Photonic Resources for the Implementation of Quantum Network Protocols

Simon Neves

Sorbonne Université

Photonic Resources for the Implementation of Quantum Network Protocols

Simon Neves

Photonic Resources for the Implementation of Quantum Network Protocols

SIMON NEVES

Thèse de Doctorat de Sorbonne Université.
Ecole Doctorale Informatique, Télécommunications et Electronique (n° 572).
Specialité Physique Quantique.

Thèse présentée et soutenue à Paris le 2 décembre 2022,
en présence du jury suivant:

M. Nicolas Brunner: Rapporteur,
Professeur, Université de Genève, Suisse.
M. Fabio Sciarrino: Rapporteur,
Professeur, Université de Rome - Sapienza, Italie.
Mme. Eleni Diamanti: Directrice de thèse,
Directrice de recherche, CNRS, Sorbonne Université, France.
M. Jean-Marc Merolla: Examinateur,
Chargé de recherche, CNRS, Université de Besançon, France.
Mme. Virginia D'Auria: Examinatrice,
Maîtresse de Conférence, Université de Nice, France.
M. Nicolas Treps: Examinateur,
Professeur, Sorbonne Université, France.

Frontpage artwork: K78 - *Tangled*, by Rémi Meyer

Formerly scientist at the French national research agency (CNRS) and specialized in ultrafast laser-matter interaction, Rémi Meyer is today a photographer and plastic artist. The heart of his artistic research still lies in laboratory and borrows the very same material as the one used for his scientific work.

Previously shaping the laser light to investigate how it interacts with matter, Rémi today explores the properties of supercontinuum laser beams as a plastic object, which he bends, curves and textures as it propagates, until it hits the sensitive surface of the camera to create in a single image a whole new universe.

Imprimé à Sorbonne Université, Paris, France.

Contact: simon.neves@laposte.net

A mon grand-père.

Abstract (English)

The security of modern communication networks can be enhanced thanks to the laws of quantum mechanics. In this way, important tasks such as encryption key distribution, anonymous transmissions or electronic voting can be made secure without computational assumptions. In this thesis, we develop a source of photonic quantum states which we use to demonstrate new quantum-cryptographic primitives: quantum weak coin flipping, and the certified transmission of quantum information through an untrusted quantum channel.

Our source produces photon-pairs via spontaneous parametric down-conversion in the telecom range. Pairs can be used as heralded single-photons, or as close-to-maximally entangled pairs. We show this source is suitable for the implementation of quantum protocols. We also provide a novel design in order to adapt this source to multipartite entanglement generation.

Weak coin flipping allows two distant players to decide of a random winner. Using quantum resources allows to enforce information-theoretic security and cheat-sensitivity. We demonstrate a refined and loss-tolerent version of a recently proposed theoretical protocol, using heralded single-photons mixed with vacuum to produce entanglement. Cheating players are detected in a verification step, which involves a carefully optimized linear optical interferometer including beam splitters with variable reflectivities and a fast optical switch. We demonstrate high values of our protocol benchmarks for attenuations corresponding to several kilometers of telecom optical fiber.

Finally, we provide a new protocol for certifying the transmission of an unmeasured qubit through a lossy and untrusted channel. The security of the primitive is based on new fundamental results of lossy quantum channels. Probing the channel with part of a maximally-entangled state allows to device-independently test its quality, using self-testing of Bell or steering inequalities. We demonstrate that protocol using photon-pairs entangled in polarization to probe the channel. We show it allows the certification of quantum communication for a large amount of losses induced by the channel.

Abstract (Français)

La sécurité des réseaux modernes de communication peut être renforcée grâce aux lois de la mécanique quantique, permettant d'effectuer sans hypothèse d'importantes tâches telles que la distribution de clés de cryptage, les transmissions anonymes ou le vote électronique. Dans cette thèse, nous développons une source d'états quantiques photoniques grâce auxquels nous démontrons de nouvelles primitives cryptographiques : le tirage à pile-ou-face faible et la transmission certifiée via un canal quantique non-fiable.

Notre source produit des paires de photons par conversion paramétrique descendante spontanée à longueurs d'onde télécoms. Les paires sont utilisées comme des photons uniques annoncés ou des paires intriquées. Nous montrons que cette source est adaptée à la mise en œuvre de protocoles quantiques, et proposons une méthode afin d'adapter cette source à la génération d'états intriqués multipartites.

Le tirage à pile-ou-face faible permet à deux joueurs distants de décider d'un gagnant aléatoire. L'utilisation de ressources quantiques rend le protocole sensible à la triche et sécurisé par la théorie de l'information. Nous démontrons une version retravaillée et tolérante aux pertes d'un protocole théorique récemment proposé. Nous utilisons des photons uniques annoncés, mélangés avec le vide pour produire de l'intrication. Un joueur malhonnête est détecté lors d'une étape de vérification, incluant un interféromètre optique linéaire comprenant des séparateurs de faisceau à réflectivités variables et un commutateur optique rapide. Nous démontrons des valeurs de référence élevées pour des atténuations correspondant à plusieurs kilomètres de fibre optique télécoms.

Enfin, nous fournissons un nouveau protocole pour certifier la transmission d'un qubit non-mesuré à travers un canal non-fiable présentant des pertes. Il est possible de tester la qualité du canal en le sondant avec une moitié d'état maximalement intriqué, et ce indépendamment du système de mesure, en utilisant la technique de *self-testing* des inégalités de Bell ou de *steering*. Nous démontrons ce protocole en utilisant des paires de photons intriqués en polarisation pour sonder le canal. Nous montrons qu'il permet la certification de communications quantiques pour une grande quantité de pertes induites par le canal.

Remerciements

Le travail réalisé pendant cette thèse n'aurait été possible sans l'aide et le soutien de nombreuses personnes. Je m'appliquerai ici à les mentionner avec le plus d'exhaustivité possible. Si toutefois vous ne vous retrouvez pas dans ces lignes malgré votre contribution, fut-elle directe ou indirecte, je vous prie d'attribuer cette négligence à la faillibilité de ma mémoire, plutôt qu'à de l'ingratitude de ma part, et je vous fais part de ma plus grande reconnaissance.

Tout d'abord, j'aimerais exprimer ma plus sincère gratitude à ma directrice de thèse, Eleni, pour m'avoir permis de vivre cette expérience exceptionnelle. Je suis particulièrement reconnaissant pour la confiance que tu m'as accordée dès le début de ce projet, ainsi que pour ton soutien indéfectible. Un grand merci pour tout ce que tu m'as appris, autant sur le plan humain que scientifique. Je tiens aussi à remercier Damian, pour avoir supervisé une grande partie de mon travail, et pour m'avoir ainsi accordé une part considérable de ton temps. À vous deux, comme à Elham, Fred, Alex et Marco, je vous fais part de ma plus grande reconnaissance pour avoir donné à cette équipe une atmosphère si chaleureuse, par votre bienveillance, votre enthousiasme, et votre générosité.

J'aimerais ensuite remercier toutes les personnes que j'ai eu l'honneur de rencontrer au sein de l'équipe QI et du LIP6. Ma reconnaissance va en premier lieu à Verena et Laura, avec qui j'ai eu la chance de travailler sur ces expériences naissantes, qui n'auraient pu aboutir sans votre contribution. Un grand merci à vous deux d'avoir partagé avec moi les victoires comme les galères. J'ai hâte de voir où vous porterez nos expériences ! Je tiens ensuite à remercier Mathieu, pour toute l'aide que tu m'as apportée, ainsi que pour tes conseils avisés et ton soutien, même après ton départ. De même, j'aimerais dire un grand merci à Adrien et Amine, là aussi pour votre soutien, mais aussi pour tout ce que vous avez fait pour l'installation de la salle d'expérience. Dans ce sens, j'ai aussi une pensée particulière pour Alisa et Eugène, sans qui je n'aurais jamais pu commencer ces expériences à temps. Je souhaite ensuite exprimer ma reconnaissance à Matteo et Pascal, pour les conseils que vous m'avez donnés au laboratoire, ainsi que pour les

super parties de *Magic The Gathering*. Pour les passionnantes collaborations scientifiques, je remercie également Ulysse, Iordanis, Ivan, Anu et Raja. À ce dernier, comme à Luka, Léo et Gabriel, je dis aussi un grand merci pour les moments militants que nous avons partagés, ainsi que pour les discussions passionnées. Enfin, j'aimerais exprimer ma plus profonde gratitude à toutes les autres formidables personnes rencontrées au cours de ma thèse, et qui ont toutes contribué à leur échelle à cette ambiance si chaleureuse (dans un ordre aléatoire): Yoann, Valentina, Adriano, Andrea, Uta, Dominik, Clément, PE, Nathan, Rawad, Robert, Yao, Victor, Federico, Rhea, Natansh, Anthia, Ilektra, Majid, Harold, Shraddha, Ioanna, Luis, Paul Hermouet and Paul Hilaire, Hela, Kim, Ellen, George, Salomé, Shane, Michael, Luís, Niraj, Tom, Shouvik, Santiago, Ieva, Mina, Bo, Damien, Gozde, Francesco, ... et tant d'autres que j'ai sans doute oubliés, et qui j'espère ne m'en tiendront pas rigueur !

Tout au long de mon parcours j'ai pu compter sur l'appui de nombreuses personnes extérieures au laboratoire. Je pense bien sûr à Nicolas Treps, Francesco Graffitti et Massimiliano Smania, pour les conseils que vous m'avez donnés au démarrage de mes expériences. Pour vos conseils avisés liés au monde de la recherche, je tiens aussi à remercier Quentin Bodart, ainsi que Rémi Meyer que je remercie également pour la magnifique illustration de première de couverture de ce manuscrit. J'aimerais ensuite exprimer ma gratitude aux enseignants remarquables qui ont su cultiver ma passion des sciences, et m'ont guidé tout au long de ma scolarité. Je mentionnerais notamment Arnaud De Araujo, Anna Oblak, Stéphane Carbonneau, Laurence Baulu et Marc Tuloup, et nombre de vos collègues qui m'ont poussé sur cette voie. Je remercie également François Courvoisier, pour ton rôle déterminant dans mon orientation vers l'optique expérimentale. Je souhaite enfin rendre hommage à Edouard Oblak, qui le premier m'a ouvert au monde de la recherche. Nos rencontres, bien que trop brèves, auront été des plus décisives dans mon parcours.

Finalement, j'aimerais remercier du fond du coeur tous mes proches qui m'ont encouragé et soutenu pendant toutes ces années. Je mentionnerai notamment Guillaume, Nicolas et Julien, éternels compagnons de questionnements existentiels, ainsi que Magdalena, pour tous ces fabuleux '*weightless moments*', les incroyables découvertes musicales, et ta présence, tout simplement. À tous mes amis avec qui j'ai passé des moments inoubliables à Paris ou ailleurs, je vous dis un grand merci. Finalement, ma plus grande reconnaissance va à ma famille, notamment à mes parents, pour m'avoir toujours soutenu et avoir cru en moi. Un hommage particulier va à mon grand-père, dont je regrette l'absence à la fin de cette aventure, et à qui je dédie ce manuscrit.

List of Abbreviations

APD	Avalanche photo-diode
BBO	β-barium borate
BS	Beam splitter
BSM	Bell-state measurement
c.c.	Coincidence counter
CHSH	Clauser, Horne, Shimony, Holt
CKA	Conference key agreement
conj.	Complex conjugate
CPTD	Completely-positive trace-decreasing
CPTP	Completely-positive trace-preserving
CW	Continuous-wave
DC	Dark count
DI	Device-independent
1sDI	One-sided device-independent
DM	Dichroic mirror
EM	Electromagnetic
EPR	Einstein, Podolsky, Rosen
FWHM	Full-width at half-maximum
GHZ	Greenberger, Horne, Zeilinger
HOM	Hong-Ou-Mandel
HWP	Half-wave plate
IID	Independent identically distributed rounds
JSA	Joint spectral amplitude
KTP	Potassium Titanyl Phosphate

LHV	Local hidden variables
MLE	Maximum likelihood estimation
PA	Polarization analyzer
PBS	Polarizing beam splitter
PC	Polarization controller
POVM	Positive operator-valued measurement
PP	Periodically-poled
QKD	Quantum key distribution
QPM	Quasi-phase-matching
QST	Quantum state tomography
QWP	Quarter-wave plate
RSA	Rivest, Shamir, Adleman
SCF	Strong coin flipping
SM	Single-mode
SNSPD	Superconducting nanowire single-photon detector
SPDC	Spontaneous parametric down-conversion
VOA	Variable optical attenuator
WCF	Weak coin flipping
WP	Wave plate

List of Notations

$\|\psi\rangle$	State vector, or *ket*
$\langle\psi\|$	Dual vector, or *bra*
$\|\psi\rangle\langle\psi\|$	Projector on ket $\|\psi\rangle$
$\langle\psi\|\phi\rangle$	Hermitian inner product (quantum states)
$\mathbf{a}\cdot\mathbf{b}$	Inner product (complex vectors)
$\mathbf{a}\times\mathbf{b}$	Vector product
$\|\mathbf{r}\|$	Norm of vector $\mathbf{r}$
$\mathbb{1}$	Identity operator
$\langle\hat{A}\rangle$	Expected value of observable $\hat{A}$
$\hat{A}^\dagger$	Hermitian conjugate of matrix $\hat{A}$
$\mathrm{Tr}(\hat{A})$	Trace of matrix $\hat{A}$
$\mathrm{Tr}_{\mathscr{H}}(\hat{A})$	Partial trace of matrix $\hat{A}$ on space $\mathscr{H}$
$\mathscr{L}(\mathscr{H})$	Endomorphism space on $\mathscr{H}$
$\dim\mathscr{H}$	Dimension of $\mathscr{H}$
$\otimes$	Tensor product
$\bigotimes_i$	Tensor product over the index i
$\sum_i$	Sum over the index i
$\mathbb{P}$	Probability
$\|\cdot\|$	Absolute value

Table of Contents

'Pearls in oysters may take years
to swell around the sand.'

— An Pierlé, *Certain Days*.

CHAPTER 1

INTRODUCTION

The ongoing development of modern communication technologies allows more and more users to connect in an ever growing global network, with high-speed data transmissions and strong data-processing capabilities. On a more local scale, the emerging idea of *smart cities* promises to connect even the most simple devices in order to improve our everyday quality of life. Despite these seemingly desirable aspects, such new technologies also raise the awareness and skepticism regarding potential threats to privacy and general security of the network. In this context, secure methods allowing to perform a collection of elementary tasks or *primitives*, including private and anonymous communications, remote shared randomness, or faithful message transmission, are needed in order to build more complex and concrete procedures, such as online banking, electronic voting or digital signatures.

The security of current cryptographic primitives generally relies on so-called computational assumptions. In other words, with the known calculation power of classical computers, cracking such a protocol is a near-impossible task, or requires an amount of time so big it makes the task useless. For instance, the RSA cypher [1], used for the encryption of world-wide banking transactions, relies on finding the prime factors of a large integer, which is an exponentially-hard problem

even for modern classical computers. Still, the security of RSA holds only thanks to our knowledge of currently available computational power, which may change as new types of computers emerge.

With the rapid development of quantum technologies, such computers may well appear in the near-future. The idea of building a quantum computer is attributed to R. Feynman in 1982 [2] and was further detailed by D. Deutsch in 1985 [3]. By exploiting the fundamental laws of quantum systems, a whole new variety of algorithms can be developed, where the classical bit of well-defined value "0" or "1" makes way for a quantum bit. The value of such *qubit* is undefined until its measurement, the result of which is fundamentally probabilistic. The arising new logic of quantum algorithms goes out of the scope of computational assumptions made to secure classical protocols, therefore threatening the security of modern encryption algorithms. In particular, P. Shor proposed in 1994 a quantum algorithm allowing to find the prime factors of any integer in polynomial time [4], showing the vulnerability of the RSA cyper to quantum attacks. The development of more resistant cryptographic primitives has since grown into one of the most prolific fields of research of the past decades.

If the existence of quantum systems has threatened the security of classical primitives, it has also allowed the development of new quantum cryptography protocols. For instance different protocols were proposed for quantum key distribution (QKD), by C. Bennett and G. Brassard in 1984 [5], and by A. Ekert in 1991 [6]. Such protocols allow two players Alice and Bob to share a private random key, that they can later use to encrypt their messages with optimal security [7, 8]. Contrary to RSA cypher, this security does not rely on any computation assumption, but solely on laws of quantum physics, such as the collapse of quantum states under measurement, Bell theorem [9] relating to quantum entanglement, or the no-cloning theorem [10, 11]. Since then, various quantum protocols have been developed to solve new cryptographic problems, including secret sharing [12–14], bit commitment [15], multipartite QKD [16], or anonymous communications [17], feeding the hope for the development of a world-wide *quantum internet* [18, 19].

Interestingly enough, the resilience of quantum protocols to malicious attacks can take different forms. In the case of a the protocol proposed by R. Spekkens and T. Rudolph for remote weak coin flipping [20], the resources' quantumness provides an advantage over classical protocols in the form of cheat-sensitivity. This primitive allows two remote players Alice and Bob to fairly design a winner between them two, using the randomness of two entangled qubits. The cheat-sensitivity arises when, after the protocol, players verify the entanglement, which unveils a potential cheating player with non-zero probability. Regarding the resilience of entanglement-based protocols, the case of *device-independent* verification procedures may be even more striking. Such procedures allow to certify a wide range of quantum resources, including quantum states [21, 22], measurements [23, 24] or channels [25], while making very few assumptions on the certified systems and measurement devices. In practice, device-independent verification protocols can be used as building blocks to perform more complex tasks involving untrusted resources, such as the recently proposed authenticated teleportation [26].

States of the quantified electromagnetic field, also known as *photons*, have since proven to be promising candidates for the implementation of quantum communications protocols, thanks to their relative ease of manipulation and transmission over large distances with limited decoherence and losses. Thus, quantum information can be encoded in various photonic degrees of freedom, including photon's path [27], orbital angular momentum [28], spectral state [29] or emission time [30]. Most importantly, the polarization degree of freedom has been widely used to demonstrate fundamental quantum properties, such as the most notorious experiment of A. Aspect in 1981 [31] proving the nonlocality of entangled quantum systems, or to implement quantum protocols such as quantum key distribution [32–35], quantum money [36–38], secret sharing [39], or conference key agreement [40, 41]. In general, the generation of entangled- and single-photons of high state quality, detection rates or purity, has become a very active research area, in order to meet the needs for complex communication and cryptography tasks. This way, sources based on spontaneous parametric down-conversion in nonlinear crystals have been used to generate close-to-maximally entangled qubits [42], probabilistic but heralded single-photons [43–45], and multipartite entangled states [46, 47]. The rapid

improvement of these photonic resources, together with the rising enthusiasm surrounding the future development of a quantum internet, further motivates the experimental implementation of new cryptographic primitives, which is the main scope of this thesis.

1.1 Thesis Outline

Chapter 2 introduces the most important concepts and tools required in this thesis. We first go through the mathematical framework of quantum mechanics and information, then we give some insight on classical and quantum optics, and we finally introduce some notions linked to quantum cryptography.

Chapter 3 gives the details of our photon-pairs source. Pairs are generated via spontaneous parametric down-conversion in a periodically-poled KTP crystal, and either used as heralded single-photons, or entangled in their polarization degree of freedom in a Sagnac interferometer [42]. The source's characterization shows in particular that it produces single-photons with relatively high heralding efficiency, and close-to-maximally entangled qubits, proving it is suitable for the implementation of quantum network protocols. In addition, we provide a novel design to upgrade our source to a multipartite source, with relatively few adjustments.

Chapter 4 presents the first implementation of a cheat-sensitive weak coin flipping protocol, based on a heralded single-photon emitted by the source detailed in chapter 3. We follow a refined recipe inspired from [48]. In this protocol, a winner is randomly designated among Alice and Bob, by measuring a photon-path entangled-state generated by Alice from a single-photon. Cheat-sensitivity arises from the entanglement-verification performed by Bob. Simulating fiber-communication losses, we show the correctness and fairness of our protocol over up to 7 km of communication distance between Alice and Bob. Implementing examples of behavior of dishonest Alice and Bob, we then demonstrate our method's cheat-sensitivity, enabled through quantum properties of photons.

Chapter 5 develops some important fundamental results of quantum channels. These objects describe the most general operations undergone by quantum states, and are therefore a necessary ingredient to describe a secure quantum network. Our result includes the extension of different metrics of non-lossy channels to lossy channels, a theorem showing the equivalence of those metrics, and another theorem extending the kwown processing inequality of non-lossy channels to lossy quantum channels.

Chapter 6 builds a protocol for certified quantum communication through an untrusted and lossy quantum channel. Our method consists in probing the channel with maximally-entangled pairs of qubits, and hiding quantum information among those probe states. The security is derived in a device-independent setting, and built in particular from our new fundamental results presented in chapter 5, and from generalizing the verification of lossless quantum channels from [25]. The protocol is particularly robust, as very few assumptions are made on the quantum channel and measurement devices. Using polarization-entangled pairs of photons emitted by our source detailed in chapter 3, we perform the first proof-of-principle implementation of this protocol, in a semi-device independent setting, where the sender's resources are trusted. For this task, we use recent self-testing results from [26]. We simulate an honest but untrusted and lossy quantum channel using a variable optical attenuator, and a dishonest channel by randomly performing bit and phase flips. In this way, we show our procedure can be used in practice to detect malicious channels and certify undisrupted quantum information, which is a fundamental building block of quantum networks.

Chapter 7 discusses the main results of this thesis, and provides potential new perspectives. We summarize the new key ideas presented in the last chapters, and point out some unsolved challenges which may be overcome in the future.

1.2 Publications

The results from chapter 4 were submitted for publication in the following manuscript:

- [49] *Experimental cheat-sensitive quantum weak coin flipping*,
  with V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti,

The results from chapters 5 and 6 are about to be submitted for publication, in the following manuscript:

- *Experimental Certification of Quantum Transmissions via Bell Theorem*,
  with L. dos Santos Martins, V. Yacoub, P. Lefebvre, I. Šupić, D. Markham, and E. Diamanti.

Some results from chapter 3 are also included in these two manuscripts, although the multipartite source is still under preparation. Results on that source will be presented when it is ready and characterized. In addition, a contribution was made in the following manuscript, which was submitted for publication:

- [50] *Quantum City: a Realistic Metropolitan Quantum Network Architecture*,
  with R. Yehia, E. Diamanti, and I. Kerenidis,

The results in this thesis were also presented as poster talks in international conferences and summer schools such as CEWQO 2019, QLight 2019, and QCMC 2022, and disseminated in nationwide public outreach event *Fête de la Science* and in a scientific radio show from radio station *France Culture*.

'L'homme est également sous le joug de ces lois qu'il feint d'ignorer, se croyant exceptionnel et le fruit d'une opération divine.'

— Edouard Oblak.

CHAPTER 2

PRELIMINARIES

We first introduce the most fundamental concepts this thesis is built upon. First we go through the basic mathematical framework of quantum mechanics and information, including details on quantum entanglement, which is at the heart of this work. Then we give some insight on classical and quantum optics, including nonlinear phenomena that later allow entanglement generation. Finally we introduce some notions linked to quantum cryptography.

2.1 Mathematical Framework

2.1.1 Quantum State

Each isolated quantum system can be associated with a quantum state, which gathers all the properties of the system, and can be used to predict its behaviour. We adopt the *Dirac notation*, such that the quantum state is a vector, or *ket* $|\psi\rangle$ in a Hilbert space $\mathscr{H}$. The *bra* $\langle\psi|$ is the associated element of the dual space $\mathscr{H}^*$ of $\mathscr{H}$, and $\hat{P}_\psi = |\psi\rangle\langle\psi|$ is the projector on state $|\psi\rangle$. The probability of measuring a particle of state $|\psi\rangle$ in a state $|\phi\rangle$ is given by the inner product $\langle .|.\rangle$:

$$\mathbb{P}(\psi \to \phi) = |\langle\phi|\psi\rangle|^2. \tag{2.1}$$

The specific case $\phi = \psi$ imposes any quantum state to be normalized, $\langle\psi|\psi\rangle = 1$. As part of the Hilbert $\mathscr{H}$, the normalized sum of two quantum states is still a quantum state. This is commonly known as the *principle of superposition*.

In our experiments, most systems are not isolated, such that the quantum state does not provide a sufficient description. Often the quantum state is indeed degraded by noise, induced by interactions with a fluctuating environment, or with other quantum systems in the form of entanglement. In such cases, the system is said to be in a *mixed state*, as opposed to a *pure state* described in the beginning of the paragraph, as it displays statistical fluctuations. Therefore, one can only know the statistical probability p_i that the system is in the pure state $|\psi_i\rangle$. With the set $\{(|\psi_i\rangle, p_i\}$, we define the *density operator* of the system:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \text{with } 0 < p_i \leq 1 \text{ and } \sum_i p_i = 1. \tag{2.2}$$

In general, a density operator is a Hermitian, nonnegative and normalized operator from $\mathscr{L}(\mathscr{H})$:

$$\rho \in \mathscr{L}(\mathscr{H}), \quad \rho^\dagger = \rho, \quad \rho \geq 0, \quad \mathrm{Tr}(\rho) = 1. \tag{2.3}$$

The hermiticity allows for the diagonalization of the operator, such that we can choose a set of orthonormal vectors $\{|\psi_i\rangle\}$ in eq. 2.2. Finally, we define the purity $P(\rho)$ of the state:

$$P(\rho) = \mathrm{Tr}(\rho^2) \in]0;1]. \tag{2.4}$$

In particular, $P(\rho) = 1$ when $\rho^2 = \rho = |\psi\rangle\langle\psi|$ such that the system is in a pure state $|\psi\rangle$. In this case we sometimes use the notation $\psi = |\psi\rangle\langle\psi|$.

2.1.2 Quantum Measurements

Projective Measurements - The most intuitive way to grasp measurements in quantum physics is through the consideration of *observables*. These are physical quantities that can be measured on a quantum system, such as the polarization or wavelength of light. An observable $\mathscr{A}$ is represented by a Hermitian operator

$\hat{A} \in \mathscr{L}(\mathscr{H})$, the eigenvalues $\{a_m\}$ of which give the possible outcomes when measuring that observable. Knowing the associated orthogonal projectors $\{\hat{P}_m\}$, one can diagonalize the operator:

$$\hat{A} = \sum_m a_m \hat{P}_m. \tag{2.5}$$

Quantum measurements are inherently probabilistic, the probability of the outcome a_m being given by:

$$\mathbb{P}(a_m|\psi) = \langle\psi|\hat{P}_m|\psi\rangle \text{ for a pure state,} \tag{2.6}$$

$$\mathbb{P}(a_m|\rho) = \mathrm{Tr}(\hat{P}_m\rho) \text{ for a mixed state.} \tag{2.7}$$

The expectation value of observable $\mathscr{A}$ therefore reads:

$$\langle\mathscr{A}\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle \text{ for a pure state,} \tag{2.8}$$

$$\langle\mathscr{A}\rangle_\rho = \mathrm{Tr}(\hat{A}\rho) \text{ for a mixed state.} \tag{2.9}$$

After the measurement, the state is projected onto the corresponding subspace:

$$|\psi\rangle \longrightarrow \frac{\hat{P}_m|\psi\rangle}{\sqrt{\mathbb{P}(a_m|\psi)}} \text{ for a pure state,} \tag{2.10}$$

$$\rho \longrightarrow \frac{\hat{P}_m\rho\hat{P}_m}{\mathbb{P}(a_m|\rho)} \text{ for a mixed state.} \tag{2.11}$$

This last property shows another well-known specificity of quantum measurements, namely the alteration of the quantum state by the observer.

General Measurements - Although projective measurements are the most intuitive way of considering quantum measurement, they do not cover the entirety of possible measurements. Indeed, postulates of quantum mechanics allow for more general measurements, based on arbitrary sets of operators $\{\hat{M}_m\}$ such that

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = \mathbb{1}. \tag{2.12}$$

Such a set is known as a *Positive Operator-Valued Measurement* (POVM). In that case, the different outcomes' probabilities are given by:

$$\mathbb{P}(m|\psi) = \langle\psi|\hat{M}_m^\dagger\hat{M}_m|\psi\rangle \text{ for a pure state,} \tag{2.13}$$

$$\mathbb{P}(m|\rho) = \mathrm{Tr}(\hat{M}_m\rho\hat{M}_m^\dagger) \text{ for a mixed state.} \tag{2.14}$$

Note that in the specific case $(\hat{M}_m^\dagger \hat{M}_m)^2 = \hat{M}_m^\dagger \hat{M}_m$, the measurement is projective. In some practical situation, the observer might be limited to a partial set of outcomes, such that accessible measurement operators $\{\hat{M}_m\}$ only verify

$$\sum_m \hat{M}_m^\dagger \hat{M}_m \leq \mathbb{1}. \tag{2.15}$$

We call such measurement a *partial POVM*. Note that in this case, one can always complete the set $\{\hat{M}_m\}$ with a failure operator:

$$\hat{M}_\varnothing = \sqrt{\mathbb{1} - \sum_m \hat{M}_m^\dagger \hat{M}_m}, \tag{2.16}$$

which is the *no-outcome* measurement operator. This way, the set $\{\hat{M}_m\} \cup \{\hat{M}_\varnothing\}$ forms a full POVM.

2.1.3 The Quantum Bit

Most simple quantum systems are 2-dimensional, and are known as *qubits*. They can be seen as the quantum analogue of the classical bit of information. The qubit Hilbert space $\mathscr{H}$ is generated by 2 orthogonal vectors, $|0\rangle$ and $|1\rangle$, forming the so-called *computational basis*. Common observables are the *Pauli operators*, of eigenvalues ± 1, and their associated eigenstates given in Table 2.1.

Operator	Matrix	Eigenvectors	
		$+1$	-1
$\hat{\sigma}_1$ or $\hat{\sigma}_x$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\lvert+_x\rangle = \frac{1}{\sqrt{2}}(\lvert0\rangle + \lvert1\rangle)$	$\lvert-_x\rangle = \frac{1}{\sqrt{2}}(\lvert0\rangle - \lvert1\rangle)$
$\hat{\sigma}_2$ or $\hat{\sigma}_y$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\lvert+_y\rangle = \frac{1}{\sqrt{2}}(\lvert0\rangle + i\lvert1\rangle)$	$\lvert-_y\rangle = \frac{1}{\sqrt{2}}(\lvert0\rangle - i\lvert1\rangle)$
$\hat{\sigma}_3$ or $\hat{\sigma}_z$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\lvert+_z\rangle = \lvert0\rangle$	$\lvert-_z\rangle = \lvert1\rangle$

Tab. 2.1: Pauli Operators and their eigenstates.

Together with the identity $\mathbb{1}_2 = \hat{\sigma}_0$, these operators form an orthogonal basis of the operators on the qubit space, for the inner product $(A,B) = \mathrm{Tr}(A^\dagger B)$. Therefore, any density operator can be written in the form:

$$\rho = \frac{1}{2}(\mathbb{1}_2 + \mathbf{r}\cdot\vec{\sigma}), \tag{2.17}$$

with $\vec{\sigma} = (\hat{\sigma}_x;\hat{\sigma}_y;\hat{\sigma}_z)$ and $\mathbf{r} = (x;y;z)$ with $\|\mathbf{r}\| \leq 1$. $\mathbf{r}$ is the Bloch vector, in the Bloch sphere (see Figure 2.1).

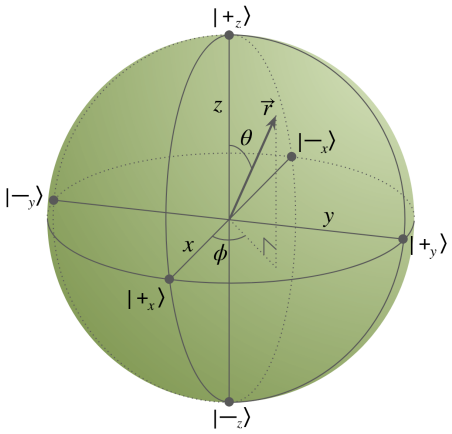


Fig. 2.1: Representation of the state of a qubit in the Bloch sphere.

The coordinates of the Bloch vector are the expectation values of the Pauli operators. This way, the qubit's density operator can easily be evaluated by measuring these expectation values, which is the root of *quantum state tomography* [51, 52]. Note that in case of a pure state $\rho = |\psi\rangle\langle\psi|$, the vector is at the surface of the sphere, and we get:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{2.18}$$

where $(r = 1,\theta,\phi)$ are the spherical coordinates of $\mathbf{r}$.

2.1.4 Quantum Entanglement

Definition - First mentioned by Erwin Schrödinger in 1935 [53], quantum entanglement is a fundamental property of composite quantum systems. Let us consider n quantum systems of Hilbert spaces $\mathscr{H}_1$, $\mathscr{H}_2$, ...,$\mathscr{H}_n$. Then the tensor product of all these spaces is a valid Hilbert space:

$$\mathcal{H} = \bigotimes_{k=1}^{n} \mathcal{H}_k = \left\{ \sum_j \lambda_j |\psi_{1,j}\rangle \otimes |\psi_{2,i}\rangle \otimes ... \otimes |\psi_{n,j}\rangle, \lambda_j \in \mathbb{C}, |\psi_{k,j}\rangle \in \mathcal{H}_k \right\}, \tag{2.19}$$

such that the ensemble of n systems is also a valid quantum system, that we can describe by its quantum state $|\psi\rangle \in \mathcal{H}$. That state is *separable* when it can be written as the tensor product of the states of its subsystems:

$$|\psi\rangle = \bigotimes_{k=1}^{n} |\psi_k\rangle, \quad \text{with } |\psi_k\rangle \in \mathcal{H}_k. \tag{2.20}$$

The subsystems are then independent from one another, and can be described separately. When the overall state $|\psi\rangle$ cannot be written in such a tensor product, the state is *entangled*. In this case, we cannot define the state of a part of the system independently from the other parts. This leads to correlations between parts of the system that cannot be explained classically, even when said parts are separated by large distances.

EPR Paradox and Non-locality - On a fundamental level, the possibility of such entangled states, allowed by quantum theory, was the source of one of the most important scientific debates of the past century. It started with the so-called *EPR paradox* in 1935 [54], as Einstein, Podolsky, and Rosen claimed quantum theory to be incomplete, such that the apparent quantum randomness should in fact arise from deterministic *local hidden variables* (LHV). This claim relied on the assumption that laws of nature should be both *realist* and *local*, meaning that physical quantities should be defined independently of whether they are observed or not, and that a measurement performed on a system should not influence the result of another measurement performed on a remote system. Later work from Bell in 1964 [9], and J. Clauser, M. Horne, A. Shimony and R. Holt (CHSH) in 1969 [55], showed that in a local realist theory the correlations measured by Alice and Bob on two remote particles should always verify the following inequality:

$$\mathcal{I} = \langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_1 \rangle - \langle \hat{A}_0 \hat{B}_1 \rangle \leq 2, \tag{2.21}$$

where $\hat{A}_0, \hat{A}_1$ and $\hat{B}_0, \hat{B}_1$ are observables measured by Alice and Bob, respectively. Yet, this CHSH inequality can be violated by the following 2-qubits entangled state, known as the *singlet* or simply *Bell state*:

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\big) = \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big). \quad (2.22)$$

Here we simply display equivalent notations for bipartite states. If Alice and Bob measure the following observables:

$$\begin{aligned} \hat{A}_0 &= \hat{\sigma}_z, & \hat{B}_0 &= -\frac{1}{\sqrt{2}}(\hat{\sigma}_z + \hat{\sigma}_x), \\ \hat{A}_1 &= \hat{\sigma}_x, & \hat{B}_1 &= \frac{1}{\sqrt{2}}(\hat{\sigma}_z - \hat{\sigma}_x), \end{aligned} \quad (2.23)$$

we indeed expect a maximum violation of CHSH inequality $\mathcal{I} = 2\sqrt{2}$ [56]. The experiment of A. Aspect [31] demonstrated such violation in 1981, therefore refuting the LHV model, and proving the inherent non-locality of quantum theory, in the form of entangled states. Interestingly enough, the violation of Bell inequality is a sufficient (but not necessary) condition for the presence of entanglement. In particular, a maximal violation $\mathcal{I} = 2\sqrt{2}$, with unknown observables $\hat{A}_0$, $\hat{A}_1$, $\hat{B}_0$ and $\hat{B}_1$, can only be achieved by measuring a singlet state, up to local rotations. This is root idea for device-independent cryptography, from which we can certify quantum states with minimal assumptions, and that is the scope of chapter 6. For more details on Bell non-locality, the reader can refer to [57].

Examples of Entangled States - The term *Bell state* generally refers to the whole class of states which are equal to the singlet up to local unitaries. In particular, this includes the four following states, which together form a basis of the 2-qubits Hilbert space:

$$|\Phi_\pm\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle \pm |11\rangle\big), \qquad |\Psi_\pm\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle \pm |10\rangle\big). \quad (2.24)$$

They are the main resource of numerous protocols such as Quantum Teleportation [58] or Ekert's entanglement-based Quantum Key Distribution (QKD) [6]. In this manuscript we also use a generalization of Bell states to d-dimensions systems, also called *qudits*:

$$|\Phi_+^d\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle|k\rangle. \quad (2.25)$$

We can also generalize Bell states to N qubits, as the Greenberger-Horne-Zeilinger (GHZ) state [59, 60]:

$$|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right). \tag{2.26}$$

The latter is at the center of multipartite protocols such as conference key agreement [61] (CKA) or anonymous communications [62], and is the basis of the GHZ paradox which also refutes the EPR theory.

Entanglement and Density Operators - A key feature of entanglement is the impossibility to attribute a well-defined quantum state to a portion of the entangled system. Still, density operators can help us predict the local behaviour of said portion. Let us take the example of a bipartite system of quantum state $|\psi\rangle \in \mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$. Using the *Schmidt decomposition*, one can write $|\psi\rangle$ in the form:

$$|\psi\rangle = \sum_k \lambda_k |\alpha_k\rangle|\beta_k\rangle \tag{2.27}$$

where $\{|\alpha_k\rangle\}$ and $\{|\beta_k\rangle\}$ are orthonormal bases of $\mathscr{H}_A$ and $\mathscr{H}_B$ respectively, and $\lambda_\mathbf{k}$ are positive real coefficients such that $\sum_k \lambda_k^2 = 1$, called *Schmidt coefficients*. Taking $\rho = |\psi\rangle\langle\psi|$, the *reduced density operator* of system A is then defined as

$$\rho_A = \mathrm{Tr}_B(\rho) = \sum_k \langle\beta_k|\rho|\beta_k\rangle = \sum_k \lambda_k^2 |\alpha_k\rangle\langle\alpha_k|, \tag{2.28}$$

where Tr_B is the partial trace on system B. This density operator ρ_A describes the behaviour of system A regardless of system B. Similarly, we can define the reduced density operator of system B, $\rho_B = \mathrm{Tr}_A(\rho)$. The purity of these two operators reads:

$$P(\rho_A) = P(\rho_B) = \sum_k \lambda_k^4 = \frac{1}{K}, \tag{2.29}$$

where $K \geq 1$ is called the *Schmidt rank*. It is maximal when ρ_A and ρ_B are maximally mixed, indicating we cannot define local states for systems A and B: the bipartite system is maximally entangled. Conversely, $K = 1$ when ρ_A and ρ_B are pure, such that the states of A and B are locally defined: the system is fully separable. The Schmidt rank is therefore a a good measure of the amount of entanglement in a bipartite state.

Interestingly enough, any density operator can be interpreted as a reduced density operator, computed from the pure state of a larger entangled system. This is the philosophy of *state purification*, which ensures that for any density operator $\rho \in \mathscr{L}(\mathscr{H}_A)$, there exists a Hilbert space $\mathscr{H}_B$ with $\dim \mathscr{H}_A = \dim \mathscr{H}_B$, and a pure state $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ such that $\rho = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. This shows a close connection between mixed state and entanglement, such that a limited purity in the state of a system can always be attributed to some entanglement with another system. Far from being a simple conceptual curiosity, this idea can have very concrete uses in experiments, particularly when searching for the source of some noise.

2.1.5 Closeness of Quantum States

Different functions can be defined in order to evaluate the closeness of two quantum states, a first common one being the *trace distance*:

$$D(\rho,\sigma) = \frac{1}{2}\mathrm{Tr}\sqrt{(\rho-\sigma)^2} = \frac{1}{2}\mathrm{Tr}\,|\rho-\sigma|. \tag{2.30}$$

It can be characterized as the maximum probability of distinguishing the two states by performing a single measurement:

$$D(\rho,\sigma) = \max_{0\leq\hat{P}\leq\mathbb{1}} \mathrm{Tr}\big(\hat{P}(\rho-\sigma)\big), \tag{2.31}$$

where the maximization can alternatively be restricted to projectors. The trace distance is indeed a distance, as $D(\rho,\sigma) = 0$ implies $\rho = \sigma$, it is symmetric $D(\rho,\sigma) = D(\sigma,\rho)$, and it verifies the triangular inequality

$$D(\rho_1,\rho_2) \leq D(\rho_1,\rho_3) + D(\rho_3,\rho_2). \tag{2.32}$$

Another important function is the Ulhmann *fidelity* [63] between two density operators:

$$F(\rho,\sigma) = \left[\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right]^2. \tag{2.33}$$

The formula is in fact symmetric in ρ and σ. This function was first defined as a generalization of the *transition probability* from one mixed state to another. More precisely, it can be written as the maximum overlap between two purifications of ρ and σ:

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle|^2, \tag{2.34}$$

where the maximization is carried over all purifications $|\psi\rangle$ and $|\phi\rangle$ of ρ and σ respectively (one can alternatively fix the purification of one state and perform the maximization on the other). The fidelity is not a distance, as it measures the *closeness* of states instead of their separation. In particular, it does not verify the triangular inequality, and $F(\rho,\sigma)=1$ when $\rho=\sigma$. Still, one can define metrics from the fidelity, such as the *angle* $A(\rho,\sigma)$ and the *sine distance* $C(\rho,\sigma)$ [64, 65]:

$$A(\rho,\sigma)=\arccos\sqrt{F(\rho,\sigma)}, \qquad C(\rho,\sigma)=\sqrt{1-F(\rho,\sigma)}. \tag{2.35}$$

This way, $A(\rho,\sigma)$ is the angle between two purifications of the states, and $\sqrt{F(\rho,\sigma)}$, $C(\rho,\sigma)$ are the cosine, sine of that angle, respectively. When one of the states is a pure state $\sigma=|\phi\rangle\langle\phi|$, the fidelity simply reads:

$$F(\rho,\sigma)=\langle\phi|\rho|\phi\rangle, \tag{2.36}$$

and when ρ is also pure $\rho=|\psi\rangle\langle\psi|$ we have

$$F(\rho,\sigma)=|\langle\psi|\phi\rangle|^2. \tag{2.37}$$

Finally, these different functions are always ordered as follows:

$$1-\sqrt{F}\leq D\leq C\leq A. \tag{2.38}$$

When one of the state is pure, we get a tighter inequality $1-F\leq D$, and $D=C$ when both states are pure. This gives a characterization for the sine distance:

$$C(\rho,\sigma)=\min_{|\psi\rangle,|\phi\rangle} D(|\psi\rangle,|\phi\rangle), \tag{2.39}$$

where the minimization is carried over all purifications $|\psi\rangle$ and $|\phi\rangle$ of ρ and σ respectively, or once again only over the purifications of one state by fixing a purification of the other one.

The choice of these functions will depend on the context. We generally try to derive results on the fidelity, which can be interpreted as a success probability of our protocols. However, we will often use the trace distance in order to derive interesting results, and then use its proximity with the sine distance in order to generalize these results to the fidelity. The angle distance will be used mostly for deriving a tight triangular inequality.

2.1.6 Quantum Operations

Quantum states can undergo various transformations through their evolution. In most cases, we consider an isolated system, so the transformation is unitary:

$$|\psi\rangle \longrightarrow \hat{U}|\psi\rangle, \qquad \text{with } \hat{U}^\dagger\hat{U} = \hat{U}\hat{U}^\dagger = \mathbb{1}. \tag{2.40}$$

Important unitaries are qubit logic gates, that we provide in Table 2.2. Note the Controlled-NOT is a 2-qubits gate, which allows for the construction of an entangled state from a product state.

Name	Notation	Matrix	Examples
Phase Flip	$\hat{Z}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\hat{Z}\|+_x\rangle = \|-_x\rangle \quad \hat{Z}\|+_y\rangle = \|-_y\rangle$
Bit Flip	$\hat{X}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\hat{X}\|0\rangle = \|1\rangle \quad \hat{X}\|+_y\rangle = \|-_y\rangle$
Bit & Phase Flip	$\hat{Y}$	$i\hat{X}\hat{Z} = i\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$\hat{Y}\|0\rangle = \|1\rangle \quad \hat{Y}\|+_x\rangle = \|-_x\rangle$
Hadamard Gate	$\hat{H}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$\hat{H}\|0\rangle = \|+_x\rangle \quad \hat{H}\|+_x\rangle = \|0\rangle$
Controlled-NOT	$C\hat{X}$	$\begin{bmatrix} \mathbb{1}_2 & 0 \\ 0 & \hat{X} \end{bmatrix}$	$C\hat{X}\|+_x\rangle\|0\rangle = \|\Phi_+\rangle$

Tab. 2.2: Most important logic quantum gates.

An important property of unitaries is the invariance of the closeness functions over their application:

$$M(\hat{U}\rho\hat{U}^\dagger, \hat{U}\sigma\hat{U}^\dagger) = M(\rho,\sigma), \tag{2.41}$$

where M stands for A, C, D, or F. Unitaries can be generalized to transformations between two different Hilbert spaces $\mathscr{H}_A$ and $\mathscr{H}_B$. Such transformations $\Gamma : \mathscr{H}_A \longrightarrow \mathscr{H}_B$, that verify $\Gamma^\dagger\Gamma = \Gamma\Gamma^\dagger = \mathbb{1}$, are called *isometries*, and are of particular use in the context of device-independent protocols, such as those studied in chapter 6. Finally, when the quantum system is not isolated, transformations can involve interactions with other unknown systems, and cannot be described by unitary operators or isometries. In such cases we adopt a more general formalism, using *quantum channels*, that we detail in chapter 5.

2.2 Optics

2.2.1 Classical Linear Optics

Free-space optics - In numerous cases the electromagnetic field can be described as a classical wave, following Maxwell's equations. In this thesis, we only consider non-magnetic dielectric media, in absence of free charges and currents, so the equations read:

$$\begin{aligned} \nabla \times \mathbf{B} &= \mu_0 \frac{\partial \mathbf{D}}{\partial t}, & \nabla \cdot \mathbf{B} &= 0, \\ \nabla \times \mathbf{E} &= -\frac{\partial \mathbf{B}}{\partial t}, & \nabla \cdot \mathbf{D} &= 0, \end{aligned} \tag{2.42}$$

where $\mathbf{E}(\mathbf{r},t)$ is the electric field, $\mathbf{D}(\mathbf{r},t)$ is the electric displacement, and $\mathbf{B}(\mathbf{r},t)$ is the magnetic field. In addition, the medium equation relates $\mathbf{E}(\mathbf{r},t)$ and $\mathbf{D}(\mathbf{r},t)$:

$$\mathbf{D} = \varepsilon_0 \mathbf{E} + \mathbf{P}, \tag{2.43}$$

where $\mathbf{P}(\mathbf{r},t)$ is the dipole-moment density, also called *medium polarization*, which gives the reaction of the medium to the electric field. In free-space we have $\mathbf{P} = 0$, so we derive specific solutions to Maxwell's equations. Monochromatic plane-waves are of the form:

$$\mathbf{E}(\mathbf{r},t) = \mathbf{E}_0 e^{i(\omega t - \mathbf{k}\cdot\mathbf{r})} + \text{conj.}, \tag{2.44}$$

where $\mathbf{E}_0 = (E_{0_x}, E_{0_y}, E_{0_z})$ is the complex amplitude vector, ω is the angular frequency, and $\mathbf{k}$ the wavevector, that verifies

$$\|\mathbf{k}\| = \omega/c, \qquad \text{and} \qquad \mathbf{E}_0 \cdot \mathbf{k} = 0. \tag{2.45}$$

The amplitude vector gives the polarization of the wave $\mathbf{p}_0 = \mathbf{E}_0/\|\mathbf{E}_0\|$. We also define the wavelength in vacuum $\lambda = 2\pi c/\omega$. Such a plane wave does not describe any real physical field, as it would otherwise be infinitely extended in space and time. Still it can be used as a limit case or a mathematical tool, as any physical field can be decomposed in an infinite sum of plane waves by Fourier transform. A more physical solution of Maxwell's equation is the monochromatic Gaussian beam. Considering such beam propagates along z-axis, the expression in the focusing plane $z = 0$ reads

$$\mathbf{E}(x,y,z=0,t) = \mathbf{E}_0 \exp(i\omega t) \exp\left(-\frac{r^2}{w_0^2}\right) + \text{conj.}, \tag{2.46}$$

where $r^2 = x^2 + y^2$, and w_0 is the beam radius, or waist. The general expression of the field in every point of space can be found in [66], but we give here some useful intuition. First we define the *Rayleigh length*:

$$z_R = \pi w_0^2 / \lambda. \tag{2.47}$$

For $|z| < z_R$, the beam can be approximated as a plane wave with $\mathbf{k} = \mathbf{u}_z \omega/c$. We say the beam is *collimated* at the scale of z_R. For $|z| > z_R$, the beam progressively diverges and spreads, with an increasing radius:

$$w(z) = w_0 \sqrt{1 + \left(\frac{z}{z_R}\right)^2}, \tag{2.48}$$

so the beam intensity at any point of space reads:

$$I(x,y,z) \propto \left(\frac{w_0}{w(z)}\right)^2 \exp\left(-\frac{2r^2}{w(z)^2}\right). \tag{2.49}$$

The beam can ultimately be approximated by a spherical wave for $z \gg z_R$. The divergence angle is given by

$$\theta = \arctan \frac{\lambda}{\pi w_0} \simeq \frac{\lambda}{\pi w_0}. \tag{2.50}$$

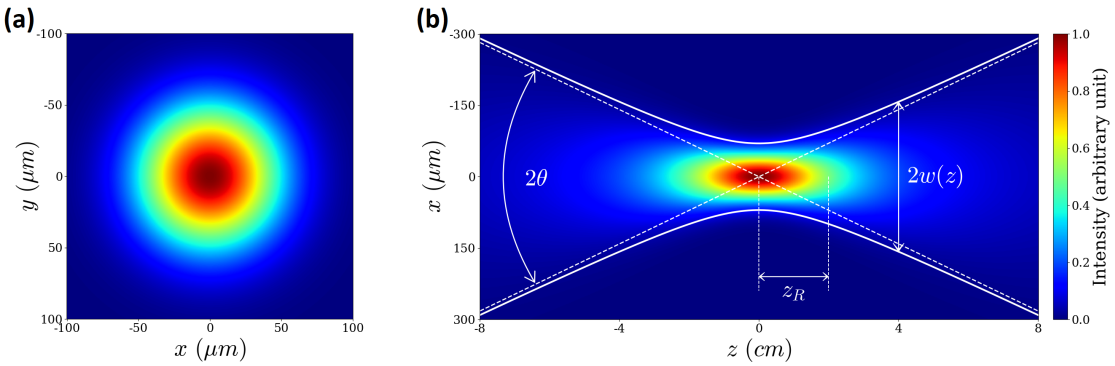


Fig. 2.2: Intensity profile of a Gaussian beam ($w_0 = 70\,\mu$m, $\lambda = 775\,$nm), (a) in the $z = 0$ plane, (b) in the $y = 0$ plane, in which we display the waist $w(z)$, the Rayleigh length z_R and the divergence angle θ.

A typical Gaussian intensity profile is displayed in Fig. 2.2, which also shows its significant characteristics. Beams emitted by a Laser or emerging from a

single-mode optical fiber are typically approximated by Gaussian beams, which therefore cover most beams studied in our experiments. Still some beams have a non-negligible spectral bandwidth, and therefore cannot be approximated with monochromatic beams. In such cases, we again decompose our beam as a sum of monochromatic waves via Fourier transform, which gives the beam's spectrum.

Linear optics in dielectric media - When electromagnetic waves propagate in a dielectric medium, it induces a non-zero dipole-moment density $\mathbf{P}$, that we can decompose into a linear part $\mathbf{P}_L$ and a nonlinear part $\mathbf{P}_{NL}$:

$$\mathbf{P} = \mathbf{P}_L + \mathbf{P}_{NL} = \varepsilon_0(\chi^{(1)}\mathbf{E} + \chi^{(2)}\mathbf{E}^2 + \chi^{(3)}\mathbf{E}^3 + ...), \tag{2.51}$$

where $\chi^{(1)}$ is the linear first order susceptibility, and $\chi^{(n)}$ for $n > 1$ is the n-th order nonlinear susceptibility, which is a tensor of order $n+1$. For low power densities the nonlinear moment density $\mathbf{P}_{NL}$ can be neglected, such that we have

$$\mathbf{D} = \varepsilon_0(1+\chi)\mathbf{E} = \varepsilon_0\varepsilon_r\mathbf{E}, \tag{2.52}$$

where χ is a 3×3 symmetric, real and positive matrix, and ε_r is the relative permittivity of the medium. ε_r can be diagonalized along 3 privileged axes of the medium

$$\varepsilon_r = \begin{bmatrix} n_x^2 & 0 & 0 \\ 0 & n_y^2 & 0 \\ 0 & 0 & n_z^2 \end{bmatrix} \tag{2.53}$$

where n_x, n_y, and n_z are the optical indices the wave experiences when it is polarized along x-, y-, or z-axes respectively. In general, the medium is dispersive, so the optical indices depend on the frequency ω. When $n_x = n_y = n_z = n$, then the medium is *isotropic*: the wave propagates at the same velocity $v = c/n$ no matter its polarization or propagation direction. This is the case for media like air, glass or optical fibers in the absence of stress.

When at least two optical indices among n_x, n_y, and n_z are different, then the medium is called *anisotropic* or *birefringent*. This includes crystals or optical fibers under stress for instance. In that case the calculation of the wave properties is more complicated than in the isotropic case (see [66] for details on that matter).

In this thesis we only consider specific cases, in which the beam propagates along one of the dielectric axes that is normal to the dielectric interface (we choose the (Oz)-axis by convention). Hence a horizontally-polarized wave ($\mathbf{p}_0 = \mathbf{u}_x$) experiences the so-called *ordinary index* $n_x = n_o$, while a vertically-polarized wave ($\mathbf{p}_0 = \mathbf{u}_y$) experiences the *extraordinary index* $n_y = n_e$.

2.2.2 Nonlinear Optics

For relatively high power densities, the nonlinear dipole-moment density $\mathbf{P}_{NL}$ in eq. 2.51 cannot be neglected, which leads to diverse phenomena. The second term in this equation involves the second order susceptibility $\chi^{(2)}$, which is only non-zero in anisotropic materials. It gives rise to processes such as *sum-frequency generation* (SFG, the emission of a field of frequency $\omega_1 = \omega_2 + \omega_3$, from two fields of respective frequencies ω_2 and ω_3), *second-harmonic generation* or frequency doubling (SHG, or SFG with $\omega_2 = \omega_3$, so $\omega_1 = 2\omega_2$), *difference-frequency generation* (DFG, a field of frequency $\omega_3 = \omega_1 - \omega_2$ is emitted from two fields of respective frequencies ω_1 and ω_2), or *optical parametric amplification* (OPA, a field of frequency ω_1 amplifies a field of frequency ω_2, and generates a field of frequency $\omega_3 = \omega_1 - \omega_2$). Most importantly, *spontaneous parametric down-conversion* (SPDC), allowed via a quantum description of the electromagnetic fields, describes the spontaneous conversion of a field of frequency ω_1 into two fields of frequencies ω_2 and ω_3, with $\omega_1 = \omega_2 + \omega_3$. This process can only be interpreted as a transformation of a *photon* of high energy into two photons of lower energies. We introduce this description in the next paragraph.

In crystals of homogeneous susceptibility, also called *bulk crystals*, all these processes occur only when the different fields verify the *energy conservation* and *phase-matching* conditions:

$$\Delta\omega = \omega_2 + \omega_3 - \omega_1 = 0, \quad (2.54) \qquad \Delta\mathbf{k} = \mathbf{k}_3 + \mathbf{k}_2 - \mathbf{k}_1 = 0, \quad (2.55)$$

where $\|\mathbf{k}_j\| = n(\omega_j)\omega_j/c$, and n is the extraordinary or ordinary index which depends on the field's frequency and polarization. We distinguish two types of phase-matching depending on the fields' polarizations:

- Type-I phase-matching: the two fields with lower frequencies have the same polarization, that is orthogonal to the third field's polarization
- Type-II phase-matching: the two fields with lower frequencies have orthogonal polarizations, one of which is parallel to the third field's polarization.

The phase-matching condition ensures that the different fields are in phase all throughout the propagation, so that all the waves generated at different points of the crystal add up in a constructive interference. If this condition is not fulfilled, then a destructive interference occurs at the scale of the crystal, and the new field cannot emerge. A priori, one has to choose specific orientations of the crystal in order to fulfill that condition at specific wavelengths. This limits the choices of parameters for our experiments, which is why we generally prefer *periodically-poled* crystals [67–69]. The nonlinear susceptibility of such crystals periodically changes sign (see Fig. 2.3):

$$\chi^{(2)}_{PP} = \chi^{(2)}\mathrm{sgn}\left[\cos\left(\tfrac{2\pi}{\Lambda}z\right)\right], \qquad (2.56)$$

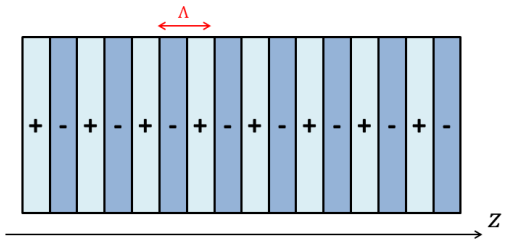


Fig. 2.3: Sketch of a periodically-poled crystal. The sign of $\chi^{(2)}$ changes periodically.

where Λ is the poling period which, if chosen carefully, allows to correct the potential phase mismatch. This results in the *quasi-phase-matching condition* (QPM):

$$\Delta\mathbf{k}' = \mathbf{k}_3 + \mathbf{k}_2 - \mathbf{k}_1 + \frac{2\pi}{\Lambda}\mathbf{u}_z = 0. \qquad (2.57)$$

In this case, an additional phase-matching type is possible:

- Type-0 phase-matching: the three fields have the same polarization.

Thanks to periodic-poling, one can choose the nonlinear material and its orientation to promote a high nonlinear interaction at the desired wavelengths, and choose the

appropriate poling period Λ to enforce the phase-matching. In general, we choose the crystal's orientation such that the propagation axis (Oz) coincides with one of the crystal's axes in eq. 2.53.

The second term in eq. 2.51 involves the third order susceptibility $\chi^{(3)}$. The resulting phenomena are generally undesired in this thesis, as are those induced by higher terms $\chi^{(k)}$ for $k \geq 3$. This includes the Kerr-effect for instance [70, 71], in which the field effectively experiences an intensity-dependent optical index $n(I) = n_0 + n_2 I$, where I is the power density or intensity. This leads to self-phase modulation, which degrades the beam's spectrum, or self-focusing, which can increase the beam's intensity up to the local ionization of the material. All materials display a non-zero $\chi^{(3)}$, so that we have to limit the field's power density in order to minimize such undesired phenomena.

2.2.3 Quantum Optics

In previous paragraphs, we have followed a classical-wave description of the electromagnetic field. However, only a quantum description can encompass all phenomena linked to this field, such as the black-body radiation [72], the photoelectric effect [73], or spontaneous parametric down-conversion (SPDC) [74, 75], which is at the heart of this thesis. In this *quantized* description, the field energy cannot increase in a continuous way, but only with finite energy increments. These so-called *photons* can be seen as finite excitations of the field, in specific modes that are defined by the field's properties (polarization, wavelength, spatial profile...) in said modes [76]. The addition or subtraction of such an excitation in a mode ν is mathematically described by the corresponding *creation operator* $\hat{a}_\nu^\dagger$ and *annihilation operator* $\hat{a}_\nu$ respectively. We define the photon number states $\{|n_\nu\rangle\}_{n_\nu \in \mathbb{N}}$ also known as *Fock states* (we omit the ν subscripts in the following), as the eigenstates of the field's Hamiltonian (or energy observable) in free space:

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger \hat{a} + \frac{1}{2}\right) = \hbar\omega\left(\hat{N} + \frac{1}{2}\right), \tag{2.58}$$

where ω is the mode's angular frequency. Using these Fock states we explicit the action of the creation and annihilation operators:

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle, \tag{2.59}$$

$$\hat{a}|n\rangle = \sqrt{n}\,|n-1\rangle, \tag{2.60}$$

and $\hat{N}$ is the photon-number observable, with $\hat{N}|n\rangle = n|n\rangle$. This way the energy of a Fock state can only take values which are half-integer multiples of $\hbar\omega$:

$$\hat{H}|n\rangle = \hbar\omega\Big(n + \frac{1}{2}\Big)|n\rangle. \tag{2.61}$$

Interestingly, the no-photon state $|0\rangle$, also known as *vacuum* state, still has a non-zero energy $\hbar\omega/2$. Different superpositions of Fock states give rise to various photonic statistics, such as the coherent state:

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{+\infty}\frac{\alpha^n}{n!}\hat{a}^{\dagger n}|0\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{+\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{2.62}$$

where $|\alpha|^2 = \mu$ is the average number of photons. Such a state displays poissonian photonic statistics

$$P(n) = |\langle n|\alpha\rangle|^2 = e^{-|\mu|^2}\frac{\mu^n}{n!}. \tag{2.63}$$

It is typical of the field emitted by a Laser. Another typical photon state is the (mixed) thermal state:

$$\rho = \sum_{n=0}^{+\infty}\frac{\mu^n}{(1+\mu)^{n+1}}|n\rangle\langle n| \tag{2.64}$$

where μ is the average number of photons, which gives geometric statistics $P(n) = \frac{1}{1+\mu}\Big(\frac{\mu}{1+\mu}\Big)^n$.

Photonic qubit - In this thesis, we use the photon's polarization degree of freedom in order to encode a qubit. Such a photonic qubit can easily be manipulated, measured and transmitted, making it one of the best platforms for implementing quantum protocols. First we define the horizontal and vertical polarizations:

$$|H\rangle = \hat{a}_H^\dagger|0_H, 0_V\rangle = |1_H, 0_V\rangle \equiv |+_z\rangle, \tag{2.65}$$

$$|V\rangle = \hat{a}_V^\dagger|0_H, 0_V\rangle = |0_H, 1_V\rangle \equiv |-_z\rangle, \tag{2.66}$$

where the H and V subscripts stand for modes that are identical except for the polarization that is either directed along the (Ox)- or the (Oy)-axis. These two orthogonal modes form the qubit computational basis. We also define the diagonal and anti-diagonal polarizations, which form the *diagonal basis*:

$$|+_x\rangle \equiv |D\rangle = \frac{1}{\sqrt{2}}\big(|H\rangle + |V\rangle\big), \quad (2.67) \qquad |-_x\rangle \equiv |A\rangle = \frac{1}{\sqrt{2}}\big(|H\rangle - |V\rangle\big), \quad (2.68)$$

as well as the left and right circular polarizations, which form the *circular basis*:

$$|+_y\rangle \equiv |L\rangle = \frac{1}{\sqrt{2}}\big(|H\rangle + i|V\rangle\big), \quad (2.69) \qquad |-_y\rangle \equiv |R\rangle = \frac{1}{\sqrt{2}}\big(|H\rangle - i|V\rangle\big). \quad (2.70)$$

Finally, we define the photonic Bell states of polarization:

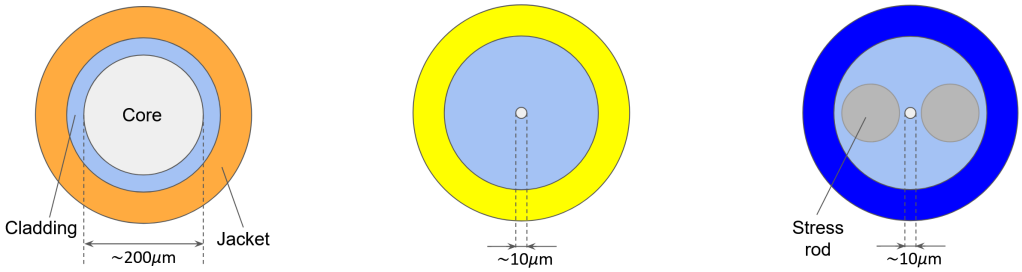
$$\begin{aligned} |\Phi_\pm\rangle &= \frac{1}{\sqrt{2}}\big(|H_A H_B\rangle \pm |V_A V_B\rangle\big) & |\Psi_\pm\rangle &= \frac{1}{\sqrt{2}}\big(|H_A V_B\rangle \pm |V_A H_B\rangle\big) \\ &= \frac{1}{\sqrt{2}}\big(\hat{a}_H^\dagger \hat{b}_H^\dagger \pm \hat{a}_V^\dagger \hat{b}_V^\dagger\big)|0\rangle, & &= \frac{1}{\sqrt{2}}\big(\hat{a}_H^\dagger \hat{b}_V^\dagger \pm \hat{a}_V^\dagger \hat{b}_H^\dagger\big)|0\rangle, \end{aligned} \quad (2.71)$$

with $\hat{a}_H^\dagger, \hat{a}_V^\dagger$ the creation operators associated with the first photon and $\hat{b}_H^\dagger, \hat{b}_V^\dagger$ those of the second photon. Generating such states is the main focus of chapter 3. Another encoding of qubits can also be adopted, by taking the vacuum state $|0_m\rangle$ and single-excitation state $|1_m\rangle = \hat{a}_m^\dagger|0_m\rangle$, in a mode m, as the computational basis. We use this encoding in chapter 4.

2.2.4 Common Optical Components

Optical fibers - Optical fibers are particularly convenient for quantum communications, as they allow to carry photons over large distances, with relatively low losses (0.2 dB/km for telecom wavelengths ≈ 1550 nm). Such fibers are composed of a silica-core, surrounded by a fluorine-doped-silica-cladding of lower optical index [77]. The fiber therefore acts as a wave-guide, carrying the field from one end to the other. In this work we mostly use *single-mode* (SM) fibers, with a $\approx 10\,\mu$m-diameter, optimized for telecom wavelengths. Such fibers also act as a spatial filter,

projecting the coupled mode on a close-to-Gaussian spatial mode, which is conserved over the propagation. Birefringence can be locally induced by stress in the fiber, which can be intentional when using so-called polarization-controllers (PC), or unintentional when casually bending the fiber. The resulting polarization rotation may be undesired in some applications. For this reason, SM fibers can be modified with two stress-rods on opposite sides of the core, which fixes the birefringence-axes along the propagation. This way, light that is polarized along one of these axes does not experience polarization rotation. Such *polarization-maintaining* (PM) fibers are useful for applications which **do not** involve polarization manipulation. In our experiments, these should therefore be avoided, as birefringence over long distances causes decoherence in photons' polarization, which destroys our quantum states. Such fibers can be distinguished by the color of their protective jacket, or by checking the normal cut with a fiberscope (see Fig. 2.4).



(a) Multi-mode fiber, with typical orange jacket and relatively large core.

(b) Single-mode fiber, with typical yellow jacket and relatively small core.

(c) Polarization-maintaining fiber, with blue jacket, small core and stress rods.

Fig. 2.4: Schematic normal cut of different optical fibers used in our experiments, with their typical protective jacket (not-to-scale).

We also use multi-mode (MM) fibers in rare cases, when the spatial mode is not a concern. Their core can take various sizes (typically $\approx 200\,\mu$m), in order to couple more light than SM fibers. Consequently MM fibers are generally less lossy than SM fibers, but cannot be used as spatial filters.

Wave-plates **-** These are made of a birefringent crystal, so that light polarized along one axis of the crystal, called *fast axis*, propagates with an optical index n_f, and light polarized along the orthogonal axis, called *slow axis* propagates with an index

$n_s > n_f$. The behaviour of any polarization can be deduced by linearity. Because n_s and n_f are different, a phase shift is introduced between the polarizations along the two axes. This way, if the slow axis is horizontal ($\theta = 0°$), one can write the transformation matrix of the wave plate, in the $|H\rangle, |V\rangle$-basis:

$$\hat{S}(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{bmatrix}, \tag{2.72}$$

where $\phi = 2\pi \frac{(n_s - n_f)}{\lambda} d$, d is the thickness of the wave plate, and λ is the wavelength of the field. The transformation of the wave plate for any value of θ reads:

$$\hat{W}(\theta, \phi) = \hat{R}(\theta)\hat{S}(\phi)\hat{R}(-\theta), \tag{2.73}$$

where $\hat{R}(\theta)$ is the rotation of angle θ (see Fig. 2.5). The cases $\phi = \pi$ and $\phi = \frac{\pi}{2}$ are called respectively *Half-wave plates* (HWP) and *Quarter-wave plates* (QWP), with the following matrix representations:

$$\hat{H}(\theta) = \hat{W}(\theta, \pi) = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix},$$

$$\hat{Q}(\theta) = \hat{W}(\theta, \frac{\pi}{2}) = \tag{2.74}$$

$$\begin{bmatrix} \cos^2\theta - i\sin^2\theta & (1+i)\cos\theta\sin\theta \\ (1+i)\cos\theta\sin\theta & \sin^2\theta - i\cos^2\theta \end{bmatrix}.$$

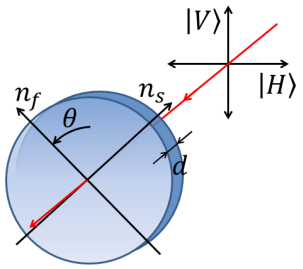


Fig. 2.5: Axes of a wave plate, relatively to $|H\rangle$ and $|V\rangle$ axes. The fast and slow axes are labeled by n_f and n_s respectively.

Each one-qubit logic gates from Tab. 2.2 can be applied to the polarization state of a single-photon, by using a single HWP or QWP at the proper angle. Moreover, any one-qubit unitary can be implemented by using three WPs in a row, a QWP, followed by a HWP, and another QWP. Finally, one can also use WPs at $\theta = 0°$ to change the phase between $|H\rangle$ and $|V\rangle$. To do so, one tilts the WP around its vertical axis, which increases the thickness d of the crystal the photon goes through, therefore changing the phase in equation (2.72). When used that way, the WP is referred to as a *phase plate*.

Beam Splitters - A *beam splitter* (BS) is an optical component that transmits a photon with probability t, and reflects it with probability r, with $r+t=1$. We often consider the case $t=r=0.5$, which gives a $50:50$ beam splitter. They can be made of a semi-reflective plate, of two prism glued together as a cube, or as a fibered component. The general transformation can be expressed using two input spatial modes $\hat{a}^\dagger$ and $\hat{b}^\dagger$, with output modes $\hat{c}^\dagger$ and $\hat{d}^\dagger$ (see Fig. 2.6):

$$\begin{bmatrix} \hat{a}^\dagger \\ \hat{b}^\dagger \end{bmatrix} \longrightarrow \begin{bmatrix} \sqrt{t} & \sqrt{r} \\ -\sqrt{r} & \sqrt{t} \end{bmatrix} \cdot \begin{bmatrix} \hat{c}^\dagger \\ \hat{d}^\dagger \end{bmatrix}. \quad (2.75)$$

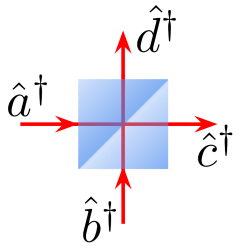


Fig. 2.6: Spatial modes in the BS transformation

Polarizing beam splitters (PBS) ideally reflect the entirety of vertically-polarized light, and transmit the horizontally-polarized light. To express the transformation of such a PBS, we also consider the polarization-mode when writing the creation operators, as shown in Figure 2.7. This way, the transformation reads:

$$\begin{bmatrix} \hat{a}_H^\dagger \\ \hat{b}_H^\dagger \\ \hat{a}_V^\dagger \\ \hat{b}_V^\dagger \end{bmatrix} \longrightarrow \begin{bmatrix} \mathbb{1}_2 & 0 \\ 0 & \hat{X}\hat{Z} \end{bmatrix} \cdot \begin{bmatrix} \hat{c}_H^\dagger \\ \hat{d}_H^\dagger \\ \hat{c}_V^\dagger \\ \hat{d}_V^\dagger \end{bmatrix}. \quad (2.76)$$

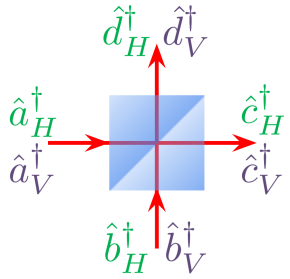
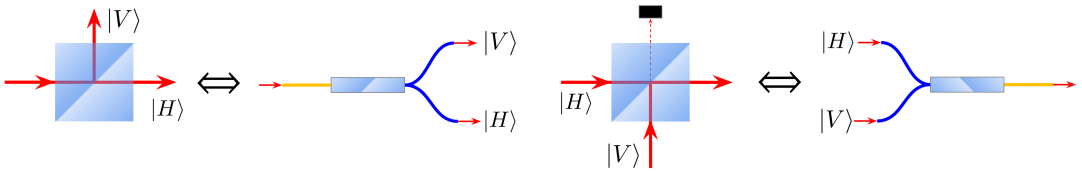


Fig. 2.7: Spatial and polarization modes in the PBS transformation

The PBS effectively entangles spatial and polarization modes of the photon, which is the first step to polarization measurement. When the polarization is an unused degree of freedom, one can use a PBS and some waveplates in order to implement a tunable BS. Fibered PBS can also be used, but generally give access to three modes only, the fourth being discarded, as shown in Fig. 2.8.

Finally, beam splitters can also be wavelength-dependent, transmitting light below a certain wavelength, and reflecting the rest (or the other way round). Such beam splitters are called *dichroic mirrors* (DM), and are generally used as spectral filters.



(a) Beam splitter configuration **(b)** Beam combiner configuration

Fig. 2.8: Fibered PBS and the equivalent configuration with a free-space cube PBS. Two ends are each dedicated to one polarization $|H\rangle$ or $|V\rangle$. The corresponding fibers are generally PM (in blue). The other end can carry any polarization, either combined from the other two ends (b), or split into those ends (a). In our experiments, the corresponding fiber is SM (in yellow).

2.2.5 Optical Interference

In its classical description, the EM field is described as a wave verifying the Maxwell equations (2.42). Thus when two EM waves hit the same point, an interference phenomenon can occur. Here we take a simple example of a plane and monochromatic wave in a Mach-Zehnder interferometer [78, 79], sketched in Fig. 2.9. The wave enters a first BS, giving two beams of same angular frequency ω, propagating with different phase retardance φ_1 and φ_2:

$$E_1(t) = \frac{E_0}{\sqrt{2}}\cos(\omega t + \varphi_1), \quad \text{and} \quad E_2(t) = \frac{E_0}{\sqrt{2}}\cos(\omega t + \varphi_2), \tag{2.77}$$

with E_0 the amplitude of the input beam. The beams are then recombined in a second BS. The average power on the two outputs of the interferometer reads

$$P_1(\Delta\varphi) \propto \frac{E_0^2}{2}\big(1+\cos(\Delta\varphi)\big), \quad \text{and} \quad P_2(\Delta\varphi) \propto \frac{E_0^2}{2}\big(1-\cos(\Delta\varphi)\big), \tag{2.78}$$

with $\Delta\varphi = \varphi_2 - \varphi_1$. This way $P_1 = E_0^2/2$ is maximal and $P_2 = 0$ for $\Delta\varphi = 0$, such that the second output is extinguished. Conversely, $P_1 = 0$ and $P_2 = E_0^2/2$ when $\Delta\varphi = \pi$.

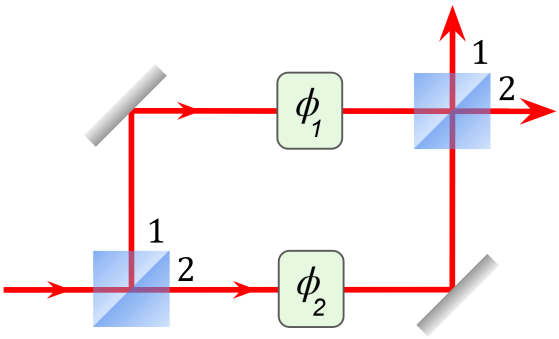


Fig. 2.9: Sketch of a Mach-Zehnder interferometer. A beam is separated in two paths, which are recombined after undergoing a phase retardance.

In real-world situations, different factors may degrade the interference, such that no phase difference $\Delta\varphi$ can extinguish either of the sides. These factors may include phase noise, imperfect alignment, or Laser pulses with limited size hitting the BS at different times. In practice the fields take the expressions

$$P_1(\Delta\varphi) \propto \frac{E_0^2}{2}\big(1 + v\cdot\cos(\Delta\varphi)\big), \text{ and } P_2(\Delta\varphi) \propto \frac{E_0^2}{2}\big(1 - v\cdot\cos(\Delta\varphi)\big), \tag{2.79}$$

with $0 \leq v \leq 1$ is called the interference *visibility*. In experiment we measure that visibility with the following formula:

$$v = \frac{P_1(0) - P_1(\pi)}{P_1(0) + P_1(\pi)} = \frac{P_2(\pi) - P_2(0)}{P_2(\pi) + P_2(0)}. \tag{2.80}$$

In general, we tend to maximize this visibility by isolating our optical setup from noise, and paying particular attention to the alignment and timing of the pulses on the BS. For the latter factor, we carefully minimize the path difference Δl, such that $\Delta l \ll l_c$, with l_c the *coherence length* of pulses, which is simply the spatial extension of said pulses.

Interference of the EM field can also be predicted in the quantum formalism. In that case two modes of a same single-photon may interfere together, so the interference pattern described in equations (2.79) now applies to the probability of the photon to go out of the BS on one side or the other. We grasp this intuition we the following transformation of the photon modes:

$$|1\rangle \xrightarrow{\text{1st BS}} \frac{e^{i\varphi_1}}{\sqrt{2}}|1_1, 0_2\rangle + \frac{e^{i\varphi_2}}{\sqrt{2}}|0_1, 1_2\rangle \xrightarrow{\text{2nd BS}} \cos\big(\tfrac{\Delta\varphi}{2}\big)|1_1, 0_2\rangle + \sin\big(\tfrac{\Delta\varphi}{2}\big)|0_1, 1_2\rangle. \tag{2.81}$$

From the last state we get the expressions (2.79), for detection probabilities of the photon. Such single-photon interference is at the heart of chapter 4, in order to ensure cheat-sensitivity in our weak coin-flipping protocol.

In that last case we emphasized, the photon displays a wave-like behaviour, which can still be predicted via a classical description of the field. Still, photons can display purely quantum behaviour, when performing two-photons interference, also-called Hong-Ou-Mandel (HOM) interference [80]. Here two single-photons hit a BS, and systematically output the BS on the same side as long as they are indistinguishable (see Fig. 2.10). This photon-bunching results in the state

$$|HOM\rangle = \frac{1}{\sqrt{2}}(|2_1, 0_2\rangle + |0_1, 2_2\rangle). \tag{2.82}$$

Interestingly, this interference is not phase-sensitive. Still a significant hardness lies in making the two photons indistinguishable. We tackle this aspect in the end of chapter 3, when detailing our plans to build a multi-photon source.

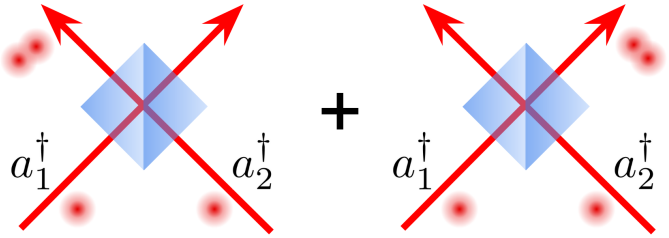
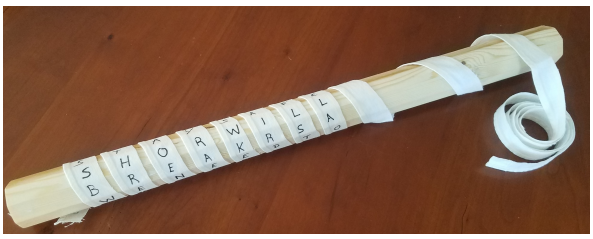


Fig. 2.10: Sketch of the Hong-Ou-Mandel interference. Indistinguishable photons hitting a BS at the same time bunch on one side of the BS or the other.

2.3 Quantum Cryptography

2.3.1 From Classical to Quantum Cryptography

Cryptography is the ensemble of knowledge and techniques one can use in order to secure, conceal, degrade or unveil information. Although encryption and decryption of information are often associated with futuristic technologies in modern fictional representations, such techniques are actually as old as human civilization. They have often relied on simple nonetheless smart ideas, such as the antique Spartan *scytale* device (see Fig. 2.11a), or Caesar's cipher [81]. The birth of modern cryptology can be dated back to the early 1930's, with the breaking of German ENIGMA machine (see Fig. 2.11b) by Polish mathematician Marian Rejewski and his team, later attributed to British mathematician Alan Turing and his team for their invention of the first digital computer. From then on, modern ciphers have relied on more and more sophisticated techniques, in order to catch up with rapidly increasing computational power.



(a) A home-made scytale, ancient Spartan device used around 400 BC. One simply rolls a strip of parchment around a wooden stick of specific shape, an write lengthwise. The message is then scrambled when unrolling the strip.

(b) The Enigma machine, used by Germans during WWII, displayed at Museo Nazionale Scienza e Tecnologia Leonardo da Vinci, Milan, Italy. Source: Wikipedia.

Fig. 2.11: Example of pre-modern encryption-decryption devices, both used for military applications.

Nowadays most encryption methods have built their security on *computational hardness assumptions*, meaning they rely on complex problems which are assumed unsolvable in polynomial time by classical computers. This is the case of the RSA protocol in particular, mentioned in the introduction [1]. However, the ongoing

race for the quantum computer [82] has since questioned the reliability of such classical algorithms, as powerful quantum attacks such as Shor's algorithm [4] are assumed impossible under computational assumptions. For the past decades, this has largely motivated investigations on new qubit-based algorithms and protocols, also known as *quantum cryptography*. Post-quantum cryptography has also provided candidates for classical algorithms which would be resistant to quantum attacks (see [83] for a review on the matter).

First quantum encryption protocols, which were actually proposed a decade before Shor's algorithm, were S. Wiesner's unforgeable quantum money [84], and C. Bennett and G. Brassard's quantum key distribution (QKD), also called BB84 protocol [5]. The latter allows Alice and Bob to generate and share a private random key, that they can use later as a one-time pad to encrypt their messages with optimal security [7, 8]. In order to generate that key, Alice sends a random sequence of bits to Bob, encoded on single-photons' polarization taken in random rectilinear and diagonal bases. Bob then measures each photon in another random basis, chosen again between rectilinear and diagonal. Both Alice and Bob then publicly announce their basis choices, and discard all outcomes for which said bases did not match. The resulting shared bit string forms the encryption key. The power of this method resides in the impossibility for a potential eavesdropper to copy the photonic qubits, thanks to the no-cloning theorem [10, 11]. Moreover, any attempt of said eavesdropper to measure the qubits will fatally degrade the states, which Alice and Bob can detect by simply comparing portions of their bit strings, and checking for differences. The encryption key is therefore secured by unbreakable laws of quantum physics, instead of computational assumptions.

Since then the QKD research area has been the focus of growing interest, leading to several long-distance on-ground experimental implementation of the BB84 protocol [32–35], and the encryption of an intercontinental video-conference between Graz and Hefei thanks to a satellite-relay [85]. In parallel, the alternative entanglement-based QKD of A. Ekert [6] was demonstrated in numerous experimental implementations [86–90], using polarization-entangled photon pairs. Moreover, other quantum protocols were developed in order to perform new cryp-

tographic tasks, with corresponding experimental demonstrations. These include secret sharing [12–14, 39], bit commitment [15], conference key agreement (the multipartite version of QKD) [16, 40, 41], or implementations of Wiesner's unforgeable quantum money [36–38]. In chapter 4 we focus on one of such primitives, known as *quantum weak coin flipping* [20, 91].

2.3.2 Quantum Cryptography and Adversary Scenarios

When studying cryptography protocols, one can put more or less trust in the different parties involved and devices used. We expect such protocols to be used in so-called *adversary scenarios*, in which players, devices or outside parties might deviate from the protocol's recipe in order to disrupt the outcome or gain information. This way, a strong security comes by making as few assumptions as possible. In the following, we define a few important notions that allow us to clarify our protocols' scenarios and the assumptions made.

Assumptions on players - A player is *honest* when it does not try to deviate from the protocol's recipe. On the contrary, a *dishonest* or *malicious* player might attempt to disrupt the protocol by different strategies. Such strategies might involve lying on a measurement result, preparing different states than those expected, disrupting the behavior of a device, or gaining some information using powerful measurements and quantum memories. Such a player might be involved in the original protocol recipe, or be an outside party trying to attack the protocol.

Assumptions on devices - Devices in a protocol may include sources of quantum states, operations, classical and quantum channels, and measurement apparatuses. A device is *trusted* when it follows a behavior that is predicted by the honest players. Such a device can be *ideal* when it has the optimal expected behavior, or *noisy* when its behavior is imperfect but can still be characterized to a certain extent. On the contrary, an *untrusted* device does not follow the predictions of honest players, and might be used by malicious players to disrupt the protocol.

Protocol Robustness - A protocol can be more or less robust to imperfect devices and attacks from dishonest players. We distinguish three significant cases. A *noise-tolerant* or *fault-tolerant* protocol can operate even if some of the devices are noisy. In such cases it is essential to estimate the influence of noise on the protocol's outcomes and performances. A *cheat-sensitive* protocol allows honest players to detect, and eventually sanction malicious players. Finally a *device-independent* protocol operates regardless of the devices' internal function. In that case, the measurements apparatuses, operations and channels are treated as potentially untrusted black boxes, and no assumption is made on the quantum states, which are therefore taken in an unkwown and arbitrarily large Hilbert space. If only parts of the devices are treated as black boxes, then the protocol is *semi device-independent*. Device-independent protocols are particularly secure in adversary scenarios, as their security relies on very few assumptions on the systems involved. This feature is specific to quantum cryptography, as allowed only by Bell non-locality.

Different kind of protocols are detailed in this thesis. We put a particular emphasis on the cheat-sensitivity of our weak coin-flipping implementation (see chapter 4) and the device-independence of our quantum channel certification protocol (see chapter 6). Both of these robustness properties are ensured by quantum phenomena, namely superposition and entanglement.

'Un scientifique dans son laboratoire est un enfant placé devant des phénomènes naturels qui l'impressionnent comme des contes de fées.'

— Marie Skłodowska-Curie.

CHAPTER 3

SOURCE OF ENTANGLED-PHOTON PAIRS

In the context of the potential near-future development of a world-wide quantum network, the design of entangled- and single-photons sources has risen significant interest in the past decades, in order to meet the needs for complex communication and cryptography tasks. Photons have been promising candidates for the implementation of such tasks, thanks to their relative ease of manipulation and transmission over large distances with limited decoherence and losses. Still, the generation of photonic quantum states remains a relatively open and active research area, as protocols often require more and more demanding features, such as on-demand state generation, high detection rates or photonic purity, all the while maintaining a high quality of the states. Sources based on spontaneous parametric down-conversion (SPDC) have been some of the most investigated solutions, as they can be used to generate pairs of close-to-maximally entangled qubits [42], encoded in photons' polarization, probabilistic but heralded single-photons [43, 44], and multipartite entangled states [46, 47]. All of these aspects motivate our choice to build such a SPDC-based source.

In the following, we start by recalling some basic notions on SPDC, and reviewing the most important SPDC-based sources of polarization-entangled photons. We then detail the design of the source that was built from scratch during this thesis,

specifically for the implementation of quantum network protocols and multi-qubits states generation. Because of those applications, the source needs to follow certain requirements. First, it should provide photon pairs around telecom wavelengths, between 1.5 µm and 1.6 µm, where optical fibers are the least lossy. Then it should be able to produce close-to-maximally entangled photons, with $> 99\%$ fidelity to Bell states. In addition, we should have the possibility to use it as a heralded single-photon source. Finally, the source should be adaptable for multi-qubits states emission. In this chapter we provide a full characterization of our source, as well as some perspectives to adapt it to multipartite-states emission, showing it indeed meets those requirements.

3.1 Prerequisite: Photon-Pair Generation

In paragraph 2.2.2 we mentioned photon pairs could be generated via SPDC in a nonlinear crystal. In the following we give more details on this phenomenon, which is at the heart of most of nowadays' entangled-photons sources, including ours. SPDC is the probabilistic conversion of a high-energy photon into two photons of lower energy. One can interpret this process as the reverse of classical sum frequency generation, or as optical parametric amplification of vacuum fluctuations. The prediction of this phenomenon comes by deriving the interaction Hamiltonian in the crystal. For that purpose, we write the energy of interaction per volume unit:

$$h_I \propto \mathbf{E}^{(+)}(\mathbf{r},t)\cdot\mathbf{P}^{(-)}(\mathbf{r},t) + \text{conj.}, \tag{3.1}$$

where $\mathbf{E}^{(+)}$ is the complex electric field, and $\mathbf{P}^{(-)} = \left(\mathbf{P}^{(+)}\right)^*$ is the complex dipole-moment density in the crystal. Only the second order dipole-moment is relevant here, such that

$$h_I \propto \mathbf{E}^{(+)}(\mathbf{r},t)\cdot\chi^{(2)}(\mathbf{r})\mathbf{E}^{(-)^2}(\mathbf{r},t) + \text{conj.}, \tag{3.2}$$

where $\mathbf{E}^{(-)} = \left(\mathbf{E}^{(+)}\right)^*$. We decompose the electric field into three interacting fields:

$$\mathbf{E}^{(+)} = \mathbf{E}_p^{(+)} + \mathbf{E}_s^{(+)} + \mathbf{E}_i^{(+)}, \tag{3.3}$$

where $\mathbf{E}_p^{(+)}$, $\mathbf{E}_s^{(+)}$ and $\mathbf{E}_i^{(+)}$ are the *pump*, *signal* and *idler* fields, respectively. As a first approximation we only consider monochromatic plane waves, of angular

frequencies $\{\omega_l\}_{l=p,s,i}$, wavevectors $\{\mathbf{k}_l\}_{l=p,s,i}$, and polarization $\{\mathbf{e}_l\}_{l=p,s,i}$ (the reader can refer to [92, 93] for a more general derivation). We then express the quantified electric field operators:

$$\hat{\mathbf{E}}_p^{(+)}(\mathbf{r},t) \propto \mathbf{e}_p e^{\omega_p t - \mathbf{k}_p \cdot \mathbf{r}} \hat{a}_p^\dagger, \tag{3.4}$$

$$\hat{\mathbf{E}}_s^{(+)}(\mathbf{r},t) \propto \mathbf{e}_s e^{\omega_s t - \mathbf{k}_s \cdot \mathbf{r}} \hat{a}_s^\dagger, \tag{3.5}$$

$$\hat{\mathbf{E}}_i^{(+)}(\mathbf{r},t) \propto \mathbf{e}_i e^{\omega_i t - \mathbf{k}_i \cdot \mathbf{r}} \hat{a}_i^\dagger, \tag{3.6}$$

where $\hat{a}_p^\dagger$, $\hat{a}_s^\dagger$ and $\hat{a}_i^\dagger$ are the creation operators in the pump, signal and idler modes, respectively. Thus we deduce the Hamiltonian of interaction, by injecting these operators in eq. 3.2 and by integrating over the volume $\mathcal{V}$ of the crystal:

$$\hat{H}_I \propto \int_{\mathcal{V}} \eta(\mathbf{r}) e^{i(\mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i)\cdot\mathbf{r}} d^3\mathbf{r} \cdot \hat{a}_p^\dagger \hat{a}_s \hat{a}_i \quad + \int_{\mathcal{V}} \eta^*(\mathbf{r}) e^{-i(\mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i)\cdot\mathbf{r}} d^3\mathbf{r} \cdot \hat{a}_p \hat{a}_s^\dagger \hat{a}_i^\dagger, \tag{3.7}$$

where $\eta(\mathbf{r}) = \mathbf{e}_p \cdot \chi^{(2)}(\mathbf{r}) \mathbf{e}_s \mathbf{e}_i$, and we only keep the terms which respect the energy conservation principle $\omega_p = \omega_i + \omega_s$. The first term describes the SFG and SHG which were mentioned earlier, while the second term is linked to DFG and OPA. This way all classical phenomena described in paragraph 2.2.2 can be interpreted through photon transformations (see Fig. 3.1). But most importantly, the second term in eq. 3.7 also predicts the spontaneous conversion of a high-energy pump photon into two lower-energy signal and idler photons, namely SPDC. This phenomenon is allowed purely by the quantization of electromagnetic field.

The phase-matching condition comes by assuming the second order susceptibility is homogeneous in the crystal $\eta(\mathbf{r}) = \eta$, and by integrating on a large volume $\mathcal{V}$. Then the Hamiltonian vanishes except for $\mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i = 0$. The quasi-phase-matching condition, on the other hand, comes by considering a periodic variation of the susceptibility along the (Oz)-axis $\eta(\mathbf{r}) = \eta \cdot p(z)$. By approximating this variation as a harmonic function $p(z) = \exp(i 2\pi z/\Lambda)$ with Λ the poling period, the Hamiltonian becomes:

$$\hat{H}_I \propto \eta \int_{\mathcal{V}} e^{i\Delta\mathbf{k}\cdot\mathbf{r}} d^3\mathbf{r} \cdot \hat{a}_p^\dagger \hat{a}_s \hat{a}_i \quad + \eta^* \int_{\mathcal{V}} e^{-i\Delta\mathbf{k}\cdot\mathbf{r}} d^3\mathbf{r} \cdot \hat{a}_p \hat{a}_s^\dagger \hat{a}_i^\dagger, \tag{3.8}$$

with $\Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i + \frac{2\pi}{\Lambda}\mathbf{u}_z$, such that $\hat{H}_I$ vanishes except for $\Delta\mathbf{k} = 0$ (see Fig. 3.2).

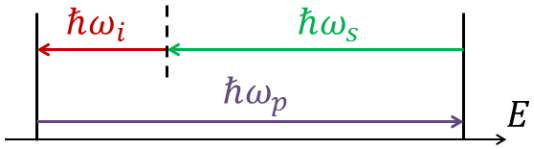


Fig. 3.1: Energy conservation in SPDC: a photon is annihilated, and two photons of the same total energy are created. In SFG and SHG, two photons are annihilated, and a photon of the same total energy is created.

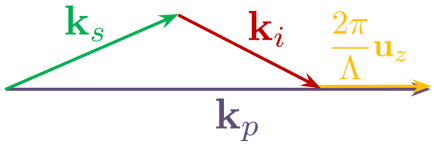


Fig. 3.2: Quasi-phase-matching SPDC, and other nonlinear effects, in a periodically-poled crystal.

Now we can grasp an idea of the photon statistics. Making the non-depleted pump assumption, meaning the pump field is strong enough to be unaffected by the interaction, and under the phase-matching condition, the Hamiltonian becomes:

$$\hat{H}_I = \mathcal{C}\,\hat{a}_s^\dagger \hat{a}_i^\dagger + \text{conj.}, \tag{3.9}$$

where $\mathcal{C}$ is a constant. Then the signal-idler quantum state reads

$$|\psi\rangle = e^{\frac{i\hat{H}_I t}{\hbar}}|0_s,0_i\rangle \xrightarrow[t\to+\infty]{} \sqrt{1-p}\sum_{n=0}^{+\infty} p^{n/2}|n_s,n_i\rangle, \tag{3.10}$$

where p is a constant that can be interpreted as the probability of emitting exactly one photon pair, as long as $p \ll 1$. The pairs statistics therefore follows a geometric law, with a probability $\mathbb{P}(n) = (1-p)p^n$ of emitting exactly n pairs. Besides the reduced density operator of the signal (or idler) mode gives a thermal state:

$$\rho_{s/i} = \sum_{n=0}^{+\infty} \frac{\mu^n}{(1+\mu)^{n+1}}|n_{s/i}\rangle\langle n_{s/i}|, \tag{3.11}$$

with an average number of photons $\mu = p/(1-p)$. This can be used in experiments in order to verify the spectral purity of down-converted photons (see [94, 95] for more details on that matter). Finally, as $p \ll 1$ we can simplify the state as $\rho_{s/i} \simeq |1_{s/i}\rangle\langle 1_{s/i}|$ which is a single-photon state. This way measuring a photon from a SPDC pair allows to announce its twin, which becomes a heralded single-photon.

In general, we may not be able to assume the pump is a monochromatic plane wave, and the crystal has a finite size. In such cases the signal and idler photons can be emitted in a superposition of different spatial and spectral modes, and

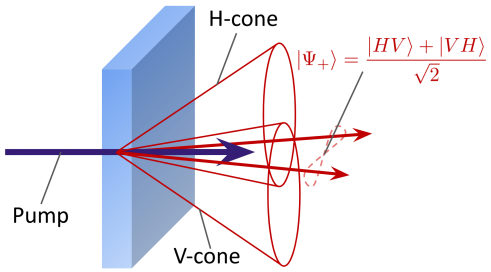
therefore display some entanglement in those modes. Then photon-pairs can still be used in order to generate heralded single-photons, but the spectral and spatial state is mixed. The full derivation of that state remains an open question, and attempts can be found in different studies [92–96]. For the rest of this thesis, we consider the photons spectral and spatial state to be close-to-separable, such that the statistics is approximated with a geometric law.

3.2 State of the Art

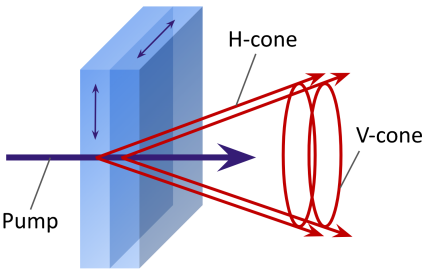
In the following we give a non-exhaustive review of the most significant demonstrations of entangled-photon sources, based on SPDC in a nonlinear crystal, which allows the spontaneous transformation of a high-energy photon into two lower-energy photons. Our own design takes inspirations from these sources.

3.2.1 Bulk Crystal Sources

The first experimental SPDC-based entangled-photon source was built by Z. Y. Ou and L. Mandel in 1988 [97], using a potassium dihydrogen phosphate crystal. Photons are generated in the same polarization, via type-I SPDC, and projected onto the singlet state $|\Psi_-\rangle = \frac{|HV\rangle - |VH\rangle}{\sqrt{2}}$ using a BS. Many bulk crystal-based sources were later demonstrated, such as that of P. G. Kwiat *et al.* [98], in which photons are emitted in a $\beta-\mathrm{BaB_2O_4}$ crystal (BBO), via type-II SPDC (see Fig. 3.3a). There photons are distributed on two cones of orthogonal polarizations, such that entanglement can be measured at the two intersections of the cones. A type-I source was also demonstrated using the same BBO crystal [99]. For this experiment, two identical crystals were used in cascade, rotated by 90° (see Fig. 3.3b). In this way the pump-photon is down-converted either in the first crystal, giving a pair of horizontally-polarized photons, or in the second one, giving a pair of vertically-polarized photons. Thus, photons can be distributed on two rings, one for each polarization. Where the rings overlap, and therefore interfere, the photons are in the entangled state $|\Phi_+\rangle = \frac{|HH\rangle + |VV\rangle}{\sqrt{2}}$. Here the entanglement can in principle be collected over the whole ring, contrary to the type-II version.



(a) Type-II source. Two cones of orthogonally-polarized photons are emitted by pumping a single BBO crystal. Entanglement is generated at the intersections of the rings [98].



(b) Type-I source. Two overlapping cones of photons are emitted by pumping two cascaded BBO crystals with orthogonal axes. Entanglement is generated all over the rings [99].

Fig. 3.3: Common sources photon pairs entangled in polarization, based on bulk-BBO crystals.

By collecting photons on parts of the type-I ring, 21×10^3 pairs/s could be measured [99], with a pump power of 150 mW. The number of pairs measured is proportional to the pump power, so we give the rate of pairs per mW of pump power, also called *brightness* of the source. In this demonstration the brightness is 140 pairs/s/mW. The fidelity of the states generated to the target Bell state was $> 88\%$, which was mostly limited by the delay between the rings that limits the interference quality. Radhika Rangarajan *et al.* demonstrated a compensation of this so-called *walk-off* [100], reaching a brightness of 5400 pairs/s/mW, and a fidelity of $99 \pm 2\%$ to the Bell state.

3.2.2 Periodically-Poled Crystal Sources

Alternatively to bulk crystals, periodically-poled crystals have become widespread, as they can be tailored for colinear emission in a wide range of wavelengths, thanks to the QPM condition. In the following, we focus on a source based on type-II periodically-poled $KTiOPO_4$ (PPKTP), in a Sagnac interferometer [101], as shown in figure 3.4. Other common sources use periodically poled $LiNbO_3$ (PPLN) [30, 102–106], which was shown to be particularly adapted to integrated optics [107].

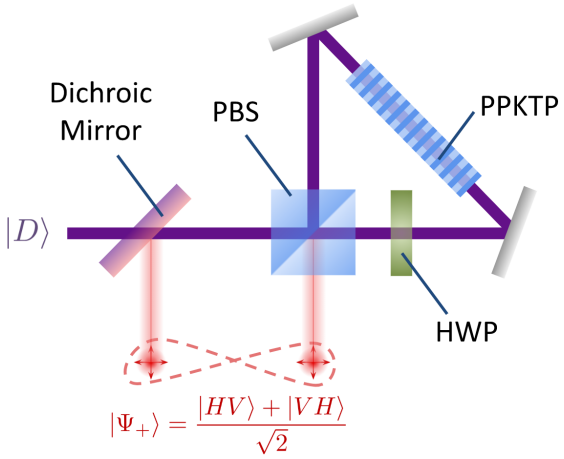


Fig. 3.4: Scheme of the Type-II PPKTP-Sagnac source of entangled photons. The pump is diagonally polarized, and is converted into lower energy photons. The dichroic mirror reflects the pairs and transmits the pump. The HWP implements a bit flip $\hat{X}$. All components are adapted to both wavelengths of pump and pairs.

In the Sagnac-PPKTP scheme, a diagonally polarized pump goes into a Sagnac interferometer, where the beam is split by the PBS. There, two situations can occur:

- If the pump photon is in state $|V\rangle$, it is reflected on the PBS and is down-converted into signal and idler photons, in state $|VH\rangle$. Then, they are transformed by a bit flip $\hat{X}$, so their state becomes $|HV\rangle$. Finally, the signal photon is reflected by the PBS while the idler is transmitted.
- If the pump photon is in state $|H\rangle$, it goes through the PBS and is flipped into the state $|V\rangle$ by the bit flip $\hat{X}$. Then, it is down-converted into signal and idler photons, in state $|VH\rangle$. Finally, the signal photon is transmitted by the PBS, and the idler photon is reflected.

A dichroic mirror is used in order to separate the pump from the photons. Provided the interferometer is properly aligned, we get a superposition of the two situations, and we collect the entangled state $|\psi_+\rangle = \frac{|HV\rangle+|VH\rangle}{\sqrt{2}}$ at the output of the interferometer. Note the Sagnac interferometer is intrinsically stable, as the interfering beams take the same round path in opposite directions. Thus a phase change in one path also affects the other path, so no relative phase appears between the paths. Thus no phase stabilization is needed for generating high-quality states [108].

Over the past decades, this PPKTP-Sagnac scheme has become widespread, thanks to its stability, adaptability and ease of conception. It was first demonstrated in 2006 by T. Kim *et al.* [109], with a brightness of $\sim 5000\,\text{pairs/s/mW}$ and a fidelity of more than 94.3% to the target Bell state. Considerable efforts have been made to increase these numbers, and extremely high performances were later achieved by Alessandro Fedrizzi *et al.* [42]. By optimizing the focusing of the pump, they could reach a brightness of $\sim 82 \times 10^3\,\text{pairs/s/mW}$ with a fidelity as high as 99.6% to the target Bell state, making it one of the best sources ever made. Furthermore, high coupling efficiencies could be demonstrated, thanks to the Gaussian colinear emission allowed by periodically-poled crystals [45, 95, 110]. It was also shown that such PPKTP-based sources can emit completely separable pairs of photons at telecom wavelength, by carefully tailoring the crystal and laser properties [111–113], which is fundamental when generating pure heralded single-photons and multipartite entangled-states [95, 111–113]. Finally, this scheme was used to perform the first satellite-to-ground entanglement distribution in 2017, where the whole source was sent into orbit [114], showing the extreme stability of such a setup. All these high performances motivate our choice to adopt this Sagnac-PPKTP scheme for our own source of entangled-photons.

3.3 Design of the Source

Our source is made of three main blocks (see Fig. 3.5). The first one is the pump emission and shaping, including the laser source, its spatial filtering and focusing. The second part is the heart of the source, made of the Sagnac interferometer and the nonlinear PPKTP crystal, in which the photons pairs are generated. Finally the third block is the photon collection, which encompasses the photon filtering and coupling into optical fibers. One could also identify a fourth block as the photons processing and measurement, though it may differ from one experiment to another. A full recipe for the alignment of that source was given in D.H. Smith's thesis [115], though our method differs slightly. We detail that method in appendix B.

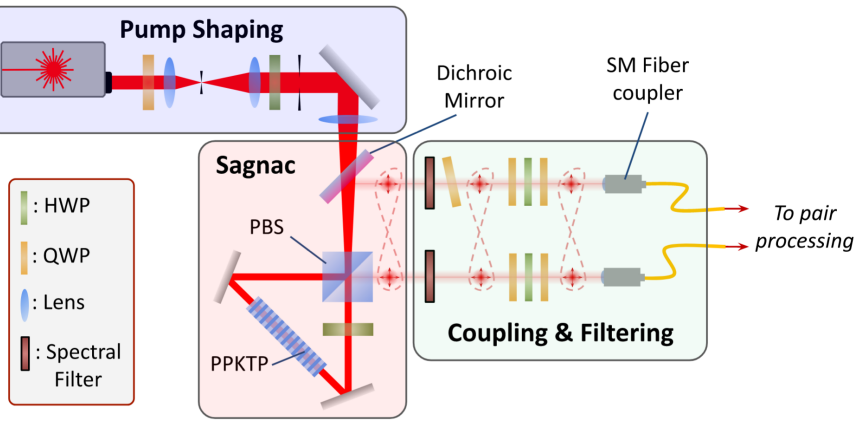


Fig. 3.5: Outline of our source, with the three main blocks described in this chapter.

3.3.1 Pump Beam

The pump beam is emitted via a Titanium-Sapphire Laser (Mira 900HP from Coherent), of $\approx 4\,\mathrm{W}$ average power. Ideally, the Laser is mode-locked, so that 2 ps-pulses are emitted at a $f = 76\,\mathrm{MHz}$ rate. The spectral intensity is approximately Gaussian (see Fig. 3.6), centered around a tunable wavelength $775\,\mathrm{nm} \pm 15\,\mathrm{nm}$ with a 0.33 nm full-width at half-maximum (FWHM).

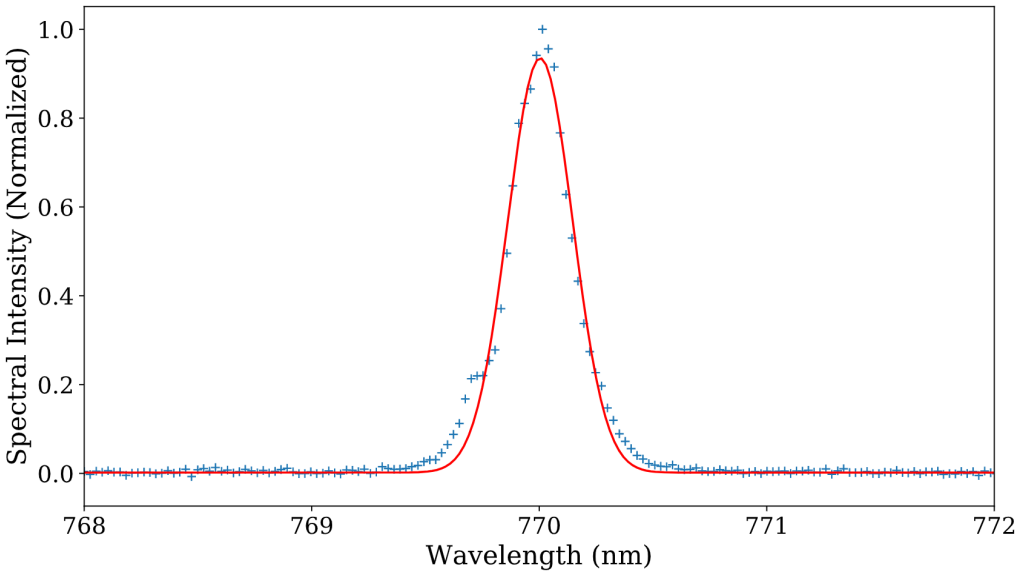


Fig. 3.6: Measured spectrum of the mode-locked pump Laser, with a Gaussian fit giving the 770 nm central wavelength and 0.48 nm FWHM.

Assuming thermal statistics of photons emitted in the crystal, the rate of simultaneous detection of $2N$ photons is given by:

$$\mathcal{R}_{2N} = f\, p^N \eta^{2N}, \tag{3.12}$$

where f is the pump repetition rate, p is the probability of emitting a pair in a pump pulse, and η is the detection efficiency of one photon. The probability p is proportional to the energy $\mathcal{U}_p$ in a pump pulse, so that

$$\mathcal{R}_{2N} = f\, \kappa^N \mathcal{U}_p^N \eta^{2N}, \tag{3.13}$$

where κ is the number pairs emitted by Joules of pump pulse, which depends on the characteristics of the crystal, and the pump focusing mode in the crystal. The pair detection-rate is directly proportional to the average pump power $\overline{P} = f\mathcal{U}_p$. This way, when only the two-photons state matters, we try to keep p quite low, typically $p \lesssim 0.01$, in order to avoid noise coming from double-pair emission, with a rate $\mathcal{R}_4$. We therefore limit the energy $\mathcal{U}_p$ while keeping the average power $\overline{P}$ at a high value. This can be achieved by increasing the repetition rate via a temporal multiplexer for instance, as demonstrated in [116, 117]. In some specific applications we can even use the Laser in continuous-wave mode (CW), instead of the pulsed mode. Thus the energy is maximally spread in time, but the different frequencies composing the Laser's spectrum are not mode-locked anymore, which effectively makes the photons' spectrum mixed. This is the method we use in chapter 6, where the spectral state has little importance. On the contrary, when attempting to prepare 4-photons states, we want to increase the probability of emitting two pairs in a pump pulse, and therefore the energy per pulse $\mathcal{U}_p$. This is the approach we suggest for multipartite-states emission.

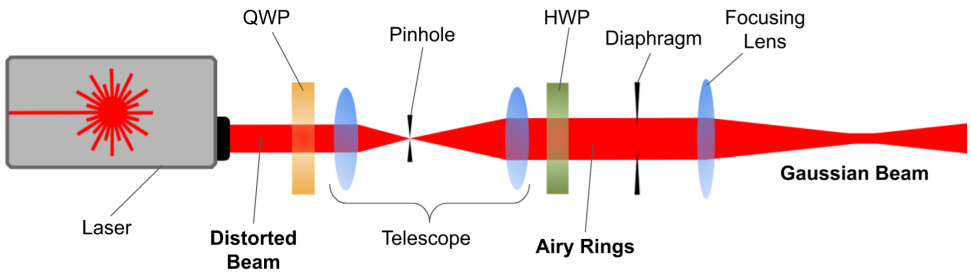


Fig. 3.7: Pump-beam shaping apparatus. In addition to the components mentioned in the main text, two waveplates are displayed, for polarization management.

The spatial profile of the Laser is of major importance in our experiments, as it conditions the spatial modes of the photons, and therefore their coupling into SM fibers. As the beam emitted by our Laser displays some distortions, we filter the spatial mode in order to make it close to a Gaussian beam, which fits the mode of a SM fiber. The beam-shaping apparatus is displayed in Fig. 3.7. It is made of two 50 mm-focal length lenses, forming a telescope, with a pinhole in the middle. The beam that outputs the telescope is then an Airy disk, with a close-to-Gaussian profile surrounded by lower intensity rings. Blocking the rings with a diaphragm allows to retrieve a satisfying Gaussian profile (see Fig. 3.8).

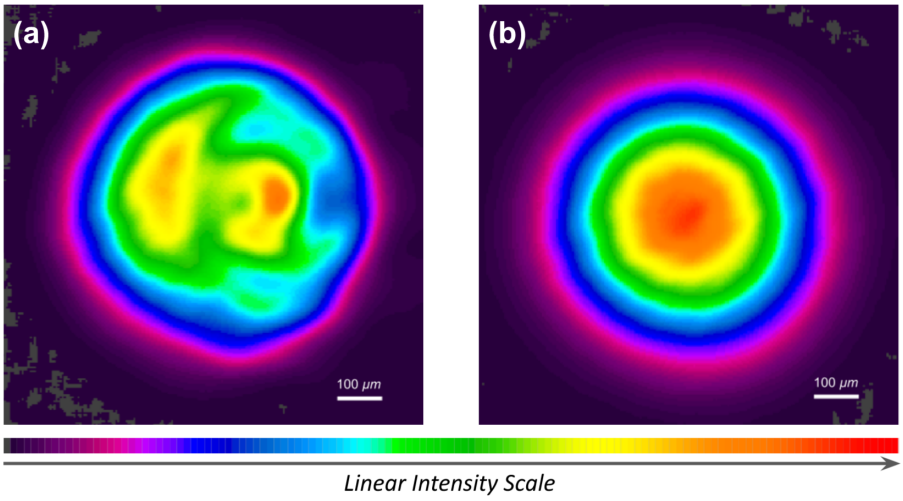


Fig. 3.8: Intensity profile measured in the focal plane of the last lens with a CCD camera, after spatial filtering of the pump beam (a) when the Airy rings are left unfiltered, (b) when the diaphragm is closed, letting the central disk through and filtering the Airy rings out. We retrieve a satisfying Gaussian profile.

Finally, the beam is focused inside the Sagnac interferometer, thanks to a 750 mm-focal length lens. The resulting Gaussian beam has a waist of $w_p \simeq 315\,\mu\text{m}$, for a Rayleigh length $z_{R,p} \simeq 40\,\text{cm}$. The choice for this waist is the result of a compromise, between a high photon-pair emission probability p, ensured by a strong focusing, and a high separability of photons spectral modes, ensured by the collimation of the pump beam, among other factors. This last point is addressed in the following paragraphs.

3.3.2 Sagnac Interferometer and PPKTP Crystal

Our entangled photon-pairs are emitted by SPDC in a nonlinear PPKTP-crystal, placed in a Sagnac interferometer. The principle of that Sagnac source is given in precious paragraph 3.2.2, and a photograph of our setup is displayed in Fig. 3.9.

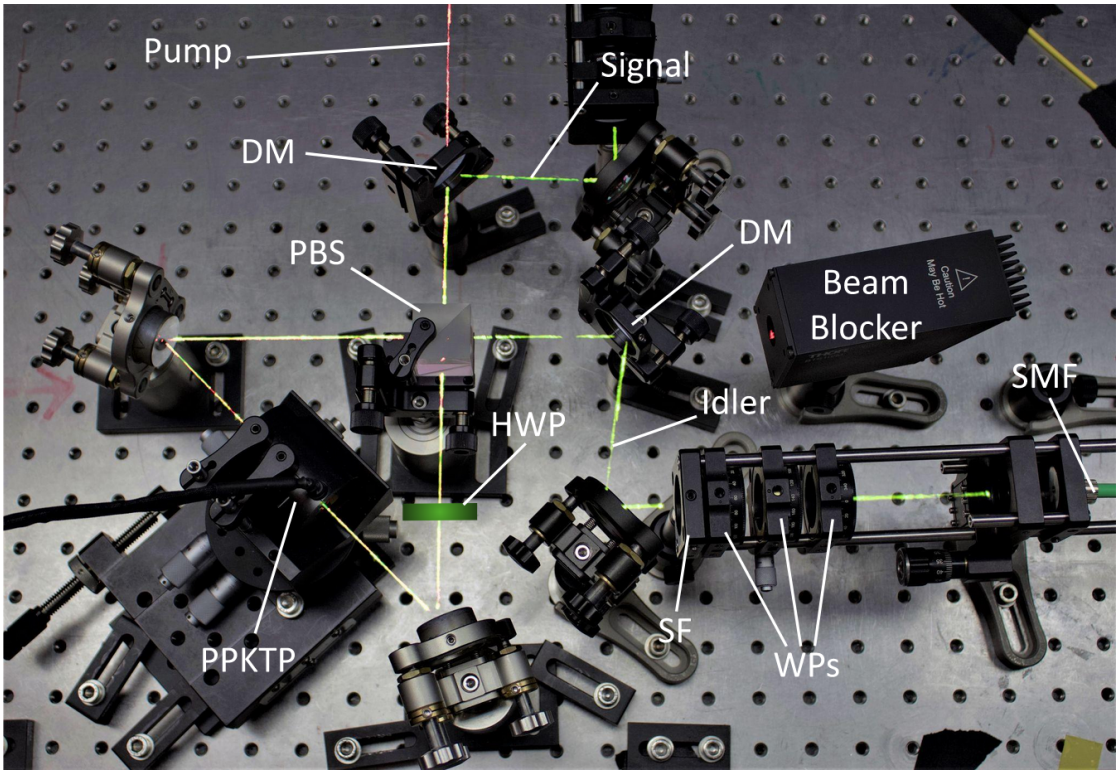


Fig. 3.9: Photograph of our Sagnac source. The achromatic HWP was removed from the source while taking the picture, for more clarity in the beams' paths. We display a green rectangle where it usually lies during the experiments. Part of the coupling and filtering block is displayed, for the signal photon, with a spectral filter (SF) and a SM-fiber coupler. Photograph made in collaboration with Julien Déoux.

The interferometer is made of a PBS, two mirrors and a HWP, all these components being compatible with the pump and photons wavelengths. Because of this last condition, these four components are chosen with special care. Our custom dual-wavelength PBS was provided by Spectral Optics, and provides a relatively high extinction ratio ($> 1000:1$) for two ranges of wavelengths, centered around 775 nm and 1550 nm. An achromatic HWP was provided by Thorlabs, made of six

different birefringent crystals ensuring a π phase-retardance between horizontal and vertical polarizations, for the whole range of wavelengths between 600 nm and 2700 nm [118]. Corners of the Sagnac are made of metallic silver mirrors, which provide a relatively high reflectivity for our wavelengths. DMs are placed at the outputs of the Sagnac, in order to separate the pump from the photon pairs.

The PPKTP crystal lies in the center of the Sagnac interferometer, in an oven that allows to tune the phase matching condition. The crystal was tailored by Raicol for type-II quasi-phase-matching at room temperature $\simeq 20\,^{\circ}$C, from a vertically-polarized pump photon at $\lambda_p = 775$ nm, to a vertically-polarized idler photon and a horizontally-polarized signal photon, at degenerate wavelengths $\lambda_i = \lambda_s$. The QPM condition $\Delta\mathbf{k}' = 0$ (see eq. 2.57), along with the energy conservation condition $\lambda_i = \lambda_s = 2\lambda_p = 1550$ nm, gives the poling period:

$$\Lambda = \frac{\lambda_p}{n_p(\lambda_p) - \frac{1}{2}\big(n_i(\lambda_i) + n_s(\lambda_s)\big)}, \tag{3.14}$$

where n_p, n_i and n_s are the respective optical indices of KTP for the pump, idler and signal modes. These depend on the wavelength and polarization of the modes, and are given by the empirical Sellmeier equations [119, 120]:

$$\begin{aligned} n_p(775\,\text{nm}) &= 1.76, \\ n_s(1550\,\text{nm}) &= 1.73, \\ n_i(1550\,\text{nm}) &= 1.82, \end{aligned} \tag{3.15}$$

which gives the poling period $\Lambda = 46.2\,\mu$m. Even though our crystal was optimized for 775 nm pump and 1550 nm signal and idler photons, we later tuned the pump wavelength to $\lambda_p = 770$ nm in order to maximize the coupling of our photons (this can be explained by the variation of diverse component's transmission with the field's wavelength). This way photons still verify the QPM condition, but at non-degenerate wavelengths $\lambda_s = 1541.5$ nm and $\lambda_i = 1538.5$ nm. During the course of these projects, choosing this non-degenerate configuration over the degenerate case did not cause any significant drawback. For other projects, the degenerate emission might still be required, for which one could tune the QPM condition by setting up the crystal's oven temperature.

We predict the photon's spectral state from the crystal and pump's characteristics. Our crystal's length is $L = 30\,\text{mm}$, so the focusing parameter reads

$$\xi_p = \frac{L}{n_p z_{R,p}} = \frac{\lambda_p L}{n_p \pi w_p^2} \simeq 0.04. \tag{3.16}$$

As $\xi_p \ll 1$, meaning L is far smaller than the pump's Rayleigh length, the pump is collimated in the crystal. Thus we adopt the same approach as N. Bruno in [95], and consider the pump, signal and idler spectral modes do not entangle with spatial mode (see [92, 93] for a more general derivation). In addition, the latter are considered to be plane waves of respective vectors:

$$\mathbf{k}_p = \frac{\omega_p n_p(\omega_p)}{c}\mathbf{z}, \qquad \mathbf{k}_s = \frac{\omega_s n_s(\omega_s)}{c}\mathbf{z}, \qquad \mathbf{k}_i = \frac{\omega_i n_i(\omega_i)}{c}\mathbf{z}, \tag{3.17}$$

where ω_p, ω_s and ω_i are the angular frequencies of the pump, signal and idler modes, respectively. In that case, it was shown that the interaction Hamiltonian (eq. 3.1) leads to the following state for the photon pairs [94, 111]:

$$|\psi_{si}\rangle = \iint d\omega_i d\omega_s \gamma(\omega_i, \omega_s) \hat{a}^\dagger_{\omega_i} \hat{a}^\dagger_{\omega_s} |0_i, 0_s\rangle, \tag{3.18}$$

where $\gamma(\omega_i, \omega_s)$ is the so-called *joint spectral amplitude* (JSA) that takes the form:

$$\gamma(\omega_i, \omega_s) \propto \alpha(\omega_i + \omega_s) \cdot \beta(\omega_i, \omega_s), \tag{3.19}$$

where $\alpha(\omega_i + \omega_s)$ is the pump envelope, that gives the frequencies allowed by energy conservation, and $\beta(\omega_i, \omega_s)$ is the phase-matching envelope, that gives the frequencies allowed by the QPM condition. In a periodically-poled crystal, under collinear-emission approximation, and assuming the pump spectrum to be Gaussian (when the Laser is mode-locked), we can express these functions:

$$\begin{aligned} |\alpha(\omega_i + \omega_s)| &= \exp\Big(-\frac{\Delta\omega^2}{2\sigma_p^2}\Big), \\ |\beta(\omega_i, \omega_s)| &= \text{sinc}(\Delta k \cdot L), \end{aligned} \tag{3.20}$$

where $\Delta\omega = \omega_p - \omega_s - \omega_i$, ω_p is the central wavelength of the pump Laser, σ_p its spectral bandwidth, L the length of the crystal and Δk is the phase mismatch:

$$\Delta k = \frac{\omega_s n_s(\omega_s)}{c} + \frac{\omega_i n_i(\omega_i)}{c} - \frac{(\omega_i + \omega_s) \cdot n_p(\omega_i + \omega_s)}{c} + \frac{2\pi}{\Lambda}. \tag{3.21}$$

In Fig. 3.10, we display a simulation of the photon pairs' JSA in our experiments. Performing the Schmidt decomposition of the spectral state, we expect a Schmidt number $K = 1.18$, and a high single-photon purity $P = 1/K = 0.85$, indicated by the central close-to-Gaussian lobe in the JSA. Thus the photons are close-to-spectrally-separable, which is a fundamental feature when performing 2-photons interference in multipartite protocols or quantum teleportation, as we will see at the end of the chapter. Still side lobes from the sinc function are responsible for some correlations in the pairs' spectral modes, which limits the purity. These can be suppressed by filtering the spectral state.

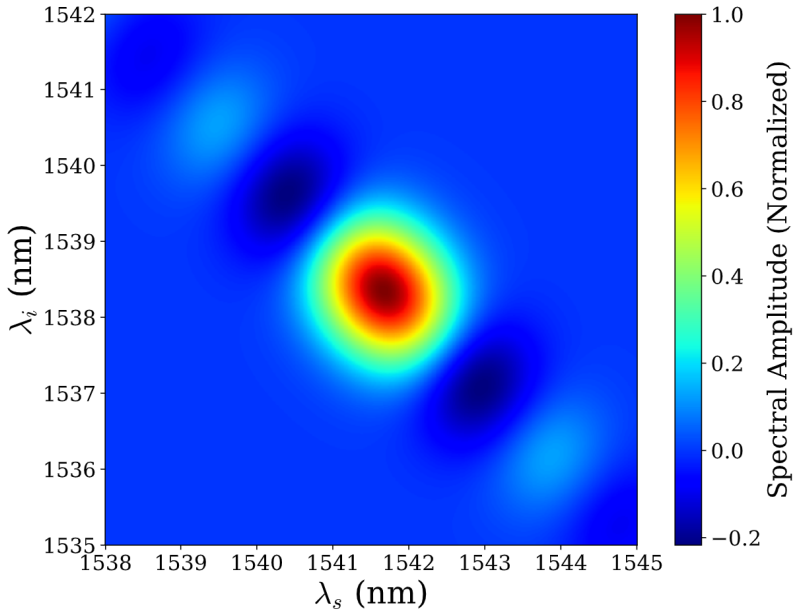


Fig. 3.10: Simulated joint spectral amplitude of the photon pairs emitted in our experiment, when the pump center wavelength is 770 nm.

3.3.3 Coupling and Filtering

Before being processed, the photons have to be cleaned from parasitic signals, such as remnants of the pump, undesired reflections and photons emitted in unwanted modes. The spectral filtering is performed in three steps. First, we already mentioned the longpass dichroic mirrors, which separate most of the pump beam from the signal and idler photons. Then, longpass filters suppress the last remnants of

the pump, while transmitting the photons. Finally, custom ultra-narrow bandpass filters, provided by Alluxa, suppress most parasitic signals emitted in the telecom range. The central wavelength can be tuned from 1550 nm to 1530 nm by tilting the filter around its vertical axis, and the FWHM is 1.3 nm as seen in Fig. 3.11. These narrow filters also allow to suppress the side lobes displayed in Fig. 3.10, which increases the purity, but induces additional losses.

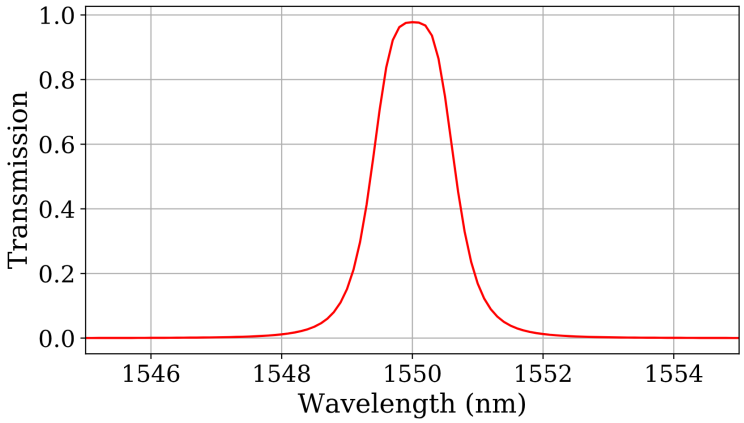


Fig. 3.11: Transmission of the ultra-narrow bandpass filters depending on the wavelength, when placed normally to the beam. The central wavelength goes down when tilting the filter. Data provided by Alluxa.

Spatial filtering is performed by coupling the photons into single-mode fibers thanks to a short focal-length lens. Tuning the distance of the lens from the fiber and the crystal center allows to select the Gaussian mode selected by the SM fiber. We wish to set these coupling modes in order to maximize the probability of detecting the signal photon, knowing the idler photon was measured. This probability is also called the asymmetric heralding efficiency, and reads:

$$\eta_{s|i} = \frac{P_{si}}{P_i}, \tag{3.22}$$

where P_{si} is the probability of detecting both signal and idler photons, and P_i is the probability of measuring the idler photon. It was shown that when the pump is collimated at the scale of the crystal, as it is in our case ($\xi_p = 0.04$), then signal and idler spatial modes are highly correlated [45, 110], such that measuring the idler photon in a Gaussian mode of waist w_i projects the signal photon in a Gaussian

mode of similar waist $w_s \simeq w_i$. Thus, choosing carefully the coupling waists allows to maximize the heralding efficiency. In our experiment, this maximum heralding efficiency was reached for $w_s = 190\,\mu\text{m}$ and $w_i = 218\,\mu\text{m}$. The corresponding focusing parameters read

$$\xi_s = \frac{L}{n_s z_{R,s}} = \frac{\lambda_s L}{n_s \pi w_s^2} \simeq 0.24, \qquad \xi_i = \frac{L}{n_i z_{R,i}} = \frac{\lambda_i L}{n_i \pi w_i^2} \simeq 0.17, \tag{3.23}$$

such that both modes are also collimated at the scale of the crystal. This comforts the assumption taken in the last paragraph, considering signal and idler as plane waves when calculating the spectrum, leading to eq. 3.17.

The heralding efficiency effectively varies from one experiment to another, depending on losses induced by various components. The maximum value reached was $\eta_{s|i} = 66\%$, in a specific situation where the pump was going through one side of the Sagnac interferometer only, and the achromatic HWP was removed from the photons' path. By discarding the losses induced by fiber connectors, and detectors efficiency, we get a corrected coupling efficiency $\eta'_{s|i} > 81\%$, comparable to state-of-the-art sources [45, 95]. This value might increase even more by choosing more transmissive optical components, in particular the Sagnac PBS which only transmits 90% of the light at maximum.

3.3.4 Photon Processing and Measurement

Photons can undergo different operations after being coupled into SM fibers. Typically, we manage their polarization via different sets of WPs, or more conveniently by using fibered polarization controllers (PC). The rest of the photon processing apparatus depends on the implemented protocol. A common processing block is the polarization-analyzer (PA), that we use to measure the photon's polarization in any qubit basis mentioned in paragraph 2.1.3. An example of such an apparatus is shown in Fig. 3.12. A HWP and a QWP are used in order to rotate the photon polarization, or equivalently the measurement basis. These are followed by a PBS, which converts two orthogonal polarization modes into spatial modes, later measured by single-photon detectors.

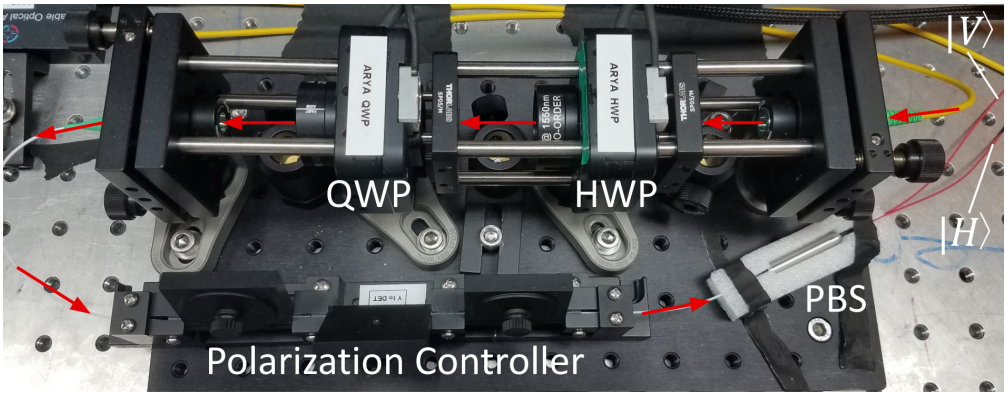


Fig. 3.12: A polarization analyzer used in our experiment. WPs are motorized, PBS is fibered, a PC ensures the PBS axes are aligned with those of the WPs.

In table 3.1, we give the different bases that we measure in our experiments, along with the ocrreponding WPs configurations. In our setup, WPs are mounted into fast and precise motorized stages, in order to automatically and swiftly change the measurement basis. This is of particular convenience when performing quantum state tomography, or quantum information protocols, as in chapter 6.

Basis	HWP angle	QWP angle
$\hat{\sigma}_z : \{\|H\rangle, \|V\rangle\}$	0°	0°
$\hat{\sigma}_x : \{\|D\rangle, \|A\rangle\}$	22.5°	0°
$\hat{\sigma}_y : \{\|L\rangle, \|R\rangle\}$	0°	45°
$(\hat{\sigma}_x + \hat{\sigma}_z)/\sqrt{2}$	11.25°	0°
$(\hat{\sigma}_x - \hat{\sigma}_z)/\sqrt{2}$	33.75°	0°

Tab. 3.1: Common polarization bases and the corresponding WPs angle used to measure the photon in said bases.

After being discriminated by the PBS, photons are carried by optical fibers to superconducting nanowire single-photon detectors (SNSPDs, ID281 by IDQuantique). These consist of an electronic circuit made of a conductor material (see Fig. 3.13), that becomes superconducting when cooled down to a cryogenic temperature $\approx 0.8\,\mathrm{K}$ (see Fig. 3.14). When the photon hits the circuit, the energy income heats the conductor up, which loses its superconductivity. The resulting increase in resistivity is then converted into an electric pulse that can be measured and

timed with maximum uncertainty (timing jitter) of ≈ 40 ps. The detection efficiency for telecom photons is typically ≈ 90%, and the rate of false detections, called *dark counts* (DC), is as low as ≈ 50 Hz, due to the cryogenic temperature. After the detection of a photon, the detector is fully operational past a recovery time of ≈ 100 ns at maximum. The characteristics of the detectors are given in table 3.2.

Detector	Efficiency	DC rate	Timing Jitter	Recovery Time
1	84% ± 4%	41.5 Hz	30.5 ps	50 ns
2	89% ± 4%	33 Hz	30.6 ps	46.6 ns
3	86% ± 4%	61 Hz	30.9 ps	79.7 ns
4	96% ± 5%	58 Hz	40.7 ps	97.5 ns

Tab. 3.2: Characteristics of our first four SNSPDs, provided by IDQuantique.

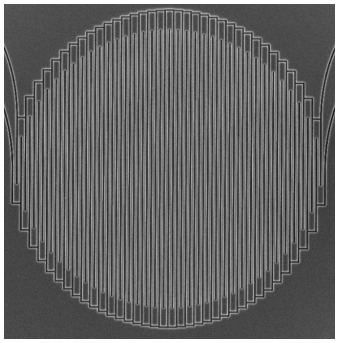


Fig. 3.13: Picture of a superconducting nanowire circuit used as SNSPD, taken via scanning electron microscope. Source: IDQuantique.

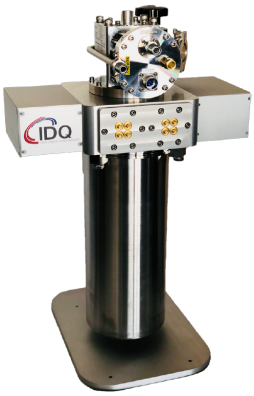


Fig. 3.14: Cryostat containing the SNSPDs, and keeping them at < 0.8 K. Picture by IDQuantique.

The electric signal of each detector is then sent to a time tagger (Ultra from Swabian Instruments), also called *coincidence counter* (c.c.), that times the different detection events with picosecond-precision. The simultaneity of different detection events can then be assessed, by setting up the right *coincidence window*, which is the maximum time interval between two simultaneous detection events. Timing delays can also be added or subtracted after recording the events, in order to compensate for differences in each photons' paths. We choose a coincidence

window of 500 ps, which is long enough compared to timing uncertainties, but small enough to cancel-out most of the noise. A summary of the setup used to measure the correlation between two photons is displayed in Fig. 3.15.

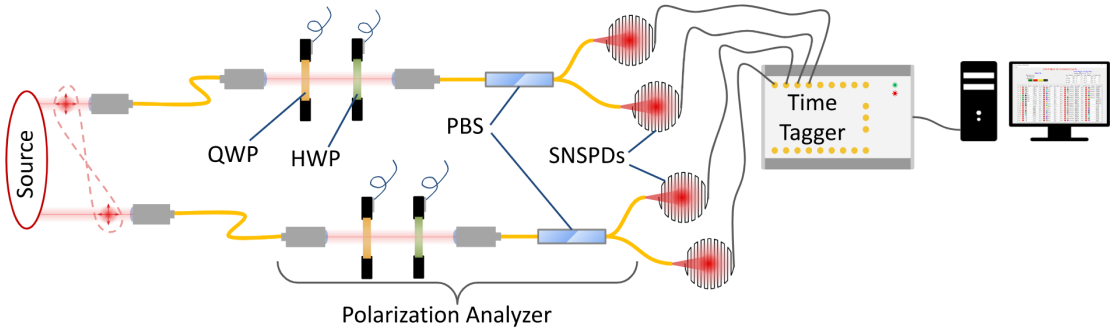


Fig. 3.15: Full apparatus used to analyze the bi-photon polarization state. Two polarization analyzers allow the local measurement of each photon of the pair. Correlations between detection events are then assessed by the time tagger and computer.

3.4 Characterization of the Source

Thanks to the biphoton polarization analyzer shown in Fig. 3.15, we could measure the most important characteristics of our source. First, sending 1 W of pump power, we measured a maximum pair-detection rate of $R_2 \simeq 400\,\text{kHz}$, depending on the alignment of the source. Accounting for the detection efficiencies, we get an emission rate $R_2' \simeq 1.1\,\text{MHz}$, and hence a brilliance $\mathcal{B} \simeq 1.1 \times 10^3\,\text{pairs/s/mW}$. This is significantly lower than previous sources [42, 95], which can be explained by the collimation of the pump beam in the crystal. When the pump is in pulsed-mode, we derive the probability of emission of a pair from a pump pulse $p = R_2'/f \simeq 0.015$, where f is the Laser repetition rate. This way, we have $p \gg p^2$, so the double-pairs emission rate is negligible compared to the pair emission rate. This feature, together with the high-heralding efficiency $\eta_{s|i} = 66\,\%$, indicates our source approaches a heralded single-photon source. Another common benchmark of single-photon sources is the autocorrelation function $g^{(2)}(0)$ of the heralded photon, detailed in [43], which quantifies the importance of higher-order effects compared

to photon pair emission. To evaluate this quantity, we herald the signal photon with its idler twin detected in a detector D_1, and we measure the signal photon in two detectors D_2 and D_3 after a 50/50 beam splitter. This way the autocorrelation function reads:

$$g^{(2)}(0) \simeq \frac{4 \cdot R_1 \cdot R_{1,2,3}}{(R_{1,2} + R_{1,3})^2}, \tag{3.24}$$

where $R_{1,2}$, $R_{1,3}$ and $R_{1,2,3}$ give the rates of simultaneous detections in the corresponding combination of detectors, and R_1 is the rate of detection of the idler photon in D_1. In Fig. 3.16 we display $g^{(2)}(0)$ as a function of the average pump power, in pulsed mode. At low power, our source indeed approaches the behaviour of a true heralded single-photon source with $g^{(2)}(0) = 0$.

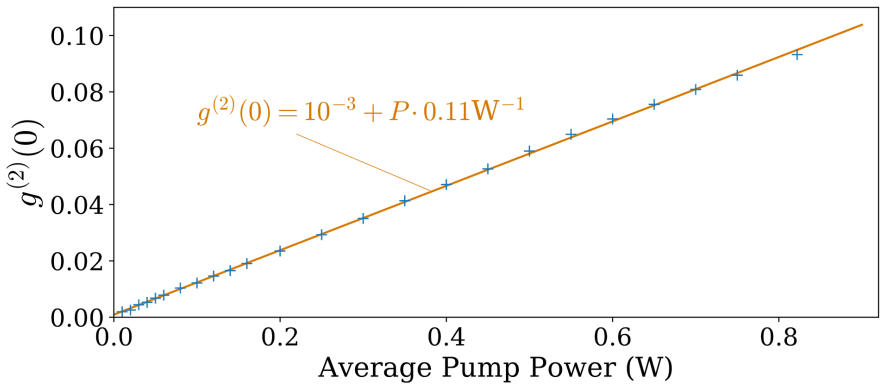
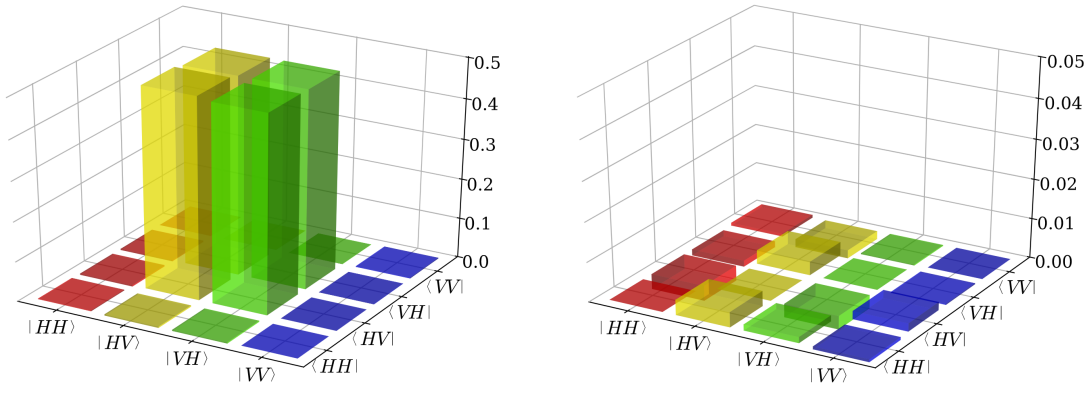


Fig. 3.16: Autocorrelation function $g^{(2)}(0)$ of the heralded signal photon, as a function of the average pump power, in pulsed mode.

Most importantly, the biphoton polarization states emitted by our source can be evaluated on quantum state tomography (QST) [51, 52], which allows to reconstruct the full density matrix of our 2-qubits state, by measuring a finite set of Pauli observables $\hat{\sigma}_{i_A} \otimes \hat{\sigma}_{i_B}$. These are easily accessible in our experiment, by measuring the two photons in all combinations of two configurations displayed in table 3.1. Details on this method are given in appendix A. Thanks to the WPs motorized stages and the relatively high pair detection rate, it typically takes only 15 min to 30 min to acquire a full data set needed for this state reconstruction.

Using the pump Laser in continuous-wave mode, double-pair emissions are negligible, such that the state quality is maximized. We display a typical density operator ρ emitted by our source in Fig. 3.17. This state displays a fidelity to maximally entangled state

$$F(\rho, \Psi_+) = \langle \Psi_+ | \rho | \Psi_+ \rangle = 99.32\% \pm 0.05\%. \tag{3.25}$$



(a) Real part. **(b)** Imaginary part.

Fig. 3.17: Typical biphoton polarization quantum state emitted by the Sagnac source, reconstructed by QST. We measure a fidelity $F(\rho, \Psi_+) = 99.32\% \pm 0.05\%$ to the Bell state $|\Psi_+\rangle$. Real and imaginary parts are not at the same scale.

We mentioned in paragraph 2.1.4 that 2-qubits maximally-entangled Bell states form a whole class of states that are all equal up to local unitary transformations. Hence in many cases the absolute closeness of the 2-qubits state to $|\Phi_\pm\rangle$ or $|\Psi_\pm\rangle$ is less relevant that its closeness up to local unitaries. This is the case of device-independent protocols in particular, as we will see in chapter 6. For this reason we often maximize the fidelity of our state ρ to $|\Phi_+\rangle = \frac{|HH\rangle + |VV\rangle}{\sqrt{2}}$, by applying local unitaries $\hat{U}_A \otimes \hat{U}_B$. This way, with an optimal alignment of the source, we measure

$$F_{\max}(\rho, \Phi_+) = \max_{\hat{U}_A, \hat{U}_B} \langle \Phi_+ | \hat{U} \rho \hat{U}^\dagger | \Phi_+ \rangle = 99.43\% \pm 0.05\%, \quad \hat{U} = \hat{U}_A \otimes \hat{U}_B, \tag{3.26}$$

which is comparable to state of the art sources [42]. Note that in practice, it is particularly convenient to tune the different WPs angles and fibered polarization controllers, in order to experimentally perform the maximization on $\hat{U}_A$ and $\hat{U}_B$.

When the Laser is in pulsed mode, the energy is concentrated in time, resulting in a higher probability of double-pair emission. This induces noise in the effective state, caused by accidental coincidences between uncorrelated photons. The consequent decrease in the fidelity of the state to a maximally-entangled state is displayed in Fig. 3.18.

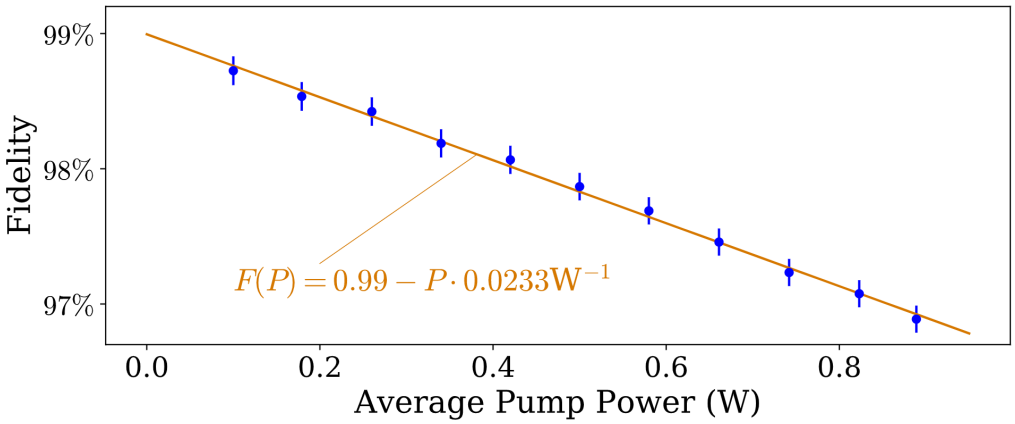


Fig. 3.18: Fidelity of the biphoton polarization quantum state emitted by the Sagnac source evaluated by QST, to the maximally-entangled state $|\Phi_+\rangle$, as a function of the pulsed-pump power.

Using the state emitted by our source, we could test the violation of Bell inequality 2.21. In CW-mode, we measure the observables $\hat{A}_0 = \hat{\sigma}_x$ and $\hat{A}_1 = \hat{\sigma}_z$ on the first photon, and the observables $\hat{B}_0 = -\frac{1}{\sqrt{2}}(\hat{\sigma}_z + \hat{\sigma}_x)$ and $\hat{B}_1 = \frac{1}{\sqrt{2}}(\hat{\sigma}_z - \hat{\sigma}_x)$ on the second photon. This way, we measure a ϵ-close-to-maximum violation

$$\mathcal{I} = 2\sqrt{2} - \epsilon = 2.8142 \pm 10^{-4}, \quad \text{with} \quad \epsilon = 0.0142 \pm 10^{-4}. \tag{3.27}$$

Finally, we show the relatively strong stability of our source over time, by performing a series of QST of the state emitted by the source, for an 8 hours duration. From the data acquired during these tomographies, we deduce the evolution of both the source's state fidelity to a maximally-entangled state and the pairs' detection rate, over time (see Fig. 3.19). By fitting the data we conclude the drift in state quality and coupling to be negligible.

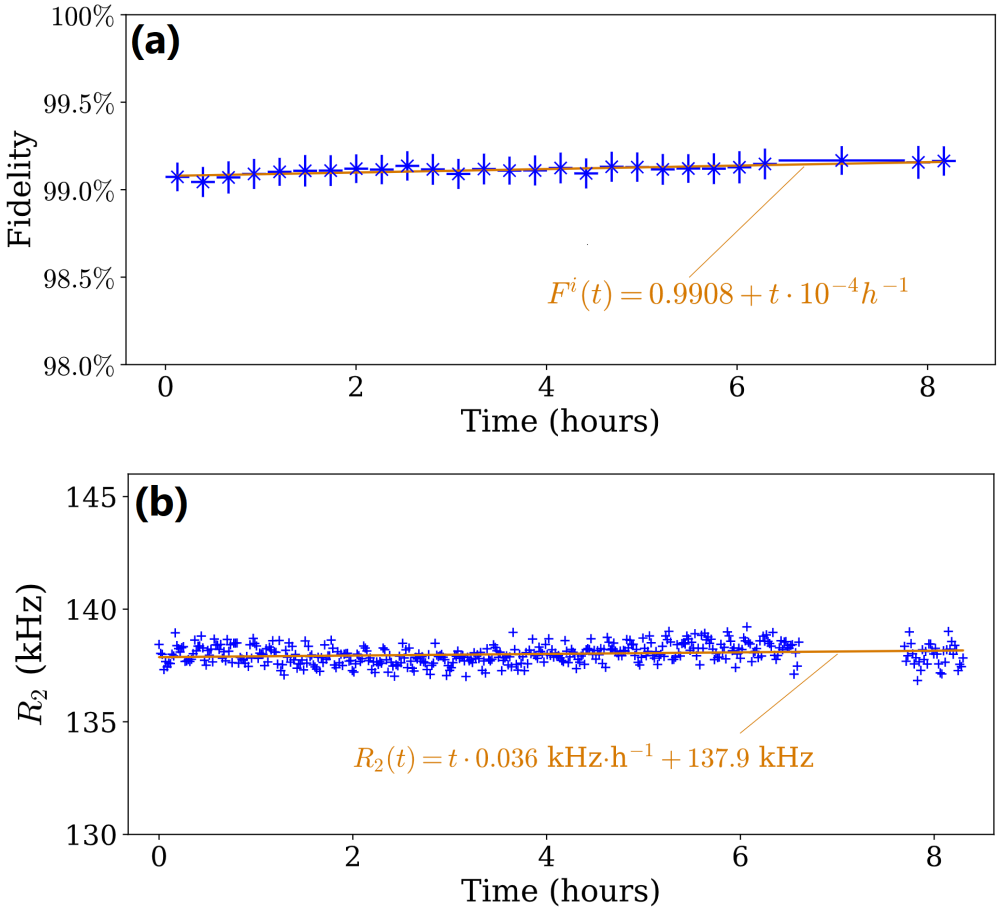


Fig. 3.19: Features of the source measured over an 8-hours time-span. The 1-hour gap at the end of the data series is due to a cooling cycle of the detectors.
(a) Fidelity of the source's state to a Bell state. **(b)** Biphoton detection rate R_2.

3.5 Toward a Multi-Photons Source

Numerous quantum network primitives require more than one pair of photons to operate. This includes authenticated teleportation [26], composable multipartite entanglement verification [121], or quantum anonymous communications [17, 122], which we would like to experimentally implement in our laboratory in a near future. Here we detail our new design for a source of multiple pairs of photons, which only requires some mild adaptations of our pair source to operate. These adaptations are currently being made in the lab.

3.5.1 Key Ingredient: Two-Photons Interference

The most common SPDC-based multipartite layout is made of at least two sources of pairs of photons, and at least one bipartite operation in order to make two pairs interact. This operation generally consists of making two photons from separate pairs interfere, in a Hong-Ou-Mandel-like setting (see paragraph 2.2.5). We display the typical experimental setting in Fig. 3.20. We can for instance use a BS, and post-select on the detection of one photon in each one of its outputs. We say photons *anti-bunch*, which effectively performs a Bell-state measurement (BSM), projecting the interfering photons on the antisymmetric state $|\Psi_-\rangle = \frac{|HV\rangle - |VH\rangle}{\sqrt{2}}$. This is a fundamental ingredient for quantum state teleportation [58]. When using a PBS, two maximally-entangled states $|\Phi_+\rangle = \frac{|HH\rangle + |VV\rangle}{\sqrt{2}}$, and with the same post-selection, then we effectively perform entanglement-fusion [46, 123]. This way we prepare a GHZ state

$$|GHZ_4\rangle = \frac{1}{\sqrt{2}}\big(|H_1H_2H_3H_4\rangle + |V_1V_2V_3V_4\rangle\big). \tag{3.28}$$

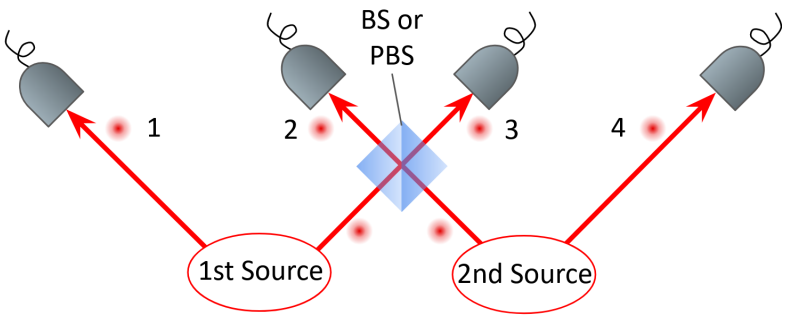


Fig. 3.20: Typical layout of a optical multipartite quantum experiment.

A wide variety of other two-photons operations are possible, summarized in the following review [124]. The quality of the operation is quantified by the HOM-interference visibility, which reads:

$$V(\rho_2, \rho_3) = \frac{P(\rho_2) + P(\rho_2) - \| \rho_2 - \rho_3 \|_2^2}{2}, \tag{3.29}$$

where ρ_2 and ρ_3 are the reduced states of photons 2 and 3 in Fig. 3.20, $P(\rho)$ is the purity of state ρ, and $\| \rho_2 - \rho_3 \|_2^2 = \mathrm{Tr}(\rho_2 - \rho_3)^2$ is the Hilbert-Schmidt distance. This way, a high-quality GHZ state or BSM relies on generating separable pairs of photons (except in the polarization degree of freedom), and in indistinguishable

states. The design of our PPKTP crystal and pump beam, as well as mild spectral filtering, ensures the photons are spectrally-separable photons, and therefore display an optimal purity. In the following we focus on the problem of generating indistinguishable pairs of photons.

3.5.2 Spatial Multiplexing and Layered Sagnac Source

A naive way to generate independent pairs of photons is to pump different non-linear crystals with the same Laser. This solution is wide-spread and functional, and was used in particular to successfully generate a 12-photons GHZ state [47]. Still the hardness of this solution resides in making all independent sources indistinguishable, such that all crystals and alignment should be rigorously the same.

An interesting solution was proposed by H. Guilbert *et al.* [125] and demonstrated by the KIKO team of M. Bourennane [126, 127] in the form of *spatial multiplexing*. It exploits the ring-distribution of entangled pairs emitted via type-I SPDC in a bulk BBO crystal. In this way, independent pairs can be collected in different parts of the ring, as shown in Fig. 3.21. These pairs are indistinguishable, as they come from the same source.

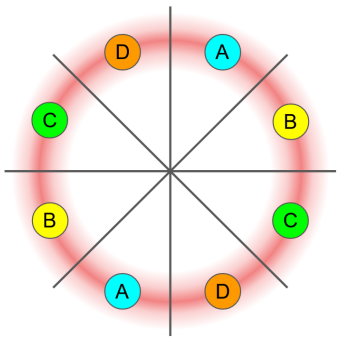


Fig. 3.21: Spatial multiplexing: independent and indistinguishable pairs of photons can be collected in different points A, B, C or D of the same type-I SPDC ring.

For now, spatial multiplexing was only proposed for bulk crystals. Thus all multipartite sources based on periodically-poled crystals have so far relied on building multiple separate interferometers, with two different crystals. This was pointed out as a limitation for the emission of indistinguishable pairs [128], aris-

ing from mild differences in separate crystals or alignments. Here we provide an original adaptation of the standard PPKTP-Sagnac source, in order to get two sources *into one* by spatial multiplexing. This method exploits the 2-dimension geometry of periodically-poled-crystal-based sources, which therefore allows to vertically stack different sources of entangled-photons in the same Sagnac interferometer and PPKTP crystal. We display this *Layered-Sagnac* configuration in Fig. 3.22. Alternatively, we call this configuration *Sagnac Mille-Feuille* in French, or even *Lasagnac* in Italian, as a tribute to the layered dishes from these two countries. In addition to ensuring the indistinguishability of photons, this layout is particular compact, such that we can consider stacking more layers in a limited space. Also, the alignment of such a layered source is expected to be particularly simple. Indeed, provided one is able to generate two parallel pump beams (by using the setup shown in Fig. 3.23 for instance), the whole source can be aligned by performing a single alignment of the Sagnac interferometer, detailed in annex B.

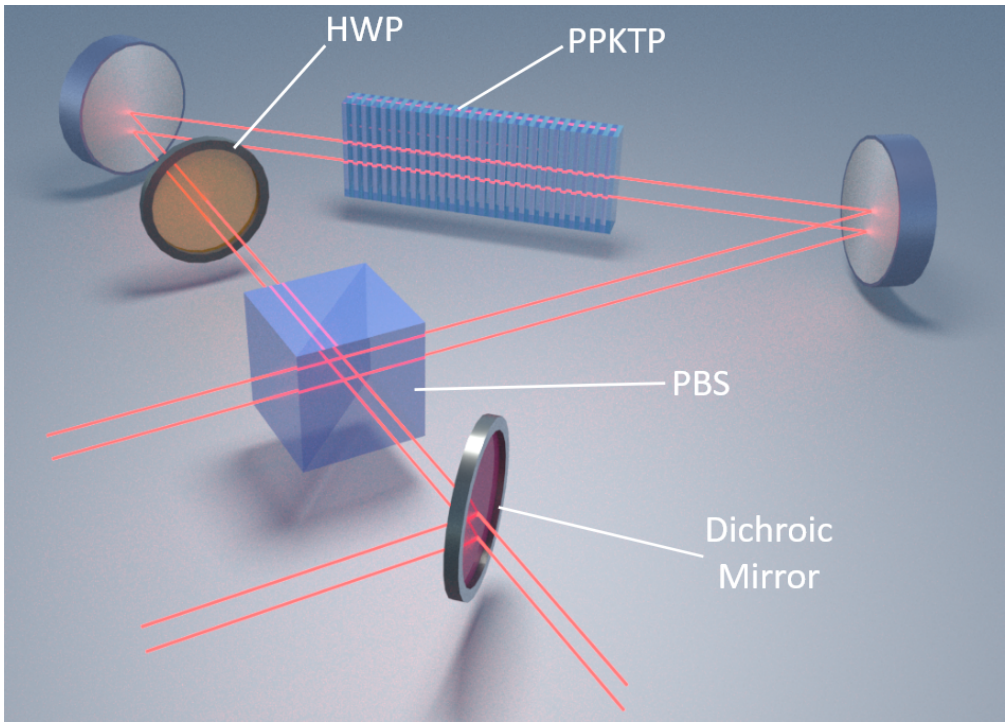


Fig. 3.22: Scheme of the Layered-Sagnac source. Two parallel beams pump the same PPKTP crystal at different heights.

3.5.3 Pump-Shaping for Layered Sagnac Source

Converting our source into a Layered Sagnac source should only require a few adaptations, the main one being the pump shaping. The main hardness comes from generating two vertically-stacked parallel beams. A spatial multiplexer made of two calcite crystals can generate two such beams, as shown in Fig. 3.23. Interestingly, as the two beams have exactly the same path, one can set the focusing optics before the multiplexer. This ensures both beams are focused inside the crystal with the same waist.

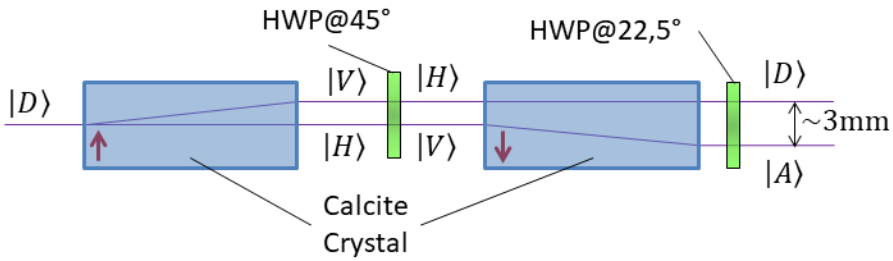


Fig. 3.23: A spatial multiplexer used to generate two parallel beams. Calcite crystals separate two parallel beams of orthogonal polarization. We use two such crystals, rotated at 180°, so the optical path-length is the same for both beams.

For this first demonstration, we consider this solution based on calcite-crystals does not provide enough degrees of freedom in order to ensure the beams are perfectly parallel. Furthermore, a multipartite source requires to use the Laser in pulsed mode, in order to maximize the probability of simultaneously emitting two pairs (see eqs. (3.12,3.13)), and thus the 4-photons emission rate:

$$\mathcal{R}_4 = f\kappa^2\mathcal{U}_p^2\eta^4. \tag{3.30}$$

Here we recall f is the pump-pulse repetition rate, $\mathcal{U}_p$ the energy per pulse, κ the number of pairs emitted per Joules of pump pulse, and η the detectors efficiency. Increasing the pulse-energy also increases higher-order emissions, and therefore limits the state quality. For this reason, we propose to use a temporal multiplexer [116, 117], as shown in Fig. 3.24. Such multiplexer consists of dividing the energy of pump pulses by 2, all the while doubling the repetition rate, so the 4-photons emission rate becomes:

$$\mathcal{R}_4' = 2f\kappa^2(\mathcal{U}_p/2)^2\eta^4 = \frac{1}{2}f\kappa^2\mathcal{U}_p^2\eta^4. \tag{3.31}$$

This way, we divide the rate of emission by 2, instead of 4 if we simply had divided the pump power by 2. At the output of the temporal multiplexer, we get two separate beams, that we propose to use for parallel spatial-multiplexing in the layout shown in Fig. 3.24. We first recombine the beams in a Mach-Zehnder interferometer, where the second cube is a PBS. This way, we can finely control the alignment of the beams by measuring the interference visibility. Then we tilt two glass plates (windows) in opposite angles, such that one beam is displaced downward and the other is displaced upward. Such glass plates are generally particularly flat, such that the two beams stay parallel.

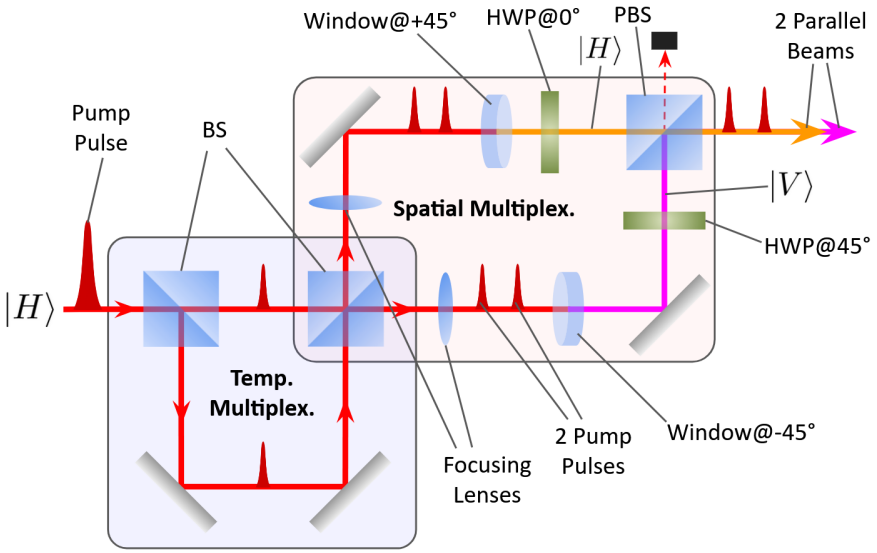


Fig. 3.24: Temporal and spatial multiplexer being built in our experiment. In the temporal multiplexer, half of the pulse power is delayed, in order to make two pulses with lower power. The windows are tilted around the horizontal axis that is perpendicular to the beams. The orange beam is displaced upward, while the magenta beam is displaced downward.

This layout is more complex than the one shown in Fig. 3.23, but can be tuned more finely. For instance, we can control the focusing of the two parallel beams separately, by adding lenses in the arms of the spatial multiplexer. Also, the parallelism and separation of the beams can be controlled finely thanks to the mirrors and glass plates. This way, we expect the multiplexer from Fig. 3.24 to be more practical in first laboratory experiments, though that of Fig. 3.23 would require more investigations for more compact and stable applications.

3.6 Discussion and Future Improvement

Combining a previously developed PPKTP-Sagnac scheme [42], with more recent adaptations for the emission of telecom photons [95, 111], we demonstrated a source of close-to-maximally entangled qubits, encoded on the polarization state of a photon pair. We showed this source to be quite flexible, as it can also be used in pulsed mode, to generate heralded single-photons with high heralding efficiency, spectral purity and low higher-order emissions. All those characteristics make our source particularly suitable for the implementation of quantum network protocols, such as weak coin-flipping with a single-photon (see chapter 4) or channel certification allowed via the self-testing of maximally-entangled states (see chapter 6).

A significant flaw of our source is its relatively low brilliance, which is limited by the weak focusing of the pump Laser. This latter feature is necessary for emitting separable photons with high coupling efficiency, as well as for our novel design of a multi-qubits source. A low brilliance is not limiting in our protocols, in which enough pump power is available for high emission rates, but may be a limitation for wider-scale applications in a near-future, in a context of energy scarcity.

A few improvements may maximize some characteristics of our photon-pair source. First, the heralding efficiency and detection rates could be improved by using more transmissive components, particularly the Sagnac PBS and achromatic HWP. Second, for applications relying mostly on maximally-entangled states, a continuous diode Laser could replace the Titanium-Sapphire Laser, which is relatively noisy when used in CW-mode. This would improve the purity of the emitted states, and thus their fidelity to Bell states. Finally, recent studies demonstrated close-to-unity spectral purity of telecom single photons emitted via SPDC [112, 113], by tailoring a custom poling pattern in the KTP crystal. In the future, such solutions could be applied in our experiments, eliminating the need for narrow spectral filtering.

Finally, we proposed a novel layout for adapting our source to multipartite-entanglement emission, with only a few adjustments. This uses the spatial multiplexing technique, which had already been demonstrated for bulk-crystal sources, emitting photons in a ring-geometry. In our case, we would stack different sources in the same PPKTP-Sagnac interferometer, exploiting the plane geometry of periodically-poled-crystal-based sources. The resulting layered-Sagnac source should be particularly compact, stable and simple to align, compared to the more usual setting, which uses several separate PPKTP-Sagnac sources. At the time of the writing of this thesis, this new source is being built in our lab, so we hope to demonstrate new multipartite communication protocols in a near-future, such as authenticated teleportation [26], composable GHZ-states verification [121], and quantum anonymous transmissions [122].

'Nic dwa razy się nie zdarza
i nie zdarzy. Z tej przyczyny
zrodziliśmy się bez wprawy
i pomrzemy bez rutyny.'

— Wisława Szymborska, *Nic dwa razy*.

CHAPTER 4

QUANTUM WEAK COIN FLIPPING WITH A SINGLE PHOTON

The security of a potential future quantum network relies on assembling different cryptographic primitives, allowing to perform elementary tasks with a certain resilience to malicious attacks and cheating strategies [129]. In particular, cheat-sensitive protocols display a form of resilience, as they can expose cheating players with a certain probability, although those players might be able to cheat and bias the protocol in their favor. This way, sanctions can be taken against players who are caught, in order to deter them from cheating.

Coin flipping is one of these fundamental building blocks, and comes in two versions. Strong coin flipping (SCF) allows two players to remotely agree on a random bit, such that none of the players can bias the outcome with probability higher than $1/2+\epsilon$, where ϵ is the protocol bias [130]. It is essential for multiparty computation [131], online gaming and more general randomized consensus protocols involving leader election [132]. Weak coin flipping (WCF), on the other hand, allows the same task when both players have a preferred, opposite outcome. This way the protocol effectively designates a winner or a loser, and players may try to bias the protocol toward their preferred outcome.

With classical communication resources, SCF and WCF protocols are only possible through computational assumptions or trusting a third party [130, 133–135]. For instance the players may trust a clock, in order to simultaneously broadcast two random bits, the sum of which provides the outcome. This implies no player would corrupt the third party to favor an outcome over another (by desynchronizing the clock for instance). In turn, such an assumption limits the protocol's security. Using quantum properties, however, one can derive information-theoretic security for SCF and WCF. Interestingly, quantum SCF can only limit the protocol bias to a minimum value $\epsilon = 1/\sqrt{2} - 1/2$ [136], whereas quantum WCF may reach arbitrarily small values of ϵ [137, 138]. The latter can also be used for the construction of optimal quantum SCF and quantum bit commitment schemes [139, 140]. While quantum SCF protocols were experimentally demonstrated [141–143], only recently a practical implementation of WCF was proposed by M. Bozzio *et al.*, using a single-photon and simple linear-optics [48]. Still the proposed quantum advantage provided by this implementation, in terms of outcome-bias from cheating players, is extremely sensitive to losses. Indeed a dishonest party may always declare an abort when they are not satisfied with the outcome of the coin flip.

In the following chapter, we present the first experimental demonstration of quantum WCF, that we performed using a single-photon, heralded from our photon-pairs source (see chapter 3), and later mixed with vacuum on a beam splitter. This effectively entangles two path-modes of the electromagnetic field, and gives the flip outcomes after detecting the presence or absence of a photon in said paths. Our protocol is a refined version of the theoretical protocol from [48], which provides a new form of quantum advantage, even in the presence of losses. This advantage relates to cheat sensitivity rather than bias from cheating players. By dropping the condition from [48] that both players should have equal probability of winning when cheating, our protocol allows them to detect whether their opponent is cheating during a verification step, and does not sanction an honest party. To this day, no classical protocol displays such cheat sensitivity with information-theoretic security [144, 145]. In order to emphasize the robustness of this quantum advantage to losses, we show that our protocol remains secure over an attenuation that corresponds to several kilometers of telecom optical fiber.

4.1 Proposed Protocol

We first introduce our protocol for quantum weak coin flipping using a single photon protocol, which accounts for potential losses and the detection of a cheating party. We provide the recipe in Protocol 4.1, built on the proposition from M. Bozzio *et al.* [48]. In the end we discern five mutually incompatible outcomes:

- Alice wins when $(b, v_1, v_2) = (0, 1, 0)$,
- Alice is sanctioned if $(b, v_2) = (0, 1)$,
- Bob wins when $(b, a) = (1, 0)$,
- Bob is sanctioned if $(b, a) = (1, 1)$,
- The protocol aborts if $(b, v_1, v_2) = (0, 0, 0)$.

The protocol uses three beam splitters, whose reflectivities x, y, and z are chosen in order to satisfy two conditions on these events. Firstly, the *fairness* condition, which states that Alice and Bob have equal winning probabilities when both of them are honest, i.e. $\mathbb{P}_h(\text{A. wins}) = \mathbb{P}_h(\text{B. wins})$, or

$$\mathbb{P}_h\big[(b, v_1, v_2) = (0, 1, 0)\big] = \mathbb{P}_h\big[(b, a) = (1, 0)\big]. \tag{4.1}$$

Secondly, the *correctness* condition, which states that an honest party should never be sanctioned for cheating, i.e. $\mathbb{P}_h(\text{A. sanctioned}) = \mathbb{P}_h(\text{B. sanctioned}) = 0$, or

$$\mathbb{P}_h\big[(b, v_2) = (0, 1)\big] = \mathbb{P}_h\big[(b, a) = (1, 1)\big] = 0. \tag{4.2}$$

Note that contrary to the previous protocol [48], we drop the *balancing* condition, which states that Alice and Bob should have equal probabilities of winning when using an optimal cheating strategy, as it cannot be satisfied together with the correctness condition in presence of experimental imperfections. Consequently, a practical balanced protocol would sanction an honest Alice for cheating, with non-zero probability. This impacts the cheat sensitivity, as one cannot trust the verification step if it sanctions honest parties. For more details on the protocol and the chosen conditions, the reader may refer to appendix C.

Protocol 4.1: Cheat-sensitive weak coin flipping with a single photon.

1. *Preparation.* Alice sends a single photon on a beam splitter of reflectivity x, keeps the reflected mode, and sends the other to Bob.

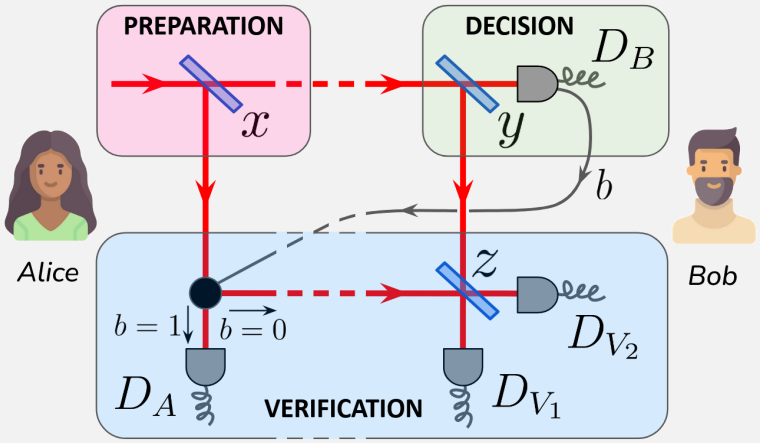
2. *Decision.* Bob sends the state he receives on a beam splitter of reflectivity y, measures the transmitted mode with a single-photon detector D_B, and broadcasts the outcome $b \in \{0,1\}$.

3. *Verification.* If $b = 0$, Alice sends her reflected mode to Bob, who mixes it with his own reflected mode on a beam splitter of reflectivity z, and measures the two outputs with single-photon detectors D_{V_1} and D_{V_2}. He distinguishes three cases depending on the outcome (v_1, v_2):

   - $v_2 = 1$: Alice is sanctioned for cheating,
   - $(v_1, v_2) = (1,0)$: Alice wins,
   - $(v_1, v_2) = (0,0)$: the protocol aborts.

   If $b = 1$, Bob discards his state. Alice measures her state with a single-photon detector D_A. She then discerns two cases depending on the outcome a:

   - $a = 0$: Bob wins,
   - $a = 1$: Bob is sanctioned for cheating.



4.2 Experimental Setup

Our implementation of Protocol 4.1 relies on the emission of heralded single-photons on Alice's side, using the source described in chapter 3. Operations described in the protocol are implemented using fibered components at telecom wavelength. As the polarization degree of freedom is not used for encoding, Alice entangles it with the spatial modes, using PBSs. In this way, the BSs reflectivities x, y, and z, can be effectively tuned by rotating the single-photon polarization before each PBS, using polarization controllers. We use a fast optical switch in order to select the party who performs the verification step, depending on the outcome b. During this operation, the photon is delayed in 300 m-long optical fiber spools. In order to simulate communication distance between Alice and Bob, and the corresponding losses induced by the photon storage that is necessary in this case, we use variable optical attenuators (VOAs). Photons are finally detected by single-photon detectors, and the measurement results are processed via our coincidence counter (c.c., see paragraph 3.3.4). The detailed setup is shown in Fig. 4.1, and discussed in the following paragraphs.

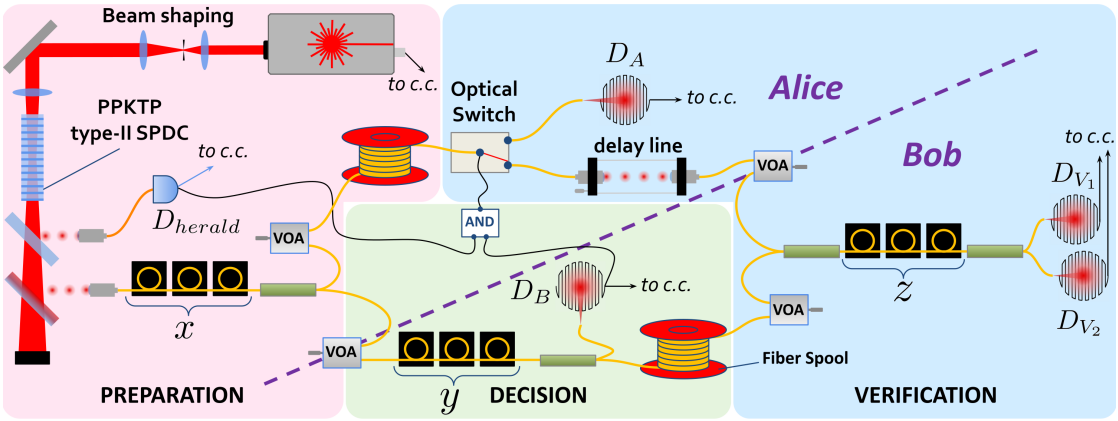


Fig. 4.1: Experimental setup for cheat-sensitive quantum weak coin flipping. Signal and idler photons are generated using the source presented in the chapter 3. The idler photon is detected in D_{herald}, heralding the signal photon which is used to perform the protocol and detected in D_A, D_B, D_{V_1}, and D_{V_2}. The dashed line marks visually the separation between Alice and Bob.

4.2.1 Heralded Single Photon

Most important details on the heralded single photon source are given in chapter 3. Still, a few additional details are worth mentioning. Firstly, the maximally-entangled states of polarization are not required in this protocol, so we only use one side of the Sagnac interferometer to produce photons in a product state of polarization $|H_i V_s\rangle$. We also remove the achromatic HWP from the Sagnac in order to minimize the losses on photons. After being collected into SM fibers, the idler photon is detected in order to herald the signal photon and trigger a protocol run. The resulting single-photon is then processed by the players to perform the protocol, and ultimately detected in 4 different path-modes with our 4 SNSPDs, which optimizes the heralding efficiency. Losses on the idler photon were not limiting, so we detect it with a 25 %-efficiency InGaAs avalanche photo-diode (APD, ID230 from IDQuantique). This way, protocol runs are triggered at a rate of 51 kHz, and without adding the fibered components we measured a maximum heralding efficiency $\eta_s = 63\%$ of the signal photon.

4.2.2 Optical Switching

During the decision step of the protocol, Bob's detection determines which party is winning, and which one has to perform the verification. In our experiment, this decision is effectively taken into account by Alice via her optical switch (Nanospeed from Agiltron, see Fig. 4.2). Hence, if Bob does not claim victory, the switch is in state "0" in order to send Alice's state to Bob, who performs the verification. If Bob claims victory, the switch goes to state "1" such that Alice keeps her state and performs the verification. In practice, we send the electronic signal from Bob's detector, together with the heralding signal, to a fast programmable logic AND gate, integrated in a time controller (ID900 from ID Quantique). This gate filters out potential detection events outside of the protocol, which might saturate the optical switch. The gate's output signal is then sent to the optical switch, which executes the decision.

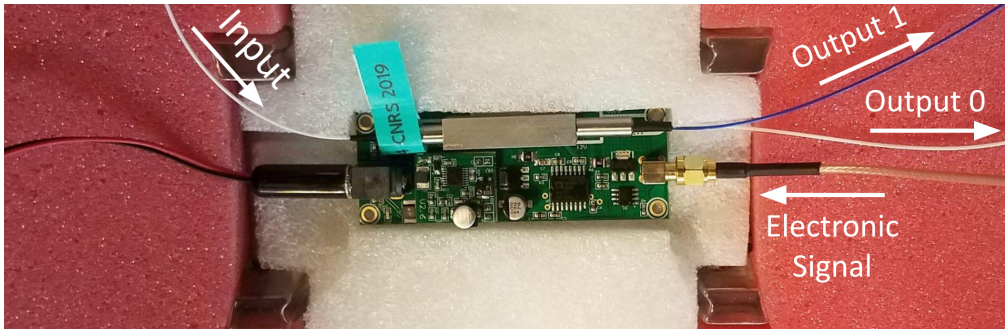
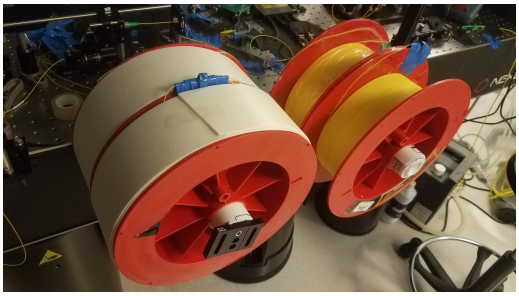


Fig. 4.2: Optical switch Nanospeed provided by Agiltron

Two timings must be set carefully in order to send the photon in the appropriate direction. First, the two detection electronic signals must be synchronized inside the AND gate in order to perform the logic operation. These timings can be tuned by programming the time controller, and we check that synchronization by measuring the rate of coincidences between the AND gate output, and the detections in the heralding detector and in Bob's detectors. Second, the wave-packet on Alice's side must pass through the switch when the latter is in the appropriate state. As it takes approximately $\simeq 800\,\text{ns}$ to perform the logic gate and the potential shift of the optical switch's state, we use 300 m-long optical fiber spools, on each party's side, in order to delay the photon for $\simeq 1.5\,\mu\text{s}$. We can then tune the timing of the AND gate's output electronic signal, again by programming the time controller, so that the photon enters the switch right after its state was set. We check the synchronization by implementing a dishonest Bob who constantly claims victory by sending a continuous electronic signal to the AND gate. Then the timing is appropriately set when the rate in Alice's verification detector is maximized.

Note that when performing the protocol with honest parties and a true single-photon, then Alice activates her switch only when Bob measures the photon, so ideally she cannot measure any signal in her verification detector. This is expected as we tend to minimize the probability of sanctioning an honest Bob, for optimal correctness. However, this questions the point of using such an optical switch and fast electronics, just to send void on Alice's verification detector. Physically speaking, this seems equivalent to using the exact same setup with no switch, and send all photons to Bob's verification apparatus. However, we cannot assume Bob

to be honest, even when he is. Therefore, it is of major importance that Alice checks that her state actually is projected on the void, in a cryptographic context.



(a) With no insulation (right), and partial insulation (left).

(b) With full sound insulation, as used in our experiments.

Fig. 4.3: Optical fiber spools used to delay the photon while the optical switch is being operated, with the sound insulation mentioned in the next paragraph.

4.2.3 Error Management

Various factors can generate undesired detection events in our protocol. This is true in particular for sanction outcomes, triggered by a detection in D_A or D_{V_2} which should never occur when a party is honest. Thus managing these error sources is of major importance in order to satisfy the correctness condition in particular, but also to minimize undesired outcomes in general.

Most of these outcomes arise from Bob's verification procedure, which relies on a Mach-Zehnder interferometer. If this interference is of poor visibility, then D_{V_2} can be triggered even if Alice is being honest, and her winning probability is also substantially lowered. Considering the length of this interferometer ($> 300\,\mathrm{m}$ because of the fiber spools), the visibility is limited by two main factors, namely the coherence length and phase fluctuations. The coherence length of photons is $\simeq 2.4\,\mathrm{mm}$ (see the pairs' spectrum in figure 3.10), which is small enough to start losing coherence after a few hours of experiment runs. This is mostly caused by length variations in the interferometer arms due to thermal fluctuations ($\simeq 2.4\,\mathrm{mm/°C}$ for a $300\,\mathrm{m}$ arm). We therefore regularly fine tune the length of one arm of the interferometer, using a free-space micro-metric delay line.

Phase fluctuations can be separated into two regimes. Slow phase fluctuations, of typical frequency $\lesssim 1\,\mathrm{Hz}$, are again caused by thermal variations, and can be easily monitored. Fast phase fluctuations, however, are caused by noise spanning the audible spectrum from 20 Hz to 2 kHz. This noise is amplified by the 300 m fiber spools, which act as a sort of microphone. These fluctuations are hard to resolve with our single-photon rate of a few 10 kHz, such that the interference pattern is averaged on that noise, and we witness an interference visibility of approximately $v \simeq 80\%$. In order to characterize that noise, we measure the interference pattern with a continuous diode laser and a fast photodiode (see Fig. 4.4). Without any sound insulation, the noise in the interference fluctuation spans the audible spectrum with a power spectral density $\simeq 7 \times 10^{-3}\,\mathrm{V}^2/\mathrm{Hz}$. In order to mitigate this noise, we wrap the fiber spools into several layers of sound-absorbing floating parquet underlay (see Fig. 4.3). The power spectral density then drops to less than $10^{-3}\,\mathrm{V}^2/\mathrm{Hz}$ except for some specific frequencies. The total noise power is divided by $\gtrsim 11$. The measured visibility then reaches $v \gtrsim 96\%$. Under these conditions, the thermally-induced fluctuations are slow enough such that we can easily post-select the protocol runs in which there was no phase difference between the two arms of the interferometer. This post-selection does not threaten the protocol security, as the parties could monitor the interference before performing the coin flip, and agree on starting the protocol only when the phase difference is null.

Undesired outcomes can also be triggered by double-pair emission inside the crystal, and dark counts in the detectors. The double-pair emission rate is limited in our experiment, as the probability of emitting a photon-pair in a pump pulse is $p \simeq 0.015$ (see the source's characterization in chapter 3), so the double-pair emission probability is negligible $p^2 \ll p$. Dark counts rates are made particularly low thanks to the use of SNSPDs for detecting the signal photon. Furthermore we use the pump internal signal in order to synchronize a 500 ps detection gate with each of the detectors signals, and all signal-photon detections are conditioned on a heralding photon detection. The probability of detecting a dark count during a protocol run is then $5 \cdot 10^{-8}$, such that undesired outcomes due to dark counts are negligible. However, the heralding photon is detected by an APD of 1 kHz dark counts rate, which is substantially higher than SNSPDs. Such dark counts trigger

protocol runs while no photon was emitted, and therefore slightly increase the abort probability. Still we evaluate the rate of such runs to be as low as $\lesssim 40\,\text{Hz}$, thanks to the gating applied by the pump laser signal. This way the surplus of abort probability caused by dark count is about $8 \cdot 10^{-4}$, which is negligible.

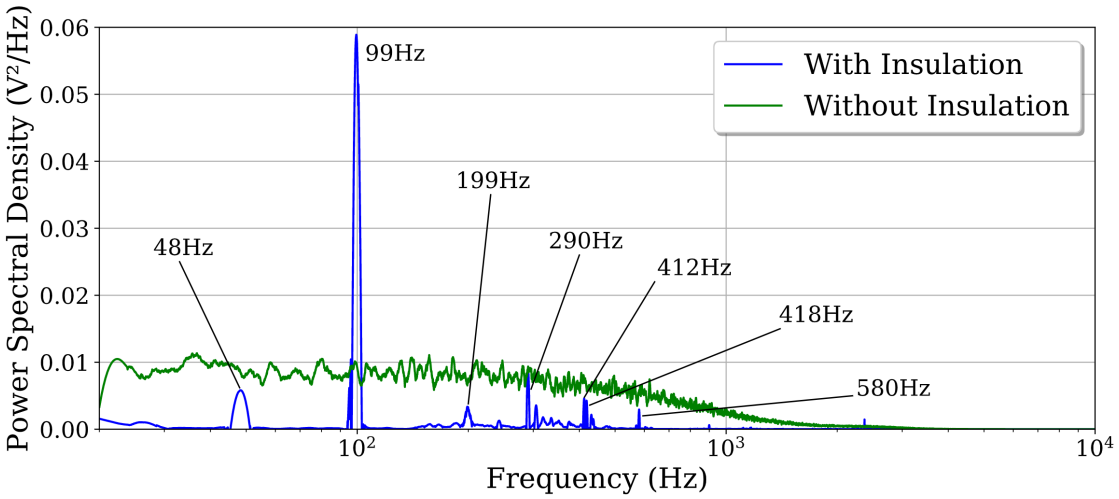


Fig. 4.4: Noise spectrum measured in the interferometer, using a continuous laser and a fast photodiode, with and without sound insulation on the fiber spools. When adding the insulation, the noise is low enough to distinguish peaks coming from the main sources of sound in the lab: 48 Hz, 99 Hz, and 199 Hz are emitted by the compressor plugged to the detectors cryostat, 290 Hz and 580 Hz are emitted by the pump in the cold water circuit, which cools down the compressor, and 412 Hz and 418 Hz are emitted by the laser chiller.

4.2.4 Losses

Because of their central role in the analysis of the protocol, we wish to distinguish the BS reflectivities from the losses induced by the rest of the components in the setup. For that purpose we define different transmission (or heralding) efficiencies, measured when the reflectivities and the state of the switch are set to trivial values $x, y, z, s \in \{0, 1\}$. These values reflect the losses in every possible path in the experiment, which are induced for instance by fiber spools, VOAs, fiber coupling and mating, or detectors. We detail the notations for the efficiencies corresponding

to each path and their measured values in Tab. 4.1. Each path is defined by the detector it ends in and the arm it goes through (Alice's or Bob's).

Notation	Path	x	y	z	s	Efficiency
η_A^s	$x \rightarrow \text{switch} \rightarrow D_A$	1			1	0.315 ± 0.008
η_B^y	$x \rightarrow y \rightarrow D_B$	0	0			0.303 ± 0.008
$\eta_A^{V_1}$	$x \rightarrow \text{switch} \rightarrow z \rightarrow D_{V_1}$	1		1	0	0.231 ± 0.008
$\eta_A^{V_2}$	$x \rightarrow \text{switch} \rightarrow z \rightarrow D_{V_2}$	1		0	0	0.219 ± 0.008
$\eta_B^{V_1}$	$x \rightarrow y \rightarrow z \rightarrow D_{V_1}$	0	1	0		0.184 ± 0.008
$\eta_B^{V_2}$	$x \rightarrow y \rightarrow z \rightarrow D_{V_2}$	0	1	1		0.175 ± 0.008

Tab. 4.1: List of notations and measured values for the efficiencies corresponding to the different paths involved in the experiment. The paths are described by the PBSs (labelled by the corresponding reflectivities) and/or the switch they go through, as well as the detector at the end of the path. We also list the values of x, y, z, and the state of the switch s, required to measure these efficiencies. Values are given for VOAs set at 0 dB.

4.2.5 Measurement of Outcome Probabilities

The probabilities of the different outcomes are evaluated by measuring the different detection rates and coincidence rates, provided by simple functions of our time tagger. However, the time tagger does not provide a direct way of measuring the rate of an event excluding some other event. For instance, in order to measure the rate of "Bob wins" event, we need to measure the rate of detection in Bob's detector, that did not occur at the same time as a detection in Alice's verification detector. In logical notation, we need the event $b \wedge \neg a$. Yet for any pair of detection events u, v, we have $u \wedge \neg v = u \wedge \neg(v \wedge u)$ such that the rate $R_{u\setminus v}$ of that event can be calculated as $R_{u\setminus v} = R_u - R_{uv}$, with R_u the rate of detection u and R_{uv} the rate of simultaneous detections u and v. In this way, we can easily deduce the formula for the rates of different outcomes in the protocol, summarized in Tab. 4.2.

Outcome	a	b	v_1	v_2	Logical	Rate
Alice wins		0	1	0	$\neg b \wedge v_1 \wedge \neg v_2$	$R_{hV_1} - R_{hV_1V_2}$ $-R_{hBV_1} + R_{hBV_1V_2}$
Bob wins	0	1			$b \wedge \neg a$	$R_{hB} - R_{hAB}$
Alice sanctioned		0		1	$\neg b \wedge v_2$	$R_{hV_2} - R_{hBV_2}$
Bob sanctioned	1	1			$b \wedge a$	R_{hAB}
Abort		0	0	0	$\neg b \wedge \neg v_1 \wedge \neg v_2$	$R_h - \{$*Rates of all other outcomes*$\}$

Tab. 4.2: Different protocol events, with the corresponding detection outcomes, logical formula and combination of coincidence rates needed to compute the corresponding probability. The rates subscripts correspond to the detectors which simultaneously trigger, h for the heralding, B for Bob's detector, A for Alice's verification detector, V_1 and V_2 for Bob's verification detectors.

4.3 Results for Honest Players

We first perform the protocol for different communication distances between Alice and Bob, when both of them are honest. These distances are simulated by setting each of the VOAs to a transmission $\eta = e^{-0.02L}$ with L the distance in kilometers, introducing additional losses to each arm of the setup. In our experiments, because of dark counts, double-pair emission, or imperfect interference visibility, Alice and Bob can still be sanctioned even though they are honest and the setup is optimized. In general, we cannot tune the reflectivities perfectly, so Alice and Bob may have slightly different winning probabilities. This means our implementation cannot satisfy perfectly the fairness and correctness conditions. Therefore, we define the fairness $\mathcal{F}$ and correctness $\mathcal{C}$ in order to quantify the closeness to these two conditions as follows:

$$\mathcal{F} = 1 - \left| \frac{\mathbb{P}_h(\text{A. wins}) - \mathbb{P}_h(\text{B. wins})}{\mathbb{P}_h(\text{A. wins}) + \mathbb{P}_h(\text{B. wins})} \right| \tag{4.3}$$

$$\mathcal{C} = 1 - \frac{\mathbb{P}_h(\text{A. sanctioned}) + \mathbb{P}_h(\text{B. sanctioned})}{\mathbb{P}_h(\text{A. wins}) + \mathbb{P}_h(\text{B. wins})} \tag{4.4}$$

Both quantities are equal to 1 when the corresponding conditions are perfectly fulfilled, and $\mathcal{C}, \mathcal{F} < 1$ otherwise. In the following we first show how honest Alice

and Bob should tune the reflectivities x, y and z, in order to maximize these two quantities. We then provide the results of our implementations of the protocol with such honest players.

4.3.1 Reflectivities with Honest Players

We first provide the theoretical values of reflectivities x_h, y_h and z_h that honest players should set. In our implementation, double-pair emissions and dark counts are very unlikely, so only the interference visibility v significantly limits $\mathcal{C}$ and $\mathcal{F}$. This way, we show that the correctness and fairness conditions are optimally approached by setting the following reflectivities:

$$x_h = \left[1 + \frac{\eta_A^{V_1}}{\eta_B^{V_1}} + \frac{\eta_A^{V_1}}{\eta_B^{y}}(1+v)\right]^{-1} \tag{4.5}$$

$$y_h = \left[1 + \frac{\eta_B^{V_1}}{\eta_B^{y}}(1+v)\right]^{-1} \tag{4.6}$$

$$z_h = \frac{1}{2} \tag{4.7}$$

The reader can refer to appendix C for the detailed proof. In particular, we show in this proof that the effective interference visibility can be expressed as the average on the fast phase fluctuations displayed in Fig. 4.4, $v = |\langle \cos \Delta\Phi_f \rangle|$.

In practive, these reflectivities are set by directly optimizing the correctness and fairness of the protocol. Bob first sets $z = 1/2$ by blocking Alice's signal, and equalizing the detection rates in D_{V_1} and D_{V_2}. This later ensures an optimized interference, and therefore the correctness condition. Then he can tune y such that the detection rate in D_B equals twice the total rate in D_{V_1} and D_{V_2}, which should ensure the fairness condition. Alice then tunes x in order to optimize the interference visibility, which should complete the setting of reflectivities. If v is significantly lower than 1, Alice and Bob might have to perform some mild adjustments on x and y in order to maximize the fairness and correctness.

After performing a protocol, we easily evaluate the reflectivities x, y, z by forcing the switch in state $s = 0$ or $s = 1$, measuring the different detection probabilities and

dividing with the different paths' efficiencies given in Tab. 4.1. We display those experimental reflectivities in Fig. 4.5, for different implementations of the protocol with honest players. We see these reflectivities can deviate from the theoretical predictions derived from the efficiency values. The most plausible explanation is that we might not perfectly set the expected reflectivities in each protocol run. This could happen if the fairness $\mathcal{F}$ and the correctness $\mathcal{C}$ are hardly sensitive to reflectivities around the optimal configuration. Also some undetected errors might have occurred when measuring the efficiencies in Table 4.1, because of some undetected fluctuations, or if we did not perfectly set the reflectivities x, y, z to trivial values when performing that measurement.

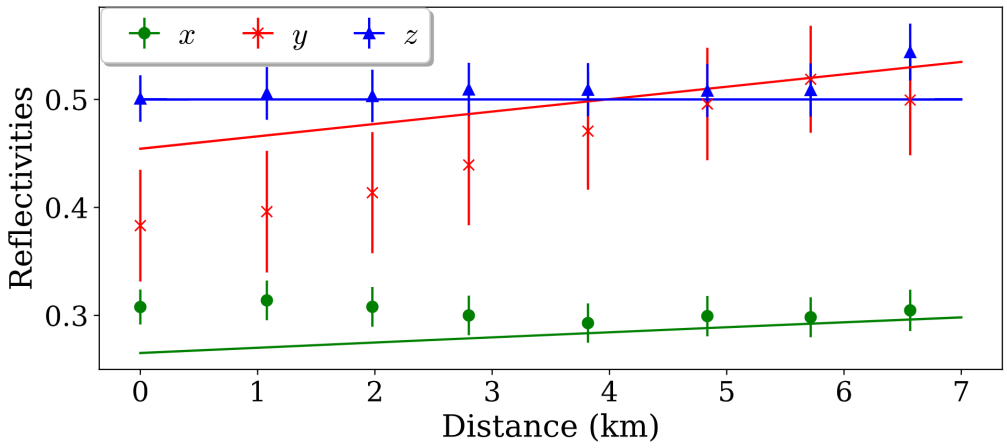


Fig. 4.5: Reflectivities measured in protocols with honest parties, for different communications distances simulated with VOAs. The lines show the prediction from eqs. (4.5) to (4.7), with efficiencies given in Table 4.1, and with additional factors $e^{-0.02L}$ induced by VOAs. The error bars are mainly due to error propagation on the efficiencies.

4.3.2 Protocol Results

For each distance L, we set the VOAs to a transmission $\eta = e^{-0.02L}$, and we optimize the fairness and correctness at each distance by tuning the reflectivities. When these are properly set to values from eqs. (4.5) to (4.7), we obtain the following probabilities for significant events (see appendix C):

$$\mathbb{P}_h\big(\text{Alice wins}\big) = \mathbb{P}_h\big(\text{B. wins}\big) = x_h \eta_A^{V_1}(1+v), \tag{4.8}$$

$$\mathbb{P}_h\big(\text{Bob sanctioned}\big) = 0, \tag{4.9}$$

$$\mathbb{P}_h\big(\text{Alice sanctioned}\big) = x_h \eta_A^{V_2}(1-v). \tag{4.10}$$

Note here the importance of maximizing the interference visibility v so that Alice is not sanctioned while being honest. We continuously run the protocol and record all detection events regardless of the phase difference between the two arms of the interferometer. As if Bob was monitoring the phase difference, we post-select the runs for which the phase spontaneously goes to zero thanks to slow temperature fluctuations, such that the rate in D_{V_2} (which essentially corresponds to the probability of honest Alice being sanctioned) is minimized. In this way, we measure at least 1.5×10^5 valid iterations of the protocol for a 15-minutes run, making the Poisson noise negligible. In Fig. 4.6 we give the probabilities of the different events for several distances.

We notice that the abort probability takes relatively high values, even when we trivially set the communication distance to $L = 0\,\text{km}$. This has to do with important losses, particularly in mating sleeves connecting the numerous optical fiber components, the delay line, or in crystalline components such as the PBSs or the optical switch. Significant improvements could be made, using integrated optics for instance. Other critical features are the single-photon coupling and SNSPD efficiencies. Both of these aspects are being actively studied [146–150] and could see significant improvement in the near future. We also notice that the winning probabilities of Alice and Bob are indeed very close and the probability of an honest party to be sanctioned is minimized.

To further illustrate the performance of our protocol, we show the fairness $\mathcal{F}$ and correctness $\mathcal{C}$ in Fig. 4.7. Thanks to the appropriate tuning of reflectivities x, y, and z, as well as low dark count rates and high visibility, we were able to keep both of these quantities very close to 1, thus approaching the ideal conditions.

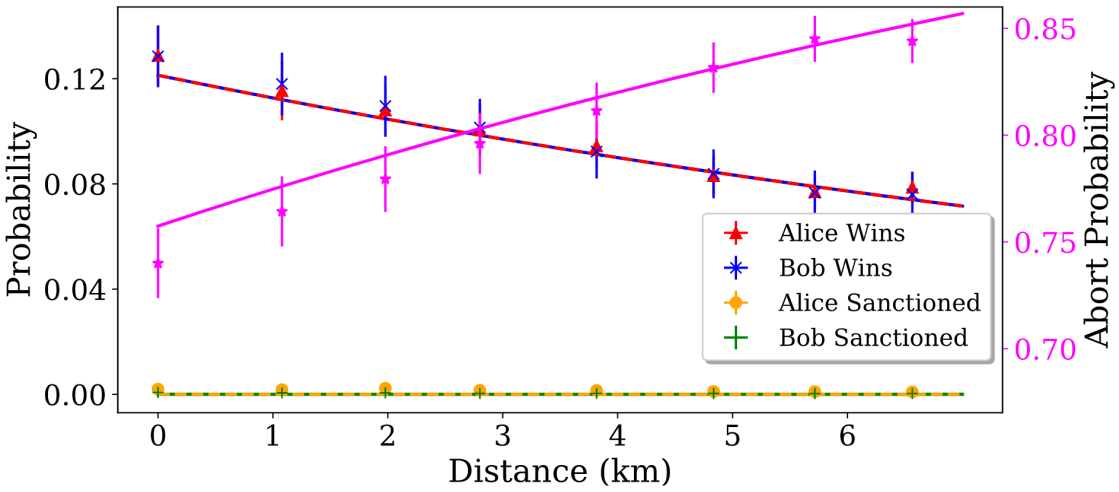


Fig. 4.6: Probability of each outcome of the protocol, measured for different communication distances between Alice and Bob. The abort probability is shown on the right axis, in magenta. The lines represent the theoretical evolution of probabilities, calculated via eqs. (4.5) to (4.10), with efficiencies given in Table 4.1. The error bars are mainly due to error propagation on these efficiencies.

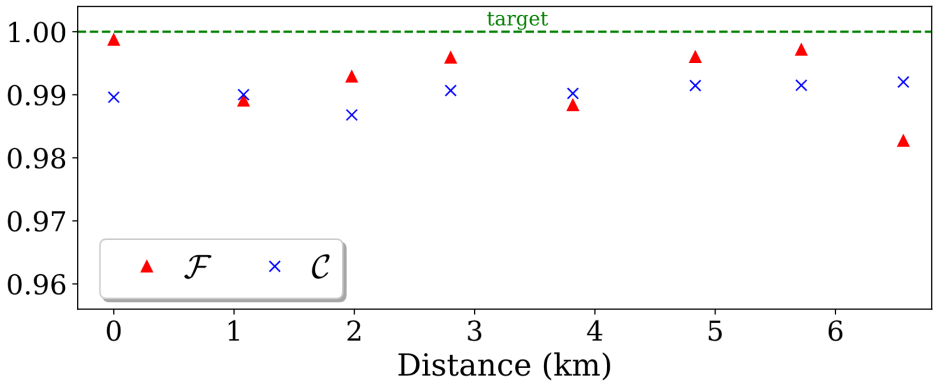


Fig. 4.7: Correctness $\mathcal{C}$ and fairness $\mathcal{F}$ measured in our experimental implementation of the protocol with honest parties, for different communication distances. The dashed line gives the target value for an ideal protocol.

4.4 Results for Dishonest Players

Now we highlight the cheat sensitivity of our protocol, by implementing attacks by dishonest parties. We consider one party to be dishonest, the other one being honest. Firstly, we implement a cheating Bob, and show the dependence of cheat-sensitivity with losses and communication distance. We then implement a cheating Alice, and show how the protocol's cheat sensitivity dissuades her from performing an optimal cheating strategy.

4.4.1 Dishonest Bob

Bob's optimal cheating strategy is quite straightforward, and consists in claiming $b = 1$ regardless of the actual measurement in detector D_B [48]. As Alice is honest she sets the reflectivity $x = x_h$ given in eq. (4.5). When Bob claims $b = 1$ then Alice's switch directs her mode in detector D_A so that she can verify whether Bob is being honest. She then detects a photon with probability:

$$\mathbb{P}(a = 1|\text{Bob cheats}) = x_h \eta_A^s, \tag{4.11}$$

in which case Bob is sanctioned for cheating. Otherwise, Bob wins with probability:

$$\begin{aligned} \mathbb{P}(a = 0|\text{Bob cheats}) &= 1 - \mathbb{P}(a = 1|\text{Bob cheats}) \\ &= 1 - x_h \eta_A^s. \end{aligned} \tag{4.12}$$

In this way, Alice's conditional verification, enabled in our setup by the fast optical switch, allows for a first kind of cheat sensitivity.

In order to illustrate this aspect, we implement Bob's optimal cheating strategy by systematically forcing the switch to send the photon to D_A. We measure the probability of sanctioning Bob for each of the communication distances simulated in the honest case. As displayed in Fig. 4.8, we show experimentally that the probability of sanctioning Bob decreases as communication-induced losses increase, therefore limiting Alice's cheat sensitivity. This gives a substantial advantage to Bob when Alice's arm is particularly lossy. Note that when Bob implements that strategy, only two events are possible, namely Bob winning or Bob being sanctioned; Alice can never win except if the sanction is precisely giving Alice the win (see discussion below).

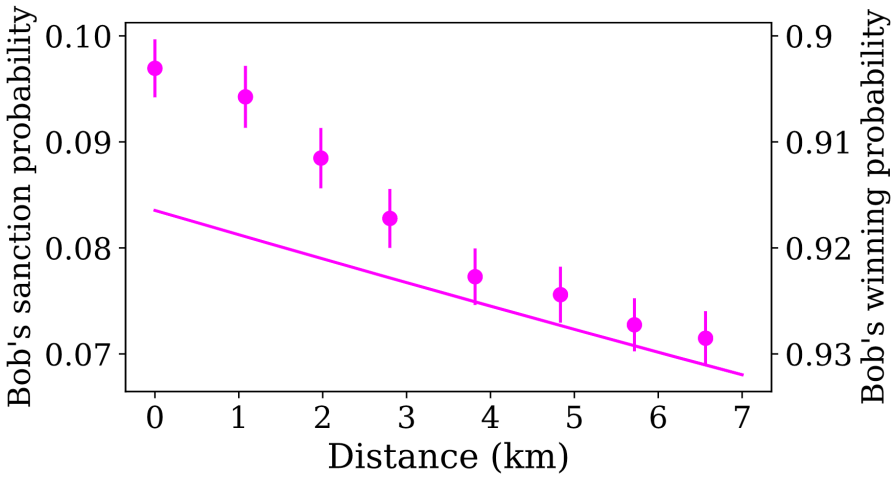


Fig. 4.8: Probabilities of Bob winning or being sanctioned, when he is performing an optimal attack, measured for different communication distances between Alice and Bob. Only one set of points is shown for the two axes, as these two events are complementary. The line is plotted from eqs. (4.11) and (4.12), with η_A^s given in Table 4.1. The error bars are mainly due to error propagation on this efficiency. The observed deviation from the theory is linked to systematic errors when setting the reflectivities.

4.4.2 Dishonest Alice

On the other hand, when Bob is honest and Alice is dishonest, her optimal cheating strategy is less straightforward. In particular, the security proof from [48] does not derive her optimal strategy but rather derives a security bound valid for all strategies. Nevertheless, we can illustrate this scenario using suboptimal strategies by simply tuning the reflectivity x, so that Alice sends the photon to her side with higher probability. Intuitively, without taking the verification setup into account, we can naively expect Alice's winning probability to increase as she increases the reflectivity x. We experimentally perform the protocol for different values of x, all of them higher than the honest value (4.5). In that case, we derive the expected event probabilities (see appendix C for the detailed proof):

$$\mathbb{P}(\text{Alice wins}) = \frac{1}{2}\left(x\eta_A^{V_1} + (1-x)y_h\eta_B^{V_1} + 2v\sqrt{x(1-x)y_h\eta_A^{V_1}\eta_B^{V_1}}\right), \tag{4.13}$$

$$\mathbb{P}(\text{Alice sanctioned}) = \frac{1}{2}\left(x\eta_A^{V_2} + (1-x)y_h\eta_B^{V_2} - 2v\sqrt{x(1-x)y_h\eta_A^{V_2}\eta_B^{V_2}}\right), \tag{4.14}$$

$$\mathbb{P}(\text{Bob wins}) = (1-x)(1-y_h)\eta_B^{y}. \tag{4.15}$$

In Fig. 4.9, we show the probabilities of significant events. Contrary to our naive conjecture, we see that thanks to Bob's verification, and thus cheat sensitivity, Alice does not have a clear interest in forcing $x = 1$, as her winning probability peaks around $x \simeq 0.78$. Alice's interest in cheating actually depends on how deterrent the sanction is. We define a factor $\delta \geq 0$, which quantifies that deterrability, or alternatively how harmful the sanction is for a cheating party. From this parameter we can derive an empirical function that quantifies Alice's interest in cheating:

$$\mathcal{I}_A(\delta) = \frac{\mathbb{P}(\text{A. wins}) - \mathbb{P}(\text{B. wins}) - \delta\mathbb{P}(\text{A. sanctioned})}{\mathbb{P}(\text{A. wins}) + \mathbb{P}(\text{B. wins}) + \delta\mathbb{P}(\text{A. sanctioned})}. \tag{4.16}$$

This function is built such that it can be linked to the fairness (4.3) when taking the appropriate sanction. Indeed, if for $\delta \in [0,1]$ we sanction a cheating Alice by giving the win to Bob with probability δ, then the relation $\mathcal{F} = 1 - |\mathcal{I}_A(\delta)|$ holds. In this way, $\delta = 0$ corresponds to a protocol that simply aborts without sanction when Alice is caught, and $\delta = 1$ gives a protocol that always declares Bob the winner when Alice is caught. Ultimately $\mathcal{I}_A(\delta)$ can be interpreted as a sort of expectation value of a cheating Alice, or a comparison between what she can gain by cheating and what she can lose. In Fig. 4.10 we plot Alice's cheating interest for different values of δ and x. If no sanction is taken ($\delta = 0$), we see that her interest in cheating grows with x. Indeed, even if her winning probability decreases for high values of x, Bob's then approaches zero, such that Alice wins with absolute certainty as long as the protocol does not abort. On the contrary, as the sanction is tightened and the value of δ increases, Alice has less interest in cheating for a given value of x. Furthermore, the value of x that maximizes $\mathcal{I}_A$ also goes down, showing how strengthening the sanction actually forces Alice to adopt a strategy that leaves a chance for Bob to win.

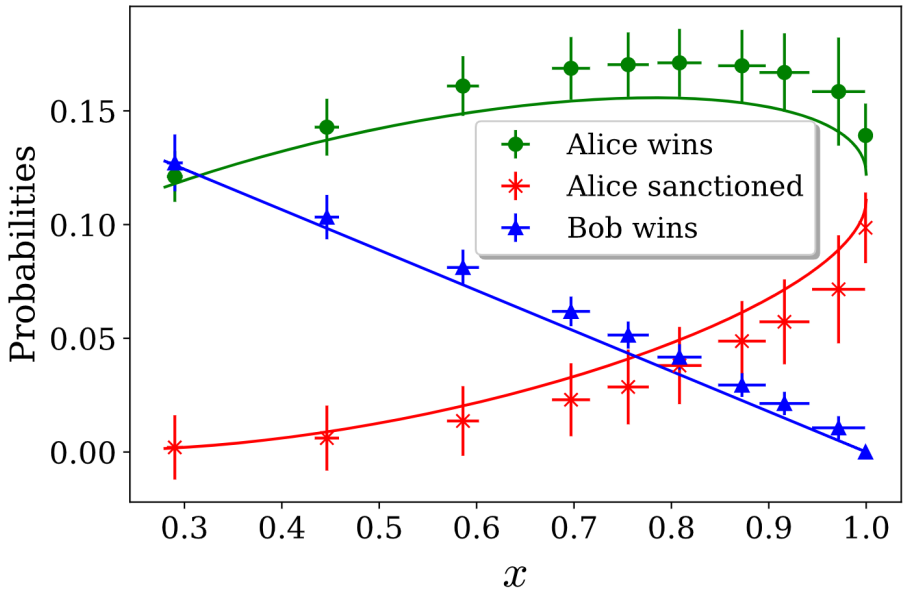


Fig. 4.9: Probabilities of different outcomes measured when Alice cheats, setting different values of x than the honest value. The lines show theoretical predictions, calculated from eqs. (4.13)-(4.16), with efficiencies given in Table 4.1.

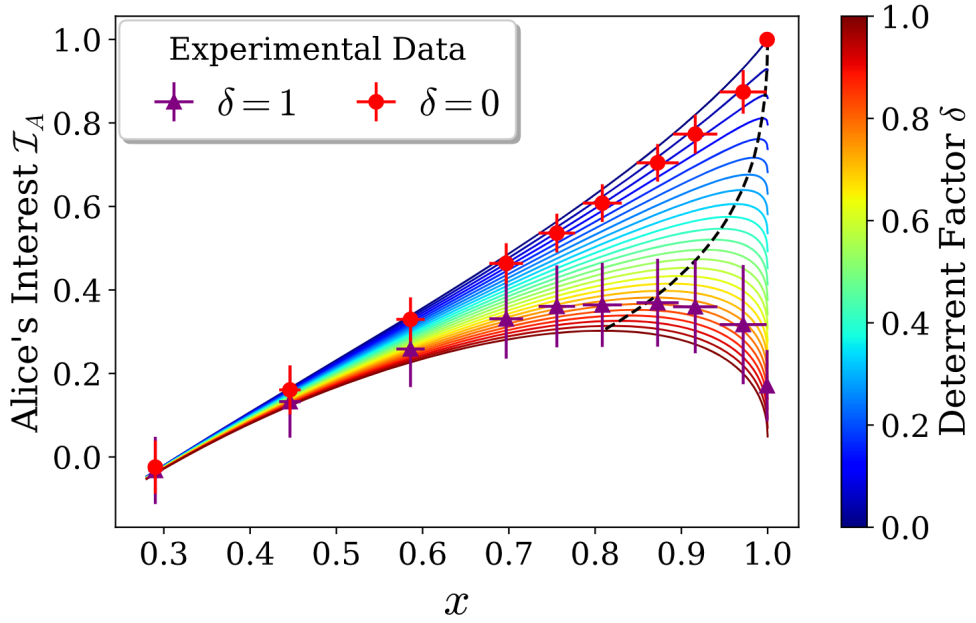


Fig. 4.10: Alice's cheating interest for different deterrent factors δ. The dashed black line indicates the points of maximum interest.

4.4.3 Case of two dishonest parties

Most quantum two-party computation security models do not consider both parties being dishonest at the same time, since security makes sense from the perspective of an honest party willing to protect against a malicious adversary. This threat model is still very general however, as one does not make any assumption on which of the two parties is dishonest: the protocol is therefore always secure for both an honest Alice and an honest Bob. In the case of our protocol however, understanding the double-dishonest scenario is fairly straightforward, and in fact reduces to a fully classical protocol. Since the protocol is designed in such a way that the same party (Bob) always declares the outcome of the flip first (while the verification is then performed by the losing party), Bob cannot win in any other way than declaring himself as the winner. The best that Alice can do is to then stop Bob from winning, claiming that she caught him cheating. Thus, the protocol will always abort, which is a desirable outcome in such a dishonest scenario. The case only becomes a little more complex when one considers sanctioning dishonest aborts. In that case, Bob will always be sanctioned for cheating first, even though Alice was also dishonest.

4.5 Discussion

After refining a previous theoretical proposal for a practical quantum weak coin flipping protocol [48], we were able to perform the first implementation of this protocol by generating a heralded single photon, and entangling it effectively with the vacuum. Thanks to the use of low dark counts SNSPDs, tunable beam splitters and a fast optical switch, while keeping a high visibility in our fibered interferometer, we demonstrated a fair and cheat-sensitive protocol. This last property allows to detect a cheating party with non-negligible probability, which to this day is not accessible to classical protocols.

Note that in order to sanction a dishonest party with high probability, one could systematically sanction the winning party, regardless of their honesty. Thus, in order to display genuine cheat sensitivity, we highlight the primary importance

of the correctness condition, which ensures an honest party is never sanctioned for cheating. This forced us to ignore the balancing of the benefit gained by each party when adopting an optimal cheating strategy, which was previously assessed as a necessary condition for a weak coin flipping protocol [48]. Still, we propose a way of restoring this balance, by using the deterrent factor and interest function introduced in the previous paragraphs.

The balance could indeed arise from choosing different sanctions for Alice and Bob, associated with different deterrent factors δ_A and δ_B, in order to equalize the corresponding interest functions $\mathcal{I}_A(\delta_A)$ and $\mathcal{I}_B(\delta_B)$. A dishonest party who could dramatically increase their winning probability would therefore take a bigger risk of being harshly sanctioned when cheating. Interestingly enough, one could actually set arbitrarily big deterrent factors $\delta > 1$ in order to account for harsher sanctions. We leave the evaluation of these sanctions, deterrent factors and potential alternative interest functions as an interesting game theory open question.

From an experimental perspective, we remark that the robustness to losses in our implementation was illustrated by simulating communication distance with variable optical attenuators. In a practical implementation of the protocol, it would be necessary to maintain a high visibility for a longer interferometer, which could be achieved with active stabilization techniques used in twin-field quantum key distribution implementations for instance [151, 152]. Furthermore, optical implementations of quantum WCF with arbitrarily small biases are yet to be discovered—such implementations would be challenging since they require a rapidly growing number of rounds of communication between the parties [153].

CHAPTER 5

THEORY OF PROBABILISTIC QUANTUM CHANNELS

Transformations undergone by quantum states are oftentimes described by unitary operators, assuming the system is isolated. However, such a formalism cannot describe more general transformations, which may involve interactions with an unknown outside system. For instance, this includes random noise introduced in a photon's polarization state during its propagation in optical fibers. Therefore, quantum channels are more suitable to describe general transformations undergone by a quantum system. In general, deterministic quantum channels are considered, that transform a quantum state with absolute certainty. The behavior of such channels is extensively detailed in quantum theory books [154], and different distances can be used to define a topology on the quantum channels' space [64]. Still, little is known about probabilistic quantum channels, which only operate with a potentially state-dependent probability. These channels describe more accurately experimental situations which involve losses and post-selection. In this chapter, we derive fundamental results related to the behavior and topology of probabilistic quantum channels. These have concrete applications in chapter 6, for deriving the security of our protocols for the certification of quantum communication through an untrusted and lossy quantum channel.

5.1 Preliminary Notions

We first recall the definition of a quantum channel, which gives the sufficient properties for a transformation to send a density operator on another operator:

Definition 5.1 (Quantum Channel)**.** *A quantum channel $\mathcal{E}$ is a convex completely-positive non-trace-increasing (CPnTI) map, meaning:*

1. *Convexity: for any sets of probabilities $\{p_k\}$ with $\sum p_k = 1$ and density operators $\{\rho_k\}$, we have:*
$$\mathcal{E}\Big[\sum_k p_k \rho_k\Big] = \sum_k p_k \mathcal{E}[\rho_k], \tag{5.1}$$
2. *Complete Positivity: for any secondary system of Hilbert space $\mathcal{S}$, $(\mathcal{E}\otimes\mathbb{1}_{\mathcal{S}})[K]$ is positive for any positive operator $K \in \mathcal{L}(\mathcal{H}_i \otimes \mathcal{S})$,*
3. *Non-Trace Increase: For any operator $K \in \mathcal{L}(\mathcal{H}_i)$, we have $\mathrm{Tr}\,\mathcal{E}[K] \leq \mathrm{Tr}\,K$.*

When $\mathcal{E}$ is also trace-preserving (CPTP map), then we have $\mathrm{Tr}\,\mathcal{E}[\rho] = 1$ for any state ρ, so we call $\mathcal{E}$ a *deterministic* or *lossless* quantum channel. Otherwise, if $\mathcal{E}$ is trace-decreasing (CPTD map), then there exists at least one state ρ such that $\mathrm{Tr}\,\mathcal{E}[\rho] < 1$, we call the map a *probabilistic* or *lossy* quantum channel. In that case, the axioms ensure that for any density operator $\rho \in \mathcal{L}(\mathcal{H}_i \otimes \mathcal{S})$, we have $0 \leq \mathrm{Tr}(\mathcal{E}\otimes\mathbb{1}_{\mathcal{S}})[\rho]) \leq 1$. This way, the channel does not operate with absolute certainty, but returns a state only with a certain probability $t(\mathcal{E}|\rho) = \mathrm{Tr}(\mathcal{E}\otimes\mathbb{1}_{\mathcal{S}})[\rho]$, that we call the channel's *transmissivity*. Then for $t(\mathcal{E}|\rho) \neq 0$ we define the output state:

$$\rho_o = (\mathcal{E}\otimes\mathbb{1}_{\mathcal{S}})[\rho]/t(\mathcal{E}|\rho). \tag{5.2}$$

When $t(\mathcal{E}|\rho) = 0$, then no state ever outputs the channel when ρ is the input, so we set $\rho_o = \mathbb{1}/\dim(\mathcal{H}_o \otimes \mathcal{S})$ by convention.

Theorem 5.1 (Kraus' Theorem)**.** *The map $\mathcal{E} : \mathcal{L}(\mathcal{H}_i) \longrightarrow \mathcal{L}(\mathcal{H}_o)$ is a quantum channel if and only if there exists a set of operators $\{\hat{K}_j\}$, each mapping $\mathcal{H}_i$ to $\mathcal{H}_o$, such that $\sum_j \hat{K}_j^\dagger \hat{K}_j \leq \mathbb{1}$ and:*
$$\mathcal{E}[\rho_i] = \sum_j \hat{K}_j \rho_i \hat{K}_j^\dagger. \tag{5.3}$$
$\mathcal{E}$ is a deterministic quantum channel when this condition holds and $\sum_j \hat{K}_j^\dagger \hat{K}_j = \mathbb{1}$. When $\sum_j \hat{K}_j^\dagger \hat{K}_j < \mathbb{1}$, the channel is probabilistic.

This theorem gives an operator-sum representation for quantum channels, which will be most useful in the following. The operators $\{\hat{K}_j\}$ are called *Kraus' operators* of the channel $\mathcal{E}$, which are not unique in general.

Quantum channels are fundamental objects that describe any transformation undergone by a quantum state. Still, most studies focus on lossless quantum channels *i.e.* CPTP maps, such that any state passes the channel with absolute certainty. In theory, any situation involving a lossy channel can be described by considering a CPTP map $\mathcal{E}[\bullet] = \mathcal{E}_s[\bullet] \otimes |s\rangle\langle s| + \mathcal{E}_f[\bullet] \otimes |f\rangle\langle f|$, with $\mathcal{E}_s$ the *successful* branch and $\mathcal{E}_f$ the *failure* branch, where the state might be considered as lost. However in most experimental situations, we generally have no access to the state when it goes through the failure branch, such that we are only interested in states sent through the success branch. This means we *post-select* states on the success branch, and we only consider the probabilistic channel $\mathcal{E}_s[\rho] = \langle s|\mathcal{E}[\rho]|s\rangle$. The transmissivity is then the probability that the channel successfully outputs the input state, so that $t(\mathcal{E}_s|\rho) = \mathrm{Tr}\,\mathcal{E}_s[\rho] = \mathrm{Tr}(\mathcal{E}[\rho]\mathbb{1} \otimes |s\rangle\langle s|)$. This way, losses are included in the expression of the channel itself.

Finally we give a few common examples of probabilistic quantum channels. A trivial probabilistic quantum channel is $\mathcal{E} = p \cdot \mathbb{1}$ with $p \in]0;1]$, that models unbiased losses. In that case the state is simply transmitted without transformation with probability p, or lost with probability $1-p$. On the contrary, a channel with fully-biased losses would be a polarizing channel $\mathcal{P}$, with $\mathcal{P}[\rho] = |\Phi\rangle\langle\Phi|\rho|\Phi\rangle\langle\Phi|$ for any state ρ, with $|\Phi\rangle$ a pure state. In that case $t(\mathcal{P}|\rho) = 1$ if and only if $\rho = |\Phi\rangle\langle\Phi|$. Finally, probabilistic channels allow us to describe an experiment where one wishes to measure a POVM $\{\hat{M}_k\}_{1\leq k\leq d}$ but only has access to the first m elements, with $m < d$. In that case we can define the following channel:

$$\mathcal{E}[\rho] = \sum_{i=1}^{m} \hat{M}_k \rho \hat{M}_k^\dagger \otimes |k\rangle\langle k|. \tag{5.4}$$

This example is of particular use for Bell state measurements using linear optics, where it was shown that one can measure only two elements out of four [155].

5.2 Extended Process Inequality

A well-known result of deterministic quantum channels is the *process inequality*, also known as monotonicity of fidelity and trace-distance under application of a quantum channel:

$$F(\mathcal{E}[\rho],\mathcal{E}[\sigma]) \geq F(\rho,\sigma), \tag{5.5}$$

$$D(\mathcal{E}[\rho],\mathcal{E}[\sigma]) \leq D(\rho,\sigma), \tag{5.6}$$

where F is the fidelity and D is the trace-distance, defined in paragraph 2.1.5, and the inequalities are true for any quantum states ρ,σ and quantum channel $\mathcal{E}$. These inequalities ensure that no quantum process can increase the probability of distinguishing two quantum states. We provide an extension of this result to probabilistic quantum channels:

Theorem 5.2 (Extended Processing Inequality)**.** *Let $\mathcal{E}$ be probabilistic quantum channel (CPTD). For any input states ρ_i and σ_i, the following inequality holds for the sine distance $C(\rho,\sigma)=\sqrt{1-F(\rho,\sigma)}$, and the trace distance D:*

$$C(\rho_i,\sigma_i) \geq t\cdot C(\rho_o,\sigma_o), \tag{5.7}$$

$$D(\rho_i,\sigma_i) \geq t\cdot D(\rho_o,\sigma_o), \tag{5.8}$$

where $\rho_o=\mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ and $\sigma_o=\mathcal{E}[\sigma_i]/t(\mathcal{E}|\sigma_i)$ are the output states of the channel, and $t=t(\mathcal{E}|\rho_i)$ or $t=t(\mathcal{E}|\sigma_i)$ is the channel's transmissivity.

Proof. Let us first prove the inequality for the trace distance D. We follow the guidelines of the demonstration given in [154] for CPTP maps. As ρ_i and σ_i have a symmetric role, let us consider $t(\mathcal{E}|\rho_i)\geq t(\mathcal{E}|\sigma_i)$, without loss of generality. We can define two Hermitian positive matrices P and Q with orthogonal support such that $\rho_i-\sigma_i=P-Q$. Therefore, we have $\mathrm{Tr}(P)-\mathrm{Tr}(Q)=\mathrm{Tr}(\rho_i)-\mathrm{Tr}(\sigma_i)=0$ so $\mathrm{Tr}(P)=\mathrm{Tr}(Q)$. Moreover, $|\rho_i-\sigma_i|=P+Q$. This way we get:

$$\begin{aligned} D(\rho_i,\sigma_i) &= \frac{1}{2}\mathrm{Tr}\,|\rho_i-\sigma_i| \\ &= \frac{1}{2}\big(\mathrm{Tr}(P)+\mathrm{Tr}(Q)\big)=\mathrm{Tr}(P). \end{aligned} \tag{5.9}$$

There also exists a projector Π such that $D(\rho_o,\sigma_o) = \mathrm{Tr}\big(\Pi\cdot(\rho_o-\sigma_o)\big)$. Keeping in mind that $\mathcal{E}$ is trace-decreasing, it follows that for any $t \le t(\mathcal{E}|\rho_i)$:

$$\begin{aligned}
D(\rho_i,\sigma_i) &= \mathrm{Tr}(P)\\
&\ge \mathrm{Tr}(\mathcal{E}[P])\\
&\ge \mathrm{Tr}(\Pi\cdot\mathcal{E}[P])\\
&\ge \mathrm{Tr}\big(\Pi\cdot(\mathcal{E}[P]-\mathcal{E}[Q])\big)\\
&= \mathrm{Tr}\big(\Pi\cdot(\mathcal{E}[\rho_i]-\mathcal{E}[\sigma_i])\big)\\
&= t(\mathcal{E}|\rho_i)\mathrm{Tr}(\Pi\rho_o) - t(\mathcal{E}|\sigma_i)\mathrm{Tr}(\Pi\sigma_o)\\
&\ge t(\mathcal{E}|\rho_i)\mathrm{Tr}\big(\Pi\cdot(\rho_o-\sigma_o)\big)\\
&= t(\mathcal{E}|\rho_i)\cdot D(\rho_o,\sigma_o)\\
&\ge t\cdot D(\rho_o,\sigma_o). \qquad (5.10)
\end{aligned}$$

This way, we have in particular $D(\rho_i,\sigma_i) \ge t\cdot D(\rho_o,\sigma_o)$ for $t = t(\mathcal{E}|\rho_i)$ or $t = t(\mathcal{E}|\sigma_i)$.

In order to prove the same inequality for the sine distance C, let us recall we can express that distance between any density operators ρ,σ as a minimization over their purifications $|r\rangle$ and $|s\rangle$ respectively:

$$C(\rho,\sigma) = \min_{|r\rangle,|s\rangle}\sqrt{1-\langle r|s\rangle} = \min_{|r\rangle,|s\rangle} D(|r\rangle\langle r|,|s\rangle\langle s|), \qquad (5.11)$$

where the minimization is taken over all the purifications. This way, we purify the input and output states in order to extend the inequality from D to C. Let us choose two pure states $|r_i\rangle,|s_i\rangle \in \mathscr{H}_i\otimes\mathscr{P}$ such that $C(\rho_i,\sigma_i) = D(|r_i\rangle\langle r_i|,|s_i\rangle\langle s_i|)$, with $\mathscr{P}$ a purification space for ρ_i and σ_i. This purifies the input states. Now let us define the operator $\hat{E}$ on $\mathscr{H}_i\otimes\mathscr{P}$ such that for any pure state $|\psi\rangle$ in that space:

$$\hat{E}|\psi\rangle = \sum_j (\hat{K}_j\otimes\mathbb{1}_{\mathscr{P}}|\psi\rangle)\otimes|e_j\rangle, \qquad (5.12)$$

where $\{\hat{K}_j\}$ are Kraus operators for $\mathcal{E}$ and $\{|e_j\rangle\}$ is an orthonormal basis of an ancillary space $\mathscr{A}$. As $\mathcal{E}$ is trace-decreasing, $\hat{E}|\psi\rangle$ is not necessarily normalized, but is a pure state when renormalized. This way, we can define the quantum operation $\tilde{\mathcal{E}}$ such that for any density operator $\rho\in\mathscr{L}(\mathscr{H}_i)\otimes\mathscr{L}(\mathscr{P})$, we have $\tilde{\mathcal{E}}[\rho] = \hat{E}\rho\hat{E}^\dagger$. This operation conserves the purity of pure states, and verifies $\mathrm{Tr}_{\mathscr{A}}(\tilde{\mathcal{E}}[\rho]) = \mathcal{E}[\rho]$

for any density operator ρ. This way, $\tilde{\mathcal{E}}[|r\rangle\langle r|]/t(\mathcal{E}|\rho_i)$, resp. $\tilde{\mathcal{E}}[|s\rangle\langle s|]/t(\mathcal{E}|\sigma_i)$, is a purification of $\mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)=\rho_o$, resp. $\mathcal{E}[\sigma_i]/t(\mathcal{E}|\sigma_i)=\sigma_o$. This purifies the output states. Now we only have to apply the extended contractivity of D to the purified states under the quantum operation $\tilde{\mathcal{E}}$, for $t=t(\mathcal{E}|\rho_i)$ or $t=t(\mathcal{E}|\sigma_i)$:

$$\begin{aligned} C(\rho_i,\sigma_i) &= D(|r_i\rangle\langle r_i|,|s_i\rangle\langle s_i|) \\ &\geq t\cdot D(\tilde{\mathcal{E}}[|r\rangle\langle r|]/t(\mathcal{E}|\rho_i),\tilde{\mathcal{E}}[|s\rangle\langle s|]/t(\mathcal{E}|\sigma_i)) \\ &\geq t\cdot \min_{|r_o\rangle,|s_o\rangle} D(|r_o\rangle\langle r_o|,|s_o\rangle\langle s_o|) \\ &= t\cdot C(\hat{\rho}_o,\hat{\sigma}_o), \end{aligned} \tag{5.13}$$

where the minimization is taken over all purifications $|r_o\rangle,|s_o\rangle$, of ρ_o,σ_o, respectively. This shows the inequality for the sine distance. ■

Note that our theorem is valid also for a trace-preserving quantum operation. Indeed, when $t(\mathcal{E}|\rho)=1$ for any state ρ, we get the well known processing inequality $D(\rho,\sigma)\geq D(\mathcal{E}[\rho],\mathcal{E}[\sigma])$ or $F(\rho,\sigma)\leq F(\mathcal{E}[\rho],\mathcal{E}[\sigma])$. This indicates that our inequality is tight.

5.3 Topology of Quantum Channels

In the following we intend to construct different metrics on probabilistic channels, and derive important properties of these metrics. We first recall different functions allowing to evaluate the closeness of deterministic quantum channels. We can derive some first functions from the Choi-Jamiołkowski isomorphism [156, 157] between quantum states and channel:

$$J:\mathcal{E}\longrightarrow\rho_{\mathcal{E}}=(\mathcal{E}\otimes\mathbb{1})[\Phi_+], \tag{5.14}$$

where $|\Phi_+\rangle=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle|i\rangle$ is the maximally entangled states on $\mathscr{H}^{\otimes 2}$, $d=\dim\mathscr{H}$ and $\mathscr{H}$ is the Hilbert space $\mathcal{E}$ acts upon. This way, we define the Choi-Jamiołkowski fidelity and trace distance:

$$\mathcal{F}_J(\mathcal{E}_1,\mathcal{E}_2)=F(\rho_{\mathcal{E}_1},\rho_{\mathcal{E}_2})=F\big((\mathcal{E}_1\otimes\mathbb{1})[\Phi_+],(\mathcal{E}_2\otimes\mathbb{1})[\Phi_+]\big), \tag{5.15}$$

$$\mathcal{D}_J(\mathcal{E}_1,\mathcal{E}_2)=D(\rho_{\mathcal{E}_1},\rho_{\mathcal{E}_2})=D\big((\mathcal{E}_1\otimes\mathbb{1})[\Phi_+],(\mathcal{E}_2\otimes\mathbb{1})[\Phi_+]\big). \tag{5.16}$$

One can also define the Choi-Jamiołkowski sine distance $\mathcal{C}_J = \sqrt{1-\mathcal{F}_J}$ and angle $\mathcal{A}_J = \arccos\sqrt{\mathcal{F}_J}$. All these functions relate to the average behavior of quantum channels [64]. In quantum cryptography, we are generally more interested in the worst case scenario, in which case we favor the diamond fidelity and trace distance:

$$\mathcal{F}_\diamond(\mathcal{E}_1,\mathcal{E}_2) = \min_\rho F\big((\mathcal{E}_1\otimes\mathbb{1})[\rho],(\mathcal{E}_2\otimes\mathbb{1})[\rho]\big), \tag{5.17}$$

$$\mathcal{D}_\diamond(\mathcal{E}_1,\mathcal{E}_2) = \max_\rho D\big((\mathcal{E}_1\otimes\mathbb{1})[\rho],(\mathcal{E}_2\otimes\mathbb{1})[\rho]\big), \tag{5.18}$$

where the maximization and minimization are carried out over pure states of $\mathscr{H}^{\otimes 2}$. We also define the diamond sine distance $\mathcal{C}_\diamond = \sqrt{1-\mathcal{F}_\diamond}$ and angle $\mathcal{A}_\diamond = \arccos\sqrt{\mathcal{F}_\diamond}$. The diamond fidelity and distances are generally harder to evaluate than their Choi-Jamiołkwoski counterparts, which is why we try to link these functions together, possibly via some equivalence bounds, as attempted in [25]. In this section, we extend those closeness functions to probabilistic channels, and derive some important equivalence bounds between them.

5.3.1 Equivalence Classes of Quantum Channels

Let us first consider two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ that are proportional to each other, *i.e.* there exists a factor $p \in]0;1]$ such that $\mathcal{E}_1 = p\cdot\mathcal{E}_2$ (or $\mathcal{E}_2 = p\cdot\mathcal{E}_1$ which is a symmetric case). Then their corresponding transmissivities also display the same proportionality $t(\mathcal{E}_1|\rho) = p\cdot t(\mathcal{E}_2|\rho)$ for any input state ρ. The two channels therefore output the same states when fed the same input state:

$$\frac{\mathcal{E}_1[\rho]}{t(\mathcal{E}_1|\rho)} = \frac{p\cdot\mathcal{E}_2[\rho]}{p\cdot t(\mathcal{E}_2|\rho)} = \frac{\mathcal{E}_2[\rho]}{t(\mathcal{E}_2|\rho)}. \tag{5.19}$$

In numerous practical situations we only consider what happens when the states are not lost, such that we post-select on the states being detected. This way, two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ that are proportional to each other actually describe the same physical situation, and we consider them as equivalent $\mathcal{E}_1 \equiv \mathcal{E}_2$. This defines mathematical equivalence classes of channels that output the same quantum states. All channels from a same class can be compared, such that if $\mathcal{E}_1 \equiv \mathcal{E}_2$, then either $\mathcal{E}_1 \geq \mathcal{E}_2$ or $\mathcal{E}_2 \geq \mathcal{E}_1$. In the first case, for instance, we have $t(\mathcal{E}_1|\rho) \geq t(\mathcal{E}_2|\rho)$. For any class of channel, we can find a maximal channel of that class $\mathcal{E}_{\max}$ such that

$\mathcal{E}_{\max} \geq \mathcal{E}$ for any channel $\mathcal{E}$ of the same class. That maximal channel is therefore the most transmissive channel, and there always exists a state ρ on which the channel operates with absolute certainty, *i.e.* $t(\mathcal{E}_{\max}|\rho) = 1$.

In the following, we will use these equivalence classes in order to define proper closeness functions on probabilistic quantum channels, with convenient physical interpretations. In addition, these classes also embody the fact that when certifying a channel $\mathcal{E}$, one can always consider a more transmissive but equivalent channel $\mathcal{E}'$, with $\mathcal{E}' \geq \mathcal{E}$ and $\mathcal{E}' \equiv \mathcal{E}$. We can then use this more transmissive channel in order to describe the physical process, which falls down to assuming a certain amount of losses are known and unbiased.

5.3.2 Closeness of Probabilistic Quantum Channels

We can finally extend the previously defined closeness functions of deterministic channels to probabilistic channels:

Definition 5.2 (Closeness of Probabilistic Quantum Channels)**.** *We define the Choi-Jamiołkowski fidelity and trace distance between two probabilistic quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$:*

$$\mathcal{F}_J(\mathcal{E}_1, \mathcal{E}_2) = F\big((\mathcal{E}_1 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_1|\Phi_+), (\mathcal{E}_2 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)\big), \tag{5.20}$$

$$\mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2) = D\big((\mathcal{E}_1 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_1|\Phi_+), (\mathcal{E}_2 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)\big), \tag{5.21}$$

and the associated Choi-Jamiołkowski sine distance $\mathcal{C}_J = \sqrt{1 - \mathcal{F}_J}$ and angle $\mathcal{A}_J = \arccos\sqrt{\mathcal{F}_J}$. We also define the diamond fidelity and trace distance:

$$\mathcal{F}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \min_\rho F\big((\mathcal{E}_1 \otimes \mathbb{1})[\rho]/t(\mathcal{E}_1|\rho), (\mathcal{E}_2 \otimes \mathbb{1})[\rho]/t(\mathcal{E}_2|\rho)\big), \tag{5.22}$$

$$\mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \max_\rho D\big((\mathcal{E}_1 \otimes \mathbb{1})[\rho]/t(\mathcal{E}_1|\rho), (\mathcal{E}_2 \otimes \mathbb{1})[\rho]/t(\mathcal{E}_2|\rho)\big), \tag{5.23}$$

where the maximization and minimization are carried out over pure states of $\mathcal{H}^{\otimes 2}$, and the associated diamond sine distance $\mathcal{C}_\diamond = \sqrt{1 - \mathcal{F}_\diamond}$ and angle $\mathcal{A}_\diamond = \arccos\sqrt{\mathcal{F}_\diamond}$.

None of these quantities are strictly speaking distances of probabilistic channels. Indeed with $\mathcal{M}$ any of the Choi-Jamiołkowski or diamond distances, we can have $\mathcal{M}(\mathcal{E}_1,\mathcal{E}_2)=0$, but still $\mathcal{E}_1\neq\mathcal{E}_2$, on the condition that $\mathcal{E}_1=p\cdot\mathcal{E}_2$ or $\mathcal{E}_2=p\cdot\mathcal{E}_1$ with $p>0$. However, we prove that $\mathcal{M}(\mathcal{E}_1,\mathcal{E}_2)=0$ if and only if $\mathcal{E}_1\equiv\mathcal{E}_2$ and the channels are equivalent, meaning they are proportional to each other. This shows the Choi-Jamiołkowski or diamond distances are proper distances for equivalence classes of probabilistic quantum channels.

Proof. For all the proof, $\mathcal{M}$ stands for any of the channel distances $\mathcal{A}$, $\mathcal{C}$ or $\mathcal{D}$, the subscript standing for the Choi-Jamiołkowski or diamond version. If $\mathcal{E}_1\equiv\mathcal{E}_2$, then there exists $p\in]0;1]$ such that $\mathcal{E}_1=p\cdot\mathcal{E}_2$ or $\mathcal{E}_2=p\cdot\mathcal{E}_1$. Then by definition of $\mathcal{M}_\diamond$ and $\mathcal{M}_J$, we trivially have $\mathcal{M}_\diamond(\mathcal{E}_1,\mathcal{E}_2)=\mathcal{M}_J(\mathcal{E}_1,\mathcal{E}_2)=0$. Now let us assume $\mathcal{E}_1$ and $\mathcal{E}_2$ are non-zero channels such that $\mathcal{M}_J(\mathcal{E}_1,\mathcal{E}_2)=0$, and let us show that $\mathcal{E}_1\equiv\mathcal{E}_2$. First, we show the following lemma, introduced in [25]:

Lemma 5.1. *Let $|\psi\rangle\in\mathscr{H}^{\otimes 2}$ be a pure 2-qudits state, with $\dim\mathscr{H}=d$. Then there exists an operator $\hat{K}_\psi=\hat{M}_\psi\hat{U}_\psi$ on $\mathscr{H}$, with $0<\hat{M}_\psi\leq\mathbb{1}$ and $\hat{U}_\psi$ a unitary, such $\mathbb{1}\otimes\hat{K}_\psi$ transforms the maximally-entangled state $|\Phi_+\rangle=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle|i\rangle$ into $|\psi\rangle$ with probability $1/d$, i.e.:*

$$(\mathbb{1}\otimes\hat{K}_\psi)|\Phi_+\rangle=\frac{1}{\sqrt{d}}|\psi\rangle. \tag{5.24}$$

To show this lemma we use the Schmidt decomposition of $|\psi\rangle$:

$$|\psi\rangle=\sum_{i=0}^{d-1}\psi_i|i\rangle|i'\rangle, \tag{5.25}$$

where $\{|i\rangle\}$ and $\{|i'\rangle\}$ are two orthonormal bases of $\mathscr{H}$. There exists a unitary operator $\hat{U}_\psi$ acting on $\mathscr{H}$ such that:

$$(\mathbb{1}\otimes\hat{U}_\psi)|\Phi_+\rangle=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle|i'\rangle, \tag{5.26}$$

with $d=\dim\mathscr{H}$. We can then define the operator $\hat{M}_\psi$ that probabilistically transforms $(\mathbb{1}\otimes\hat{U}_\psi)|\Phi_+\rangle$ into $|\psi\rangle$:

$$\hat{M}_\psi=\sum_{i=0}^{d-1}\psi_i|i'\rangle\langle i'|. \tag{5.27}$$

Now by we defining the operator $\hat{K}_\psi = \hat{M}_\psi \hat{U}_\psi$, we have:

$$(\mathbb{1} \otimes \hat{K}_\psi)|\Phi_+\rangle = \frac{1}{\sqrt{d}}|\psi\rangle, \tag{5.28}$$

which completes the proof of the lemma.

From here, as we have $\mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2) = 0$, then we have

$$M\big((\mathcal{E}_1 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_1|\Phi_+), (\mathcal{E}_2 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)\big) = 0, \tag{5.29}$$

where $M = A, C$ or D, so the states in the distance are equal:

$$(\mathcal{E}_1 \otimes \mathbb{1})[\Phi_+] = \frac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)} \cdot (\mathcal{E}_2 \otimes \mathbb{1})[\Phi_+]. \tag{5.30}$$

For any pure state $|\psi\rangle \in \mathscr{H}^{\otimes 2}$ we define the operator $\hat{K}_\psi$ from Lemma 5.1, such that $(\mathbb{1} \otimes \hat{K}_\psi)|\Phi_+\rangle = \frac{1}{\sqrt{d}}|\psi\rangle$. We apply that operator on both sides of equation (5.30):

$$(\mathbb{1} \otimes \hat{K}_\psi)(\mathcal{E}_1 \otimes \mathbb{1})[\Phi_+](\mathbb{1} \otimes \hat{K}_\psi^\dagger) = \frac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)} \cdot (\mathbb{1} \otimes \hat{K}_\psi)(\mathcal{E}_2 \otimes \mathbb{1})[\Phi_+](\mathbb{1} \otimes \hat{K}_\psi^\dagger), \tag{5.31}$$

which, since $\mathbb{1} \otimes \hat{K}_\psi$ commutes with $\mathcal{E}_1 \otimes \mathbb{1}$ and $\mathcal{E}_2 \otimes \mathbb{1}$, implies:

$$(\mathcal{E}_1 \otimes \mathbb{1})\Big[(\mathbb{1} \otimes \hat{K}_\psi)\Phi_+(\mathbb{1} \otimes \hat{K}_\psi^\dagger)\Big] = \frac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)} \cdot (\mathcal{E}_2 \otimes \mathbb{1})\Big[(\mathbb{1} \otimes \hat{K}_\psi)\Phi_+(\mathbb{1} \otimes \hat{K}_\psi^\dagger)\Big], \tag{5.32}$$

or equivalently:

$$(\mathcal{E}_1 \otimes \mathbb{1})[\psi] = \frac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)} \cdot (\mathcal{E}_2 \otimes \mathbb{1})[\psi]. \tag{5.33}$$

This way, taking either $p = \frac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)}$ or $p = \frac{t(\mathcal{E}_2|\Phi_+)}{t(\mathcal{E}_1|\Phi_+)}$ we get $(\mathcal{E}_1 \otimes \mathbb{1})[\psi] = p \cdot (\mathcal{E}_2 \otimes \mathbb{1})[\psi]$ or $(\mathcal{E}_2 \otimes \mathbb{1})[\psi] = p \cdot (\mathcal{E}_1 \otimes \mathbb{1})[\psi]$ for all state $|\psi\rangle \in \mathscr{H}^{\otimes 2}$, with $p \in]0;1]$. This gives either $\mathcal{E}_1 = p \cdot \mathcal{E}_2$ or $\mathcal{E}_2 = p \cdot \mathcal{E}_1$, and therefore $\mathcal{E}_1 \equiv \mathcal{E}_2$. This prooves the result for the Choi-Jamiołkowski distances. For diamond distances, we straightforwardly get the same result, as we always have $\mathcal{M}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \geq \mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2)$.

The triangular inequality and symmetry of $\mathcal{M}_J$ and $\mathcal{M}_\diamond$ come trivially from the distance properties of A, C and D. Therefore, $\mathcal{M}_J$ and $\mathcal{M}_\diamond$ define proper distances on classes of non-zero probabilistic channels. ■

Note that from the sine or angle channel distances, we also deduce that the $\mathcal{F}_J(\mathcal{E}_1, \mathcal{E}_2) = \mathcal{F}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = 1$ if and only if $\mathcal{E}_1 \equiv \mathcal{E}_2$.

5.3.3 Comparison of Quantum Channels Distances

Choi-Jamiołkowski and diamond metrics underline different properties of quantum channels. As pointed out in [64], the Choi-Jamiołkowki metrics are linked to average probability of distinguishing two quantum channels when sending unknown states, while the diamond metrics are linked to the maximum probability of distinguishing these channels. Here we show the equivalence of Choi-Jamiołkowski metrics and their diamond counterpart, which allows to get some information on the channel's behavior in the worst-case scenario, based on the sole knowledge of its action on a maximally-entangled state. We mention that an attempt to show such bounds was done in [25], linking the diamond trace distance with the Choi-Jamiołkowski sine distance. However, it does not give a direct bound on the diamond fidelity, which is more suitable in cryptography in order to evaluate a protocol's success probability.

Theorem 5.3 (Channels' Metrics Equivalence)**.** *For any probabilistic channel $\mathcal{E}_1$, and any $\mathcal{E}_2$ that is proportional to a deterministic channel (CPTP map), both acting on $\mathscr{L}(\mathscr{H})$, the following inequalities hold:*

$$\mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2) \leq \mathcal{C}_\diamond(\mathcal{E}_1,\mathcal{E}_2) \leq \dim\mathcal{H} \times \mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2), \tag{5.34}$$

$$\mathcal{D}_J(\mathcal{E}_1,\mathcal{E}_2) \leq \mathcal{D}_\diamond(\mathcal{E}_1,\mathcal{E}_2) \leq \dim\mathcal{H} \times \mathcal{D}_J(\mathcal{E}_1,\mathcal{E}_2). \tag{5.35}$$

Proof. The left-side inequalities are straightforwardly following from the definition of the distances. The right-side inequalities come from the following lemma:

Lemma 5.2. *For any pure state $\rho \in \mathscr{L}(\mathscr{H}^{\otimes 2})$ and any pair of probabilistic quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$ both acting on $\mathscr{L}(\mathscr{H})$ we have:*

$$x \cdot D(\rho_1,\rho_2) \leq \dim\mathcal{H} \times \mathcal{D}_J(\mathcal{E}_1,\mathcal{E}_2), \tag{5.36}$$

$$x \cdot C(\rho_1,\rho_2) \leq \dim\mathcal{H} \times \mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2), \tag{5.37}$$

for any $x \leq \max\left[\frac{t(\mathcal{E}_1|\rho)}{t(\mathcal{E}_1|\Phi_+)}, \frac{t(\mathcal{E}_2|\rho)}{t(\mathcal{E}_2|\Phi_+)}\right]$, and with $\rho_k = (\mathcal{E}_k \otimes \mathbb{1})[\rho]/t(\mathcal{E}_k|\rho)$.

Let us proove the lemma. We consider a pure state $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \mathscr{H}^{\otimes 2}$, and two probabilistic channels $\mathcal{E}_1$ and $\mathcal{E}_2$. We define the corresponding transmissivities $t(\mathcal{E}_k|\rho)$ and output states $\rho_k = (\mathcal{E}_k \otimes \mathbb{1})[\rho]/t(\mathcal{E}_k|\rho)$ for $k = 1$ and 2. Using the operator $\hat{K}_\psi$ defined in Lemma 5.1, the map $\mathcal{O}$ defined as $\mathcal{O}[\rho] = \hat{K}_\psi \rho \hat{K}_\psi^\dagger$ is a valid quantum operation on $\mathscr{L}(\mathscr{H})$. Furthermore, $\mathbb{1} \otimes \mathcal{O}$ transforms $|\Phi_+\rangle$ into $|\psi\rangle$ with probability $1/\dim\mathscr{H}$, and commutes with the channels $\mathcal{E}_1 \otimes \mathbb{1}$ and $\mathcal{E}_2 \otimes \mathbb{1}$, such that for $k = 1$ or 2 and $d = \dim\mathscr{H}$:

$$(\mathbb{1} \otimes \mathcal{O})[(\mathcal{E}_k \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_k|\Phi_+)] = \tfrac{1}{d \cdot t(\mathcal{E}_k|\Phi_+)}(\mathcal{E}_k \otimes \mathbb{1})[\rho] \tag{5.38}$$

$$= \tfrac{t(\mathcal{E}_k|\rho)}{d \cdot t(\mathcal{E}_k|\Phi_+)}\rho_k. \tag{5.39}$$

This way, $\mathbb{1} \otimes \mathcal{O}$ transforms the state $(\mathcal{E}_k \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_k|\Phi_+)$ into ρ_k, with probability $\frac{t(\mathcal{E}_k|\rho)}{d \cdot t(\mathcal{E}_k|\Phi_+)}$. This way, using Lemma 5.2 for extented metrics monotonicity to the quantum operation $\mathcal{O} \otimes \mathbb{1}$, we deduce the following inequality:

$$M\big((\mathcal{E}_1 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_1|\Phi_+), (\mathcal{E}_2 \otimes \mathbb{1})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)\big) \geq t \cdot M(\rho_1, \rho_2), \tag{5.40}$$

for any $t \leq \max\big[\frac{t(\mathcal{E}_1|\rho)}{d \cdot t(\mathcal{E}_1|\Phi_+)}, \frac{t(\mathcal{E}_2|\rho)}{d \cdot t(\mathcal{E}_2|\Phi_+)}\big]$, and $M = C, D$. The left term is $\mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2)$ for $\mathcal{M} = \mathcal{C}, \mathcal{D}$, and by taking $x = t \cdot d \leq \max\big[\frac{t(\mathcal{E}_1|\rho)}{t(\mathcal{E}_1|\Phi_+)}, \frac{t(\mathcal{E}_2|\rho)}{t(\mathcal{E}_2|\Phi_+)}\big]$ we get inequalities (5.36) and (5.37), which shows the lemma.

If one of the channels, $\mathcal{E}_2$ for instance, is proportional to a trace-preserving channel, then $t(\mathcal{E}_2|\rho) = t(\mathcal{E}_2|\Phi_+)$ for any ρ. This way, we can take $x = 1$, so that the following inequality holds for any pure state $\rho \in \mathscr{L}(\mathscr{H}^{\otimes 2})$:

$$M(\rho_1, \rho_2) \leq d \cdot \mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2). \tag{5.41}$$

As it holds for any pure state ρ, we showed that $\mathcal{M}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq d \times \mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2)$, which shows the theorem. ■

The lemma we just showed allows us to bound the deviation of any output states, with the sole knowledge of the operations actions on a maximally-entangled state, even if both channels are probabilistic. Yet in a lot of cases, such as the protocol presented in chapter 6, $\mathcal{E}_2$ is a reference quantum channel $\mathcal{E}_0$ that is deterministic, and we can use the special case $\mathcal{M}_\diamond(\mathcal{E}, \mathcal{E}_0) \leq \dim\mathcal{H} \times \mathcal{M}_J(\mathcal{E}, \mathcal{E}_0)$ from the theorem, which does not require to evaluate any transmissivity.

5.4 Discussion

In this chapter we introduced some novel results on CPTD maps, which model quantum channels which only operate with a certain probability. This includes an extension of the process inequality to probabilistic channels, the definition of classes of channels which perform the same operation with different probabilities, the construction of different distances on these classes, and an equivalence of Choi-Jamiołkowski and diamond distances. The latter result is also significant for CPTP maps, as it shows the behavior of a quantum channel on any quantum state can be evaluated from the behavior of that channel on one part of a maximally-entangled pair of qudits. This gives a preliminary idea of the protocol we build in the next chapter, in which we certify the transmission of an unmeasured qubit through a quantum channel by testing the behaviour of that channel with a maximally-entangled state. On a more general note, these results may encourage future studies focusing on lossy quantum channels, which model experimental situations involving post-selection with more accuracy than deterministic channels.

'The gardeners dig a hole, drop in a seed and water it. They know what kind of seed it is, but as the plant comes up and they water it, they don't know how many branches it's going to have, they find out as it grows.'

— George R.R. Martin.

CHAPTER 6

CERTIFIED QUANTUM TRANSMISSION VIA BELL THEOREM

The potential future development of a quantum network would rely on a collection of elementary building-blocks, allowing to generate, process, transmit and measure quantum information. In the context of potential malicious attacks and noisy devices, the ability to reliably certify the quality of these different building-blocks in a scalable way is therefore a fundamental step to developing world-wide quantum technologies. While methods for certifying quantum states proliferate in the literature [21, 22, 158], similar methods applicable to quantum channels are much scarcer.

In a cryptographic context, device-independent (DI) certification techniques are particularly reliable, as all used devices are considered to be completely uncharacterized black-boxes [159, 160]. Such certification procedures are highly resilient to attacks relying on corrupting the inner functioning of quantum devices. A necessary ingredient for DI certification of a quantum channel is channel self-testing procedure [161]. An important theoretical contribution to self-testing of quantum channels was recently provided by P. Sekatski *et al.* [25], allowing the certification of a lossless quantum channel (CPTP map) even with a certain amount of noise.

The first obstacle towards making Sekatski's result practically applicable is the fact that the authors consider CPTP maps, which only include lossless deterministic operations. Next, as is the case for most self-testing results, its immediate application to certification is possible only in the case of infinite number of identical and independent rounds, that is to say it requires the IID assumption. In real-world conditions, channels are lossy and probabilistic, might evolve through time, or can even be controlled by a malicious party who could, for instance, perform powerful quantum memory-based attacks. Therefore, a practical certification procedure should consider general trace-decreasing maps and relax the IID assumption. In addition, all channel-certification studies so far have focused on verifying the ability of a tested channel to preserve entanglement [25, 29]. Still, a practical procedure should not only inform the players about the ability of a previously used channel to transmit a maximally-entangled state, but it should also certify the transmission of an arbitrary state through an unmeasured channel.

In the following, we provide a practical method to certify the transmission of a single qubit through a probabilistic channel, in a semi-device independent scenario, where the sender trusts their devices but the receiver does not. Thanks to the new results on lossy quantum channels presented in chapter 5, we deduce a bound on the diamond fidelity between the untrusted channel and a reference unitary channel using the sole knowledge of the fidelity of a probe state to a maximally-entangled state, before and after passing through the channel. From this bound, we build a protocol that allows to certify with high confidence the fidelity between an unknown input state and the corresponding output state, received from an untested quantum channel. This protocol relies on the self-testing through steering inequalities in a one-sided device-independent and non-IID scenario, building upon the developments reported in [26, 162]. Finally, we perform a proof-of-principle experiment, by preparing photon-pairs displaying close-to-maximum entanglement in polarization and witnessing steering after a lossy and/or malicious quantum channels. This way we show that such protocol could be used with current technology, in order to certify long-distance fibered quantum communications, quantum teleportation or quantum memories.

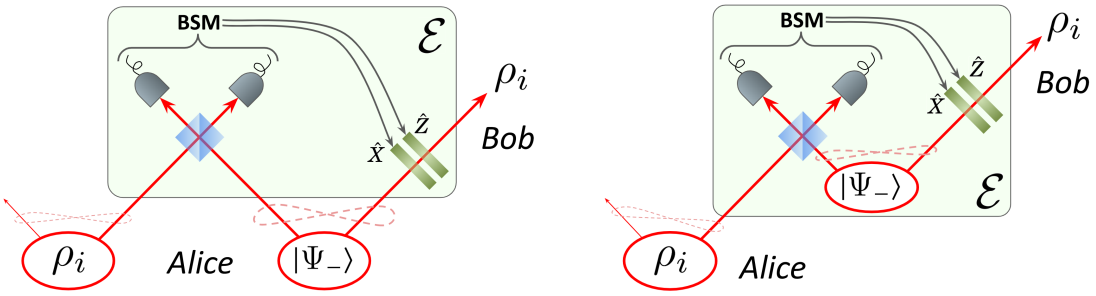
6.1 Genesis: Authenticated Teleportation

The original idea of this project came as an attempt to construct a practical protocol for semi device-independent authenticated teleportation, inspired from the theoretical work of A. Unnikrishnan and D. Markham [26]. The original protocol for quantum teleportation, summarized in Fig. 6.1, was first proposed by C.H. Bennett and G. Brassard [58], and allows a player Alice to send a qubit to Bob without sending the physical system. Let us call $\rho_i \in \mathscr{L}(\mathscr{H}_i \otimes \mathscr{S})$ the total input state, with Alice's qubit being encoded in Hilbert space $\mathscr{H}_i$, and $\mathscr{S}$ is the Hilbert space of a potential secondary system with which the qubit is entangled. Alice and Bob share a maximally-entangled state $|\Psi_-\rangle = \frac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}} \in \mathscr{H}_A \otimes \mathscr{H}_B$. Alice performs a Bell state measurement (BSM), jointly on the input qubit from $\mathscr{H}_i$ and her part of the maximally-entangled pair from $\mathscr{H}_A$. This BSM consists of 4 projectors on maximally-entangled states $\{|\Phi_\pm\rangle, |\Psi_\pm\rangle\}$. Alice then sends the measurement result to Bob, who applies a unitary operation on his part of the maximally-entangled state depending on that result, and this way retrieve the quantum state ρ_i between $\mathscr{L}(\mathscr{S})$ and $\mathscr{L}(\mathscr{H}_B)$.

The authenticated teleportation protocol from [26] proposes to certify the maximally entangled state shared by Alice and Bob, in order to bound the transmission fidelity between the input state Alice sends and the ouput state Bob receives. To derive this result however, the authors assume the BSM is a full POVM made of 4 perfect projectors on the Bell states. This assumption is not faithful to experimental linear-optics-based BSM, in which the projectors are noisy, and we only have access to two elements of the POVM, $|\Phi_\pm\rangle$ or $|\Psi_\pm\rangle$ [163]. This way, in addition to the maximally-entangled state, Alice and Bob also have to certify the BSM.

We discern two possible approaches to tackle this problem, both based on the consideration of a probabilistic quantum channel. The first approach consists in separating the teleportation protocol into two blocks, the first one consisting of the maximally-entangled state preparation, the second of the operations, including the partial BSM, classical communications and unitary operations. As displayed in Fig. 6.1a, we can express the probabilistic channel $\mathcal{E}$ including all operations

performed on the input state and the maximally-entangled state, such that the output state of the protocol is $(\mathbb{1}_{\mathcal{S}} \otimes \mathcal{E})[\rho_i \otimes \Psi_-]$. This way, one could certify the maximally-entangled state following the method from [26], and the BSM thanks to elements provided in [23, 24]. In the second approach, we consider the teleportation protocol consists of feeding the input state ρ_i into a probabilistic channel $\mathbb{1}_{\mathcal{S}} \otimes \mathcal{E}$, which includes the BSM and the state preparation, and other operations (see Fig. 6.1b). Therefore the channel is a black box which is expected to perform the identity operation. Some elements to certify such a black box are provided by P. Sekatski *et al.* [25], though more developments are required to apply such results to a probabilistic quantum channel. In this work we focus on that second approach, as it can also be used to certify any untrusted quantum device that is expected to perform the identity operation, such as quantum memories or any quantum transmission link. Still, we expect further investigations may show the first approach provides some advantage in the specific case of quantum teleportation.



(a) First approach to practical authenticated teleportation. The maximally-entangled state is certified separately from the operations, which are included in the probabilistic quantum channel $\mathcal{E}$.

(b) Second approach to practical authenticated teleportation. The quantum channel $\mathcal{E}$ is a black box including the maximally-entangled state and the operations, that we certify all-together.

Fig. 6.1: Sketch of the quantum teleportation protocol. Alice preforms a BSM on her part of a maximally-entangled pair, together with the input state. Depending on the result, Bob applies unitaries on his system to retrieve Alice's input state.

6.2 Prerequisite: Self-Testing of Quantum States

Our method for self-testing quantum channels is built on the self-testing of quantum states. This procedure, first proposed by D. Mayers and A. Yao [161, 164], relies on Bell theorem (see paragraph 2.1.4) to certify a maximally-entangled state [57], by making very few assumptions on the underlying quantum systems. In the most common setting, Alice and Bob measure multiple copies of a bipartite system, and under the IID assumption (independent, identically distributed rounds of experiment), they evaluate the probabilities $\mathbb{P}(a,b|x,y)$ of measuring the outcome a,b when adopting different measurement parameters x,y respectively. Then they can test a Bell inequality, which consists of a function $\mathcal{I}$ of these probabilities and a value β such that

$$\mathcal{I}\big(\mathbb{P}(a,b|x,y)\big) \leq \beta, \tag{6.1}$$

if the state is not entangled, and $\mathcal{I} > \beta$ for some entangled states. This way, such inequalities can be used by Alice and Bob in order to certify entanglement. Interestingly enough, such a certification does not require any assumption on the physical system being measured, or on the internal functioning of the measurement apparatus, meaning it is device-independent.

6.2.1 Self-Testing via CHSH Inequalities

The specific case of CHSH inequalities, defined in equation (2.21), is one of the most popular example of such inequalities. In this scenario, Alice and Bob wish to self-test the maximally-entangled state $|\Phi_+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \in \mathscr{H}_{A'} \otimes \mathscr{H}_{B'}$, in a physical bipartite quantum system of state $|\psi_{AB}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$. We consider a pure state, as Hilbert spaces $\mathscr{H}_A$ and $\mathscr{H}_B$ can be taken of arbitrary high dimensions. Alice and Bob each measure the system with two possible local POVMs $\{\hat{M}_{a|x}\}_{a=0,1}$ for $x=0,1$ and $\{\hat{N}_{b|y}\}_{b=0,1}$ for $y=0,1$ respectively. We define the corresponding observables:

$$\hat{A}_x = \hat{M}_{0|x} - \hat{M}_{1|x}, \tag{6.2}$$

$$\hat{B}_y = \hat{N}_{0|y} - \hat{N}_{1|y}. \tag{6.3}$$

By measuring the correlations of these observables, if Alice and Bob measure a maximum violation of CHSH inequality

$$\mathcal{I} = \langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_1 \rangle - \langle \hat{A}_0 \hat{B}_1 \rangle = 2\sqrt{2}, \tag{6.4}$$

it was shown [165–168] that a maximally-entangled state can be extracted from their system. More precisely, there exist two local isometries $\Gamma_A : \mathcal{H}_A \longrightarrow \mathcal{H}_A \otimes \mathcal{H}_{A'}$ and $\Gamma_B : \mathcal{H}_B \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_{B'}$, with $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ two qubit spaces, such that:

$$(\Gamma_A \otimes \Gamma_B)[|\psi_{AB}\rangle] = |\Phi_+\rangle \otimes |\psi_{trash}\rangle, \tag{6.5}$$

where $|\psi_{trash}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ corresponds to extra degrees of freedom in the system, that do not contribute to the entangled state. This result alone is not applicable in practice, as only $\epsilon-$close to maximum violation of Bell inequality can be measured in experiments, in which noise limits the value $\mathcal{I} = 2\sqrt{2} - \epsilon$. A robust self-testing method allows to derive a function $f(\epsilon)$ such that when we extract the state with isometries Γ_A, Γ_B, we can bound the fidelity to $|\Phi_+\rangle$:

$$F\big(\mathrm{Tr}_{A,B}(\Gamma_A \otimes \Gamma_B)[|\psi_{AB}\rangle], |\Phi_+\rangle\big) \geq f(\epsilon). \tag{6.6}$$

Many examples of such functions $f(\epsilon)$ were derived in the last decade [169–173], and finding one with the best convergence still remains an open question. In this work, we mostly use the result from A. Unnikrishnan and D. Markham [26]:

$$F\big(\mathrm{Tr}_{A,B}(\Gamma_A \otimes \Gamma_B)[|\psi_{AB}\rangle], |\Phi_+\rangle\big) \geq 1 - \alpha \cdot \epsilon \quad \text{with} \quad \alpha = 1.19. \tag{6.7}$$

Most importantly, the authors extend this result to a finite number of measurement rounds in a non-IID setting, which is particularly applicable in a cryptographic setting. This result is further detailed in paragraph 6.4 and appendix D.

6.2.2 Self-Testing via EPR-Steering

Recently the one-sided device-independent (1sDI) paradigm has been pointed out as an interesting compromise to derive more practical bounds with a reasonable amount of assumptions. In this setting, Bob still does not make any assumption on his part of the quantum system nor his measurement apparatus. Alice, however,

measures a qubit, such that $\mathscr{H}_A = \mathscr{H}_{A'}$, and she trusts her measurement apparatus so that $\hat{A}_0 = \hat{X}$ and $\hat{A}_1 = \hat{Z}$. In this case, self-testing can be derived from EPR-steering [174], in the form of a violation of the following inequality [175]:

$$\mathcal{I} = |\langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_1 \rangle| \leq \sqrt{2}. \tag{6.8}$$

There, a maximum violation $\mathcal{I} = 2$ implies a maximally-entangled state $|\Phi_+\rangle$ can be extracted from the system, by applying an isometry on Bob's side. Once again, A. Unnikrishnan and D. Markham provide a robust self-testing bound, when the players witness an ϵ-close to maximum violation $\mathcal{I} = 2 - \epsilon$ [26]:

$$F\big(\mathrm{Tr}_B(\mathbb{1} \otimes \Gamma_B)[|\psi_{AB}\rangle], |\Phi_+\rangle\big) \geq 1 - \alpha \cdot \epsilon \quad \text{with} \quad \alpha = 1.26, \tag{6.9}$$

which can also extended to a finite non-IID setting. In this work we experimentally demonstrate a protocol in this 1sDI scenario. It is indeed more practical to achieve than a full-DI version, all the while being suitable for real-world situations in which a powerful server (Alice) wishes to provide a weaker receiver (Bob) with quantum information. We still provide full-DI recipes whenever possible.

6.2.3 On the Isometries Formalism

A counter-intuitive aspect of the self-testing procedure is the fact that states are not certified in absolute terms, but only up to local isometries Γ_A, Γ_B. This questions the validity of such a method, as one might require a more absolute definition of state. To understand how this method is still valid, we first highlight that the Hilbert space's structure, *i.e.* the scalar product and orthogonality, is conserved under application of isometries. In addition, quantum states are always defined from a certain reference in experiments. Typically, the horizontal and vertical polarizations of photons, defined in the laboratory's reference frame, may have different definitions in other reference frames (they even rotate though time in the geocentric reference frame). This way, quantum states are generally not defined in absolute terms, but relatively to the experimenter's perception, in the form of the measurement apparatus' calibration. In proofs of self-testing results, isometries are generally built from Alice's and Bob's measurement operators $\{\hat{M}_{a|x}\}_{a=0,1}$ and $\{\hat{N}_{b|y}\}_{b=0,1}$ (take for instance the Swap isometry, detailed in [26, 176–178]), and

therefore encompass this reference frame. Instead of claiming states are certified "up to isometries", one could more intuitively claim a certification "relatively to the experimenter's apparatus". This way, in order to use certified states in later experiments, one would have to calibrate their own apparatus on the certification apparatus, which may involve self-testing Alice's and Bob's measurement operators together with the state. In particular, the self-testing results we use in this thesis were proposed in [26], which also includes such device-independent certification of the measurement apparatuses.

6.3 The Problem

In our framework, a player Alice wishes to send one part of a 2-qubits state $\rho_i \in \mathscr{L}(\mathscr{H}_i^{\otimes 2})$ to Bob, through a local unitary quantum channel $\mathcal{E}_0$. This channel takes any state $\rho_i \in \mathscr{H}_i$ to another qubit state $\rho_o = (\mathcal{E}_0 \otimes \mathbb{1})[\rho_i] = (\hat{U} \otimes \mathbb{1})\rho_i(\hat{U}^\dagger \otimes \mathbb{1})$ in $\mathscr{L}(\mathscr{H}_o \otimes \mathscr{H}_i)$, where $\hat{U}$ is a local unitary operator and $\mathbb{1}$ the identity. Such channel models perfect unitary gates in quantum computer, quantum transmission links (carried on through quantum teleportation or a simple optical fiber) or quantum memories. Without loss of generality, we take $\hat{U} = \mathbb{1}$ and $(\mathcal{E}_0 \otimes \mathbb{1})[\rho_i] = \rho_i$, as this case encompasses all unitaries in a device-independent scenario [25]. This channel is called the *reference channel*.

In real world situations, the channel would be lossy, noisy, or even operated by a malicious party Eve. Also, Alice and Bob normally do not have access to isolated qubit spaces, but operate with physical systems such as photons or atoms, displaying other degrees of freedom. This way, without further assumptions, Alice and Bob have access to a CPTD map $\mathcal{E}$, *i.e.* a probabilistic channel, that sends density operators from an input Hilbert space $\mathscr{H}_{A_1}$ to positive operators of trace smaller than 1 on an output Hilbert space $\mathscr{H}_B$. This channel is called the *physical channel*. Alice possesses a bipartite state Φ_i shared between $\mathscr{H}_{A_1}$ and a secondary Hilbert space $\mathscr{H}_{A_2}$, that we call the *probe* input state. She can send the first part of Φ_i through the channel $\mathcal{E}$, resulting in the *probe* output state Φ_o, shared with Bob:

$$\Phi_o = (\mathcal{E} \otimes \mathbb{1})[\Phi_i]/t(\mathcal{E}|\Phi_i), \tag{6.10}$$

where $t(\mathcal{E}|\Phi_i) = \mathrm{Tr}(\mathcal{E}\otimes\mathbb{1})[\Phi_i]$ is the channel's transmissivity (see chapter 5 for more details on that notion). Finally, the players can measure states with 2-outcomes (POVMs) $\{\hat{M}^P_{l|q}\}_{l=0,1}$ where $P = A_1, A_2$ or B indicating the Hilbert space on which the measurement is acting, and q indicates which POVM is measured.

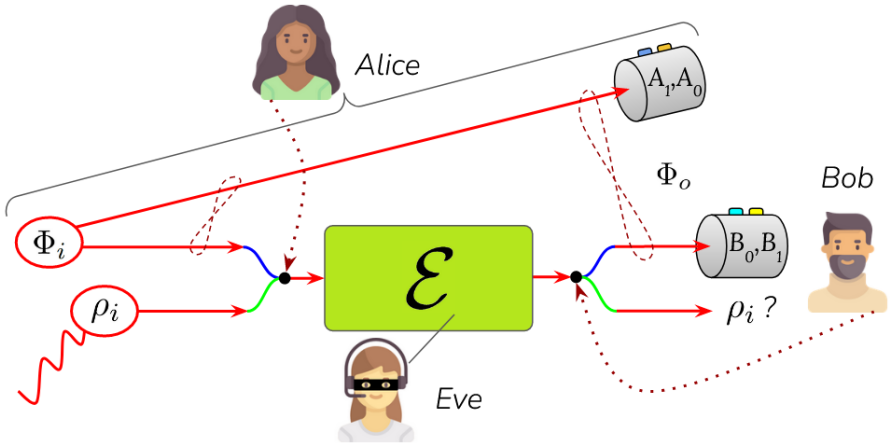


Fig. 6.2: Sketch of the problem. Alice sends a qubit state ρ_i to Bob through an untrusted quantum channel $\mathcal{E}$ (green path). Alice can send half of a close-to-maximally entangled probe state Φ_i through $\mathcal{E}$ (blue path). Alice and Bob can then measure the output state Φ_o, and try to deduce the probability of applying $\mathcal{E}_0$ to ρ_i.

In an adversarial scenario, Alice and Bob wish to draw device-independent conclusions, making as few assumptions as possible on the states or the measurements. In particular, physical Hilbert spaces $\mathscr{H}_{A_1}$, $\mathscr{H}_{A_2}$ and $\mathscr{H}_B$ are of arbitrary big dimensions, including all degrees of freedom of the physical systems and possible entanglement with the rest of the universe. This way players only certify objects up to local isometries, mapping the physical spaces onto the qubit spaces $\mathscr{H}_i$ and $\mathscr{H}_o$. For this task, we wish to derive a self-testing method for quantum channels, similarly to quantum states, described in the last paragraph. A first method was provided by P. Sekatski *et al.* [25], to device-independently test the equivalence between the physical deterministic channel $\mathcal{E}\otimes\mathbb{1}$ and the reference operation $\mathcal{E}_0\otimes\mathbb{1}$, up to local isometries. In our case, a trace-decreasing physical channel only returns a state with a certain probability, such that it can only be compared to the reference channel when post-selecting on rounds when the transmission actually happened, *i.e.* by using the equivalence classes of lossy channels described in chapter 5. This way, we provide a new definition for the self-testing of a lossy channel:

Definition 6.1 (Self-testing of a CPTD map)**.** *Let $\mathcal{E} : \mathscr{L}(\mathscr{H}_{A_1}) \longrightarrow \mathscr{L}(\mathscr{H}_B)$ be a physical lossy channel, and $\mathcal{E}_0 : \mathscr{L}(\mathscr{H}_i) \longrightarrow \mathscr{L}(\mathscr{H}_o)$ a reference channel. With two local isometries $\Gamma_i : \mathscr{H}_{A_1} \otimes \mathscr{H}_i \longrightarrow \mathscr{H}_{A_1} \otimes \mathscr{H}_i^{ext}$ and $\Gamma_o : \mathscr{H}_B \longrightarrow \mathscr{H}_o \otimes \mathscr{H}_o^{ext}$, and an ancillary state $\rho_{A_1} \in \mathscr{L}(\mathscr{H}_{A_1})$, we can define an extracted channel:*

$$\mathcal{E}_{i,o} : \rho \in \mathcal{L}(\mathcal{H}_i) \longrightarrow \mathrm{Tr}_{ext}\big((\Gamma_o \circ \mathcal{E} \circ \Gamma_i)[\rho_{A_1} \otimes \rho\,]\big) \tag{6.11}$$

where the trace is taken over $\mathscr{H}_i^{ext}$ and $\mathscr{H}_o^{ext}$. The self-testing equivalence between the physical channel $\mathcal{E}$ and the reference channel $\mathcal{E}_0$ is established if:

$$\mathcal{E}_{i,o} \equiv \mathcal{E}_0. \tag{6.12}$$

Note the equivalence in equation (6.12) is defined in chapter 5, such that $\mathcal{E}_{i,o} \equiv \mathcal{E}_0$ when there exists $t \in]0;1]$ giving $\mathcal{E}_{i,o} = t\mathcal{E}_0$. Physically speaking, these two channels output the same states, on the condition those were not lost. Also, unlike in self-testing of quantum states, two isometries are required in order to extract a qubit-to-qubit channel $\mathcal{E}_{i,o}$ from a physical channel $\mathcal{E}$, as a quantum channel is associated to two Hilbert spaces (one in input and the other in output). This way, the input isometry brings a qubit input state to a physical state that can be fed into the physical channel, while the output isometry extracts a qubit state from the physical channel's output state.

In experiments, we can never perfectly certify $\mathcal{E}$, therefore we quantify the ability of this probabilistic channel to implement the deterministic channel $\mathcal{E}_0$ by using channels closeness functions defined in chapter 5. In a cryptographic scenario, we wish to bound that closeness in the worst case scenario, so we favor the diamond fidelity:

$$\mathcal{F}_{\diamond}^{\Gamma_{i,o}}(\mathcal{E},\mathcal{E}_0) = \mathcal{F}_{\diamond}(\mathcal{E}_{i,o},\mathcal{E}_0) = \min_{\rho} F\big((\mathcal{E}_{i,o}\otimes\mathbb{1})[\rho]/t(\mathcal{E}_{i,o}|\rho),(\mathcal{E}_0\otimes\mathbb{1})[\rho]\big), \tag{6.13}$$

where the minimization is carried out over all pure states of $\mathscr{L}(\mathscr{H}^{\otimes 2})$. The diamond fidelity is particularly useful here, as it can be interpreted as the minimum probability that $\mathcal{E}\otimes\mathbb{1}$ successfully implements the operation $\mathcal{E}_0\otimes\mathbb{1}$ on any state, on the condition that a state successfully passes through the channel. The main goal of our protocol is therefore to certify that fidelity.

6.4 Theoretical Protocols

We now propose different protocols that can be used in order to certify the transmission of a qubit through an untrusted quantum channel. These protocols assume different levels of trust on the probe states and Alice's measurement apparatus. The first one assumes Alice can certify her source and measurement system prior to the protocol, which are therefore trusted. The second one assumes the source and measurement appartus are untrusted, though we still consider the probe states to follow an IID statistics. In both protocols, the channel is completely untrusted, which can possibly evolve through time depending on previous rounds of experiments, and may display state-dependent losses. Bob measurement apparatus is also untrusted in both protocols.

6.4.1 Certification Bound and General Recipe

The general protocol recipe comes straight from bounding the channel fidelity with specific states fidelity, that can be evaluated via self-testing. For that purpose, let us consider the situation where Alice can certify the probe input state Φ_i up to two local isometries $\Gamma^{A_1/A_2} : \mathscr{H}_{A_1/A_2} \longrightarrow \mathscr{H}_{A_1/A_2} \otimes \mathscr{H}_i$ with the following fidelity to a maximally-entangled state $|\Phi_+\rangle$:

$$F^i = F\big((\Lambda^{A_1} \otimes \Lambda^{A_2})[\Phi_i], \Phi_+\big), \tag{6.14}$$

where $\Lambda^j[\cdot] = \mathrm{Tr}_j(\Gamma^j[\cdot])$. We also assume that Alice and Bob are able to certify the probe output state Φ_o up to local isometries Γ^{A_2} and $\Gamma^B : \mathscr{H}_B \longrightarrow \mathscr{H}_B \otimes \mathscr{H}_o$ with the following fidelity:

$$F^o = F\big((\Lambda^B \otimes \Lambda^{A_2})[(\mathcal{E} \otimes \mathbb{1})[\Phi_i]]/t(\mathcal{E}|\Phi_i)(\mathcal{E}_0 \otimes \mathbb{1})[\Phi_+]\big). \tag{6.15}$$

We then show in appendix D that there exist isometries Γ_i, Γ_o such that we can lower bound the diamond fidelity on the corresponding extracted channel $\mathcal{E}_{i,o}$:

$$\mathcal{F}_\diamond(\mathcal{E}_{i,o}, \mathcal{E}_0) \geq 1 - 4\sin^2\Big(\arcsin\big(C^i/t(\mathcal{E}|\Phi_i)\big) + \arcsin C^o\Big), \tag{6.16}$$

where $C^j = \sqrt{1-F^j}$ are sine distances associated to their corresponding fidelities. This bound generalizes what is shown in [25] to probabilistic channels. It also

uses the diamond fidelity $\mathcal{F}_\diamond$, which informs on the behavior of the channel on any state, instead of the Choi-Jamiołkowski fidelity $\mathcal{F}_J$, which only informs on the behavior of the channel on a maximally-entangled state (see chapter 5). Note that all isometries involved in the certification and summarized in Fig. 6.3.

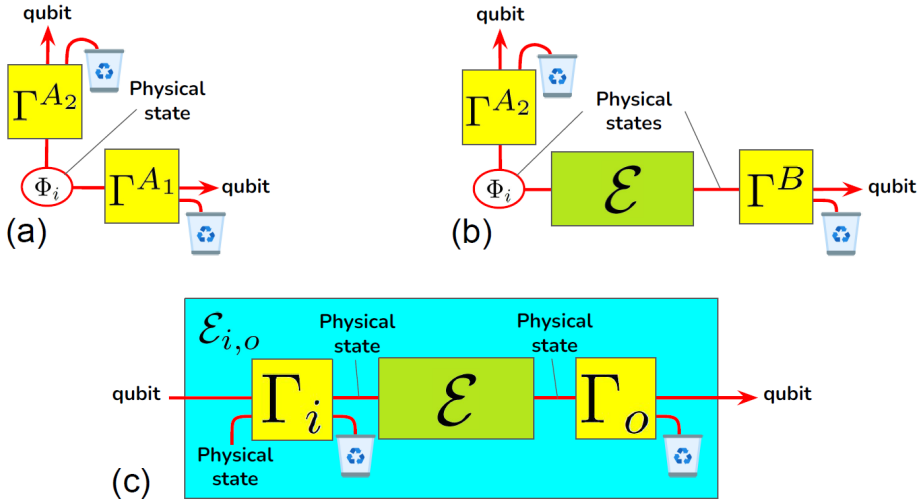


Fig. 6.3: Isometries' involved in the certification, acting on the probe state Φ_i (a) and corresponding output state Φ_o (b), and the channel $\mathcal{E}$ (c). Γ_i encodes a qubit state onto a physical state that can be fed into $\mathcal{E}$. Other isometries extract a qubit state from a physical system. Extra degrees of freedom are discarded. Together, Γ_i and Γ_o extract a qubit-to-qubit channel from a physical channel.

From bound (6.16) we deduce the recipe for bounding the fidelity of a quantum channel to a reference channel. Alice first evaluates the fidelity F^i of the probe input state to a Bell state, then sends one part of the probe through the channel, and finally evaluates the fidelity F^o of the corresponding output state to the same Bell state. Such procedure is possible using recent self-testing results [26, 162], but requires a very large number of experimental rounds in the absence of IID assumption, as both input and output probe states require certification. This number can be significantly decreased by making the IID assumption on the probe input state, or by leaving its full characterization to Alice's responsibility. Still, as we make no IID assumption on the channel, optimal security cannot be reached by first testing that channel, and only then using it to send the input state, as Eve may change the channel's expression in the last moment. Our protocol works around this problem by allowing Alice to hide the state ρ_i among a large number of

probe states, at a random position r unknown to Eve. Then we show in appendix D that bound (6.16) holds for the average channel $\bar{\mathcal{E}}_{i,o}$ over the whole protocol:

$$\bar{\mathcal{E}} = \frac{1}{N+1}\sum_{k=1}^{N+1} \mathcal{E}_{k|[k-1]}, \tag{6.17}$$

where $\mathcal{E}_{k|[k-1]}$ is the channel that operates on the k-th state sent by Alice through the protocol ($[k-1] = k-1, k-2, ..., 1$). In particular, Alice sends the input state ρ_i through channel $\mathcal{E}_{r|[r-1]}$. Then the *transmission fidelity* between the expected output state $\bar{\rho}_o = (\bar{\mathcal{E}}_{i,o} \otimes \mathbb{1})[\rho_i]/t(\bar{\mathcal{E}}|\rho_i)$ and the input state ρ_i is certified:

$$F(\bar{\rho}_o, \rho_i) \geq \mathcal{F}_\diamond(\bar{\mathcal{E}}_{i,o}, \mathbb{1}). \tag{6.18}$$

As long as r stays hidden and random, any measurement performed on the output state later after the protocol would follow the same statistics as if it was performed on $\bar{\rho}_o$. Therefore we can use this expected state to describe accurately any experiment that would be carried out after the protocol. The general recipe for the protocol is summarized in Fig. 6.4, although details depend on the amount of trust put in the states and player's apparatuses, and are given in the next paragraphs.

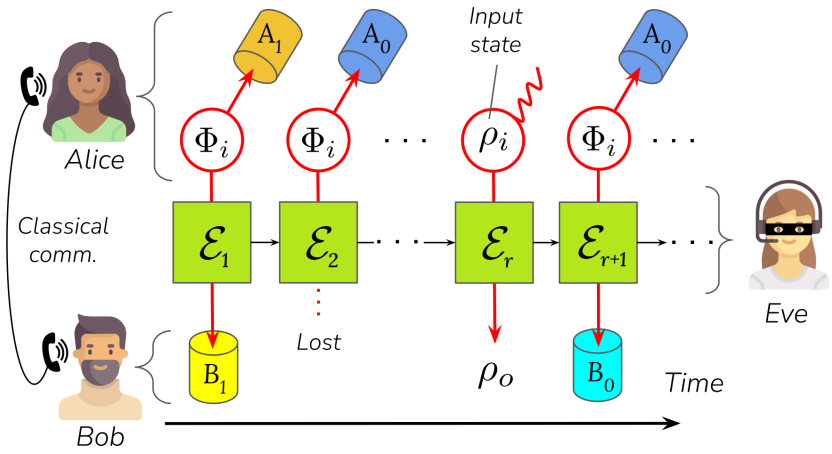


Fig. 6.4: Summary of the protocol for certified quantum transmission: Alice sends N copies of a probe state Φ_i, as well as ρ_i at a random secret position r, through an untrusted channel $\mathcal{E}$ that varies with time. If ρ_i was lost, then the protocol aborts. Otherwise, Bob stores ρ_i, and tests the violation of steering or CHSH inequalities with Alice with the output probe states. They deduce the average channel quality over the protocol, which gives the probability that the state ρ_i was accurately transmitted to Bob, up to isometries.

6.4.2 Protocol with One-Sided Trust

We first focus on a 1sDI scenario, where Alice's measurement setup is trusted, so her Hilbert spaces are qubit spaces $\mathscr{H}_{A_1} = \mathscr{H}_{A_2} = \mathscr{H}_i$, her isometries are trivial $\Gamma_i = \Gamma^{A_1} = \Gamma^{A_2} = \mathbb{1}$, and she performs measurements in the Pauli $\hat{X}$ and $\hat{Z}$ bases:

$$\hat{A}_0 = \hat{M}^{A_2}_{0|0} - \hat{M}^{A_2}_{1|0} = \hat{Z}, \tag{6.19}$$

$$\hat{A}_1 = \hat{M}^{A_2}_{0|1} - \hat{M}^{A_2}_{1|1} = \hat{X}. \tag{6.20}$$

Similarly, the probe state Φ_i is trusted and characterized. This fits a variety of scenarios where Alice is a powerful server, trying to provide to a weaker client, Bob, whose measurement apparatus is still untrusted. This way Bob's observables

$$\hat{B}_0 = \hat{M}^{B}_{0|0} - \hat{M}^{B}_{1|0}, \tag{6.21}$$

$$\hat{B}_1 = \hat{M}^{B}_{0|1} - \hat{M}^{B}_{1|1}, \tag{6.22}$$

are *a priori* unknown. Alice and Bob bound F^o from eq. (6.15) using self-testing via steering [26, 174] as detailed in paragraph 6.2.2, and certify the transmission fidelity from bound (6.16). We give the detailed recipe for the certification protocol in protocol box 6.1.

Note that the purpose of step 1.(b) is simply to inform Alice of the minimum amount of states she has to prepare in order to ensure security. If the channel's operator Eve overstates the tranmissivity t, then Alice will not prepare enough probe states, which in turn makes the protocol abort in step 6. On the contrary if Eve understates t, then Alice is going to prepare more probe states than she and Bob require, which will in fact improve the certification confidence.

Protocol 6.1: Certified quantum transmission via Bell theorem, 1sDI scenario.

1. Prior to the protocol:

   (a) Alice characterizes the state Φ_i emitted by her source and evaluates the quantity F^i. She also receives or prepares the state ρ_i, possibly shared with an outside party.

   (b) Eve announces the minimum transmissivity t of the quantum channel $\mathcal{E}$ for any quantum state.

2. Alice and Bob agree on parameters ϵ, K, depending on their requirements and experimental limitations.

3. Alice prepares $N = \lceil K/t \rceil$ copies of the probe state Φ_i.

4. Alice successively sends each state through $\mathcal{E}$, including ρ_i in a random r-th position, with $r \leq N+1$.

5. Bob establishes the set $\mathbb{S}_P$ of states which successfully passed through $\mathcal{E}$, and broadcasts it publicly.

6. If $r \notin \mathbb{S}_P$ or $|\mathbb{S}/\{r\}| < K$, Alice aborts the protocol. Otherwise, Alice sends r to Bob.

7. Alice separates $\mathbb{S}/\{r\}$ into two random sets $\mathbb{S}_0$ and $\mathbb{S}_1$.

8. For each $k \in \mathbb{S}_q$, $q = 0, 1$:

   (a) Alice measures observable $\hat{A}_q$ on her part of the k-th state and gets outcome a_k.

   (b) She tells Bob to measure observable $\hat{B}_q$ on his part of the k-th state and he gets outcome b_k.

   (c) Alice and Bob calculate their correlation for round k as $c_k = a_k b_k$.

9. Alice and Bob deduce the average value of $\mathcal{I} = |\langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_1 \rangle|$ over all rounds.

10. If $\mathcal{I} \geq 2 - \epsilon$, then Alice successfully sent the state $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ to Bob, with a certified average fidelity to ρ_i, up to isometry.

Protocol Security. The security of the protocol is in principle ensured by the fact that the position r of state ρ_i stays hidden to Eve. Thus as we mention in paragraph 6.4.1, we derive the minimum transmission fidelity between the expected output state $\bar{\rho}_o$ and ρ_i by applying bound (6.16) to the average channel $\bar{\mathcal{E}}$. In particular, the output probe state's fidelity to a maximally-entangled state now reads:

$$F^o = F\Big((\Lambda^B \otimes \Lambda^{A_2})[(\mathcal{E} \otimes \mathbb{1})[\Phi_i]]/t(\bar{\mathcal{E}}|\Phi_i), (\mathcal{E}_0 \otimes \mathbb{1})[\Phi_+]\Big). \tag{6.23}$$

Using the results from [26] for self-testing through steering, in a non-IID and 1sDI setting, applied to the output probe state, we show in appendix D that for any $x > 0$, the distance $C^o = \sqrt{1-F^o}$ can be bounded by two terms, with confidence of at least $c_x = (1-e^{-x}) \cdot (1-2e^{-x})^2$:

$$\arcsin C^o \leq \arcsin \sqrt{\alpha f_x(\epsilon, K)} + \Delta_x(\eta_s, K), \tag{6.24}$$

where $\eta_s = K/N$ is the measured transmission ratio, $\Delta_x(\eta_s, K)$ is an error function that goes to 0 for high values of K, αf_x gives self-testing bound on the output state, in a finite non-IID regime, with $\alpha = 1.26$ and

$$f_x(\epsilon, K) = 8\sqrt{\frac{x}{K}} + \frac{\epsilon}{2} + \frac{\epsilon + 8/K}{2 + 1/K} \xrightarrow[K \to +\infty]{} \epsilon, \tag{6.25}$$

such that we get bound (6.9) in the asymptotic regime. Note that the error function is due to both the non-IID regime and the lack of information on channels that do not output any state. A similar error occurs when we evaluate the transmissivity as the measured transmission ratio:

$$t(\bar{\mathcal{E}}|\Phi_i) \gtrsim \tau_x(\eta_s, K), \tag{6.26}$$

where $\tau_x(\eta_s, K) \simeq \eta_s$ for high values of K. This way, the actual bound on the fidelity between the input and output state reads, with confidence c_x

$$F(\bar{\rho}_o, \rho_i) \geq 1 - 4 \cdot \sin^2\Big(\arcsin\big(C^i/\tau_x\big) + \arcsin \sqrt{\alpha f_x(\epsilon, K)} + \Delta_x\Big), \tag{6.27}$$

which includes additive error terms compared to bound (6.16). Note that the expressions and proofs for all the mentioned functions are detailed in appendix D.

6.4.3 Protocol with No Trust

While the previous protocol has high relevance when devices in Alice's laboratory can be trusted, a completely adversarial scenario would demand a fully device-independent protocol. Theoretically, such a protocol can be formulated, but would be very resource-demanding and therefore difficult to perform. It could be built from protocol 6.1, by certifying the fidelity F^i in a device-independent manner, which could be done via self-testing of the violation the CHSH inequality. In the absence of IID assumption, every single probe state Alice sends through the channel requires certification, by measuring an additional number M of copies of the probe state. All in all, assuming M is of the same order as N, a fully device-independent protocol *a priori* requires $M \cdot N \approx N^2$ copies of the probe state for optimal security. This corresponds to a very low sample-efficiency of the certification protocol, which is hardly practical for experimental implementations.

One can simplify the protocol by assuming the source is producing independent and identically distributed copies, i.e. that the source functions in the IID scenario. In that case, probe states only require a single certification step with M extra copies, so the total sample size is $M+N$ instead of $M \cdot N$. We provide the recipe for that certification protocol in protocol box 6.2, making the IID assumption on the input probe state. In this framework, our fully device-independent protocol simply consists in performing a very similar protocol to the 1sDI one, by replacing step 1.(a) by a self-testing-based certification, and using the CHSH inequality [55] instead of the steering inequality for certification, as all measurement apparatus are untrusted. In that version, Alice measures the observables $\hat{A}_3, \hat{A}_4$ on the part of the system she can send through the channel.

Protocol 6.2: Certified quantum transmission via Bell theorem, DI scenario.

1. Prior to the protocol Eve announces the minimum transmissivity t of $\mathcal{E}$ for any quantum state.

2. Alice and Bob agree on parameters ϵ, η, K, M depending on their requirements and experimental limitations.

3. Alice prepares $N+M$ copies of Φ_i, where $N = \lceil K/t \rceil$.

4. Alice measures M random copies of Φ_i, and deduces the value of $\mathcal{I}_i = |\langle \hat{A}_0 \hat{A}_2 \rangle + \langle \hat{A}_0 \hat{A}_3 \rangle + \langle \hat{A}_1 \hat{A}_2 \rangle - \langle \hat{A}_1 \hat{A}_3 \rangle|$.

5. If $\mathcal{I}_i < 2\sqrt{2} - \eta$, Alice aborts the protocol.

6. Alice successively sends each state through $\mathcal{E}$, including ρ_i in a random r-th position, with $r \leq N+1$.

7. Bob establishes the set $\mathbb{S}_P$ of states which successfully passed through $\mathcal{E}$, and broadcast it publicly.

8. If $r \notin \mathbb{S}_P$ or $|\mathbb{S}/\{r\}| < K$, Alice aborts the protocol. Otherwise, Alice sends r to Bob.

9. For each $k \in \mathbb{S}_q$, $q = 0, 1$:

   (a) Alice measures observable $\hat{A}_u$ on her part of the k-th state with $u = 0$ or 1 at random. She gets outcome a_k.

   (b) Bob to measures the observable $\hat{B}_v$ on her part of the k-th state, with $v = 0$ or 1 at random. He gets the outcome b_k.

   (c) Alice and Bob calculate their correlation for round k as $c_k = a_k b_k$.

10. Alice and Bob deduce the average value over all rounds, of $\mathcal{I}_o = |\langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_0 \hat{B}_1 \rangle + \langle \hat{A}_1 \hat{B}_0 \rangle - \langle \hat{A}_1 \hat{B}_1 \rangle|$.

11. If $\mathcal{I}_o \geq 2\sqrt{2} - \epsilon$, then Alice successfully sent the state $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ to Bob, with a certified average fidelity to ρ_i, up to isometry.

Protocol Security. The security of this protocol can be derived from that of protocol 1, with some slight adjustments. First we use another bound for the self-testing of CHSH inequalities, in a fully device-independent and non-IID scenario [162], in order to certify the output probe state. We still have the following bound with confidence at least $c_x = (1-e^{-x})\cdot(1-2e^{-x})^2$

$$\arcsin C^o \leq \arcsin\sqrt{\alpha f_x(\epsilon,K)} + \Delta_x(\eta_s,K), \tag{6.28}$$

though this time $\alpha = 1.19$ and f_x takes another form

$$f_x(\epsilon,K) = 16\sqrt{\frac{2x}{K}} + \frac{3\epsilon}{4} + \frac{\epsilon + (4+2\sqrt{2})/K}{4+4/K}. \tag{6.29}$$

The input state is also certified via self-testing of CHSH inequality in a fully device-independent scenario but keeping the IID assumption, with a confidence level $(1-e^{-x})$:

$$F^i = F\big((\Lambda^{A_1}\otimes\Lambda^{A_2})[\Phi_i],\Phi_+\big) \geq 1-\alpha\cdot g_x(\eta,M) \underset{M\to+\infty}{\longrightarrow} 1-\alpha\cdot\eta, \tag{6.30}$$

with $\Lambda^{A_1}[\cdot] = \mathrm{Tr}_{A_1}(\Gamma^{A_1}[\cdot])$, $\Lambda^{A_2}[\cdot] = \mathrm{Tr}_{A_1}(\Gamma^{A_2}[\cdot])$, $\alpha = 1.19$, and $g_x(\eta,M) = 8\sqrt{2x/M}+\eta$. We can then plug the two certified fidelities in our bound 6.16, so the transmission fidelity between input and expected output state is bounded with confidence level $c'_x = (1-e^{-x})^2\cdot(1-2e^{-x})^2$

$$F(\bar{\rho}_o,\rho_i) \geq 1-4\cdot\sin^2\Big(\arcsin\big(\sqrt{\alpha g_x(\eta,M)}/\tau_x\big) + \arcsin\sqrt{\alpha f_x(\epsilon,K)} + \Delta_x\Big). \tag{6.31}$$

which gives the full certification bound for protocol 6.2.

6.5 Experimental Implementation

In order to test the feasibility of the certification procedure, we perform a proof-of-principle experiment based on polarization-entangled-photon pairs, emitted by our Sagnac-PPKTP source, described in chapter 3. A sketch of the experimental setup is given in Fig. 6.5. For practical reasons, different assumptions are implicitly made during this first implementation, that we summarize at the end of this paragraph.

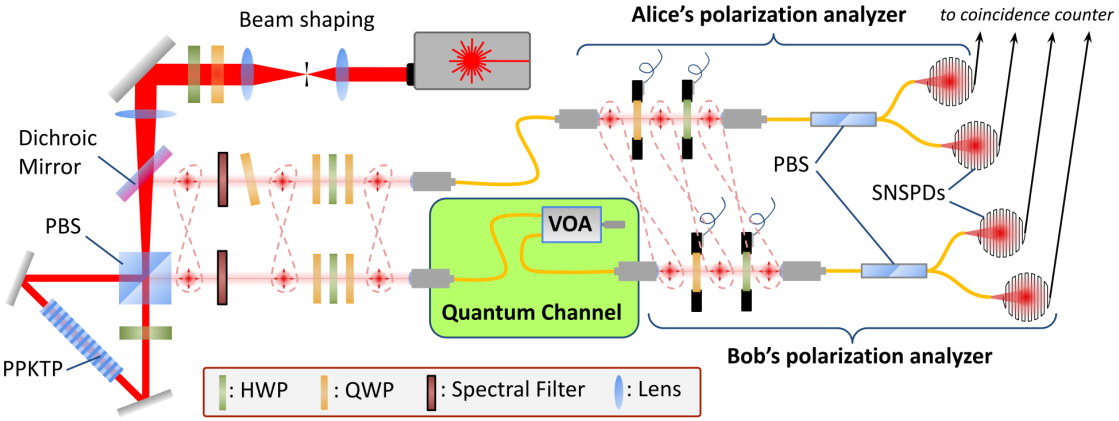


Fig. 6.5: Experimental setup for photonic certified quantum communication through an unstrusted channel. Photon pairs are generated by our Sagnac-PPKTP source, detailed in chapter 3. The idler photon is both used to herald a probe state, and as Alice's part of the state. The signal photon is sent to Bob through the untrusted lossy channel. A VOA allows to simulate an honest channel with a tunable amount of loss. Quantum correlations and channel transmissivity are measured via the biphoton polarization analyzer shown in Fig. 3.15.

For this first attempt we focus on protocol 6.1, in the one-sided device-independent scenario. This way the probe states Φ_i emitted by the source are characterized at each protocol attempt via quantum state tomography (see appendix A), without inserting any untrusted quantum channel (green box in Fig. 6.5). Polarization analyzers (PA) are trusted for that task, as it is performed by Alice. Following the IID assumption, the state Φ_i is assumed to remain the same for a whole protocol run, which is supported by the stability of our source argued in paragraph 3.4. In order to evaluate the input fidelity F^i in equation (6.14), up to local isometries, we maximize the quantity

$$F_U^i = F\big((\mathbb{1}\otimes\hat{U})\Phi_i(\mathbb{1}\otimes\hat{U}^\dagger),\Phi_+\big), \tag{6.32}$$

on a local unitary $\hat{U}$. This way the fidelity of the probe's polarization state to a Bell state is $F^i = 99.20\% \pm 0.02\%$ on average over all protocol attempts, with a maximum reached fidelity of $F^i = 99.43\% \pm 0.05\%$.

We then send the probe states through an untrusted quantum channel. For this first implementation, we use a variable optical attenuator (VOA) to simulate

a quantum channel with different losses. Detecting an idler-photon in Alice's PA heralds a signal-photon being sent through the quantum channel, which is then detected in Bob's PA. This way, we measure $K \simeq 10^9$ copies of the probe state in order to minimize the error terms in certification bounds, and maximize the confidence level $c_x > 99.5\%$. This takes from 1 to 3 hours in our experiments depending on the channel's transmissivity. We measure the pairs in random bases $\hat{A}_0\hat{B}_0$ or $\hat{A}_1\hat{B}_1$, and evaluate a close-to-maximum violation of steering inequality $\mathcal{I} = 2 - \epsilon$. Players should in principle randomize the measurement basis for each new photon pair. However, because of technical limitations of our motorized waveplate stages, we only operate this randomization at a limited rate of 1 Hz. A fully secure protocol would require faster electronics and active optical components.

In each protocol attempt, the transmissivity is identified as the probability that Bob detects a state, knowing Alice heralded that state, and is also known as the heralding efficiency η_s:

$$t(\mathcal{E}|\Phi_i) \simeq \eta_s = R_{si}/R_i, \tag{6.33}$$

where R_{si} is the pairs' detection rate and R_i the idler's detection rate. We set different transmissivities of the channel by tuning the VOA, such that η_s ranges from 21.9% to 47.3%, the maximum value corresponding to the replacement of the VOA by a simple fiber connector (η_s does not reach 66% as in chapter 3 because of extra components in the setup). We can consider that a certain fraction of the losses is not induced by the channel itself, but by other components which are characterized by Alice, as part of the source. Such losses are considered homogeneous and trusted, so the channel reads

$$\mathcal{E} = (1 - \lambda_c)\mathcal{E}', \tag{6.34}$$

where λ_c is the amount of losses that is trusted and state-independent, and $\mathcal{E}' \equiv \mathcal{E}$ in the sense defined in chapter 5, meaning both channels return the same output states (see Fig. 6.6). This way we can certify $\mathcal{E}'$ instead of $\mathcal{E}$. In that case the transmissivity in bound (6.16) can be re-written

$$t(\mathcal{E}'|\Phi_i) = t(\mathcal{E}|\Phi_i)/(1 - \lambda_c) = \eta_s/(1 - \lambda_c), \tag{6.35}$$

which tightens the bound compared to the naive approach where all losses are attributed to the channel. Adopting this interpretation is quite realistic, considering

Alice preforms a full characterization of the probe states, which potentially includes a lower bound on the coupling losses. In the worst case scenario, she can always set $\lambda_c = 0$ and attribute all the coupling and detection losses to the channel.

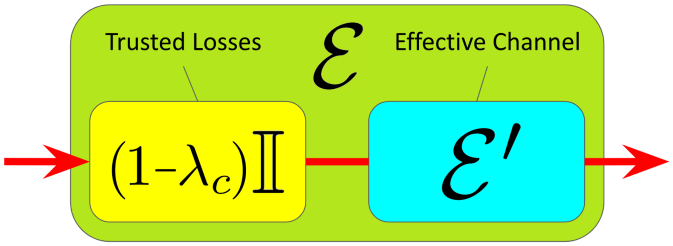


Fig. 6.6: Schematic decomposition of the untrusted channel $\mathcal{E}$, into an equivalent channel $\mathcal{E}'$ that the protocol effectively certifies, and a trusted channel, translating for the characterized and homogeneous losses λ_c.

6.5.1 Results for a Honest Channel

We first test our protocol on an untrusted but honest channel, by tuning the channel transmissivity with the VOA. We show the results of our implementations in Figs. 6.7 and 6.8. We measure a close-to-maximum violation of steering inequality $2-\epsilon$ with $\epsilon = 1.42 \cdot 10^{-2}$ on average, and $\epsilon_{\min} = 1.32 \cdot 10^{-2}$ in the best case. Thanks to this high violation and a relatively high coupling efficiency, we are able to certify the sending of an unknown qubit state through the untrusted channel, with a non-trivial transmission fidelity $F(\rho_i, \rho_o) > 50\%$. This is true even when Alice attributes all losses to the channel, *i.e.* $\lambda_c = 0$, for channels with the highest transmissivities. The certified fidelity increases as Alice trusts a larger amount of homogeneous losses λ_c, reaching value $F(\rho_i, \rho_o) = 77.1\% \pm 0.6\%$ when she assumes a maximum value $\lambda_c = 0.526$ and the channel is close to lossless. In any case, the certified fidelity decreases as the channel gets more lossy, as a direct consequence of bound (6.16), highlighting the difficulties of certifying lossy channels. This gives further motivation to ensure that a fraction of the losses are trusted, in order to certify, for example, long-distance quantum communications. In our implementation, assuming maximum trusted losses $\lambda_c = 0.526$, we could certify a non-trivial transmission fidelity $F(\rho_i, \rho_o) > 50\%$, for total transmissivities as low as $t(\mathcal{E}|\Phi_i) = \eta_s \simeq 0.263$, while such certification was possible only for $\eta_s \gtrsim 0.44$ with no trusted losses $\lambda_c = 0$.

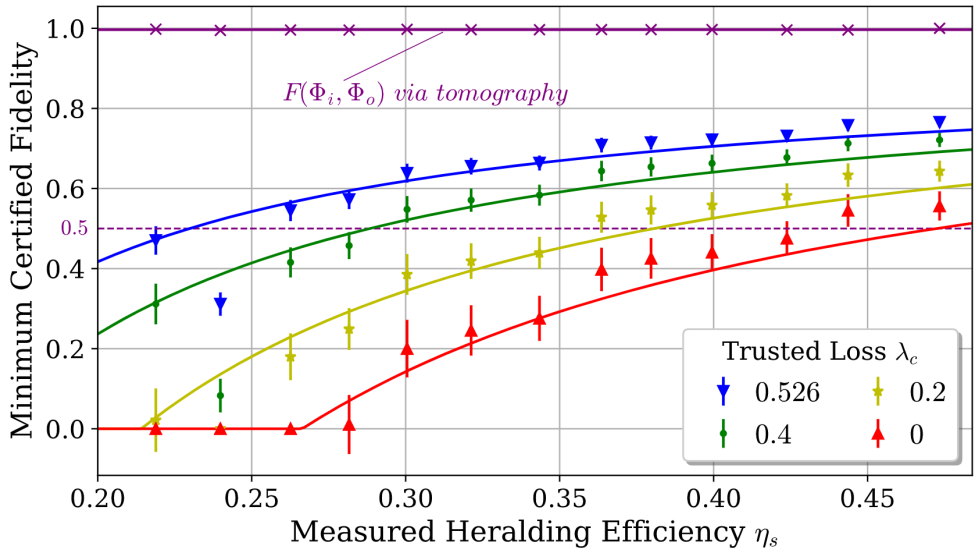


Fig. 6.7: Minimum fidelity $F(\rho_i, \rho_o)$ certified via our protocol, using an honest channel with different losses induced by the VOA. We display the data as a function of the measured heralding efficiency, and assume different amounts of trusted losses λ_c. Curves are plotted by taking the average fidelity of the probe state to a Bell state F^i, and the average of the deviation from maximum violation ϵ, over all protocol iterations. Experimental results deviate from these curves, as F^i and ϵ vary between implementations. Errors induced by the finite statistics (seen in equations 6.26 and 6.27) are directly subtracted to the certified fidelity. Error bars include errors induced by the unbalance in detectors' efficiency, and the propagation of errors on F^i. We also display the fidelity $F(\rho_i, \rho_o)$ measured via quantum state tomography, for $\rho_i = \Phi_i$.

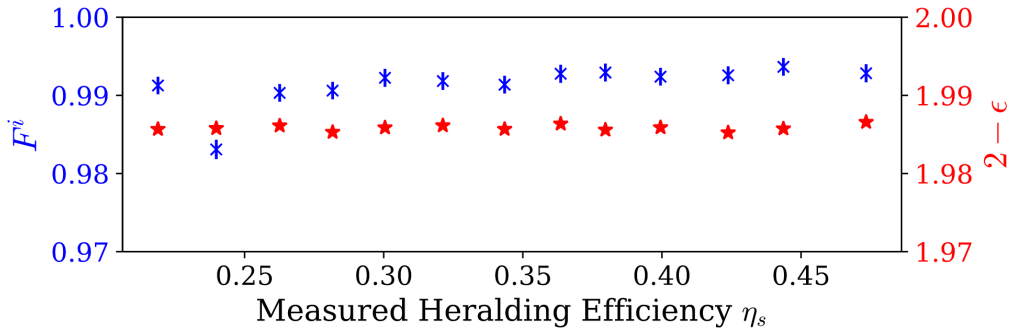


Fig. 6.8: Measured probe-state fidelity F^i to a maximally-entangled state, and close-to-maximum violation of steering inequality $2-\epsilon$.

In order to fully demonstrate the protocol, one should send a single input state ρ_i through the channel, hidden among the probe states. The specific choice of that state does not matter in our implementation as we do not use it in a later protocol, so we choose $\rho_i = \Phi_i$ and consider that a random copy of the probe state is actually the input state. To show the correctness of our protocol, we then perform a tomography of the corresponding output state ρ_o after the channel, and evaluate a transmission fidelity of $F(\rho_i, \rho_o) = 99.79\% \pm 0.02\%$ on average over all protocol attempts, with a minimum value of $F(\rho_i, \rho_o) = 98.7\% \pm 0.5\%$. This is far higher than the values certified by our protocol, as displayed on Fig. 6.7, which shows the state was indeed properly transmitted. Note that the channel and measurement stations are trusted during the output state's tomography, as it is performed outside of the protocol. This allows us to measure numerous copies of ρ_o, which is necessary for a full characterization of the state. In order to show the correctness of our certification protocol would hold for other input states ρ_i, we perform a full-process tomography of the quantum channel [179], and lower-bound the fidelity between the physical channel and the identity $\mathcal{F}_\diamond(\mathcal{E}, \mathbb{1}) \geq 94\% \pm 3\%$. We expect this bound to be far from tight, as it is evaluated using the equivalence between diamond and Choi-Jamiołkowski distances (theorem 5.3 from chapter 5). Still, the fidelity is greatly above the values certified by our protocol, showing the certification procedure is indeed valid for any input state ρ_i.

6.5.2 Results for a Dishonest Channel

The strength of our certification procedure is further shown by experimentally simulating examples of dishonest channels. Let us first recall that the channel operator has no information on the position of the input state ρ_i before the end of the protocol. This way, a typical attack consists in applying a disruptive transformation with small probability, hoping it will be applied to ρ_i and stay undetected by Alice and Bob. Here we consider such a transformation to be a bit flip $\hat{X}$ or a phase flip $\hat{Z}$. For this experimental demonstration, we remove the VOA and consider that all losses are trusted. Note that performing a phase flip is equivalent to turning Bob's first measurement B_0 into $-B_0$:

$$\hat{B}_0 = \hat{M}^{\mathscr{B}}_{0|0} - \hat{M}^{\mathscr{B}}_{1|0} \longrightarrow -\hat{B}_0 = \hat{M}^{\mathscr{B}}_{1|0} - \hat{M}^{\mathscr{B}}_{0|0}. \tag{6.36}$$

Similarly, a bit flip is equivalent to turning Bob's second measurement B_1 into $-B_1$. Thus, we perform these flips in practice by randomly changing the waveplates' angles in order to get the opposite measurement bases. This simulates dishonest channels of the form:

$$\mathcal{E}_{p,q}[\rho] = (1-p)(1-q)\rho + p(1-q)\hat{X}\rho\hat{X} + pq\hat{Y}\rho\hat{Y} + (1-p)q\hat{Z}\rho\hat{Z}, \tag{6.37}$$

where p, q are the bit flip and phase flip probabilities, respectively. In fact, we simulate approximately 5000 different channels $\mathcal{E}_{p,q}$ by performing a single 7-hours protocol run, and picking random measurement samples with different proportions of disrupted measurements. In order to simulate a larger variety of data samples, we perform that randomization at a 5 Hz-rate. We then generate the data for the certification of channel $\mathcal{E}_{p,q}$, by picking random samples with the following proportions:

- $q/2$ in basis $-\hat{A}_0\hat{B}_0$,
- $(1-q)/2$ in basis $\hat{A}_0\hat{B}_0$,
- $p/2$ in basis $-\hat{A}_1\hat{B}_1$,
- $(1-p)/2$ in basis $\hat{A}_1\hat{B}_1$.

The data acquired in basis $-\hat{A}_0\hat{B}_0$ and $-\hat{A}_1\hat{B}_1$ is then treated as if it was acquired in basis $\hat{A}_0\hat{B}_0$ and $\hat{A}_1\hat{B}_1$, respectively, when calculating the average violation of steering inequality $\mathcal{I} = |\langle\hat{A}_0\hat{B}_0\rangle + \langle\hat{A}_1\hat{B}_1\rangle|$. When performing this data acquisition, the probe state's fidelity to a Bell state is $F^i = 99.16\% \pm 0.04\%$, and we trust a maximum amount of losses $\lambda_c = 0.526$.

The certification results are displayed in Fig. 6.9, for different bit and phase flip probabilities. These show that our implementation is quite sensitive to these attacks, such that a flip probability of 0.01 induces a collapse of 16% of the certified fidelity, and we only certify $F(\rho_i, \rho_o) > 58\%$. The certified fidelity falls below the trivial value 50% for flip probabilities as low as 0.017. This way, any attempt of Eve to disrupt the input state ρ_i with such method can only succeed with very small probabilities $p, q < 0.02$, or will be detected by Alice and Bob.

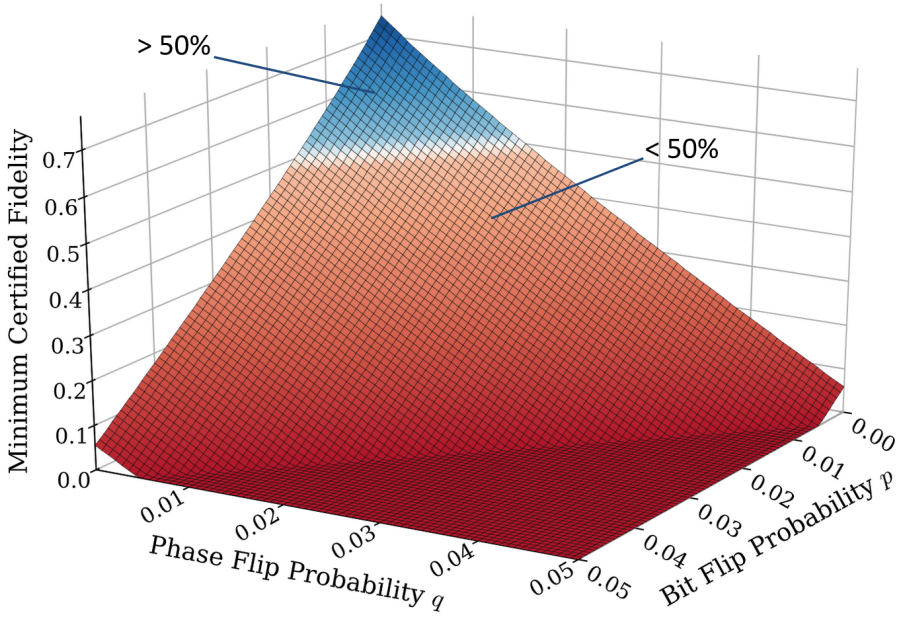


Fig. 6.9: Minimum fidelity $F(\rho_i, \rho_o)$ certified via our protocol, for malicious channels $\mathcal{E}_{p,q}$, with p, q the bit/phase flip probabilities, respectively.

6.5.3 Additional Implicit Assumptions

Due to technical limits, a few additional but reasonable assumptions are made in the course of our experiments, in order to draw conclusions from these implementations. We detail these in the following.

First, we assume Alice and Bob can communicate via a trusted private classical channel. It allows the players to agree on their measurement settings, Alice to send Bob the position r of the input state ρ_i, and Bob to tell Alice if the states were properly received. This way the players can perform measurements on the fly, instead of storing all the states, then deciding of the measurement bases and finally measuring the states, which would require a billion of quantum memories with hours-long storage-time. This effectively slightly changes the recipe of the protocol we implement in practice. We detail this recipe in the following protocol box. We assume the security to be the equivalent to that of protocol 6.1.

Protocol 6.3: Practical certified quantum transmission via Bell theorem

1. Prior to the protocol:

   (a) Alice characterizes the state Φ_i emitted by her source and evaluates the quantity F^i. She also receives or prepares the state ρ_i, possibly shared with an outside party.

   (b) Eve announces the minimum transmissivity t of the channel $\mathcal{E}$ for any quantum state.

2. Alice and Bob agree on parameters ϵ, K, depending on their requirements and experimental limitations. They also privately agree on the random position of the input state $r \leq N+1$, with $N = \lceil K/t \rceil$.

For k from 1 to $N+1$:

3. If $k \neq r$:

   (a) Alice prepares a copy of the probe state Φ_i and sends half of it through the channel.

   (b) Alice and Bob privately agree on a random $q \in \{0,1\}$ and measure the observable $\hat{A}_q \hat{B}_q$, with an outcome $c_k = a_k b_k$ if Bob received a state, or no outcome if the state was lost through the channel.

4. If $k = r$:

   (a) Alice sends ρ_i through the channel.

   (b) If Bob does not receive any state, the protocol aborts. Otherwise, Bob sets the state aside.

5. If the number of "no-outcome" events during step 3.(b) is bigger than $N-K$, then the protocol aborts.

6. From the correlations $\{c_k\}$, Alice and Bob deduce the average value over all rounds, of $\mathcal{I} = |\langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle|$.

7. If $\mathcal{I} \geq 2-\epsilon$, then Alice successfully sent the state $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ to Bob, with a certified average fidelity to ρ_i, up to isometry.

Secondly, the fair sampling assumption is required on the measurement apparatus for the self-testing procedure, as we allow a large amount of losses to be induced by the quantum channel. Alice's measurement apparatus is completely trusted and characterized, according to the one-sided device-independent scenario. On Bob's side, we assume the efficiency of the measurement apparatus to be independent of the measurement setting $\hat{B}_0$ or $\hat{B}_1$. If the efficiency depends on the state measured, then we consider that dependence to be part of the quantum channel. A slight unbalance of efficiency is allowed between the two different measurement outcomes, and we show in the appendix D.2 that the error induced by this unbalance is negligible. Still, this assumption opens the detection loophole [57], which is therefore inherent to the certification of lossy channels.

6.6 Discussion

In this chapter we have provided a first protocol to certify the transmission of a qubit through an untrusted and lossy quantum channel, by probing the latter with close-to-maximally entangled states and witnessing steering at its output. Our theoretical investigations rely mostly on assumptions made on the probe state's source and the sender's measurement apparatus, while very few assumptions are made on the quantum channel and the receiver's measurement apparatus. This setting proves to be an interesting trade-off between realistic experimental conditions and reasonable cryptographic requirements. It also embodies a practical scenario in which a strong server provides a weaker receiver with a quantum bit.

Compared to previously proposed verification procedures, our protocol not only certifies the probed channels, but also an unmeasured channel through which a single unknown state can be sent. As quantum measurement deteriorates the quantum states, this task can only be performed at the price of measuring a huge amount of probe states, which limits the repeatability of the protocol with current technology. Until further theoretical considerations or technological improvements provide higher repeatability, our protocol can still serve as a practical primitive for other single-shot protocols that require a single quantum state, such as the quantum weak coin-flipping protocol presented in chapter 4.

Our proof-of-principle implementation shows the correctness of this certification procedure, and its feasibility with current technology. This way we could certify non-trivial transmission fidelities for a wide range of losses induced by the channel, by making some mild but realistic assumptions, such as the characterization of a fraction of trusted losses, induced for instance by the coupling of probe states inside optical fibers. By implementing random bit and phase flips, we could show that even a highly improbable attempt to disrupt the quantum information degrades the certified transmission fidelity, and is therefore detected by the players.

Future developments could demonstrate the feasibility of a version of our protocol with full device-independence, in which Alice's measurement or even the probe states' source are not trusted. Such protocol could be achieved by linking the probe state's quality to that of the corresponding output state, or by making the IID assumption on the probe state's source. Also, more investigation on quantum-memory-based attacks could give a sharper idea on the possibilities of deceiving the certification procedure.

This work opens the way to certification of a wide variety of more sophisticated lossy quantum channels. In particular, the rapid improvements of quantum technologies could soon provide possible applications of this protocol to the authentication of quantum teleportation, memories or repeaters.

'Le temps est le meilleur des critiques;
et la patience le meilleur des professeurs.'

— Frédéric Chopin.

CHAPTER 7

CONCLUSION

For the past couple of decades, the field of quantum communications has become most fruitful, providing a wide variety of information-theoretic secure primitives for a potential future quantum network. These have the potential to ensure a stronger security than the current classical protocols relying on computation assumptions. Making such quantum protocols concrete has required to overcome practical and fundamental challenges, some of which are only starting to be addressed thanks to the availability of new quantum technologies, such as high-efficiency single-photon detectors and deterministic single-photon sources [180]. This work has been intended to contribute to this effort, by developing and demonstrating new quantum primitives in the lab, thanks to a photon source built from scratch during the preparation of this thesis.

This photon-pair source, presented and characterized in chapter 3, was shown to be a promising candidate as a resource for the implementation of quantum network protocols. In particular the high heralding efficiency of the photons makes it suitable for numerous single-photon based protocols such as quantum weak coin flipping presented in chapter 4, and the high fidelity of the biphoton polarization-state to a maximally-entangled state enables device-independent-type protocols, such as that detailed in chapter 6 for certified quantum transmission through an

untrusted channel. In the future, some important modifications could be made on the setup, to improve its performances or provide more complex applications. In particular, at the time of the writing of this manuscript, a second source is being built in the lab, with very close characteristics to the one which was detailed here, but with limited noise, which should enhance the quality of close-to-maximally-entangled states. In addition, we provided a possible adaptation to our source, in order to demonstrate a novel compact layout for a multipartite-state generation. This could be used to demonstrate new protocols such as anonymous transmissions [122], authenticated teleportation [26] or composable GHZ-state verification [121].

We first used our source to generate heralded single-photons, allowing to demonstrate the first information-theoretic and cheat-sensitive weak coin flipping protocol in chapter 4, thanks to path-encoded entanglement. This way, even if players can bias the protocol in their favor, they can never do so without risking being sanctioned for cheating. Interestingly enough, in the absence of loss in the setup, the protocol we designed approaches a unit success probability, meaning it always designates a winner. This motivates further experimental investigations in order to minimize the losses in our implementation, by using integrated optics for instance. In addition such an information-theoretically secure and cheat-sensitive protocol for weak coin flipping was never proposed in classical cryptography, showing a concrete advantage brought by quantum systems.

We then used the source to generate photon-pairs entangled in polarization, allowing to demonstrate a novel protocol for the certification of quantum transmission through an untrusted and lossy quantum channel in chapter 6. Building this protocol required some new fundamental theoretical developments on lossy quantum channels, which are detailed in 5. This way, thanks to self-testing of a steering inequality, we could certify the transmission of an unmeasured state through the channel, in a semi-device independence setting. This assumption was used as a trade-off, ensuring security in a relatively realistic scenario in which the sender is trusted, while the channel and receiver's apparatus are not. More theoretical developments may extend this implementation to a fully device-independent setting, or experimental authenticated teleportation.

This last protocol showed how adapting theoretical quantum primitives for practical quantum network applications often implies making important assumptions, therefore deviating from the ideal recipes. What remains of the so-called quantum advantage can then legitimately be questioned. In the case of authenticated teleportation [26], or more generally the certification of quantum transmission via untrusted channels presented in chapter 6, realistic but nonetheless important assumptions are required in order to derive practical applications. This involves trusting a part of the setup, or assumptions on the statistics of untrusted states or measurement outcomes. We see then that to build a practical and fully secure quantum network, one has to address the implication of any assumption made in the primitives. This may involve stacking different verification procedures, or developing ways of detecting potential disruption or cheating strategies, such as the cheat-sensitivity displayed by our weak coin flipping protocol. In this context, the composability of protocols is an important property to seek out for, as found in the recently proposed composable GHZ-state verification [121].

Another important aspect of quantum protocols, which was not tackled in this thesis, is their energetic footprint. In the context of resources scarcity and climate emergency, this was recently pointed out by A. Auffèves as a major feature to consider when building quantum computers [181], and by extension a world-wide quantum network. Let us for instance consider the certification of quantum transmission through an untrusted channel. With our protocol and the current technology, certifying the transmission of a single qubit requires a few kJ of pump power, for a good level of security. For now, this makes it impractical to certify the sending of every qubit in a quantum network with such a protocol. Different solutions may be explored to reduce this energy consumption and make quantum protocols more practical. This includes experimental efforts in order to lower the energy required to obtain quantum resources, but also theoretical efforts in order to build protocols which require a minimum amount of quantum resources [182]. Finally, more assumptions may have to be made on protocols, highlighting a trade-off between energy consumption and optimal network security. This might temper the quantum advantage of certain primitives.

APPENDIX A

QUANTUM STATE TOMOGRAPHY

Characterizing the state of a quantum system remains an open question in the field of quantum information, as one cannot get a complete knowledge of the state of a system by performing a single measurement. Still *quantum state tomography* allows to estimate the density operator of a system, by performing several measurements on different copies of the system. In the following, we detail that method that is used extensively in polarization-based photonic experiments, in the specific 2-qubits case.

A.1 General Method

The idea of qubits-state tomography was first presented by D.F. James et al. in 2001 [51]. It makes use of the decomposition of any $n-$qubits density operator as a linear combination of tensor products of Pauli operators, which reads, in the 2-qubits case:

$$\rho = \frac{1}{4} \sum_{i_A, i_B=0}^{3} \mathrm{Tr}(\rho \cdot \hat{\sigma}_{i_A} \otimes \hat{\sigma}_{i_B}) \cdot \hat{\sigma}_{i_A} \otimes \hat{\sigma}_{i_B} = \frac{1}{4} \sum_{i_A, i_B=0}^{3} \langle \hat{\sigma}_{i_A} \otimes \hat{\sigma}_{i_B} \rangle_\rho \cdot \hat{\sigma}_{i_A} \otimes \hat{\sigma}_{i_B}, \qquad \text{(A.1)}$$

where $\{\hat{\sigma}_k\}_{k=0,\dots,3}$ are Pauli operators (see paragraph 2.1.3). The expectation values $\langle \hat{\sigma}_{i_A} \otimes \hat{\sigma}_{i_B} \rangle_\rho$ can be estimated via the method described in paragraph 3.4. Injecting

these in eq. (A.1), we get an estimation of ρ, called the *Direct Inversion Operator* (DI operator). In general, because of fluctuations in the experimental measurements, this operator is not a physical density operator, as it displays negative eigenvalues. A common workaround is to use the *maximum likelihood estimation* (MLE) method [52], which consists in finding the physical density operator that is the most likely to return our experimental data. Making a few minor assumptions which are acceptable in our case such as a Gaussian statistics of measurement data, a fast version of the MLE can be derived [183]. In this way, one only has to find the density operator ρ that minimizes its Hilbert-Schmidt distance to the DI operator μ:

$$D_2(\hat{\mu}-\hat{\rho})^2 = \mathrm{Tr}[(\mu-\rho)^2] = \sum_{i,j=1}^{4} |\mu_{i,j}-\rho_{i,j}|^2. \tag{A.2}$$

Note this distance can be written in an eigenbasis $\{|\mu_i\rangle\}$ of μ, in which the optimal ρ should also be diagonal, such that:

$$D_2(\hat{\mu}-\hat{\rho})^2 = \sum_{i=1}^{4} |\mu_i-\rho_i|^2, \tag{A.3}$$

where $\{\mu_i\}$ and $\{\rho_i\}$ are the eigenvalues of μ and $\hat{\rho}$ respectively, with the two constraints $\sum_i \rho_i = 1$ and $\rho_i > 0$. This way, we find these optimal eigenvalues using a fast algorithm provided in [183]. Hence the optimal matrix would be:

$$\hat{\rho}_{opt} = \sum_{i=1}^{4} \rho_i |\mu_i\rangle\langle\mu_i|. \tag{A.4}$$

This method was demonstrated to be highly efficient, allowing the reconstruction of 8-qubits states in less than a few minutes. In addition, one can use the linear regression estimation method [184] to get a better estimation of the DI operator μ.

A.2 Error Analysis

In order to estimate the errors in the reconstructed quantum state, we follow the method detailed in [52]. In our experiments, the PBSs in polarization analyzers have a very high extinction ratio, such that the number of $|H\rangle$-polarized photons going on the $|V\rangle$-side of the analyzer is negligible, and vice versa. Furthermore, the background noise is negligible, thanks to the low dark-count rates of our

detectors. This way, systematic errors are mostly caused by differences in the detectors' efficiencies. Relative efficiencies can be evaluated by exchanging the roles of detectors in each polarization analyzer, and the measurement data can then be corrected to account for the potential efficiency unbalance. Another source of systematic error is the uncertainty in the position of our WPs axis, which is evaluated when calibrating the polarization analyzers. It potentially induces a shift in the angles displayed in Tab. 3.1, which we treat as a statistical error. Another source of statistical error is the Poisson noise in the photon counting, that we minimize by measuring a large amount of states (more than 10^7 for each measurement basis). Uncertainties on the reconstructed states, induced by this noise and systematic errors in the WPs angles, are evaluated by using the Monte Carlo method. This way, we simulate 1000 new data samples with random perturbations, from which we reconstruct 1000 new density matrices. From these we evaluate the standard deviation on any relevant quantities related to the quantum state. Finally, tests on the fast MLE method showed that the numerical reconstruction itself involved no significant error, provided the number of copies of the state measured was large enough, typically $> 10^7$ in each measurement basis.

APPENDIX B

SAGNAC SOURCE ALIGNMENT

Even though Sagnac sources are well known and characterized, we found very few recipes for the alignment of the whole optical setup. In the following we detail our own recipe, developed with some inspiration from [115]. This recipe is meant to be quite systematic, and was repeated many times in order to obtain close-to-maximally-entangled states. The main components we refer to are displayed in Fig. B.1.

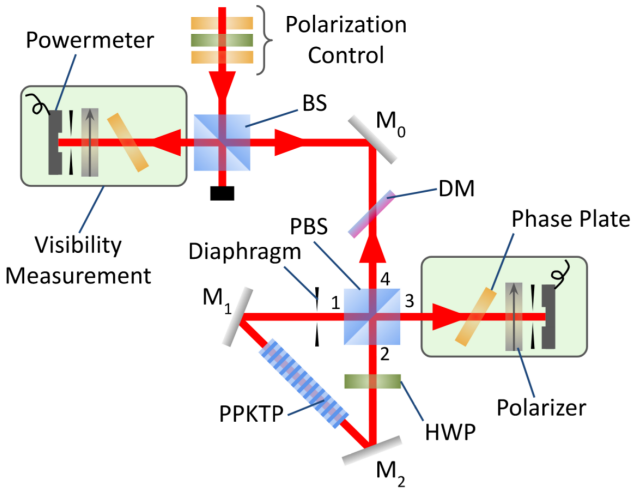


Fig. B.1: Configuration of the setup in our alignment recipe, including the most important components. Numbers label each side of the PBS.

1. Align the pump beam horizontally, and along a row of holes of the optical table. Place all the optics required for the pump shaping, including focusing lenses and WPs for polarization control.

2. Place the non-polarizing BS in the path of the beam, such that the reflected beam is horizontal and approximately perpendicular to the incident beam. The BS is supposed to stay in place after the alignment of the source.

3. Place the mirror M_0 in the path of the reflected beam. Tune the mirror's angles in order to make the beam as horizontal as possible, and aligned along a row of hole of the optical table. This step is of major importance and determines how many iterations of the Sagnac alignment will be required.

4. Place the dichroic mirror in the path of the beam, at rougly 45°. Any optics that might deviate the pump beam should also be placed at this step.

5. Place the PBS in the path of the beam. Tune its angles so the reflected beam is as horizontal as possible, and perpendicular to the incident beam (aligned along a line of holes).

6. Rotate the polarization of the pump beam, such that the reflected and transmitted beam after the PBS are of similar intensity.

7. Place a mirror on each sides of the PBS, at equal distances of the faces. The incident angle of the beam should be $\approx 22.5°$ on both mirrors, so the beam coming from side 1 goes back to the PBS on side 2, and vice versa.

8. With a semi-transparent sheet (such as an optical cleaning tissue), check the beams' positions on sides 1 and 2 of the PBS. Tune the mirrors' angles until clockwise and anticlockwise beams are visibly overlapped on both sides.

9. Equalize the power of clockwise and anticlockwise beams with the help of a powermeter, by rotating the polarization of the pump beam.

10. Place a QWP after side 3 of the PBS, at 0° (axes aligned to horizontal and vertical polarization, relatively to the PBS), as well as a polarizer at ±45°.

11. Check the interference pattern after the polarizer with a powermeter, by tilting the QWP around its vertical axis. If steps 3., 5. and 8. were done correctly, one should already note a non-zero visibility:

$$V = \frac{|P(45°) - P(-45°)|}{P(45°) + P(-45°)}, \tag{B.1}$$

where $P(\pm 45°)$ is the power measured when the polarizer is at $\pm 45°$.

12. Tune the mirrors' angles in order to maximize the visibility, and write down the value reached $V_{\max}$. This value can be increased by placing a diaphragm in front of the powermeter, which filters out side-reflections that do not correspond to the mode coupled in SM fibers.

At this stage, the Sagnac interferometer may seem aligned, particularly if steps 3. and 5. were done properly. However, many geometrical configurations allow the interference to be optimized at the output of the Sagnac, without the clockwise and anticlockwise beams overlapping inside the interferometer, as displayed in Fig. B.2. For this reason, we provide a few additional steps, in order to check the overlap of the beams, and correct their position.

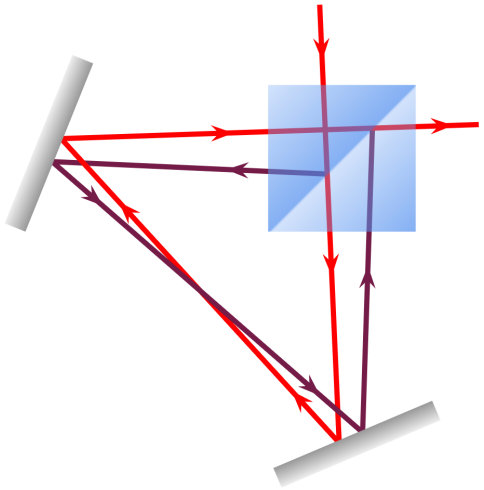


Fig. B.2: An example of Sagnac configuration, that may display a high visibility though the beams are not overlapped inside the interferometer.

13. As in step 8. check the overlap of the beams with a semi-transparent sheet. However this time, instead of tuning mirrors M_1 and M_2, tune the angles of

mirror M_0, until the beams are seemingly overlapped. Tuning this mirror allows to control the configuration of the beams inside the interferometer, while maintaining a relatively high interference at the output of the Sagnac.

14. Place a diaphragm inside the Sagnac, mounted on a fine transversal translation stage, close to side 1 of the PBS. Remove the polarizer and keep the powermeter in place.

15. Close the diaphragm, and maximize the transmitted power, by tuning both the angles of M_0 and the diaphragm transversal position. When the transmitted power is maximized, the clockwise and anticlockwise beams are maximally overlapped inside the interferometer.

16. Open the diaphragm, and place the polarizer back in front of the powermeter. Check the interference visibility V_{final} as in step 11.. If this visibility is higher or equal to the value that was previously reached $V_{\text{max}} \lesssim V_{\text{final}}$, then the Sagnac interferometer is aligned. Otherwise, repeat steps 12. to 16. until reaching this condition.

Among other factors, the number of iterations of steps 12. to 16. depends on the precision of the alignments in steps 3. and 5.. After step 16., we should not touch the mirrors M_0, M_1, M_2, nor the PBS or any optics which might deviate the pump beam. Now we only need to properly place the HWP and PPKTP crystal.

17. Place the HWP inside of the interferometer, with its axes aligned to horizontal and vertical polarizations, as perpendicular to the beam as possible.

18. Check the interference visibility, as done in step 11.. Carefully tilt the HWP until you reach a value V_{final} measured in step 16.. If the visibility cannot reach this value, try rotate the HWP at $\pm 90°$ or $180°$ and repeat the procedure. If the visibility is still lower than V_{final}, then the interferometer is probably misaligned. It is recommended to restart the alignment from scratch.

19. Fix the HWP to the optical table, while checking the visibility remains at V_{final}. Rotate it at $\pm 45°$ in order to minimize the power that goes out on side 3 of the PBS. This way all power goes backward on side 4. Half of this power can be measured on the left side of the BS, as shown in Fig. B.1.

20. Place the PPKTP crystal on the path of the beam, in the center of the interferometer. If possible, the crystal should be mounted on a multi-axes platform. Maximize the power transmitted on the side of the BS, by roughly positioning the crystal.

21. Measure the interference visibility on the side of the BS, using the same method as described in step 11. and shown in Fig. B.1. Carefully tilt the crystal in all possible directions, until you reach a value V_{final} measured in step 16.. Here it is highly recommended to place a diaphragm in front of the powermeter, as side reflections are more likely to degrade the interference.

After this last step, provided the visibility V_{final} was reached, the source is optimally aligned, and no optics should be touched inside or before the Sagnac for the remainder of the experiment, except for rotating waveplates. Then one just has to collect the photons inside optical fibers and optimize the state, which is described in other works [115].

The particularity of our alignment method compared to more common ones resides in the steps 13. to 16., in which we tune the incidence angle of pump in the interferometer, though it is seemingly aligned. Adding this procedure seems indispensable in order to check the beams are overlapped inside the Sagnac, even when one perfectly aligns the pump beam before alignment of the interferometer. When using a particularly long crystal, as our 30 mm-long PPKTP, placing it inside the Sagnac without performing those steps may result in loss of coherence between the two sides of the interferometer, distortions in the photon's spectral and spatial modes, or a drop in the pair's emission rate.

Also, note that in step 21., we do not measure the interference pattern after the Sagnac, as in steps 11. and 18.. The reason is that because of the crystal's birefringence, placing that crystal inside the Sagnac introduces a path difference of $\approx 3\,\text{mm}$ between the clockwise and anticlockwise beams, as long as the HWP is at 0°. This result in partial or total loss of coherence, particularly in pulsed mode, where the pump beam has a coherence length of $\approx 0.6\,\text{mm}$. When rotating the HWP at ±45°, the transmitted horizontally-polarized beam is rotated to vertical

polarization, so both reflected and transmitted beam enter the crystal with the same polarization and experience no path difference. This way, we retrieve a high visibility, and the beam is sent backward, so we can measure the interference pattern on the left of the BS. Still, this BS can hardly be removed for the pump's path without disaligning the setup, such that 50 % of the pump power does not contribute to the generation of pairs in this Sagnac interferometer. In many cases though, the pump power that is transmitted through the BS can be sent to another source of photons. The two sources can be used independently, or to perform multi-photons experiments. In our specific case, this BS is used as an integral part of the spatial multiplexer, described in Fig. 3.24.

APPENDIX C

QUANTUM WEAK COIN FLIPPING: PREDICTIONS

In the following we give some theoretical predictions for the results we observe in our experimental implementation of cheat-sensitive weak coin flipping, presented in chapter 4. In the first two sections, we derive general expressions for event probabilities, for any values of beam splitter reflectivities x, y, and z. In the third section we obtain the values of these reflectivities which maximize fairness and correctness, when both parties are honest, as well as the probabilities of the different outcomes. Finally, we show such predictions when one of the parties is dishonest and performs an attack which we implement in this work. In general, these predictions differ from those derived in previous work [48], as we drop the *balancing* condition for the correctness, and we adopt a different parametrization. We give some development on that matter in the last section.

C.1 Photon Propagation in the Interferometer

We first describe the propagation of the photon in the interferometer (see Fig. C.1), for any values of x, y, z, and deduce the probabilities of the different events. To simplify our proofs, we neglect dark counts and double-pair emissions. Experimental

details in chapters 3 and 4 support the legitimacy of this approximation. In this scenario, when Alice detects a photon in detector D_{herald}, then exactly one photon is generated, corresponding to the action of the creation operator $a_1^\dagger$. Some first losses occur when coupling the photon to single-mode fibers, such that the operator transforms as:

$$a_1^\dagger \longrightarrow \sqrt{\eta_c}\, a_1^\dagger, \tag{C.1}$$

where η_c is the induced transmission. Then Alice sends the photon to a BS of reflectivity x:

$$\sqrt{\eta_c}\, a_1^\dagger \longrightarrow \sqrt{x\eta_c}\, a_1^\dagger + \sqrt{(1-x)\eta_c}\, a_2^\dagger, \tag{C.2}$$

where 1 (resp. 2) stands for the reflected (resp. transmitted) mode. Alice keeps mode 1 and Bob gets mode 2. On each side, the photon undergoes losses due to fiber transmission and connectors, storage, and diverse other components. We note η_{A1} (resp. η_{B1}) the transmission on Alice's (resp. Bob's) side. Some phases are also induced by the propagation, and we note Φ_{A1} (resp. Φ_{B1}) the phase introduced on Alice's (resp. Bob's) side. In this way, we get the following transformation:

$$\sqrt{x\eta_c}\, a_1^\dagger + \sqrt{(1-x)\eta_c}\, a_2^\dagger \longrightarrow \sqrt{x\eta_c\eta_{A1}}\, e^{i\Phi_{A1}} a_1^\dagger + \sqrt{(1-x)\eta_c\eta_{B1}}\, e^{i\Phi_{B1}} a_2^\dagger. \tag{C.3}$$

Bob sends the photon to a BS of reflectivity y:

$$\begin{aligned} \sqrt{x\eta_c\eta_{A1}}\, e^{i\Phi_{A1}} a_1^\dagger + \sqrt{(1-x)\eta_c\eta_{B1}}\, e^{i\Phi_{B1}} a_2^\dagger & \\ \longrightarrow \sqrt{x\eta_c\eta_{A1}}\, e^{i\Phi_{A1}} a_1^\dagger + \sqrt{(1-x)y\eta_c\eta_{B1}}\, e^{i\Phi_{B1}} a_2^\dagger & \\ + \sqrt{(1-x)(1-y)\eta_c\eta_{B1}}\, e^{i\Phi_{B1}} a_3^\dagger. & \end{aligned} \tag{C.4}$$

Bob sends the third mode to the detector D_B, inducing another loss. We note η_y the transmission, including the detector efficiency, and we have $\eta_B^y = \eta_c\eta_{B1}\eta_y$ (here we omit the dephasing as no interference will occur in this mode). The second mode undergoes some loss and dephasing, and we note η_{B2} and Φ_{B2} the transmission and dephasing. There we note $\eta_B = \eta_c\eta_{B1}\eta_{B2}$ the total loss on Bob's arm of the interferometer, and $\Phi_B = \Phi_{B1} + \Phi_{B2}$ the total dephasing. On Alice's side, the path depends on the detection of the third mode that triggers the optical switch. In absence of dark counts and when Bob is honest, a detection on the third mode means no detection will occur on Alice's verification detector, such that Bob is not sanctioned and wins the coin flip. In other words, Alice trusts Bob's measurement

on the third mode, such that we can omit her verification detector and the optical switch. In that case she simply sends the first mode to Bob to proceed to verification of the state. That mode undergoes some loss and dephasing, and we note η_{A2} and Φ_{A2} the transmission and dephasing. There we note $\eta_A = \eta_c \eta_{A1} \eta_{A2}$ the total loss on Alice's arm of the interferometer, and $\Phi_A = \Phi_{A1} + \Phi_{A2}$ the total dephasing. The total transformation becomes:

$$\begin{aligned} &\sqrt{x\eta_c\eta_{A1}}\, e^{i\Phi_{A1}} a_1^\dagger + \sqrt{(1-x)y\eta_c\eta_{B1}}\, e^{i\Phi_{B1}} a_2^\dagger + \sqrt{(1-x)(1-y)\eta_c\eta_{B1}}\, e^{i\Phi_{B1}} a_3^\dagger \\ &\longrightarrow \sqrt{x\eta_A}\, e^{i\Phi_A} a_1^\dagger + \sqrt{(1-x)y\eta_B}\, e^{i\Phi_B} a_2^\dagger + \sqrt{(1-x)(1-y)\eta_B^y}\, e^{i\Phi_B} a_3^\dagger. \end{aligned} \tag{C.5}$$

After receiving the first mode, Bob makes it interfere with the second mode on a BS of reflectivity z, such that we get:

$$\begin{aligned} &\sqrt{x\eta_A}\, e^{i\Phi_A} a_1^\dagger + \sqrt{(1-x)y\eta_B}\, e^{i\Phi_B} a_2^\dagger + \sqrt{(1-x)(1-y)\eta_B^y}\, e^{i\Phi_B} a_3^\dagger \\ &\longrightarrow (\sqrt{xz\eta_A}\, e^{i\Phi_A} + \sqrt{(1-x)y(1-z)\eta_B}\, e^{i\Phi_B}) a_1^\dagger \\ &\qquad - (\sqrt{x(1-z)\eta_A}\, e^{i\Phi_A} - \sqrt{(1-x)yz\eta_B}\, e^{i\Phi_B}) a_2^\dagger \\ &\qquad + \sqrt{(1-x)(1-y)\eta_B^y}\, e^{i\Phi_B} a_3^\dagger. \end{aligned} \tag{C.6}$$

Bob sends the first and second modes to detectors D_{V_1} and D_{V_2}, with efficiencies η_{V_1} and η_{V_2}, and we note $\eta_A^{V_1} = \eta_A \eta_{V_1}$, $\eta_A^{V_2} = \eta_A \eta_{V_2}$, $\eta_B^{V_1} = \eta_B \eta_{V_1}$, and $\eta_B^{V_2} = \eta_B \eta_{V_2}$. Up to an irrelevant global phase $e^{i\Phi_A}$, we get:

$$\begin{aligned} &(\sqrt{xz\eta_A}\, e^{i\Phi_A} + \sqrt{(1-x)y(1-z)\eta_B}\, e^{i\Phi_B}) a_1^\dagger \\ &\qquad - (\sqrt{x(1-z)\eta_A}\, e^{i\Phi_A} - \sqrt{(1-x)yz\eta_B}\, e^{i\Phi_B}) a_2^\dagger \\ &\qquad + \sqrt{(1-x)(1-y)\eta_B^y}\, e^{i\Phi_B} a_3^\dagger \\ &\longrightarrow \left(\sqrt{xz\eta_A^{V_1}} + \sqrt{(1-x)y(1-z)\eta_B^{V_1}}\, e^{i\Delta\Phi}\right) a_1^\dagger \\ &\qquad - \left(\sqrt{x(1-z)\eta_A^{V_2}} - \sqrt{(1-x)yz\eta_B^{V_2}}\, e^{i\Delta\Phi}\right) a_2^\dagger \\ &\qquad + \sqrt{(1-x)(1-y)\eta_B^y}\, e^{i\Delta\Phi} a_3^\dagger, \end{aligned} \tag{C.7}$$

where $\Delta\Phi = \Phi_B - \Phi_A$ is the phase difference. We deduce the detection probabilities in each detector:

$$P_{V_1} = \mathbb{P}_h\big((b,v_1,v_2)=(0,1,0)\big) = xz\eta_A^{V_1} + (1-x)y(1-z)\eta_B^{V_1} + 2\cos(\Delta\Phi)\sqrt{x(1-x)yz(1-z)\eta_A^{V_1}\eta_B^{V_1}}, \tag{C.8}$$

$$P_{V_2} = \mathbb{P}_h\big((b,v_2)=(0,1)\big) = x(1-z)\eta_A^{V_2} + (1-x)yz\eta_B^{V_2} - 2\cos(\Delta\Phi)\sqrt{x(1-x)yz(1-z)\eta_A^{V_2}\eta_B^{V_2}}, \tag{C.9}$$

$$P_{D_B} = \mathbb{P}_h\big((b,a)=(1,0)\big) = (1-x)(1-y)\eta_B^{y}. \tag{C.10}$$

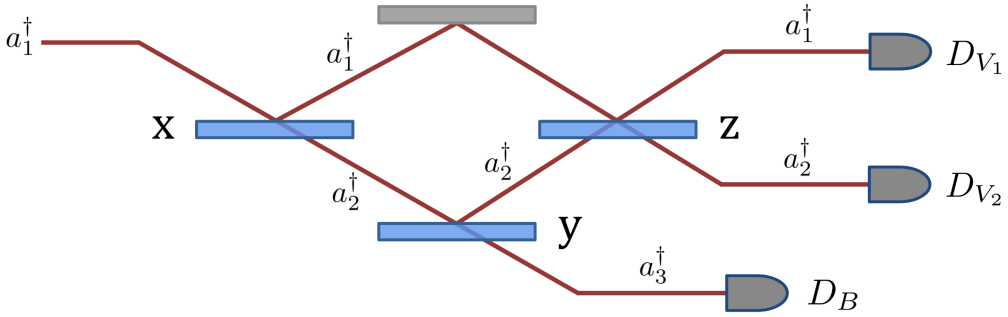


Fig. C.1: Sketch of the interferometer with most relevant notations.

C.2 Phase Fluctuations

In our experiment, the phase difference $\Delta\Phi$ evolves through time, because of thermal fluctuations and diverse vibrations or noise. Slow phase drifts, typically caused by thermal fluctuations, are generally resolved when counting photons, provided the photon rate is high enough. Fast phase fluctuations however, typically caused by noise, are hard to resolve by counting photons, due to low rates and detector recovery time. Hence, the probabilities P_{V_1} and P_{V_2} are averaged over the typical temporal resolution τ of our detectors. We distinguish two types of behaviour in the phase difference $\Delta\Phi(t) = \Delta\Phi_f(t) + \Delta\Phi_s(t)$, with $\Delta\Phi_f(t)$ corresponding to fast fluctuations of typical period $\tau_f \ll \tau$, and $\Delta\Phi_s(t)$ corresponding to slow fluctuations of typical period $\tau_s \gg \tau$. For fast fluctuations, the average value $\langle\cos\Delta\Phi_f\rangle_\tau$ is approximately constant. For slow fluctuations, the value of $\Delta\Phi_s(t)$ is approximately constant over a time lapse of τ. In this way, we get:

$$\begin{aligned}\langle\cos\Delta\Phi\rangle_\tau(t) &= \langle\cos(\Delta\Phi_f+\Delta\Phi_s)\rangle_\tau(t)\\ &= \langle\cos\Delta\Phi_f\cos\Delta\Phi_s\rangle_\tau(t)-\langle\sin\Delta\Phi_f\sin\Delta\Phi_s\rangle_\tau(t_0)\\ &= \langle\cos\Delta\Phi_f\rangle_\tau\cos\Delta\Phi_s(t)-\langle\sin\Delta\Phi_f\rangle_\tau\sin\Delta\Phi_s(t)\\ &= v\left(\mathrm{C}\cdot\cos\Delta\Phi_s(t)-\mathrm{S}\cdot\sin\Delta\Phi_s(t)\right),\end{aligned} \tag{C.11}$$

with $v := \sqrt{\langle\cos\Delta\Phi_f\rangle_\tau^2+\langle\sin\Delta\Phi_f\rangle_\tau^2}$, $\mathrm{C} := \langle\cos\Delta\Phi_f\rangle_\tau/v$, and $\mathrm{S} := \langle\sin\Delta\Phi_f\rangle_\tau/v$. By definition we have $\mathrm{C}^2+\mathrm{S}^2=1$, so there exists a phase Φ_{eff} with $\mathrm{C}=\cos\Phi_{\text{eff}}$ and $\mathrm{S}=\sin\Phi_{\text{eff}}$. We then get:

$$\begin{aligned}\langle\cos\Delta\Phi\rangle_\tau(t) &= v\left(\cos\Phi_{\text{eff}}\cos\Delta\Phi_s(t)-\sin\Phi_{\text{eff}}\sin\Delta\Phi_s(t)\right)\\ &= v\,\cos(\Delta\Phi_s(t)+\Phi_{\text{eff}}).\end{aligned} \tag{C.12}$$

Here Φ_{eff} appears as an additional constant dephasing, such that we can include it inside the slow dephasing $\Delta\Phi_s(t_0)$. Effectively, it means taking $\Phi_{\text{eff}}=0$, such that $\mathrm{S}=0$ and $\langle\sin\Delta\Phi_f\rangle_\tau=0$. In this way, we have:

$$\langle\cos\Delta\Phi\rangle_\tau(t) = v\,\cos\Delta\Phi_s(t), \tag{C.13}$$

with $v=|\langle\cos\Delta\Phi_f\rangle_\tau|\in[0,1]$, that we later interpret as the interference visibility. Now we average P_{V_1} and P_{V_2}:

$$\begin{aligned}\langle P_{V_1}\rangle_\tau(t) = xz\eta_A^{V_1}+(1-x)y(1-z)\eta_B^{V_1}\\ +2v\cos\big(\Delta\Phi_s(t)\big)\sqrt{x(1-x)yz(1-z)\eta_A^{V_1}\eta_B^{V_1}},\end{aligned} \tag{C.14}$$

$$\begin{aligned}\langle P_{V_2}\rangle_\tau(t) = x(1-z)\eta_A^{V_2}+(1-x)yz\eta_B^{V_2}\\ -2v\cos\big(\Delta\Phi_s(t)\big)\sqrt{x(1-x)yz(1-z)\eta_A^{V_2}\eta_B^{V_2}},\end{aligned} \tag{C.15}$$

which are the effective expressions of P_{V_1} and P_{V_2} we can use for our estimations in the following. For this reason, we omit the averaging and time dependence in the remainder of this thesis.

C.3 Predictions with Honest Players

We now consider a protocol where both parties are honest, and we derive the parameters x, y and z that maximize the fairness and correctness. The fairness condition imposes:

$$\mathbb{P}_h\big((b,a)=(1,0)\big)=\mathbb{P}_h\big((b,v_1,v_2)=(0,1,0)\big), \tag{C.16}$$

and the correctness condition imposes:

$$\mathbb{P}_h\big((b,a)=(1,1)\big)=\mathbb{P}_h\big((b,v_2)=(0,1)\big)=0. \tag{C.17}$$

As we neglected dark counts and double-pair emissions, we already have $\mathbb{P}_h\big((b,a)=(1,1)\big)=0$. However, we have *a priori* $\mathbb{P}_h\big((b,v_2)=(0,1)\big)>0$ for any non-trivial parameters $x,y,z\notin\{0,1\}$ (these cases do not allow to verify the fairness condition). It is therefore impossible in principle to verify the correctness condition. Still, we minimize $\mathbb{P}_h\big((b,v_2)=(0,1)\big)$ in order to approach the condition. As a reminder, we have:

$$\begin{aligned}\mathbb{P}_h\big((b,v_2)=(0,1)\big)=P_{V_2}=x(1-z)\eta_A^{V_2}+(1-x)yz\eta_B^{V_2}\\ -2v\cos\big(\Delta\Phi_s\big)\sqrt{x(1-x)yz(1-z)\eta_A^{V_2}\eta_B^{V_2}}.\end{aligned} \tag{C.18}$$

We first notice that minimizing that expression imposes $\Delta\Phi_s=0$. Now we recall that $\eta_A^{V_2}=\eta_A\eta_{V_2}$ and $\eta_B^{V_2}=\eta_B\eta_{V_2}$, and define $\Pi_A=x\eta_A$ and $\Pi_B=(1-x)y\eta_B$ that we interpret as the probabilities of measuring the photon in Alice's side or Bob's side, before the last tunable BS. We can then rewrite the probability:

$$P_{V_2}=\eta_{V_2}\cdot\Big((1-z)\Pi_A+z\Pi_B-2v\sqrt{z(1-z)\Pi_A\Pi_B}\Big). \tag{C.19}$$

We can then define a variable $\xi:=\frac{\Pi_A}{\Pi_{\text{tot}}}\in[0,1]$ with $\Pi_{\text{tot}}=\Pi_A+\Pi_B$, such that:

$$P_{V_2}=\eta_{V_2}\Pi_{\text{tot}}\Big((1-z)\xi+z(1-\xi)-2v\sqrt{z(1-z)\xi(1-\xi)}\Big). \tag{C.20}$$

P_{V_2} is minimized for $\partial P_{V_2}/\partial\xi=0$ and $\partial P_{V_2}/\partial z=0$. One can easily show that for $v<1$, this system has a single solution $\xi=z=1/2$, such that $\Pi_A=\Pi_B$. This drastically simplifies the expressions of the probabilities:

$$P_{V_1}=x\eta_A^{V_1}(1+v), \tag{C.21}$$

$$P_{V_2}=x\eta_A^{V_2}(1-v), \tag{C.22}$$

$$x\eta_A^{V_1}=(1-x)y\eta_B^{V_1}. \tag{C.23}$$

The case $v=1$ corresponds to a perfect interference, and implies $\partial P_{V_2}/\partial\xi=\partial P_{V_2}/\partial z$ for any set of parameters ξ and z. This way, an infinite number of ξ and z satisfy

$\partial P_{V_2}/\partial\xi = 0$ and $\partial P_{V_2}/\partial z = 0$. One can therefore impose another condition, such as the *balance* condition introduced in [48], in order to find a unique solution (ξ, z). This case is not relevant for our study as the interference is imperfect as in all practical scenarios.

Now we can apply the fairness condition, which in the honest case with no dark counts and no double-pair emission reduces to $P_{V_1} = P_{D_B}$. This gives the following equation on the parameters:

$$x\eta_A^{V_1}(1+v) = (1-x)(1-y)\eta_B^{y}. \tag{C.24}$$

Combining eqs. (C.23) and (C.24), we can derive the expressions of the three parameters x, y and z that optimize both fairness and correctness:

$$x_h = \left[1 + \frac{\eta_A^{V_1}}{\eta_B^{V_1}} + \frac{\eta_A^{V_1}}{\eta_B^{y}}(1+v)\right]^{-1}, \tag{C.25}$$

$$y_h = \left[1 + \frac{\eta_B^{V_1}}{\eta_B^{y}}(1+v)\right]^{-1}, \tag{C.26}$$

$$z_h = \frac{1}{2}. \tag{C.27}$$

Then, the probabilities of the different events are calculated straightforwardly:

$$\mathbb{P}_h\big(\text{Alice wins}\big) = \mathbb{P}_h\big(\text{Bob wins}\big) = P_{V_1} = P_{D_B} = x_h\eta_A^{V_1}(1+v), \tag{C.28}$$

$$\mathbb{P}_h\big(\text{Bob sanctioned}\big) = 0, \tag{C.29}$$

$$\mathbb{P}_h\big(\text{Alice sanctioned}\big) = P_{V_2} = x_h\eta_A^{V_2}(1-v). \tag{C.30}$$

One can notice that the condition $\Pi_A = \Pi_B$, which later translates to eq. (C.23), gives the expected result that we should equalize the power of the two arms of the interferometer in order to display an optimized interference. This condition is used in the recipe for tuning the reflectivities with honest players, in paragraph 4.3.1. Finally, by keeping the same reflectivities, and comparing the values of P_{V_1} and P_{V_2} when $\Delta\Phi_s = 0$ or $\Delta\Phi_s = \pi$, we get:

$$v = \left|\frac{P_{V_1}(\Delta\Phi_s=0) - P_{V_1}(\Delta\Phi_s=\pi)}{P_{V_1}(\Delta\Phi_s=0) + P_{V_1}(\Delta\Phi_s=\pi)}\right| = \left|\frac{P_{V_2}(\Delta\Phi_s=0) - P_{V_2}(\Delta\Phi_s=\pi)}{P_{V_2}(\Delta\Phi_s=0) + P_{V_2}(\Delta\Phi_s=\pi)}\right|, \tag{C.31}$$

so we can indeed interpret v as the interference visibility, which can be easily evaluated experimentally. Finally, we mention that each path's transmission efficiency can be measured by setting the reflectivities and switch's state to trivial values $x, y, z, s \in \{0, 1\}$ given in Table 4.1 of in chapter 4, in which we also give the experimentally measured values of these efficiencies. From these efficiencies we can compute the above theoretically predicted reflectivities x_h, y_h and z_h, which maximize the fairness $\mathcal{F}$ and correctness $\mathcal{C}$. The evolution of these values with the communication distance are shown in Fig. 4.5, together with the reflectivities measured in our experiments.

C.4 Predictions for a Dishonest Alice

Now we derive results for the case when Alice is dishonest and Bob is honest. In general, Alice might be able to perform more sophisticated strategies, involving more complex quantum states, such as those mentioned in [48]. Yet, finding optimal cheating strategies for Alice remains an open question. To illustrate the cheat sensitivity of our protocol, we consider a naive strategy, by simply setting up a reflectivity $x > x_h$, which *a priori* favors Alice (such a strategy is optimal in the case of a lossless protocol [48]). As Bob is honest, we still keep $y = y_h$ and $z = z_h = 1/2$ from eqs. (4.6) and (4.7), and Alice's verification setup is not required. In that case we can derive the expressions for the probabilities of the different events:

$$\mathbb{P}(\text{A. wins}) = \langle P_{V_1} \rangle = \frac{1}{2}\left(x\eta_A^{V_1} + (1-x)y_h\eta_B^{V_1} + 2v\sqrt{x(1-x)y_h\eta_A^{V_1}\eta_B^{V_1}}\right), \tag{C.32}$$

$$\mathbb{P}(\text{A. sanctioned}) = \langle P_{V_2} \rangle = \frac{1}{2}\left(x\eta_A^{V_2} + (1-x)y_h\eta_B^{V_2} - 2v\sqrt{x(1-x)y_h\eta_A^{V_2}\eta_B^{V_2}}\right), \tag{C.33}$$

$$\mathbb{P}(\text{B. wins}) = P_{D_B} = (1-x)(1-y_h)\eta_B^{y}. \tag{C.34}$$

These come straightforwardly from equations (C.10), (C.14) and (C.15), by noting that a dishonest Alice would still set $\Delta\Phi_s = 0$, which maximizes her winning probability and minimizes her sanction probability. This gives the curves plotted in Fig. 4.9 from chapter 4.

APPENDIX D

SECURITY FOR QUANTUM CHANNEL CERTIFICATION

The security of our protocols for certified transmission through untrusted quantum channels relies on some certification bounds, given in equation (6.27) in the 1sDI protocol, and equation (6.31) in the full-DI protocol. The first section is dedicated to deriving the certification bounds for the 1sDI and full-DI protocols. The fair-sampling assumption also plays a significant role in the security of these protocols, so we clarify the assumptions made on the detection apparatus in the second section.

D.1 Bounding the Transmission Fidelity

In the following, we give the full proof for the certification bounds used to secure our protocols for quantum transmission through an untrusted quantum channel. We first give some further intuition on the average channel over the protocol and the expected output state. We then show the certification bound (6.16), which relies on the evaluation of the fidelity of a probe state to a maximally-entangled state, and the fidelity of the corresponding output state after the channel to the same maximally-entangled state. This bounds the fidelity between any state that outputs a quantum channel and the corresponding unknown input state. In the next para-

graph, we show how to evaluate the two probe states' fidelities up to isometries, even when no IID assumption is made and the state source might be untrusted. This method relies on self-testing of steering inequalities in a semi-device independent scenario, where Alice's measurement setup is trusted. Still, this method requires the measurement of a large sample of close-to-maximally-entangled states, going through a channel that might evolve through time. In particular, the channel might not have the same action on the probe states than on the transmitted state. Therefore, we then give some important statistical development in the next paragraph, in order to bound the errors made on the different evaluated fidelities, due to finite state sample in a non-IID setting, as well as losses in the untrusted channel. Finally, we tie up the security proof, combining the previous parts' results in order to provide a bound on the expected fidelity of the transmitted output state to the input state. We also give some way to generalize that security proof to a fully-device independent setting. Note that we extensively use our new results from chapter 5 in order to derive the following proofs.

D.1.1 Average Channel and Expected States

We first recall most important notations for the understanding of the proof. When the protocol does not abort, Alice and Bob wish to bound the probability that it successfully implements the channel $\mathcal{E}_0 \otimes \mathbb{1}_i$ on the input state ρ_i. During the protocol Alice sends $N+1$ states through the channel, including N states Φ_i, and one copy of ρ_i. On the $k-$th state, the channel takes the expression $\mathcal{E}_{k|[k-1]}$. The average channel reads:

$$\bar{\mathcal{E}} = \frac{1}{N+1} \sum_{k=1}^{N+1} \mathcal{E}_{k|[k-1]}. \tag{D.1}$$

This defines a physical channel, which would randomly apply any of the $\mathcal{E}_{k|[k-1]}$. Similarly as we did in (6.11), we call $\bar{\mathcal{E}}_{i,o}$ the average channel when the isometries Γ_i and Γ_o are applied. From these two definitions follow the ouput states when sending the probe state Φ_i or the input state ρ_i:

$$\bar{\Phi}_o = (\bar{\mathcal{E}} \otimes \mathbb{1})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i), \tag{D.2}$$

$$\bar{\rho}_o = (\bar{\mathcal{E}}_{i,o} \otimes \mathbb{1})[\rho_i]/t(\bar{\mathcal{E}}_{i,o}|\rho_i). \tag{D.3}$$

Only one copy of the state ρ_i is sent through the channel during the protocol, at a random position r. Assuming the channel's operator has no way of guessing that position, that state has the same probability of going through any one of the channels $\mathcal{E}_{k|[k-1]}$, such that it is expected to undergo the operation $\bar{\mathcal{E}}_{i,o}$. Therefore, $\bar{\rho}_o$ is the expected output state, and the fidelity $F\big(\bar{\rho}_o, (\mathcal{E}_0 \otimes \mathbb{1})[\rho_i]\big)$ can be interpreted as the average probability of successfully implementing the channel $\mathcal{E}_0$ on ρ_i, up to isometry [26]. In the following, we show how to bound that fidelity using only the measurements performed during the protocol when sending the probe states Φ_i through the channel.

D.1.2 Bounding Channel Fidelity with State Fidelities

We now prove the key theoretical result of this chapter (6.16), which allows one to bound the quality of a channel with probe states fidelities to a maximally-entangled state, up to isometries. More precisely, we show the following lemma:

Lemma D.1 (Probabilistic Channel Certification)**.** *Let us consider a deterministic channel $\mathcal{E}_0$ from $\mathscr{L}(\mathcal{H}_i)$ to $\mathscr{L}(\mathcal{H}_o)$, a probabilistic channel $\mathcal{E}$ from $\mathscr{L}(\mathcal{H}_{A_1})$ to $\mathscr{L}(\mathcal{H}_B)$, and a secondary space $\mathscr{L}(\mathcal{H}_{A_2})$. For any isometries $\Gamma^{A_1/A_2} : \mathcal{H}_{A_1/A_2} \longrightarrow \mathcal{H}_{A_1/A_2} \otimes \mathcal{H}_i$ and $\Gamma^B : \mathcal{H}_B \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_o$ we define the corresponding fidelities of a state $\Phi_i \in \mathscr{L}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2})$ to a maximally-entangled state $\Phi_+ \in \mathscr{L}(\mathcal{H}_i^{\otimes 2})$, before and after application of the channels:*

$$\begin{aligned} F^i &= F((\Lambda^{A_1} \otimes \Lambda^{A_2})[\Phi_i], \Phi_+), \\ F^o &= F((\Lambda^B \otimes \Lambda^{A_2})[(\mathcal{E} \otimes \mathbb{1})[\Phi_i]]/t(\mathcal{E}|\Phi_i), (\mathcal{E}_0 \otimes \mathbb{1})[\Phi_+]), \end{aligned} \tag{D.4}$$

where $\Lambda^P[\cdot] = \mathrm{Tr}_P(\Gamma^P[\cdot])$ for $P = A_1, A_2$ or B. Then there exist two isometries Γ_i and Γ_o, built from Γ^{A_1}, Γ^{A_2} and Γ^B, such that the diamond fidelity between $\mathcal{E}$ and $\mathcal{E}_0$ is bounded, up to isometries:

$$\sqrt{1 - \mathcal{F}_\diamond(\mathcal{E}_{i,o}, \mathcal{E}_0)} \leq d \cdot \sin\Big(\arcsin\big(C^i/t(\mathcal{E}|\Phi_i)\big) + \arcsin C^o\Big), \tag{D.5}$$

where $d = \dim \mathcal{H}_i$, $\mathcal{E}_{i,o} = \mathrm{Tr}_{ext}\big((\Gamma_o \circ \mathcal{E} \circ \Gamma_i)[\rho_{A_1} \otimes \bullet]\big)$, ρ_{A_1} an ancillary state in $\mathscr{L}(\mathcal{H}_{A_1})$, and $C^i = \sqrt{1 - F^i}$ and $C^o = \sqrt{1 - F^o}$.

Proof. This theorem is a generalization of the result from [25] to trace-decreasing channels. We follow the same guidelines for our proof. In order to forget about the injection map on Alice's second subsystem that leaves channel $\mathcal{E}$ unaffected, we first we define $\Phi_i' = (\mathbb{1} \otimes \Lambda^{A_2})[\Phi_i]$. Then, we note that according to Proposition 2 from [25], if one is given a target pure state $\rho_0 \in \mathscr{L}(\mathscr{H}_{sys})$ and any state $\Gamma[\rho] \in \mathscr{L}(\mathscr{H}_{ext} \otimes \mathscr{H}_{sys})$ with $\Lambda[\rho] = \mathrm{Tr}_{ext}(\Gamma[\rho]) \in \mathscr{L}(\mathscr{H}_{sys})$, then the following relation holds

$$F(\Lambda[\rho], \rho_0) = F(\Gamma[\rho], \rho_{ext} \otimes \rho_0), \tag{D.6}$$

where $\rho_{ext} = \dfrac{\mathrm{Tr}_{sys}(\Gamma[\rho]\rho_0 \otimes \mathbb{1})}{\mathrm{Tr}(\Gamma[\rho]\rho_0 \otimes \mathbb{1})}$. We start by applying this proposition to F^i, with Hilbert spaces $\mathscr{H}_{sys} = \mathscr{H}_i^{\otimes 2}$ and $\mathscr{H}_{ext} = \mathscr{H}_{A_1}$, so that fidelity reads:

$$F^i = F\big((\Gamma^{A_1} \otimes \mathbb{1})[\Phi_i'], \rho_{A_1} \otimes \Phi_+\big), \tag{D.7}$$

where $\rho_{A_1} = \dfrac{\mathrm{Tr}_{\mathscr{H}_i \otimes \mathscr{H}_i}\big((\Gamma^{A_1} \otimes \mathbb{1})[\Phi_i']|\Phi_+\rangle\langle\Phi_+|\mathbb{1}\big)}{\mathrm{Tr}\big((\Gamma^{A_1} \otimes \mathbb{1})[\Phi_i']|\Phi_+\rangle\langle\Phi_+|\mathbb{1}\big)}$. The isometry Γ^{A_1} can be written as a unitary, applied on a Hilbert state of larger dimension, so that

$$(\Gamma^{A_1} \otimes \mathbb{1})[\Phi_i'] = (U^i \otimes \mathbb{1})[\sigma_{ext} \otimes \Phi_i'], \tag{D.8}$$

where σ_{ext} is an ancillary pure state and U^i a unitary operation applied on that state and $\mathscr{H}_{A_1}$. This way we get:

$$\begin{aligned} F^i &= F\big((U^i \otimes \mathbb{1})[\sigma_{ext} \otimes \Phi_i'], \rho_{A_1} \otimes \Phi_+\big) \\ &= F\big(\sigma_{ext} \otimes \Phi_i', (U^{i\dagger} \otimes \mathbb{1})[\rho_{A_1} \otimes \Phi_+]\big) \\ &\leq F\big(\Phi_i', \mathrm{Tr}_{ext,i}(U^{i\dagger} \otimes \mathbb{1})[\rho_{A_1} \otimes \Phi_+]\big), \end{aligned} \tag{D.9}$$

where we use the fidelity invariance under unitary operation, and the fact that it can only increase upon tracing out, here of the Hilbert space of σ_{ext}. This allows us to define the input isometry $\Gamma^i = (U^{i\dagger} \otimes \mathbb{1})[\,\bullet\,]$ so we have:

$$F^i \leq F\big(\Phi_i', \mathrm{Tr}_{ext,i}(\Gamma^i[\rho_{A_1} \otimes \Phi_+])\big). \tag{D.10}$$

Now by defining the output isometry $\Gamma^o = \Gamma^B$, we can apply the map $\Gamma^o \circ \bar{\mathcal{E}} \otimes \mathbb{1}$ to both states on the right-hand side of the inequality, and our new extended process

inequality from chapter 5 (see theorem 5.2), and once again fidelity monotonicity when tracing out subsystems:

$$\begin{aligned} C^i &= \sqrt{1-F^i} \\ &\geq C\big(\Phi'_i, \mathrm{Tr}_{ext,i}(\Gamma^i[\rho_{A_1}\otimes\Phi_+])\big) \\ &\geq t(\bar{\mathcal{E}}|\Phi'_i)\cdot C\big((\Gamma^o\circ\bar{\mathcal{E}}\otimes\mathbb{1})[\Phi'_i]/t(\bar{\mathcal{E}}|\Phi'_i), \mathrm{Tr}_{ext,i}((\Gamma^o\circ\bar{\mathcal{E}}\circ\Gamma^i\otimes\mathbb{1})[\rho_{A_1}\otimes\Phi_+])/\tilde{t}\big) \\ &\geq t(\bar{\mathcal{E}}|\Phi'_i)\cdot C\big((\Lambda^B\circ\bar{\mathcal{E}}\otimes\mathbb{1})[\Phi'_i]/t(\bar{\mathcal{E}}|\Phi'_i), \mathrm{Tr}_{ext}((\Gamma^o\circ\bar{\mathcal{E}}\circ\Gamma^i\otimes\mathbb{1})[\rho_{A_1}\otimes\Phi_+])/\tilde{t}\big). \end{aligned} \tag{D.11}$$

Here in order to apply the theorem 5.2, we noted that $t(\bar{\mathcal{E}}|\Phi'_i) = \mathrm{Tr}((\bar{\mathcal{E}}\otimes\mathbb{1})[\Phi'_i])$ is the transmissivity of the first state, which does not vary under application of isometry Γ^o. Also $\tilde{t}$ is the transmissivity of the second state, *i.e.* $\tilde{t} = t(\bar{\mathcal{E}}_{i,o}|\Phi_+)$ as we define $\bar{\mathcal{E}}_{i,o} = \mathrm{Tr}_{ext}((\Gamma^o\circ\bar{\mathcal{E}}\circ\Gamma^i)[\rho_{A_1}\otimes\bullet])$. The last partial trace in the inequality is carried out over all subsystems except $\mathscr{L}(\mathscr{H}_o\otimes\mathscr{H}_i)$, so the distance can only decrease. Noting $(\Lambda^B\circ\bar{\mathcal{E}}\otimes\mathbb{1})[\Phi'_i]/t(\bar{\mathcal{E}}|\Phi'_i) = (\Lambda^B\otimes\Lambda^{A_2})\circ(\bar{\mathcal{E}}\otimes\mathbb{1})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i)$ we get:

$$C^i/t(\bar{\mathcal{E}}|\Phi'_i) \geq C\big((\Lambda^B\otimes\Lambda^{A_2})[\bar{\Phi}_o], (\bar{\mathcal{E}}_{i,o}\otimes\mathbb{1})[\Phi_+]/t(\bar{\mathcal{E}}_{i,o}|\Phi_+)\big). \tag{D.12}$$

Finally, we can apply an equivalent of triangular inequality to Ulhmann's fidelity:

$$\begin{aligned} \arccos\sqrt{F(\rho_1,\rho_3)} &= \arcsin C(\rho_1,\rho_3) \\ &\leq \arccos\sqrt{F(\rho_1,\rho_2)} + \arccos\sqrt{F(\rho_2,\rho_3)} \\ &= \arcsin C(\rho_1,\rho_2) + \arcsin C(\rho_2,\rho_3), \end{aligned} \tag{D.13}$$

with the following states

$$\rho_1 = (\bar{\mathcal{E}}_{i,o}\otimes\mathbb{1})[\Phi_+]/t(\bar{\mathcal{E}}_{i,o}|\Phi_+), \tag{D.14}$$

$$\rho_2 = (\Lambda^B\otimes\Lambda^{A_2})[\bar{\Phi}_o], \tag{D.15}$$

$$\rho_3 = (\mathcal{E}_0\otimes\mathbb{1})[\Phi_+]. \tag{D.16}$$

ρ_1 is the output state of the real channel when sending a perfect maximally entangled state, ρ_2 the average output state we effectively measure after application of the real channel on a close-to-maximally-entangled state, and ρ_3 the output state of the target channel when sending a perfect maximally entangled state. This way we have $C(\rho_2,\rho_3) = C^o$ and $C(\rho_1,\rho_3) = \arccos\sqrt{\mathcal{F}_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)}$ by definition, and $C(\rho_1,\rho_2) \leq C^i/t(\bar{\mathcal{E}}|\Phi_i)$ via inequality (D.12). This gives the result:

$$\arccos\sqrt{F_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)} = \arcsin\mathcal{C}_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0) \leq \arcsin\big(C^i/t(\bar{\mathcal{E}}|\Phi_i)\big) + \arcsin(C^o). \tag{D.17}$$

From here, one just has to use the comparison between Choi-Jamiołkowski and diamond distances, as we showed in chapter 5 (see theorem 5.3), in order to get the bound (D.5) and lemma D.1. ■

The isometries mentioned in the proof are fundamental in a device-independent study, in order to extract ideal qubit spaces to real-world infinite-dimension physical Hilbert spaces. Γ^{A_1}, Γ^{A_2} and Γ^{B} are the same type of isometries as in all standard self-testing results [158], and they extract a qubit state from the full state of a physical system, which encompasses all other degrees of freedom. The unused degrees of freedom are then thrown away. The channel isometries Γ_i and Γ_o were introduced more recently [25] and together extract a qubit channel from a physical channel acting on all degrees of freedom of a physical system. The output isometry Γ_o performs the same operation as Γ^{B}, extracting a qubit out of a physical system. The isometry Γ_i however, performs the inverse operation than the other isometries, encoding the qubit state into a physical system, such that it can be fed into the physical channel. We give a schematic view of these channels in Figure 6.3. In Protocol 6.1, the input state Φ_i is assumed to be fully characterized, so we can ignore the input isometry and $\Gamma_i = \Gamma^{A_1} = \mathbb{1}$. Yet, we must include that isometry when building the fully device-independent Protocol 6.2.

The result we just showed allows us to deduce the protocol's success probability, by evaluating the fidelities F^i and F^o to a Bell state, as well as the transmissivity $t(\bar{\mathcal{E}}|\Phi_i)$. The two following paragraphs are dedicated to evaluating F^o and $t(\bar{\mathcal{E}}|\Phi_i)$, using data received by Alice and Bob only. In order to tie up the security of Protocol 2, we tackle the certification of F^i in a later paragraph.

D.1.3 Certifying the average Bell output state

In order to certify the average output state $\bar{\Phi}_o = (\bar{\mathcal{E}} \otimes \mathbb{1})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i)$, we use self-testing results from previous works [162] that consider steering-based certification of the Bell pair in a finite number of measurement rounds, without making the common IID assumption. In a non-IID scenario the channel may change its behaviour throughout the protocol, such that we define $\mathcal{E}_{k|[k-1]}$ the expression of the channel when Alice sends the $k-$th state. Then, we call the output state

$\Phi_k = (\mathcal{E}_{k|[k-1]} \otimes \mathbb{1})[\Phi_i]/t_k$ when Alice sends the state Φ_i, with $t_k = t(\mathcal{E}_{k|[k-1]}|\Phi_i)$ being the transmissivity of the state Φ_i through the channel $\mathcal{E}_{k|[k-1]}$. Using this notation, we can define the following state:

$$\bar{\Phi}_t = \Big(\sum_{k=1}^{N+1} \mathcal{T}_k \Phi_k\Big)/(K+1), \tag{D.18}$$

where $\mathcal{T}_k = 1$ when a state is detected by Bob, and $\mathcal{T}_k = 0$ otherwise, such that $\sum_{k=1}^{N+1} \mathcal{T}_k = K+1$. We take $\mathcal{T}_r = 1$, in order to include the state $\Phi_r = (\mathcal{E}_{r|[r-1]} \otimes \mathbb{1})[\Phi_i]/t_r$ in the sum. $\bar{\Phi}_t$ is the average output state of the protocol, in the particular case $\rho_i = \Phi_i$ and when the protocol did not abort. Therefore, we expect $\bar{\Phi}_t$ to be a good approximation for $\bar{\Phi}_o$, the expected output state when sending Φ_i through the average channel $\bar{\mathcal{E}}_{i,o}$. However, we leave that consideration for the next paragraph, and now show certification results for $\bar{\Phi}_t$ in place of $\bar{\Phi}_o$.

When $\rho_i = \Phi_i$, we can see our protocol as an attempt to authenticate an unmeasured Bell pair, emerging from an untrusted source. The latter is made of Alice's trusted source, sending copies of Φ_i in the untrusted quantum channel. The state emerging from the $\mathcal{E}_r$ is the unmeasured pair, and the K other output states are measured by Alice and Bob in order to perform a Bell test. In that case, our protocol corresponds to that described in [26, 162], such that we can apply the self-testing-based security results from that work, in a non-IID and 1sDI setting, to our protocol:

Proposition D.1. *Let us consider our protocol where $\rho_i = \Phi_i$, Alice and Bob measure K states and witness an average violation of either steering inequality of $2-\epsilon$. We can bound the fidelity of the average state $\bar{\Phi}_t$ to a maximally-entangled state Φ_+, up to isometry. More precisely, there exist isometries Γ^{A_2} and Γ^B acting respectively on $\mathscr{L}(\mathscr{H}_{A_2})$ and $\mathscr{L}(\mathscr{H}_B)$, such that by defining the local maps $\Lambda^{A_2}[\cdot] = \mathrm{Tr}_{A_2}(\Gamma^{A_2}[\cdot])$ and $\Lambda^B[\cdot] = \mathrm{Tr}_B(\Gamma^B[\cdot])$, for any $x > 0$ we have with probability at least $(1-e^{-x})$:*

$$F((\Lambda^B \otimes \Lambda^{A_2})[\bar{\Phi}_t], \Phi_+) \geq 1 - \alpha \cdot f_x(\epsilon, K) \underset{K \to +\infty}{\longrightarrow} 1 - \alpha\epsilon, \tag{D.19}$$

where α is a constant and f is a function which both depend on the inequality used:

$$f_x(\epsilon, K) = 8\sqrt{\frac{x}{K}} + \frac{\epsilon}{2} + \frac{\epsilon + 8/K}{2 + 1/K}, \tag{D.20}$$

and $\alpha = 1.26$.

It is worth noting that as the r-th state is left unmeasured in this protocol, and we assume the channel's operator has no way of guessing r, then the measurements performed on the test EPR pairs follow the same statistics in the general case as in the special case $\rho_i = \Phi_i$. We can therefore use the correlations witnessed in our protocol in Proposition D.1, even when sending any ρ_i in r-th position, in order to certify the hypothetical state $\bar{\Phi}_t$ up to isometry.

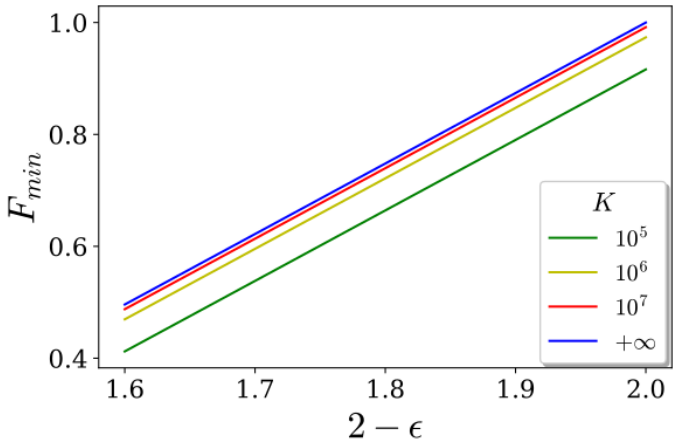


Fig. D.1: Minimum fidelity of the average output state to a Bell state, up to isometries, as a function of the deviation to maximum violation. As we make no IID assumption, we give the evolution for different numbers K of states measured. We set a confidence level $1-e^{-x} \approx 0.999$.

Finally, we give some insight on the behaviour of those bounds with the parameters of the problem (see Fig. D.1). First, we can take $x = 7$ in order to get a bound with almost absolute certainty, as $(1-e^{-x}) \approx 0.999$. The corresponding term in $\sqrt{x/K}$ can be made arbitrarily small by measuring a large number K of states. Similarly, when measuring a reasonable amount of states $K > 10^8$, we reach the asymptotic regime where the fidelity is simply bounded by $1-\alpha\epsilon$.

D.1.4 Errors due to Post-Selection and Finite Statistics

We now show the validity of approximating the state $\bar{\Phi}_o$ (D.2) with $\bar{\Phi}_t$ (D.18), as well as the following approximation:

$$t(\bar{\mathcal{E}}|\Phi_i) \approx R = \frac{K+1}{N+1}, \tag{D.21}$$

where $K+1 = |\mathbb{S}_P|$ is the number of states that Bob is able to measure after they are sent through the channel. Alice and Bob have direct access to the value R in the end of the protocol, as the fraction of states that successfully pass through the channel, which we identify as the heralding efficiency η_s in experiments. Therefore, they can easily evaluate $t(\bar{\mathcal{E}}|\Phi_i)$ by using (D.21).

Proposition D.2. *In our protocol, provided that Bob measured a large enough number $K+1$ of states, the transmissivity $t(\bar{\mathcal{E}}|\Phi_i)$ of Φ_i through the average channel $\bar{\mathcal{E}}$ can be approximated by the proportion R of states which were successfully detected by Bob, and the state $\bar{\Phi}_o$ can be approximated by $\bar{\Phi}_t$. More precisely, for any $x>0$ we have with probability at least $(1-2e^{-x})^2$:*

$$\arccos\sqrt{F(\bar{\Phi}_t,\bar{\Phi}_o)} \leq \Delta_x(R,K), \tag{D.22}$$

$$t(\bar{\mathcal{E}}|\Phi_i) \geq \tau_x(R,K), \tag{D.23}$$

where

$$\Delta_x(R,K) = \arccos\tfrac{1-3\delta_x(R,K)}{1-\delta_x(R,K)}, \tag{D.24}$$

$$\tau_x(R,K) = R\,(1-\delta_x(R,K)), \tag{D.25}$$

$$\delta_x(R,K) = \tfrac{1}{K+1} + \sqrt{\tfrac{2x}{R(K+1)}}. \tag{D.26}$$

In particular, this proposition gives the error terms mentioned given in equations (6.26) and (6.27) from chapter 6.

Proof. First let us rewrite the transmissivity through the average channel using the expressions at each rounds:

$$t(\bar{\mathcal{E}}|\Phi_i) = \mathrm{Tr}\Big(\frac{1}{N+1}\sum_{k=1}^{N+1}\mathcal{E}_k[\Phi_i]\Big) = \frac{1}{N+1}\sum_{k=1}^{N+1} t_k. \tag{D.27}$$

Alice and Bob do not have direct access to that quantity, as they cannot measure t_k individually. However, they have access to the random variables $\{\mathcal{T}_k\}_{1\leq k\leq N+1}$ defined in the previous subsection, the sum of which gives the number of states that were measured by Bob during the protocol:

$$K+1 = |\mathbb{S}_P| = \sum_{k=1}^{N+1}\mathcal{T}_k. \tag{D.28}$$

As no IID assumption is made, the variables $\mathcal{T}_k$ may differ from one another and depend on the experiment's history. Taking the difference with transmissivities, we define a new random variable, for $j \neq k$:

$$\mathcal{D}_j = \sum_{\substack{k=1 \\ k\neq r}}^{j} (\mathcal{T}_k - \mathbb{E}[\mathcal{T}_k]) = \sum_{\substack{k=1 \\ k\neq r}}^{j} (\mathcal{T}_k - t_k), \tag{D.29}$$

and $\mathcal{D}_r = \mathcal{D}_{r-1}$. The expectation value of $\mathcal{D}_j$ is finite for any j, as it is zero, and we have $\mathbb{E}[\mathcal{D}_{j+1}|\mathcal{H}_j] = \mathcal{D}_j$, where $\mathcal{H}_j$ is the history of the experiment after the j-th state is sent through the channel. This makes $\mathcal{D}_j$ a martingale. We also note that $|\mathcal{D}_{j+1} - \mathcal{D}_j| \leq 1$ for any j, such that we can apply the Azuma-Hoeffding inequality:

$$\mathcal{P}(|\mathcal{D}_j| \geq \gamma) \leq 2\exp\Big(-\frac{\gamma^2}{2j}\Big). \tag{D.30}$$

Note that $\mathcal{D}_{N+1} = (N+1)\cdot(R - t(\bar{\mathcal{E}}|\Phi_i)) - 1 + t_r$, such that by taking $j = N+1$ we get:

$$\mathcal{P}\big(\tfrac{-\gamma+1-t_r}{N+1} \leq R - t(\bar{\mathcal{E}}|\Phi_i) \leq \tfrac{\gamma+1-t_r}{N+1}\big) \geq 1 - 2\exp\Big(-\frac{\gamma^2}{2(N+1)}\Big). \tag{D.31}$$

Now considering $0 \leq 1 - t_r \leq 1$, and taking the relative difference we get:

$$\mathcal{P}\big(\tfrac{|R - t(\bar{\mathcal{E}}|\Phi_i)|}{R} \leq \tfrac{\gamma+1}{K+1}\big) \geq 1 - 2\exp\Big(-\frac{\gamma^2}{2(N+1)}\Big), \tag{D.32}$$

such that by taking $x = \frac{\gamma^2}{2(N+1)} > 0$ we get the following bound with probability at least $(1 - 2e^{-x})$:

$$|\Delta_1| = \frac{|R - t(\bar{\mathcal{E}}|\Phi_i)|}{R} \leq \delta_x(R,K), \tag{D.33}$$

where $\delta_x(R,K) = \frac{1}{K+1} + \sqrt{\frac{2x}{R(K+1)}}$. This straightly gives the inequality in (D.23):

$$t(\bar{\mathcal{E}}|\Phi_i) \geq \tau_x(R,K), \tag{D.34}$$

where $\tau_x(R,K) = R\,(1 - \delta_x(R,K))$. Note that as the value of x can be chosen arbitrarily, we can take the same value as in Proposition D.1, which will simplify the notation. To show the bound (D.22), we now assume bound (D.33) stands, such that $|\Delta_1| \leq \delta_x(R,K)$. We then re-write $\bar{\Phi}_o$ using the states Φ_k and transmissivities t_k:

$$\begin{aligned} \bar{\Phi}_o &= (\bar{\mathcal{E}} \otimes \mathbb{1})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i) \\ &= \Big(\frac{1}{N+1}\sum_{k=1}^{N+1} (\mathcal{E}_k \otimes \mathbb{1})[\Phi_i]\Big)/t(\bar{\mathcal{E}}|\Phi_i) \\ &= \Big(\frac{1}{N+1}\sum_{k=1}^{N+1} t_k \Phi_k\Big)/t(\bar{\mathcal{E}}|\Phi_i). \end{aligned} \tag{D.35}$$

We pick a projector $\hat{P}$ that allows to express the trace distance between $\bar{\Phi}_o$ and $\bar{\Phi}_t$:

$$\begin{aligned} D(\bar{\Phi}_t,\bar{\Phi}_o) &= \mathrm{Tr}(\hat{P}(\bar{\Phi}_t-\bar{\Phi}_o)) \\ &= \sum_{k=1}^{N+1}\left(\frac{\mathcal{T}_k}{K+1}-\frac{t_k}{(N+1)t(\bar{\mathcal{E}}|\Phi_i)}\right)\mathrm{Tr}(\hat{P}\Phi_k) \\ &\leq \left(\left|\sum_{k=1}^{N+1}\left(\frac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1}-\frac{1}{N+1}\right)\mathcal{T}_k\,\mathrm{Tr}(\hat{P}\Phi_k)\right|+\left|\sum_{k=1}^{N+1}\frac{\mathcal{T}_k-t_k}{N+1}\,\mathrm{Tr}(\hat{P}\Phi_k)\right|\right)/t(\bar{\mathcal{E}}|\Phi_i). \end{aligned} \tag{D.36}$$

Let us call the second term in parenthesis $|\Delta_2|$ and bound the first term:

$$\begin{aligned} \left|\sum_{k=1}^{N+1}\left(\frac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1}-\frac{1}{N+1}\right)\mathcal{T}_k\,\mathrm{Tr}(\hat{P}\Phi_k)\right| &= \sum_{k=1}^{N+1}\mathcal{T}_k\,\mathrm{Tr}(\hat{P}\Phi_k)\left|\frac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1}-\frac{1}{N+1}\right| \\ &\leq (K+1)\left|\frac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1}-\frac{1}{N+1}\right| \\ &= \left|t(\bar{\mathcal{E}}|\Phi_i)-R\right| \\ &\leq R\,\delta_x(R,K). \end{aligned} \tag{D.37}$$

In order to bound $|\Delta_2|$, we make the exact same proof as for $|\Delta_1|$, taking $\mathrm{Tr}(\hat{P}\Phi_k)\cdot\mathcal{T}_k$ in place of $\mathcal{T}_k$ and $\mathrm{Tr}(\hat{P}\Phi_k)\cdot t_k$ in place of t_k, when defining $\mathcal{D}_j$ in equation (D.29). This new sum of variables $\tilde{\mathcal{D}}_j$ is still a martingale such that $|\tilde{\mathcal{D}}_{j+1}-\tilde{\mathcal{D}}_j|\leq 1$. Therefore it still verifies equation (D.30), and we have

$$\tilde{\mathcal{D}}_{N+1} = (N+1)\Delta_2 - \mathrm{Tr}(\hat{P}\Phi_r)(1-t_r), \tag{D.38}$$

such that:

$$\mathbb{P}\left(\frac{-\gamma+\mathrm{Tr}(\hat{P}\Phi_r)(1-t_r)}{N+1}\leq\Delta_2\leq\frac{\gamma+\mathrm{Tr}(\hat{P}\Phi_r)(1-t_r)}{N+1}\right)\geq 1-2\exp\left(-\frac{\tilde{\gamma}^2}{2(N+1)}\right). \tag{D.39}$$

As $0\leq\mathrm{Tr}(\hat{P}\Phi_r)(1-t_r)\leq 1$ we can simplify:

$$\Pr\left(|\Delta_2|\leq\frac{\tilde{\gamma}+1}{N+1}\right)\geq 1-2\exp\left(-\frac{\tilde{\gamma}^2}{2(N+1)}\right), \tag{D.40}$$

such that by taking $\frac{\tilde{\gamma}^2}{2(N+1)}=x$ we get the following bound with probability at least $(1-2e^{-x})$:

$$|\Delta_2|\leq R\,\delta_x(R,K). \tag{D.41}$$

This way, coming back to (D.37) we get:

$$D(\bar{\Phi}_t,\bar{\Phi}_o)\leq\frac{2R\,\delta_x(R,K)}{t(\bar{\mathcal{E}}|\Phi_i)}\leq\frac{2\,\delta_x(R,K)}{1-\delta_x(R,K)}. \tag{D.42}$$

Now we use a comparison between fidelity and trace distance $1-\sqrt{F}\leq D$ in order to bound the angle distance between $\bar{\Phi}_t$ and $\bar{\Phi}_o$:

$$\begin{aligned} A(\bar{\Phi}_t,\bar{\Phi}_o) &= \arccos\sqrt{F(\bar{\Phi}_t,\bar{\Phi}_o)} \leq \Delta_x(R,K), \\ \text{where } \Delta_x(R,K) &= \arccos\frac{1-3\,\delta_x(R,K)}{1-\delta_x(R,K)}. \end{aligned} \tag{D.43}$$

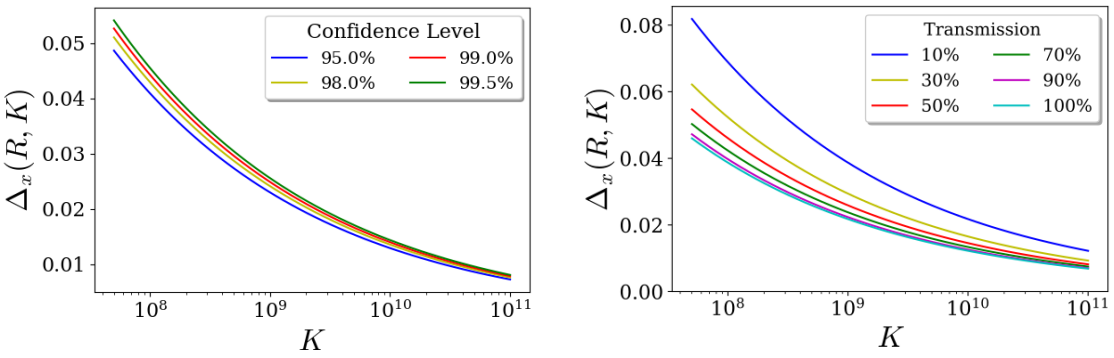
Finally, we point out that this bound is true with probability $(1-2e^{-x})$ and at the condition that bound (D.33) holds, which also happens with probability $(1-2e^{-x})$, such that both bounds hold with probability $(1-2e^{-x})^2$. This ties up the proof of Proposition D.2. ■

This proposition highlights the purely statistics-induced error on states and transmissivities. It is mostly due to the fact that Alice and Bob only have access to a finite number of states, in a non-IID setting. Most importantly, as the channel is allowed to be lossy, these states only give information on a sample of the different expressions $\mathcal{E}_{k|[k-1]}$ that it might take during the protocol, causing more uncertainty than when certifying a source of state without channel. This error must be included in the bounds in order to derive the protocol's security. Also note that we can use this theorem when applying the injection map $\Lambda^B\otimes\Lambda^{A_2}$ defined in the previous subsection to both states, as we always have:

$$F\left((\Lambda^B\otimes\Lambda^{A_2})[\bar{\Phi}_t],(\Lambda^B\otimes\Lambda^{A_2})[\bar{\Phi}_o]\right)\geq F(\bar{\Phi}_t,\bar{\Phi}_o). \tag{D.44}$$

This is fundamental to derive the final security bound for our protocol. Finally, we give some insight on the dependence of this error on the different parameters of the problem. First we notice that this error can be made arbitrarily small by measuring a large enough number K of states, which still needs to be limited for practical applications. The error tends to increase with the confidence level, such that we need more states K in order to ensure a smaller error with reasonable certainty. Similarly, the more lossy the channel is, *i.e.* the smaller R, the bigger the error. Therefore having a lossy channel also imposes to measure more states in order to accurately certify the protocol. We give an idea of the evolution of that error in Fig. D.2, for different confidence levels and different channel's transmission ratios R. We see that with a transmission ratio $R=50\%$, corresponding to telecom

light propagating in a 15km-long optical fiber or ideal quantum teleportation, we can ensure an error $\Delta_x(R,K) \leq 0.015$ with a confidence level of 99.5%, by measuring a reachable number of states $K \approx 10^{10}$.



(a) For different minimum confidence levels, with a transmission ratio $R = 50\%$.

(b) With a minimum confidence level 99.5%, with different transmission ratios.

Fig. D.2: Minimum statistics-induced error $\Delta_x(R,K)$, as a function of the number of states measured K.

D.1.5 Certifying the Output State of the Protocol

Combining the last three paragraphs allows us to extract a bound for the fidelity of the expected output state $\bar{\rho}_o$ to the input state ρ_i up to isometry. We assume that Alice prepared N states with fidelity F^i to a Bell state, that Bob received K of those states during the protocol, and that they measured an ϵ-close to maximum violation of the steering inequality. First, they can use Lemma D.1, implying that there exist isometries Γ_i, Γ_o, Γ^{A_1}, Γ^{A_2}, and Γ^B, giving the result from (6.16):

$$\begin{aligned}\sqrt{1-F\big((\Lambda^B\otimes\Lambda^{A_2})[\bar{\rho}_o],\rho_i\big)} &\leq \sqrt{1-\mathcal{F}_\diamond(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)}\\ &= C_\diamond(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)\\ &\leq 2C_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)\\ &\leq 2\sin\big(\arcsin\big(C^i/t(\bar{\mathcal{E}}|\Phi_i)\big)+\arcsin(C^o)\big).\end{aligned} \tag{D.45}$$

Now we fix $x > 0$ in order to apply Proposition D.2, such that we have both:

$$t(\bar{\mathcal{E}}|\Phi_i) \geq \tau_x(R,K), \tag{D.46}$$

$$\begin{aligned}\arccos\sqrt{F}\big((\Lambda^B \otimes \Lambda^{A_2})[\bar{\Phi}_t],(\Lambda^B \otimes \Lambda^{A_2})[\bar{\Phi}_o]\big) &\leq \arccos\sqrt{F}(\bar{\Phi}_t,\bar{\Phi}_o) \\ &\leq \Delta_x(R,K).\end{aligned} \tag{D.47}$$

with probability at least $(1-2e^{-x})^2$, where τ_x and Δ_x are functions detailed in paragraph D.1.4. In that case, we can apply the triangular inequality to $\arcsin(C^o)$:

$$\arcsin(C^o) \leq \arcsin C\big((\Lambda^B \otimes \Lambda^{A_2})[\bar{\Phi}_t],\Phi_+\big) + \Delta_x(R,K), \tag{D.48}$$

and bound $t(\bar{\mathcal{E}}|\Phi_i)$ in order to get:

$$\arcsin\big(C^i/t(\bar{\mathcal{E}}|\Phi_i)\big) \leq \arcsin\big(C^i/\tau_x(R,K)\big). \tag{D.49}$$

We can then bound $C((\Lambda^B \otimes \Lambda^{A_2})[\bar{\Phi}_t],\Phi_+)$ using Proposition D.1, with a confidence level $(1-e^{-x})$:

$$\arcsin\big(C((\Lambda^B \otimes \Lambda^{A_2})[\bar{\Phi}_t],\Phi_+)\big) \leq \arcsin\sqrt{\alpha f_x(\epsilon,K)}. \tag{D.50}$$

Combining (D.45), (D.48), (D.49), and (D.50) we can bound the input-output fidelity up to isometries:

$$\sqrt{1-F(\bar{\rho}_o,\rho_i)} \leq 2\cdot\sin\Big(\arcsin\big(C^i/\tau_x(R,K)\big) + \arcsin\sqrt{\alpha f_x(\epsilon,K)} + \Delta_x(R,K)\Big), \tag{D.51}$$

where α and f are given in Proposition D.1. This way, for any $x > 0$ we can bound the output state fidelity to the input state with probability at least $(1-e^{-x})\cdot(1-2e^{-x})^2$:

$$F(\bar{\rho}_o,\rho_i) \geq 1 - 4\cdot\sin^2\Big(\arcsin\big(C^i/\tau_x\big) + \arcsin\sqrt{\alpha f_x(\epsilon,K)} + \Delta_x\Big). \tag{D.52}$$

D.1.6 Full-Device Independence: Probe State Certification

In protocol 2 Alice does not trust her measurement setup anymore, nor the source of input state Φ_i. However we still make the IID assumption on that source. In that case we deduce the following theorem from a previous work [162]:

Proposition D.3. *When Alice measures an average violation of Bell inequality* $2\sqrt{2}-\eta$ *on* M *identical copies of* Φ_i *with untrusted measurement apparatus, then for any* $x>0$ *we can bound the fidelity of* Φ_i *to* Φ_+ *up to isometries, with probability* $(1-e^{-x})$*, meaning that there exists two isometries* Γ^{A_1} *and* Γ^{A_2} *on* $\mathscr{L}(\mathscr{H}_{A_1})$ *and* $\mathscr{L}(\mathscr{H}_{A_2})$ *such that:*

$$F\left((\Lambda^{A_1}\otimes\Lambda^{A_2})[\Phi_i],\Phi_+\right)\geq 1-\alpha\cdot g_x(\eta,M)\underset{M\to+\infty}{\longrightarrow}1-\alpha\cdot\eta, \tag{D.53}$$

with $\Lambda^{A_1}[\cdot]=\mathrm{Tr}_{A_1}(\Gamma^{A_1}[\cdot])$*,* $\Lambda^{A_2}[\cdot]=\mathrm{Tr}_{A_1}(\Gamma^{A_2}[\cdot])$*,* $\alpha=1.19$*, and* $g_x(\eta,M)=8\sqrt{2x/M}+\eta$*.*

Then, if Alice and Bob measure K *states at the output of the channel with untrusted measurement apparatus, and witness an average violation of CHSH inequality of* $2\sqrt{2}-\epsilon$*, we can bound the fidelity of the average state* $\bar{\Phi}_t$ *to a maximally-entangled state* Φ_+*, up to isometries, with probability at least* $(1-e^{-x})$*, meaning that there exist isometries* Γ^{A_2} *and* Γ^{B} *on* $L(\mathscr{H}_{A_2})$ *and* $L(\mathscr{H}_B)$*, such that:*

$$F((\Lambda^{B}\otimes\Lambda^{A_2})[\bar{\Phi}_t],\Phi_+)\geq 1-\alpha\cdot f_x(\epsilon,K)\underset{K\to+\infty}{\longrightarrow}1-\alpha\cdot\epsilon, \tag{D.54}$$

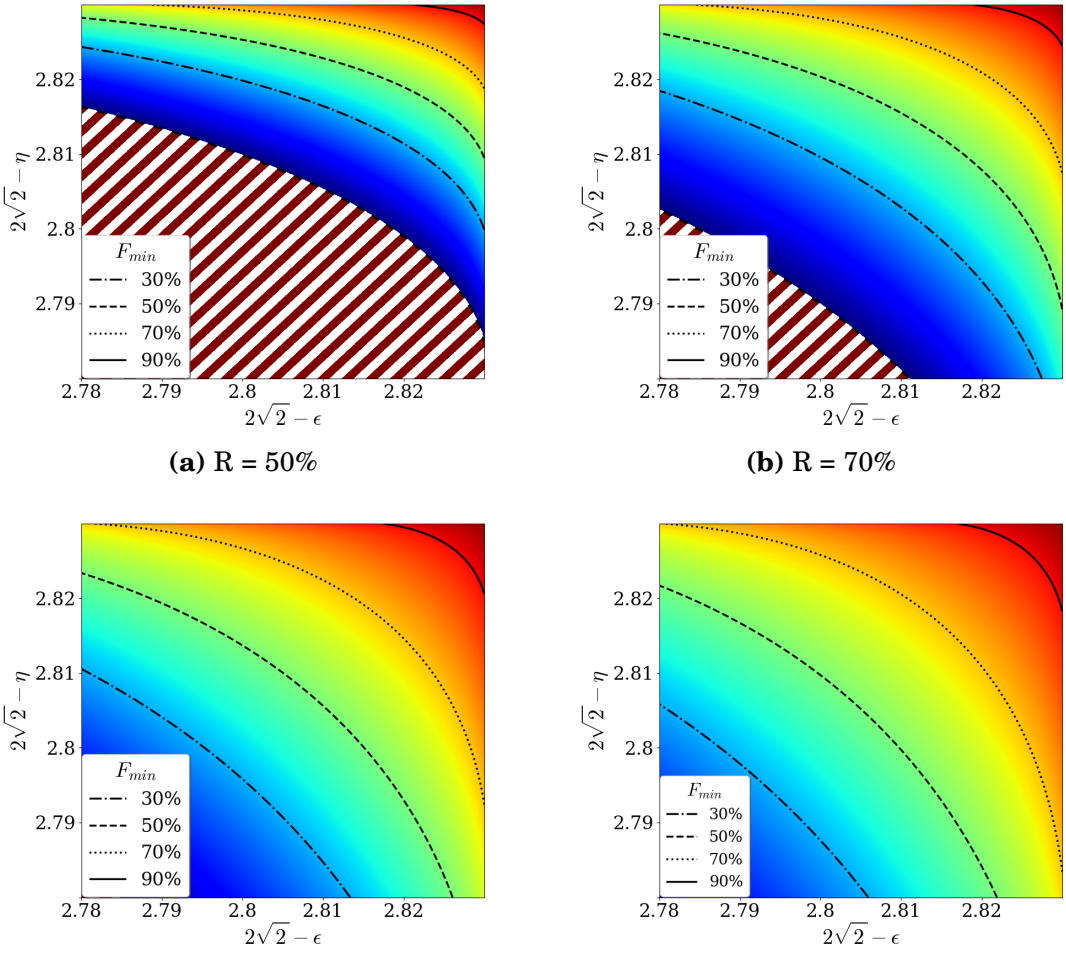
with $\Lambda^{A_2}[\cdot]=\mathrm{Tr}_{A_2}(\Gamma^{A_2}[\cdot])$*,* $\Lambda^{B}[\cdot]=\mathrm{Tr}_{B}(\Gamma^{B}[\cdot])$*,* $\alpha=1.19$ *and*

$$f_x(\epsilon,K)=16\sqrt{\tfrac{2x}{K}}+\tfrac{3\epsilon}{4}+\tfrac{\epsilon+(4+2\sqrt{2})/K}{4+4/K}. \tag{D.55}$$

Thanks to the IID assumption made on the probe-state source, we still consider all input probe states to be equal to Φ_i, so the first part of Proposition D.3 enables Alice and Bob to certify the quantity F^i once, for the whole protocol. This way, compared to Proposition D.1 for protocol 1, we bound $C^i\leq\sqrt{\alpha g_x(\eta,M)}$, and replace the expression of f_x and α. We also multiply the confidence level by $(1-e^{-x})$ to account for the confidence on the input bound, due to the finite number M of input state tested. This straightly gives the bound:

$$F(\bar{\rho}_o,\rho_i)\geq 1-4\cdot\sin^2\left(\arcsin\left(\sqrt{\alpha g_x(\eta,M)}/\tau_x\right)+\arcsin\sqrt{\alpha f_x(\epsilon,K)}+\Delta_x\right), \tag{D.56}$$

with confidence level at least $(1-e^{-x})^2\cdot(1-2e^{-x})^2$ for any $x>0$, therefore showing the security bound for protocol 2. We show the corresponding certified fidelity with examples of experimental parameters in Fig. D.3.



(a) R = 50%

(b) R = 70%

(c) R = 90%

(d) R = 100%

Fig. D.3: Minimum certified fidelity of the output state of Protocol 2, to the state sent through the channel, as a function of the deviations η,ϵ from maximum violation of CHSH inequality. We set $x = 7$ for a confidence level $> 99.4\%$, a number of probe states $M = K = 10^{10}$, and different ratios of transmission $R = K/N$.

D.2 Detectors Model in Experiment

We now detail the assumptions made on the players' detection systems, in order to perform our proof-of-principle experimental protocol, as well as the consequences on the protocol's results. We focus on the detectors used in order to certify the output probe state in the one-sided device-independent protocol, and therefore omit the system that Alice uses in order to certify the input state Φ_i. Both Alice and Bob each possess a local measurement apparatus, ideally made of 2-outcomes POVMs $\{\hat{M}^{A_2}_{l|q}\}_{l=0,1}$ and $\{\hat{M}^{B}_{l|q}\}_{l=0,1}$, for $q = 0,1$. In reality, these detectors have non-unit efficiency, meaning they only return a result with a certain probability which may depend on the parameter q, the outcome l, or even the quantum state ρ. This way we adopt a similar description as that of [185], such that we get the probabilities of returning outcome l, when measuring ρ with measurement parameter q:

$$\mathbb{P}_A(l|q,\rho) = \mathrm{Tr}(\rho \hat{M}^{A_2}_{l|q}) \cdot \eta^A(l,q,\rho), \tag{D.57}$$

$$\mathbb{P}_B(l|q,\rho) = \mathrm{Tr}(\rho \hat{M}^{B}_{l|q}) \cdot \eta^B(l,q,\rho), \tag{D.58}$$

where η^A and η^B are the efficiencies. For a bipartite state, the probability of getting outcomes (l_A, l_B) with parameters (q_A, q_B) becomes:

$$\mathbb{P}(l_A,l_B|q_A,q_B,\rho) = \mathrm{Tr}\left(\rho \cdot \hat{M}^{A_2}_{l_A|q_A} \otimes \hat{M}^{B}_{l_B|q_B}\right) \cdot \eta^A(l_A,q_A,\rho_A) \cdot \eta^B(l_B,q_B,\rho_B), \tag{D.59}$$

where $\rho_A = \mathrm{Tr}_B(\rho)$ and $\rho_B = \mathrm{Tr}_A(\rho)$ are the local states, such that the efficiencies are local. In the following we focus on the assumptions made on these efficiencies in our protocol, and the consequences on the results. First, in a one-sided device-independent scenario, we assume that Alice fully characterizes her measurement apparatus, and proves her efficiency to be independent of the state ρ and the measurement parameter q, such that:

$$\eta^{A_2}(l,q,\rho) = \eta^{A_2}(l). \tag{D.60}$$

The values of $\eta^{A_2}(l)$ are accessible to Alice, as part of her detectors' characterization. This way, for l_+ and l_- such that $\eta^{A_2}(l_+) > \eta^{A_2}(l_-)$, Alice can ignore the outcomes l_+ with probability $1 - \eta^{A_2}(l_-)/\eta^{A_2}(l_+)$ in order to effectively equalize the efficiencies of the two outcomes. In that case the efficiency on Alice's side is a constant η^{A_2}, such that

$$\eta^{A_2}(l,q,\rho) = \eta^{A_2}. \tag{D.61}$$

On Bob's side, we first make the weak fair sampling assumption [185], stating that we can factorize the efficiencies due to classical parameters from those due to quantum states:

$$\eta^B(l,q,\rho) = \eta^B_C(l,q)\cdot\eta^B_Q(\rho). \tag{D.62}$$

We then make a form of strong fair-sampling assumption, stating the efficiency does not depend on q, such that:

$$\eta^B(l,q,\rho) = \eta^B_C(l)\cdot\eta^B_Q(\rho). \tag{D.63}$$

Now we could assume the state-dependent efficiency to be unit, which leads to an unbalanced-outcomes homogeneous fair-sampling assumption, and leaves the protocol more vulnerable to attacks. Another solution is to consider $\eta^B_Q(\rho)$ as a part of the quantum channel being tested, as shown in Fig. D.4. In that case our protocol is more secure but certifies a different channel, the output of which is necessarily measured by Bob measurement apparatus. This would require further investigation if the quantum communication is followed by another protocol which does not involve Bob's measurement apparatus. In both cases, we can neglect the state-dependent efficiency, such that

$$\eta^B(l,q,\rho) = \eta^B_C(l), \tag{D.64}$$

is an efficiency which *a priori* depends on the result l. The detection probability then becomes

$$\mathbb{P}_B(l|q,\rho) = \mathrm{Tr}(\rho\hat{M}^B_{l|q})\cdot\eta^B(l). \tag{D.65}$$

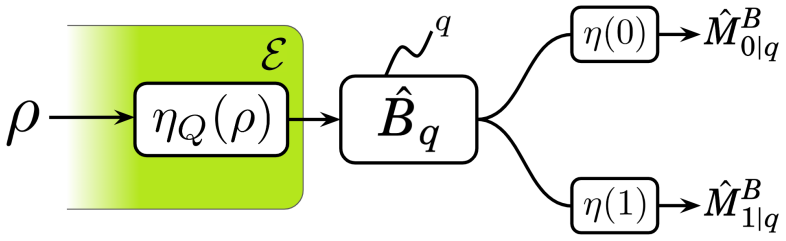


Fig. D.4: Schematic representation of Bob's measurement apparatus, taking our assumptions into account. The apparatus first displays some state-dependent transmissivity η_Q, that we can include inside the channel $\mathcal{E}$. Bob then measures the observable $\hat{B}_q$, the result $l \in \{0,1\}$ of which is filtered with efficiency $\eta(l)$.

Similarly to [185], we now show that even though the efficiency η^B slightly varies with the outcome l, we can still use the measured outcome without any correction on Bob's side, and still get a good evaluation of $\mathcal{I} = |\langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_1 \hat{B}_1 \rangle|$. By definition we have:

$$\langle \hat{A}_q \hat{B}_q \rangle = \langle \hat{M}^{A_2}_{0|q} \hat{M}^{B}_{0|q} \rangle + \langle \hat{M}^{A_2}_{1|q} \hat{M}^{B}_{1|q} \rangle - \langle \hat{M}^{A_2}_{0|q} \hat{M}^{B}_{1|q} \rangle + \langle \hat{M}^{A_2}_{1|q} \hat{M}^{B}_{0|q} \rangle. \tag{D.66}$$

With their imperfect detectors, Alice and Bob approximate that quantity by measuring the following:

$$\overline{\hat{A}_q \hat{B}_q} = \frac{n_{0,0|q} + n_{1,1|q} - n_{0,1|q} - n_{1,0|q}}{n_{0,0|q} + n_{1,1|q} + n_{0,1|q} + n_{1,0|q}}, \tag{D.67}$$

where $n_{l_A,l_B|q}$ is the number of times the measurement of a pair gave the outcome (l_A, l_B), when Alice and Bob both measured with parameter q. When measuring a big number of state $\mathcal{N}$ we approximate

$$n_{l_A,l_B|q} = \mathcal{N} \cdot \mathbb{P}(l_A, l_B | q_A, q_B, \rho) = \mathcal{N} \cdot \mathrm{Tr}(\rho \cdot \hat{M}^{A_2}_{l_A|q} \otimes \hat{M}^{B}_{l_B|q}) \cdot \eta^A \cdot \eta^B(l_B), \tag{D.68}$$

so we rewrite the evaluation of $\langle \hat{A}_q \hat{B}_q \rangle$, symplifying the constant terms $\mathcal{N}$ and η_A:

$$\begin{aligned}
\overline{\hat{A}_q \hat{B}_q} &= \frac{\mathrm{Tr}\big[\rho \cdot (\hat{M}^{A_2}_{0|q} \otimes \hat{M}^{B}_{0|q} - \hat{M}^{A_2}_{1|q} \otimes \hat{M}^{B}_{0|q})\big] \cdot \eta^B(0) + \mathrm{Tr}\big[\rho \cdot (\hat{M}^{A_2}_{1|q} \otimes \hat{M}^{B}_{1|q} - \hat{M}^{A_2}_{0|q} \otimes \hat{M}^{B}_{1|q})\big] \cdot \eta^B(1)}{\mathrm{Tr}\big[\rho \cdot (\hat{M}^{A_2}_{0|q} \otimes \hat{M}^{B}_{0|q} + \hat{M}^{A_2}_{1|q} \otimes \hat{M}^{B}_{0|q})\big] \cdot \eta^B(0) + \mathrm{Tr}\big[\rho \cdot (\hat{M}^{A_2}_{1|q} \otimes \hat{M}^{B}_{1|q} + \hat{M}^{A_2}_{0|q} \otimes \hat{M}^{B}_{1|q})\big] \cdot \eta^B(1)} \\
&= \frac{\mathrm{Tr}\Big[\rho \cdot \hat{A}_q \otimes \big(\hat{M}^{B}_{0|q} \cdot \eta^B(0) - \hat{M}^{B}_{1|q} \cdot \eta^B(1)\big)\Big]}{\mathrm{Tr}\Big[\rho \cdot \big(\hat{M}^{B}_{0|q} \cdot \eta^B(0) + \hat{M}^{B}_{1|q} \cdot \eta^B(1)\big)\Big]}.
\end{aligned} \tag{D.69}$$

Then we take ξ such that $\eta^B(1)/\eta^B(0) = 1 + \xi$, and we get

$$\begin{aligned}
\overline{\hat{A}_q \hat{B}_q} &= \frac{\mathrm{Tr}\Big[\rho \cdot \hat{A}_q \otimes \big(\hat{M}^{B}_{0|q} - \hat{M}^{B}_{1|q} \cdot \eta^B(1)/\eta^B(0)\big)\Big]}{\mathrm{Tr}\Big[\rho \cdot \big(\hat{M}^{B}_{0|q} + \hat{M}^{B}_{1|q} \cdot \eta^B(1)/\eta^B(0)\big)\Big]} \\
&= \frac{\langle \hat{A}_q \hat{B}_q \rangle - \mathrm{Tr}\big[\rho \cdot \hat{A}_q \otimes \hat{M}^{B}_{1|q}\big] \cdot \xi}{1 + \mathrm{Tr}\big[\rho \cdot \hat{M}^{B}_{1|q}\big] \cdot \xi}.
\end{aligned} \tag{D.70}$$

Considering $\eta^B(1) \approx \eta^B(0)$, such that $|\xi| \ll 1$, we approximate the difference between the expected and measured correlations $\langle \hat{A}_q \hat{B}_q \rangle$ and $\overline{\hat{A}_q \hat{B}_q}$, at first order:

$$\begin{aligned}
\overline{\hat{A}_q \hat{B}_q} - \langle \hat{A}_q \hat{B}_q \rangle &\approx -\mathrm{Tr}\big[\rho \cdot \hat{A}_q \otimes \hat{M}^{B}_{1|q}\big] \cdot \xi - \langle \hat{A}_q \hat{B}_q \rangle \cdot \mathrm{Tr}\big[\rho \cdot \hat{M}^{B}_{1|q}\big] \cdot \xi \\
&= (1 - \langle \hat{A}_q \hat{B}_q \rangle) \cdot \mathrm{Tr}\big[\rho \cdot \hat{M}^{A_2}_{1|q} \otimes \hat{M}^{B}_{1|q}\big] \cdot \xi \\
&\qquad - (1 + \langle \hat{A}_q \hat{B}_q \rangle) \cdot \mathrm{Tr}\big[\rho \cdot \hat{M}^{A_2}_{0|q} \otimes \hat{M}^{B}_{1|q}\big] \cdot \xi.
\end{aligned} \tag{D.71}$$

Provided Alice and Bob witness a close-to-maximum violation of steering inequality, we also have $(1-\langle\hat{A}_q\hat{B}_q\rangle) \ll 1$ and $\mathrm{Tr}\big[\rho\cdot\hat{M}^{A_2}_{0|q}\otimes\hat{M}^{B}_{1|q}\big] \ll 1$. This way, that difference is doubly negligible, such that even noticeable unbalance between the detectors efficiencies should not significantly deviate the measured correlation from the expected correlation. We therefore assume $\overline{\hat{A}_q\hat{B}_q} \approx \langle\hat{A}_q\hat{B}_q\rangle$, such that the value of $\mathcal{I}$ can be accurately measured even without correction for the detectors efficiency. In our experiment, we measure the relative efficiency between Bob's detectors, for each protocol iteration. This way we get $\xi \lesssim 0.03$, while witnessing a close-to-maximum violation of steering inequality, legitimizing the approximation. We still compute the violation that would be measured if detectors were perfectly balanced, and $\eta^B(1) = \eta^B(0)$, by correcting the data with the relative efficiencies. The difference between the corrected and uncorrected data is included in the error bars displayed in Fig. 6.7.

BIBLIOGRAPHY

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] P. Richard, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6-7, pp. 467–488, 1982.

[3] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[4] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[5] C. Bennett and G. Brassard, "Quantum cryptography: Public key cryptography and coin tossing," in *Proceedings of the International Conference on Computers, Systems and Signal processing*, vol. 175, pp. 175–179, 1984.

[6] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, aug 1991.

[7] G. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. XIV, pp. 295–301, 1926.

[8] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[9] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, 1964.

[10] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[11] D. Dieks, "Communication by epr devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[12] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[13] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical review letters*, vol. 83, no. 3, p. 648, 1999.

[14] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Physical Review A*, vol. 78, no. 4, p. 042309, 2008.

[15] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Physical review letters*, vol. 109, no. 13, p. 130501, 2012.

[16] A. Cabello, "Multiparty key distribution and secret sharing based on entanglement swapping," *arXiv preprint quant-ph/0009025*, 2000.

[17] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *International conference on the theory and application of cryptology and information security*, pp. 217–235, Springer, 2005.

[18] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, June 2008.

[19] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.

[20] R. W. Spekkens and T. Rudolph, "Quantum protocol for cheat-sensitive weak coin flipping," *Physical Review Letters*, vol. 89, no. 22, p. 227901, 2002.

[21] A. Gočanin, I. Šupić, and B. Dakić, "Sample-efficient device-independent quantum state verification and certification," *PRX Quantum*, vol. 3, feb 2022.

[22] J.-D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, "Self-testing with finite statistics enabling the certification of a quantum network link," *arXiv:1812.09117 [quant-ph]*, July 2020.

[23] J.-D. Bancal, N. Sangouard, and P. Sekatski, "Noise-Resistant Device-Independent Certification of Bell State Measurements," *Physical Review Letters*, vol. 121, p. 250506, Dec. 2018.

[24] M. O. Renou, J. Kaniewski, and N. Brunner, "Self-Testing Entangled Measurements in Quantum Networks," *Physical Review Letters*, vol. 121, p. 250507, Dec. 2018.

[25] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, "Certifying the Building Blocks of Quantum Computers from Bell's Theorem," *Physical Review Letters*, vol. 121, p. 180505, Nov. 2018.

[26] A. Unnikrishnan and D. Markham, "Authenticated teleportation with one-sided trust," *Physical Review A*, vol. 100, p. 032314, Sept. 2019.

[27] F. Monteiro, V. C. Vivoli, T. Guerreiro, A. Martin, J.-D. Bancal, H. Zbinden, R. T. Thew, and N. Sangouard, "Revealing genuine optical-path entanglement," *Physical review letters*, vol. 114, no. 17, p. 170504, 2015.

[28] A. Suprano, D. Zia, E. Polino, T. Giordani, L. Innocenti, M. Paternostro, A. Ferraro, N. Spagnolo, and F. Sciarrino, "Enhanced detection techniques of orbital angular momentum states in the classical and quantum regimes," *New Journal of Physics*, vol. 23, no. 7, p. 073014, 2021.

[29] F. Graffitti, A. Pickston, P. Barrow, M. Proietti, D. Kundys, D. Rosset, M. Ringbauer, and A. Fedrizzi, "Measurement Device Independent Verification of Quantum Channels," *Physical Review Letters*, vol. 124, p. 010503, Jan. 2020.

[30] P. Lefebvre, R. Valivarthi, Q. Zhou, L. Oesterling, D. Oblak, and W. Tittel, "Compact energy–time entanglement source using cascaded nonlinear interactions," *JOSA B*, vol. 38, no. 4, pp. 1380–1385, 2021.

[31] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via bell's theorem," *Physical Review Letters*, vol. 47, no. 7, p. 460, 1981.

[32] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Physical review letters*, vol. 98, no. 1, p. 010505, 2007.

[33] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," *Physical review letters*, vol. 98, no. 1, p. 010503, 2007.

[34] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[35] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.

[36] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental demonstration of practical unforgeable quantum money," *Preprint at: http://arxiv. org/abs/1705.01428*, 2017.

[37] M. Bozzio, A. Orieux, L. Trigo Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Information*, vol. 4, no. 1, pp. 1–8, 2018.

[38] M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," *Physical Review A*, vol. 99, no. 2, p. 022336, 2019.

[39] B. Bell, D. Markham, D. Herrera-Martí, A. Marin, W. Wadsworth, J. Rarity, and M. Tame, "Experimental demonstration of graph-state quantum secret sharing," *Nature communications*, vol. 5, no. 1, pp. 1–12, 2014.

[40] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, "Experimental quantum conference key agreement," *Science advances*, vol. 7, no. 23, p. eabe0395, 2021.

[41] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz, "Experimental anonymous conference key agreement using linear cluster states," *arXiv preprint arXiv:2207.09487*, 2022.

[42] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, "A wavelength-tunable fiber-coupled source of narrowband entangled photons," *Optics Express*, vol. 15, no. 23, p. 15377, 2007.

[43] S. Krapick, H. Herrmann, V. Quiring, B. Brecht, H. Suche, and C. Silberhorn, "An efficient integrated two-color source for heralded single photons," *New Journal of Physics*, vol. 15, no. 3, p. 033010, 2013.

[44] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, "High-quality asynchronous heralded single-photon source at telecom wavelength," *New Journal of Physics*, vol. 6, no. 1, p. 163, 2004.

[45] T. Guerreiro, A. Martin, B. Sanguinetti, N. Bruno, H. Zbinden, and R. Thew, "High efficiency coupling of photon pairs in practice," *Optics express*, vol. 21, no. 23, pp. 27641–27651, 2013.

[46] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, pp. 3891–3894, 1998.

[47] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, *et al.*, "12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion," *Physical review letters*, vol. 121, no. 25, p. 250505, 2018.

[48] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, "Quantum weak coin flipping with a single photon," *Phys. Rev. A*, vol. 102, p. 022414, Aug 2020.

[49] S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti, "Experimental cheat-sensitive quantum weak coin flipping," *arXiv preprint arXiv:2211.03472*, 2022.

[50] R. Yehia, S. Neves, E. Diamanti, and I. Kerenidis, "Quantum city: simulation of a practical near-term metropolitan quantum network," *arXiv preprint arXiv:2211.01190*, 2022.

[51] D. F. James, P. G. Kwiat, W. J. Munro, and A. G. White, "Measurement of qubits," *Physical Review A*, vol. 64, no. 5, p. 052312, 2001.

[52] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, "Photonic state tomography," *Advances in Atomic, Molecular, and Optical Physics*, vol. 52, pp. 105–159, 2005.

[53] E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," *Naturwissenschaften*, vol. 23, no. 49, pp. 823–828, 1935.

[54] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[55] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[56] B. S. Cirel'son, "Quantum generalizations of bell's inequality," *Letters in Mathematical Physics*, vol. 4, no. 2, pp. 93–100, 1980.

[57] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of Modern Physics*, vol. 86, no. 2, p. 419, 2014.

[58] C. H. Bennett, G. Brassard, *et al.*, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, 1993.

[59] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond bell's theorem," in *Bell's theorem, quantum theory and conceptions of the universe*, pp. 69–72, Springer, 1989.

[60] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities," *American Journal of Physics*, vol. 58, no. 12, pp. 1131–1143, 1990.

[61] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, "Quantum conference key agreement: A review," *Advanced Quantum Technologies*, vol. 3, no. 11, p. 2000025, 2020.

[62] M. Christandl and S. Wehner, "Quantum anonymous transmissions," *Advances in Cryptology, ASIACRYPT*, pp. 217–235, 2005.

[63] R. Jozsa, "Fidelity for mixed quantum states," *Journal of modern optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[64] A. Gilchrist, N. K. Langford, and M. A. Nielsen, "Distance measures to compare real and ideal quantum processes," *Physical Review A*, vol. 71, no. 6, p. 062310, 2005.

[65] A. E. Rastegin, "Sine distance for quantum states," *arXiv:quant-ph/0602112*, Feb. 2006.

[66] B. E. Saleh and M. C. Teich, *Fundamentals of photonics*.
john Wiley & sons, 2019.

[67] J. Armstrong, N. Bloembergen, J. Ducuing, and P. S. Pershan, "Interactions between light waves in a nonlinear dielectric," *Physical review*, vol. 127, no. 6, p. 1918, 1962.

[68] P. Franken and J. Ward, "Optical harmonics and nonlinear phenomena," *Reviews of Modern Physics*, vol. 35, no. 1, p. 23, 1963.

[69] A. Yariv, "Coupled-mode theory for guided-wave optics," *IEEE Journal of Quantum Electronics*, vol. 9, no. 9, pp. 919–933, 1973.

[70] J. Kerr, "Xl. a new relation between electricity and light: Dielectrified media birefringent," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 50, no. 332, pp. 337–348, 1875.

[71] J. Kerr, "Liv. a new relation between electricity and light: Dielectrified media birefringent (second paper)," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 50, no. 333, pp. 446–458, 1875.

[72] M. Planck and M. Masius, *The Theory of Heat Radiation*.
Blakiston, 1914.

[73] A. Einstein, "Uber einen die erzeugung und verwandlung des lichtes betreffenden heurischen gesichtpunkt," *Ann. Phys*, vol. 17, pp. 132–148, 1905.

[74] W. Louisell, A. Yariv, and A. Siegman, "Quantum fluctuations and noise in parametric processes. i.," *Physical Review*, vol. 124, no. 6, p. 1646, 1961.

[75] D. C. Burnham and D. L. Weinberg, "Observation of simultaneity in parametric production of optical photon pairs," *Physical Review Letters*, vol. 25, no. 2, p. 84, 1970.

[76] C. Fabre and N. Treps, "Modes and states in quantum optics," *Reviews of Modern Physics*, vol. 92, no. 3, p. 035005, 2020.

[77] J. W. Fleming and D. L. Wood, "Refractive index dispersion and related properties in fluorine doped silica," *Applied optics*, vol. 22, no. 19, pp. 3102–3104, 1983.

[78] L. Mach, "Ueber einen interferenzrefraktor," *Zeitschrift für Instrumentenkunde*, vol. 12, no. 3, p. 89, 1892.

[79] L. Zehnder, "Ein neuer interferenzrefraktor," 1891.

[80] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, pp. 2044–2046, 1987.

[81] D. Bouwmeester and A. Zeilinger, "The physics of quantum information: basic concepts," in *The physics of quantum information*, pp. 1–14, Springer, 2000.

[82] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," *Software: Practice and Experience*, vol. 52, no. 1, pp. 66–114, 2022.

[83] C. Peikert *et al.*, "A decade of lattice cryptography," *Foundations and trends® in theoretical computer science*, vol. 10, no. 4, pp. 283–424, 2016.

[84] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[85] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, "Satellite-relayed intercontinental quantum network," *Physical review letters*, vol. 120, no. 3, p. 030501, 2018.

[86] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," *Physical Review A*, vol. 63, no. 1, p. 012309, 2000.

[87] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, *et al.*, "Entanglement-based quantum communication over 144 km," *Nature physics*, vol. 3, no. 7, pp. 481–486, 2007.

[88] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Physical Review A*, vol. 76, no. 1, p. 012307, 2007.

[89] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, *et al.*, "Long-distance entanglement-based quantum key distribution over optical fiber," *Optics Express*, vol. 16, no. 23, pp. 19118–19126, 2008.

[90] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.

[91] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, "Quantum weak coin flipping with a single photon," *Physical Review A*, vol. 102, no. 2, p. 022414, 2020.

[92] J.-L. Smirr, M. Deconinck, R. Frey, I. Agha, E. Diamanti, and I. Zaquine, "Optimal photon-pair single-mode coupling in narrow-band spontaneous parametric downconversion with arbitrary pump profile," *Journal of the Optical Society of America B*, vol. 30, p. 288, jan 2013.

[93] J.-L. Smirr, *Towards a narrow-band source of polarisation entangled entangled photon at 1550 nm*.
Phd thesis, Université Paris Sud - Paris XI, Nov. 2010.

[94] N. Bruno, *Single photon entanglement: from foundations to applications*.
PhD thesis, Université de Genève, Mar. 2015.

[95] N. Bruno *et al.*, "Pulsed source of spectrally uncorrelated and indistinguishable photons at telecom wavelengths," *Optics Express*, vol. 22, p. 17246, jul 2014.

[96] R. S. Bennink, "Optimal collinear gaussian beams for spontaneous parametric down-conversion," *Physical Review A*, vol. 81, may 2010.

[97] Z. Y. Ou and L. Mandel, "Violation of bell's inequality and classical probability in a two-photon correlation experiment," *Physical Review Letters*, vol. 61, pp. 50–53, jul 1988.

[98] P. G. Kwiat *et al.*, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letters*, vol. 75, pp. 4337–4341, dec 1995.

[99] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultra-bright source of polarization-entangled photons," *Physical Review A*, vol. 60, pp. 773–776, aug 1999.

[100] R. Rangarajan, M. Goggin, and P. Kwiat, "Optimizing type-i polarization-entangled photons," *Opt. Express*, vol. 17, p. 18920, 2009.

[101] G. Sagnac, "L'éther lumineux démontré par l'effet du vent relatif d'éther dans un interféromètre en rotation uniforme," *CR Acad. Sci.*, vol. 157, pp. 708–710, 1913.

[102] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed energy-time entangled twin-photon source for quantum communication," *Physical Review Letters*, vol. 82, no. 12, p. 2594, 1999.

[103] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. DeMicheli, D. B. Ostrowsky, and N. Gisin, "Ppln waveguide for quantum communication," *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, vol. 18, no. 2, pp. 155–160, 2002.

[104] A. Martin, A. Issautier, H. Herrmann, W. Sohler, D. B. Ostrowsky, O. Alibart, and S. Tanzilli, "A polarization entangled photon-pair source based on a type-ii ppln waveguide emitting at a telecom wavelength," *New Journal of Physics*, vol. 12, no. 10, p. 103005, 2010.

[105] F. Kaiser, A. Issautier, O. Alibart, A. Martin, and S. Tanzilli, "Guided-wave photonics for narrowband polarization entanglement," *arXiv preprint arXiv:1111.5683*, 2011.

[106] T. E. Stuart, J. A. Slater, F. Bussières, and W. Tittel, "Flexible source of nondegenerate entangled photons based on a two-crystal sagnac interferometer," *Physical Review A*, vol. 88, no. 1, p. 012301, 2013.

[107] S. Tanzilli, A. Martin, F. Kaiser, M. P. De Micheli, O. Alibart, and D. B. Ostrowsky, "On the genesis and evolution of integrated quantum optics," *Laser & Photonics Reviews*, vol. 6, no. 1, pp. 115–143, 2012.

[108] B.-S. Shi and A. Tomita, "Generation of a pulsed polarization entangled photon pair using a sagnac interferometer," *Physical Review A*, vol. 69, jan 2004.

[109] T. Kim, M. Fiorentino, and F. N. C. Wong, "Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer," *Physical Review A*, vol. 73, jan 2006.

[110] R. S. Bennink, "Optimal collinear gaussian beams for spontaneous parametric down-conversion," *Physical Review A*, vol. 81, no. 5, p. 053805, 2010.

[111] R.-B. Jin, R. Shimizu, K. Wakui, H. Benichi, and M. Sasaki, "Widely tunable single photon source with high purity at telecom wavelength," *Optics Express*, vol. 21, p. 10659, apr 2013.

[112] C. Chen *et al.*, "Efficient generation and characterization of spectrally factorable biphotons," *Optics Express*, vol. 25, p. 7300, mar 2017.

[113] F. Graffitti, P. Barrow, M. Proietti, D. Kundys, and A. Fedrizzi, "Independent high-purity photons created in domain-engineered crystals," *Optica*, vol. 5, pp. 514–517, May 2018.

[114] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[115] D. H. Smith, "An ultrafast source of polarization entangled photon pairs based on a sagnac interferometer," Master's thesis, University of Waterloo, 2009.

[116] M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White, "Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing," *Optics express*, vol. 19, no. 23, pp. 22698–22708, 2011.

[117] C. Greganti *et al.*, "Tuning single-photon sources for telecom multi-photon experiments," *Optics Express*, vol. 26, p. 3286, jan 2018.

[118] S. Pancharatnam, "Achromatic combinations of birefringent plates," in *Proceedings of the Indian Academy of Sciences-Section A*, vol. 41, pp. 137–144, Springer, 1955.

[119] K. Fradkin *et al.*, "Tunable midinfrared source by difference frequency generation in bulk periodically poled ktiopo4," *Applied Physics Letters*, vol. 74, no. 7, pp. 914–916, 1999.

[120] F. König and F. N. C. Wong, "Extended phase matching of second-harmonic generation in periodically poled ktiopo4 with zero group-velocity mismatch," *Applied Physics Letters*, vol. 84, no. 10, pp. 1644–1646, 2004.

[121] R. Yehia, E. Diamanti, and I. Kerenidis, "Composable security for multipartite entanglement verification," *Physical Review A*, vol. 103, no. 5, p. 052609, 2021.

[122] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Physical review letters*, vol. 122, no. 24, p. 240501, 2019.

[123] A. Zeilinger, M. A. Horne, H. Weinfurter, and M. Żukowski, "Three-particle entanglements from two entangled pairs," *Phys. Rev. Lett.*, vol. 78, pp. 3031–3034, 1997.

[124] F. Bouchard, A. Sit, Y. Zhang, R. Fickler, F. M. Miatto, Y. Yao, F. Sciarrino, and E. Karimi, "Two-photon interference: the hong–ou–mandel effect," *Reports on Progress in Physics*, vol. 84, no. 1, p. 012402, 2020.

[125] H. E. Guilbert, Y.-P. Wong, and D. J. Gauthier, "Observation of elliptical rings in type-i spontaneous parametric down-conversion," *Journal of the Optical Society of America B*, vol. 32, p. 2096, oct 2015.

[126] M. Smania, *Photonic multipartite entanglement : Generation, measurement and applications*.
PhD thesis, Stockholm University, Department of Physics, 2020.

[127] H. Anwer, *Photonic Multipartite Communication: Complexity, measurements and Bell inequalities*.
PhD thesis, Department of Physics, Stockholm University, 2021.

[128] R.-B. Jin, M. Takeoka, U. Takagi, R. Shimizu, and M. Sasaki, "Highly efficient entanglement swapping and teleportation at telecom wavelength," *Scientific Reports*, vol. 5, mar 2015.

[129] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, pp. 351–382, 2016.

[130] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *SIGACT News*, vol. 15, p. 23–27, jan 1983.

[131] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, p. 218–229, 1987.

[132] D. Alistarh, J. Aspnes, V. King, and J. Saia, "Communication-efficient randomized consensus," *Distrib. Comput.*, vol. 31, no. 6, pp. 489–501, 2018.

[133] R. Cleve, "Limits on the security of coin flips when half the processors are faulty," *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, p. 364–369, 1986.

[134] A. Ambainis, "A new protocol and lower bounds for quantum coin flipping," *Journal of Computer and System Sciences*, vol. 68, no. 2, pp. 398–416, 2004.

[135] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, "Fair loss-tolerant quantum coin flipping," *Phys. Rev. A*, vol. 80, p. 062321, 2009.

[136] A. Kitaev, "Quantum coin flipping," *6th Workshop on Quantum Information Processing*, 2003.

[137] C. Mochon, "Quantum weak coin flipping with arbitrarily small bias," *arXiv*, vol. 0711.4114, 2007.

[138] 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, pp. 633–679, 2016.

[139] A. Chailloux and I. Kerenidis, "Optimal quantum strong coin flipping," *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, p. 527–533, 2009.

[140] A. Chailloux and I. Kerenidis, "Optimal bounds for quantum bit commitment," *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, p. 354–362, 2011.

[141] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, "Experimental quantum coin tossing," *Phys. Rev. Lett.*, vol. 94, p. 040501, Jan 2005.

[142] 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.

[143] 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.

[144] L. Hardy and A. Kent, "Cheat sensitive quantum bit commitment," *Phys. Rev. Lett.*, vol. 92, p. 157901, Apr 2004.

[145] R. W. Spekkens and T. Rudolph, "Quantum protocol for cheat-sensitive weak coin flipping," *Phys. Rev. Lett.*, vol. 89, p. 227901, Nov 2002.

[146] L. You, "Superconducting nanowire single-photon detectors for quantum information," *Nanophotonics*, vol. 9, no. 9, pp. 2673–2692, 2020.

[147] S. Steinhauer, S. Gyger, and V. Zwiller, "Progress on large-scale superconducting nanowire single-photon detectors," *Applied Physics Letters*, vol. 118, no. 10, p. 100501, 2021.

[148] A. Pickston, F. Graffitti, P. Barrow, C. L. Morrison, J. Ho, A. M. Brańczyk, and A. Fedrizzi, "Optimised domain-engineered crystals for pure telecom photon sources," *Optics Express*, vol. 29, no. 5, pp. 6991–7002, 2021.

[149] L. Stasi, P. Caspar, T. Brydges, H. Zbinden, F. Bussières, and R. Thew, "Enhanced heralded single-photon source with a photon-number-resolving parallel superconducting nanowire single-photon detector," *arXiv preprint arXiv:2210.16005*, 2022.

[150] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, *et al.*, "Device-independent randomness expansion with entangled photons," *Nature Physics*, vol. 17, no. 4, pp. 452–456, 2021.

[151] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni, and D. Calonico, "Coherent phase transfer for real-world twin-field quantum key distribution," *Nat. Commun.*, vol. 13, jan 2022.

[152] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, p. 070501, Feb 2020.

[153] C. A. Miller, "The impossibility of efficient quantum weak coin flipping," in *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 916–929, 2020.

[154] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*.
Cambridge University Press, 2000.

[155] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, "Bell measurements for teleportation," *Physical Review A*, vol. 59, pp. 3295–3300, May 1999.

[156] A. Jamiołkowski, "Linear transformations which preserve trace and positive semidefiniteness of operators," *Reports on Mathematical Physics*, vol. 3, pp. 275–278, Dec. 1972.

[157] M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear Algebra and its Applications*, vol. 10, pp. 285–290, June 1975.

[158] I. Šupić and J. Bowles, "Self-testing of quantum systems: a review," *Quantum*, vol. 4, p. 337, Sept. 2020.

[159] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," *Physical Review Letters*, vol. 98, p. 230501, June 2007.

[160] R. Colbeck, "Quantum And Relativistic Protocols For Secure Multi-Party Computation," *arXiv:0911.3814 [quant-ph]*, Feb. 2011.

[161] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pp. 503–509, Nov. 1998.

[162] A. Unnikrishnan, *Enforcing trust in quantum networks*.
PhD thesis, University of Oxford, University of Oxford, 2019.

[163] J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical bell-state analyzer," *Applied Physics B*, vol. 72, no. 1, pp. 67–71, 2001.

[164] D. Mayers and A. Yao, "Self testing quantum apparatus," *QIC*, vol. 4, pp. 273–286, jul 2004.

[165] S. J. Summers and R. Werner, "Maximal violation of bell's inequalities is generic in quantum field theory," *Communications in Mathematical Physics*, vol. 110, no. 2, pp. 247–259, 1987.

[166] S. L. Braunstein, A. Mann, and M. Revzen, "Maximal violation of bell inequalities for mixed states," *Physical Review Letters*, vol. 68, no. 22, p. 3259, 1992.

[167] B. S. Tsirelson, "Some results and problems on quantum bell-type inequalities," *Hadronic Journal Supplement*, vol. 8, no. 4, pp. 329–345, 1993.

[168] S. Popescu, "Bell's inequalities and density matrices: revealing "hidden" nonlocality," *Physical Review Letters*, vol. 74, no. 14, p. 2619, 1995.

[169] M. McKague, "Self-testing graph states," in *Conference on Quantum Computation, Communication, and Cryptography*, pp. 104–120, Springer, 2011.

[170] M. McKague, T. H. Yang, and V. Scarani, "Robust self-testing of the singlet," *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 45, p. 455304, 2012.

[171] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, "Robust self-testing of the three-qubit w state," *Physical Review A*, vol. 90, no. 4, p. 042339, 2014.

[172] C. Bamps and S. Pironio, "Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing," *Physical Review A*, vol. 91, no. 5, p. 052111, 2015.

[173] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, "Self-testing protocols based on the chained bell inequalities," *New Journal of Physics*, vol. 18, no. 3, p. 035013, 2016.

[174] I. Šupić and M. J. Hoban, "Self-testing through epr-steering," *New Journal of Physics*, vol. 18, no. 7, p. 075006, 2016.

[175] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, "Experimental criteria for steering and the einstein-podolsky-rosen paradox," *Physical Review A*, vol. 80, no. 3, p. 032112, 2009.

[176] T. H. Yang and M. Navascués, "Robust self-testing of unknown quantum systems into any entangled two-qubit states," *Physical Review A*, vol. 87, no. 5, p. 050102, 2013.

[177] A. Coladangelo, K. T. Goh, and V. Scarani, "All pure bipartite entangled states can be self-tested," *Nature communications*, vol. 8, no. 1, pp. 1–5, 2017.

[178] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, "Self-testing multipartite entangled states through projections onto two systems," *New journal of Physics*, vol. 20, no. 8, p. 083041, 2018.

[179] I. Bongioanni, L. Sansoni, F. Sciarrino, G. Vallone, and P. Mataloni, "Experimental quantum process tomography of non-trace-preserving maps," *Physical Review A*, vol. 82, no. 4, p. 042307, 2010.

[180] S. Thomas, M. Billard, N. Coste, S. Wein, H. Ollivier, O. Krebs, L. Tazaïrt, A. Harouri, A. Lemaitre, I. Sagnes, *et al.*, "Bright polarized single-photon source based on a linear dipole," *Physical review letters*, vol. 126, no. 23, p. 233601, 2021.

[181] A. Auffèves, "Quantum technologies need a quantum energy initiative," *PRX Quantum*, vol. 3, no. 2, p. 020101, 2022.

[182] A. Dimić, I. Šupić, and B. Dakić, "Sample-efficient device-independent quantum state verification and certification," *arXiv preprint arXiv:2105.05832*, 2021.

[183] J. A. Smolin, J. M. Gambetta, and G. Smith, "Efficient method for computing the maximum-likelihood quantum state from measurements with additive gaussian noise," *Physical Review Letters*, vol. 108, feb 2012.

[184] B. Qi, Z. Hou, L. Li, D. Dong, G. Xiang, and G. Guo, "Quantum state tomography via linear regression estimation," *Scientific Reports*, vol. 3, dec 2013.

[185] D. Orsucci, J.-D. Bancal, N. Sangouard, and P. Sekatski, "How post-selection affects device-independent claims under the fair sampling assumption," *Quantum*, vol. 4, p. 238, Mar. 2020.

Photonic Resources for the Implementation of Quantum Network Protocols

The security of modern communication networks can be enhanced thanks to the laws of quantum mechanics. In this way, important tasks such as encryption key distribution, anonymous transmissions or electronic voting can be made secure without computational assumptions. In this thesis, we developed a source of photonic quantum states which we use to demonstrate important cryptographic primitives, namely quantum weak coin flipping, and the certified transmission of quantum information through an untrusted and lossy quantum channel. Our source produces photon-pairs at telecom wavelengths, with high heralding efficiency and closeness to a maximally-entangled state. Pairs are used as heralded single-photons to perform the first implementation of a quantum weak coin flipping protocol, allowing two distant players to decide of a random winner. Using quantum resources allows to enforce information-theoretic security and cheat-sensitivity. Cheating players are detected in a verification step, which involves a carefully optimized linear optical interferometer including beam splitters with variable reflectivities and a fast optical switch. We demonstrate high values of our protocol benchmarks for attenuations corresponding to several kilometers of telecom optical fiber. Alternatively, photon-pairs are used as maximally-entangled qubits to certify the transmission of a single qubit through an untrusted and lossy quantum channel. We provide a whole new protocol, based on the already-known self-testing technique and new fundamental results on lossy quantum channels. We demonstrate that protocol using photon-pairs entangled in polarization to probe the channel. We show it allows the certification of quantum communication for a large amount of losses induced by the channel. Finally, we provide a novel design in order to adapt this source to multipartite entanglement generation, enabling the implementation of new protocols involving more than two players.

Thèse défendue le 2 décembre 2022 à Sorbonne Université, Paris, France.

Doctoral Thesis