\eta_f^{(B)}} \right)^2 \\ P_h(B) &= \eta_t \eta_d^{(B)} (1-x)(1-y) \\ P_h(X) &= 1 - P_h(A) - P_h(B). \end{aligned} \tag{7.33}$$

Therefore, the overall correctness does not depend on Alice's detection efficiency $\eta_d^{(A)}$. We also emphasize that allowing for abort cases may enable some classical WCF protocols

to perform better than quantum WCF. This is because increasing the abort probability effectively decreases Alice and Bob's cheating probabilities. We say that the protocol allows a quantum advantage when it provides better bounds than any classical coin flipping protocol. In Section 7.6, we derive conditions on the protocol parameters which yield quantum advantage, as well as fairness and balance.

7.5.2 Dishonest Bob

In order to maximize his winning probability, Bob's best strategy in the lossy setting is to perform the same attack as in the lossless case, because he has no control over Alice's half of the subsystem. His winning probability is then upper-bounded by:

$$P_d(B) \leqslant 1 - x\eta_f^{(A)}\eta_d^{(A)}. \tag{7.34}$$

However, we emphasize that Bob's best strategy will in fact depend on the rewards and sanctions associated with honest aborts and "getting caught cheating" aborts. In other words, Bob has to minimize his risk-to-reward ratio. Maximizing his winning probability makes him run the risk of getting caught cheating with probability $x\eta_f^{(A)}\eta_d^{(A)}$.

7.5.3 Dishonest Alice: outline

Dishonest Alice must still generate the state which maximizes the $(1,0,0)$ outcome after Bob's honest transformations have been applied. However, the expression for Bob's corresponding projector now changes, as there is a finite probability $(1-\eta_d)^n$ that the n-photon component is projected onto the vacuum. The 0 outcome on one spatial mode is therefore triggered by the projection $\sum_{n=0}^{\infty}(1-\eta_d)^n |n\rangle\langle n|$. The total projector responsible for the $(1,0,0)$ outcome then reads:

$$\Pi_{(1,0,0)} = \left[\mathbb{1} - \sum_m (1-\eta_d)^m |m\rangle\langle m|\right] \otimes \left[\sum_{n,p}(1-\eta_d)^{n+p}|n\rangle\langle n| \otimes |p\rangle\langle p|\right]. \tag{7.35}$$

The security analysis is two-fold: we first show that Alice's maximum winning probability when Bob is using a delay line of transmission $\eta_f < 1$ is always lower than when Bob's delay line is perfect (i.e. $\eta_f = 1$), independently of the efficiency η_d of his detectors. We then show that Alice's maximum winning probability reads:

$$P_d(A) = \max_{l>0}\left[\left(1-(1-y\eta_f^{(B)})(1-z)\eta_d^{(B)}\right)^l - \left(1-\eta_d^{(B)}\right)^l\right] \leqslant y + z - yz. \tag{7.36}$$

The upper bound in Eq.(7.36) is Alice's cheating probability in the lossless case. This shows that Alice cannot take advantage of Bob's imperfect detectors nor lossy delay line in order to increase her cheating probability.

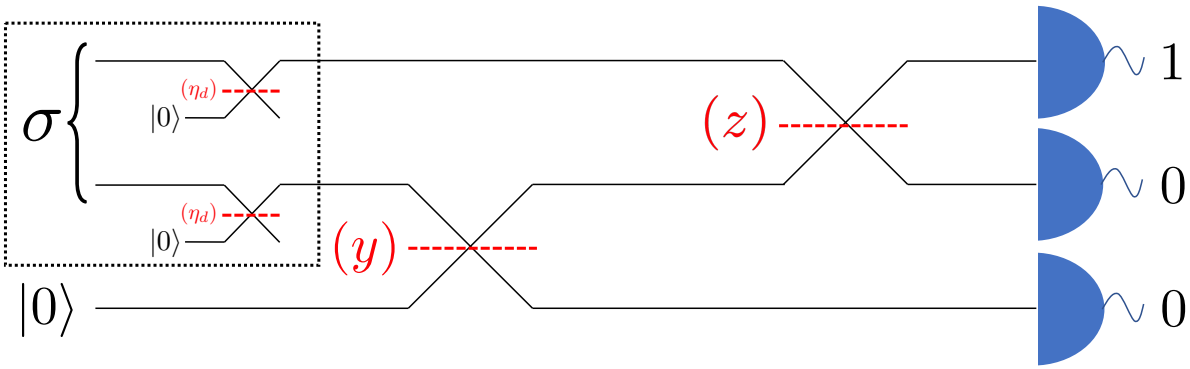


Figure 7.5: **Equivalent picture for Dishonest Alice without a delay line.** Alice aims to maximize the outcome $(1,0,0)$ by sending the state σ. In this picture, the losses of the detectors have been commuted back to Alice's state preparation.

We now give a sketch of the security proof for the following sections: since passive linear optical elements act linearly on creation operators, equal losses on different modes may be commuted through the interferometer of the protocol. This allows to upper bound Alice's maximum winning probability by her winning probability in an equivalent picture in which the losses happen just after her state preparation, then followed by a lossless protocol. In that case, the picture is equivalent to Dishonest Alice cheating in the lossless protocol (Fig. 7.3), while being restricted to lossy state preparation, instead of generic state preparation (Fig. 7.5).

The losses correspond to a probability $(1-\eta)$ of losing a photon. These can be modelled as a mixing with the vacuum on a beam splitter of reflectivity η. We first recall a useful simple property, which will be extensively used in the following analysis. The result was proven in [108], but a quick proof is provided in Appendix C.3 for completeness:

Lemma 7.2. *Equal losses can be commuted through passive linear optical elements.*

7.5.4 Dishonest Alice with lossy delay

We first show that Alice's maximum winning probability when Bob is using a delay line of transmission $\eta_f < 1$ is always lower than when Bob's delay line is perfect, i.e. $\eta_f = 1$, independently of the efficiency η_d of his detectors. The lossy delay line of transmission η_f may be modelled as a mixing with the vacuum on a beam splitter of reflectivity η_f.

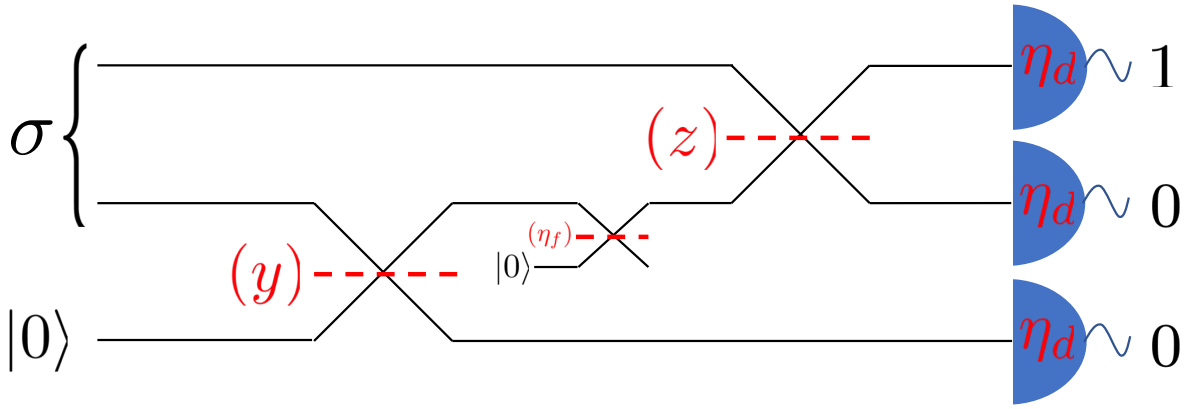


Figure 7.6: **First equivalent picture for Dishonest Alice with Bob's lossy delay line.** Alice aims to maximize the outcome $(1,0,0)$ by sending the state σ. The lossy delay line is represented by a mixing with the vacuum on a beam splitter of reflectivity η_f.

Alice prepares a state σ, which goes through the interferometer depicted in Fig. 7.6, and wins if the measurement outcome obtained by Bob is $(1,0,0)$.

In particular, note that the outcome 0 must be obtained for the third mode. Hence Alice's winning probability is always lower than if the third mode was mixed with the vacuum on a beam splitter of reflectivity η_f just before the detection, since this increases the probability of the outcome 0 for this mode. Let us assume that this is the case. Then, by Lemma 7.2, the losses η_f on output modes 2 and 3 may be commuted back through the beam splitter of reflectivity y, acting on modes 2 and 3. Since the input state on mode 3 is the vacuum, the losses on this mode may then be removed (Fig. 7.7).

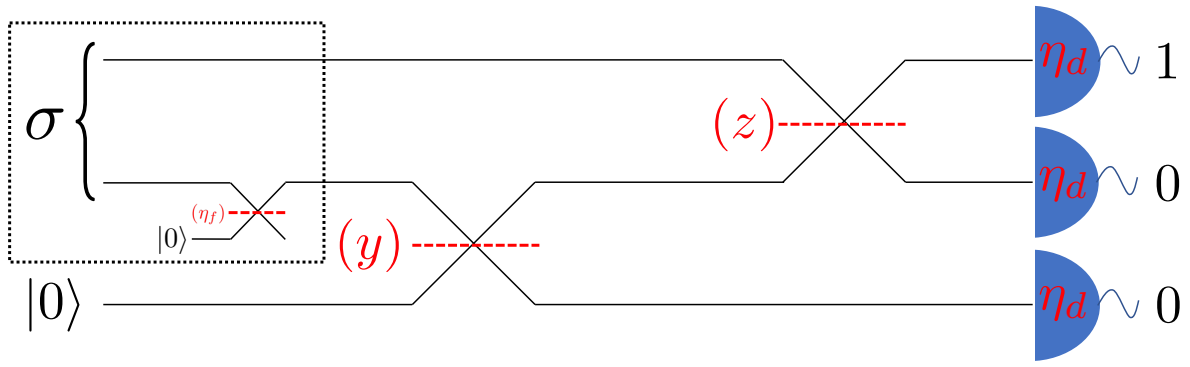


Figure 7.7: **Second equivalent picture for Dishonest Alice with Bob's lossy delay line.** Adding losses on the third mode increases Alice's winning probability. The losses η_f are commuted back to Alice's state preparation. The losses on input mode 3 can be omitted since the input state is the vacuum.

In that case, the probability of winning is clearly lower than when the delay line is perfect (Fig. 7.8), because Alice is now restricted to lossy state preparation instead of generic state preparation. This reduction shows that Alice's maximum winning probability when Bob is using a lossy delay line is always lower than when Bob's delay line is perfect, independently of the efficiency η_d of his detectors. Moreover, Alice's maximum cheating probability and optimal cheating strategy may be inferred from the case where Bob has a perfect delay line, as we show in what follows.

By convexity of the probabilities, Alice's best strategy is to send a pure state $|\psi\rangle = \sum_{k,l\geqslant 0}\psi_{kl}|kl\rangle$. Let us consider the evolution of Alice's state and the vacuum on the third input mode through the interferometer W in Fig. 7.6, including the detection losses. The creation operator for the first mode evolves as:

$$\begin{aligned}\hat{a}_1^\dagger &\to \sqrt{z}\,\hat{a}_1^\dagger + \sqrt{1-z}\,\hat{a}_2^\dagger \\ &\to \sqrt{z\eta_d}\,\hat{a}_1^\dagger + \sqrt{(1-z)\eta_d}\,\hat{a}_2^\dagger \\ &= W\hat{a}_1^\dagger W^\dagger,\end{aligned} \tag{7.37}$$

while the creation operator for the second mode evolves as:

$$\begin{aligned}\hat{a}_2^\dagger &\to \sqrt{y}\,\hat{a}_2^\dagger + \sqrt{1-y}\,\hat{a}_3^\dagger \\ &\to \sqrt{y\eta_f}\,\hat{a}_2^\dagger + \sqrt{1-y}\,\hat{a}_3^\dagger \\ &\to \sqrt{y(1-z)\eta_f}\,\hat{a}_1^\dagger - \sqrt{yz\eta_f}\,\hat{a}_2^\dagger + \sqrt{1-y}\,\hat{a}_3^\dagger \\ &\to \sqrt{y(1-z)\eta_f\eta_d}\,\hat{a}_1^\dagger - \sqrt{yz\eta_f\eta_d}\,\hat{a}_2^\dagger + \sqrt{(1-y)\eta_d}\,\hat{a}_3^\dagger \\ &= W\hat{a}_2^\dagger W^\dagger.\end{aligned} \tag{7.38}$$

Hence, the output state (before the ideal threshold detection) is given by:

$$\begin{aligned}W|\psi 0\rangle &= W\sum_{k,l\geqslant 0}\psi_{kl}|kl0\rangle \\ &= W\left[\sum_{k,l\geqslant 0}\frac{\psi_{kl}}{\sqrt{k!l!}}(\hat{a}_1^\dagger)^k(\hat{a}_2^\dagger)^l\right]|000\rangle \\ &= \left[\sum_{k,l\geqslant 0}\frac{\psi_{kl}}{\sqrt{k!l!}}(W\hat{a}_1^\dagger W^\dagger)^k(W\hat{a}_2^\dagger W^\dagger)^l\right]|000\rangle \\ &= \sum_{k,l\geqslant 0}\frac{\psi_{kl}}{\sqrt{k!l!}}\left(\sqrt{z\eta_d}\,\hat{a}_1^\dagger + \sqrt{(1-z)\eta_d}\,\hat{a}_2^\dagger\right)^k\left(\sqrt{y(1-z)\eta_f\eta_d}\,\hat{a}_1^\dagger - \sqrt{yz\eta_f\eta_d}\,\hat{a}_2^\dagger + \sqrt{(1-y)\eta_d}\,\hat{a}_3^\dagger\right)^l|000\rangle\,.\end{aligned} \tag{7.39}$$

Now Alice's maximum cheating probability reads:

$$P_d(A) = Tr[W|\psi 0\rangle\langle\psi 0|W^\dagger(\mathbb{1} - |0\rangle\langle 0|)|00\rangle\langle 00|]. \tag{7.40}$$

Hence, the state after a successful projection $(\mathbb{1} - |0\rangle\langle 0|)|00\rangle\langle 00|$, which has norm $P_d(A)$, is given by:

$$\left[\sum_{k+l>0} \frac{\psi_{kl}}{\sqrt{k!l!}} (z\eta_d^{k/2}[y(1-z)\eta_f\eta_d]^{l/2}(\hat{a}_1^\dagger)^{k+l}\right]|000\rangle\,. \tag{7.41}$$

When Bob has a perfect delay line ($\eta_f = 1$), this state reads:

$$\left[\sum_{k+l>0} \frac{\psi_{kl}}{\sqrt{k!l!}} (z\eta_d^{k/2}[y(1-z)\eta_d]^{l/2}(\hat{a}_1^\dagger)^{k+l}\right]|000\rangle\,, \tag{7.42}$$

and its norm is the winning probability of Alice in that case. Hence,

$$P_d(A)[\eta_f, \eta_d, y, z] = P_d(A)[1, \eta_d, y\eta_f, z], \tag{7.43}$$

i.e. we can obtain Alice's optimal strategy by solving the case with perfect delay line, and replacing the parameter y by $y\eta_f$. In the following, we thus derive Alice's optimal strategy in that case.

7.5.5 Dishonest Alice with perfect delay

Let σ be the state sent by Alice, and η_d. She needs to maximize the probability of the overall outcome $(1,0,0)$ at the output of the interferometer depicted in Fig. 7.8, hence the overlap with the projector:

$$\Pi^{\eta_d}_{(1,0,0)} = \left[\mathbb{1} - \sum_m (1-\eta_d)^m |m\rangle\langle m|\right] \otimes \left[\sum_{n,p} (1-\eta_d)^{n+p} |n\rangle\langle n| \otimes |p\rangle\langle p|\right]. \tag{7.44}$$

By convexity of the probabilities, we may assume without loss of generality that Alice sends a pure state $\sigma = |\psi\rangle\langle\psi|$. Moreover, the imperfect threshold detectors of quantum efficiency η_d can be modelled by mixing the state to be measured with the vacuum on a beam splitter of reflectivity η_d followed by an ideal threshold detection [109]. In that case, this corresponds to losses η_d on modes 1, 2, and 3, followed by ideal threshold detections. By Lemma 7.2, commuting the losses back through the interferometer leads to the equivalent picture depicted in Fig. 7.9, where the losses on input mode 3 have been omitted, since the input state is the vacuum.

In that case, Alice's probability of winning is clearly lower than when the threshold detectors are perfect (Fig. 7.3), because she is restricted to lossy state preparation instead

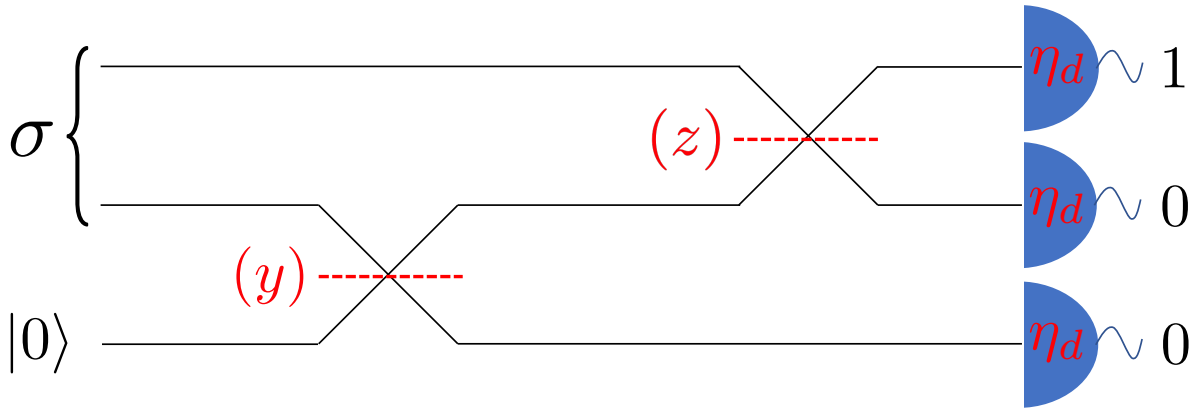


Figure 7.8: **First equivalent picture for Dishonest Alice without a delay line.** Alice aims to maximize the outcome $(1,0,0)$ by sending the state σ. The quantum efficiency of the detectors is indicated in red inside the detectors.

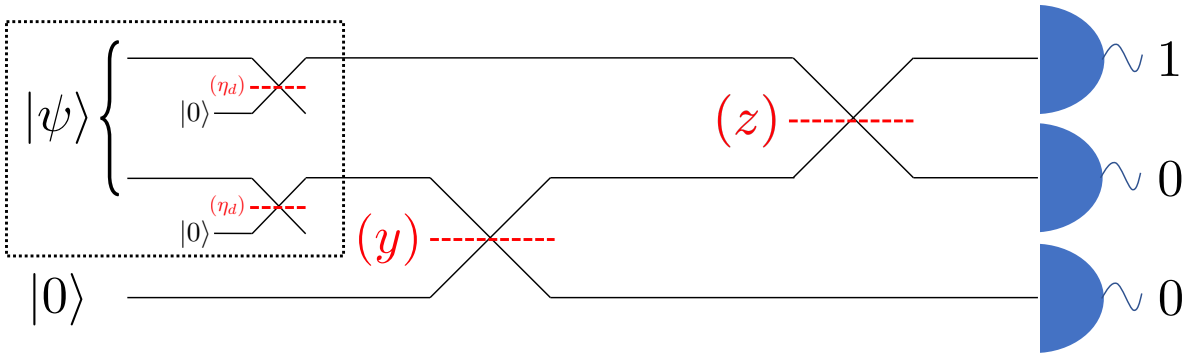


Figure 7.9: **Second equivalent picture for Dishonest Alice without a delay line.** The quantum efficiency are modelled as losses η_d on modes 1, 2, and 3, which are then commuted through the interferometer, back to Alice's state preparation. The losses on input mode 3 can be omitted since the input state is the vacuum.

of generic state preparation. Let $|\tilde{\psi}\rangle$ be the lossy state obtained by applying losses η_d on both modes of Alice's prepared state $|\psi\rangle$. Alice's winning probability may then be written:

$$\begin{aligned} P_d(A) &= Tr[U(|\tilde{\psi}\rangle\langle\tilde{\psi}|\otimes|0\rangle\langle 0|)U^\dagger(\mathbb{1}-|0\rangle\langle 0|)\otimes|00\rangle\langle 00|] \\ &= Tr[U(|\tilde{\psi}\rangle\langle\tilde{\psi}|\otimes|0\rangle\langle 0|)U^\dagger(\mathbb{1}\otimes|00\rangle\langle 00|)] - Tr[U(|\tilde{\psi}\rangle\langle\tilde{\psi}|\otimes|0\rangle\langle 0|)U^\dagger|000\rangle\langle 000|], \end{aligned} \tag{7.45}$$

where $U = (H^{(z)}\otimes\mathbb{1})(\mathbb{1}\otimes H^{(y)})$ is the unitary corresponding to the general interferometer of the lossless protocol. By Lemma 7.1, we have

$$Tr[(\tau\otimes|0\rangle\langle 0|)U^\dagger(\mathbb{1}\otimes|00\rangle\langle 00|)U] = Tr[(\tau\otimes|0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0|\otimes\mathbb{1}\otimes|0\rangle\langle 0|)V], \tag{7.46}$$

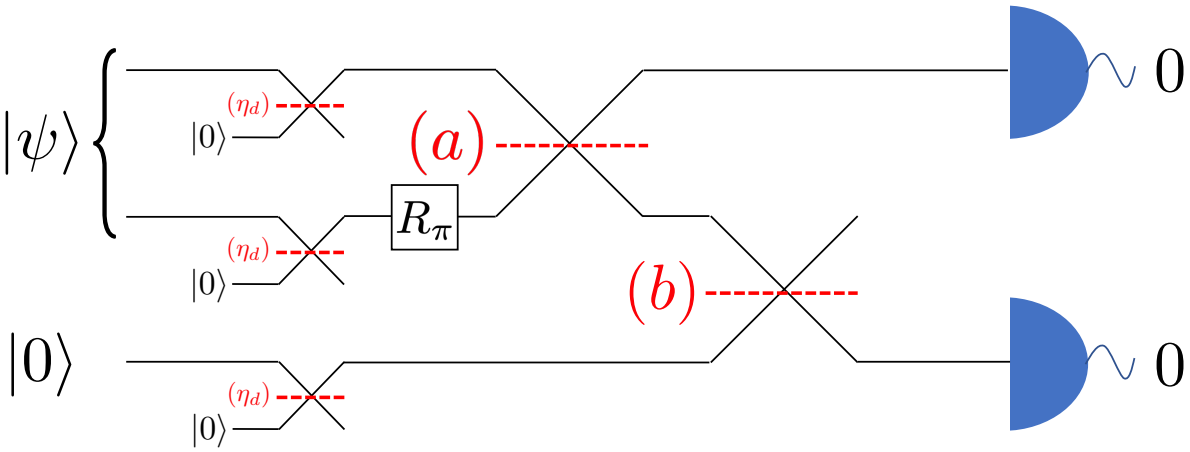


Figure 7.10: **Equivalent picture for term P_1 of Eq. (7.48).** The term P_1 is the probability of the simultaneous outcomes 0 for modes 1 and 3.

for any density matrix τ, where $V = (\mathbb{1}\otimes H^{(b)})(H^{(a)}\otimes\mathbb{1})(\mathbb{1}\otimes R(\pi)\otimes\mathbb{1})$, with $a = \frac{y(1-z)}{y+z-yz}$ and $b = y+z-yz$, and $R(\pi)$ a phase shift of π acting on mode 2. Hence,

$$P_d(A) = Tr[V(|\tilde{\psi}\rangle\langle\tilde{\psi}|\otimes|0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0|\otimes\mathbb{1}\otimes|0\rangle\langle 0|)] - Tr[|\tilde{\psi}\rangle\langle\tilde{\psi}|\,|00\rangle\langle 00|], \tag{7.47}$$

where we used $U^\dagger|000\rangle = |000\rangle$ for the second term. Setting $|\tilde{\psi}_x\rangle = (H^{(a)}\otimes\mathbb{1})(\mathbb{1}\otimes R(\pi))|\tilde{\psi}\rangle$ yields:

$$P_d(A) = \underbrace{Tr[(|\tilde{\psi}_x\rangle\langle\tilde{\psi}_x|\otimes|0\rangle\langle 0|)(\mathbb{1}\otimes H^{(b)})(|0\rangle\langle 0|\otimes\mathbb{1}\otimes|0\rangle\langle 0|)(\mathbb{1}\otimes H^{(b)})]}_{\equiv P_1} - \underbrace{Tr[|\tilde{\psi}_x\rangle\langle\tilde{\psi}_x|\,|00\rangle\langle 00|]}_{\equiv P_2}, \tag{7.48}$$

where we used $|00\rangle = (\mathbb{1}\otimes R(\pi))H^{(a)}|00\rangle$ for the second term P_2.

Let us consider the first term P_1. Since $|\tilde{\psi}\rangle$ is the state obtained by applying losses η_d on both modes of the state $|\psi\rangle$, we obtain the equivalent picture in Fig. 7.10, where we have added losses η_d also on mode 3, since the input state is the vacuum.

Let $|\psi_x\rangle = H^{(a)}(\mathbb{1}\otimes R(\pi))|\psi\rangle$. With Lemma 7.2, commuting the losses η_d to the output of the interferometer in Fig. 7.10, and combining the losses on mode 2 and 3 yields:

$$P_1 = Tr[|\psi_x\rangle\langle\psi_x|\,\Pi_{(0)}^{\eta_d}\otimes\Pi_{(0)}^{\eta_d(1-b)}], \tag{7.49}$$

where $\Pi_{(0)}^{\eta}$ is the POVM element corresponding to no click for a threshold detector of quantum efficiency η (recall that this is the same as an ideal detector preceded by a mixing with the vacuum on a beam splitter of reflectivity η). The same reasoning for the second term P_2 gives:

$$P_2 = Tr[|\psi_x\rangle\langle\psi_x|\,\Pi_{(0)}^{\eta_d}\otimes\Pi_{(0)}^{\eta_d}], \tag{7.50}$$

and we finally obtain with Eq. (7.48),

$$P_d(A) = Tr[|\psi_x\rangle\langle\psi_x| \Pi_{(0)}^{\eta_d} \otimes (\Pi_{(0)}^{\eta_d(1-b)} - \Pi_{(0)}^{\eta_d})]. \tag{7.51}$$

Let us write $|\psi_x\rangle = \sum_{k,l\geq 0}^{+\infty} \psi_{kl} |kl\rangle$. With the expression of the POVM in Eq. (7.44) the last equation rewrites:

$$\begin{aligned} P_d(A) &= \sum_{k,l\geq 0} |\psi_{kl}|^2 (1-\eta_d)^k [(1-\eta_d(1-b))^l - (1-\eta_d)^l] \\ &\leqslant \max_{k,l\geqslant 0} (1-\eta_d)^k [(1-\eta_d(1-b))^l - (1-\eta_d)^l] \sum_{k,l\geqslant 0} |\psi_{kl}|^2 \\ &= \max_{k,l\geqslant 0} (1-\eta_d)^k [(1-\eta_d(1-b))^l - (1-\eta_d)^l] \\ &= \max_{l\geqslant 1} [(1-\eta_d(1-b))^l - (1-\eta_d)^l] \\ &= \max_{l\geqslant 1} [(1-\eta_d(1-y)(1-z))^l - (1-\eta_d)^l], \end{aligned} \tag{7.52}$$

where we used $b = y + z - yz$. Let $l_0 \in \mathbb{N}^*$ such that $\max_{l\geqslant 1}[(1-\eta_d(1-b))^l - (1-\eta_d)^l] = (1-\eta_d(1-b))^{l_0} - (1-\eta_d)^{l_0}$. This last expression is an upperbound for $P_d(A)$, which is attained for $\psi_{kl} = \delta_{k,0}\delta_{l,l_0}$, i.e. $|\psi_x\rangle = |0 l_0\rangle$. Thus, the best strategy for Alice is to send the state:

$$\begin{aligned} |\psi\rangle &= (\mathbb{1} \otimes R(\pi)) H^{(a)} |\psi_x\rangle \\ &= (\mathbb{1} \otimes R(\pi)) H^{(a)} |0 l_0\rangle, \end{aligned} \tag{7.53}$$

where $a = \frac{y(1-z)}{y+z-yz}$, and her winning probability is then:

$$P_d(A) = (1-\eta_d(1-y)(1-z))^{l_0} - (1-\eta_d)^{l_0}, \tag{7.54}$$

when Bob has a perfect delay line. Recalling Eq. (7.43), the best strategy for Alice when Bob has a lossy delay line of transmission η_f is to send the state:

$$\begin{aligned} |\psi\rangle &= (\mathbb{1} \otimes R(\pi)) H^{(a)} |\psi_x\rangle \\ &= (\mathbb{1} \otimes R(\pi)) H^{(a)} |0 l_1\rangle, \end{aligned} \tag{7.55}$$

where $a = \frac{y(1-z)\eta_f}{y\eta_f+z-yz\eta_f}$, where $l_1 \in \mathbb{N}^*$ maximizes $(1-\eta_d(1-y\eta_f)(1-z))^l - (1-\eta_d)^l$, and her

winning probability is then:

$$\begin{aligned}
P_d(A) &= (1-\eta_d(1-y\eta_f)(1-z))^{l_1} - (1-\eta_d)^{l_1} \\
&= \eta_d[1-(1-y\eta_f)(1-z)] \sum_{j=0}^{l_1-1} (1-\eta_d)^j (1-\eta_d(1-y\eta_f)(1-z))^{l_1-j-1} \\
&\leqslant \eta_d[1-(1-y\eta_f)(1-z)] \sum_{j=0}^{l_1-1} (1-\eta_d)^j \\
&= \eta_d\eta_d[1-(1-y\eta_f)(1-z)] \frac{1-(1-\eta_d)^{l_1}}{1-(1-\eta_d)} \\
&= [1-(1-y\eta_f)(1-z)](1-(1-\eta_d)^{l_1}) \\
&\leqslant 1-(1-y\eta_f)(1-z) \\
&\leqslant y+z-yz,
\end{aligned} \tag{7.56}$$

which is the winning probability when there are no losses. Let us finally derive the value of l_1. For this, we define:

$$\begin{aligned}
r &= 1-\eta_d(1-y\eta_f)(1-z) \\
s &= 1-\eta_d.
\end{aligned} \tag{7.57}$$

We then consider a $\lambda_1 \in \mathbb{R}^{*+}$ which maximizes $(r^\lambda - s^\lambda)$ for $\lambda \in \mathbb{R}^{*+}$. We have that:

$$\frac{d}{d\lambda_1}(r^{\lambda_1} - s^{\lambda_1}) = 0 \Leftrightarrow \lambda_1 = \frac{\ln\ln s - \ln\ln r}{\ln r - \ln s}, \tag{7.58}$$

for strictly non-zero r and s and where ln denotes the complex logarithm function. This allows to deduce:

$$l_1 = \begin{cases} \text{floor}(\lambda_1) & \text{if} \quad r^{\text{floor}(\lambda_1)} - s^{\text{floor}(\lambda_1)} \geqslant r^{\text{ceil}(\lambda_1)} - s^{\text{ceil}(\lambda_1)} \\ \text{ceil}(\lambda_1) & \text{if} \quad r^{\text{ceil}(\lambda_1)} - s^{\text{ceil}(\lambda_1)} \geqslant r^{\text{floor}(\lambda_1)} - s^{\text{floor}(\lambda_1)}. \end{cases} \tag{7.59}$$

Note that if $l_1 = 0$ is obtained, we must take $l_1 = 1$ instead, since the condition $l \geqslant 1$ must be satisfied from Eq. (7.52).

7.6 Practical protocol performance

7.6.1 Solving the system

We now analyze the performance of our protocol in a practical setting, by enforcing three conditions on the free parameters: the protocol must be fair, balanced, and it must

provide better security bounds than any classical protocol. These conditions may be translated into the follow system of equations:

$$\begin{cases} (i) & P_h(A) = P_h(B) \quad \text{fairness} \\ (ii) & P_d(A) = P_d(B) \quad \text{balance} \\ (iii) & Q > C \quad \text{quantum advantage} \end{cases} \tag{7.60}$$

Condition (i) enforces a fair protocol and we aim to solve for y as a function of x and z. From Eq. (7.33), we can write:

$$\begin{aligned} (i) &\Leftrightarrow \eta_t \eta_d^{(B)} \left(\sqrt{xz\eta_f^{(A)}} + \sqrt{(1-x)y(1-z)\eta_f^{(B)}} \right)^2 = \eta_t \eta_d^{(B)} (1-x)(1-y) \\ (i) &\Leftrightarrow (1-x)\left[(1-z)\eta_f^{(B)} + 1 \right] y + 2\sqrt{x(1-x)z(1-z)\eta_f^{(A)}\eta_f^{(B)}}\sqrt{y} + xz\eta_f^{(A)} - (1-x) = 0. \end{aligned} \tag{7.61}$$

We make the substitution $Y = \sqrt{y}$ in order to transform Eq. (7.61) into a second-order polynomial equation. We then take only the positive solution (since y must be positive) which reads:

$$Y = \frac{\sqrt{xz(1-z)\eta_f^{(A)}\eta_f^{(B)} - \left[(1-z)\eta_f^{(B)} + 1 \right] \left[xz\eta_f^{(A)} - (1-x) \right]} - \sqrt{xz(1-z)\eta_f^{(A)}\eta_f^{(B)}}}{\sqrt{1-x}\left[(1-z)\eta_f^{(B)} + 1 \right]}. \tag{7.62}$$

We may finally write:

$$(i) \Leftrightarrow \; y = f\left(x, z, \eta_f^{(i)}, \eta_d, \eta_t \right), \tag{7.63}$$

where:

$$f\left(x, z, \eta_f^{(i)}, \eta_d, \eta_t \right) = \frac{\left(\sqrt{(1-x)\left[(1-z)\eta_f^{(B)} + 1 \right] - xz\eta_f^{(A)}} - \sqrt{xz(1-z)\eta_f^{(A)}\eta_f^{(B)}} \right)^2}{(1-x)\left[(1-z)\eta_f^{(B)} + 1 \right]^2}. \tag{7.64}$$

Note that y should be a real number, and hence we require that the expression under the first square root of $f\left(x, z, \eta_f^{(i)}, \eta_d, \eta_t \right)$ is positive, i.e:

$$z \leqslant \frac{(1-x)(1+\eta_f^{(B)})}{x\eta_f^{(A)} + (1-x)\eta_f^{(B)}}. \tag{7.65}$$

Furthermore, note that, for $\eta_f^{(A)} = \eta_f^{(B)} = \eta_f$, y should be an increasing function of η_f, and therefore a decreasing function of d when $\eta_f = 0.95^d$. Mathematically speaking, this is to prevent $y'(d) \to \infty$ and $y(d) > 1$. Physically speaking, this condition ensures that, as the probability of transmitting the photon (and of preserving it for verification) gets smaller, Bob should encourage a detection on the third mode, which evens out the honest probabilities of winning.

Condition (ii) enforces a balanced protocol. Recalling the cheating probabilities from Eqs.(7.34) and (7.36), this translates into the following expression for x:

$$(ii) \Leftrightarrow x = g\left(y, z, \eta_f^{(i)}, \eta_d^{(i)}\right), \tag{7.66}$$

where

$$g\left(y, z, \eta_f^{(i)}, \eta_d^{(i)}\right) = \frac{1}{\eta_f^{(A)} \eta_d^{(A)}} \left[1 - \max_{l \geqslant 1} [(1 - \eta_d^{(B)}(1 - y\eta_f^{(B)})(1 - z))^l - (1 - \eta_d^{(B)})^l]\right]. \tag{7.67}$$

Condition (iii) requires the general coin flipping formalism from Section 3.4.3. In this formalism, our lossy weak coin flipping protocol may be expressed as a:

$$CF\left(P_h(A), P_h(B), P_d(A), \eta_d^{(B)}, 1, P_d(B)\right), \tag{7.68}$$

where $P_d(A) = \max_{l>0}\left(1 - (1 - y\eta_f^{(A)})(1 - z)\eta_d^{(B)}\right)^l - \left(1 - \eta_d^{(B)}\right)^l$ and $P_d(B) = 1 - x\eta_f^{(A)}\eta_d^{(A)}$.

Recalling Eq. (3.18), the condition for which quantum protocols achieve strictly better bounds than classical protocols (Q>C), reads:

$$Q > C \Longleftrightarrow \begin{cases} P_A^{(0)} + P_A^{(1)} > 1 \\ P_B^{(0)} + P_A^{(1)} > 1 \end{cases} \tag{7.69}$$

In our case, this may be written:

$$Q > C \Longleftrightarrow \begin{cases} P_d(A) > 1 - \eta_d^{(B)} \\ 1 + P_d(B) > 1 \end{cases} \tag{7.70}$$

Since we allow $x \in [0, 1[$ and $\eta_f^{(A)}\eta_d^{(A)} > 0$, the second condition is always satisfied. We must therefore ensure that:

$$P_d(A) > 1 - \eta_d^{(B)}. \tag{7.71}$$

Assuming a balanced protocol, i.e. enforcing $P_d(A) = P_d(B)$ as in condition (ii), then implies that:

$$\begin{aligned} &P_d(B) > 1-\eta_d^{(B)} \\ &1-x\eta_f^{(A)}\eta_d^{(A)} > 1-\eta_d^{(B)} \\ &\eta_d^{(B)} > x\eta_f^{(A)}\eta_d^{(A)}. \end{aligned} \tag{7.72}$$

When both parties have the same detection efficiency, this condition becomes trivial since we always have that $1 > x\eta_f^{(A)}$. Hence (iii) is always satisfied in this case.

7.6.2 Results

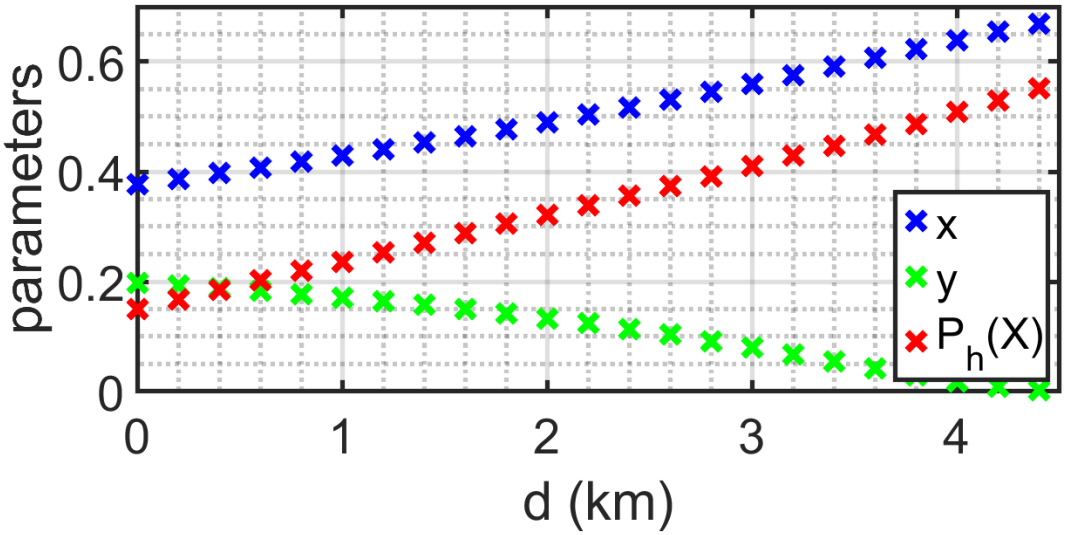


Figure 7.11: **Practical performance for a fair and balanced protocol.** x and y are represented by blue and green crosses, respectively, which satisfy Eq. (7.73) as a function of distance d. The abort probability is indicated with red crosses. Over a few km, classical communication time is assumed to be equal to quantum communication time (i.e. $\approx d/c$), since it is around two orders of magnitude larger than typical computer processing times ($\approx ns$) and commercial optical switching times ($\approx 100ns$). We therefore choose $\eta_f = 0.95^{2d}$ (i.e. the delay transmission associated with travelling distance d for quantum communication and another d for classical communication). Finally, we picked $z = 0.75$ and $\eta_d = 0.85$.

Overall, the conditions from Eq. (7.60) reduce to:

$$\begin{cases} (i) & y = f\left(x,z,\eta_f^{(i)}\right) \\ (ii) & x = g\left(y,z,\eta_f^{(i)},\eta_d^{(i)}\right) \\ (iii) & \eta_d^{(B)} > x\eta_f^{(A)}\eta_d^{(A)}. \end{cases} \tag{7.73}$$

From these conditions, we can numerically obtain a range of parameters for which system (7.73) is satisfied. In particular, when both parties have the same detection efficiency, condition (iii) is always true for $x < 1$. Fig. 7.11 shows a choice of parameters for which our protocol satisfies fairness, balance, and quantum advantage, up to a distance of d.

7.7 Extension to lower bias (preliminary results)

7.7.1 Framework

As a brief introduction, we describe the general n-rounded weak coin flipping framework presented in Fig. 7.12, which involves unitaries and projective measurements. Alice and Bob start with a separable state on Hilbert space $\mathscr{A} \otimes \mathscr{M} \otimes \mathscr{B}$, where $\mathscr{M}$ is the message space, in which the quantum message which they exchange lives.

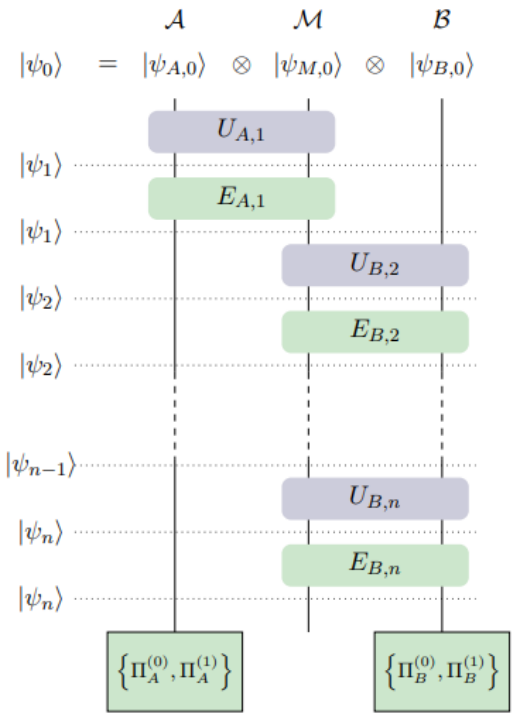


Figure 7.12: **Framework for the honest n-rounded protocol.** Alice and Bob start with a separable state on $\mathscr{A} \otimes \mathscr{M} \otimes \mathscr{B}$. Before sending the ith odd message, Alice applies a unitary $U_{A,i}$ and projection $E_{A,i}$ on $\mathscr{A} \otimes \mathscr{M}$. Before sending the ith even message, Bob applies a unitary $U_{B,i}$ and projection $E_{B,i}$ on $\mathscr{M} \otimes \mathscr{B}$. At the end, each party measures their private register to obtain the final outcome. *This diagram and description were taken from [103].*

Alice first applies an entangling unitary $U_{A,1}$ on $\mathscr{A} \otimes \mathscr{M}$, followed by a projection $E_{A,1}$. She sends the quantum message register to Bob, in order for him to apply a unitary $U_{B,2}$ and projection $E_{B,2}$ on $\mathscr{M} \otimes \mathscr{B}$. The two parties exchange messages likewise for n rounds, and measure their private registers $\mathscr{A}$ and $\mathscr{B}$ after the nth round to conclude on the flip outcome.

We recall that our protocol is the linear-optical equivalent of the protocol from [18]. The latter may in fact be interpreted as a 1-rounded version of the larger family of weak coin flipping protocols studied by Mochon in [106], which follows the structure from Fig. 7.12. By constructing a protocol in which the number of rounds tends to infinity, Mochon showed that the bias converges to 1/6 [106].

In Section 7.7.2, we propose a construction for the n-rounded linear optical version of our protocol, in order to study whether the bias can be lowered in a similar manner. We note that the structure and framework will differ from that in Fig. 7.12, since our n-rounded protocol may stop and designate a winner before the n rounds are over. We also emphasize that this section involves **preliminary results only**, and *investigates* the extension to lower bias. Although the question of convergence to 1/6 for our family of protocols remains open, we show in Section 7.7.6 that the 2-rounded version of our proposed n-rounded protocol indeed achieves a bias $1/6 < \epsilon < (1/\sqrt{2} - 1/2)$ within numerical error. This, however, is reached by probably under-estimating Alice's cheating probability, as underlined in Section 7.7.5.

7.7.2 Protocol with n rounds

In Fig. 7.13, we describe the n-rounded version of our original protocol. We label the spaces in the same way as Fig. 7.12, but note that they are now infinite-dimensional, as we are dealing with Fock spaces. We label by A, M and B the systems living in spaces $\mathscr{A}$, $\mathscr{M}$ and $\mathscr{B}$, respectively. Throughout this section, we assume that n is *even* for simplicity.

1. Prior to the first round, Alice and Bob share a separable state $|100\rangle_{AMB}$.
2. For odd $i \leqslant n$:
    - Alice mixes A and M on a beam splitter of reflectivity x_i.
    - Alice keeps A and sends M to Bob.
    - Bob mixes M with B on a beam splitter of reflectivity y_i.
    - Bob measures M with a photon-number-resolving detector, and broadcasts the outcome $c_i \in \{0, 1\}$.

- If $c_i = 1$, the protocol follows to Step 4. If $c_i = 0$, the protocol follows to round $(i+1)$.

3. For even $i \leqslant n$:

   - Bob mixes M and B on a beam splitter of reflectivity x_i.
   - Bob keeps B and sends M to Alice.
   - Alice mixes A with M on a beam splitter of reflectivity y_i.
   - Alice measures M with a photon-number-resolving detector, and broadcasts the outcome $c_i \in \{0,1\}$.
   - If $c_i = 0$, the protocol follows to Step 4. If $c_i = 1$, Alice generates a new single photon on space M and the protocol follows to round $(i+1)$.

4. When the protocol stops, the party who has *not* declared the outcome performs a verification step (except when $i = n$):

   - Bob declared $c_i = 1$: Alice measures A and declares Bob the winner only if she detects vacuum.
   - Alice declared $c_i = 0$: Bob mixes Alice's private register A with B on a beam splitter of amplitude v_i (which disentangles the state on $\mathscr{A} \otimes \mathscr{B}$) and declares Alice the winner only if he measures $|01\rangle_{AB}$. Alice declared $c_i = 1$ (can only happen when $i = n$): she declares Bob the winner only if she measures vacuum on register B.

7.7.3 Correctness for 2 rounds

In this section, we derive the correctness for a 2-rounded version of the protocol from Fig.7.13. The full quantum state evolution up to the beam splitter with amplitude y_2 is provided in Appendix C.4.

Alice wins when system M is projected onto $|0\rangle$ in the second round, provided that it was also projected onto $|0\rangle$ in the first round. From Appendix C.4, her winning probability therefore reads:

$$P_h(A) = \left[\sqrt{y_2 x_1} + \sqrt{(1-y_2)(1-x_2)(1-y_1)(1-x_1)}\right]^2 + x_2(1-y_1)(1-x_1). \tag{7.74}$$

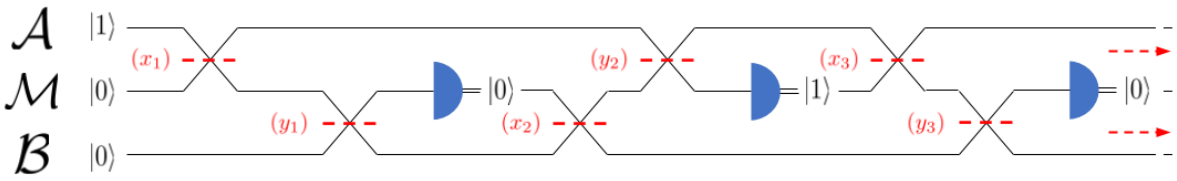


Figure 7.13: **Linear-optical setup for the n-rounded protocol.** Alice and Bob start with a separable state $|100\rangle$ on space $\mathscr{A}\otimes\mathscr{M}\otimes\mathscr{B}$. At every odd round i, Alice mixes A and M on a beam splitter of amplitude x_i and sends M to Bob. Bob mixes M with B on a beam splitter of amplitude y_i, and measures M. If $c_i = 0$, the protocol follows to round $(i+1)$. If $c_i = 1$, Alice declares Bob the winner provided that he passes the verification test. At every even round i, the protocol behaves symmetrically by simply switching Alice and Bob's roles, as well as the winning outcomes. If $c_i = 1$, Alice generates a new single photon and the protocol follows to round $(i+1)$. If $c_i = 0$, Bob declares Alice the winner provided that she passes the verification test.

Bob wins when system M is projected onto $|1\rangle$ in the first round, which, according to Eq. (7.3) from the 1-rounded protocol, occurs with probability $(1-x_1)y_1$. He also wins when M is projected onto $|1\rangle$ in the second round, provided that it was projected onto $|0\rangle$ in the first round. Following Appendix C.4, his winning probability therefore reads:

$$P_h(B) = (1-x_1)y_1 + \left[\sqrt{(1-y_2)x_1} - \sqrt{y_2(1-x_2)(1-y_1)(1-x_1)}\right]^2. \tag{7.75}$$

The protocol is fair when both parties have equal winning probabilities:

$$P_h(A) = P_h(B) = \frac{1}{2}. \tag{7.76}$$

7.7.4 Dishonest Bob

Let us consider a 2-rounded version of the protocol from Section 7.7.2. The setup for Dishonest Bob reduces to that in Fig. 7.14. In the security proof, we dismiss Bob's private register living in $\mathscr{B}$ since he has complete control over it. We however introduce a new 2-dimensional classical register, living in $\mathscr{C}$, which allows to keep track of Bob's declaration of outcome c_1. Note that all other register spaces are infinite-dimensional.

Bob wins when he declares outcome $c_1 = 1$ and passes Alice's verification test after the first round, or when he declares $c_1 = 0$, Alice declares $c_2 = 1$ and he passes Alice's verification test after the second round. When Bob declares $c_1 = 1$, the state which passes Alice's verification test is $|0\rangle\langle 0|_A \otimes \mathbb{1}_M$. When Bob declares $c_1 = 0$, the state must yield the

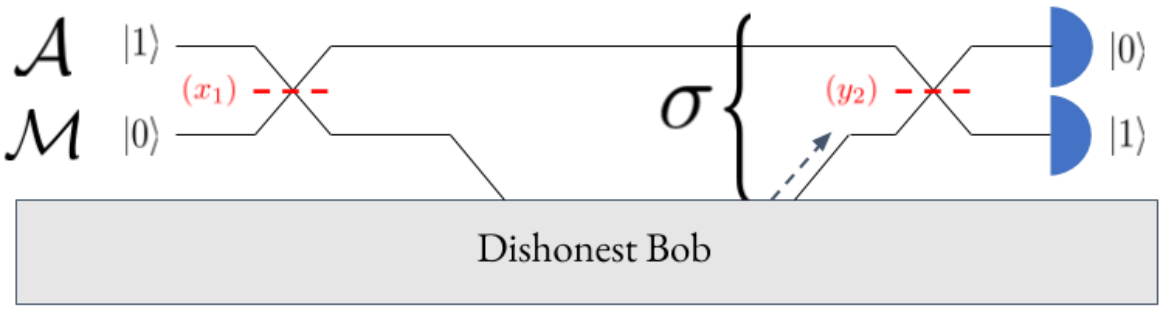


Figure 7.14: **Reduction of the 2-rounded protocol for Dishonest Bob.** Alice mixes a single photon with vacuum on a beam splitter of amplitude x_1, and sends register M to Bob. Dishonest Bob wins when he declares $c_1 = 1$ and passes Alice's verification test in the first round, or when he declares $c_1 = 0$, Alice declares $c_2 = 1$, and he passes Alice's verification test in the second round. After declaring the first outcome, he may send any infinite-dimensional state on $\mathcal{M}$, as a subsystem of state σ.

outcome $(0,1)$ after Alice applies the y_2 beam splitter (in order for her to declare $c_2 = 1$ *and* Bob to pass her verification test). The state before the beamsplitter must therefore be: $H^{(y_2)}|01\rangle\langle 01|_{AM} H^{(y_2)}$. The projector associated with winning Bob may therefore be expressed as:

$$\Pi_{AMC} = |0\rangle\langle 0|_A \otimes \mathbb{1}_M \otimes |1\rangle\langle 1|_C + \left(H^{(y_2)}_{AM}|01\rangle\langle 01|H^{(y_2)}_{AM}\right) \otimes |0\rangle\langle 0|_C \,. \tag{7.77}$$

Bob's optimal strategy involves optimizing over all states on $\mathcal{M}\otimes\mathscr{C}$, such that the overlap of the total state σ_{AMC} with Π_{AMC} is maximized. This may be recast as the following primal optimization problem:

$$\begin{aligned} \max \quad & \mathrm{Tr}(\sigma_{AMC}\Pi_{AMC}) \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathcal{M}\otimes\mathscr{C}}(\sigma_{AMC}) = x_1|1\rangle\langle 1| + (1-x_1)|0\rangle\langle 0| = \sigma_0 \\ & \sigma_{AMC} \geqslant 0. \end{aligned} \tag{7.78}$$

The constraint enforces that the state on Alice's private register is the state dictated by the honest protocol. Following the method from Section 2.2.3, we may express the associated dual problem, optimizing over dual variable Z, as:

$$\begin{aligned} \min \quad & \mathrm{Tr}(\sigma_0 Z) \\ \text{s.t.} \quad & Z \otimes \mathbb{1}_{MC} \geqslant \Pi_{AMC} \\ & Z = Z^\dagger. \end{aligned} \tag{7.79}$$

We shall now derive an analytical upper bound on Bob's cheating probability by finding a feasible solution to problem (7.79). Rewriting the constraint with $\mathbb{1}_C = |0\rangle\langle 0|_C + |1\rangle\langle 1|_C$ and applying the projectors $\mathbb{1}_{AM} \otimes |0\rangle\langle 0|_C$ and $\mathbb{1}_{AM} \otimes |1\rangle\langle 1|_C$ separately on both sides of the inequality provides us with two inequalities:

$$\begin{cases} (i) & Z \otimes \mathbb{1}_M \otimes |0\rangle\langle 0|_C \geqslant \left(H_{AM}^{(y_2)} |01\rangle\langle 01| H_{AM}^{(y_2)}\right) \otimes |0\rangle\langle 0|_C , \\ (ii) & Z \otimes \mathbb{1}_M \otimes |1\rangle\langle 1|_C \geqslant |0\rangle\langle 0|_A \otimes \mathbb{1}_M \otimes |1\rangle\langle 1|_C . \end{cases} \tag{7.80}$$

These conditions are true if and only if:

$$\begin{cases} (i) & Z \otimes \mathbb{1}_M \geqslant \left(H_{AM}^{(y_2)} |01\rangle\langle 01| H_{AM}^{(y_2)}\right), \\ (ii) & Z \otimes \mathbb{1}_M \geqslant |0\rangle\langle 0|_A \otimes \mathbb{1}_M . \end{cases} \tag{7.81}$$

Sylvester's criterion states that a symmetric matrix is positive semidefinite if and only if all its principal minors are non-negative. Assuming that Z is diagonal, condition (ii) is then satisfied for $Z^{00} = \langle 0|Z|0\rangle \geqslant 1$ and $Z^{kk} = \langle k|Z|k\rangle \geqslant 0$, with $k \geqslant 1$. Condition (i) is satisfied for $Z^{00} \geqslant y_2$, $Z^{11} \geqslant (1-y_2)$, $\left(Z^{00} - y_2\right)\left(Z^{00} - (1-y_2)\right) \geqslant y_2(1-y_2)$ and $Z^{kk} \geqslant 0$, with $k \geqslant 2$. Satisfying both conditions then implies the following conditions on diagonal matrix Z:

$$\begin{cases} (a) & Z^{00} \geqslant 1 \\ (b) & Z^{11} \geqslant (1-y_2) \\ (c) & \left(Z^{00} - y_2\right)\left(Z^{11} - (1-y_2)\right) \geqslant y_2(1-y_2) \\ (d) & Z^{kk} \geqslant 0 \quad \text{for} \quad k \geqslant 2 \end{cases} \tag{7.82}$$

We now aim to minimize the dual objective function from (7.79):

$$D = \mathrm{Tr}(\sigma_0 Z) = (1-x_1)Z^{00} + x_1 Z^{11}, \tag{7.83}$$

given the constraints from system (7.82). Since the $k \geqslant 2$ diagonal elements of Z do not contribute to the expression of D, we dismiss condition (d). We now rewrite condition (c) as:

$$\begin{aligned} (c) \quad \Leftrightarrow \quad & Z^{11} - (1-y_2) \geqslant \frac{y_2(1-y_2)}{Z^{00} - y_2} \\ & Z^{11} \geqslant 1 - y_2 + \frac{y_2(1-y_2)}{Z^{00} - y_2} \\ & Z^{11} \geqslant \frac{(1-y_2)Z^{00}}{Z^{00} - y_2}, \end{aligned} \tag{7.84}$$

and note that the second line of (7.84) implies condition (b), which we therefore also dismiss. We must now minimize D with the following constraints:

$$\begin{cases} (a) & Z^{00} \geqslant 1 \\ (c) & Z^{11} \geqslant \frac{(1-y_2)Z^{00}}{Z^{00}-y_2}. \end{cases} \tag{7.85}$$

Using (c), we have:

$$D \geqslant (1-x_1)Z^{00} + x_1 \frac{(1-y_2)Z^{00}}{Z^{00}-y_2}, \tag{7.86}$$

and rewrite the function on the right-hand side as:

$$f\left(Z^{00}\right) = x_1(1-y_2) + (1-x_1)Z^{00} + \frac{x_1 y_2 (1-y_2)}{Z^{00}-y_2}. \tag{7.87}$$

The minimum of f is reached when $f'\left(Z^{00}\right) = 0$, i.e. when:

$$f'\left(Z^{00}\right) = 1 - x_1 - \frac{x_1 y_2 (1-y_2)}{\left(Z^{00}-y_2\right)^2} = 0, \tag{7.88}$$

which implies:

$$Z^{00} = y_2 + \sqrt{\frac{x_1 y_2 (1-y_2)}{(1-x_1)}}. \tag{7.89}$$

Substituting this expression back into Eq. (7.87) finally gives:

$$\begin{aligned} f\left(Z^{00}\right) &= x_1(1-y_2) + (1-x_1)y_2 + \sqrt{x_1 y_2 (1-x_1)(1-y_2)} + \sqrt{x_1 y_2 (1-x_1)(1-y_2)} \\ &= x_1(1-y_2) + (1-x_1)y_2 + 2\sqrt{x_1 y_2 (1-x_1)(1-y_2)} \\ &= \left(\sqrt{x_1(1-y_2)} + \sqrt{y_2(1-x_1)}\right)^2, \end{aligned} \tag{7.90}$$

from which we conclude:

$$D \geqslant \left(\sqrt{x_1(1-y_2)} + \sqrt{y_2(1-x_1)}\right)^2. \tag{7.91}$$

This bound is attained for:

$$Z^{00} = y_2 + \sqrt{\frac{x_1 y_2 (1-y_2)}{(1-x_1)}}, \quad Z^{11} = \frac{(1-y_2)Z^{00}}{Z^{00}-y_2}. \tag{7.92}$$

We recall that condition (a) must also be satisfied, which gives:

$$\begin{aligned}(a) \;\Leftrightarrow\; Z^{00} \geqslant 1 \;\Leftrightarrow\; & \sqrt{x_1 y_2 (1-y_2)} \geqslant (1-y_2)\sqrt{1-x_1} \\ & x_1 y_2 \geqslant (1-y_2)(1-x_1) \\ & y_2 \geqslant 1 - x_1.\end{aligned} \tag{7.93}$$

We may therefore finally upper-bound Bob's cheating probability by:

$$P_d(B) \leqslant \left(\sqrt{x_1(1-y_2)} + \sqrt{y_2(1-x_1)}\right)^2, \tag{7.94}$$

with $y_2 \geqslant 1 - x_1$.

7.7.5 Dishonest Alice

Let us consider a 2-rounded version of the protocol from Section 7.7.2. The setup for Dishonest Alice reduces to that in Fig. 7.15. In the security proof, we dismiss Alice's private register living in $\mathscr{A}$ since she has complete control over it. Note that all spaces are infinite-dimensional.

Alice wins when outcomes $c_1 = c_2 = 0$ are declared (first by Bob, and then by herself). She must also pass Bob's verification test, which consists of a beam splitter of amplitude v, followed by a projection onto state $|01\rangle_{AB}$. The coefficient v must unentangle the incoming registers A and B, and is given by:

$$v = 2(1-x_1)x_2(1-y_1). \tag{7.95}$$

Following the reduction from Fig. 7.15, we can set up the primal problem which maximizes Alice's cheating probability. She may send any two states on register M, which, together with system B, form the optimization variables ρ_1 and ρ_2. The objective function will maximize the overlap of ρ_2 after undergoing the $H^{(v)}$ transformation with the acceptance projector $|01\rangle\langle 01|$. We may then write the following primal problem:

$$\begin{aligned}\max \quad & \mathrm{Tr}\left(H^{(v)}_{MB} \rho_2 H^{(v)}_{MB} |01\rangle\langle 01|_{MB}\right) \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathscr{M}}\left(\rho_1\right) = |0\rangle\langle 0| = \rho_0 \\ & \mathrm{Tr}_{\mathscr{M}}\left(\rho_2\right) = \mathrm{Tr}_{\mathscr{M}}\,\Omega(\rho_1) \\ & \rho_1, \rho_2 \geqslant 0.\end{aligned} \tag{7.96}$$

where the constraints follow from Bob's honest action on systems M and B:

$$\Omega(\rho_1) = \left[H^{(x_2)}(|0\rangle\langle 0| \otimes \mathbb{1}) H^{(y_1)}\right] \rho_1 \left[H^{(y_1)}(|0\rangle\langle 0| \otimes \mathbb{1}) H^{(x_2)}\right]. \tag{7.97}$$

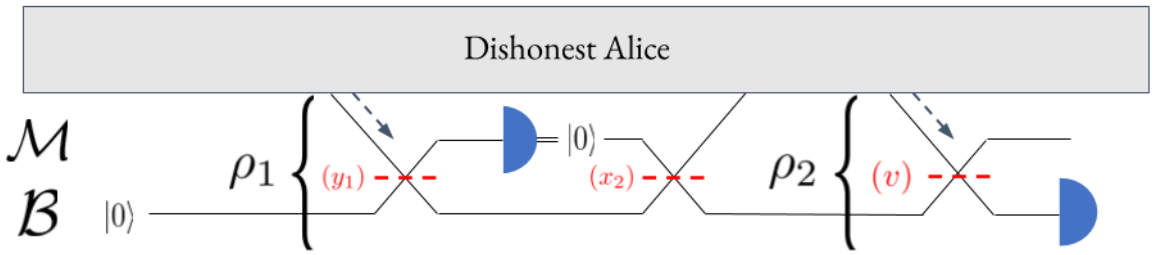


Figure 7.15: **Reduction of the 2-rounded protocol for Dishonest Alice.** Bob starts with the vacuum state on his private register, and Alice can send any state on $\mathscr{M}$ (as a subsystem of ρ_1) which will force Bob to declare outcome $c_1 = 0$. She then declares $c_1 = 0$, and can send any state on $\mathscr{M}$ (as a subsystem of ρ_2) to Bob for verification.

Following Section 2.2.3 and Theorem 2 from [105] allows to derive the following dual problem:

$$\begin{aligned} \min \quad & \mathrm{Tr}(Z_1 |0\rangle\langle 0|) \\ \text{s.t.} \quad & \mathbb{1}_M \otimes Z_1 \geqslant \Omega^*(\mathbb{1}_M \otimes Z_2) \\ & \mathbb{1}_M \otimes Z_2 \geqslant Z_3 \\ & Z_3 = H_{MB}^{(v)} |01\rangle\langle 01| H_{MB}^{(v)} \\ & Z_1 = Z_1^\dagger, \quad Z_2 = Z_2^\dagger. \end{aligned} \tag{7.98}$$

We shall now derive an analytical upper bound on Alice's cheating probability by finding a feasible solution to problem (7.98). We recall Sylvester's criterion, which states that a symmetric matrix is positive semidefinite if and only if all its principal minors are non-negative. This allows to infer the following conditions from the second and third constraints of (7.98):

$$\begin{cases} Z_2^{00}\left(Z_2^{11} - v\right) - Z_2^{01} Z_2^{10} & \geqslant 0 \\ \left(Z_2^{00} - (1-v)\right) Z_2^{11} - Z_2^{01} Z_2^{10} & \geqslant 0 \\ \left(Z_2^{11} - v\right)\left(Z_2^{00} - (1-v)\right) - v(1-v) & \geqslant 0 \\ Z^{kk} \geqslant 0 \qquad \text{for} \quad k \geqslant 2. \end{cases} \tag{7.99}$$

Note that if these conditions are enforced, then Sylvester's criterion is trivially satisfied for all other principal minors of $\mathbb{1}_M \otimes Z_2 - Z_3$. Given these conditions, we now study the first constraint of problem (7.98). We start by applying the $H^{(y_1)}$ transformation to both sides of the inequality:

$$
\begin{aligned}
&H^{(y_1)}(\mathbb{1}_M \otimes Z_1)H^{(y_1)} \geqslant H^{(y_1)}H^{(y_1)}(|0\rangle\langle 0| \otimes \mathbb{1})H^{(x_2)}(\mathbb{1}_M \otimes Z_2)H^{(x_2)}(|0\rangle\langle 0| \otimes \mathbb{1})H^{(y_1)}H^{(y_1)} \\
&H^{(y_1)}(\mathbb{1}_M \otimes Z_1)H^{(y_1)} \geqslant \mathbb{1}_{MB}(|0\rangle\langle 0| \otimes \mathbb{1})H^{(x_2)}(\mathbb{1}_M \otimes Z_2)H^{(x_2)}(|0\rangle\langle 0| \otimes \mathbb{1})\mathbb{1}_{MB} \\
&H^{(y_1)}(\mathbb{1}_M \otimes Z_1)H^{(y_1)} \geqslant (|0\rangle\langle 0| \otimes \mathbb{1})H^{(x_2)}(\mathbb{1}_M \otimes Z_2)H^{(x_2)}(|0\rangle\langle 0| \otimes \mathbb{1}).
\end{aligned}
\tag{7.100}
$$

We now introduce the following lemma, proven in Appendix C.5:

Lemma 7.3. *Let $H^{(t)}$ represent a beam splitter transformation of amplitude t on $\mathscr{M} \otimes \mathscr{B}$, Z_B a Hermitian matrix living on $\mathscr{B}$, and:*

$$
E^{(t)}(Z_B) = (|0\rangle\langle 0| \otimes \mathbb{1})H^{(t)}(\mathbb{1}_M \otimes Z_B)H^{(t)}(|0\rangle\langle 0| \otimes \mathbb{1}). \tag{7.101}
$$

If matrix Z_B is diagonal, we have:

$$
E^{(t)}(Z_B) = |0\rangle\langle 0| \otimes \sum_{m=0}^{\infty}\sum_{l=0}^{m}\binom{m}{l} Z_B^{ll}(1-t)^{m-l}t^l\,|m\rangle\langle m|. \tag{7.102}
$$

The rigorous treatment of this calculation is now left for further work. However, as an investigation which might slightly under-estimate Alice's cheating probability, we now apply the projector $(|0\rangle\langle 0| \otimes \mathbb{1})$ to both sides of Eq. (7.100). This will only yield a necessary condition regarding positivity, since in order for the equivalence to hold, we should in fact apply projectors onto each two-mode p-photon subspace, given by:

$$
\Pi^{(p)} = \sum_{j=0}^{p} |p,(p-j)\rangle\langle p,(p-j)|. \tag{7.103}
$$

Applying such projectors onto the block-diagonal subspaces (instead of $(|0\rangle\langle 0| \otimes \mathbb{1})$) will give a set of conditions (one for each two-mode p-photon subspace), which are equivalent to Eq. (7.100). This will then enable us to calculate Alice's cheating probability rigorously.

For now, we nevertheless apply $(|0\rangle\langle 0| \otimes \mathbb{1})$, which, using Lemma 7.3, implies $E^{(y_1)}(Z_1) \geqslant E^{(x_2)}(Z_2)$:

$$
\sum_{m=0}^{\infty}\sum_{l=0}^{m}\binom{m}{l} Z_1^{ll}(1-y_1)^{m-l}y_1^l\,|m\rangle\langle m| \geqslant \sum_{m=0}^{\infty}\sum_{l=0}^{m}\binom{m}{l} Z_2^{ll}(1-x_2)^{m-l}x_2^l\,|m\rangle\langle m|. \tag{7.104}
$$

Since the operators on each side of Eq.(7.104) are diagonal, we can simply compare their elements one by one. This allows to derive the following set of conditions:

$$\begin{cases} Z_1^{00} \geqslant Z_2^{00} & m=0 \\ (1-y_1)Z_1^{00} + y_1 Z_1^{11} \geqslant (1-x_2)Z_2^{00} + x_2 Z_2^{11} & m=1 \\ \sum_{l=0}^{m} \binom{m}{l} Z_1^{ll} (1-y_1)^{m-l} y_1^l \geqslant \sum_{l=0}^{m} \binom{m}{l} Z_2^{ll} (1-x_2)^{m-l} x_2^l & m \geqslant 2 \end{cases} \tag{7.105}$$

Looking back at the conditions from Eq. (7.99), and assuming that Z_2 is diagonal, we may set:

$$\begin{cases} Z_2^{00} = 1 - v + \frac{1}{n_0} \\ Z_2^{11} = v + n_0 v(1-v), \end{cases} \tag{7.106}$$

where $n_0 \in \mathbb{N}^*$. We may then saturate the bounds for all m conditions of Eq.(7.105) to obtain the following recursive relation between Z_1^{mm}, the free parameter Z_2^{mm}, and the previous set of Z_2^{ll} with $l < m$:

$$Z_1^{mm} y_1^m = Z_2^{mm} x_2^m + \sum_{l=0}^{(m-1)} \binom{m}{l} \left[Z_2^{ll} (1-x_2)^{m-l} x_2^l - Z_1^{ll} (1-y_1)^{m-l} y_1^l \right]. \tag{7.107}$$

This we may re-write as:

$$Z_1^{mm} = \left(\frac{x_2}{y_1} \right)^m Z_2^{mm} + F\left(\{Z_2^{ll}\}_{l<m} \right), \tag{7.108}$$

where $F\left(\{Z_2^{ll}\}_{l<m}\right)$ is a linear function of all previously fixed Z_2^{ll}. For a given m, we note that we can always tune Z_2^{mm} such that the condition is enforced, provided that $Z_2^{mm} \geqslant 0$ from Eq.(7.105).

We may then finally choose $n_0 \to \infty$ and, in this limit, upper-bound Alice's cheating probability by:

$$P_d(A) \leqslant 1 - v, \tag{7.109}$$

where we recall $v = 2(1-x_1)x_2(1-y_1)$. We emphasize once again that this bound may be under-estimated, as we have derived it from a necessary condition only. Nevertheless, we choose to consider it for the following section as the start of an investigation to whether the bias can indeed be lowered to 1/6.

7.7.6 Numerical results

We now aim to solve a system of equations which enforces the fairness and balance of the 2-rounded version of the protocol from Section 7.7.2:

$$\begin{cases} (i) & P_h(A) = P_h(B) \quad \text{fairness} \\ (ii) & P_d(A) = P_d(B) \quad \text{balance} \end{cases} \tag{7.110}$$

Combining the results from Sections 7.7.3, 7.7.4 and 7.7.5 leads to the following system:

$$\begin{cases} (i) & \left[\sqrt{y_2 x_1} + \sqrt{(1-y_2)(1-x_2)(1-y_1)(1-x_1)}\right]^2 + x_2(1-y_1)(1-x_1) \\ & \quad = (1-x_1)y_1 + \left[\sqrt{(1-y_2)x_1} - \sqrt{y_2(1-x_2)(1-y_1)(1-x_1)}\right]^2 \\ (ii) & 1 - 2(1-x_1)x_2(1-y_1) = \left[\sqrt{x_1(1-y_2)} + \sqrt{y_2(1-x_1)}\right]^2. \end{cases} \tag{7.111}$$

We solve this system numerically with Matlab software, by scanning all possible values of the tuple $\{x_1, y_1, x_2, y_2\}$ contained in $[0,1]$ with an increment of 10^{-3}. We enforce the equalities for (i) and (ii) such that:

$$\begin{cases} (i) & |P_h(A) - P_h(B)| \leqslant 10^{-6} \\ (ii) & |P_d(A) - P_d(B)| \leqslant 10^{-6}. \end{cases} \tag{7.112}$$

Although a multitude of tuples $\{x_1, y_1, x_2, y_2\}$ satisfy system (7.111) within desired accuracy, we are interested in the tuple which provides the lowest cheating probability $P_d(A) = P_d(B)$, such that $y_2 \geqslant (1-x_1)$. The numerical results for such a tuple are summarized in Table 7.1:

$P_h(A/B)$	$P_d(A/B)$	x_1	y_1	x_2	y_2
0.500	0.669	0.333	0.273	0.090	1.000

Table 7.1: **Numerical solutions for system (7.111).** The numerical error on all parameters is of order 10^{-4}, while we have enforced $|P_h(A) - P_h(B)| \leqslant 10^{-6}$ and $|P_d(A) - P_d(B)| \leqslant 10^{-6}$.

We conclude this chapter by noticing that our 2-rounded protocol extension might allow to lower the numerical bias ϵ to a value very close to 1/6:

$$\frac{1}{6} < \epsilon \approx 0.169 < \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right). \tag{7.113}$$

However, the convergence to 1/6 seems to be very fast, which is certainly due to the under-estimated cheating probability of Dishonest Alice. Our further work will confirm whether this is actually the case.

7.8 Conclusion

By noticing a non-trivial connection between the early protocol from [18] and linear optical transformations, we answer the question of the implementability of quantum weak coin flipping, and show that it is achievable with current technology over a few kilometers. Both parties require a set of beam splitters and single photon threshold detectors. State generation on Alice's side can be performed with any heralded probabilistic single-photon source, for which photon indistinguishability and state purity do not matter. Only Alice requires an optical switch, which is commercially available. Although short-term quantum storage is needed, a spool of optical fiber with twice the length of the quantum channel suffices, and provides the required storage/retrieval efficiency.

On the fundamental level, our results have raised the question of a potentially deep connection between the large family of protocols from [102, 105, 106] (which achieves biases as low as 1/6) and the linear optics formalism. In order to investigate this, we have constructed an extension of the protocol to n rounds, and numerically investigated the bias for $n = 2$.

This opens interesting perspectives. First, the rigorous derivation for cheating Alice in the 2-rounded protocol must be pursued, since it has potentially been under-estimated. Solving the set of conditions for a fair and balanced protocol with more than 2 rounds could then help us investigate whether our protocol resembles the 1/6 family, or whether it is fundamentally different and can actually achieve biases below 1/6. Furthermore, unveiling the potential explicit mapping between these two frameworks could allow a deeper understanding of how to lower the bias below 1/6. Finally, our implementation proposal for the 1-rounded protocol opens the door to a near-future experimental demonstration of weak coin flipping.

CHAPTER 8

CONCLUSION

Quantum cryptography is a promising candidate for improving the security of today's communication networks, as it provides a quantitative advantage for many tasks and primitives. However, in order to succeed in implementing large-scale quantum networks, the gap between theory and experiment must be bridged on several levels. Technical skills must be shared across fields which appear very different at first sight, such as fundamental computer science and experimental physics. Furthermore, a common and simple dissemination language should be established to facilitate communication between fields. This is the aim and direction offered by the quantum protocol zoo [24].

This thesis aimed to follow this direction by providing a smooth transition from abstract theoretical protocols to secure experimental implementations, regarding two pillars of quantum communication: quantum money, which offers a new information-theoretically secure form of unforgeability, and quantum weak coin flipping, which is a crucial building block for many cryptographic tasks. Three experimental platforms and encodings have been considered, each of which opened new security loopholes and required different techniques to solve them. These are summarized in Table 8.1.

Chapters 4, 5 and 6 followed a natural path to introducing secure quantum money schemes into the real world. In Chapter 4, we have set the steps towards a practical security proof for quantum money with a trusted payment terminal. We have then proposed a proof-of-principle implementation without a quantum storage device, and realized it with polarization-encoded coherent states at telecom wavelengths, in order to facilitate future integration within communication networks. These results were the

chapter	encoding	platform	resource
4	polarization	telecom fiber	superposition
6	collective magnetic atomic excitation	free space	superposition
7	photon number	linear-optical circuit	entanglement

Table 8.1: **Summary of the encodings, experimental platforms, and quantum resources used throughout the thesis.**

first attempt to demonstrate quantum money experimentally. In Chapter 5, we have refined the practical security analysis for trusted payment terminals, by developing an optimization framework which takes into account the full spectrum of loss-dependent attacks. As a natural step, we have then extended this security analysis to untrusted payment terminals, in the prospect of more robust and secure implementations. In Chapter 6, we have described new security loopholes which arise when attempting to map photonic states onto collective atomic excitations, in a quantum memory based on electromagnetically induced transparency. We have then proposed an experimental setup to demonstrate the trusted terminal protocol from Chapter 5 with the full quantum credit card storage process. We are currently attempting to demonstrate this protocol experimentally, which should embody the first demonstration of a quantum-cryptographic task with a realistic quantum memory.

Although this is left for future work, we point out that the implementation will first remain proof-of-principle, as the detectors we use have a quantum efficiency which is still too low to implement a strictly secure version of the protocol from Chapter 5. However, the demonstration of information-theoretic security in the presence of an imperfect storage device only is definitely within reach. In the near-future, acquiring superconducting nanowire single photon detectors with higher detection efficiency, as well as optimizing the storage/retrieval efficiency of the quantum memory, will hopefully give us the opportunity to implement an information-theoretically secure quantum money scheme with less assumptions. In the long-term, we hope that further technological breakthroughs could also potentially allow to implement the untrusted terminal scheme, which would be highly beneficial to quantum communication networks.

Finally, Chapter 7 provided the first implementation proposal for quantum weak coin flipping (WCF), along with its rigorous security analysis and performance in the presence of noise and losses. Although crucial to the construction of other quantum-cryptographic primitives, the WCF literature was lacking an encoding proposal which allows to implement this protocol with current technology. We have noticed a connection

between unitaries and linear-optical circuits, and constructed a simple protocol which involves a single photon and three beamsplitters only. We have then started to investigate how the bias could be lowered by extending this protocol to n rounds.

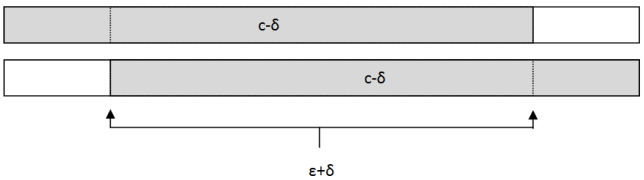
These results also open the door to interesting perspectives, both on the theoretical and experimental sides. Theoretically, now that the connection between unitaries and linear optics has been established, the explicit mapping to infinite-dimensional Fock spaces should be derived in order to investigate the true lower bound on the bias which our n-rounded protocol can achieve. Experimentally, our implementation proposal encourages a full demonstration of this milestone primitive with a heralded single photon source, three beamsplitters and a spool of optical fiber.

APPENDIX A

PROOF-OF-PRINCIPLE CREDIT CARD SCHEME

A.1 Explicit derivation of the δ parameter

For the correctness of game G', we have that the honest client must ensure at least $(c-\delta)$ of the Q_{xx} challenges, or at least $(c-\delta)$ of the Q_{zz} challenges, are answered correctly. The correctness c' in the first half of Eq. (4.6) comes from a simple Chernoff bound, since the client succeeds with probability c in the challenge. In order to prove that the security parameter ϵ' is the one given in the second part of Eq. (4.6), it suffices to show that the cheating client must ensure the challenge Q_ϵ is answered correctly for a fraction of at least $(\epsilon+\delta)$ of the games G in order to cheat in G'. Note that the client must be able to ensure the correct answer for at least a fraction of $(c-\delta)$ of each of the two challenges and hence the fraction of games where both challenges must be answered is at least $2(c-\delta)-1$, as illustrated below:



Equating this to $(\epsilon+\delta)$ provides the value of δ for the "single-photon state" protocol:

$$\begin{aligned} \epsilon+\delta &= 2(c-\delta)-1 \\ \delta &= \frac{2c-\epsilon-1}{3} \end{aligned} \tag{A.1}$$

For the "weak coherent state" protocol, taking into account the Poissonian nature of these states, we have that the extra probability $(1+\eta)P_D$ of successful USD per pulse goes straight to the adversary. Equation (A.1) may then be rewritten as

$$\delta = \frac{2c-\epsilon-(1+\eta)P_D-1}{3}. \tag{A.2}$$

A.2 Phase randomization

The adversary receives a coherent state with average photon number μ, whose global phase ϕ is picked uniformly at random from $[0,2\pi]$. From their point of view, the state's density matrix can be expressed:

$$\rho = \frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}e^{i\phi}\rangle\langle\sqrt{\mu}e^{i\phi}|\,d\phi \tag{A.3}$$

$$\rho = \frac{e^{-\mu}}{2\pi}\int_0^{2\pi}\left(\sum_{n=0}^{\infty}\frac{(\sqrt{\mu}e^{i\phi})^n}{\sqrt{n!}}|n\rangle\right)\left(\sum_{m=0}^{\infty}\frac{(\sqrt{\mu}e^{-i\phi})^m}{\sqrt{m!}}\langle m|\right)d\phi \tag{A.4}$$

$$\rho = \frac{e^{-\mu}}{2\pi}\sum_{n,m=0}^{\infty}\frac{(\sqrt{\mu})^{n+m}}{\sqrt{n!m!}}|n\rangle\langle m|\int_0^{2\pi}e^{i(n-m)\phi}d\phi \tag{A.5}$$

We know that we will be integrating between 0 and 2π, so the integral will be zero for all values of the integer $(n-m)$ apart from when $n=m$, for which the integral reduces to:

$$\rho = \frac{e^{-\mu}}{2\pi}\sum_{n=0}^{\infty}\frac{(\sqrt{\mu})^{2n}}{\sqrt{n!^2}}|n\rangle\langle n|\int_0^{2\pi}d\phi \tag{A.6}$$

$$\rho = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n| \tag{A.7}$$

The adversary sees a Poisson-distributed classical mixture of Fock states.

A.3 Simulation of the evolution of c as a function of μ

The correctness parameter and its evolution with μ can be simulated with a simple theoretical model taking into account experimental parameters. This model was used to

plot the simulation curves in Fig. 4.6. We model the polarization state generated by the polarization controller as a density matrix:

$$\rho = p\,|s\rangle\langle s| + (1-p)\frac{\mathbb{1}}{2}, \tag{A.8}$$

where $|s\rangle$ is the ideal target state, with $s = 0, 1, +, -$, and p is the polarized fraction of the light. This polarization state is associated with a weak coherent state $|\alpha\rangle = e^{-\frac{\mu}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$ with mean photon number $\mu = |\alpha|^2$. For a threshold single-photon detector with detection efficiency η_{det} and dark count probability per detection gate P_{dc}, the click probabilities for ρ can be expressed as:

$$\begin{aligned} P(D_s) &= P_{dc} + \left(1 - e^{-\mu\eta_{\text{det}}}\right)(1+p)/2 \\ P(D_{\bar{s}}) &= P_{dc} + \left(1 - e^{-\mu\eta_{\text{det}}}\right)(1-p)/2, \end{aligned} \tag{A.9}$$

where $s = 0/+$ and $\bar{s} = 1/-$ if $s = 0, +$, and $s = 1/-$ and $\bar{s} = 0/+$ if $s = 1, -$. If instead, we consider true single-photon states, with an emission efficiency μ, the click probabilities for ρ read:

$$\begin{aligned} P(D_s) &= P_{dc} + \mu\eta_{\text{det}}(1+p)/2 \\ P(D_{\bar{s}}) &= P_{dc} + \mu\eta_{\text{det}}(1-p)/2, \end{aligned} \tag{A.10}$$

In both cases, the state correctness, post-selected on events with at least one click, can be expressed as:

$$c_s = \frac{P(D_s)\left(1 - P(D_{\bar{s}})\right)}{1 - \left(1 - P(D_s)\right)\left(1 - P(D_{\bar{s}})\right)}. \tag{A.11}$$

APPENDIX B

TRUSTED AND UNTRUSTED PAYMENT TERMINALS

B.1 Outline of the squashing model

Implementations of quantum key distribution with coherent states sometimes share the same measurement setup as the one used in our quantum money scheme. With polarization-encoding for instance, the measurement basis is selected via a half-waveplate (HWP), followed by a projective measurement realized with a polarizing beamsplitter (PBS). A threshold detector is then placed after each arm of the PBS to register the clicks.

Regardless of the dimensionality of the incoming states, threshold detectors cannot distinguish between exactly 1 photon and more than 1 photon. As was pointed out in Chapter 4, some practical attacks may exploit this by sending coherent states with very high photon number. Assuming that the bank measures the incoming state in its correct preparation basis, this will lead to double clicks (i.e. a simultaneous click on both detectors) when the incoming state is incorrect, and to an accepted single click when the incoming state is correct. If the bank discards double clicks (as it cannot conclude on whether the correct detector clicked), this effectively allows the dishonest client to always succeed: the bank will always accept a state when it is correct, and simply ignore a state that is incorrect.

This means that, in all generality, the security analysis and the bank's measurement operators F_M must be expressed in an infinite dimensional Fock-space, which is inconvenient. In [46] however, it was shown that, by enforcing a specific form of classical

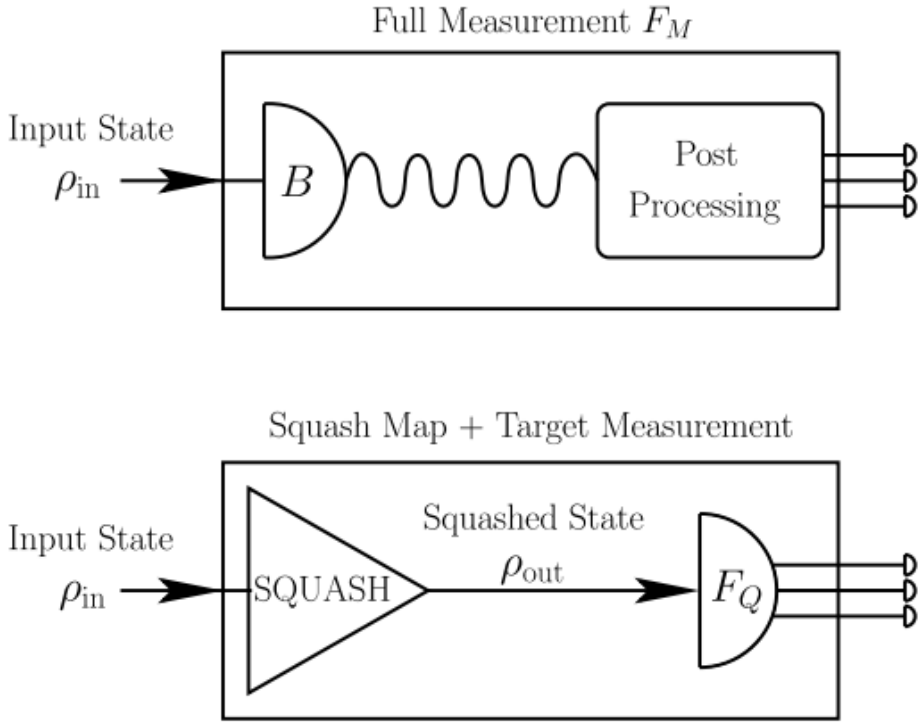


Figure B.1: The full measurement F_M (above) has a general optical input ρ_{in}, which is first measured by the bank's terminal detector B, followed by classical post-processing. In our case, this post-processing involves assigning a random measurement outcome to any double-click. The squashed measurement (below) has the same general optical input ρ_{in}, which is then squashed by a map Λ to a smaller Hilbert space, followed by a fixed physical measurement F_Q. It is required that both of these measurements produce the same output statistics for all ρ_{in}. *This diagram and part of its description were taken from [46].*

processing on the outcomes of the detectors, there exists a CPTP map, called a squashing map, which maps these full measurement operators onto some finite-dimensional measurement operators F_Q, such that the detectors' output statistics are preserved. Such a model is explicited in Fig. B.1.

In QKD and quantum money schemes with this specific setup, the classical post-processing involves assigning a random measurement outcome to any double click. In other words, by making the classical post-processing more noisy (assigning a random outcome to each double click introduces more errors) allows to derive an equivalent, finite-dimensional framework in which to perform our security analysis without loss of generality.

The projective measurements from Eq.(5.8) may then be reduced to a set of projectors living in a squashed space spanned by $\{|0\rangle, |1\rangle, |\varnothing\rangle\}$, where the first two vectors denote the usual qubit space, and the third vector denotes a projection onto vacuum. In this basis, we can therefore express the squashed qubit projector $|\beta_k\rangle\langle\beta_k|$ corresponding to a measurement of state $|\alpha_k\rangle$ in its correct preparation basis, with $|\beta_0\rangle = |+\rangle$, $|\beta_1\rangle = |+i\rangle$, $|\beta_2\rangle = |-\rangle$, $|\beta_3\rangle = |-i\rangle$, and $|\beta_k^{\perp}\rangle$ is its orthogonal qubit state.

B.2 Proof of Lemma 5.1

For a completely positive trace-preserving linear map $\Lambda : \mathscr{H}_1^d \to \mathscr{H}_3^{d'}$ and its associated Choi–Jamiołkowski operator $J(\Lambda)$, and $|\psi_1\rangle \in \mathscr{H}_1^d$, $|\psi_3\rangle \in \mathscr{H}_3^{d'}$, we can write:

$$\begin{aligned}
\mathrm{Tr}\left(|\psi_3\rangle\langle\psi_3| \otimes |\overline{\psi_1}\rangle\langle\overline{\psi_1}| J(\Lambda)\right) &= \langle\psi_3| \otimes \langle\overline{\psi_1}| J(\Lambda) |\psi_3\rangle \otimes |\overline{\psi_1}\rangle \\
&= \langle\psi_3| \otimes \langle\overline{\psi_1}| \left(\sum_{i,j=1}^{d} \Lambda(|i\rangle\langle j|) \otimes |i\rangle\langle j| \right) |\psi_3\rangle \otimes |\overline{\psi_1}\rangle \\
&= \sum_{i,j=1}^{d} \langle\psi_3| \Lambda(|i\rangle\langle j|) |\psi_3\rangle \otimes \langle\overline{\psi_1}|i\rangle\langle j|\overline{\psi_1}\rangle \\
&= \sum_{i,j=1}^{d} \langle\psi_3| \Lambda(|i\rangle\langle j|) |\psi_3\rangle \otimes \langle i|\psi_1\rangle\langle\psi_1|j\rangle \\
&= \sum_{i,j=1}^{d} \langle\psi_3| \Lambda(\psi_{1,ij}|i\rangle\langle j|) |\psi_3\rangle \\
&= \langle\psi_3| \Lambda(|\psi_1\rangle\langle\psi_1|) |\psi_3\rangle \\
&= \mathrm{Tr}\left(|\psi_3\rangle\langle\psi_3| \Lambda(|\psi_1\rangle\langle\psi_1|)\right),
\end{aligned} \tag{B.1}$$

where we have defined the scalar $\psi_{1,ij} := \langle i|\psi_1\rangle\langle\psi_1|j\rangle$.

B.3 Explicit expression for phase-randomized states

We may express the four states in our protocol as:

$$\left| e^{i\phi} \frac{\alpha}{\sqrt{2}} \right\rangle \otimes \left| e^{i(\phi+\theta)} \frac{\alpha}{\sqrt{2}} \right\rangle,$$

with global phase $\phi = 0$ and relative phase $\theta \in \{0, \frac{\pi}{2}, 2\pi, \frac{3\pi}{2}\}$. This implies that an adversary must access θ to unveil the information encoded in the states. Phase randomization scrambles the global phase reference by allowing ϕ to take values from $[0, 2\pi]$ uniformly at random instead of a single value. By considering the state $|e^{i\phi}\alpha\rangle$ and integrating over

all possible values of ϕ, the adversary sees a classical mixture of Fock states given by [75]:

$$\frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}e^{i\phi}\rangle\langle\sqrt{\mu}e^{i\phi}|\,d\phi = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|,$$

where $\mu = |\alpha|^2$ is the average photon number, and $|n\rangle$ are the photon number states. As the coherent superpositions of number states vanish, the security proof may simply proceed according to the result of quantum non demolition (QND) photon number measurements. If there is no photon in the state, then there is no information. If there is 1 photon, then the qubit security proof may be applied. If there are more than 2 photons in the pulse, perfect cheating is possible, since one photon can be sent to a terminal 1 and another to terminal 2. For our protocol, this allows us to express the phase randomized states ρ_k in a 7-dimensional orthonormal basis $\{|v\rangle, |q_0\rangle, |q_1\rangle, |m_0\rangle, |m_1\rangle, |m_2\rangle, |m_3\rangle\}$, where $|v\rangle$ is the vacuum state, $|q_0\rangle$ and $|q_1\rangle$ span a qubit space, and $|m_i\rangle$ constitute the four orthogonal outcomes which materialize the four perfectly distinguishable states in the multiphoton subspace. Our four phase-randomized coherent states may then be written as the following density matrices :

$$\begin{aligned}
\rho_0 &= p_0(\mu)|v\rangle\langle v| + \quad p_1(\mu)|+\rangle\langle +| + p_m(\mu)|m_0\rangle\langle m_0|\\
\rho_1 &= p_0(\mu)|v\rangle\langle v| + p_1(\mu)|+i\rangle\langle +i| + p_m(\mu)|m_1\rangle\langle m_1|\\
\rho_2 &= p_0(\mu)|v\rangle\langle v| + \quad p_1(\mu)|-\rangle\langle -| + p_m(\mu)|m_2\rangle\langle m_2|\\
\rho_3 &= p_0(\mu)|v\rangle\langle v| + p_1(\mu)|-i\rangle\langle -i| + p_m(\mu)|m_3\rangle\langle m_3|,
\end{aligned}$$

where $|+\rangle$,$|+i\rangle$, $|-\rangle$, $|-i\rangle$ are the usual σ_x and σ_y eigenstates in the qubit space spanned by $|q_i\rangle$ and the Poisson distribution coefficients are given by

$$p_0(\mu) = e^{-\mu}, \qquad p_1(\mu) = \mu e^{-\mu}, \qquad p_m(\mu) = 1-(1+\mu)e^{-\mu}.$$

APPENDIX C

QUANTUM WEAK COIN FLIPPING

C.1 Proof of Lemma 7.1

The action of U on the creation operators is given by:

$$\begin{aligned}\tilde{U} &= \begin{pmatrix} \sqrt{z} & \sqrt{1-z} & 0 \\ \sqrt{1-z} & -\sqrt{z} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{y} & \sqrt{1-y} \\ 0 & \sqrt{1-y} & -\sqrt{y} \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{z} & \sqrt{y(1-z)} & \sqrt{(1-y)(1-z)} \\ \sqrt{1-z} & -\sqrt{yz} & -\sqrt{(1-y)z} \\ 0 & \sqrt{1-y} & -\sqrt{y} \end{pmatrix},\end{aligned} \tag{C.1}$$

where we used $(1-2x)(1-y) = y$. Linear interferometers map product coherent states onto product coherent states, and, for all $\alpha \in \mathbb{C}$, we have that $U^\dagger |\alpha 00\rangle = |\beta_1 \beta_2 \beta_3\rangle$, where

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} \alpha\sqrt{z} \\ \alpha\sqrt{y(1-z)} \\ \alpha\sqrt{(1-y)(1-z)} \end{pmatrix}. \tag{C.2}$$

We have $V = (\mathbb{1}\otimes H^{(b)})(H^{(a)}\otimes\mathbb{1})(\mathbb{1}\otimes R(\pi)\otimes\mathbb{1})$, with $a,b\in[0,1]$, and $R(\pi)$ a phase shift of π acting on mode 2. The action of V on the creation operators is given by

$$\begin{aligned}\tilde{V} &= \begin{pmatrix}1 & 0 & 0\\ 0 & \sqrt{b} & \sqrt{1-b}\\ 0 & \sqrt{1-b} & -\sqrt{b}\end{pmatrix}\begin{pmatrix}\sqrt{a} & \sqrt{1-a} & 0\\ \sqrt{1-a} & -\sqrt{a} & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}\sqrt{a} & -\sqrt{1-a} & 0\\ \sqrt{b(1-a)} & \sqrt{ab} & \sqrt{1-b}\\ \sqrt{(1-a)(1-b)} & \sqrt{a(1-b)} & -\sqrt{b}\end{pmatrix}.\end{aligned} \tag{C.3}$$

For all $\alpha\in\mathbb{C}$, $V^\dagger|0\alpha0\rangle = |\gamma_1\gamma_2\gamma_3\rangle$, where

$$\begin{pmatrix}\gamma_1\\ \gamma_2\\ \gamma_3\end{pmatrix} = \begin{pmatrix}\alpha\sqrt{b(1-a)}\\ \alpha\sqrt{ab}\\ \alpha\sqrt{1-b}\end{pmatrix}. \tag{C.4}$$

Since $a=\frac{y(1-z)}{y+z-yz}$ and $b=y+z-yz$, we have $(\beta_1,\beta_2,\beta_3)=(\gamma_1,\gamma_2,\gamma_3)$. Then,

$$\begin{aligned}Tr[(\tau\otimes|0\rangle\langle0|)U^\dagger(\mathbb{1}\otimes|00\rangle\langle00|)U] &= \frac{1}{\pi}\int_{\mathbb{C}} d^2\alpha\, Tr[(\tau\otimes|0\rangle\langle0|)U^\dagger|\alpha00\rangle\langle\alpha00|U]\\ &= \frac{1}{\pi}\int_{\mathbb{C}} d^2\alpha\, Tr[(\tau\otimes|0\rangle\langle0|)V^\dagger|0\alpha0\rangle\langle0\alpha0|V]\\ &= Tr[(\tau\otimes|0\rangle\langle0|)V^\dagger(|0\rangle\langle0|\otimes\mathbb{1}\otimes|0\rangle\langle0|)V],\end{aligned} \tag{C.5}$$

where we used the completeness relation of coherent states $\mathbb{1}=\frac{1}{\pi}\int_{\mathbb{C}} d^2\alpha\,|\alpha\rangle\langle\alpha|$.

C.2 Creation operator evolution in the lossy protocol

The evolution of the creation operator on mode 1 is given, in terms of creation operators on modes 2 and 3, by:

$$
\begin{aligned}
\hat{a}_1^\dagger &\to \sqrt{x}\hat{a}_1^\dagger + \sqrt{1-x}\hat{a}_2^\dagger \\
&\to \sqrt{x\eta_f^{(A)}}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t}\hat{a}_2^\dagger \\
&\to \sqrt{x\eta_f^{(A)}}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t y}\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t}\hat{a}_3^\dagger \\
&\to \sqrt{x\eta_f^{(A)}}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t y}\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t\eta_d^{(B)}}\hat{a}_3^\dagger \\
&\to \sqrt{x\eta_f^{(A)}\eta_t}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t y\eta_f^{(B)}}\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t\eta_d^{(B)}}\hat{a}_3^\dagger \\
&\to \left(\sqrt{x\eta_f^{(A)}\eta_t z} + \sqrt{(1-x)\eta_t y\eta_f^{(B)}(1-z)}\right)\hat{a}_1^\dagger + \left(\sqrt{x\eta_f^{(A)}\eta_t(1-z)} - \sqrt{(1-x)\eta_t y\eta_f^{(B)}z}\right)\hat{a}_2^\dagger \\
&\quad + \sqrt{(1-x)(1-y)\eta_t\eta_d^{(B)}}\hat{a}_3^\dagger \\
&\to \left(\sqrt{x\eta_f^{(A)}\eta_t z\eta_d^{(B)}} + \sqrt{(1-x)\eta_t y\eta_f^{(B)}(1-z)\eta_d^{(B)}}\right)\hat{a}_1^\dagger + \left(\sqrt{x\eta_f^{(A)}\eta_t(1-z)\eta_d^{(B)}} - \sqrt{(1-x)\eta_t y\eta_f^{(B)}z\eta_d^{(B)}}\right)\hat{a}_2^\dagger \\
&\quad + \sqrt{(1-x)(1-y)\eta_t\eta_d^{(B)}}\hat{a}_3^\dagger.
\end{aligned}
\tag{C.6}
$$

C.3 Proof of Lemma 7.2

One way to prove this statement is to use the fact that any interferometer may be decomposed as beam splitters and phase shifters [110]. Then, losses trivially commute with phase shifters, and are easily shown to commute with beam splitters. Indeed, consider a beam splitter of reflectivity r acting on modes 1 and 2. Its action on the creation operators of the modes is given by

$$
\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{r}\hat{a}_1^\dagger + \sqrt{1-r}\hat{a}_2^\dagger, \sqrt{1-r}\hat{a}_1^\dagger - \sqrt{r}\hat{a}_2^\dagger, \tag{C.7}
$$

while equal losses $(1-\eta)$ on both modes act as:

$$
\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{1-\eta}\hat{a}_1^\dagger, \sqrt{1-\eta}\hat{a}_2^\dagger. \tag{C.8}
$$

Hence, the action of the beam splitter followed by losses is given by:

$$
\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{1-\eta}(\sqrt{r}\hat{a}_1^\dagger + \sqrt{1-r}\hat{a}_2^\dagger), \sqrt{1-\eta}(\sqrt{1-r}\hat{a}_1^\dagger - \sqrt{r}\hat{a}_2^\dagger), \tag{C.9}
$$

while losses followed by the beam splitter act as:

$$
\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{r}(\sqrt{1-\eta}\hat{a}_1^\dagger) + \sqrt{1-r}(\sqrt{1-\eta}\hat{a}_2^\dagger), \sqrt{1-r}(\sqrt{1-\eta}\hat{a}_1^\dagger) - \sqrt{r}(\sqrt{1-\eta}\hat{a}_2^\dagger), \tag{C.10}
$$

which is equal to the previous evolution.

C.4 State evolution in the 2-rounded protocol

Here, we derive the quantum state evolution for the 2-rounded version of the protocol from Fig.7.13.

$$
\begin{aligned}
|100\rangle &\underset{(x_1),AM}{\rightarrow} \sqrt{x_1}\,|100\rangle + \sqrt{1-x_1}\,|010\rangle \\
&\underset{(y_1),MB}{\rightarrow} \sqrt{x_1}\,|100\rangle + \sqrt{y_1(1-x_1)}\,|010\rangle + \sqrt{(1-y_1)(1-x_1)}\,|001\rangle \\
&\underset{|0\rangle\langle 0|,M}{\rightarrow} \sqrt{x_1}\,|100\rangle + \sqrt{(1-y_1)(1-x_1)}\,|001\rangle \\
&\underset{(x_2),MB}{\rightarrow} \sqrt{x_1}\,|100\rangle + \sqrt{(1-x_2)(1-y_1)(1-x_1)}\,|010\rangle - \sqrt{x_2(1-y_1)(1-x_1)}\,|001\rangle \\
&\underset{(y_2),AM}{\rightarrow} \left[\sqrt{y_2 x_1} + \sqrt{(1-y_2)(1-x_2)(1-y_1)(1-x_1)}\right]|100\rangle - \sqrt{x_2(1-y_1)(1-x_1)}\,|001\rangle \\
&\qquad + \left[\sqrt{(1-y_2)x_1} - \sqrt{y_2(1-x_2)(1-y_1)(1-x_1)}\right]|010\rangle .
\end{aligned}
\tag{C.11}
$$

From the last line, which describes the unnormalized state right before Alice's measurement in the second round, we may easily calculate the two parties' winning probabilities. Alice wins when system M is projected onto $|0\rangle$ in the second round, provided that it was also projected onto $|0\rangle$ in the first round (third line of Eq. (C.11)). Her winning probability therefore reads:

$$
P_h(A) = \left[\sqrt{y_2 x_1} + \sqrt{(1-y_2)(1-x_2)(1-y_1)(1-x_1)}\right]^2 + x_2(1-y_1)(1-x_1). \tag{C.12}
$$

Bob wins when system M is projected onto $|1\rangle$ in the first round, which, according to Eq. (7.3) from the 1-rounded protocol, occurs with probability $(1-x_1)y_1$. He also whens when M is projected onto $|1\rangle$ in the second round, provided that it was projected onto $|0\rangle$ in the first round (third line of Eq. (C.11)). His winning probability therefore reads:

$$
P_h(B) = (1-x_1)y_1 + \left[\sqrt{(1-y_2)x_1} - \sqrt{y_2(1-x_2)(1-y_1)(1-x_1)}\right]^2. \tag{C.13}
$$

C.5 Proof of Lemma 7.3

Let:

$$
E^{(t)}(Z_B) = (|0\rangle\langle 0| \otimes \mathbb{1}) H^{(t)} (\mathbb{1}_M \otimes Z_B) H^{(t)} (|0\rangle\langle 0| \otimes \mathbb{1}), \tag{C.14}
$$

assuming a diagonal matrix Z_B and a beam splitter of amplitude t. We start by expanding $(\mathbb{1}_M \otimes Z_B)$ in terms of Fock states, followed by creation operators:

$$\begin{aligned}\mathbb{1}_M \otimes Z_B &= \sum_{k,l=0}^{\infty} Z_B^{ll} \left|kl\right\rangle \left\langle kl\right|, \\ &= \sum_{k,l=0}^{\infty} \frac{Z_B^{ll}}{k!l!} \left(\hat{a}_M^\dagger\right)^k \left(\hat{a}_B^\dagger\right)^l \left|00\right\rangle \left\langle 00\right| \hat{a}_M^k \hat{a}_B^l.\end{aligned} \tag{C.15}$$

Recalling Section 2.3.2, we now apply the $H^{(t)}$ transformation to the creation and annihilation operators:

$$\begin{aligned}H^{(t)}(\mathbb{1}_M \otimes Z_B)H^{(t)} = \sum_{k,l=0}^{\infty} \frac{Z_B^{ll}}{k!l!} &\left(\sqrt{t}\hat{a}_M^\dagger + \sqrt{1-t}\hat{a}_B^\dagger\right)^k \left(\sqrt{1-t}\hat{a}_M^\dagger - \sqrt{t}\hat{a}_B^\dagger\right)^l \left|00\right\rangle \\ &\times \left\langle 00\right| \left(\sqrt{t}\hat{a}_M + \sqrt{1-t}\hat{a}_B\right)^k \left(\sqrt{1-t}\hat{a}_M - \sqrt{t}\hat{a}_B\right)^l.\end{aligned} \tag{C.16}$$

Applying the $(\left|0\right\rangle \left\langle 0\right| \otimes \mathbb{1})$ projector on Eq.(C.16) then allows to dismiss all terms which raise the photon number on space $\mathscr{M}$:

$$\begin{aligned}E^{(t)}(Z_B) &= \sum_{k,l=0}^{\infty} \frac{Z_B^{ll}}{k!l!} \left(\sqrt{1-t}\hat{a}_B^\dagger\right)^k \left(-\sqrt{t}\hat{a}_B^\dagger\right)^l \left|00\right\rangle \left\langle 00\right| \left(\sqrt{1-t}\hat{a}_B\right)^k \left(-\sqrt{t}\hat{a}_B\right)^l \\ &= \sum_{k,l=0}^{\infty} \frac{Z_B^{ll}}{k!l!} (1-t)^k (-1)^{2l} t^l \left(\hat{a}_B^\dagger\right)^{k+l} \left|00\right\rangle \left\langle 00\right| \hat{a}_B^{k+l} \\ &= \left|0\right\rangle \left\langle 0\right| \otimes \sum_{k,l=0}^{\infty} Z_B^{ll} \frac{(k+l)!}{k!l!} (1-t)^k t^l \left|k+l\right\rangle \left\langle k+l\right|\end{aligned} \tag{C.17}$$

We now perform the substitution $m = k + l$ and notice some binomial coefficients:

$$\begin{aligned}E^{(t)}(Z_B) &= \left|0\right\rangle \left\langle 0\right| \otimes \sum_{m=0}^{\infty} \sum_{l=0}^{q} Z_B^{ll} \frac{m!}{(m-l)!l!} (1-t)^{m-l} t^l \left|m\right\rangle \left\langle m\right| \\ &= \left|0\right\rangle \left\langle 0\right| \otimes \sum_{m=0}^{\infty} \sum_{l=0}^{m} \binom{m}{l} Z_B^{ll} (1-t)^{m-l} t^l \left|m\right\rangle \left\langle m\right|.\end{aligned} \tag{C.18}$$

APPENDIX D

RÉSUMÉ EN FRANÇAIS (FRENCH SUMMARY)

Les lois de la mécanique quantique présentent un fort potentiel d'amélioration pour la sécurité des réseaux de communication, de la distribution de clé secrète au vote électronique, en passant par la banque en ligne. La sécurité d'un grand nombre de ces tâches repose actuellement sur des hypothèses de calcul: la complexité de l'encodage est telle qu'un adversaire utilisant une technologie de pointe ne pourra obtenir la puissance de calcul suffisante pour compromettre la sécurité du protocole (sur une échelle de temps donnée). Cependant, les progrès en algorithmique, ainsi que l'émergence de nouvelles plateformes quantiques permettant une augmentation drastique de la puissance de calcul pour certaines tâches, présentent une menace pour ce type de sécurité. Il est donc naturel de s'intéresser aux avantages que peut nous apporter la théorie quantique afin d'éliminer le recours aux hypothèses de calcul.

Cette thèse porte sur l'analyse de sécurité pratique et la réalisation expérimentale de deux tâches cryptographiques importantes, dont la sécurité est garantie par les lois de la mécanique quantique: la monnaie quantique et le tirage à pile-ou-face faible. Contrairement à la distribution de clé secrète, où les parties impliquées coopèrent face à un adversaire commun, ces protocoles impliquent des parties n'ayant aucune confiance mutuelle.

La monnaie quantique exploite le théorème de non-clonage quantique pour générer des jetons, billets ou cartes de crédit strictement infalsifiables. Ceci est impossible sans hypothèse de calcul en utilisant des ressources uniquement classiques. Nous réalisons la première démonstration expérimentale de cette fonctionnalité sur une plateforme

photonique aux longueurs d'onde télécom. Un numéro de série classique, ainsi qu'une clé secrète, sont associés à une carte de crédit, constituée d'une chaîne d'impulsions de lumière cohérente très atténuée. Chaque bit de la clé secrète est encodé sur la polarisation d'une de ces impulsions. La sécurité est garantie par un choix d'encodage aléatoire, constitué de deux bases quantiques conjuguées possibles, inconnues de l'adversaire. Grâce au principe d'incertitude, une tentative de contrefaçon, réalisée par le biais de mesures quantiques, entraînera la modification de la polarisation de certains états de la carte; cette modification pourra alors être détectée par la banque, connaissant les bases d'encodage de la carte de crédit originale.

Dans un second temps, nous développons une analyse de sécurité pratique pour les cartes de crédit quantiques, prenant en compte l'effet du bruit et des pertes expérimentales sur la sécurité du protocole, en présence d'un terminal de paiement honnête. Nous étendons l'analyse aux terminaux de paiement malhonnêtes, afin que la banque puisse vérifier l'authenticité de la carte à distance.

Dans un troisième temps, nous proposons une expérience permettant le stockage sécurisé des états cohérents constituant la carte de crédit quantique en utilisant la transparence électromagnétiquement induite au sein d'un nuage d'atomes refroidis. Dans l'expérience proposée, les deux composantes de la polarisation des états cohérents sont multiplexées spatialement pour permettre le stockage, puis recombinées à la sortie du nuage d'atomes. Nous estimons le temps de vie sécurisé de la carte de crédit en fonction des paramètres du dispositif de stockage.

Le tirage à pile-ou-face faible est une primitive cryptographique fondamentale: elle permet en effet la construction de tâches plus complexes, telles que la mise en gage de bit et le calcul multipartite sécurisé. Lors d'un tirage à pile ou face, deux entités distantes et méfiantes jettent une pièce. Grâce à l'intrication quantique, il est possible de limiter la probabilité que l'entité malhonnête biaise la pièce. Il est important de rappeler qu'en utilisant des ressources classiques uniquement, la sécurité de ce protocole requiert nécessairement des hypothèses de calcul. Dans ce projet, nous proposons la première implémentation du pile-ou-face faible. Celle-ci requiert un photon unique, une plateforme d'optique linéaire et trois détecteurs de photons uniques. Nous présentons l'analyse de sécurité en présence de bruit et de pertes, et démontrons que le protocole est réalisable à l'échelle d'une ville sur une réseau de fibres optiques. Enfin, nous proposons de réduire davantage la probabilité du biais du protocole, en explorant des versions du protocole à plusieurs intéractions.

BIBLIOGRAPHY

[1] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," *Proceedings of the Symposium on Theory of Computing*, vol. 19, pp. 218–229, 1987.

[2] D. Alistarh, J. Aspnes, V. King, and J. Saia, "Communication-efficient randomized consensus," *Distrib. Comput.*, vol. 31, no. 6, pp. 489–501, 2018.

[3] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1997.

[4] W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802, 1982.

[5] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, p. 78, 1983.

[6] F. Miller, *Telegraphic code to ensure privacy and secrecy in the transmission of telegrams*.
C.M. Cornwell, 1882.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, vol. 1, (Bangalore, India), pp. 175–179, 1984.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, p. 145, 2002.

[9] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, p. 1301, 2009.

[10] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," *Phys. Rev. Lett.*, vol. 95, p. 010503, 2005.

[11] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, and S. Wehner, "Local quantum measurement and no-signaling imply quantum correlations," *Phys. Rev. Lett.*, vol. 104, p. 140401, 2010.

[12] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, pp. 351–382, 2016.

[13] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, p. 190502, 2018.

[14] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, p. 16025, 2016.

[15] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society A*, vol. 400, 1985.

[16] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J.Sci.Statist.Comput. 26*, vol. 26, 1997.

[17] J. Bell, "On the einstein-podolsky-rosen paradox," *Physics*, vol. 1, pp. 195–290, 1964.

[18] R. W. Spekkens and T. Rudolph, "A quantum protocol for cheat-sensitive weak coin flipping," *Phys. Rev. Lett.*, vol. 89, p. 227901, 2002.

[19] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Phys. Rev. Lett.*, vol. 122, 2019.

[20] A. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, p. 661, 1991.

[21] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, 1993.

[22] A. Unnikrishnan and D. Markham, "Authenticated teleportation with one-sided trust," *Phys. Rev. A*, vol. 100, 2019.

[23] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: a vision for the road ahead," *Science*, vol. 362, 2018.

[24] "Quantum protocol zoo," *https://wiki.veriqloud.fr/index.php?title=Main_Page*.

[25] A. Chailloux and I. Kerenidis, "Optimal quantum strong coin flipping," *50th Annual IEEE Symposium on Foundations of Computer Science*, pp. 527–533, 2009.

[26] A. Chailloux and I. Kerenidis, "Optimal bounds for quantum bit commitment," *52nd Annual IEEE Symposium on Foundations of Computer Science*, p. 354–362, 2011.

[27] M. D. sek, M. Jahma, and N.Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A*, vol. 62, p. 022306, 2000.

[28] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Information*, vol. 4, p. 5, 2018.

[29] M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," *Phys. Rev. A*, vol. 99, no. 2, p. 022336, 2019.

[30] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, p. 880, 1969.

[31] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities," *Phys. Rev. Lett.*, vol. 49, p. 91, 1982.

[32] A. Molina, T. Vidick, and J. Watrous, "Optimal counterfeiting attacks and generalizations for wiesner's quantum money," in *TQC 2012: Theory of Quantum Computation, Communication, and Cryptography* (K. Iwama, Y. Kawano, and M. Murao, eds.), vol. 7582 of *Lecture Notes in Computer Science*, Springer, 2013.

[33] J. Watrous, *Semidefinite Programming*, ch. 7.
University of Waterloo, 2011.

[34] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, no. 1, pp. 49–95, 1996.

[35] T. Chanelière, G. Hétet, and N. Sangouard, "Quantum optical memory protocols in atomic ensembles," *Advances In Atomic, Molecular, and Optical Physics*, vol. 67, pp. 77–150, 2018.

[36] H. P. Specht, C. Nölleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, "A single-atom quantum memory," *Nature*, vol. 473, pp. 190–193, 2011.

[37] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. J. Twitchen, J. I. Cirac, and M. D. Lukin, "Room-temperature quantum bit memory exceeding one second," *Science*, vol. 336, pp. 1283–1286, 2012.

[38] P. Lambropoulos and D. Petrosyan, *Fundamentals of Quantum Optics and Quantum Information*, ch. 5.
Springer, 2007.

[39] J. Keeling, *Light-Matter Interactions and Quantum Optics*, ch. 12.
University of Saint Andrews, 2019.

[40] S. Moulik and P. Panigrahi, "Quantum cheques," *Quantum Information Processing*, vol. 15, pp. 2475–2486, 2016.

[41] D. Gavinski, "Quantum money with classical verification," in *Proc. IEEE 27th Annual Conference on Computational Complexity (CCC)*, pp. 42–52, IEEE, 2012.

[42] A. Brodutch, D. Nagaj, O. Sattath, and D. Unruh, "An adaptive attack on wiesner's quantum money," *Quantum Information & Computation*, vol. 16, no. 11–12, pp. 1048–1070, 2016.

[43] R. Mittal and M. Szegedy, "Product rules in semidefinite programming," *Fundamentals of Computation Theory. FCT*, pp. 435–445, 2007.

[44] M. Georgiou and I. Kerenidis, "New constructions for quantum money," in *Proc. 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)* (S. Beigi and R. König, eds.), vol. 44, (Dagstuhl, Germany), pp. 92–110, Schloß Dagstuhl–Leibniz-Zentrum für Informatik, 2015.

[45] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, "Unforgeable noise-tolerant quantum tokens," *PNAS*, vol. 109, no. 40, pp. 16079–16082, 2012.

[46] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing models for optical measurements in quantum communication," *Phys. Rev. Lett.*, vol. 101, p. 093601, 2008.

[47] K. Horodecki and M. Stankiewicz, "Semi-device independent quantum money," *arXiv*, vol. 1811.10552, 2018.

[48] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor, "Breaking and making quantum money: towards a new quantum cryptographic protocol," in *Proc. Innovations in Computer Science (ICS)*, pp. 20–31, 2010.

[49] M. Mosca and D. Stebila, "Quantum coins," *Error-Correcting Codes, Finite Geometries and Cryptography*, vol. 523, pp. 35–47, 2010.

[50] S. Aaronson and P. Christiano, "Quantum money from hidden subspaces," *Theory of Computing*, vol. 9, no. 9, pp. 349–401, 2013.
Conference version in Proc. ACM STOC, pp. 41–60, 2012.

[51] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor, "Quantum money from knots," in *Proc. 3rd Innovations in Theoretical Computer Science Conference, ITCS'12*, (New York, NY, USA), pp. 276–289, 2012.

[52] G. Alagic and B. Fefferman, "On quantum obfuscation," *arXiv*, vol. 1602.01771, 2016.

[53] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, "Experimental quantum forgery of quantum optical money," *npj Quantum Information*, vol. 3, p. 7, 2017.

[54] C. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," *Advances in Cryptology*, vol. Proceedings of Crypto 82, pp. 267–275, 1983.

[55] A. Iqbal, M. J. Aslam, and H. S. Nayab, "Quantum cryptography: a brief review of the recent developments and future perspectives," *Proceedings of the International Conference on Digital Information Processing, Electronics, and Wireless Communications, Dubai, UAE*, 2016.

[56] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, p. 2818, 1996.

[57] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, p. 1330, 2000.

[58] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quant. Inf. Comput.*, vol. 8, p. 431, 2007.

[59] J. L. Duligall, M. S, Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum cryptography," *New J. Phys.*, vol. 8, p. 249, 2006.

[60] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, 2002.

[61] A. Kitaev, "Quantum coin flipping," *6th Workshop on Quantum Information Processing*, 2003.

[62] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, "Experimental plug and play quantum coin flipping," *Nat. Commun.*, vol. 5, p. 3717, 2014.

[63] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, "Experimental loss-tolerant quantum coin flipping," *Nat. Commun.*, vol. 2, p. 561, 2011.

[64] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, "Experimental quantum coin tossing," *Phys. Rev. Lett.*, vol. 94, p. 040501, 2005.

[65] E. Hänggi and J. Wullschleger, "Tight bounds for classical and quantum coin flipping," *Proceedings of TCC*, pp. 468–485, 2011.

[66] J. M. Arrazola, M. Karasamanis, and N. Lütkenhaus, "Practical quantum retrieval games," *Phys. Rev. A*, vol. 93, p. 062311, 2016.

[67] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, "Exponential separation of quantum and classical one-way communication complexity," in *Proc. 36th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 128–137, 2004.

[68] R. Amiri and J. M. Arrazola, "Quantum money with nearly optimal error tolerance," *Phys. Rev. A*, vol. 95, p. 062334, 2017.

[69] J.-Y. Guan, J.-M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J.-W. Pan, "Experimental preparation and verification of quantum money," *Phys. Rev. A*, vol. 97, p. 032338, 2018.

[70] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*.
Cambridge University Press, 2005.

[71] A. Nicolas, L. Veissier, L. Giner, E. Giacobino, D. Maxein, and J. Laurat, "A quantum memory for orbital angular momentum photonic qubits," *Nature Photon.*, vol. 8, p. 34, 2014.

[72] J. Rui, Y. Jiang, S.-J. Yang, B. Zhao, X.-H. Bao, and J.-W. Pan, "Operating spin echo in the quantum regime for an atomic-ensemble quantum memory," *Phys. Rev. Lett.*, vol. 115, p. 133002, 2015.

[73] A. Chefles, "Unambiguous discrimination between linearly independent states," *Phys. Lett. A*, vol. 239, no. 6, pp. 339–347, 1998.

[74] A. Chefles and S. M. Barnett, "Optimum unambiguous discrimination between linearly independent symmetric states," *Phys. Lett. A*, vol. 250, no. 4, pp. 223–229, 1998.

[75] H.-K. Lo and J. Preskill, "Phase randomization improves the security of quantum key distribution," no. CALT-68-2556, 2005.

[76] Y. Zhao, B. Qi, and H.-K. Lo, "Experimental quantum key distribution with active phase randomization," *Appl. Phys. Lett.*, vol. 90, p. 044106, 2007.

[77] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, 2007.

[78] X. Ma and N. Lütkenhaus, "Improved data post-processing in quantum key distribution and application to loss thresholds in device independent qkd," *Quantum Information & Computation*, vol. 12, pp. 202–204, Mar 2012.

[79] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," *Phys. Rev. A*, vol. 85, p. 010301, Jan 2012.

[80] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[81] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, Mar 2012.

[82] Y.-C. Liang, T. Vértesi, and N. Brunner, "Semi-device-independent bounds on entanglement," *Phys. Rev. A*, vol. 83, p. 022108, Feb 2011.

[83] M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," *Phys. Rev. A*, vol. 84, p. 010302, Jul 2011.

[84] O. Gittsovich and T. Moroder, "Key rate for calibration robust entanglement based bb84 quantum key distribution protocol," in *Proc. of 11th Int. Conf. on Quantum Communication, Measurement and Computation (QCMC12)*, vol. 1633 of *AIP Conference Proceedings*, p. 156, American Institute of Physics, 2013.

[85] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, "Semi-device-independent framework based on natural physical assumptions," *Quantum*, vol. 1, p. 33, 2017.

[86] K. Jiráková, K. Bartkiewicz, A. Černoch, and K. Lemr, "Experimentally attacking quantum money schemes based on quantum retrieval games," 2018.

[87] O. Gittsovich, N. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, "Squashing model for detectors and applications to quantum key distribution protocols," *Phys. Rev. A*, vol. 89, p. 012325, 2014.

[88] K. C. Toh, M. J. Todd, and R. H. Tütüncü, "Sdpt3 — a matlab software package for semidefinite programming," *Optimization Methods and Software*, vol. 11, no. 1–4, pp. 545–581, 1999.

[89] R. H. Tütüncü, K. C. Toh, and M. J. Todd, "Solving semidefinite-quadratic-linear programs using sdpt3," *Mathematical Programming*, vol. 95, pp. 189–217, Feb 2003.

[90] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1." `http://cvxr.com/cvx`, Mar. 2014.

[91] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control* (V. Blondel, S. Boyd, and H. Kimura, eds.), vol. 371 of *Lecture Notes in Control and Information Sciences*, pp. 95–110, Springer, 2008.

[92] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nat. Photonics*, vol. 3, pp. 696–705, 2009.

[93] A. E. Lita, A. J. Miller, and S. Woo Nam, "Counting near-infrared single-photons with 95% efficiency," *Opt. Express*, vol. 16, no. 5, pp. 3032–3040, 2008.

[94] G. M. D'Ariano, G. Chiribella, and P. Perinotti, pp. 39–40.
Cambridge University Press, 2017.

[95] A. S. Arora, J. Roland, and S. Weis, "Quantum weak coin flipping," *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pp. 205–216, 2019.

[96] P. Mironowicz and M. Pawlowski, "Experimentally feasible semi-device-independent certification of 4 outcome povms," *arXiv*, vol. 1811.12872, 2018.

[97] J. Bavaresco, M. Araújo, Brukner, and M. T. Quintino, "Semi-device-independent certification of indefinite causal order," *arXiv*, vol. 1903.10526, 2019.

[98] P. Vernaz-Gris, K. Huang, M. Cao, A. Sheremet, and J. Laurat, "Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble," *Nat. Comm.*, vol. 9, p. 363, 2018.

[99] V. Tiporlini and K. Alameh, "High sensitivity optically pumped quantum magnetometer," *The Scientific World Journal*, vol. 2013, p. 858379, 2013.

[100] Y.-F. Hsiao, P.-J. Tsai, S.-X. L. Hung-Shiue Chen, C.-C. Hung, C.-H. Lee, Y.-H. Chen, Y.-F. Chen, I. A. Yu, and Y.-C. Chen, "Highly efficient coherent optical memory based on electromagnetically induced transparency," *Phys. Rev. Lett.*, vol. 120, p. 183602, 2018.

[101] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, "Fair loss-tolerant quantum coin flipping," *Phys. Rev. A*, vol. 80, p. 062321, 2009.

[102] C. Mochon, "Quantum weak coin flipping with arbitrarily small bias," *arXiv*, vol. 0711.4114, 2007.

[103] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, and L. Magnin, "A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias," *SIAM J. Comput.*, vol. 45, no. 3, p. 633–679, 2016.

[104] I. Kerenidis and A. Nayak, "Weak coin flipping with small bias," *Inf. Proc. Lett.*, vol. 89, pp. 131–135, 2004.

[105] C. Mochon, "Quantum weak coin flipping with bias of 0.192," *45th Symposium on Foundations of Computer Science*, pp. CALT–68–2486, 2004.

[106] C. Mochon, "Large family of quantum weak coin-flipping protocols," *Phys. Rev. A*, vol. 72, no. 2, p. 022341, 2005.

[107] C. Couteau, "Spontaneous parametric down-conversion," *Contemporary Physics*, vol. 59, no. 3, pp. 291–304, 2018.

[108] D. Berry and A. Lvovsky, "Linear-optical processing cannot increase photon efficiency," *Phys. Rev. Lett.*, vol. 105, no. 20, p. 203601, 2010.

[109] A. Ferraro, S. Olivares, and M. G. Paris, "Gaussian states in continuous variable quantum information," *arXiv preprint quant-ph/0503237*, 2005.

[110] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," *Phys. Rev. Lett.*, vol. 73, no. 1, p. 58, 1994.

université PARIS-SACLAY

ÉCOLE DOCTORALE
Ondes et Matière (EDOM)

Titre : Sécurité et implémentation en cryptographie quantique avancée : *monnaie quantique et tirage à pile ou face faible.*

Mots clés : cryptographie quantique, optique quantique, réseaux quantiques, mémoire quantique

Résumé : Les lois de la mécanique quantique présentent un fort potentiel d'amélioration pour la sécurité des réseaux de communication, du cryptage à clé publique au vote électronique, en passant par la banque en ligne. Cette thèse porte sur la sécurité pratique et l'implémentation de deux tâches cryptographiques quantiques : la monnaie quantique et le tirage à pile-ou-face faible.
La monnaie quantique exploite le théorème de non-clonage quantique pour générer des jetons, billets ou cartes de crédit strictement infalsifiables. Nous réalisons la première démonstration expérimentale de cette fonctionnalité sur une plateforme photonique aux longueurs d'onde télécom. Nous développons ensuite une analyse de sécurité pratique pour les cartes de crédit quantiques. La banque peut ainsi vérifier l'authenticité de la carte à distance, même en présence d'un terminal de paiement malhonnête. Enfin, nous proposons une expérience permettant le stockage sécurisé d'une carte de crédit quantique en utilisant la transparence électromagnétiquement induite au sein d'un nuage d'atomes refroidis.
Le tirage à pile-ou-face faible est une primitive cryptographique fondamentale : elle permet en effet la construction de tâches plus complexes telles que la mise en gage de bit et le calcul multipartite sécurisé. Lors d'un tirage à pile ou face, deux entités distantes et méfiantes jettent une pièce. Grâce à l'intrication quantique, il est possible de limiter la probabilité que l'entité malhonnête biaise la pièce. Dans ce projet, nous proposons la première implémentation du pile-ou-face faible. Celle-ci requiert un photon unique et une plateforme d'optique linéaire. Nous présentons l'analyse de sécurité en présence d'erreurs et de pertes, et démontrons que le protocole est réalisable à l'échelle d'une ville. Enfin, nous proposons de réduire davantage la probabilité du biais du protocole.

Title : Security and implementation of advanced quantum cryptography: *quantum money and quantum weak coin flipping.*

Keywords : quantum cryptography, quantum optics, quantum networks, quantum memory

Abstract : Harnessing the laws of quantum theory can drastically boost the security of modern communication networks, from public key encryption to electronic voting and online banking. In this thesis, we bridge the gap between theory and experiment regarding two quantum-cryptographic tasks : quantum money and quantum weak coin flipping.
Quantum money exploits the no-cloning property of quantum physics to generate unforgeable tokens, banknotes, and credit cards. We provide the first proof-of-principle implementation of this task, using photonic systems at telecom wavelengths. We then develop a practical security proof for quantum credit card schemes, in which the bank can remotely verify a card even in the presence of a malicious payment terminal. We finally propose a setup for secure quantum storage of the credit card, using electromagnetically-induced transparency in a cloud of cold cesium atoms.
Quantum weak coin flipping is a fundamental cryptographic primitive, which helps construct more complex tasks such as bit commitment and multiparty computation. It allows two distant parties to flip a coin when they both desire opposite outcomes. Using quantum entanglement then prevents any party from biasing the outcome of the flip beyond a certain probability. We propose the first implementation for quantum weak coin flipping, which requires a single photon and linear optics only. We provide the complete security analysis in the presence of noise and losses, and show that the protocol is implementable on the scale of a small city with current technology. We finally propose a linear-optical extension of the protocol to lower the coin bias.

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France