universität wien

MASTERARBEIT | MASTER'S THESIS

Titel | Title

Practical quantum weak coin flipping based on a GHZ game

verfasst von | submitted by

Anton Lu BSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 066 876
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Physics
Betreut von | Supervisor:	Univ.-Prof. Dipl.-Ing. Dr. Philip Walther
Mitbetreut von | Co-Supervisor:	Dr. Mathieu Bozzio

Acknowledgements

First and foremost, I would like to express my sincere gratitude to Prof. Philip Walther and my co-supervisor, Dr. Mathieu Bozzio, for giving me the opportunity to join the research group and for providing me with the resources and guidance necessary to contribute to this project as a Master's student.

I would also like to thank all members of the Walther group for fostering such a welcoming and positive working environment. In particular, I am deeply grateful to Rebecca for her guidance and support on the theoretical aspects of this thesis, and to Danny, Yann, and Lee for their precious assistance and supervision during the experimental work.

Furthermore, I would like to thank my girlfriend Caro for her continuous emotional support and encouragement throughout the study. Last but not least, I am profoundly grateful to my family for their support in pursuing my path toward becoming a quantum physicist.

Abstract

Weak coin flipping is a fundamental cryptographic primitive. In a weak coin flipping protocol, two mutually distrustful parties attempt to agree on the outcome of a coin toss, where both parties desire opposite outcomes. A well-designed weak coin flipping protocol ensures fairness, correctness, and low bias. Fairness means that both honest players have an equal chance of winning; correctness guarantees that the protocol does not abort if both players are honest; and low bias ensures that a cheating player cannot significantly influence the outcome to their advantage. In classical settings, it is known to be impossible to achieve zero bias in such protocols [NST15]. However, quantum weak coin flipping protocols can achieve arbitrarily small bias, demonstrating an advantage over classical protocols [Moc07].

In this thesis, we introduce a new quantum weak coin flipping protocol whose security is based on the GHZ game and present a loss-tolerant version suitable for practical implementation. The protocol is experimentally realized using hyper-encoding of polarization and spatial qubits on entangled 1550 nm photons generated via type-II spontaneous parametric down-conversion. The experimental results demonstrate the feasibility of implementing a secure, loss-tolerant weak coin flipping protocol under realistic experimental conditions. This thesis also provides a strong framework for future extensions into a leader election protocol.

Kurzfassung

Weak Coin-Flipping ist ein fundamentales kryptographisches Primitive. Bei einem Weak Coin Flipping-Protokoll versuchen zwei gegenseitig misstrauische Parteien, sich auf das Ergebnis eines Münzwurfs zu einigen, wobei beide Parteien jeweils entgegengesetzte Ergebnisse bevorzugen. Ein gut konstruiertes Weak Coin Flipping-Protokoll gewährleistet Fairness, Korrektheit und geringe *Bias*. Fairness bedeutet, dass beide ehrlichen Parteien die gleiche Gewinnchance haben; Korrektheit garantiert, dass das Protokoll nicht abbricht, wenn beide Parteien ehrlich agieren; und ein geringer Bias stellt sicher, dass eine betrügerische Partei das Ergebnis nicht wesentlich zu ihrem Vorteil beeinflussen kann. In klassischen Szenarien ist es bekannt, dass ein Null-Bias-Protokoll nicht möglich ist [NST15]. Quanten Weak Coin Flipping-Protokolle hingegen können beliebig kleinen Bias erreichen und zeigen damit einen Vorteil gegenüber klassischen Protokollen [Moc07].

In dieser Arbeit stellen wir ein neues Quanten-Weak-Coin-Flipping-Protokoll vor, dessen Sicherheit auf dem *GHZ-Game* basiert, und präsentieren eine verlusttolerante Version, die für die praktische Umsetzung geeignet ist. Das Protokoll wird experimentell mittels *Hyper-Encoding* von Polarisation und Spatial Qubits auf verschränkten 1550 nm-Photonen realisiert, die durch Typ-II Spontaneous Parametric Down-Conversion erzeugt werden. Die experimentellen Ergebnisse zeigen die Machbarkeit der sicheren, verlusttoleranten Implementierung eines Weak Coin Flipping-Protokolls unter realistischen experimentellen Bedingungen. Darüber hinaus liefert diese Arbeit eine solide Grundlage für zukünftige Erweiterungen, beispielsweise hin zu einem *Leader Election*-Protokoll.

Contents

1. Introduction

1.1. Classical cryptography and cryptographic primitives

Cryptography allows secure communication in the presence of adversarial entities. It provides security guarantees that restrict an unauthorized party from learning or tampering with transmitted information. These guarantees include core properties such as confidentiality, integrity, and availability. Confidentiality ensures that information is not made available or disclosed to unauthorized parties, while integrity guarantees the correctness and completeness of the content. Lastly, availability means the property of being accessible and usable on demand by an authorized entity. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability, can also be involved. [Int18] In some settings, these properties can be achieved with information theoretical (i.t.) security, which does not rely on computational assumptions. In contrast, computational security assumes that certain mathematical problems are hard to solve for adversaries within realistic time and computational power.

Modern cryptographic systems are built on so-called cryptographic primitives. These are fundamental protocols that can be combined to form more complex protocols and applications that provide security guarantees. An example of such primitives is *bit commitment*. It allows one party (Alice) to commit to a bit a with some publicly known encryption algorithms so that the other party (Bob) must not learn the value of a until Alice reveals it. Additionally, Alice must not be able to change the value of a once committed. A natural extension of this primitive is *coin flipping*, where two mistrustful parties jointly generate a random bit such that neither can bias the outcome. Classically, this can be achieved by running a *bit commitment* protocol on Alice's input a, and then Bob will publicly declare a random bit b before Alice reveals her input. Once Alice reveals a, the outcome of the coin flip is set to $a \oplus b$. Such protocol can then be further extended to allow the construction of *leader election* protocols , which are important primitives in distributed computation and applications such as Blockchain.[BCWW25]

Classical cryptography schemes can be divided into two branches: symmetric cryptography and asymmetric cryptography. Symmetric encryption involves one key for both encryption and decryption, the key must be shared securely between sender and receiver ahead of time. A prominent example for this encryption scheme is one-time pad, in which a message is encrypted using a pre-shared key of the same length. If the key is truly random and used only once, the ciphertext reveals no information about the message and it is information theoretically secure.[Ver26] However, prior distributions of symmetric keys are often impractical in real world applications. This motivates the use of asymmetric encryption schemes, which typically involves a pair of mathematically related private

and public keys. Security in such scheme is based on computational hardness of certain mathematical problems, such as prime factorization of large integers or computing discrete logarithms. The most widely used computationally secure asymmetric encryption schemes, RSA [RSA78] and Diffie-Hellman key exchange [DH22], are based on such mathematical problems.

1.2. Advantages of quantum cryptography

The rise of quantum computing and the development of quantum algorithms poses an imminent threat to classical cryptographic security. In particular, Shor's algorithm enables efficient quantum computation of prime factorization and discrete logarithms, making encryption schemes like RSA and Diffie–Hellman vulnerable.[Sho99]

In some quantum cryptographic protocols, the security of information can be guaranteed by fundamental principles of quantum mechanics without any computational assumptions. It relies on certain quantum laws such as the no-cloning theorem, which states that an arbitrary unknown quantum state cannot be copied without altering it. This principle, among others, guarantees the i.t. security of protocols like quantum key distribution (QKD), where two parties can distribute a mutual key on a mistrustful channel. Any attempt at eavesdropping inevitably disturbs the quantum system and can thus be detected. [BB84] The QKD scheme is based on conjugate coding, where classical information is mapped onto quantum states in two conjugate bases. Any adversary attempting to access the information without knowing the encoding basis will be detected. [Wie83]

1.3. Quantum cryptography beyond QKD

So far, QKD is the most well-developed and widely implemented primitive in quantum cryptography. Recent advances have demonstrated QKD over distances exceeding 1000 km through optical fiber[LCG+24], as well as QKD via free-space links using satellites. [YLL+20] However, QKD is not without limitations: the distributed keys ultimately need to be stored and processed using classical devices, which remain vulnerable to classical attacks such as device hacking. [Szt23]

Building on the success of QKD, researchers have turned their attention to the development of mistrustful quantum cryptography. In contrast to QKD, where two parties collaborate to ensure the security of the protocol, mistrustful quantum cryptography involves parties that do not fully trust each other and may attempt to cheat or gain an advantage. These include fundamental primitives such as bit commitment, coin flipping and oblivious transfer, where the challenge lies in ensuring that no cheating parties can bias the protocol to their advantage without being detected. Unfortunately, it was proven that perfect i.t. secure quantum bit commitment (QBC) is impossible. [LC98] Nevertheless, i.t. secure QBC is possible in a setting where both parties can bias the protocol with a non-negligible probability strictly bounded away from 1. [BCWW25] Perfect quantum strong coin flipping (SCF) is later proven to be impossible too, with an optimal achievable bias of 0.207 using semi-definite programming. [Kit03]

Weak coin flipping (WCF) is a variant of the coin flipping primitive in which the participating parties have opposing preferences for the outcome. Classically, a WCF protocol can be derived from a SCF protocol, which in turn can be constructed from a bit commitment protocol. The same hierarchy holds in the quantum setting. However, unlike in the classical case, quantum WCF protocols can achieve arbitrarily small bias without relying on bit commitment as an intermediate primitive. [Moc07, ACG+16] Despite the existence of such protocols that achieve arbitrarily small bias in theory, no explicit protocol has yet attained such minimal bias in practice. Nevertheless, quantum WCF has been experimentally demonstrated using a large single-photon interferometer and an optical switch for verification, showing a bias as low as 0.207, and the protocol is feasible over a few kilometers of optical fiber. [BCKD20, NYC+23] The quantum leader election protocol, which builds upon WCF, can therefore be implemented both securely and efficiently. This motivates the focus of this thesis and the subject of my Master's degree project.

1.4. Contribution of this thesis

I began my Master's project as a theorist and together with PhD student Rebecca Hofer under the supervision of Mathieu Bozzio, we developed a new weak coin-flipping protocol. Later, I joined the experimental team and together with PhD student Daniel Kun, under the supervision of Lee Rozema, to implement the protocol in practice.

This thesis is structured into two main parts. In Chapter 2, I provide a brief introduction to the fundamentals of quantum mechanics and the theoretical background necessary to understand this work. Chapters 3 and 4 present the theoretical contributions of my Master's project, including the development of the weak coin-flipping protocol and its security proof. Chapters 5 and 6 describe the experimental aspects, covering the setup of the photon source and the practical implementation of the weak coin-flipping protocol.

2. Preliminaries

2.1. Basics of quantum mechanics

2.1.1. Quantum states

Linear algebra is a useful tool to describe quantum states. In general, quantum states can be described by state vectors in a Hilbert space, which is a complex vector space with an inner product. Quantum state vectors are commonly represented using the Dirac notation, also known as *bra-ket* notation. A vector $|\psi\rangle$ is called a *ket* and its dual $\langle\psi|$ is called a *bra*.

The inner product $\langle\psi| \cdot |\phi\rangle$, or dot product, takes a bra and a ket as input and produces a complex number as output:

$$\langle\psi| \cdot |\phi\rangle = \langle\psi|\phi\rangle = \begin{bmatrix} a_1^* & \cdots & a_n^* \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \sum_i a_i^* b_i \tag{2.1}$$

The outer product $|\phi\rangle \otimes \langle\psi|$, or tensor product, takes a ket and a bra as input and produces a matrix as output:

$$|\phi\rangle \otimes \langle\psi| = |\phi\rangle \langle\psi| = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \begin{bmatrix} a_1^* & \cdots & a_n^* \end{bmatrix} = \begin{bmatrix} b_1 a_1^* & \cdots & b_1 a_n^* \\ \vdots & \ddots & \vdots \\ b_n a_1^* & \cdots & b_n a_n^* \end{bmatrix} \tag{2.2}$$

When using the bra-ket notation, one often neglects the dot and tensor multiplication symbols.

In quantum information, the fundamental unit of information is the qubit, or quantum bit. A qubit is the quantum version of the classical bit, which takes on values 0 or 1. Qubits are described by state vectors in a two-dimensional complex Hilbert space and can exist in superpositions of the states $|0\rangle$ and $|1\rangle$. Physically, qubits can be realized by two-level quantum systems such as the spin states of an electron, the polarization states of a photon, or energy levels of an atom.

A basis is a set of linearly independent vectors that span a vector space. In linear algebra, the choice of basis is often arbitrary and it depends on the context or convenience of representation. The most commonly used basis for representing a qubit is the computational basis, which consists of the orthonormal states $|0\rangle$ and $|1\rangle$. In the context of the polarization of a photon, an equivalent orthonormal basis $|H\rangle$ and $|V\rangle$, corresponding to horizontal and vertical polarization, is often used. In vector form, these basis states can

be written as:

$$|0\rangle = |H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.3}$$

A general qubit state can be written as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.4}$$

where $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$ are spherical coordinates on the Bloch sphere. Bloch sphere representation offers great visualization of a qubit state, as an example shows:

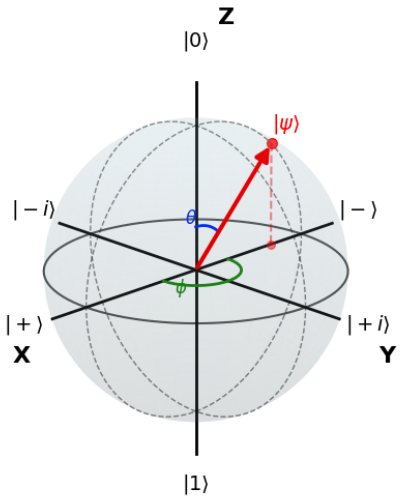


Figure 2.1.: Bloch representation of the state $|\psi\rangle$ with $\theta = \pi/4$ and $\phi = \pi$

In general, a quantum state can be fully described using its density matrix ρ. For a pure state $|\psi\rangle$, the density matrix is given by:

$$\rho = |\psi\rangle\langle\psi|$$

All density matrices must have the following properties:

- **Hermiticity:** $\rho = \rho^\dagger$
- **Trace one:** $\mathrm{Tr}(\rho) = 1$
- **Positive semi-definite:** All eigenvalues of ρ are non-negative, i.e., $\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle$.

A general single-qubit density matrix can be written using the Bloch vector representation as:

$$\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})$$

where $\vec{r}$ is the Bloch vector and $\vec{\sigma} = (X, Y, Z)$ are the Pauli matrices. The Bloch vector provides a geometric representation of qubit states, where its direction corresponds to the orientation of the state and its length indicates the purity of the state. Pauli matrices, which form the basis for qubit operators, are given by:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.5}$$

For pure states, their Bloch vectors lie on the surface of the sphere, i.e., $|\vec{r}| = 1$. However, in practical scenarios, the system is not in a perfect pure state but rather in a probabilistic mixture of several quantum states, which are called mixed states. For example, a qubit that is in state $|0\rangle$ with probability 0.5 and in state $|1\rangle$ with probability 0.5 is described by the density matrix:

$$\rho = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|$$

This is known as the maximally mixed state, corresponding to the center of the Bloch sphere.

2.1.2. Quantum operators and measurements

In quantum mechanics, the evolution and measurement of quantum systems are described using quantum operators. They are linear operators acting on a Hilbert space and can represent physical observables, unitary evolutions or state measurements.

Observables are physically measurable properties of a quantum state, such as position or momentum. Observables are represented by hermitian operators, which means their eigenvalues are real and correspond to the possible outcomes of a measurement. When an observable $\hat{O}$ is measured on a quantum state $|\psi\rangle$, the outcome is one of the eigenvalues λ_i of $\hat{O}$, and the system collapses to the corresponding eigenstate $|\lambda_i\rangle$. The probability of obtaining a specific outcome is given by the Born rule:

$$P(\lambda_i) = |\langle \lambda_i | \psi \rangle|^2$$

The expectation value of an observable in state ρ is:

$$\langle \hat{O} \rangle = \mathrm{Tr} \rho \hat{O}$$

The evolution of a quantum system is governed by a unitary operator. A unitary operator must satisfy the condition:

$$U^\dagger U = U U^\dagger = I$$

If a system is initially in the state $|\psi\rangle$, then under unitary evolution, its state at a later time is given by:

$$|\psi'\rangle = U |\psi\rangle$$

Unitary operators preserve inner products and are reversible. In quantum computing, unitary operations represent quantum logic gates. For example, the Hadamard gate, Pauli gates X, Y, Z, and multi-qubit gates like the CNOT gate are all unitary operators. These operations manipulate qubit states without measurement, preserving coherence of quantum states.

2.1.3. Quantum entanglement

Quantum entanglement is a unique feature of quantum mechanics. Entangled quantum states exhibit strong correlations that cannot be explained classically. Consider a bipartite quantum system described by the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. A pure state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is *entangled* if it cannot be written as a product state:

$$|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$$

Examples of entangled states are the Bell states, which are maximally entangled:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle \pm |11\rangle\right)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle \pm |10\rangle\right)$$

The Greenberger–Horne–Zeilinger (GHZ) state is another type of maximally entangled state that involves three or more subsystems. The 3 qubit GHZ state is given by:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right)$$

In general, entanglement is defined through separability. A mixed state is *separable* if it can be expressed as:

$$\rho_{AB} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad \text{where } p_i \geq 0, \sum_i p_i = 1$$

If no such decomposition exists, the state is entangled. Detecting entanglement in mixed states is generally more challenging and often requires entanglement witnesses or criteria such as the Peres-Horodecki (PPT) criterion.

2.2. Quantum information theory

2.2.1. No-signaling theorem

The no-signaling theorem implies that quantum entanglement cannot be used to transmit information faster than the speed of light. This principle ensures compatibility between quantum mechanics and relativity. Two distant observers Alice and Bob share a bipartite quantum state ρ_{AB}. The no-signaling theorem states that Alice's choice of measurement cannot influence the marginal outcome probabilities observed by Bob, and vice versa. Mathematically, Bob's reduced density matrix $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ remains unchanged regardless of Alice's measurement choice or outcome.

2.2.2. No-cloning theorem

The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state. Formally, there exists no unitary operation U such that for all quantum states $|\psi\rangle$ and a blank state $|0\rangle$, the following transformation holds:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

Suppose, for the sake of contradiction, that there exists a universal unitary operator U that can clone an arbitrary unknown quantum state. That is, for any states $|\psi\rangle$ and $|\phi\rangle$, and for an arbitrary blank state $|0\rangle$, the cloning operation would act as:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \quad U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$$

Since U is unitary, taking the inner product of both equations yields:

$$\langle\psi|\langle 0|U^\dagger U|\phi\rangle|0\rangle = \langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$$

The only solutions to this equation are either the states $|\phi\rangle$ and $|\psi\rangle$ are identical or they are orthogonal. Since quantum states are generally not orthogonal and may be unknown, no universal unitary operation can clone all arbitrary states. Hence, the cloning of arbitrary unknown quantum states is impossible. [NC10]

2.2.3. Quantum channels

In quantum information theory, the concept of a quantum channel plays a central role. It models any physical process that affects a quantum system. Mathematically, a quantum channel can be described as a **completely positive trace-preserving** (CPTP) map $\mathcal{E}$, which takes a quantum state ρ living in Hilbert space $\mathcal{H}_a$ to another quantum state ρ' living in Hilbert space $\mathcal{H}_b$.

A map $\mathcal{E}$ is said to be **completely positive** if, when it acts on a subspace of a larger Hilbert space, it still maps any positive semi-definite density matrix to another positive semi-definite density matrix. Formally, this means:

$$(\mathcal{E}\otimes\mathcal{I}_n)(\rho) \geq 0 \quad \text{for all } \rho \geq 0,$$

where $\mathcal{I}_n$ is the identity map on an auxiliary n-dimensional Hilbert space.

A map is **trace-preserving** if it preserves the trace of any input state:

$$\mathrm{Tr}[\mathcal{E}(\rho)] = \mathrm{Tr}[\rho] = 1,$$

which guarantees that the total probability is conserved after the transformation.

Furthermore, any CPTP map $\mathcal{E}$ can be decomposed into a sum of Kraus operators $\hat{K}$:

$$\mathcal{E} = \sum_i \hat{K}_i \rho \hat{K}_i^\dagger \tag{2.6}$$

and $\hat{K}$ must satisfy $\sum_i \hat{K}\hat{K}_i^\dagger = \mathbb{1}$

2.2.4. Choi-Jamiołkowski isomorphism

There are many different ways to describe a quantum channel. A convenient way to represent quantum channels is through the **Choi–Jamiołkowski isomorphism**, also known as *channel-state duality*.

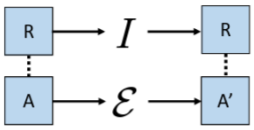


Figure 2.2.: Graphic visualization of Choi-Jamiołkowski isomorphism, screenshot taken from lecture notes of [Pre21]

Let us consider a d-dimensional linear CPTP map $\mathcal{E}$ that acts on $\mathcal{H}_{\mathrm{A}}$ to $\mathcal{H}_{\mathrm{A}'}$ and an auxillary d-dimensional system $\mathcal{H}_{\mathrm{R}}$. The corresponding state matrix, also known as the *Choi matrix*, is defined as:

$$J_{\mathcal{E}} = (\mathcal{I} \otimes \mathcal{E})(|\Phi\rangle_{\mathrm{RA}} \langle\Phi|_{\mathrm{RA}}),$$

where $|\Phi\rangle_{\mathrm{RA}} = \sum_{i=0}^{d-1} |i\rangle_{\mathrm{R}} \otimes |i\rangle_{\mathrm{A}}$ is an unnormalized maximally entangled state on $\mathcal{H}_{\mathrm{R}} \otimes \mathcal{H}_{\mathrm{A}}$, and $\mathcal{I}$ is the identity map. The resulting Choi matrix $J_{\mathcal{E}}$ fully characterizes the action of the quantum channel $\mathcal{E}$, in particular:

- $\mathcal{E}$ is completely positive if and only if $J_{\mathcal{E}} \geq 0$,
- $\mathcal{E}$ is trace-preserving if and only if $\mathrm{Tr}_{\mathcal{H}_{\mathrm{A}'}}[J_{\mathcal{E}}] = \mathcal{I}_{\mathcal{H}_{\mathrm{A}}}$,

The Choi-Jamiołkowski isomorphism plays an important role in semi-definite programming, where optimization problems involving quantum channels are involved. The details of semi-definite programming will be introduced later.

2.3. Quantum cryptography

Quantum cryptography utilizes the laws of quantum mechanics to enable secure communication between multiple parties. It typically provides *information-theoretic* (i.t.) security, meaning that its security does not rely on computational assumptions.

In general, quantum cryptographic primitives can be divided into two categories: **trustful** and **mistrustful** quantum cryptography. In trustful quantum cryptography, the involved parties cooperate to achieve a common goal—for example, establishing a secure key that remains private from any eavesdropper. In contrast, mistrustful quantum cryptography involves parties that do not trust each other; each party may attempt to cheat in order to influence the protocol's outcome in their favor.

This chapter introduces key examples from both categories and presents mathematical tools such as *semi-definite programming* that are used in security proofs.

2.3.1. Quantum key distribution

Quantum Key Distribution (QKD) is the most well-known and widely implemented protocol in quantum cryptography. It is the flagship example of trustful quantum cryptography, where two honest parties, Alice and Bob, collaborate to establish a shared secret key against any eavesdropper.

In the BB84 QKD protocol [BB84], Alice encodes her secret key into a sequence of quantum states using two pairs of mutually unbiased bases—for example, horizontal/vertical (H/V) and diagonal/anti-diagonal (D/A) polarization states. For each bit, she randomly chooses one of the two bases and prepares a corresponding quantum state, which she then sends to Bob over a quantum channel. Upon receiving the states, Bob independently and randomly chooses a measurement basis (H/V or D/A) for each qubit. After the quantum measurement, Alice and Bob communicate over a classical channel to compare their basis choices. They discard all outcomes where their bases did not match, leaving behind a sifted key composed of bits where both used the same basis.

To detect the presence of an eavesdropper, Alice and Bob randomly select a subset of the sifted key and compare their measurement results. If the error rate is below a certain threshold, they proceed with further post-processing steps such as error correction. If the error rate is too high, indicating possible eavesdropping, the protocol is aborted.

The security of BB84 is guaranteed by the *no-cloning theorem*: since Eve does not know the basis in which each qubit was prepared, any attempt to intercept and measure the quantum states introduces detectable disturbances. In an ideal case, the probability that an eavesdropper correctly guesses the basis and escapes detection on a single bit is $\frac{3}{4}$, making the probability of undetected eavesdropping on an n-bit key equal to $\left(\frac{3}{4}\right)^n$. Once verified, the final shared key can be used as a one-time pad to encrypt any message, providing i.t. security as long as it is used only once.

2.3.2. Quantum bit commitment

Bit commitment (BC) is a cryptographic protocol involving two mutually distrustful parties, where one party (the sender) commits to a binary value and sends a piece of information to the other party (the receiver) for temporary storage. Later, the sender reveals the committed value. A typical BC protocol consists of two phases: the *commit phase* and the *unveil phase*. In the *commit phase*, the sender transmits a commitment message $\mathrm{com}(b)$ to the receiver. This message hides the value b in such a way that the receiver cannot determine it beforehand. In the *unveil phase*, the sender sends a second message $\mathrm{reveal}(b)$, which discloses the original value. The receiver uses a public verification algorithm to check that the revealed value matches the initial commitment.[BCWW25]

A secure BC protocol should guarantee two properties: **binding** and **hiding**. Binding refers to the property that once the sender has committed to a value b, they cannot change it at any point during the protocol. Hiding ensures that the receiver cannot correctly determine the value b in any way before the sender reveals it. In classical BC protocols, the security is guaranteed by the time-bounded computational power of at least one party.

The first quantum BC protocol was proposed in the famous BB84 paper, where QKD

was also introduced. However, the authors presented an attack against their own protocol in the same work [BB84]. Despite many ideas on proposing a i.t.-secure quantum BC, it was later proven that a perfectly i.t.-secure quantum BC protocol is impossible [LC98].

Suppose Alice commits to a value b by preparing an entangled state ρ_{AB}^{b} on $\mathcal{H}_A \otimes \mathcal{H}_B$ and sending the subsystem on $\mathcal{H}_B$ to Bob. If the protocol is perfectly hiding, then Bob's reduced density matrix must be identical regardless of Alice's choice of b, i.e.,

$$\mathrm{Tr}_A\left(\rho_{AB}^{(0)}\right) = \mathrm{Tr}_A\left(\rho_{AB}^{(1)}\right).$$

This condition implies that there exists a unitary operation on Alice's subsystem that can transform $\rho_{AB}^{(0)}$ into $\rho_{AB}^{(1)}$, thereby violating the binding property.

Despite the no-go theorem for perfect quantum BC, it is possible to implement the protocol in a setting where both parties can bias the binding and hiding conditions with a non-negligible probability, strictly bounded away from 1. In such cases, there is a non-zero probability of detecting a cheating party, causing the protocol to abort. These BC schemes are known as *cheat-sensitive* quantum bit commitment [BCH+08]. Without cheat-sensitivity, it is also possible to derive a quantum BC scheme from quantum weak coinflipping with arbitrarily small bias [CK11].

2.3.3. Quantum coin flipping

Coin flipping protocols, also known as *coin flipping by telephone* [Blu83], are cryptographic protocols in which two spatially separated and mutually distrustful parties attempt to agree on a random bit. Such protocols can be classified into two categories: *strong coin flipping* (SCF) and *weak coin flipping* (WCF). In SCF, neither party has a preferred outcome; the goal is to generate a fair random bit. In contrast, in WCF, each party has a preferred outcome (for example, Alice prefers 0 while Bob prefers 1), and the protocol aims to ensure that neither party can force their preferred outcome with probability greater than 1/2.

An ideal SCF protocol should guarantee that the output is a uniformly random bit. Moreover, a dishonest party should not be able to force their opponent to output $i \in \{0, 1\}$ with probability greater than $P_D^i = \frac{1}{2} + \epsilon_D^i$, where ϵ_D^i is called the *bias* of the protocol. In a balanced SCF protocol, the biases ϵ_A^0, ϵ_A^1, ϵ_B^0, and ϵ_B^1 are all equal. Classical SCF protocols can be deployed using BC or relying on computational assumptions. Quantum coin flipping, however, can limit the cheating advantage to a fixed bound strictly less than 1 without commputational assumptions. Quantum WCF is particularly notable because there exist protocols that make the bias arbitrarily small, as shown in Mochon's proof [Moc07]. Nevertheless, no practical experimental implementation has yet achieved an arbitrarily small bias.

Quantum coin flipping protocols have potential practical applications in scenarios such as leader election in distributed networks and online gaming. The main goal of this thesis is to implement a loss-tolerant quantum WCF protocol, which can be further extended to a quantum leader election protocol.

2.3.4. Semi-definite programming

Semi-definite programming (SDP) is a class of convex optimization problems where one optimizes a linear objective function over the intersection of an affine space with the cone of positive semidefinite matrices. SDPs generalize linear programs by replacing vector variables constrained to be non-negative with matrix variables constrained to be positive semidefinite.

An SDP can be written in its *primal form* as

$$\begin{aligned} \max \quad & \langle C, X\rangle = \mathrm{Tr}(C^\dagger X) \\ \text{subject to} \quad & \Lambda(X) = B, \\ & X \succeq 0, \end{aligned}$$

where X is the positive semidefinite matrix variable, C and B are Hermitian operators, and Λ is a linear Hermiticity-preserving map. Any X satisfying the constraints is said to be *primal feasible*, and the optimal primal value is

$$\alpha = \sup\{\langle C, X\rangle : X \succeq 0,\, \Lambda(X) = B\}.$$

Any SDP can be written in its *dual form*, obtained via the Lagrange multipliers:

$$\begin{aligned} \min \quad & \langle B, Y\rangle = \mathrm{Tr}(B^\dagger Y) \\ \text{subject to} \quad & \Lambda^*(Y) \succeq C, \\ & Y = Y^\dagger, \end{aligned}$$

where Λ^* is the adjoint of Λ. Any Hermitian Y satisfying the constraints is said to be *dual feasible*, and the optimal dual value is

$$\beta = \inf\{\langle B, Y\rangle : Y = Y^\dagger,\, \Lambda^*(Y) \succeq C\}.$$

The relationship between primal and dual problems is captured by the notions of weak and strong duality. *Weak duality* ensures that $\alpha \leq \beta$ always holds. In many quantum-cryptographic applications however, we wish to ensure that the upper bound derived in the primal problem is tight, i.e. $\alpha = \beta$. The dual problem will help to prove this when there exists such strong duality. Slater's theorem states the conditions for such strong duality to hold. [Boz25]

SDPs are especially useful in security proofs of quantum cryptographic protocols, where the adversary's optimal cheating strategy is expressed as a positive semidefinite variable, and the protocol's security parameter (e.g., the bias of a coin flipping protocol) corresponds to the optimal value of the SDP.

2.4. Basics of Quantum Optics

In this subchapter, I briefly introduce the essential quantum formalism of the photon together with fundamental concepts of quantum optics, with a focus on linear optics that are directly relevant for the experiment of this thesis. Moreover, I introduce the process of spontaneous parametric down-conversion (SPDC), which is important for understanding the single-photon source used in the experiment.

2.4.1. Second Quantization

A multi-particle system can be described by a product of single-particle wavefunctions in the first-quantization formalism. However, for systems with many indistinguishable photons, the state of the system can be given by the occupation numbers of each mode, rather than a product of individual particle wavefunctions. This is referred to as the *second quantization* in quantum optics. In the second quantization, the electromagnetic field is quantized and each mode of the field is a quantum harmonic oscillator. The field modes each corresponds to a oscillator that makes up the *Fock space*.

The *Fock space* is built from the *Fock basis* $\{|n\rangle\}_{n=0}^{\infty}$, where $|n\rangle$ denotes a state with exactly n photons in a given mode. The creation operator

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

and annihilation operator

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

act as ladder operators that increase or decrease the photon number. These operators are not Hermitian, and therefore do not correspond directly to observables. However, it is possible to construct observables from them. An example of which is the photon number operator

$$N = a^\dagger a,$$

which has eigenvalues n corresponding to the photon number in the mode, i.e.

$$N|n\rangle = n|n\rangle.$$

The quantized Hamiltonian of a single field mode is given by

$$H = \hbar\omega\left(a^\dagger a + \tfrac{1}{2}\right),$$

The vacuum state $|0\rangle$, defined by $a|0\rangle = 0$, represents the absence of photons but still carries the zero-point energy $\hbar\omega/2$.

2.4.2. Linear Optics and Linear Optical Devices

Optical devices used in the lab, such as mirrors and beam splitters, are examples of *linear optical devices*. This means that their response to the electric field is linear and does not depend on the intensity of the light.

In the framework of second quantization, these devices can be described by Hamiltonians composed of annihilation and creation operators. Consider a *phase shifter*: it changes the phase of the electromagnetic field in a given mode, which can be a material that alters the path length of incoming photons. Its corresponding unitary transformation is

$$a_{\text{out}} = e^{i\phi a_{\text{in}}^\dagger a_{\text{in}}}\, a_{\text{in}}\, e^{-i\phi a_{\text{in}}^\dagger a_{\text{in}}} = e^{i\phi} a_{\text{in}}. \tag{2.7}$$

Thus, a phase shifter simply multiplies the field operator by a phase factor $e^{i\phi}$. [KMN+07]

Another prominent example is the *beam splitter* (BS). The action of the beam splitter on the creation operator of mode a is

$$a^\dagger \longrightarrow U_{\mathrm{BS}}\, a^\dagger\, U_{\mathrm{BS}}^\dagger. \tag{2.8}$$

One can show that this transformation yields [Str23]

$$\begin{aligned} a^\dagger &\longrightarrow \cos\theta\, a^\dagger - ie^{-i\phi}\sin\theta\, b^\dagger, \\ b^\dagger &\longrightarrow -ie^{i\phi}\sin\theta\, a^\dagger + \cos\theta\, b^\dagger. \end{aligned} \tag{2.9}$$

In the mode basis

$$a^\dagger = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad b^\dagger = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

the beam splitter transformation can be written as the unitary matrix

$$U_{\mathrm{BS}} = \begin{pmatrix} \cos\theta & -ie^{-i\phi}\sin\theta \\ -ie^{i\phi}\sin\theta & \cos\theta \end{pmatrix}. \tag{2.10}$$

In the common case of a 50:50 beam splitter, the unitary transformation reduces to

$$U_{\mathrm{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.11}$$

The corresponding action on the creation operators is

$$\begin{aligned} a_{\mathrm{out}}^\dagger &= \frac{1}{\sqrt{2}} \left(a_{\mathrm{in}}^\dagger + b_{\mathrm{in}}^\dagger \right), \\ b_{\mathrm{out}}^\dagger &= \frac{1}{\sqrt{2}} \left(a_{\mathrm{in}}^\dagger - b_{\mathrm{in}}^\dagger \right). \end{aligned} \tag{2.12}$$

This corresponds to a balanced mixing of the two input modes, where each output mode is an equal superposition of the inputs. The overall transformation is unitary and conserves the total photon number.

A *polarizing beam splitter* (PBS) is an optical device that transmits horizontally polarized light and reflects vertically polarized light. Its action on the creation operators can be expressed as

$$\begin{aligned} a_H^\dagger &\longrightarrow a_H^\dagger, \qquad & a_V^\dagger &\longrightarrow b_V^\dagger, \\ b_H^\dagger &\longrightarrow b_H^\dagger, \qquad & b_V^\dagger &\longrightarrow a_V^\dagger, \end{aligned} \tag{2.13}$$

where H and V denote horizontal and vertical polarization components, respectively. Thus, the PBS separates the two polarization components into different spatial output modes. It is an essential tool for measurements in polarization basis.

There are also optical devices that alter the polarization state of incoming light; such devices are called *waveplates*. Waveplates are birefringent crystals that introduce a relative phase retardance between two orthogonal polarization components of the electromagnetic field. The crystal is cut into a thin plate, with the orientation of the cut chosen such that

one of the principal axes, called the *fast axis*, lies parallel to the surface of the plate, while the other axis, called the *slow axis*, is parallel to the direction of light propagation. The difference in refractive indices along these axes causes a controlled phase delay between the orthogonal polarization components.

Waveplates are commonly classified into *half-waveplates* (HWP) and *quarter-waveplates* (QWP). A HWP introduces a phase shift of π between the two orthogonal polarization components, effectively rotating the polarization direction, while a QWP introduces a phase shift of $\pi/2$, allowing the conversion between linear and circular polarization states depending on the input polarization and the waveplate orientation.

Using Jones Calculus, one can show that the evolution of the creation operators under a HWP oriented at an angle θ with respect to the horizontal axis is given by

$$\begin{aligned} a_H^\dagger &\longrightarrow \cos 2\theta\, a_H^\dagger + \sin 2\theta\, a_V^\dagger, \\ a_V^\dagger &\longrightarrow \sin 2\theta\, a_H^\dagger - \cos 2\theta\, a_V^\dagger. \end{aligned} \tag{2.14}$$

and for a QWP oriented at an angle θ, the transformation is

$$\begin{aligned} a_H^\dagger &\longrightarrow e^{i\pi/4}\Big((\cos^2\theta + i\sin^2\theta)\, a_H^\dagger + (1-i)\cos\theta\, \sin\theta\, a_V^\dagger\Big), \\ a_V^\dagger &\longrightarrow e^{i\pi/4}\Big((1-i)\cos\theta\, \sin\theta\, a_H^\dagger + (\sin^2\theta + i\cos^2\theta)\, a_V^\dagger\Big). \end{aligned} \tag{2.15}$$

Lastly, a *linear polarizer* is an optical device that transmits only the component of light aligned along a specific linear polarization direction while blocking all other components. Linear polarizers are commonly used for polarization preparation and characterization, and they are essential for characterizing the zero angle of an uncharacterized waveplate in combination with a PBS or a polarimeter.

2.4.3. SPDC Photon Source

The single-photon source used in the experiment exploits the process of *spontaneous parametric down-conversion* (SPDC). To understand this mechanism, it is necessary to introduce the concept of *nonlinear optics*. This subsection briefly explains the essential nonlinear optical process, followed by the quantum description of SPDC.

In classical nonlinear optics, the polarization density of a medium can be expressed as a power series in the electric field:

$$\mathbf{P}(t) = \varepsilon_0 \left(\chi^{(1)}\mathbf{E}(t) + \chi^{(2)}\mathbf{E}^2(t) + \chi^{(3)}\mathbf{E}^3(t) + \cdots\right), \tag{2.16}$$

where ε_0 is the vacuum permittivity, $\chi^{(1)}$ is the linear susceptibility, and $\chi^{(2)}, \chi^{(3)}, \ldots$ are the nonlinear susceptibilities of higher order. The total polarization can thus be written as the sum of a linear and a nonlinear contribution:

$$\mathbf{P}(t) = \mathbf{P}^{(L)}(t) + \mathbf{P}^{(NL)}(t). \tag{2.17}$$

In the regime of linear optics, the nonlinear terms are typically negligible. However, when the medium is driven by a strong electric field, the nonlinear contributions become

significant. In this context, we focus on the *second-order* nonlinear term, governed by the susceptibility tensor $\chi^{(2)}$.

Recall that by expanding Maxwell's equations, one obtains the following wave equation for the electric field:

$$\frac{\partial^2 \mathbf{E}}{\partial x^2} = -\mu_0 \varepsilon_0 \frac{\partial^2 \mathbf{E}}{\partial t^2} + \mu_0 \frac{\partial^2 \mathbf{P}^{(NL)}}{\partial t^2}, \tag{2.18}$$

A general solution to this equation, where the non-linear term is 0, takes the form

$$\mathbf{E}(x,t) = \mathbf{A}\, e^{i(kx-\omega t)} + \text{c.c.}, \tag{2.19}$$

where $\mathbf{A}$ is the complex amplitude, k is the wavevector, and "c.c." denotes the complex conjugate.

As an example, consider the process of *sum-frequency generation* (SFG). In SFG, two input photons with frequencies ω_1 and ω_2 interact through the second-order nonlinearity to produce an output photon with frequency ω_3, such that

$$\hbar\omega_3 = \hbar\omega_1 + \hbar\omega_2 \tag{2.20}$$

We also have

$$\mathbf{E}_3(x,t) = \mathbf{E}_{3,0}\, e^{i(k_3 x-\omega_3 t)} + \text{c.c.}, \tag{2.21}$$

$$\mathbf{P}_3(x,t) = \mathbf{P}_{3,0}\, e^{i(k_3 x-\omega_3 t)} + \text{c.c.}, \tag{2.22}$$

where

$$\mathbf{P}_{3,0} = 4\varepsilon_0 d_{\text{eff}} \mathbf{E}_1 \mathbf{E}_2, \tag{2.23}$$

and d_{eff} denotes the effective nonlinearity of the material.

By inserting Eqs. (2.21) and (2.22) into the wave equation (Eq. 2.18) and solving for the amplitude A_3, one obtains the following expression for the intensity $I_3 \propto |\mathbf{A}_3|^2$ [Cou18]:

$$I_3 = \frac{8 d_{\text{eff}}^2 \omega_3^2 I_1 I_2 L^2}{n_1 n_2 n_3 \varepsilon_0 c^3} \left(\frac{\sin(\Delta k L/2)}{\Delta k L/2} \right)^2 = I_3^{\max} \operatorname{sinc}^2 \left(\frac{\Delta k L}{2} \right), \tag{2.24}$$

where $\Delta k = k_3 - k_1 - k_2$ is the phase mismatch, n_1, n_2, and n_3 are the corresponding refractive indices, and L is the crystal length. It becomes apparent that I_3 reaches its maximum when $\Delta k = 0$, which defines the *phase-matching condition*:

$$k_3 = k_1 + k_2, \qquad \frac{n_3 \omega_3}{c} = \frac{n_1 \omega_1}{c} + \frac{n_2 \omega_2}{c}. \tag{2.25}$$

Such a phase-matching condition can be satisfied by using a birefringent crystal, which exhibits different refractive indices along distinct optical axes. However, it is important to note that the process of SPDC, in which a single photon of higher frequency is converted into two photons of lower frequencies—although often regarded as the reverse process of SFG, cannot be fully explained within the framework of classical optics. Therefore, a quantum description is required. Without going into further detail, we can infer an effective interaction Hamiltonian for SPDC [Cou18]:

$$\hat{H}_{\text{SPDC}} = i\hbar\kappa \left(\hat{a}_i \hat{a}_s \hat{a}_p^\dagger e^{i(\Delta\vec{k}\cdot\vec{r}-\Delta\omega t)} - \hat{a}_i^\dagger \hat{a}_s^\dagger \hat{a}_p e^{-i(\Delta\vec{k}\cdot\vec{r}-\Delta\omega t)} \right), \tag{2.26}$$

where the first term accounts for the SFG process and the second term for the SPDC process. κ is a constant depending on the nonlinearity of the crystal. The photon number state with N_p pump photons evolves in the Schrödinger picture as

$$|\psi(t)\rangle = \exp\left[-\frac{i}{\hbar}\int_0^t \hat{H}_{\mathrm{SPDC}}(t')\,dt'\right]|0_s, 0_i, N_p\rangle \approx C_0|0_s, 0_i, N_p\rangle + \kappa C_1 e^{-i\Delta\vec{k}\cdot\vec{r}}|1_s, 1_i, N_p - 1\rangle, \tag{2.27}$$

The intensity will be proportional to the square norm of the wave function in Eq. 2.27. Note that κ is usually very small, so when the crystal is pumped with a laser, only a small fraction of the input photons is converted into pairs of down-converted photons. Also, since we only consider the first two terms of the Taylor expansion in Eq. 2.27, a sufficiently strong pump can lead to a non-zero probability of generating multiple photon pairs. Such multi-photon emission is generally undesired in cryptographic protocols, where only a single photon pair is required, as it can potentially compromise security. [BVC+22]

The SPDC process can be categorized into three types. If the pump, signal, and idler photons all have the same polarization, the process is classified as Type-0 SPDC. If the pump polarization is orthogonal to that of the signal and idler photons, it is referred to as Type-I SPDC. Finally, if the signal and idler photons are orthogonally polarized with respect to each other, the process is called Type-II SPDC. [CFH+13]

2.4.4. Quasi Phase Matching and PPKTP Crystal

For an efficient SPDC source, both the energy and momentum of the pump, signal, and idler photons must be conserved. As discussed in Chapter 2.4.3, this is ensured by satisfying the phase-matching condition. One common method is *birefringent phase matching*, as implemented for example using a β-barium borate (BBO) crystal [KMW+95], where the optical axis is oriented at a specific angle and the spatial modes of the ordinary and extraordinary photons are subsequently overlapped.

An alternative approach is *quasi-phase matching*. In this method, the phase-matching condition is achieved by periodically inverting the sign of the nonlinear susceptibility of the crystal, leading to an effective momentum compensation:

$$\Delta k = k_p - k_s - k_i \pm \frac{2\pi}{\Lambda} \approx 0,$$

where Λ is the poling period of the crystal. By choosing an appropriate poling period and temperature, the phase-matching condition can be engineered for a wide range of pump, signal, and idler wavelengths. [BRHS10]

Quasi-phase matching also enables highly efficient type-0 SPDC processes, in which the pump, signal, and idler photons all share the same polarization along a principal axis. Such interactions cannot be achieved using birefringent phase matching but become possible when the nonlinear susceptibility is periodically inverted, as in periodically poled potassium titanyl phosphate (PPKTP) crystals. Additional advantage of quasi-phase matching is the ability to freely select the largest component of the nonlinear susceptibility tensor, thereby maximizing the conversion efficiency.

3. Weak coin-flipping protocol based on GHZ game

3.1. Preliminary weak coin-flipping protocol

Before the start of my Master's project, a symmetric weak coin-flipping protocol based on an interferometer shared between two parties had already been proposed. In this chapter, I will briefly discuss why this proposal failed due to trivial attacks, and how it subsequently inspired the development of a new weak coin-flipping protocol based on the GHZ game.

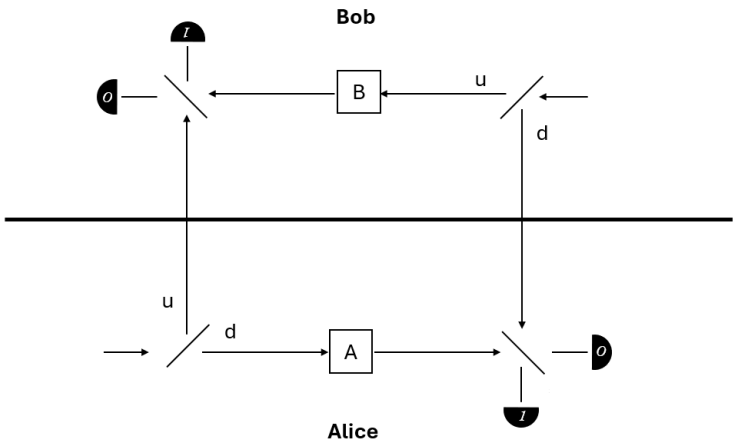


Figure 3.1.: An interferometer shared between two parties executing a weak coin-flipping protocol. u denotes the case where the photon propagates through the upper path of the interferometer, while d denotes the lower path.

Consider the interferometer shown in Fig. 3.1, where both parties send a single photon from their respective sources. Each photon first encounters a 50/50 beam splitter (BS), after which it can either travel to the other party or acquire a local phase ϕ_A or ϕ_B. The photons then propagate to a second BS. If both photons arrive at the same BS, they may bunch and exit together through either output port **0** or **1**; otherwise, they are detected separately at both ports. Conversely, if both photons remain on their respective sender's sides or if both photons travel to the opposite sides, each party will observe a detection event at one of the output ports on their own side. The state after both photons pass through the first beam splitter can be expressed as

$$\frac{1}{2}\left(\hat{a}_u^\dagger + \hat{a}_d^\dagger\right) \otimes \left(\hat{b}_u^\dagger + \hat{b}_d^\dagger\right) |0_A 0_B\rangle \,. \tag{3.1}$$

Here, u denotes the case where the photon propagates through the upper path of the interferometer, while d denotes the lower path. The state $|0_A 0_B\rangle$ represents the vacuum state. After passing through the corresponding second beam splitter, the state can be described as

$$\frac{1}{4}\left(e^{i\phi_A}(\hat{a}_0^\dagger + \hat{a}_1^\dagger) + \hat{a}_0^\dagger + \hat{a}_1^\dagger\right) \otimes \left(\hat{b}_0^\dagger + \hat{b}_1^\dagger + e^{i\phi_B}(\hat{b}_0^\dagger - \hat{b}_1^\dagger)\right) |0_A 0_B\rangle \,. \tag{3.2}$$

Now, consider the case where both photons either remain on their respective sender's sides or both travel to the opposite sides. In other words, we examine the state

$$\begin{aligned} |\Psi\rangle = \frac{1}{2}\Big[& e^{i(\phi_A+\phi_B)}\big(\,|\mathbf{0}_A\mathbf{0}_B\rangle - |\mathbf{0}_A\mathbf{1}_B\rangle + |\mathbf{1}_A\mathbf{0}_B\rangle - |\mathbf{1}_A\mathbf{1}_B\rangle\,\big) \\ & + \big(\,|\mathbf{0}_A\mathbf{0}_B\rangle + |\mathbf{0}_A\mathbf{1}_B\rangle - |\mathbf{1}_A\mathbf{0}_B\rangle - |\mathbf{1}_A\mathbf{1}_B\rangle\,\big)\Big]. \end{aligned} \tag{3.3}$$

Here, **0** and **1** denote the output ports of the second BS on each side, as shown in Fig. 3.1. One can see that when $\phi_A + \phi_B = 0$, the outcomes on both sides are correlated, whereas when $\phi_A + \phi_B = \pi$, the outcomes are anti-correlated.

In this weak coin-flipping protocol, Alice and Bob share the same interferometric setup described earlier. Each party sends a single photon into their respective input port and measures the outcome at their output ports. Afterward, they announce their local phase choice, $\phi_{A/B} \in \{0, \pi\}$. If their phase choices match (correlated), Alice wins when the measurement result is **0**, and Bob wins when the result is **1**. Conversely, if their phase choices differ (anti-correlated), the player who measures the outcome **0** is declared the winner. Since the setup is symmetric, both parties know the outcome of the coin-flip after the announcement of the phase.

Table 3.1.: Truth table of all possible outcomes of this weak coin-flipping protocol.

Correlation	ϕ_A	ϕ_B	Alice	Bob	Winner
Correlated	0	0	**0**	**0**	Alice
	π	π	**0**	**0**	Alice
	0	0	**1**	**1**	Bob
	π	π	**1**	**1**	Bob
Anti-correlated	0	π	**0**	**1**	Alice
	π	0	**0**	**1**	Alice
	0	π	**1**	**0**	Bob
	π	0	**1**	**0**	Bob

It is easy to spot a trivial attack in this protocol. If a dishonest Alice obtains a measurement outcome that would cause her to lose the coin flip, she can simply announce the opposite of her chosen phase. Since an honest Bob has no way to verify Alice's actual

phase and must rely solely on her declaration, he will be misled into believing the opposite correlation case and conclude that he lost the coin flip. Consequently, Alice can win with a probability of 100%. The same argument applies symmetrically to a dishonest Bob, showing that this protocol is insecure.

Moreover, this protocol relies on the cases where each party detects a photon at one of their output ports, which occurs with only 50% probability. The remaining 50% of events in which both photons bunch at one of the parties must be discarded and are treated as losses or as an abort of the protocol.

Based on these observations, we began exploring alternative approaches to realize a secure weak coin-flipping protocol. Inspired by the work of [ASVH24], we developed a new weak coin-flipping protocol that uses the GHZ game as a verification mechanism against dishonest parties.

3.2. GHZ game

Before introducing the new weak coin-flipping protocol, we should understand the mechanism of the GHZ game. This subchapter will introduce how the GHZ game works and why it can be helpful in the new weak coin-flipping protocol.

Consider a cooperative three-player game between Alice, Bob, and Charlie. Each player receives a 1-bit input r, s, and t, respectively. Each player is also required to output 1 bit a, b, and c, respectively. It is promised that the input given fulfills the condition $r \oplus s \oplus t = 0$. The players can previously agree on a winning strategy, but after the game starts, no communication between the players is allowed. The players win the game if their outputs satisfy the condition $r \oplus s \oplus t = a \vee b \vee c$. The winning condition can be summarized in the table below:

rst	$a \oplus b \oplus c$
000	0
011	1
101	1
110	1

It can be shown that, classically, there exists no perfect winning strategy that allows the players to always win the game. [Cle21] Even with the optimal classical strategy, the players can win with at most a probability of 3/4. In contrast, in the quantum case, there exists a perfect strategy that allows the players to win the game with certainty.

In quantum strategy, all three players share an entangled three-partite GHZ state in computational basis (Z-basis):

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right)$$

When a player receives an input bit 0, they measure their qubit in the X basis and output the measurement result. If the input bit is 1, they measure their qubit in the Y basis and output the result. It can be shown that, following this strategy, the outcomes

satisfy the winning condition $r \oplus s \oplus t = a \vee b \vee c$ in every round [ASVH24]. Since this winning condition can only be achieved when all players share a GHZ state, and cannot be achieved with certainty classically or without the GHZ state, this property can be used to verify the correctness of the protocol or to detect the presence of a dishonest party. This verification process is also referred to as the GHZ test, which plays an essential role in the new weak coin-flipping protocol.

3.3. Non loss-tolerant weak coin-flipping protocol

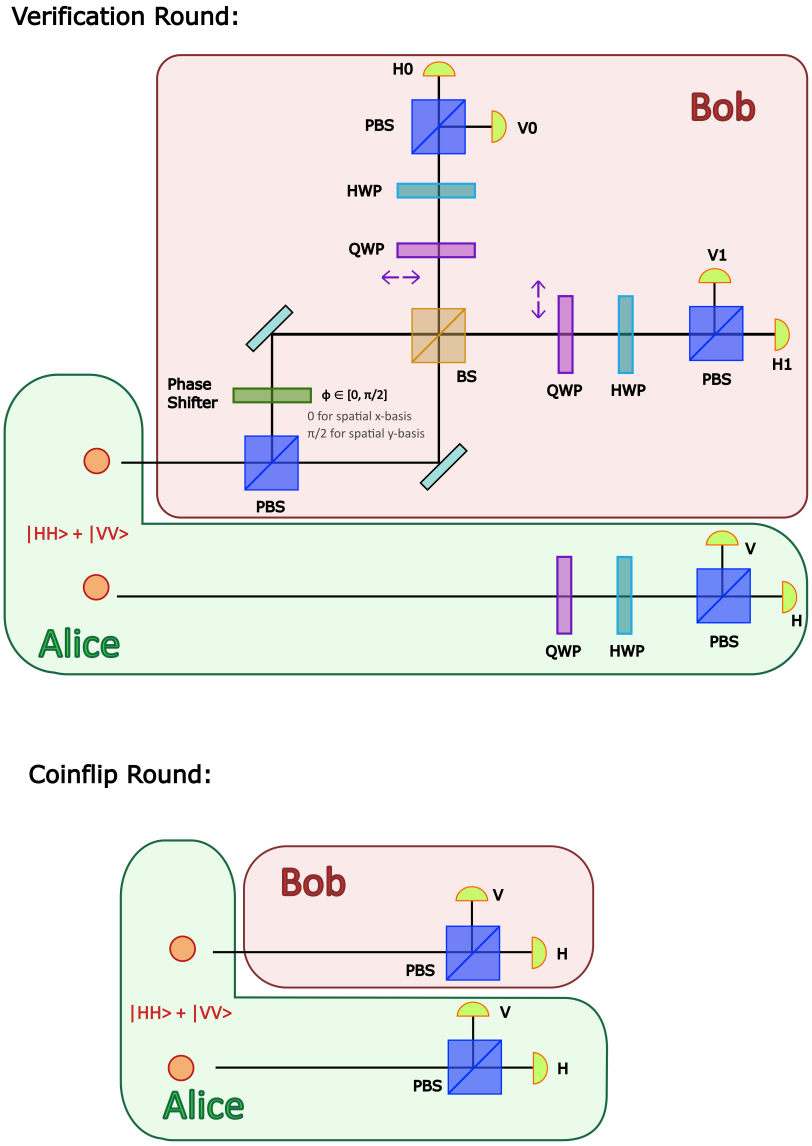


Figure 3.2.: Scheme of the protocol. Alice generates two pairs of Bell $|\Phi^+\rangle$ states and sends one photon from each pair to Bob. They use one photon pair to execute the coin-flip round, which determines the winner, and the other pair to execute the verification round, allowing Bob to check the integrity of the protocol.

Figure 3.2 represents the basic optical elements required to implement the protocol. The protocol can be divided into the following steps:

1. **State Preparation by Alice**

   Alice prepares two pairs of Bell states entangled in the polarization degree of freedom:

   $$|\psi\rangle = |\Phi^+\rangle_i \otimes |\Phi^+\rangle_{1-i} = \frac{1}{2}\left(a^\dagger_{H0}a^\dagger_{H0} + a^\dagger_{V0}a^\dagger_{V0}\right) \otimes \left(a^\dagger_{H0}a^\dagger_{H0} + a^\dagger_{V0}a^\dagger_{V0}\right)|0000\rangle\,, \quad (3.4)$$

   where $i \in \{0, 1\}$, and $a^\dagger_{H0}$ denotes the creation operator for a horizontally polarized photon in spatial mode 0.

2. **Distribution of Photons**

   Alice keeps one photon from each Bell pair and sends the other photon of each pair to Bob. Since only Bob's spatial modes are relevant to the protocol, we can simplify the notation as:

   $$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|HH0\rangle_{a,b,b} + |VV0\rangle_{a,b,b}\right) \otimes \frac{1}{\sqrt{2}}\left(|HH0\rangle_{a,b,b} + |VV0\rangle_{a,b,b}\right). \quad (3.5)$$

3. **Assigning Verification and Coin-flipping photons.**

   After receiving his photons, Bob chooses which Bell pair will serve as the *verification* state and which as the *coin-flip* state:

   $$|\,Ver\rangle = |\Phi^+\rangle_i\,, \qquad |\,Coin\rangle = |\Phi^+\rangle_{1-i}\,.$$

   He announces his chosen index i to Alice. Bob then sends his $|\,Ver\rangle$ photon through a polarizing beam splitter (PBS), after which Alice and Bob share:

   $$|\psi\rangle = |\,Ver\rangle \otimes |\,Coin\rangle\,. \quad (3.6)$$

   Substituting $H \equiv 0$ and $V \equiv 1$, the verification state takes the GHZ-like form:

   $$|\,Ver\rangle = \frac{1}{\sqrt{2}}\left(|HH0\rangle_{a,b,b} + |VV1\rangle_{a,b,b}\right), \quad (3.7)$$

   $$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|HH0\rangle_{a,b,b} + |VV1\rangle_{a,b,b}\right), \quad (3.8)$$

   while the coin-flip state simplifies to the usual Bell state, since the spatial qubit is irrelevant for the coin-flip:

   $$|\,Coin\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle_{a,b} + |VV\rangle_{a,b}\right). \quad (3.9)$$

4. **Alice's Measurement on Verification Photon**

   Alice randomly selects a measurement basis for her polarization qubit, defined by the parameter r: Alice randomly selects a parameter $r \in \{0, 1\}$. The chosen basis is then

$$\begin{cases} x\text{-basis}, & \text{if } r = 0, \\ y\text{-basis}, & \text{if } r = 1. \end{cases}$$

   She implements the corresponding unitary operation $U_{a,r}$, which is realized by the corresponding waveplate settings and an additional PBS (as seen in Fig.3.2) and performs a polarization measurement. Her measurement outcomes are assigned as:

$$\begin{cases} a = 0, & \text{if detector } H \text{ clicks}, \\ a = 1, & \text{if detector } V \text{ clicks}. \end{cases}$$

   Alice then communicates her basis choice r and outcome a to Bob.

5. **Bob's Measurement on Verification Photon**

   Upon receiving Alice's message, Bob chooses two basis indices $s, t \in \{0, 1\}$ that satisfy

$$r \oplus s \oplus t = 0.$$

   Similar to Alice, the parameter s specifies Bob's polarization measurement basis, and t specifies the spatial-mode basis. Bob applies the corresponding unitaries:

   - $U_{b,s}$ — polarization rotation (implemented by waveplates),
   - $U_{b,t}$ — phase shift on mode 1 before the BS, with

$$U_{b,t} = \begin{cases} \text{phase shift } \theta = 0, & \text{if } t = 0, \\ \text{phase shift } \theta = \pi/2, & \text{if } t = 1. \end{cases}$$

   Bob's measurement outcomes are mapped as:

$$\begin{cases} \text{when detector } H0 \text{ clicks:} & b = 0,\ c = 0, \\ \text{when detector } V0 \text{ clicks:} & b = 1,\ c = 0, \\ \text{when detector } H1 \text{ clicks:} & b = 0,\ c = 1, \\ \text{when detector } V1 \text{ clicks:} & b = 1,\ c = 1. \end{cases}$$

   The protocol's integrity is verified if

$$a \oplus b \oplus c = r \vee s \vee t;$$

   otherwise, Bob aborts the protocol.

6. **Coin-Flip Outcome**

   If the verification succeeds, Alice and Bob proceed to measure their $|Coin\rangle$ photons in the polarization basis. If the result is H, then Alice wins the coin-flip, otherwise Bob wins the coin-flip. An example of the full setup is illustrated schematically in Fig. 3.2.

Discussion

It is evident that when both parties act honestly, measurements on the state $|Coin\rangle$ yield identical outcomes for Alice and Bob. Each party therefore has a 50% chance of winning the coin flip, ensuring that the protocol is balanced.

Furthermore, if both parties follow the protocol steps, the measurement on $|Ver\rangle$ guarantees a successful verification with certainty, as discussed earlier in relation to the GHZ game. To understand this, let us look at how the verification state $|Ver\rangle$ evolves when both participants act honestly throughout the protocol.

When Alice generates a Bell state $|\Phi^+\rangle$ and sends one of the photons to Bob, the state can be expressed as

$$|Ver\rangle = \tfrac{1}{\sqrt{2}}\big(a_H^\dagger b_H^\dagger + a_V^\dagger b_V^\dagger\big)\,|00\rangle\,. \tag{3.10}$$

For simplicity, the vacuum state notation $|00\rangle$ will be omitted in the following expressions, but it is always implicitly assumed.

When Bob sends his photon through a PBS, applies a local phase shift, and then recombines the paths at a BS, the state evolves as follows:

$$\begin{aligned}
|Ver\rangle &= \tfrac{1}{\sqrt{2}}\big(a_H^\dagger b_{H0}^\dagger + a_V^\dagger b_{V1}^\dagger\big) \quad \text{(PBS)} \\
&= \tfrac{1}{\sqrt{2}}\big(a_H^\dagger b_{H0}^\dagger + e^{i\phi}\, a_V^\dagger b_{V1}^\dagger\big) \quad \text{(Phase)} \\
&= \tfrac{1}{\sqrt{2}}\big(a_H^\dagger b_{H0}^\dagger + a_H^\dagger b_{H1}^\dagger + e^{i\phi} a_V^\dagger b_{V0}^\dagger - e^{i\phi} a_V^\dagger b_{V1}^\dagger\big) \quad \text{(BS)}
\end{aligned} \tag{3.11}$$

Assume that Alice obtains $r = 1$ and measures in the Y basis, while Bob chooses $s = 0$ and $t = 1$, measuring in the X and Y bases, respectively. The resulting state can be written as

$$\begin{aligned}
|\Psi\rangle = \tfrac{1}{4}\Big[&\big(a_H^\dagger b_{H0}^\dagger + a_H^\dagger b_{V0}^\dagger + a_V^\dagger b_{H0}^\dagger + a_V^\dagger b_{V0}^\dagger\big) \\
&+ \big(a_H^\dagger b_{H1}^\dagger + a_H^\dagger b_{V1}^\dagger + a_V^\dagger b_{H1}^\dagger + a_V^\dagger b_{V1}^\dagger\big) \\
&- \big(a_H^\dagger b_{H0}^\dagger - a_H^\dagger b_{V0}^\dagger - a_V^\dagger b_{H0}^\dagger + a_V^\dagger b_{V0}^\dagger\big) \\
&+ \big(a_H^\dagger b_{H1}^\dagger - a_H^\dagger b_{V1}^\dagger - a_V^\dagger b_{H1}^\dagger + a_V^\dagger b_{V1}^\dagger\big)\Big] \\
= \tfrac{1}{2}\Big[&a_H^\dagger\big(b_{V0}^\dagger + b_{H1}^\dagger\big) + a_V^\dagger\big(b_{H0}^\dagger + b_{V1}^\dagger\big)\Big] \\
= \tfrac{1}{2}\Big(&|010\rangle + |001\rangle + |100\rangle + |111\rangle\Big).
\end{aligned} \tag{3.12}$$

Regardless of which of the four states is obtained, they all satisfy

$$a \oplus b \oplus c = r \vee s \vee t = 1.$$

Similarly, the same relation holds for other combinations of r, s, and t.

Of course, this protocol works perfectly only when both parties follow strictly to the protocol steps. In practice however, a dishonest party might attempt to cheat in order to increase their chance of winning the coin-flip. Intuitively, since Alice is responsible for generating and distributing the quantum states, she could attempt to send two copies of the state $|HH\rangle$ to Bob. This strategy would always ensure her victory in the coin-flip round, but it carries a risk: such a state would pass the verification round with only a 50% probability, and she could be caught cheating and the protocol aborts.

Conversely, a dishonest Bob could ignore the verification round entirely and instead send both photons directly to the coin-flip measurement. In doing so, he would obtain two coin-flip outcomes and could then declare the outcome in which he loses as the verification state. This manipulation would allow Bob to increase his chances of winning.

The security proofs based on semidefinite programs (SDPs), which upper-bound the maximum winning probability of a dishonest party in this protocol, are presented in the Appendix. Nevertheless, a significant limitation of this protocol is its lack of loss tolerance. Specifically, the loss of either the coin-flip state or the verification state results in an abort of the protocol.

In principle, this issue can be mitigated by Alice sending multiple copies of the states. However, doing so introduces vulnerabilities to multi-photon attacks. Consequently, despite the upper bounds established by the security proofs, increasing the number of states compromises the security assumptions of the protocol. This directly motivates the derivation of a new loss-tolerant weak coin-flipping protocol, which will be introduced in the next subchapter.

3.4. Loss-tolerant weak coin-flipping protocol

The loss-tolerant weak coin-flipping protocol is divided into 3 phases, the initial phase, the reveal phase and the result phase. The same optical setup as in figure 3.2 is used for this protocol.

3.4.1. Protocol

Initial Phase:

1. For each $n \in \{0, 1\}$, Alice prepares a copy of the state

$$|\mathrm{GHZ}^{(\mathrm{n})}\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{AB_1B_2} + |111\rangle_{AB_1B_2})$$

   on $\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$, keeps system A and forwards systems B_1 and B_2 to Bob.

2. Alice samples $k_A \in_R \{0, 1\}$:

- If $k_A = 0$, she measures system A of $|\text{GHZ}^{(0)}\rangle$ in the Z basis and system A of $|\text{GHZ}^{(1)}\rangle$ in the Y basis.
- If $k_A = 1$, she measures system A of $|\text{GHZ}^{(0)}\rangle$ in the Y basis and system A of $|\text{GHZ}^{(1)}\rangle$ in the Z basis.

She stores her measurement outcome in the Z basis as $m_c^{(A)}$ (where c denotes the *coin-flip round* outcome) and the outcome in the Y basis as $m_v^{(A)}$ (where v denotes the *verification round* outcome). We use the terms *coin-flip* and *verification* to remain consistent with the setup introduced in Fig. 3.2 for the non-loss-tolerant protocol.

The **actual coin flip result** depends solely on the choices of k_A and k_B, which will be shown in the **Result Phase**.

3. Bob samples $k_B \in_R \{0, 1\}$:
   - If $k_B = 0$, he measures systems (B_1, B_2) of $|\text{GHZ}^{(0)}\rangle$ in the $Z \otimes Z$ basis and systems (B_1, B_2) of $|\text{GHZ}^{(1)}\rangle$ in the $X \otimes Y$ basis.
   - If $k_B = 1$, he measures systems (B_1, B_2) of $|\text{GHZ}^{(0)}\rangle$ in the $X \otimes Y$ basis and systems (B_1, B_2) of $|\text{GHZ}^{(1)}\rangle$ in the $Z \otimes Z$ basis.

   He stores his measurement outcomes for the $Z \otimes Z$ basis as $\left(m_{c,1}^{(B)}, m_{c,2}^{(B)}\right)$ and the one for the $X \otimes Y$ basis as $\left(m_{v,1}^{(B)}, m_{v,2}^{(B)}\right)$.

Reveal phase:

1. Alice sends $s = m_c^{(A)} \oplus m_v^{(A)}$ to Bob.
2. Bob sends k_B to Alice.
3. Alice sends k_A to Bob.

Result phase:

1. Both parties compute and verify the protocol outcomes in the following way:
   - If $k_A = k_B$, Alice sends $m_c^{(A)}$ and $m_v^{(A)}$ to Bob. He verifies that:
     - $m_c^{(A)} = m_c^{(B)}$,
     - $m_v^{(A)} \oplus m_{v,1}^{(B)} \oplus m_{v,2}^{(B)} = 1$,
     - $m_c^{(A)} \oplus m_v^{(A)} = s$.

     If all of the above hold, he declares Alice the winner; otherwise, he aborts.
   - If $k_A \neq k_B$, Alice declares Bob the winner.

This protocol is *loss-tolerant* because both Alice and Bob may independently perform multiple measurements during the initial phase and locally store all detection outcomes. In the subsequent reveal phase, the parties each post-select a pair of photon states for which they both have registered valid detection events, and only their basis choices k are used to determine the result of the coin flip. Consequently, photon loss does not force an abort of the protocol, but merely reduces the number of usable pairs of photon states.

The security of the protocol is rooted in the non-classical correlations of the GHZ game, with the winning condition depending explicitly on the basis choices k_A and k_B. In particular, Alice is declared the winner only if $k_A = k_B$ and the corresponding measurement outcomes satisfy the GHZ parity constraints. When the basis choices are aligned, the structure of the GHZ correlations ensures that Bob's measurement results are statistically consistent with Alice's declared outcomes, whereas any deviation from honest behaviour leads to a violation of these constraints with a non-zero probability.

In the reveal phase, Bob therefore possesses sufficient information to verify Alice's announced basis choice and measurement outcomes. Since Bob has already measured his subsystems in the corresponding bases and stored the results, he can directly check whether Alice's declarations are compatible with the expected correlations. This verification step is crucial for the security of the protocol, as it prevents Alice from falsely claiming a winning outcome by misreporting her basis choice or measurement results.

4. Security Proof

At the time the loss-tolerant protocol was developed, I joined the experimental team and began implementing the experimental part of this project. The security proof was developed by my colleague Rebecca Hofer. In this chapter, I briefly summarize her work on the security proof of the ideal protocol and explain the intuition behind it.

4.1. Theorems and Definitions

In this section, we list out definitions and theorems taken from [GW07] that describes *quanntum strategies*, which will be used for the security proof.

Definition 1 *Let $n \geq 1$ and $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces. An n-turn measuring **strategy** having input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ consists of:*

1. *Complex Euclidean spaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_n$, which will be called memory spaces.*
2. *An n-tuple of admissible mappings $(\Phi_1, \ldots, \Phi_n)$ having the form*

$$\begin{aligned} \Phi_1 &: \mathcal{L}(\mathcal{X}_1) \to \mathcal{L}(\mathcal{Y}_1 \otimes \mathcal{Z}_1) \\ \Phi_k &: \mathcal{L}(\mathcal{X}_k \otimes \mathcal{Z}_{k-1}) \to \mathcal{L}(\mathcal{Y}_k \otimes \mathcal{Z}_k) \quad (2 \leq k \leq n). \end{aligned}$$

3. *A measurement $\{P_a : a \in \sum\}$ on the last memory space $\mathcal{Z}_n$*

Definition 2 *Let $n \geq 1$ and $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces. An n-turn measuring **co-strategy** having input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ consists of:*

1. *Complex Euclidean spaces $\mathcal{W}_0, \ldots, \mathcal{W}_n$, which will be called memory spaces.*
2. *A density operator $\rho_0 \in \mathcal{X}_1 \otimes \mathcal{W}_0$.*
3. *An n-tuple of admissible mappings $(\Psi_1, \ldots, \Psi_n)$ having the form*

$$\begin{aligned} &\Psi_k : \mathcal{L}(\mathcal{Y}_k \otimes \mathcal{W}_{k-1}) \to \mathcal{L}(\mathcal{X}_{k+1} \otimes \mathcal{W}_k) \qquad (1 \leq k \leq n-1) \\ &\Psi_n : \mathcal{L}(\mathcal{Y}_n \otimes \mathcal{W}_{n-1}) \to \mathcal{L}(\mathcal{W}_n) \end{aligned}$$

4. *A measurement $\{Q_b : b \in \Gamma\}$ on the last memory space $\mathcal{W}_n$*

Definition 3 *A sequence of admissible super-operators* $(\Phi_1, \ldots, \Phi_n)$ *can be expressed as a single admissible super-operator*

$$\Xi : \mathcal{L}(\mathcal{X}_1 \otimes \mathcal{X}_2 ... \otimes \mathcal{X}_n) \to \mathcal{L}(\mathcal{Y}_1 \otimes \mathcal{Y}_2 ... \otimes \mathcal{Y}_n).$$

The Choi-Jamiolkowski representation of the strategy described by $(\Phi_1, \ldots, \Phi_n)$ *is then defined as the Choi-matrix* $J(\Xi)$ *of the super-operator* Ξ*.*

Theorem 1 *Without any loss of generality, the admissible mappings* $(\Phi_1, \ldots, \Phi_n)$ *of Definition 1 can be written as* $\Phi_k(X) = A_k X A_k^*$ *for* $1 \leq k \leq n$*, where* $(A_1, \ldots, A_n)$ *is a tuple of linear isometries.*

Theorem 2 *The Choi-Jamiolkowski representation of the n-turn strategy excluding the measurement step is given by* $Tr_{\mathcal{Z}_n}(vec(A)vec(A)^*)$*, where* $A \in \mathcal{L}(\mathcal{X}_1 \otimes ... \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes ... \otimes \mathcal{Y}_n \otimes \mathcal{Z}_n)$ *is defined by the product*

$$A = (\mathbb{1}_{\mathcal{Y}_{1...n-1}} \otimes A_n)(\mathbb{1}_{\mathcal{Y}_{1...n-2}} \otimes A_{n-1} \otimes \mathbb{1}_{\mathcal{X}_n}) \ldots (A_1 \otimes \mathbb{1}_{\mathcal{X}_{2...n}}).$$

The map

$$\mathrm{vec}(|i\rangle\langle j|) = |i\rangle \otimes |j\rangle$$

is a standard reshaping of matrices to vectors, it is used to compactly express Choi matrices as

$$J(\Xi) = \mathrm{vec}(A)\,\mathrm{vec}(A)^*$$

Theorem 3 *The Choi-Jamiolkowski representation of the n-turn strategy including the measurement step is given by* $\{Q_a : a \in \Sigma\}$ *for* $Q_a = Tr_{\mathcal{Z}_n}(vec(B_a)vec(B_a)^*)$ *where*

$$B_a = (\sqrt{P_a} \otimes \mathbb{1}_{\mathcal{Y}_{1...n}})A$$

for A *as defined above.* P_a *describes some finite, non-empty set* Σ *of measurement outcomes.*

Theorem 4 *A positive operator*

$$Q \in S_n(\mathcal{X}_{1...n}, \mathcal{Y}_{1...n})$$

corresponds to some valid n-turn strategy S_n *if and only if it satisfies*

$$Tr_{\mathcal{Y}_n}(Q) = R \otimes \mathbb{1}_{\mathcal{X}_n}$$

for $R \in S_{n-1}(\mathcal{X}_{1...n-1}, \mathcal{Y}_{1...n-1})$ *itself being a valid* $(n-1)$*-turn strategy.*

Theorem 5 *Similarly, an operator*

$$Q \in co\text{-}S_n(\mathcal{X}_{1...n}, \mathcal{Y}_{1...n})$$

corresponds to a co-strategy co-S_n iff:

$$Q = R \otimes \mathbb{1}_{\mathcal{Y}_n}$$

for $R \in Pos(\mathcal{Y}_{1\ldots n-1} \otimes \mathcal{X}_{1\ldots n-1})$ *satisfying:*

$$Tr_{\mathcal{X}_n}(R) \in \text{co-}S_{n-1}(\mathcal{X}_{1\ldots n-1}, \mathcal{Y}_{1\ldots n-1})$$

Theorem 6 *Let $n \geq 1$, let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be complex Euclidean spaces, and let $\{Q_a : a \in \Sigma\}$ represent an n-turn measuring strategy with input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. Then, for each $a \in \Sigma$, the maximum probability with which this strategy can be forced to output a, maximized over all choices of compatible co-strategies, is given by*

$$min\{p \in [0,1] : Q_a \leq pR \text{ for some } R \in S_n(\mathcal{X}_{1\ldots n}, \mathcal{Y}_{1\ldots n})\}.$$

(Maybe this part is too technical for the thesis?)

4.2. Security against Dishonest Alice

We now analyze the security of the protocol against a dishonest Alice who attempts to bias the outcome of the coin flip in her favor. Alice's objective is to force an honest Bob to declare her as the winner with maximum probability.

The interaction is modeled as a two-turn quantum interaction, where Bob follows the honest protocol and Alice is allowed to deviate arbitrarily within the laws of quantum mechanics. Alice's optimal cheating probability is given by the maximum value of an SDP defined by Bob's honest strategy.

During the initial phase, the steps of Bob's honest strategy may be represented using the isometry

$$\begin{aligned} &A_1 : \mathcal{X}_1 \to \mathcal{Y}_1 \otimes \mathcal{Z}_1, \\ &A_1 = \frac{1}{\sqrt{2}} \sum_{k_B=0}^{1} \sum_{m \in M_{k_B}} |k_B\rangle_{\mathcal{Y}_1} \otimes |k_B, f(m)\rangle_{\mathcal{Z}_1} \otimes \langle m|_{\mathcal{X}_1}, \end{aligned} \tag{4.1}$$

where the sets M_{k_B} is the sets of all possible measurement outcomes for that choice of basis k_B, and $|k_B, f(m)\rangle_{\mathcal{Z}_1}$ is the stored classical outcomes.

Next in the reveal phase, Bob receives Alice's bit $k_A \in \{0,1\}$ and her claimed measurement outcomes $m_c^{(A)}$ and $m_v^{(A)}$ on $\mathcal{X}_2$. Since Alice is dishonest, we can always assume that $k_A = k_B$ as this is her winning condition, and Bob only stores $m_c^{(A)}$ and $m_v^{(A)}$ in an output register $\mathcal{Z}_2$. He copies the bits of $\mathcal{Z}_1$ into the memory register $\mathcal{Z}_2$ and leaves an empty register $\emptyset$ on $\mathcal{Y}_2$.

The isometry A_2 which captures this step can be written as

$$A_2 : \mathcal{X}_2 \otimes \mathcal{Z}_1 \to \mathcal{Y}_2 \otimes \mathcal{Z}_2,$$
$$A_2 = \sum_{k_B=0}^{1} \sum_{m \in M_{k_B}} \sum_{m_c^{(A)}, m_v^{(A)}=0}^{1} |\emptyset\rangle_{\mathcal{Y}_2} \otimes |m_c^{(A)} m_v^{(A)} k_B f(m)\rangle_{\mathcal{Z}_2} \otimes \langle k_B f(m)|_{\mathcal{Z}_1} \otimes \langle m_c^{(A)} m_v^{(A)}|_{\mathcal{X}_2}. \tag{4.2}$$

We may then derive the operator A from the Choi representation of Theorem 2 as

$$\begin{aligned} A =& (\mathbb{1}_{\mathcal{Y}_1} \otimes A_2 \otimes \mathbb{1}_{\mathcal{X}_3})(A_1 \otimes \mathbb{1}_{\mathcal{X}_2 \mathcal{X}_3}) \\ =& \frac{1}{\sqrt{2}} \sum_{k_B=0}^{1} \sum_{m_c^{(A)}, m_v^{(A)}=0}^{1} \sum_{m \in M_{k_B}} |\emptyset\rangle_{\mathcal{Y}_2} \otimes |k_B\rangle_{\mathcal{Y}_1} \otimes |m_c^{(A)} m_v^{(A)} k_B f(m)\rangle_{\mathcal{Z}_2} \otimes \langle m_c^{(A)} m_v^{(A)}|_{\mathcal{X}_2} \otimes \langle m|_{\mathcal{X}_1} \otimes \mathbb{1}_{\mathcal{X}_3} \end{aligned} \tag{4.3}$$

In the honest protocol, Bob receives two quantum systems prepared by Alice and chooses a basis bit $k_B \in \{0, 1\}$. Depending on this choice, he measures the systems in either the Z or Y basis and records outcomes $(m_{c,1}^{(B)}, m_{c,2}^{(B)}, m_{v,1}^{(B)}, m_{v,2}^{(B)})$. Bob accepts Alice as the winner if and only if the reported classical values and measurement outcomes satisfy the GHZ winning conditions, which include agreement of the basis choices and a parity constraint on the measurement outcomes.

These acceptance conditions define a projector Π onto a set of valid outcome strings. The corresponding measurement operator Q_a fully characterizes Bob's honest strategy:

$$\begin{aligned} Q_a &= \mathrm{Tr}_{\mathcal{Z}_2}[\mathrm{vec}(B_a)\,\mathrm{vec}(B_a)^*] \\ &= \frac{1}{\sqrt{2}} \sum_{\substack{k_B, m_c^{(A)}, m_v^{(A)}, \\ m \in W}} |\emptyset\rangle\langle\emptyset|_{\mathcal{Y}_2} \otimes |k_B\rangle\langle k_B|_{\mathcal{Y}_1} \\ &\qquad \otimes |m_c^{(A)}\, m_v^{(A)}\rangle\langle m_c^{(A)}\, m_v^{(A)}|_{\mathcal{X}_2} \otimes |m\rangle\langle m|_{\mathcal{X}_1} \otimes \mathbb{1}_{\mathcal{X}_3}. \end{aligned} \tag{4.4}$$

Now we can use Theorems 4 and 6 to derive the maximum probability dishonest Alice can force honest Bob to output her as the winner, described by the following SDP:

$$\begin{aligned} \text{minimize} \quad & p \\ \text{subject to} \quad & \mathrm{Tr}_{\mathcal{Y}_1}(R_1) = p\,\mathbb{1}_{\mathcal{X}_1}, \qquad R_1 \in \mathrm{Pos}(\mathcal{X}_1 \otimes \mathcal{Y}_1), \\ & \mathrm{Tr}_{\mathcal{Y}_2}(R_2) = R_1 \otimes \mathbb{1}_{\mathcal{X}_2}, \qquad R_2 \in \mathrm{Pos}(\mathcal{X}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2), \\ & Q_a \leq R_2. \end{aligned} \tag{4.5}$$

which gives $p = 0.8535$ as the maximum cheating probability for Alice. (R_1, R_2) represents valid co-strategies in the two rounds. The partial trace constraints enforce that Alice's actions in later rounds cannot affect earlier messages.

Intuitively, Alice's cheating advantage stems from her ability to prepare entangled states that partially correlate with both of Bob's possible basis choices. However, the GHZ

winning conditions impose incompatible constraints across the two bases. Any strategy that improves Alice's success probability for one basis would necessarily downgrade her success probability in the other, preventing perfect cheating.

4.3. Security against Dishonest Bob

We now analyze the security of the protocol against a dishonest Bob, whose objective is to force the honest co-strategy of Alice to declare him as the winner with maximum probability. Similarly, the interaction between Alice and Bob can be modeled as a two-turn quantum interaction, where Alice sends a quantum system to Bob in the first round, Bob responds with a classical guess bit, and Alice performs a final measurement to announce the outcome. Bob's optimal cheating probability can given by the maximum value of a SDP defined by Alice's honest co-strategy.

In the honest protocol, Alice prepares two GHZ states and secretly chooses a basis bit $k_A \in \{0,1\}$. Depending on k_A, she measures one qubit in the Z basis and the other in the Y basis, obtaining outcomes $m_c^{(A)}$ and $m_v^{(A)}$. Bob receives state together with the classical bit $s = m_c^{(A)} \oplus m_v^{(A)}$.

The quantum states that Bob observes depend on Alice's hidden basis choice. When Alice measures in the Z basis, Bob observes computational basis states $|00\rangle$ or $|11\rangle$. When Alice measures in the Y basis, Bob observes superposition states $(|00\rangle \pm |11\rangle)/\sqrt{2}$. It is apparent that Bob cannot perfectly determine Alice's basis choice.

Alice declares Bob as the winner if Bob's announced guess bit l differs from her basis choice k_A. This acceptance condition defines a measurement operator Q_b, which fully characterizes Alice's honest co-strategy and is given by:

$$Q_b = \frac{1}{8} \sum_{k,m_1,m_2 \in \{0,1\}^3} |\phi_{m_1}^{B(k)}\rangle\langle\phi_{m_1}^{B(k)}|_{\mathcal{X}_1} \otimes |\phi_{m_1}^{B(k-1)}\rangle\langle\phi_{m_1}^{B(k-1)}|_{\mathcal{X}_1} \otimes |p\rangle\langle p|_{\mathcal{X}_1} \otimes |k\rangle\langle k|_{\mathcal{Y}_1} \tag{4.6}$$

Bob's maximum cheating probability is obtained by optimizing over all admissible strategies compatible with the protocol. By Theorem 6, this optimization reduces to an SDP whose optimal value upper-bounds Bob's success probability, and it is given by:

$$\begin{aligned} \text{minimize} \quad & p \\ \text{subject to} \quad & Q_b \leq pR_n \\ & R_n = P_n \otimes \mathbb{1}_{\mathcal{Y}_n} \qquad \text{for} \quad 1 \leq k \leq n \\ & \mathrm{Tr}_{\mathcal{X}_n}(P_n) = R_{n-1} \\ & \cdots \\ & R_0 = 1 \end{aligned} \tag{4.7}$$

The upper bound for Bob's maximal cheating probability is 0.75. The result of the SDP can be understood quite intuitively. By measuring the received quantum systems in

the computational basis, Bob can implement a strategy that reliably distinguishes Alice's Z-basis preparation whenever a conclusive outcome occurs. Such outcomes arise with probability $1/2$, corresponding to cases in which Alice measured in the Z basis, allowing Bob to deterministically choose his guess bit to win. In the remaining cases, corresponding to Alice's Y-basis measurements, the resulting quantum states yield indistinguishable measurement statistics in the computational basis. As a consequence, Bob gains no deterministic information about Alice's basis choice and is forced to guess randomly. Combining these contributions, Bob's overall winning probability is

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = 0.75$$

5. SPDC Single-Photon Source

In this experiment, we use a type-II SPDC source to generate pairs of entangled photons. The theoretical background of SPDC is already introduced in Chapter 2.4.3; this chapter focuses on the experimental setup, alignment procedure, and performance of the SPDC source used in our measurements.

We use a 30 mm-long PPKTP crystal manufactured by Raicol Crystals. The crystal is placed inside a Sagnac interferometer and pumped by a cw-laser at a wavelength of 775 nm. Through type-II SPDC, the crystal generates pairs of signal and idler photons at a wavelength of 1550 nm.

5.1. Sagnac interferometer

An SPDC single photon source generates pairs of single photons, however, in this experiment, one requires pairs of entangled photons. This chapter introduces how a Sagnac interferometer can be used to generate entangled photons.

A Sagnac interferometer can be understood as a Mach–Zehnder interferometer in a triangular configuration. Figure 5.1 shows a simple schematic of the experimental setup.

The pump photon first passes through a focusing lens whose focal point is positioned at the center of the PPKTP crystal. It then propagates through the dichroic mirror and reaches the PBS.

The polarization of the pump photon is prepared in the diagonal basis. As a result, the horizontally polarized component of the pump propagates clockwise within the Sagnac loop, while the vertically polarized component propagates in the counterclockwise direction. In the clockwise path, the pump photon reaches the crystal, where it undergoes type-II down-conversion, producing two photons with orthogonal polarizations. These photons then pass through a HWP set at 45° and return to the PBS. At the PBS, the horizontally polarized photon is transmitted and collected by a lens in one output arm, while the vertically polarized photon is reflected by the PBS, then by the dichroic mirror, and finally collected by a lens in the other output arm.

Similarly, in the counterclockwise path, the vertically polarized pump photon first passes through the HWP, which rotates its polarization to the horizontal basis. The pump photon then reaches the crystal and undergoes type-II down-conversion, again producing two photons with orthogonal polarizations. Upon returning to the PBS, the horizontally polarized photon is transmitted through the PBS, reflected by the dichroic mirror, and collected by a lens in one output arm, while the vertically polarized photon is reflected by the PBS and collected by a lens in the other output arm.

It may not be immediately apparent why an additional HWP is required inside the

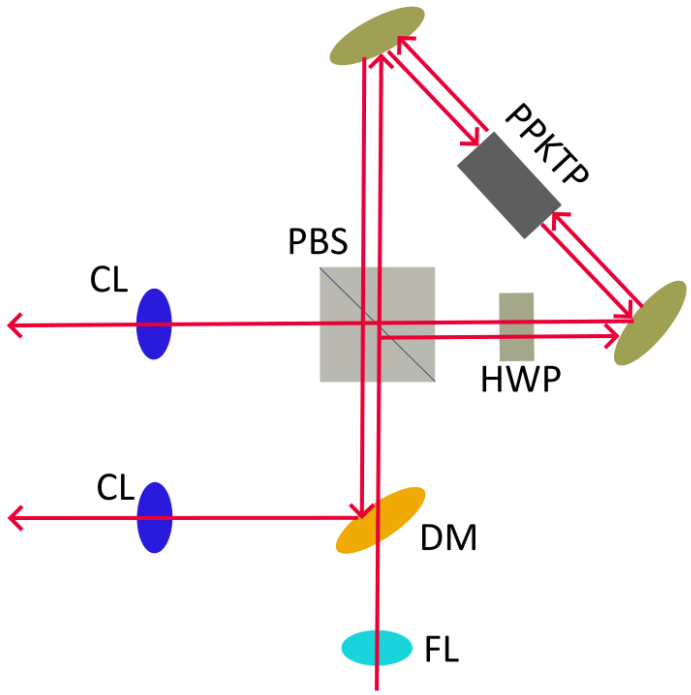


Figure 5.1.: Sagnac loop designed to generate two single photons entangled in polarization basis, DM = dichroic mirror (transmit light at 775 nm and reflects light at 1550 nm), CL = collecting lens, FL = focusing lens

Sagnac loop; however, it plays an important role in the overall setup. By rotating the polarization of both the pump and the down-converted photons, the HWP erases the path information and makes the clockwise and counterclockwise processes indistinguishable in polarization at the output ports. This indistinguishability is essential for coherent interference between the two paths and, consequently, for the generation of high-quality polarization-entangled photon pairs. In addition, the HWP makes sure that the nonlinear crystal experiences the same pump polarization for both propagation directions. As a result, only one phase-matching condition is required (e.g., $H \rightarrow HV$) for both the clockwise and counterclockwise directions. Without this polarization rotation, different phase-matching conditions would be needed for the two directions.

5.2. Aligning the Sagnac source

This subchapter serves as a simple and concise guide for aligning the Sagnac source. I would like to especially thank my colleague Yann for providing his expertise and guidance during the source alignment.

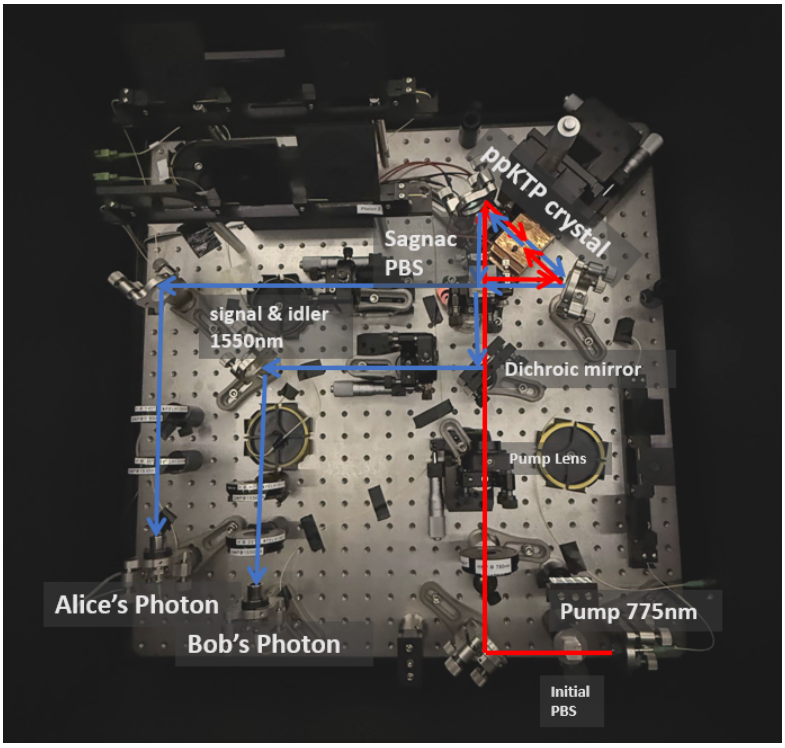


Figure 5.2.: Photograph of the single-photon source setup. The red line indicates the beam path of the pump beam at a wavelength of 775 nm, while the blue line indicates the beam paths of the down-converted photons at a wavelength of 1550 nm.

Before starting the alignment, all relevant optics should be placed on the optical table, and the area where the Sagnac loop will be located should be reserved. In addition, the position of the focusing lens should be approximately marked, such that its focal point is located at the center of the Sagnac loop. Finally, space should be reserved for the two collection arms, which consist of collection lenses, mirrors, collimators, sets of HWP and QWP to compensate fiber polarization and most importantly, 1550 nm bandpass filters. These two arms collect the single photons generated by the nonlinear crystal. Note that the oven housing the crystal is very bulky; therefore, sufficient space must be reserved on the optical table.

The setup is shown in figure 5.2.

5.2.1. Aligning the pump collimator

The alignment of the pump collimator is the first step in aligning the Sagnac source. It is crucial to ensure that the pump beam remains parallel throughout the entire setup. The procedure is carried out as follows:

1. Clamp the pump collimator onto the optical table.

2. Place two pinholes at the same height, one located close to the pump collimator and one located as far as possible. Adjust the collimator such that the beam passes through both pinholes, verifying that the beam is straight and parallel to the optical table.

3. Insert a PBS into the beam path of the pump collimator. Temporarily place a polarizer transmitting horizontally polarized light before the PBS. Fine-tune the orientation of the PBS to maximize the transmission through the transmission port. This step defines and purifies the pump polarization.

4. Insert a HWP between the polarizer and the PBS to characterize its zero angle. Remove the HWP and the polarizer after the characterization.

5. Use this initial PBS to set the polarization of the pump beam. In combination with a fiber polarization controller (fiber paddles), the PBS can also be used to adjust the input power of the pump beam.

6. Insert a mirror to redirect the pump beam toward the "Sagnac PBS". Perform beam walking with the mirror and the pump collimator to ensure that the pump beam remains parallel to the optical table.

7. Install the Sagnac PBS. As before, insert a polarizer transmitting horizontally polarized light and adjust the PBS orientation to achieve the best extinction ratio, defined as the ratio between the power of the transmitted light and the power of unwanted reflected light. Higher extinction ratios ensure the generation of entangled states with higher purity.

8. As before, characterize HWPs with the polarizer and the Sagnac PBS. These HWPs will be used later in the Sagnac interferometer.

9. Mount the focusing lens on a translation stage and position it such that its focal point is approximately located at the center of the Sagnac loop. Use a cross filter to ensure that the beam passes through the center of the lens, thereby minimizing chromatic aberration.

10. Adjust the tilt of the focusing lens and use a pinhole to verify that the focused beam remains parallel to the optical table.

11. Install the dichroic mirror and assemble the two collecting arms made of pairs of QWPs and HWPs together with collection collimators. Direct a laser at 1550 nm from the collection collimator and align the beam such that it overlaps with the pump beam path.

12. Verify that the pump beam remains parallel after passing through the Sagnac PBS. If necessary, readjust the mirror and the pump collimator.

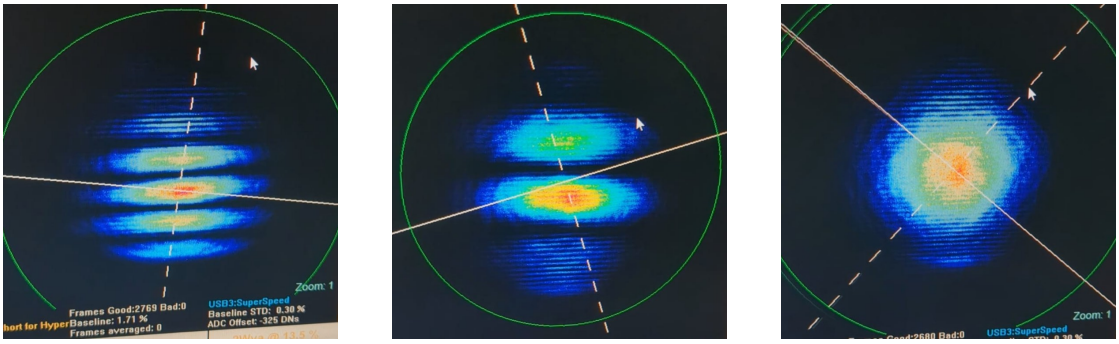
5.2.2. Aligning the Sagnac Interferometer

1. Place one pinhole on each output port of the Sagnac PBS and verify that the beams emerging from both ports are still parallel.

2. Install two dual-wavelength mirrors to complete the Sagnac loop. The angle of incidence should be 22.5° to create the triangular configuration.

3. Set the HWP before the focusing lens to 22.5° to set the pump polarization to $|D\rangle$. Adjust one mirror until the beam propagating in the clockwise direction passes through the pinhole on its return path. Then adjust the second mirror until the beam propagating in the counter-clockwise direction passes through the other pinhole. Iterate this procedure until both counter-propagating beams pass through their respective pinholes.

4. Remove the pinholes and replace them with HWPs, with one set to 0° and the other set to 45°. In contrary to 5.1, a second HWP is placed to compensate the optical axis mismatch between the Sagnac PBS and the non-linear crystal.



(a) Initial state showing interference fringes, indicating misalignment.

(b) Improved alignment, showing reduced interference fringes.

(c) Final state showing a single spot, alignment is complete

Figure 5.3.: Evolution of the interference patterns observed at the dark port of the PBS during the Sagnac alignment. Images from Yann Valibouse.

5. Place a beam profiler at the reflection port of the Sagnac PBS. Initially, interference fringes will be observed. Beam walk and fine-tune the mirrors to merge the interference pattern into a single spot. This step is illustrated in Fig. 5.3.

6. Use a Faraday isolator to perform self-back-alignment of the interferometer. A Faraday isolator consists of an input PBS, a Faraday rotator, and an output PBS oriented at 45° with respect to the input PBS. In the forward direction, the beam passes through the input PBS and is rotated by 45° in the Faraday rotator, allowing it to transmit through the output PBS with maximum efficiency. In contrast, the backward-propagating beam does not retrace the same polarization transformation;

after passing again through the Faraday rotator, its polarization is rotated by an additional 45° due to the non-reciprocal nature of the Faraday effect, such that it is reflected by the input PBS. This configuration allows direct observation of the retro-reflected beam. By iteratively adjusting the interferometer mirrors to maximize the power of the backward-propagating beam, precise self-alignment of the interferometer can be achieved.

7. Similarly, optimize the position of the focusing lens by translating it along the beam path while monitoring the power detected at the circulator. If necessary, repeat the previous step (see step 6) to further improve alignment.

8. Carefully insert the nonlinear crystal into the oven. Apply thermal paste to improve heat conductivity. Install a TEC element and a temperature sensor to enable precise temperature control of the oven. Finally, connect them to an evaluation board; in this experiment, we use the MTDEVAL1 from Thorlabs.

9. Place the oven at the center of the Sagnac interferometer. The oven is mounted on a stage that allows adjustment in the horizontal and vertical directions, as well as tilt. Adjust the oven position so that the beam passes straight through the crystal in both directions of the Sagnac loop.

5.2.3. Optimizing single photon counts and heralding efficiency

1. Install two collecting lenses, with their focal points approximately aligned to the collecting collimators. Reinsert pinholes into the Sagnac interferometer and check the alignment of the two collection arms by back-aligning with a 1550 nm laser.

2. Ensure that the bandpass filters are properly installed, and connect the collecting collimators to the single-photon detectors. The bandpass filters are crucial, as they prevent stray light from the pump beam from reaching the detectors. In this experiment, we use superconducting nanowire single-photon detectors (SNSPDs), which are highly sensitive single photon detectors capable of registering individual photons with high detection efficiency.

3. When everything is properly aligned, you should already observe single photon counts in both arms. Adjust the alignment of both collecting arms until the single photon counts reach the maximum.

4. By setting the correct coincidence window and delays, coincidence counts between the two single photons should be observed. If no coincidences are detected, troubleshoot by checking the alignment using Step 6 from the previous subchapter. If necessary, a beam profiler can also be placed at the reflection port of the initial PBS in the back-propagating direction. When the alignment is correct, a single spot should be observed, as shown in Fig. 5.3.

5. The heralding efficiency η can now be calculated, which is given by the ratio of the coincidence detections to the singles detections.

$$\eta = \frac{coincidences}{singles} \tag{5.1}$$

   Optimize alignment of the collecting arms to improve the heralding efficiency.

6. Adjust the positions of the collecting lenses to optimize the heralding efficiency. This step can be challenging, as changing the lens position may slightly misalign the corresponding collection arm. A practical approach is to start with a given lens position, optimize the alignment, and record the heralding efficiency. Repeat this procedure for several different lens positions. The resulting data should form a Gaussian-like curve when plotted, which can then be used to determine the optimal lens position for maximum heralding efficiency.

   At this stage, the source is ready for application. In our experiment, we aim to generate a $|\Phi^+\rangle$ state, whereas our source initially produces a $|\psi^-\rangle$ state. Therefore, we use waveplates and fiber paddles in combination to effectively rotate the produced state to the desired state $|\Phi^+\rangle$. To evaluate the quality of our source, we perform a quantum state tomography.

5.3. Quantum State Tomography

Quantum state tomography (QST) is a standard experimental technique used to reconstruct the full quantum state of a system from measurement data. Since a quantum state cannot be directly accessed in a single measurement, QST relies on performing a complete set of measurements on an ensemble of identically prepared systems and subsequently reconstructing the density matrix from the measured expectation values [AJK04].

To reconstruct the quantum state, one needs to determine the Stokes parameters. Any single-qubit density matrix $\hat{\rho}$ can be uniquely represented by the Stokes parameters $\{S_1, S_2, S_3\}$ as

$$\hat{\rho} = \frac{1}{2}\sum_{i=0}^{3} S_i \hat{\sigma}_i, \tag{5.2}$$

where $\hat{\sigma}_0 = I$ is the identity operator and $\hat{\sigma}_{1,2,3} = \{\sigma_x, \sigma_y, \sigma_z\}$ are the Pauli matrices.

The Stokes parameters are given by

$$S_1 = P_{|+\rangle} - P_{|-\rangle}, \tag{5.3}$$
$$S_2 = P_{|L\rangle} - P_{|R\rangle}, \tag{5.4}$$
$$S_3 = P_{|H\rangle} - P_{|V\rangle}, \tag{5.5}$$

where $P_{|\psi\rangle}$ denotes the probability of projecting the state onto $|\psi\rangle$.

In principle, the density matrix can therefore be fully reconstructed using measurements in the polarization bases $\{H, V, +, -, L, R\}$. However, since orthogonal projection probabilities satisfy the relation $P_{|\psi\rangle} - P_{|\psi^\perp\rangle} = 2P_{|\psi\rangle} - 1$, the number of required measurement settings can be reduced to four independent settings, for example $\{H, V, +, L\}$.

More generally, the density matrix of an n-qubit quantum state can be written as

$$\hat{\rho} = \frac{1}{2^n} \sum_{i_1,i_2,\ldots,i_n=0}^{3} S_{i_1,i_2,\ldots,i_n}\, \hat{\sigma}_{i_1} \otimes \hat{\sigma}_{i_2} \otimes \cdots \otimes \hat{\sigma}_{i_n}. \tag{5.6}$$

This representation involves 4^n Stokes parameters. In a standard overcomplete tomographic scheme, these parameters are obtained from 6^n measurement settings corresponding to projections onto the eigenstates of the Pauli operators. For a two-qubit system, this results in 16 Stokes parameters and 36 measurement settings. Since the density matrix has only $4^n - 1$ independent real parameters, an overcomplete set of 6^n measurements is not strictly necessary for state reconstruction [AJK04]. In general, it is beneficial to perform the overcomplete set of measurements, as it will reduce uncertainties when reconstructing the density matrix using maximum likelihood estimation.

In this experiment, two tomography stages and a total of four single-photon detectors are used to perform 36 measurement settings: $\{H, V, +, -, L, R\} \times \{H, V, +, -, L, R\}$; from which the two-qubit density matrix is reconstructed.

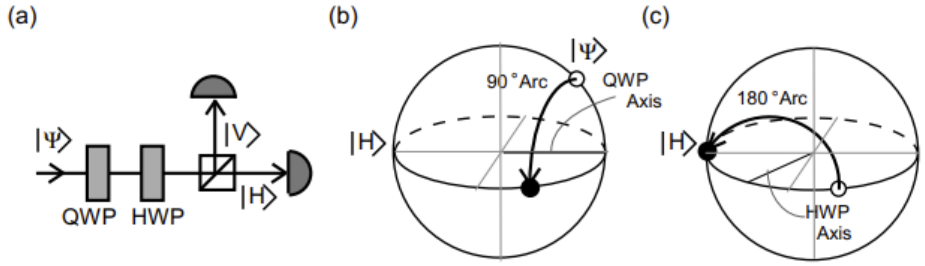


Figure 5.4.: (a) Tomography setup consisting of a QWP and HWP followed by a PBS, projecting an arbitrary input state $|\psi\rangle$ onto the $|H\rangle$ and $|V\rangle$ bases. (b) Representation on the Poincaré sphere of the transformation induced by the QWP, corresponding to a 90° rotation that maps $|\psi\rangle$ into the linear polarization plane. (c) Subsequent rotation by the HWP, completing the mapping to $|H\rangle$.[AJK04]

A tomography stage consists of a QWP, a HWP, and a PBS, followed by two single-photon detectors placed at the transmitted and reflected ports of the PBS. The unitary transformations implemented by the HWP and QWP are given by [Str23]:

$$U_{\mathrm{HWP}}(\theta) = e^{-i\pi/2} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}, \tag{5.7}$$

and

$$U_{\mathrm{QWP}}(\theta) = e^{-i\pi/4} \begin{pmatrix} \cos^2\theta + i\sin^2\theta & (1-i)\cos\theta\sin\theta \\ (1-i)\cos\theta\sin\theta & i\cos^2\theta + \sin^2\theta \end{pmatrix}. \tag{5.8}$$

To measure in the H/V basis, the angles of both waveplates are set to 0°. The PBS then separates the incoming polarization state into its $|H\rangle$ and $|V\rangle$ components, which are detected at the corresponding output ports.

Measurements in other polarization bases are performed by applying a unitary transformation that maps the desired measurement basis onto the H/V basis prior to the PBS. For example, to measure the positive eigenstate of σ_x, one applies a unitary transformation that maps $|+\rangle$ onto $|H\rangle$. The required waveplate angle settings for the different measurement bases are summarized in Table 5.1.

Table 5.1.: Waveplate angle settings for different measurement bases.

Basis	H/V	D/A	R/L
QWP	0°	45°	45°
HWP	0°	−22.5°	0°

5.3.1. Results

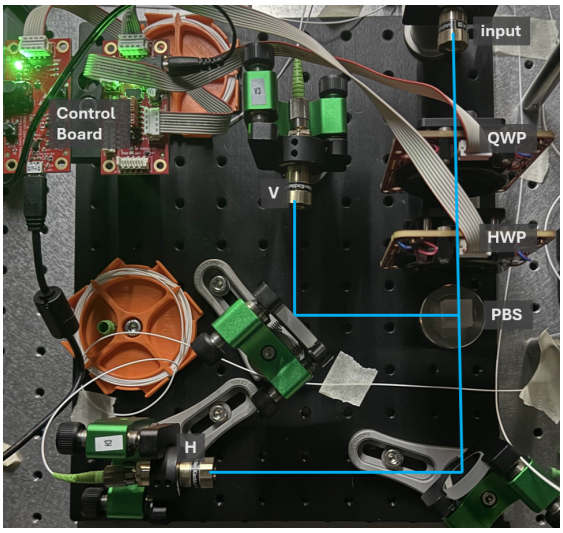


Figure 5.5.: Photograph of the tomography stage used in the experiment. The blue lines indicate the beam paths of the single photons. The waveplates are mounted on rotation mounts equipped with resonant piezoelectric motors from Thorlabs (ELL14). Using a control board and a bus distributor, the waveplate angles can be set remotely, allowing automated selection of the measurement basis. H and V indicates the output collimators which are connected to single photon detectors.

In the experiment, we use two tomography stages, as illustrated in Figure 5.5. The rotation mounts, equipped with resonant piezoelectric motors from Thorlabs, allow automated adjustment of the waveplate angles to the desired settings for each measurement basis.

Before performing the measurements, the polarization transformations introduced by the optical fibers must be compensated using fiber polarization controllers, together with the QWP and HWP placed in front of the collection collimators. [SSW24] Bending and stress in optical fibers generally introduce an unknown unitary transformation U_f on the photon polarization state. The goal of fiber polarization compensation is therefore to correct this unknown transformation such that the effective operation is the identity I.

Since the source is based on type-II SPDC, it initially generates a $|\psi\rangle$-type entangled state. In this experiment, however, the desired output state is $|\phi^+\rangle$. Consequently, the fiber polarization controllers and waveplates are adjusted such that the combined transformation effectively maps the generated $|\psi\rangle$ state onto the target $|\phi^+\rangle$ state.

To begin compensating the polarization transformations of the two fibers connecting the collection collimators to the tomography stages, both QWPs placed before the collection collimators are first set to 45°. The tomography stages are then configured to measure in the H/V basis. The fiber polarization controllers are adjusted to minimize the coincidence counts corresponding to the $|HV\rangle$ and $|VH\rangle$ outcomes, i.e., events where $|H\rangle$ is detected at the first tomography stage and $|V\rangle$ at the second, and vice versa. Once these coincidence counts are minimized in the H/V basis, the tomography stages are switched to the D/A basis. The HWPs placed before the collection collimators are then adjusted to again minimize the $|HV\rangle$ and $|VH\rangle$ coincidence counts. These two optimization steps are iterated until the $|HV\rangle$ and $|VH\rangle$ coincidences are simultaneously minimized in both measurement bases, and the source now effectively generates a $|\Phi^+\rangle$ state.

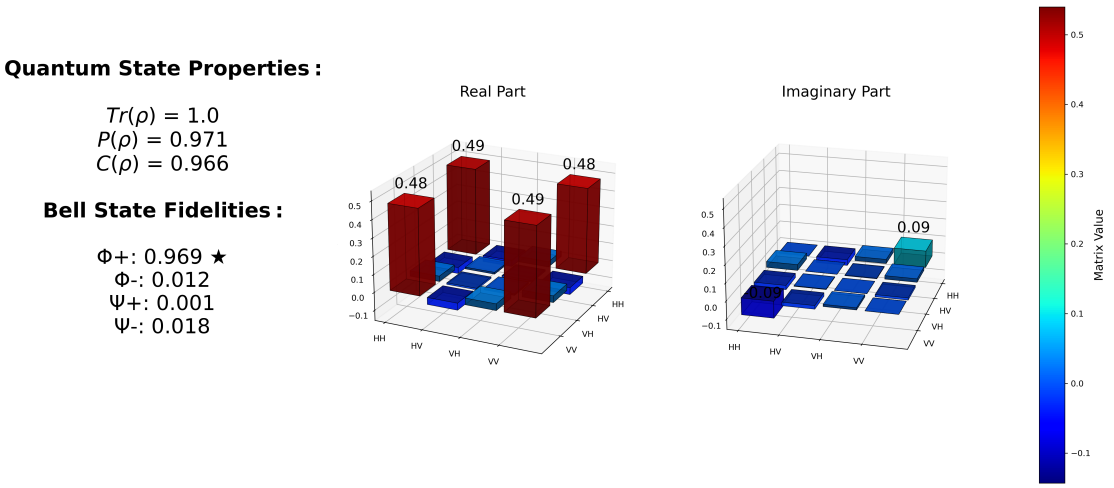


Figure 5.6.: Reconstructed density matrix of the entangled $|\Phi^+\rangle$ generated by the Sagnac source. Coincidence window was set at 2 ns

Coincidence counts between the two tomography stages are then recorded for all 36

measurement settings with an automated python script. The two-qubit density matrix is subsequently reconstructed using the maximum likelihood estimation (MLE) method provided by the Python Tomography Library [Kwi]. MLE is a statistical method that reconstructs the physical density matrix by finding the state that maximizes the probability of obtaining the experimentally obtained measurement data. The reconstructed density matrix can be found at figure 5.6.

From the reconstructed density matrix ρ, several quantities can be extracted to characterize the generated entangled state.

The *purity* is defined as $P(\rho) = \mathrm{Tr}(\rho^2)$ and quantifies the degree of mixedness of the state. It takes the value $P = 1$ for a pure state and $P = 1/d$ for a maximally mixed state in a d-dimensional Hilbert space.

The *fidelity* between the reconstructed state ρ and a target state σ is used as a measure of how closely the generated state matches the ideal theoretical state. In the general case, it is given by [AJK04]

$$F(\rho, \sigma) = \left[\mathrm{Tr} \left(\sqrt{\sqrt{\rho}\, \sigma \sqrt{\rho}} \right) \right]^2 . \tag{5.9}$$

The fidelity ranges from 0, indicating no overlap between the states, to 1, corresponding to perfect agreement between the reconstructed and target states. To quantify entanglement, the *concurrence* is evaluated. For two-qubit states, the concurrence is defined as

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{5.10}$$

where the λ_i are the square roots of the eigenvalues, in decreasing order, of the matrix

$$\hat{R} = \rho\, \hat{\Sigma}\, \rho^T\, \hat{\Sigma}, \tag{5.11}$$

with the superscript T denoting the matrix transpose. The spin-flip matrix $\hat{\Sigma}$ is defined as [AJK04]

$$\hat{\Sigma} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} . \tag{5.12}$$

The concurrence ranges from $C = 0$ for separable states to $C = 1$ for maximally entangled states, such as Bell states.

The final performance of the SPDC source is summarized below:

- Heralding efficiency: $\eta = (20.0 \pm 0.2)\%$.
- Purity: 97.1%
- Concurrence: 96.6%
- Fidelity with respect to $|\phi^+\rangle$: 96.6%

Overall, the QST result demonstrates high state purity and good state fidelity for the protocol. The concurrence of 96.6% indicates a high degree of entanglement, which is

crucial for low error rates in the protocol. Similarly, the fidelity of 96.6% with respect to the $|\phi^+\rangle$ state shows that the experimentally generated state closely approximates the desired state,.

The heralding efficiency of $\eta = (20.0 \pm 0.2)\%$ is mediocre and primarily limited by optical losses. While this does not directly translates into the loss of state quality, it impacts the overall data acquisition rate and increases the probability of loss events. This can be be improved by further alignment procedures.

6. Implementation of the Protocol

This chapter describes the implementation of the weak coin-flipping protocol, focusing on the setup and alignment of the Mach–Zehnder–type interferometer at Bob's lab. In addition, preliminary experimental results are presented at the level of statistical analysis.

The experimental setup is similar to the schematic shown in figure 3.2. Alice controls the SPDC source, keeps one photon, and sends it directly to a tomography stage, while the other photon is sent to Bob. Bob directs his photon into an interferometer to encode a spatial qubit with the polarization qubit in his photon. The two output paths of the beam splitter are then collected and forwarded to two tomography stages. Both Alice and Bob can use the tomography stages to choose the measurement basis. This can be done by remotely setting the waveplate angles to predetermined values using ELL14 rotation mounts at the tomography stages.

6.1. Setup of the interferometer

The Mach–Zehnder–type interferometer installed in Bob's lab is a crucial component for the experimental realization of the protocol. Since the source at Alice's lab generates only a Bell state, Bob's interferometer is used to extend this state into a 3-qubit $|\mathrm{GHZ}\rangle$ state.

Initially, Bob's photon carries only a polarization qubit that is entangled with Alice's photon. Upon entering the interferometer, the photon passes through a PBS, which separates the polarization components into two distinct spatial modes (paths). In this way, the polarization degree of freedom becomes correlated with the path degree of freedom. This technique is also known as *hyper-encoding*. This process effectively creates a second qubit — the spatial qubit — and entangles it with the polarization qubit of the same photon.

Precisely, if Bob's incoming photon is in a superposition $\alpha\,|H\rangle + \beta\,|V\rangle$, the PBS transforms the state into

$$\alpha\,|H\rangle\,|0\rangle + \beta\,|V\rangle\,|1\rangle\,,$$

where $|0\rangle$ and $|1\rangle$ denote the two spatial paths of the interferometer. The polarization and spatial degrees of freedom are now entangled. When combined with Alice's polarization qubit, this results in an effective three-qubit entangled state of the form required for the GHZ-game-based protocol. In other words, the spatial mode of Bob's photon acts as the third qubit in the GHZ state.

At the output of the interferometer, a final BS recombines the two spatial modes. By controlling the relative phase between the arms, Bob can choose the measurement basis of the spatial qubit. The interference at the BS therefore enables measurements in the spatial qubit, while the tomography stages allow measurements of the polarization qubit.

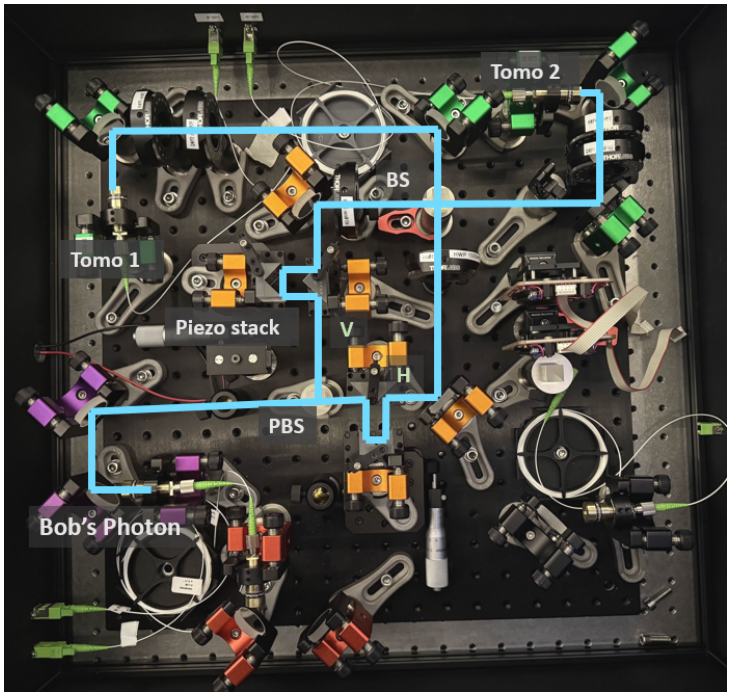


Figure 6.1.: Photograph of the interferometer at Bob's lab. Cyan lines indicate the beam paths. Phase shifts of the spatial qubit are implemented using a piezoelectric stack mounted on a translation stage, which controls the path-length difference between the two interferometer arms.

This joint control over polarization and path is what enables the realization of the GHZ correlations required for the verification step of the protocol.

As shown in Fig. 6.1, the interferometer begins with a PBS and is closed by a BS. Along the interferometer paths, knife-edge mirrors in combination with hollow retroreflector mirrors mounted on translation stages are used to create delay lines to match the optical path lengths of the two arms. In addition, a piezoelectric stack mounted on a translation stage is placed in the upper-left arm to control the path-length difference between the interferometer arms, thereby setting the relative phase and the measurement basis of the spatial qubit. The BS here acts as a measurement on the spatial qubit.

The two output arms after the BS are followed by a pair of QWP and HWP, and collection collimators, which are connected to two tomography stages. The QWP and HWP are used in combination with fiber polarization controllers to compensate for polarization changes introduced by the optical fibers. The collected photons are then forwarded to the two tomography stages and subsequently to single-photon detectors, allowing Bob to select his polarization measurement basis.

To verify proper alignment of the interferometer, classical light is first sent into the system and an HWP set to 45° is placed in one arm of the interferometer. Alignment procedures are then applied to make sure that the beam paths before and after the BS are

perfectly overlapped. Once approximate overlap is achieved, interference fringes become visible. Further fine-tuning of the alignment merges the fringes into a single bright spot at one output port of the BS, with a corresponding dark port at the other output. The quality of the interference is quantified by the visibility, which is given by the formula

$$V = \frac{N_{\max} - N_{\min}}{N_{\max} + N_{\min}},$$

where $N_{\max}$ and $N_{\min}$ denote the maximum and minimum detected intensities, respectively. Using a power meter at both output ports of the BS, an interference visibility of approximately 99% is obtained for classical light.

Since the coherence length of the SPDC single photons is much shorter (on the order of $\sim 1\,\mathrm{mm}$) than that of the classical laser light, the interferometer path-length difference requires further fine-tuning. The translation stage in one arm is adjusted carefully until single-photon interference is observed. The optimal position of the translation stage is then determined by maximizing the visibility of the single-photon interference. This directly influences the error rates of the GHZ-game.

A DC piezo controller is used to apply a fixed voltage to the piezoelectric stack, thereby stabilizing the interferometer phase. To further improve the overall stability of the interferometer, the entire setup is enclosed in a plastic box to reduce temperature drifts and air fluctuations. In addition, careful grounding of the control electronics are employed to suppress electrical noise.

Lastly, fiber polarization compensation is applied. First, the fibers connecting the interferometer to Bob's tomography stages are compensated such that their overall polarization transformation is effectively the identity. Similarly, the fiber connecting the source to Alice's tomography stage is compensated to implement an identity operation. Finally, the fiber connecting the source to Bob's interferometer is compensated such that the reconstructed state before the interferometer corresponds to a $|\phi^+\rangle$ Bell state.

6.2. Results

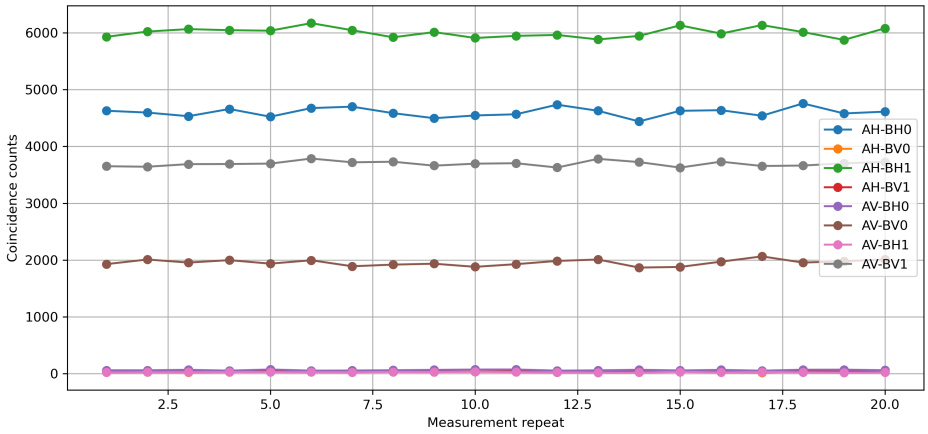


Figure 6.2.: Coincidence counts obtained when both Alice and Bob measure in the polarization Z basis. (*coin flip* setting as in figure 3.2) The spatial qubit is irrelevant for this measurement. The legend labels denote the measurement outcomes, where AH (AV) corresponds to an H (V) outcome at Alice. Similarly, BH (BV) denote H (V) outcomes at Bob, with 0 and 1 indicating the output ports of Bob's interferometer.

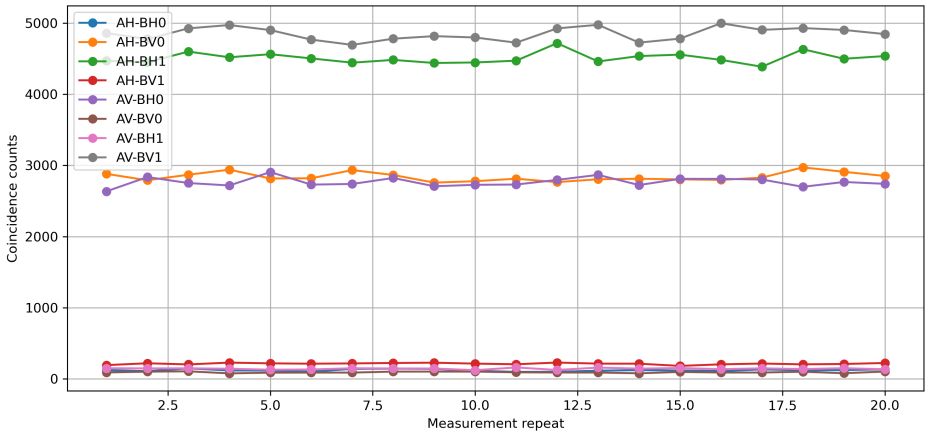


Figure 6.3.: Coincidence counts obtained when Alice measures in the polarization Y basis and Bob measures in the polarization X basis. (*verification* setting as in figure 3.2) The spatial qubit is prepared in the Y basis such that $r \oplus s \oplus t = 0$. The corresponding GHZ parity for this setting is $r \vee s \vee t = 1$. The legend labels denote the measurement outcomes: AH (AV) corresponds to an H (V) outcome at Alice, while BH (BV) denotes H (V) outcomes at Bob, with 0 and 1 indicating the output ports of Bob's interferometer.

The measurement results are shown in figures 6.2 and 6.3. The experiment is controlled by a Python script, which sets the desired measurement bases for both parties and records the corresponding coincidence counts. Prior to the measurements, the relative delays between the six single-photon detectors connected to the tomography stages are carefully calibrated to ensure accurate detection of coincidences.

A total of 40 measurement runs were performed, with 20 runs corresponding to the *coin-flip* setting and 20 runs corresponding to the *verification* setting as referred in figure 3.2. The coincidence window was set to 2 ns, and each measurement was recorded over an exposure time of 1 s.

From the measured coincidences, we extract the error rates for the two measurement settings:

$$\epsilon_{\text{coin-flip}} = 0.91 \pm 0.07\%,$$

$$\epsilon_{\text{verification}} = 3.69 \pm 0.16\%.$$

The *coin-flip* error rate is below 1%, indicating a high GHZ-state fidelity for the *coin flip* outcomes. The *coin-flip* error rate is solely dependent on the purity of the $|\Phi^+\rangle$ state generated by the source, as the spatial qubit is irrelevant in the *coin-flip* round. The slightly higher error observed in the *verification* setting is expected, as it involves the spatial qubit; in this case, not only the intrinsic purity of the SPDC source but also the visibility of the interferometer affects the overall quality of the generated GHZ state. In particular, imperfect interferometer visibility reduces the coherence between the two paths of Bob's photon. This reduction in coherence effectively lowers the purity of the GHZ state, thereby increasing the error rate in the *verification* setting.

7. Discussion

In this thesis, we derived and presented a novel weak coin-flipping protocol whose security is based on the GHZ game. Moreover, the loss-tolerant version of the protocol makes it suitable for practical experimental implementation. We also presented an idealized security proof in which dishonest parties may induce protocol aborts with non-zero probability. The protocol was experimentally implemented using hyper-encoding of polarization and spatial qubits on entangled 1550 nm photons generated by an SPDC source. The experimental setup enables Alice and Bob to perform measurements independently and to apply post-selection during the reveal phase, thereby avoiding abort events caused by photon loss. The obtained preliminary results demonstrate the feasibility of realizing the proposed protocol under realistic experimental conditions.

This thesis presents only an ideal security proof, which relies on idealized models of quantum cryptographic systems. In a real-world setting, however, practical implementations may be vulnerable to a broader range of attacks, such as multiphoton attacks [BCD+21]. Idealized protocols typically assume that Alice possesses perfect single-photon sources, that the quantum channel is lossless, and that Bob employs ideal detectors with perfect efficiency. In practice, losses and other experimental imperfections require Bob to report which pulses are successfully detected. A malicious Alice may exploit this information by sending multiphoton pulses and tracking detection events, thereby gaining information about Bob's measurement choices and potentially compromising the security of the protocol.

At the time of writing this thesis, my colleague Rebecca Hofer is deriving the full practical version of the weak coinflipping protocol together with a corresponding security proof that explicitly accounts for multiphoton attacks. In short, the idea is to combine statistical characterization of the photon source from Bob together with a post-selection strategy relying on time stamps that upper bounds the malicious Alice's advantage with high confidence.

Another potential limitation of the protocol is the imbalance in the cheating biases of Alice and Bob. In the current version of the protocol, a dishonest Alice can achieve a bias of up to 85%, whereas a dishonest Bob is limited to a bias of 75%. This asymmetry is undesirable in a realistic cryptographic setting, as it implies that one party has a greater advantage when deviating from the protocol, leading to an "unfair" situation even though the protocol remains fair when both parties are honest. Addressing this imbalance remains an open research problem. In particular, it would be desirable to modify or "twist" the protocol parameters or measurement settings such that the maximal cheating biases of both parties are comparable, thereby achieving a more symmetric weak coin-flipping protocol.

Another open research direction of interest is the implementation of a leader election

protocol. In leader election problems, a group of mutually distrustful parties aim to elect a leader in a fair manner, making it a natural generalization of the weak coin-flipping problem. In this thesis, we introduced a loss-tolerant version of weak coin flipping, which is particularly well suited for leader election, as protocol aborts because of photon losses become negligible.

In the experiment, we demonstrated a successful implementation of the practical protocol with low error rates. The measured error rates for the two operational settings reflect the different experimental sensitivities of the protocol. In the *coin-flip* setting, we obtain an error rate of

$$\epsilon_{\text{coin-flip}} = 0.91 \pm 0.07\%,$$

which primarily serves as an indicator of the fidelity of the initial state preparation and polarization measurements.

In contrast, the *verification* setting yields a higher error rate of

$$\epsilon_{\text{verification}} = 3.69 \pm 0.16\%,$$

as the verification measurements involve not only the polarization qubit but also the spatial qubit encoded in Bob's interferometer. Consequently, the observed error rate is influenced by the interferometer visibility and phase stability, in addition to the purity of the entangled photon source. These nonzero error rates lead to *honest aborts* of the protocol, as they originate from imperfect state preparation and measurement rather than from dishonest behavior by either party. By improving the source purity as well as the interferometer visibility and stability, both error rates could be further reduced in future implementations. Despite these limitations, the experimentally observed error rates remain well within the expectation for a secure implementation of the loss-tolerant protocol.

A further step toward completing the practical implementation of the protocol is including the time-stamp information for all detection events. By comparing time stamps for each detection click, Alice and Bob can reliably identify which measurement outcomes originate from the same emission event. This is crucial because the protocol relies on post-selecting detection events. Moreover, by incorporating time-stamped measurements, it becomes possible to implement the additional steps required prior to the protocol start to detect and account for multiphoton attacks, ensuring the security of the practical protocol under realistic experimental conditions.

In summary, this thesis presents both a theoretical and experimental investigation of a novel weak coin-flipping protocol. We introduced a loss-tolerant version that is practical for implementation with current photonic technologies and experimentally demonstrated its feasibility using hyper-encoded polarization and spatial qubits. While the idealized security proof guarantees the protocol's security under perfect conditions, practical considerations such as multiphoton attacks, error rates due to imperfect interferometer visibility require some additional steps, including a time stamp-based post-selection measurement and also source characterization. Nevertheless, the experimental results demonstrate that the protocol can be reliably implemented. Overall, this thesis provides

a strong foundation for future work aimed at extending the protocol to applications such as leader election.

Bibliography

[ACG+16] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Magnin. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. *SIAM Journal on Computing*, 45(3):633–679, 2016.

[AJK04] Joseph B. Altepeter, Daniel F. V. James, and Paul G. Kwiat. Quantum state tomography. *Lecture Notes in Physics*, 649:113–145, 2004.

[ASVH24] Atul Singh Arora, Jamie Sikora, and Thomas Van Himbeeck. Improving device-independent weak coin flipping protocols. *arXiv preprint arXiv:2404.17079*, 2024.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984.

[BCD+21] Mathieu Bozzio, Adrien Cavaillès, Eleni Diamanti, Adrian Kent, and Damián Pitalúa-García. Multiphoton and side-channel attacks in mistrustful quantum cryptography. *PRX Quantum*, 2:030338, Sep 2021.

[BCH+08] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Physical Review A—Atomic, Molecular, and Optical Physics*, 78(2):022316, 2008.

[BCKD20] Mathieu Bozzio, Ulysse Chabaud, Iordanis Kerenidis, and Eleni Diamanti. Quantum weak coin flipping with a single photon. *Physical Review A*, 102(2):022414, 2020.

[BCWW25] Mathieu Bozzio, Claude Crépeau, Petros Wallden, and Philip Walther. Quantum cryptography beyond key distribution: theory and experiment. *Reviews of Modern Physics*, 97(4):045006, 2025.

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, 1983.

[Boz25] Mathieu Bozzio. Part B, Lecture 3: "Modern (Quantum) Cryptography" Lecture Notes. Lecture notes, Dr. Mathieu Bozzio, University of Vienna, 2025. Accessed: 2025-09-01.

[BRHS10] Agata M Brańczyk, TC Ralph, Wolfram Helwig, and Christine Silberhorn. Optimized generation of heralded fock states using parametric down-conversion. *New Journal of Physics*, 12(6):063001, 2010.

[BVC+22] Mathieu Bozzio, Michal Vyvlecka, Michael Cosacchi, Cornelius Nawrath, Tim Seidelmann, Juan C Loredo, Simone L Portalupi, Vollrath M Axt, Peter Michler, and Philip Walther. Enhancing quantum cryptography with quantum dot single-photon sources. *npj Quantum Information*, 8(1):104, 2022.

[CFH+13] Andreas Christ, Alessandro Fedrizzi, Hannes Hübel, Thomas Jennewein, and Christine Silberhorn. Parametric down-conversion. In *Experimental Methods in the Physical Sciences*, volume 45, chapter 11, page 355. Academic Press / Elsevier, San Diego, CA, 2013.

[CK11] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 354–362. IEEE, 2011.

[Cle21] Richard Cleve. Quantum information processing: Quantum information theory (iii). Lecture notes, Institute for Quantum Computing & Cheriton School of Computer Science, University of Waterloo, December 2021.

[Cou18] Christophe Couteau. Spontaneous parametric down-conversion. *Contemporary Physics*, 59(3):291–304, 2018.

[DH22] Whitfield Diffie and Martin E Hellman. New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pages 365–390. 2022.

[GW07] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, page 565–574, New York, NY, USA, 2007. Association for Computing Machinery.

[Int18] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27000:2018 - Information technology – Security techniques – Information security management systems – Overview and vocabulary. `https://www.iso.org/standard/73906.html`, 2018. Clause 3.28.

[Kit03] Alexei Kitaev. Quantum coin flipping. In *6th Workshop on Quantum Information Processing (QIP 2003)*, 2003. Talk presented at QIP 2003, not formally published.

[KMN+07] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135–174, January 2007.

[KMW+95] Paul G Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, 75(24):4337, 1995.

[Kwi] Kwiat Quantum Information Group. Documentation: Python tomography library. `https://quantumtomo.web.illinois.edu/Doc/`. Accessed: 2026-01-01.

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

[LCG+24] Yong Liu, Yaojian Chen, Chu Guo, Jiawei Song, Xinmin Shi, Lin Gan, Wenzhao Wu, Wei Wu, Haohuan Fu, Xin Liu, et al. Verifying quantum advantage experiments with multiple amplitude tensor network contraction. *Physical Review Letters*, 132(3):030601, 2024.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. *arXiv preprint arXiv:0711.4114*, 2007.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition edition, 2010.

[NST15] Ashwin Nayak, Jamie Sikora, and Levent Tunçel. Quantum and classical coin-flipping protocols based on bit-commitment and their point games. *arXiv preprint arXiv:1504.04217*, 2015.

[NYC+23] Simon Neves, Verena Yacoub, Ulysse Chabaud, Mathieu Bozzio, Iordanis Kerenidis, and Eleni Diamanti. Experimental cheat-sensitive quantum weak coin flipping. *Nature Communications*, 14(1):1855, 2023.

[Pre21] John Preskill. Lecture notes of ph219/cs219 quantum computation fall 2021, 2021. Accessed: 2025-06-25.

[RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[SSW24] Teodor Strömberg, Peter Schiansky, and Philip Walther. Prescriptive method for fiber polarization compensation in two bases. *Applied Optics*, 63(7):1822–1827, 2024.

[Str23] Karl Teodor Alexander Trygve Strömberg. *Exploring Quantum Information with Single Photons*. Phd thesis, University of Vienna, 2023.

[Szt23] Esther Sztatecsny. Practical security and proof-of-principle implementation of quantum-digital payments. Master's thesis, University of Vienna, 2023.

[Ver26] Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.

[Wie83] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[YLL+20] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505, 2020.

A. Appendix

A.1. Security proof of the non loss-tolerant protocol

Alice's Optimal Cheating Strategy

The goal is to upper-bound the maximal probability with which a dishonest Alice can win the coin-flipping round while maintaining a fixed, small probability of being caught cheating (i.e., failing the verification round, which causes the protocol to abort). Rather than sending two standard Bell pairs, Alice can, in general, prepare an arbitrary six-qubit state ρ that maximizes her probability of winning.

Conditioned on Bob's choice of $i \in \{0,1\}$, which determines the verification and coin-flip states ($|\Phi^+\rangle_i$ and $|\Phi^+\rangle_{1-i}$, respectively), Alice may additionally apply a local completely positive trace-preserving (CPTP) map D_i to ρ, yielding the transformed state $\tilde{\rho} = D_i(\rho)$. Honest Bob then applies the unitaries $U_{b,s}$ and $U_{b,t}$ to check whether Alice has cheated, depending on her basis choice $r \in \{0,1\}$ and her measurement outcome a.

We first assume that Alice can *only optimize the initial quantum state* ρ that she sends at the beginning of the protocol. Beyond this, she follows the protocol honestly by applying the unitary operation $U_{a,r}$ to her verification photon.

The following SDP determines the optimal cheating strategy for Alice by identifying the quantum state ρ that maximizes her probability of *jointly* passing the verification and winning the coin flip:

$$\begin{aligned}
\max_{\rho} \Bigg\{ \frac{1}{8} \sum_{\substack{r,s,t\in\{0,1\} \\ r\oplus s\oplus t=0}} \Big[& \operatorname{Tr}\Big[(U_{a,r}\otimes U_{b,s}\otimes U_{b,t}\otimes \mathbb{1}_8)\,\rho\,(U_{a,r}^\dagger\otimes U_{b,s}^\dagger\otimes U_{b,t}^\dagger\otimes \mathbb{1}_8)\,(\Pi_{\mathrm{ver},(r,s,t)}\otimes\Pi_{\mathrm{coin}})\Big] \\
& + \operatorname{Tr}\Big[(\mathbb{1}_8\otimes U_{a,r}\otimes U_{b,s}\otimes U_{b,t})\,\rho\,(\mathbb{1}_8\otimes U_{a,r}^\dagger\otimes U_{b,s}^\dagger\otimes U_{b,t}^\dagger)\,(\Pi_{\mathrm{coin}}\otimes\Pi_{\mathrm{ver},(r,s,t)})\Big] \Big] \Bigg\} \\
\text{s.t.}\quad & \rho \succeq 0, \\
& \operatorname{Tr}[\rho] = 1.
\end{aligned} \tag{A.1}$$

Here, Π_{coin} projects onto the outcome where Alice wins the coin-flipping round:

$$\Pi_{\mathrm{coin}} = |H\rangle\langle H| \otimes |H\rangle\langle H| \otimes |0\rangle\langle 0|,$$

and the verification projectors $\Pi_{\mathrm{ver},(r,s,t)}$ denote the measurement outcomes that Bob

accepts:

$$\begin{aligned}\Pi_{\text{ver},0} &= |H\rangle\langle H| \otimes |H\rangle\langle H| \otimes |0\rangle\langle 0| + |V\rangle\langle V| \otimes |V\rangle\langle V| \otimes |0\rangle\langle 0| \\ &\quad + |V\rangle\langle V| \otimes |H\rangle\langle H| \otimes |1\rangle\langle 1| + |H\rangle\langle H| \otimes |V\rangle\langle V| \otimes |1\rangle\langle 1|, \\ \Pi_{\text{ver},1} &= |H\rangle\langle H| \otimes |H\rangle\langle H| \otimes |1\rangle\langle 1| + |V\rangle\langle V| \otimes |H\rangle\langle H| \otimes |0\rangle\langle 0| \\ &\quad + |H\rangle\langle H| \otimes |V\rangle\langle V| \otimes |0\rangle\langle 0| + |V\rangle\langle V| \otimes |V\rangle\langle V| \otimes |1\rangle\langle 1|.\end{aligned}$$

Since Alice learns which pair is used for verification *only after* sending ρ, she must maximize her success probability across both possible verification choices. The optimal value of (A.1) is 0.75, which represents the joint probability of passing verification and winning the coin-flip.

Including General CPTP Maps. Alice need not apply the honest unitary $U_{a,r}$ during verification; instead, she may apply any CPTP map $\mathcal{U}_r$. Let $\tilde{\rho}_0 = \mathcal{U}_{r=0}(\rho)$ and $\tilde{\rho}_1 = \mathcal{U}_{r=1}(\rho)$. Then the SDP becomes:

$$\begin{aligned}\max_{\tilde{\rho}_0,\tilde{\rho}_1} \quad & \frac{1}{8} \sum_{\substack{r,s,t\in\{0,1\} \\ r\oplus s\oplus t=0}} \Bigg\{ \operatorname{Tr}\Big[\big(U_{a,r}\otimes U_{b,s}\otimes U_{b,t}\otimes \mathbb{1}_8\big)\,\tilde{\rho}_r\,\big(U_{a,r}^\dagger\otimes U_{b,s}^\dagger\otimes U_{b,t}^\dagger\otimes \mathbb{1}_8\big)\,\big(\Pi_{\text{ver},(r,s,t)}\otimes\Pi_{\text{coin}}\big)\Big] \\ & \qquad + \operatorname{Tr}\Big[\big(\mathbb{1}_8\otimes U_{a,r}\otimes U_{b,s}\otimes U_{b,t}\big)\,\tilde{\rho}_r\,\big(\mathbb{1}_8\otimes U_{a,r}^\dagger\otimes U_{b,s}^\dagger\otimes U_{b,t}^\dagger\big)\,\big(\Pi_{\text{coin}}\otimes\Pi_{\text{ver},(r,s,t)}\big)\Big] \Bigg\} \\ \text{s.t.} \quad & \tilde{\rho}_0,\tilde{\rho}_1 \succeq 0, \qquad \operatorname{Tr}[\tilde{\rho}_0] = \operatorname{Tr}[\tilde{\rho}_1] = 1.\end{aligned} \tag{A.2}$$

This yields the same optimal value of 0.75.

Conditioning on Bob's Choice. Finally, if Alice may apply an additional local CPTP map $\mathcal{D}_i$ conditioned on Bob's announcement i, the total operation becomes $\tilde{\rho}_{i,r} = \mathcal{U}_r(\mathcal{D}_i(\rho))$. She can only act on her subsystem, hence the marginal over Bob's systems must remain unchanged:

$$\begin{aligned}\max_{\tilde{\rho}_{i,r}} \quad & \frac{1}{8}\sum_{i=0}^{1} \sum_{\substack{r,s,t\in\{0,1\} \\ r\oplus s\oplus t=0}} \operatorname{Tr}\Big[\tilde{\rho}_{i,r}\tilde{\Lambda}_{\text{joint},i}\Big] \\ \text{s.t.} \quad & \tilde{\rho}_{i,r} \succeq 0, \quad \operatorname{Tr}[\tilde{\rho}_{i,r}] = 1, \\ & \operatorname{Tr}_{\mathcal{A}_0\mathcal{A}_1}\tilde{\rho}_{i,r} = \operatorname{Tr}_{\mathcal{A}_0\mathcal{A}_1}\tilde{\rho}_{1-i,r} = \operatorname{Tr}_{\mathcal{A}_0\mathcal{A}_1}\tilde{\rho}_{1-i,1-r}.\end{aligned} \tag{A.3}$$

Here,

$$\tilde{\Lambda}_{\text{joint},i} = \begin{cases} (\mathbb{1}\otimes U_{b,s}^\dagger\otimes U_{b,t}^\dagger\otimes\mathbb{1}_8)(\Pi_{\text{ver},(r,s,t)}\otimes\Pi_{\text{coin}})(\mathbb{1}\otimes U_{b,s}\otimes U_{b,t}\otimes\mathbb{1}_8), & i=0, \\ (\mathbb{1}_8\otimes\mathbb{1}\otimes U_{b,s}^\dagger\otimes U_{b,t}^\dagger)(\Pi_{\text{coin}}\otimes\Pi_{\text{ver},(r,s,t)})(\mathbb{1}_8\otimes\mathbb{1}\otimes U_{b,s}\otimes U_{b,t}), & i=1. \end{cases}$$

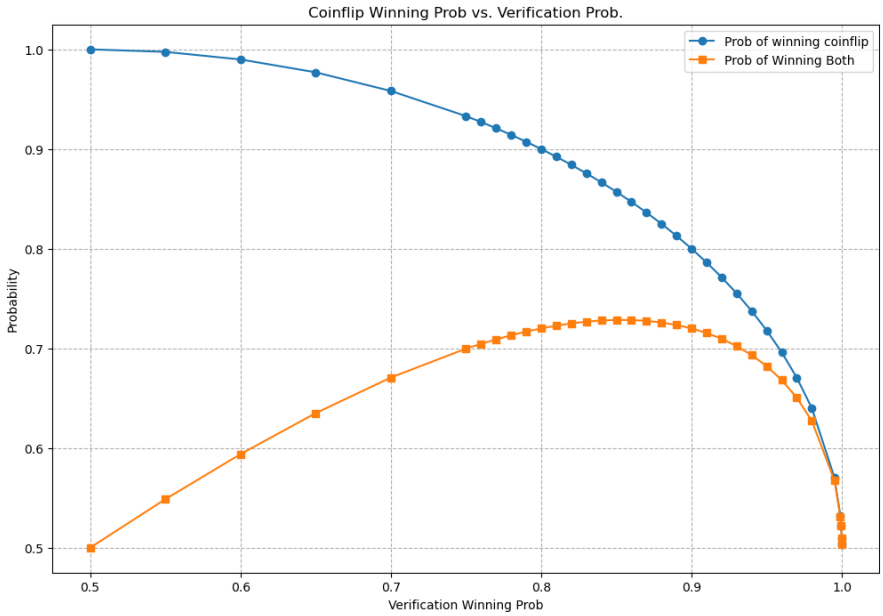


Figure A.1.: Winning probability of the coin-flip as a function of the success probability of passing the verification round, obtained by solving the SDP with the verification success probability as a constraint.

This SDP again achieves the same optimal value of 0.75.

One may alternatively formulate an SDP where the objective maximizes the probability of winning the coin-flip, while the probability of passing verification is fixed as a constraint:

$$\begin{aligned}
\max_{\tilde{\rho}_{i,r}} \quad & \frac{1}{8}\sum_{i=0}^{1}\sum_{\substack{r,s,t\in\{0,1\}\\ r\oplus s\oplus t=0}} \mathrm{Tr}\left[\tilde{\rho}_{i,r}\tilde{\Lambda}_{\mathrm{coin},i}\right] \\
\text{s.t.} \quad & \frac{1}{8}\sum_{i=0}^{1}\sum_{\substack{r,s,t\in\{0,1\}\\ r\oplus s\oplus t=0}} \mathrm{Tr}\left[\tilde{\rho}_{i,r}\tilde{\Lambda}_{\mathrm{ver},i,(r,s,t)}\right] = \{\text{threshold}\}_k, \qquad \text{(A.4)} \\
& \tilde{\rho}_{i,r} \succeq 0, \quad \mathrm{Tr}[\tilde{\rho}_{i,r}] = 1, \\
& \mathrm{Tr}_{\mathcal{A}_0\mathcal{A}_1}\,\tilde{\rho}_{i,r} = \mathrm{Tr}_{\mathcal{A}_0\mathcal{A}_1}\,\tilde{\rho}_{1-i,r} = \mathrm{Tr}_{\mathcal{A}_0\mathcal{A}_1}\,\tilde{\rho}_{1-i,1-r}.
\end{aligned}$$

with

$$\tilde{\Lambda}_{\mathrm{coin/ver},i} = \begin{cases} (\mathbb{1}\otimes U_{b,s}^{\dagger}\otimes U_{b,t}^{\dagger})\Pi_{\mathrm{coin/ver}}(\mathbb{1}\otimes U_{b,s}\otimes U_{b,t}), & i=0, \\ (U_{b,s}^{\dagger}\otimes U_{b,t}^{\dagger}\otimes\mathbb{1})\Pi_{\mathrm{coin/ver}}(U_{b,s}\otimes U_{b,t}\otimes\mathbb{1}), & i=1. \end{cases} \qquad \text{(A.5)}$$

By varying the values of the verification threshold $\{\text{threshold}\}_k \in [0.5, 1]$, as shown in Fig. A.1, the optimal probability of passing the verification and winning the coin-flip is

found numerically to be 0.7285. This result is *inconsistent* with the joint probability of 0.75 obtained from SDP A.3.

The reason for this inconsistency remains unclear and is to be further researched.

Bob's optimal cheating strategy

Dishonest Bob must find the optimal map λ that maximizes his probability of winning the coin-flip. Since Bob decides which subsystem is used for verification and which for the actual coin-flip, he can choose the subsystem that maximizes his success probability. He wins whenever he can map one or both of Alice's states onto his winning state.

After receiving photons from Alice, the state shared between Alice and Bob is

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}\big(|HH\rangle + |VV\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|HH\rangle + |VV\rangle\big) \\ &\in \mathcal{H}_{\mathcal{A}_0} \otimes \mathcal{H}_{\mathcal{B}_0} \otimes \mathcal{H}_{\mathcal{B}_1} \otimes \mathcal{H}_{\mathcal{A}_1}, \end{aligned} \tag{A.6}$$

where again the indices 0 and 1 denote the first and second state received from Alice.

Bob can only act on his subsystems $\mathcal{H}_{\mathcal{B}_0} \otimes \mathcal{H}_{\mathcal{B}_1}$, via a completely positive trace-preserving (CPTP) map

$$\lambda : \mathcal{H}_{\mathcal{B}_0} \otimes \mathcal{H}_{\mathcal{B}_1} \longrightarrow \mathcal{H}_{\tilde{\mathcal{B}}_0} \otimes \mathcal{H}_{\tilde{\mathcal{B}}_1}. \tag{A.7}$$

Choi representation of the map. The Choi operator of λ is defined as

$$J_\lambda = \sum_{r,r',s,s'} \lambda\big(|r\rangle\langle r'| \otimes |s\rangle\langle s'|\big) \otimes |r\rangle\langle r'| \otimes |s\rangle\langle s'|, \tag{A.8}$$

and satisfies

$$\lambda(\rho) = \mathrm{Tr}_{\tilde{\mathcal{B}}_0', \tilde{\mathcal{B}}_1'}\Big[J_\lambda \left(\mathbb{1}_{\tilde{\mathcal{B}}_0} \otimes \mathbb{1}_{\tilde{\mathcal{B}}_1} \otimes \rho^T\right)\Big], \tag{A.9}$$

Action of the map on the shared state. Writing $\rho = |\psi\rangle\langle\psi|$, Bob's action on the joint state can be expressed as

$$(\mathbb{1}_{\mathcal{A}_0} \otimes \lambda \otimes \mathbb{1}_{\mathcal{A}_1})(\rho) = \mathrm{Tr}_{\tilde{\mathcal{B}}_0', \tilde{\mathcal{B}}_1'}\Big[\left(\mathbb{1}_{\mathcal{A}_0} \otimes J_\lambda \otimes \mathbb{1}_{\mathcal{A}_1}\right) \rho^{T_{\mathcal{B}_0\mathcal{B}_1}}\Big], \tag{A.10}$$

where $T_{\mathcal{B}_0\mathcal{B}_1}$ denotes the partial transpose on Bob's subsystems. Equation (A.10) is the standard Choi–Jamiołkowski representation of a CPTP map acting locally on part of a bipartite state.

Optimization problem. Bob's goal is to maximize his winning probability

$$P_{\text{win}}^{(B)} = \max_\lambda \mathrm{Tr}\Big[\Pi_{B_{\text{win}}} \left(\mathbb{1}_{\mathcal{A}_0} \otimes \lambda \otimes \mathbb{1}_{\mathcal{A}_1}\right)(\rho_1)\Big]. \tag{A.11}$$

Using Eq. (A.10), this becomes a SDP in the Choi operator:

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}\Big[\Pi_{B_{\text{win}}}\, \mathrm{Tr}_{\tilde{\mathcal{B}}_0',\tilde{\mathcal{B}}_1'}\Big[\big(\mathbb{1}_{\mathcal{A}_0}\otimes J_\lambda\otimes\mathbb{1}_{\mathcal{A}_1}\big)\,\rho_1^{T_{\mathcal{B}_0\mathcal{B}_1}}\Big]\Big] \\ \text{subject to} \quad & J_\lambda \succeq 0, \\ & \mathrm{Tr}_{\tilde{\mathcal{B}}_0,\tilde{\mathcal{B}}_1}[J_\lambda] = \mathbb{1}_{\tilde{\mathcal{B}}_0'\tilde{\mathcal{B}}_1'}. \end{aligned} \tag{A.12}$$

The operator projecting onto Bob's winning subspace is

$$\begin{aligned} \Pi_{B_{\text{win}}} = {} & \big(|0\rangle\langle 0|_{\mathcal{A}_0}\otimes\mathbb{1}_{\mathcal{B}_0}\otimes\mathbb{1}_{\mathcal{B}_1}\otimes\mathbb{1}_{\mathcal{A}_1}\big) + \big(\mathbb{1}_{\mathcal{A}_0}\otimes\mathbb{1}_{\mathcal{B}_0}\otimes\mathbb{1}_{\mathcal{B}_1}\otimes|0\rangle\langle 0|_{\mathcal{A}_1}\big) \\ & - \big(|0\rangle\langle 0|_{\mathcal{A}_0}\otimes\mathbb{1}_{\mathcal{B}_0}\otimes\mathbb{1}_{\mathcal{B}_1}\otimes|0\rangle\langle 0|_{\mathcal{A}_1}\big), \end{aligned} \tag{A.13}$$

which corresponds to Bob winning if either of Alice's subsystems projects onto $|0\rangle$, but not both.

Compact SDP form. The optimization in Eq. (A.12) can equivalently be written in the standard linear form

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}[J_\lambda\, M_B] \\ \text{subject to} \quad & J_\lambda \succeq 0, \\ & \mathrm{Tr}_{\tilde{\mathcal{B}}_0,\tilde{\mathcal{B}}_1}[J_\lambda] = \mathbb{1}_{\tilde{\mathcal{B}}_0'\tilde{\mathcal{B}}_1'}, \end{aligned} \tag{A.14}$$

where

$$M_B = \mathrm{Tr}_{\mathcal{A}_0,\mathcal{A}_1}\Big[\big(\Pi_{B_{\text{win}}}\otimes\mathbb{1}_{\tilde{\mathcal{B}}_0'\tilde{\mathcal{B}}_1'}\big)\,\rho_1^{T_{\mathcal{B}_0\mathcal{B}_1}}\Big] \tag{A.15}$$

is a fixed Hermitian operator acting on Bob's output and input spaces.

The optimal value of the SDP yields 0.75, which is the maximum winning probability of a dishonest Bob.