NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCES
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

COMPUTER, TELECOMMUNICATIONS AND NETWORK ENGINEERING

MSc THESIS

Multi-User Measurement Device Independent Quantum Key Distribution Protocol

Nikolaos P. Stefanakos

Supervisors: **Syvridis Dimitrios**, Professor NKUA
Mandilara Aikaterini, Doctor NKUA

ATHENS

SEPTEMBER 2024

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΜΗΧΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Measurement Device Independent Πρωτόκολλο Κβαντικής Διανομής Κλειδιών Πολλών Χρηστών

Νικόλαος Π. Στεφανάκος

Επιβλέποντες: **Συβρίδης Δημήτριος**, Καθηγητής ΕΚΠΑ
Μανδηλαρά Αικατερίνη, Δόκτωρ ΕΚΠΑ

ΑΘΗΝΑ

ΣΕΠΤΕΜΒΡΙΟΣ 2024

MSc THESIS

Multi-User Measurement Device Independent Quantum Key Distribution Protocol

Nikolaos P. Stefanakos
S.N.: EN22200006

SUPERVISORS: **Syvridis Dimitrios**, Professor NKUA
Mandilara Aikaterini, Doctor NKUA

EXAMINATION COMMITTEE: **Mandilara Aikaterini**, Doctor NKUA
Syvridis Dimitrios, Professor NKUA
Kanellos Georgios, Professor NKUA

Examination Date: September 2024

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Measurement Device Independent Πρωτόκολλο Κβαντικής Διανομής Κλειδιών Πολλών Χρηστών

Νικόλαος Π. Στεφανάκος
Α.Μ.: EN22200006

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Συβρίδης Δημήτριος**, Καθηγητής ΕΚΠΑ
Μανδηλαρά Αικατερίνη, Δόκτωρ ΕΚΠΑ

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: **Μανδηλαρά Αικατερίνη**, Δόκτωρ ΕΚΠΑ
Συβρίδης Δημήτριος, Καθηγητής ΕΚΠΑ
Κανέλλος Γεώργιος, Καθηγητής ΕΚΠΑ

Ημερομηνία Εξέτασης: **Σεπτέμβριος 2024**

ABSTRACT

In the realm of modern network communications, ensuring the security of data transmission is paramount, yet typical cryptographic methods fall short of providing unconditional security due to their vulnerability to sophisticated attacks. Quantum Key Distribution (QKD) offers a massive shift by leveraging the fundamental principles of quantum mechanics to facilitate the secure exchange of cryptographic keys, ensuring unbreakable encryption regardless of computational advancements.

This thesis explores the advancements in QKD, particularly focusing on the evolution from traditional QKD protocols to Measurement-Device-Independent QKD (MDI-QKD). MDI-QKD addresses critical security concerns by outsourcing the measurement process to a potentially untrusted third party, thus neutralizing the threat posed by imperfect measurement devices and extending the effective communication range between users.

Building on this foundation, this thesis introduces an extension of an existing MDI-QKD protocol to a three-user configuration, aiming to establish a secure Quantum Conference Key Agreement (QCKA) among the users. This proposed protocol utilizes coherent states, balanced beam-splitters and photon detectors to distribute a common key securely to three users.

This thesis is structured to provide a comprehensive overview of the transition from typical to quantum cryptography, the quantum mechanical and optical principles underlying QKD and the various types of QKD systems and their security challenges. Detailed descriptions of the proposed three-party phase encoding protocol are presented, including a rigorous security proof and the derivation of the related Secure Key Rate (SKR) formula.

SUBJECT AREA: Multiple user MDI QKD protocol

KEYWORDS: Cryptography, QKD, MDI, QCKA

ΠΕΡΙΛΗΨΗ

Στο σύγχρονο κόσμο των τηλεπικοινωνιών, η ασφαλής μεταφορά των δεδομένων είναι ένα ζήτημα ύψιστης αξίας. Ωστόσο, οι μέθοδοι της κλασικής κρυπτογραφίας δεν μπορούν πάντα να τη παρέχουν, καθώς είναι αρκετά ευάλωτες σε επιθέσεις. Η Κβαντική Διανομή Κλειδιών (ΚΔΚ) χρησιμοποιώντας τις βασικές αρχές της Κβαντικής Μηχανικής για τη δημιουργία των κρυπτογραφικών κλειδιών, εξασφαλίζει μια ασυναγώνιστα δυνατή κρυπτογράφηση απέναντι σε επιθέσεις ανεξαρτήτως των υπολογιστικών ικανοτήτων τους.

Η συγκεκριμένη διπλωματική εργασία ερευνά τις εξελίξεις στο τομέα της Κβαντικής Διανομής Κλειδιών, εστιάζοντας στην εξέλιξη απο τα κλασικά πρωτόκολλα Κβαντικής Διανομής Κλειδιών σε Measurement Device Independent (MDI) πρωτόκολλα. Τα MDI πρωτόκολλα αντιμετωπίζουν σημαντικά ζητήματα ασφάλειας, καθώς αναθέτουν τη διαδικασία μέτρησης των κβαντικών καταστάσεων σε ένα δυνητικά μη αξιόπιστο τρίτο μέλος μέσα στο σχήμα της επικοινωνίας. Με αυτό το τρόπο εξουδετερώνουν τις απειλές που μπορεί να προέρχονται από τις ατελής (imperfect) συσκευές του συστήματος και αυξάνουν την θεωρητική απόσταση που μπορούν να έχουν τα δύο μέλη που θέλουν να επικοινωνήσουν.

Με αφορμή αυτή την ιδέα, προτείνεται μια επέκταση ενός κλασικού MDI πρωτοκόλλου Κβαντικής Διανομής Κλειδιών (δύο χρηστών) σε ένα τριών χρηστών, με τελικό στόχο τη διασφάλιση της δημιουργίας ενός κλειδιού μεταξύ και των τριών χρηστών με τη χρήση της τεχνολογίας του Quantum Conference Key Agreement (QCKA). Το πρωτόκολλο που προτείνεται κάνει χρήση coherent κβαντικών καταστάσεων, balanced beam-splitters και ανιχνευτών φωτονίων για να διανεμηθεί με ασφάλεια το κοινό κλειδί.

Η διπλωματική αυτή είναι δομημένη με τέτοιο τρόπο ώστε να παρέχει μια λεπτομερή επισκόπηση στους λόγους και στον τρόπο για τον οποίο γίνεται η μετάβαση από τη κλασική στη κβαντική κρυπτογραφία, τις αρχές της κβαντικής μηχανικής και της κβαντικής οπτικής στις οποίες βασίζεται η Κβαντική Διανομή Κλειδιών και τους διάφορους τύπους συστημάτων της με τις αντίστοιχες προκλήσεις ασφαλείας τους. Τέλος, παρουσιάζεται μια λεπτομερής ανάλυση των βημάτων του πρωτοκόλλου που προτείνεται, καθώς και η αντίστοιχη μελέτη για την ασφάλεια του και τον τρόπο με τον οποίο μπορούμε να εξάγουμε τον τύπο του ρυθμού δημιουργίας ασφαλών κλειδιών (Secure Key Rate).

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: MDI Πρωτόκολλο ΚΔΚ πολλών χρηστών

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Κρυπτογραφία, Κβαντκή Διανομή Κλειδιών, MDI, QCKA

ACKNOWLEDGMENTS

I would like to express my gratitude and appreciation to my supervisor, Prof. Syvridis Dimitrios whose support and encouragement has been invaluable throughout this study. Further, i would like to thank Dr. Mandilara Aikaterini, for providing guidance and feedback throughout this thesis and without whom I would not have been able to complete this research.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Security and cryptography are crucial aspects of our everyday network communications. Since traditional networking methods are vulnerable to a variety of attacks, classic data encryption cannot provide unconditional security for its party members. Quantum Key Distribution (QKD) protocols enable legitimate party members to share secret keys with unconditional security. In contrast to traditional cryptographic methods that rely on the computational complexity of mathematical functions, the security of QKD is based on quantum physical laws. For this reason, the encryption can be considered computationally unbreakable by quantum means.

Four decades after the introduction of the first QKD protocol, BB84 [3], the field has much evolved driven for the need for provable unconditional security in realistic use cases. The introduction of the first Measurement Device Independent (MDI) protocol [4] has marked the QKD field for two reasons. First, the Measurement Unit (MU) was moved to a third party which can be untrusted and under the control of an eavesdropper, and whose imperfections do not affect the security of the protocol. The second reason, is the increase of achievable distance between two users. The latter, is a key point for the cutting-edge at the moment Twin-Field (TF) protocols, which can be considered as variations of the first MDI protocols.

In this thesis, we propose an extension of one of the two-user phase encoding MDI protocol [5] to a three-user scenario. The aim is to distribute a common key to all of them, following the steps of the original protocol ,i.e., Alice, Bob_1 and Bob_2 send out signals, they wait for MU's successful announcements of detection, and then they perform the standard post-processing on their sifted data. The task of distributing a common key to multiple users in a secure way, is also known under the name of Conference Key Agreement (CKA). In Quantum CKA protocols, both device dependent and device independent have been devised [6–8] exploiting the correlations of multipartite entangled states. Recently, a multi-party TF MDI protocol [6] has been proposed without the need of entanglement and in addition this asks for the same physical resources as in this work, namely, coherent states, Balanced Beam-Splitters (BBS) and photon-detectors. On the other hand, the exact experimental settings and steps of the two protocols differ as presented in Chapter 7.

The road-map of this work is as follows. In Chapter 2 we describe how and why we transitioned from the Typical to the Quantum cryptography. In Chapter 3 and Chapter 4 we analyze the basic Quantum mechanic principles and the Quantum optic principles that are used in the QKD field, respectively. In Chapter 5, we name the different QKD system types, we present the concept of the Quantum Conference Key Agreement and talk about the attacks and security in a QKD system. In Chapter 6, we make an introduction into the field of MDI-QKD and its various ways that we can encode information in this. In Chapter 7, we propose a three user party phase encoding protocol, giving detailed information about the steps of the protocol and we sketch the security proof deriving the formula that connects the Secure Key Rate (SKR) with measurable quantities. Lastly, in Chapter 8,

we give a synopsis on what we accomplish with our work and we discuss about future possibilities.

2. CLASSIC AND QUANTUM CRYPTOGRAPHY

2.1 Typical cryptography

In conventional cryptography, we want to make a message unreadable by anyone except the conversation party members. At first we have the **message** (M) that we want to send, the so called plain-text. Using an encryption block and with the help of a **key** (K), we generate an encrypted text. This encrypred text we call the **Cipher-text** (C). Then, we send the Cipher-text through an insecure channel and the key through a secure channel to the receiver. The receiver possess a decryption block, that with the help of the key, has the ability to reverse the changes implemented on the starting message and reconstruct the original plain-text. This process can be mathematically written with the following equations. For the encryption procedure:

$$E_K(M) = C \ ,$$

where E_K is the encryption block. For the decryption procedure:

$$D_K(C) = M \ ,$$

where D_K is the decryption block. The Key (K) is usually generated from a key generation machine that picks it randomly from a **key-space**. With the word key-space we mean the amount of all possible keys that the key generator can produce.

There are two categories of cryptographic algorithms:

- **Symmetric algorithms**: The symmetric algorithms are algorithms that use the same key for both the encryption and the decryption of the message. Often they are called secret-key algorithms. The reason is that during the whole procedure they try to key their key secret from any eavesdropper. As in the event that the key is compromised, anyone could decrypt and read their conversation or encrypt a malicious message and send it to the members. One very strong algorithm in this category is the AES-256, where 256 denotes its key length in bits. This algorithm due to its big key length can be assumed quantum secure. This can be easily proven if we try to brute force the encryption key with a quantum search algorithm as the Grover Algorithm and still needing to perform 2^{128} algorithmic iterations.
- **Asymmetric algorithms**: As their name hints, the asymmetric algorithms have an “asymmetric” behaviour considering their encrypting and decrypting keys. That is, because they use different keys in their encryption and decryption blocks. This type of algorithms have a public key for the encryption of the plain-text and a secret key for the decryption of the cipher-text. As an example, we’ll describe the communication between two users that use the RSA asymmetric algorithm. Below we present a pseudocode that describes the process that each user needs to do to create their public (encryption) and secret (decryption) key.

Algorithm 1 The structure of RSA algorithm

Choose: p, q
Require: p, q = prime ▷ Require p, q be prime numbers
Compute:
1: $n \leftarrow p \times q$ ▷ n gives the key length in bits
2: $\lambda(n) \leftarrow lcm(p-1, q-1)$
Compute:
3: $k \leftarrow 0$
4: $e \leftarrow 1$
5: **while** $k \neq 1$ **do** ▷ We need gcd$(e, \lambda(n)) = 1$
6: $e \leftarrow e + 1$
7: $k \leftarrow \text{gcd}(e, \lambda(n))$
8: $d \leftarrow e^{-1} mod(\lambda(n))$
9: **end while**
Encryption:
10: $c(m) \leftarrow m^e mod(n)$
Decrytpion:
11: $m(c) \leftarrow c^d mod(n)$

To choose what cryptographic algorithm we need to use is not a simple task and depends on the needs of each application. These two categories have their own advantages and disadvantages, some of them are:

1. **Processing time/Speed**: Usually symmetric algorithms tend to need a lot fewer resources than the asymmetric algorithms, as they need only one key for the encryption and decryption of the message.

2. **Implementation complexity**: Symmetric algorithms require a secure channel to exchange the secret key. This can some times become a problem in conventional cryptography with a number of attacks that can compromise the channel.

3. **Security against classic computers**: Symmetric algorithms don't give the same level of security as the asymmetric ones. As the use of one key can lead to the compromise of the whole communication, if it gets stolen. On the other hand, asymmetric algorithms using a private key for the decryption of the cipher-text, can guarantee in a lot more cases a foolproof communication.

4. **Security against quantum computers**: As the asymmetric algorithms can be broken with a brute-force attack, the use of a quantum computer makes their security obsolete. In comparison, a symmetric algorithm with a large key can be proven more reliable against quantum machines (AES-256).

2.2 From typical to Quantum cryptography

Conventional cryptographic systems, while robust against current computational capabilities, are vulnerable to attacks by quantum computers. Quantum algorithms, such as Shor's algorithm, can efficiently solve the mathematical problems underlying public-key cryptography, rendering these systems insecure. Unlike typical cryptography, whose security depends on computational complexity, the security of quantum cryptography is based on the fundamental principles of quantum mechanics. This provides unconditional security, meaning that no amount of computational power can break the encryption. The most prominent application of quantum cryptography is QKD, which allows two or more parties to generate a shared secret key. Protocols like BB84 and E91 utilize quantum states to detect eavesdropping, ensuring secure key exchange. The algorithms that are used are symmetric, as the members of the communication party use the same key for the encryption and the decryption of the messages.

Quantum cryptographic protocols inherently detect eavesdropping and any attempt to intercept the quantum states introduces detectable disturbances. This phenomenon can alert the communicating parties to the presence of an eavesdropper. Unfortunately, these technologies are still in the early stages of development and deployment. Current systems require highly specialized equipment, such as single-photon sources and detectors, which are not yet widely available. Integrating quantum cryptographic systems with existing communication infrastructure poses significant challenges. This includes developing compatible hardware and protocols to ensure seamless operation alongside conventional cryptographic systems.

3. ELEMENTS OF QUANTUM MECHANICS IN QKD

In this chapter we'll discuss some of the quantum mechanic laws that are essential in the field of Quantum Cryptography, such as the Uncertainty principle, entanglement and the non-cloning theorem.

3.1 Quantum Harmonic Oscillator

The Quantum Harmonic Oscillator is one of the most important and well-studied systems in quantum mechanics, as it provides a foundation for more complex quantum systems and is integral to both theoretical and applied quantum physics. It serves as a fundamental model for understanding a wide range of physical phenomena, from the behavior of atoms in a lattice, to the modes of light in a cavity. In this work we are interested in the quantum harmonic oscillator since its Hamiltonian coincides with the Hamiltonian of photonic states.

The Hamiltonian of a quantum harmonic oscillator describes the total energy of the system and is given by:

$$\hat{H} = \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega^2\hat{x}^2 \ , \tag{3.1}$$

where $\hat{p}$ is the momentum operator, $\hat{x}$ is the position operator, m is the mass of the particle, and ω is the angular frequency of the oscillator. The position and momentum operators can be expressed in terms of the creation ($\hat{a}^\dagger$) and annihilation ($\hat{a}$) operators, which describe the creation and annihilation of photons in the vacuum, respectively:

$$\begin{aligned}\hat{a}^\dagger &= \sqrt{\frac{\pi m\omega}{h}}\left(\hat{x} - \frac{i}{m\omega}\hat{p}\right)\\ \hat{a} &= \sqrt{\frac{\pi m\omega}{h}}\left(\hat{x} + \frac{i}{m\omega}\hat{p}\right) \ .\end{aligned}$$

If we calculate the quantity $\hat{a}^\dagger\hat{a}$, we get:

$$\begin{aligned}\hat{a}^\dagger\hat{a} &= \frac{\pi m\omega}{h}\left(\hat{x} - \frac{i}{m\omega}\hat{p}\right)\left(\hat{x} + \frac{i}{m\omega}\hat{p}\right)\\ &= \frac{\pi m\omega}{h}\left(\hat{x}^2 + \frac{i\hat{x}\hat{p}}{m\omega} - \frac{i\hat{p}\hat{x}}{m\omega} + \frac{\hat{p}^2}{(m\omega)^2}\right)\\ &= \frac{\pi m\omega}{h}\left(\hat{x}^2 + \frac{i[\hat{x},\hat{p}]}{m\omega} + \frac{\hat{p}^2}{(m\omega)^2}\right) \ .\end{aligned}$$

We know that $[\hat{x},\hat{p}] = i\frac{h}{2\pi}$, so now we have:

$$\begin{aligned}\hat{a}^\dagger\hat{a} &= \frac{\pi m\omega}{h}\left(\hat{x}^2 - \frac{h}{2\pi m\omega} + \frac{\hat{p}^2}{(m\omega)^2}\right) \\ &= \left(\frac{\pi m\omega}{h}\right)\left(\frac{2}{m\omega^2}\right)\left(\frac{1}{2}m\omega^2\hat{x}^2 + \frac{1}{2}\frac{\hat{p}^2}{m} - \frac{h\omega}{4\pi}\right) \ .\end{aligned}$$

Finally, using equation 3.1, we get:

$$\hat{a}^\dagger\hat{a} = \frac{2\pi}{h\omega}\left(\hat{H} - \frac{h\omega}{4\pi}\right)$$

$$\hat{H} = \frac{h\omega}{2\pi}\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) \ . \tag{3.2}$$

We now define the number operator as:

$$\hat{N} = \hat{a}^\dagger\hat{a} \ , \tag{3.3}$$

where we know that:

$$\begin{aligned}\hat{a}^\dagger\left|n\right\rangle &= \sqrt{n+1}\left|n+1\right\rangle \\ \hat{a}\left|n\right\rangle &= \sqrt{n}\left|n-1\right\rangle \ .\end{aligned}$$

If we replace equation 3.3 in equation 3.2, we have:

$$\hat{H} = \frac{h\omega}{2\pi}\left(\hat{N} + \frac{1}{2}\right) \ . \tag{3.4}$$

To find the eigenstates of the energy, we apply the Hamiltonian (equation 3.4) to a number state $|n\rangle$:

$$\hat{H}\left|n\right\rangle = \frac{h\omega}{2\pi}\left(\hat{N} + \frac{1}{2}\right)\left|n\right\rangle \ . \tag{3.5}$$

Using the property of the number operator:

$$\hat{N}\left|n\right\rangle = n\left|n\right\rangle \ ,$$

we can write that:

$$\hat{H}\left|n\right\rangle = \frac{h\omega}{2\pi}\left(n + \frac{1}{2}\right)\left|n\right\rangle \ . \tag{3.6}$$

And finally we conclude that the eigenstates of the energy for the Harmonic oscillator are expressed in terms of $|0\rangle$ as:

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}} |0\rangle \tag{3.7}$$

The equation 3.7 is called number state and can express a quantum state if we have one photon, two photons, etc.

3.2 Uncertainty principle

The uncertainty principle (or Heisenberg's uncertainty principle), was proposed from W. Heisenberg and is regarded as one of the principles of quantum mechanics. It states that certain pairs of physical properties, such as position and momentum, cannot be simultaneously measured to arbitrary precision. In the context of QKD, this principle underlines the security of the communication protocols by ensuring that any attempt at eavesdropping inevitably introduces detectable disturbances. The uncertainty principle for the quadrutures of an electromagnetic field can be mathematically expressed as:

$$\Delta_x \Delta_p \geq \frac{1}{2} \left(\frac{h}{2\pi} \right) ,$$

where Δ_x is the uncertainty in position, Δ_p is the uncertainty in momentum and h is Planck's constant.

In the realm of quantum information, this principle is often discussed in terms of non-commuting observables, such as the components of a qubit. For example, the uncertainty in measuring a qubit in the X-basis versus the Z-basis illustrates this principle and is given form the mathematical expression that follows:

$$\Delta X \Delta Z \geq \left| \frac{1}{2i} \langle \psi | [X, Z] | \psi \rangle \right| , \tag{3.8}$$

where $[X, Z] = XZ - ZX$.

3.3 Entanglement

Quantum entanglement provides the fundamental basis for the security of several key distribution protocols in the QKD field. The entanglement is a phenomenon where two or more quantum particles become linked such that the state of one particle instantaneously influences the state of the other(s), regardless of the distance separating them. This unique property is pivotal for detecting any eavesdropping attempts. When two party members (Alice and Bob) share entangled particles, any interception or measurement by

an eavesdropper (Eve) will inevitably disturb the entangled state. These disturbances are detectable through statistical correlations in the measurement outcomes, allowing Alice and Bob to identify and mitigate security threats.

Some typical entanglement-based protocols are:

- **The Ekert 91 (or E91)**: a protocol that leverages the principles of quantum entanglement and Bell's inequalities to ensure secure key distribution.
- **The BBM92**: a protocol that follows the steps of the typical BB84 protocol, with the main difference that it is using entangled photon pairs instead of single photons to reinforce its security against eavesdropping.

Similarly, MDI-QKD leverages entanglement to eliminate vulnerabilities associated with measurement devices. By using an untrusted intermediary to perform BSMs on entangled states sent by Alice and Bob, MDI-QKD ensures that any attempt to tamper with the measurement results is detectable, thereby providing a high level of security even with potentially compromised devices. Thus, entanglement not only enhances the robustness of QKD systems but also extends their practical applicability, making it a vital element in the development and implementation of secure quantum communication networks.

3.4 Non-cloning theorem

The non-cloning theorem is a fundamental principle of quantum mechanics that states it is impossible to create an exact copy of an arbitrary unknown quantum state. It is an essential component of the quantum mechanics theory, as if it were possible to clone wavefunctions, it would be possible to circumvent the uncertainty of quantum measurements by making a very large number of copies of a wavefunction, measuring different properties of each copy, and reconstructing the exact state of the original wavefunction. A quick proof of this principle is shown below:

Let us assume that we have two arbitrary quantum states $|\psi\rangle$ and $|\phi\rangle$, a blank state $|0\rangle$ and a unitary matrix U, that can clone arbitrary quantum states. First, we assume that the cloning machine exists and it has to satisfy these equations:

$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$
$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Then we take the inner product of our states before the cloning procedure:

$$(|\phi\rangle \otimes |0\rangle) \cdot (|\psi\rangle \otimes |0\rangle) = \langle\phi|\psi\rangle \langle 0|0\rangle = \langle\phi|\psi\rangle$$

And after the cloning procedure:

$$(|\phi\rangle \otimes |\phi\rangle) \cdot (|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle \langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

But since unitary matrices conserve inner products, we have that:

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

Which, can only give two solutions:

$$\langle\phi|\psi\rangle = 0$$
$$\langle\phi|\psi\rangle = 1$$

That means that $|\psi\rangle$ and $|\phi\rangle$ can be either orthogonal or equal but not arbitrary. So there can not exist a unitary matrix that can clone arbitrary quantum states. This principle is in contrast with classical principles.

4. ELEMENTS OF QUANTUM OPTICS IN QKD

QKD leverages the quantum properties of photons, such as superposition and entanglement, in order to perform the exchange of cryptographic keys between parties. For this reason we describe various subjects within quantum optics that are essential to QKD, including coherent states, the results of two interfering states in a beam splitter and the Hong–Ou–Mandel (HOM) effect. These topics illustrate how quantum optics principles are harnessed to enable secure communication and highlight the sophisticated techniques used in modern QKD systems.

4.1 Coherent states

Coherent states [9] are specific states of the quantum harmonic oscillator that closely resemble classical states. These states were first introduced by R. J. Glauber in the context of quantum optics and have since become fundamental to various areas of quantum mechanics and quantum information theory. They can be described as the eigenstates of the annihilator operator $\hat{\alpha}$.

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \ , \tag{4.1}$$

where $\alpha = |\alpha|e^{i\theta_\alpha}$.

Coherent states can only be produced using high quality lasers, because they need to have a well defined amplitude ($|\alpha|$) and phase (θ_α). Their name is derived from the fact that their fields are perfectly coherent and they come as close as quantum mechanics allows to wavelike states of the electromagnetic oscillator.

It can be easily proven, using equation 4.1, that the vacuum $|0\rangle$ is a coherent state if we assume that $\alpha = 0$. For this reason we can say that the vacuum is a zero amplitude coherent state. We can also write the mean energy of a coherent state, using equation 3.2:

$$\begin{aligned}
\langle \hat{H} \rangle &= \langle \alpha |\, \hat{H}\, |\alpha\rangle \\
&= \langle \alpha |\, \frac{h\omega}{2\pi} \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right) |\alpha\rangle \\
&= \frac{h\omega}{2\pi} \left(\langle \alpha |\, \hat{a}^\dagger \hat{a}\, |\alpha\rangle + \frac{1}{2} \right) \\
&= \frac{h\omega}{2\pi} \left(|\alpha|^2 + \frac{1}{2} \right) \ .
\end{aligned}$$

If we consider that $\alpha = \sqrt{\mu}$ the above equation is written as:

$$\langle \hat{H} \rangle = \frac{h\omega}{2\pi} \left(\mu + \frac{1}{2} \right) \ . \tag{4.2}$$

So, the mean energy of a coherent state can be expressed in relation with the intensity of the photons (μ).

4.2 Coherent States in a Beam Splitter

The Bell state measurement (BSM) [10], is the projection of two qubits onto four orthogonal maximally entangled states. It is an important tool in the field of MDI-QKD, as we explain in later chapters. In this section, we'll describe how these measurements are calculated in the concept of an MDI scheme between two users Alice and Bob.

To begin with, Alice and Bob create coherent states $\left|\sqrt{\mu}e^{i\theta}\right\rangle$ and send them to Charlie. Then, Charlie performs a BSM with the two Coherent State pulses he received and announces the result to Bob and Alice. An in-depth analysis on how the Bell States are created is shown in the equations below.

Consider a state $|\alpha\rangle$, we can write it as:

$$|\alpha\rangle = e^{\alpha\hat{\alpha}^\dagger - \alpha^*\hat{\alpha}} |0\rangle = e^{-\frac{|\alpha|^2}{2}} e^{\alpha\hat{\alpha}^\dagger} e^{-\alpha^*\hat{\alpha}} |0\rangle$$

$$\Rightarrow |\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} e^{|\alpha|e^{i\theta}\hat{\alpha}^\dagger} |0\rangle \ , \tag{4.3}$$

where α is the Euler formula $|\alpha|e^{i\theta}$

Let us consider $\alpha = \sqrt{\mu}$, so the $|\alpha\rangle$ state is written as:

$$|\alpha\rangle = e^{-\frac{|\sqrt{\mu}|^2}{2}} e^{\sqrt{\mu}e^{i\theta}\hat{\alpha}^\dagger} |0\rangle \ .$$

Alice prepares the state:

$$|\alpha_A\rangle = e^{-\frac{|\sqrt{\mu}|^2}{2}} e^{\sqrt{\mu}e^{i\theta}\hat{\alpha}_A^\dagger} |0\rangle$$

and Bob prepares the state:

$$|\alpha_B\rangle = e^{-\frac{|\sqrt{\mu}|^2}{2}} e^{\sqrt{\mu}e^{i\theta}\hat{\alpha}_B^\dagger} |0\rangle$$

and broadcast them to Charlie. When these states interfere in the BS we get the following state:

$$|\alpha_{BS}\rangle = |\alpha_A\rangle \cdot |\alpha_B\rangle$$

$$\Rightarrow |\alpha_{BS}\rangle = e^{-\frac{|\sqrt{\mu}|^2}{2}} e^{\sqrt{\mu}e^{i\theta}\hat{\alpha}_A^\dagger} |0\rangle \cdot e^{-\frac{|\sqrt{\mu}|^2}{2}} e^{\sqrt{\mu}e^{i\theta}\hat{\alpha}_B^\dagger} |0\rangle \ . \tag{4.4}$$

We know that:

$$\hat{\alpha}_A^\dagger = \frac{\sqrt{2}}{2}(\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger) \tag{4.5}$$

$$\hat{\alpha}_B^\dagger = \frac{\sqrt{2}}{2}(-\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger)\ , \tag{4.6}$$

we denote as $\hat{\alpha}_0^\dagger$ the part of the equation that corresponds to Detector D_0 and $\hat{\alpha}_1^\dagger$ to Detector D_1.

Using Equations 4.4, 4.5 and 4.6 we get:

$$\begin{aligned} |\alpha_{BS}\rangle &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}e^{i\theta_A}(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+\frac{\sqrt{2}}{2}e^{i\theta_B}(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}\,|00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}\hat{\Theta}}\,|00\rangle\ , \end{aligned} \tag{4.7}$$

where $\hat{\Theta} = (e^{i\theta_A}(\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger) + e^{i\theta_B}(-\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger))$.

The result of the measurement onto the state $|\alpha_{BS}\rangle$ from the Detectors (D_0, D_1) of Charlie, is called Bell State.

4.3 Probability of a Single Photon Detection

To calculate the probability of each detection, we have to consider that a coherent state, if we are using the Folk representation, has a Poissonian photon statistics. Keeping that in mind, the probability is calculated as follows.

Using Poissonian photon statistics, we know that the probability to measure n photons can be described as:

$$p_n = \frac{|\alpha|^{2n}}{n!}e^{-|\alpha|^2}.$$

Using that $\alpha = \sqrt{\mu}$, we have:

$$p_n = \frac{\mu^n}{n!}e^{-\mu}.$$

Since the photon detectors cannot usually distinguish the number of photons, the probability for a ”click”, i.e., firing of a photon detector is:

$$P_{click} = 1 - p_0$$

$$\Rightarrow P_{click} = 1 - \frac{\mu^0}{0!}e^{-\mu}$$

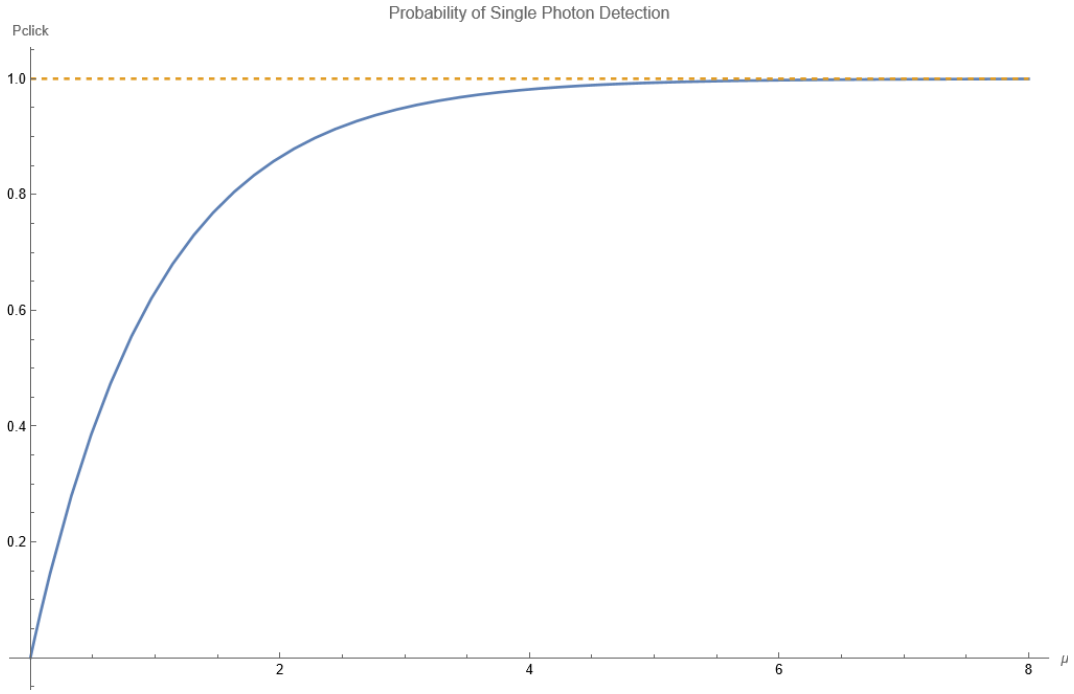

Figure 4.1: Illustration of the relation between the intensity of the coherent state (μ) and the probability of detection, according to the equation 4.8.

$$\Rightarrow P_{click} = 1 - e^{-\mu} \ . \tag{4.8}$$

In figure 4.1, we present the relation between the probability of detection and the intensity of the coherent state (μ), as expressed by the equation 4.8.

4.4 HOM effect

The Hong–Ou–Mandel [10] (HOM) effect, is a quantum interference phenomenon that occurs when two indistinguishable photons are incident on a beam splitter, as seen in the figure that follows (4.2). This effect is a fundamental demonstration of the quantum nature of light and has significant applications in quantum information science, including QKD. In MDI-QKD, the HOM effect is essential. When Alice and Bob send photons to an untrusted intermediary (Charlie), the HOM effect allows Charlie to perform quantum interference measurements that are critical for ensuring the security of the protocol. A basic principle of the HOM effect is when two identical photons enter a 50/50 beam splitter from different input ports, they interfere in such a way that they exit from the same output port. A mathematical explanation of this effect is presented below.

Assume a Beam splitter operator:

$$U_{BS} = A_t \left|d_2\right\rangle \left\langle l\right| + A_r \left|d_1\right\rangle \left\langle l\right| + A_r \left|d_2\right\rangle \left\langle r\right| + A_t \left|d_1\right\rangle \left\langle r\right| \ ,$$

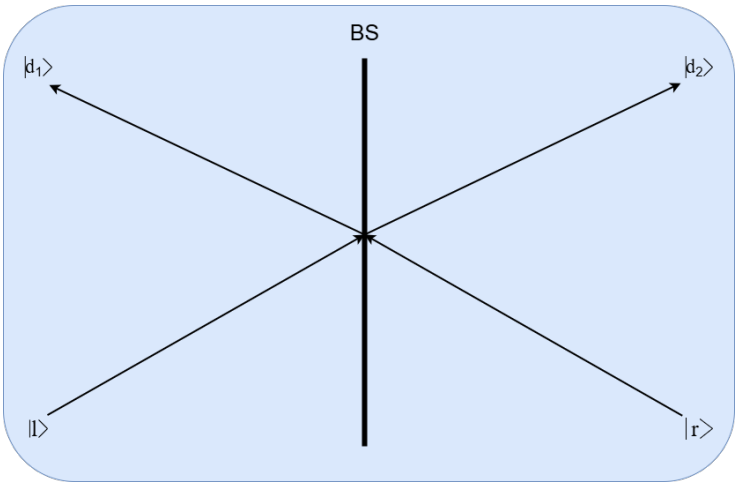

Figure 4.2: Illustration of the HOM effect.

where A_t is the transmission amplitude coefficient, A_r is the reflection amplitude coefficient, the $\langle l|$ state denotes that the photonic signal comes from the left port and the $\langle r|$ state denotes that it comes from the right port of the Beam Splitter. Also, we know that $|A_t|^2 + |A_r|^2 = 1$.

If we have two photons at the Beam splitter (BS) inputs, following the above equation, we can write the joint output state of the BS as follows:

$$\begin{aligned}
|\Psi\rangle_{out} &= (U_{BS}\,|l\rangle) \otimes (U_{BS}\,|r\rangle) \\
&= ((A_t\,|d_2\rangle\,\langle l| + A_r\,|d_1\rangle\,\langle l| + A_r\,|d_2\rangle\,\langle r| + A_t\,|d_1\rangle\,\langle r|)\,|l\rangle) \\
&\times ((A_t\,|d_2\rangle\,\langle l| + A_r\,|d_1\rangle\,\langle l| + A_r\,|d_2\rangle\,\langle r| + A_t\,|d_1\rangle\,\langle r|)\,|r\rangle) \\
&= (A_t\,|d_2\rangle\,\langle l|l\rangle + A_r\,|d_1\rangle\,\langle l|l\rangle + A_r\,|d_2\rangle\,\langle r|l\rangle + A_t\,|d_1\rangle\,\langle r|l\rangle) \\
&\times (A_t\,|d_2\rangle\,\langle l|r\rangle + A_r\,|d_1\rangle\,\langle l|r\rangle + A_r\,|d_2\rangle\,\langle r|r\rangle + A_t\,|d_1\rangle\,\langle r|r\rangle) \\
&= (A_t\,|d_2\rangle + A_r\,|d_1\rangle)(A_r\,|d_2\rangle + A_t\,|d_1\rangle) \\
&= (A_t A_r\,|d_2\rangle\,|d_2\rangle + {A_t}^2\,|d_2\rangle\,|d_1\rangle + {A_r}^2\,|d_1\rangle\,|d_2\rangle + A_r A_t\,|d_1\rangle\,|d_1\rangle)
\end{aligned}$$

Now, we have to replace A_r = cos θ and A_t = i sin θ and if we consider that in a 50/50 BS, cos θ = sin $\theta = \frac{1}{\sqrt{2}}$, we finally get:

$$\begin{aligned}
|\Psi\rangle_{out} &= (i \sin\theta \cos\theta\,|d_2\rangle\,|d_2\rangle + (i \sin\theta)^2\,|d_2\rangle\,|d_1\rangle + \cos\theta^2\,|d_1\rangle\,|d_2\rangle + i \cos\theta \sin\theta\,|d_1\rangle\,|d_1\rangle) \\
&= (i\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\,|d_2\rangle\,|d_2\rangle - \left(\frac{1}{\sqrt{2}}\right)^2\,|d_2\rangle\,|d_1\rangle + \left(\frac{1}{\sqrt{2}}\right)^2\,|d_1\rangle\,|d_2\rangle + i\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\,|d_1\rangle\,|d_1\rangle) \\
&= (\frac{i}{2}\,|d_2\rangle\,|d_2\rangle - \frac{1}{2}\,|d_2\rangle\,|d_1\rangle + \frac{1}{2}\,|d_1\rangle\,|d_2\rangle + \frac{i}{2}\,|d_1\rangle\,|d_1\rangle) \\
&= (\frac{i}{2}\,|d_2\rangle\,|d_2\rangle + \frac{i}{2}\,|d_1\rangle\,|d_1\rangle)
\end{aligned}$$

This result means that the output beam can either exit from the left exit and hit Detector 1 ($\frac{i}{2}\left|d_1\right\rangle\left|d_1\right\rangle$) or it can exit from the right exit and hit Detector 2 ($\frac{i}{2}\left|d_2\right\rangle\left|d_2\right\rangle$).

5. BASICS OF QKD

5.1 QKD Systems

The QKD technology can be divided into two categories of systems. Those that the users communicate directly with each other and those that need a remote node, to create a trusted key.

1. **Direct communication technology**
    - **Device-Dependent QKD (DD-QKD)**: This is the first QKD system that has been proposed. Usually in this system the source is placed on Alice and the detector on Bob.
2. **Remote node technology**
    - **Source-Device-Independent QKD (SDI-QKD)**: In this system Alice and Bob are assigned with the role of the detectors and Charlie (Remote Node) is the source. This technology mainly uses entanglement based protocols and schemes, as those that we present in the following section.
    - **Measurement-Device-Independent QKD (MDI-QKD)**: This system was proposed to counter the inefficiencies of faulty measurement devices, strengthen the security of QKD protocols (as we exaplin in later sections) and help increase the effective distance that a QKD system can operate. It applies to the users the role of the source and to the trusted node the role of the detector.

We present a figure with the architecture of each type in figure 5.1.

5.2 Quantum Conference Key Agreement

QCKA is an advanced cryptographic protocol designed to allow multiple parties to securely agree on a shared secret key using the principles of quantum mechanics. Unlike traditional QKD, which involves two parties, QCKA extends the capabilities of QKD to a multi-user scenario, facilitating secure communication within a group.

QCKA could be achieved with the help of standard two-party QKD schemes, generating a set of N-1 pair-wise keys either via prepare-and-send schemes or via shared entangled Bell pairs. Using though this method needs more resources and adds complexity to the system. On top of that, with the increase on the number of users we notice an exponential decrease on the probability of the protocol's success.

The first protocols proposed for the QCKA focused on the multipartite correlations between the N-party GHZ states. The GHZ states take their name from the scientists that conceived them, Greenberger, Horne and Zeilinger. The N-party GHZ states can be written as:

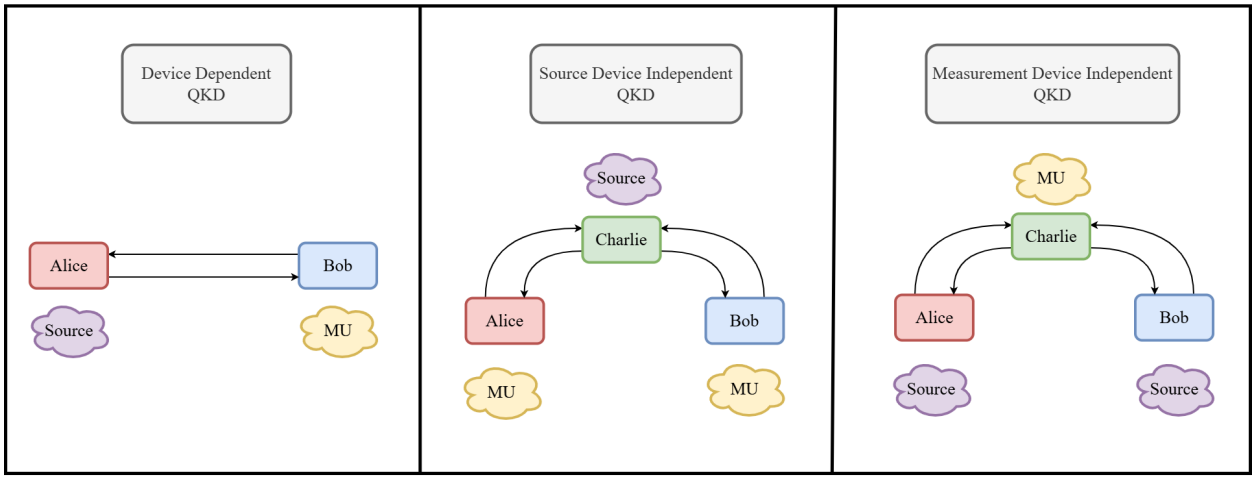

Figure 5.1: Presentation of the QKD system schemes.

$$|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0...0\rangle + |1...1\rangle)$$

,where $|0\rangle$, $|1\rangle$ is the Z-basis, composed by the eigenstates of the Pauli operator σ_z. For reference a 3-party GHZ state can be expressed as:

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

Another type of protocols emerged, that do not rely on the correlation provided by the GHZ states. Instead they exploit the multipartite entanglement of the W states. The W states for N-users can be express as:

$$|W_N\rangle = \frac{1}{\sqrt{N}}(|0...001\rangle + |0...010\rangle + |0...100\rangle + ... + |1...000\rangle)$$

For reference a 3-party W state can be written as:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

Some of the disadvantages of using an entanglement based CKA protocol are presented below:

- Implementing QCKA protocols requires sophisticated quantum technologies, including reliable sources of multi-partite entangled states, high-efficiency detectors, and robust quantum channels.
- Quantum systems are highly sensitive to noise and decoherence, which can degrade the entangled states and affect the protocol's performance. Developing error

correction techniques and improving quantum hardware are crucial for overcoming these challenges.

- Integrating QCKA into existing communication infrastructures involves significant effort. It requires the development of compatible hardware, protocols, and interfaces to ensure seamless operation alongside classical communication systems

5.3 Attacks and Imperfect Devices in QKD

In this section, we'll review the results of using imperfect devices. Also we'll analyze the attacks that an eavesdropper can do in order to learn more information about the secret key.

5.3.1 Types of Attacks in QKD

An eavesdroppers main objective, in a Quantum system, is to temper with the quantum channels in order to find correlations and eventually learn information about the secret key. All the possible attacks that an eavesdropper can perform, can be grouped into three categories.

1. The category of **Individual Attacks**. In this category we assume that the eavesdropper (Eve) can attack in each round of the protocol individually. This is happening because we do not allow Eve to have a Quantum Memory. For that reason, she is bound to measure each quantum information she was able to intercept in every around, without prior knowledge.

2. The **Collective Attacks** category. This category, resembles a lot of the Individual Attacks one, with the only difference that now we allow Eve to possess a Quantum memory. Now, Eve can store the Quantum information she intercepts in each round and perform a collective attack on all that she stored in the end. With this method she can more easily find correlations between each round and finally uncover valuable information about the key.

3. The **Coherent Attacks** category. In this category, we don't make any assumption for the behaviour of Eve and her capabilities. She has to abide though by the laws of Quantum Mechanics.

5.3.2 Examples of attacks in QKD

In QKD schemes, adversaries aim to intercept or tamper with the key exchange process without being detected by the communicating parties. The robustness of QKD lies in its

ability to detect any such interference through the inherent properties of quantum mechanics. In this section, we'll present some of the possible attacks that can happend in a QKD system.

- **Photon-Number-Splitting Attack**: Ideally a QKD system would use a true single photon source, which never generates more than one photon in each output pulse. However, an attenuated laser diode is often used instead. The coherent states/pulses from an attenuated laser are superpositions of several photons. For these, the same information is redundantly encoded on all the photons in the pulse, thus creating the conditions for Eve to attack the system through a photon-number-splitting attack. Eve then can subtract one photon and keep it for herself, while forwarding the remaining photons to the QKD receiver. During the public discussion, Eve will learn the encoding basis and will then be able to reliably measure the photons she captured. This way, Eve gains full information whereas the QKD receiver interprets the undetected photons as a normal loss due to the communication channel, leaving Eve undetected.

- **Trojan-horse Attack**: Eve can inject light into the sending module to probe and retrieve information about the encoding devices, thus realizing a quantum version of the "Trojan-horse attack". Light injected by Eve passes through the same devices encoding information on the quantum signals and some of this light is then reflected back to Eve due to the non-zero reflectivity of the electro-optic components.

- **Bright-light Attack**: A crucial part of most QKD systems are the single-photon detectors, used in the QKD receiver to detect the weak optical signals sent by the transmitter through the communication channel. The most common single-photon detectors are the Avalanche Photodiodes (APDs). The APD are reverse-biased above the breakdown voltage so that a single photon can trigger a self-sustained avalanche easily detectable by a sudden increase in the output current. However, any detector necessarily spends part of its time below the breakdown voltage, because at some point the detection avalanche has to be quenched to reset the detector to the initial conditions. When this happens, the detector enters the linear mode, where it is not sensitive to single-photon light anymore. Eve can exploit this linearity to control the output of the detectors and determine, unnoticed, bits of the final key. In some cases, Eve can even push a single-photon detector into the linear mode by sending bright-light into the receiver module, to then exploit her controlling abilities and steal key bits.

- **Back-flash Attack**: In case of a detection event, the secondary photons emitted by the APD during the avalanche of charge carriers can travel from the detectors back to Eve through the communication channel. This consists a passive way that allows Eve to learn the bit values associated with detection events and is the so-called back-flash attack.

5.3.3 Imperfections in devices

Although using a system with perfect devices would be ideal, it is not that easy to be achieved. Devices in the source or detector side can have flaws that compromise the integrity and the security of a Quantum Distribution system [11]. Some of the possible results of using imperfect devices are presented below.

1. One result of a faulty source device is the phenomenon of tagging. Sometimes a faulty source can incorporate information, about the base that was used in the preparation phase, into the qubits. Eve can take advantage of this in order to learn more about the secret key.
2. An imperfect detector has the tendency to misfire. When a detector misfires, the probability that a qubit is detected successfully is basis dependent. Eve can exploit this vulnerability if she control when the detector misfires. If Eve can control when the detector misfires, she can eavesdrop some qubits and then actively cause the detector to fire depending on what she measured.
3. Another result of using imperfect devices is the ability of Eve to hide the disturbance of her eavesdropping. This happens when the source device and the detector device are not aligned correctly to omit or detect a qubit in the proper basis.

5.4 Security in QKD

Security in QKD is of most important because it ensures the integrity and confidentiality of the communication between parties. As outlined before QKD leverages the principles of quantum mechanics, such as the uncertainty principle and quantum entanglement, to detect any eavesdropping attempts. Given the increasing threats to data privacy and the potential vulnerabilities of classical cryptographic methods, the robust security provided by QKD is crucial for safeguarding sensitive information in an era of growing cyber threats. In this section, we'll analyse what makes a QKD protocol secure and which are the algorithms that help its robustness.

5.4.1 Basic principles of a secure protocol

There are some conditions that a multiparty protocol needs to satisfy in order to be considered secure [7].

- A protocol needs to be **correct**. A correct protocol has to satisfy the inequality that follows:

$$p(Key_A = Key_{B_1} = ... = Key_{B_n}) \geq 1 - \epsilon_{correct}$$

,where $p(Key_A = Key_{B_1} = ... = Key_{B_n})$ is the probability that all the keys are identical and $\epsilon_{correct}$ symbolizes the degree of the protocols correctness.

- A protocol needs to be **secret**. To satisfy the secrecy requirement, we need Alice's key to be randomly chosen among a set of possible strings and the eavesdropper to not have any information about the key, except for a probability symbolized with ϵ_{secret}. This requirement can be written as the inequality that follows:

$$p(\Omega)\frac{1}{2} \parallel \rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_{E|\Omega} \parallel \leq \epsilon_{secret}$$

  ,where $p(\Omega)$ is the possibility of the event Ω that the protocol does not abort, $\rho_{K_A E|\Omega}$ is a shared state between Alice and Eve when we have the event Ω, τ_{K_A} is the maximally mixed state of all the possible Alice's keys and $\rho_{E|\Omega}$ is the state that Eve has in the end of the protocol.

- A protocol needs to be **complete**. In order to fulfill the requirement of completeness, a protocol needs to have an honest implementation such that the possibility that it does not abort is greater than $1 - \epsilon_{complete}$.

To summarize, for a protocol to be considered secure it needs to satisfy two conditions:

1. It needs to be $\epsilon_{correct}$ & $_{secret}$. That is, it needs to meet the requirements of **Correctness** and **Secrecy**.
2. It needs to meet the requirements of **Completeness**

5.4.2 Resolving errors with CSS codes

Due to attacks, such as those that were described before, and the imperfections in the quantum channels, the raw key generated in QKD protocols often contains errors and usually some information of the secret key is leaked to the adversaries. The most used way to counter this phenomenon is the employment of entanglement distillation and error correction techniques to produce a final key that is secure and error-free. As entanglement distillation, we refer to the process by which Alice and Bob improve the quality and security of the raw key by reducing the error rate and eliminating any information potentially leaked to an eavesdropper. This is achieved through the processes of error correction and privacy amplification.

- Error correction is the process where Alice and Bob compare portions of their raw key to identify and correct discrepancies. Classical error-correcting codes are used at this stage to reconcile their keys.
- Privacy amplification we characterize the process where Alice and Bob try to minimize any information an eavesdropper might have obtained. This involves applying a hash function to the corrected key, reducing its length but ensuring that the final key is secure.

The most known quantum error-correcting codes are called CSS or Calderbank-Shor-Steane [12,13] as they were named after their inventors. CSS codes combine two classical linear codes, typically one for bit-flip errors (C_1) and another for phase-flip errors (C_2), where we know that $C_2 \subset C_1 \subset {F_2}^n$. CSS codes can correct both bit-flip and phase-flip errors. By performing syndrome measurements, Alice and Bob can detect and correct errors without directly measuring the quantum state, thus preserving the superposition and entanglement properties.

6. MEASUREMENT DEVICE INDEPENDENT QKD

An MDI scheme consists, as was mentioned in a previous chapter, of two parts. The Users (Bob and Alice) and the MU (Charlie). The main differences from a typical QKD scheme, is that the MU is located in a remote location away from the users and that it can work with a compromised MU by an adversary. A typical MDI-QKD protocol usually works following the steps that follow below:

1. At first, Bob and Alice prepare quantum states that contain information and send them to a remote location, known as Charlie.

2. After that, the two states arrive at Charlie's location where a BS is placed, to create an interference between them.

3. Lastly, Charlie performs a measurement and announces the results to the users.

6.1 Different MDI-QKD schemes

In this section, we will describe the three main schemes that an MDI-QKD system can operate. These are the One-Mode, Two-Mode and Mode Pairing scheme.

1. **Two-Mode** was the first scheme that was proposed, and it took its name from the fact that it needs two different types of pulses (Reference and Signal) to arrive at the MU one after the other. This scheme although it can provide a stable optical interference, using the Reference pulses in-front of the Signals, it depends heavily on coincidence that prevents it from increasing the Key Rate.

2. Second came the **One-Mode** scheme. This scheme encodes information into one pulse that sends across the channel. To make this scheme work successfully we need global phase locking, to prevent a destructive phase difference between the interfering coherent states of the two parties. One main MDI-QKD scheme that belongs to this category is the Twin-Field QKD, that can either encode the information in the phase or the intensity of the pulse.

3. Lastly, a new scheme has been proposed, the **Mode Pairing** scheme. This scheme depends neither in coincidence or phase locking. To achieve that, in this scheme Bob and Alice, through a post processing operation, match their clicked pulses together and use them as Reference or Source, depending on their needs.

We present in figure 6.1 the main MDI-QKD scheme types.

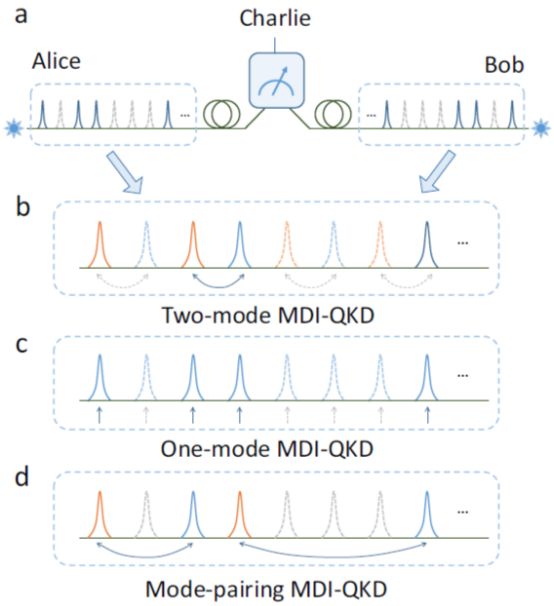

Figure 6.1: Presentation of the main MDI-QKD scheme types [1].

6.2 Typical MDI protocols

There are two main ways that one can encode information into a pulse. By using the phase, with Phase encoding and the polarization of the laser beam with Polarization encoding. In what follows we describe the first MDI protocols which have pubished in 2012 by Lo et al. These are now considered as the basic MDI protocols, since the last years one can find in the literature many publications with more advanced schemes.

6.2.1 Architecture of the phase encoding protocol

A simple phase encoding protocol usually follows an architecture as shown in figure 6.2.

Now, we are going to explain what each module in the architecture of the figure 6.2 means. The source can be a Weak Coherent State (WCS) laser that produces coherent states. These states can take random values, for example the logical 0 (phase 0 for base X, $\frac{\pi}{2}$ for base Y) or the logical 1 (phase π for base X and phase $\frac{3\pi}{2}$ for base Y) with the help of the Phase Modulator (PM). The IM is the Intensity Modulator and can be used to create the concept of decoy states [14], especially useful to reinforce the security of a protocol. Last, the coherent states interfere onto a BS and the outputs are guided into two Single Photon Detectors (SPDs) D_0 and D_1.

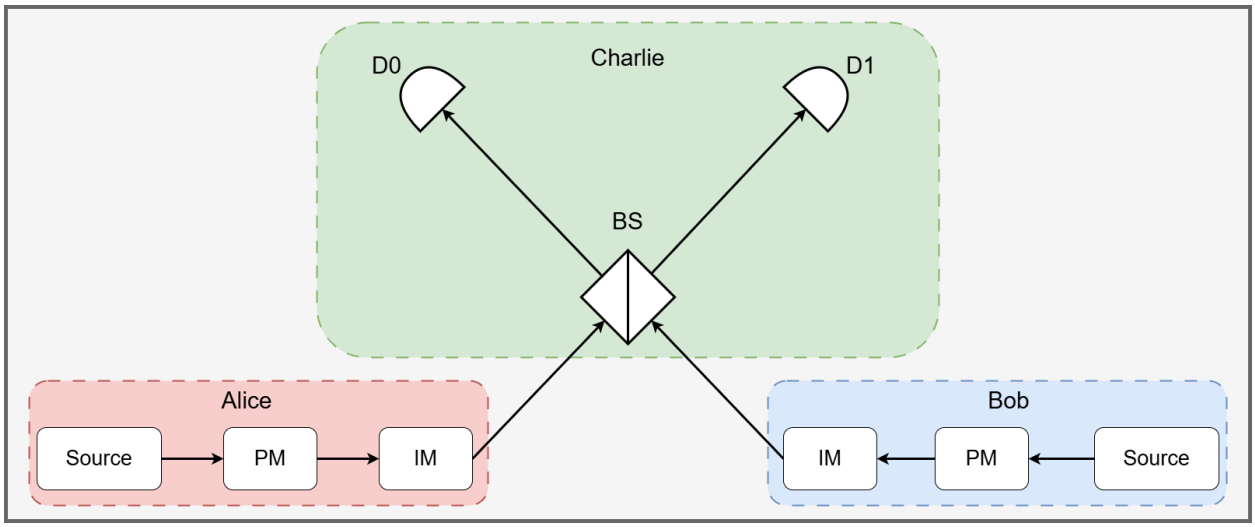

Figure 6.2: Architecture of a Phase Encoding Protocol, where BS is the beam splitter, PM is the phase modulator and IM is the intensity modulator.

6.2.2 Architecture of the polarization encoding protocol

The architecture of a polarization encoding protocol is similar to the one of phase encoding. The main difference is the use of the Polarization Beam Splitters (PBSs). The figure 6.3 that follows, displays this difference.

As mentioned above the architectures of polarization and phase encoding schemes are similar. Their only two differences are:

1. In the polarization scheme the Phase Modulator (PM) is replaced with a Polarization Modulator (PolM). This change can provide more possible random states. For example, $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$. Where we have the horizontal polarization denote by the state $|0\rangle$, vertical polarization denote by the state $|1\rangle$ and the diagonal polarizations, 45 degrees denote by the state $|+\rangle$ and -45 degrees by $|-\rangle$.

2. Two Polarization Beam Splitters (PBS) are added, that project the input beams into Horizontal or Vertical polarization states.

6.3 The phase encoding MDI-QKD protocol

In the following subsections, we focus more in detail on how the phase encoding protocol works and in the next chapter we introduce an expansion of it, that makes possible a communication between three members.

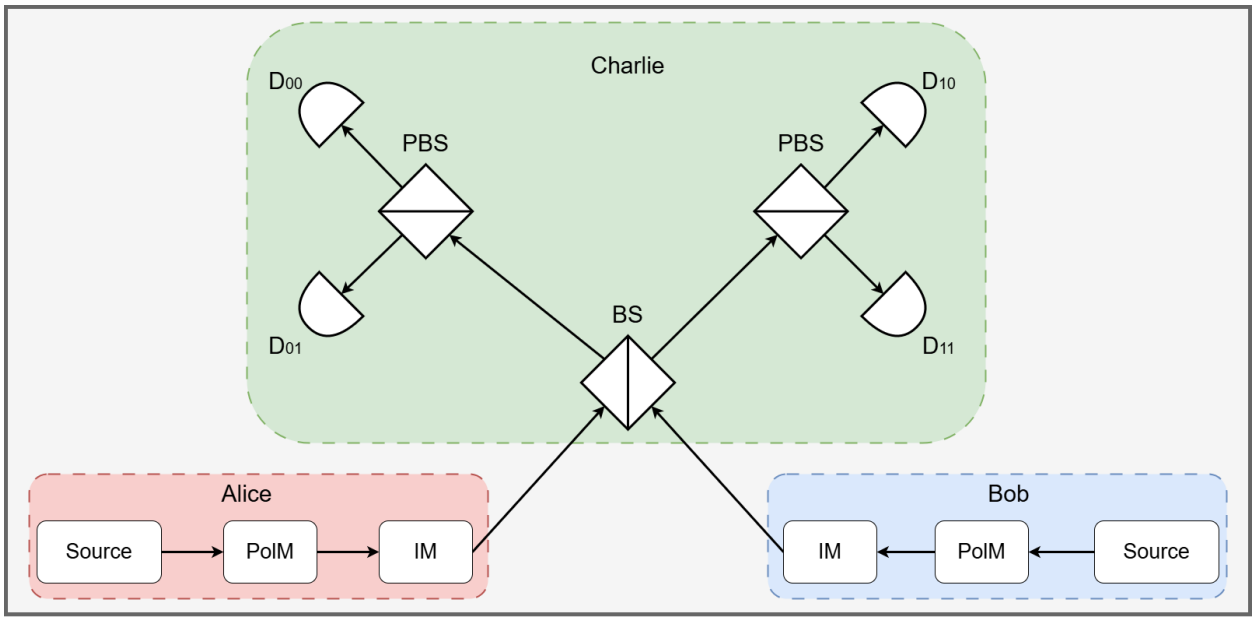

Figure 6.3: Architecture of a Polarization Encoding Protocol, where BS is the beam splitter, PBS are the polarization beam splitters, PolM is the polarization modulator and IM is the intensity modulator.

6.3.1 Steps of a phase encoding protocol

First, we describe the typical protocol emphasizing on its individual steps. A phase encoding protocol usually follows the steps that are presented below.

1. Alice and Bob prepare two different categories of pulses, one that can be described as the signal pulse and one as the reference pulse. The signal pulse is the one that contains the valuable information and will be used for the key generation. The reference pulse is used for the global phase locking. Alice and Bob randomly apply phase modulation on the signal pulse, and choose from four different phases (0, $\pi/2$, π, $3\pi/2$). Those four phases are divided into pairs that define the bases X (0, π) and Y ($\pi/2$, $3\pi/2$).

2. Alice and Bob send their pulses to Charlie that has a Measuring Unit (MU). Charlie performs measurements onto the pulses and announces if the measurements were successful or not. With the term successful measurement we consider the event when we have a detection on only one of the two detectors. Also, if the measurement was successful, he announces the type of the detection (0 or 1).

3. In a scenario that the measurement was not successful Alice and Bob discard their data and begin the process from step 1. If it was successful, they keep them and broadcast the bases they used. If their bases don't match, they discard them and begin from the start again. If they do match, they begin to create the sifted key.

4. Alice and Bob continue to follow these three steps until they create a sifted key that's large enough for their needs.

5. When they create the sifted key, they proceed to estimate two parameters of the channel, the Bit Error Rate (BER) and the Phase Error Rate. To achieve that, they use a piece of the sifted key as the test bits for the BER estimation and the remaining bits to estimate the phase error rate. If these two parameters are too high, Alice and Bob abort the protocol.

6. Alice and Bob choose on an error correcting code and a hash function that they will both use, depending on the values of the two parameters (BER and Phase Error Rate). Lastly, they perform error correction and privacy amplification before they finally share the key.

6.3.2 Results of the measurement

To further understand how Alice and Bob create the shifted key, we need to explain what Charlie announces in each successful detection depending on the phase (Basis) Alice and Bob used. As described in Section 4.2, Charlie performs a BSM with the two coherent states that Alice and Bob sent to him. Using Equation 4.7, we can assign the four phase values of the θ_A and θ_B and we finally get the following table.

Table 6.1: Results of the Bell State Measurements for two users.

A\B	0		π		π/2		3π/2	
0	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**
	0	$\sqrt{2\mu}$	$\sqrt{2\mu}$	0	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$
π	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**
	$\sqrt{2\mu}$	0	0	$\sqrt{2\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$
$\pi/2$	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**
	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	0	$\sqrt{2\mu}$	$\sqrt{2\mu}$	0
π	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**	**D0**	**D1**
	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{\mu}$	$\sqrt{2\mu}$	0	0	$\sqrt{2\mu}$

In table 6.1 we color:

- with red the events that are discarded by the system because we have a detection in both the detectors.
- with light blue when we have a detection on detector 1 (detection type 1).

- with pink when we have a detection on detector 0 (detection type 0).

A detailed analysis on the calculations of the table 6.1 can be found in Appendix A.1.

6.3.3 Security of a typical MDI protocol

To prove the security strength of a phase encoding protocol, we'll follow the steps of Ref. [5]. First, we consider a virtual protocol in which Bob and Alice make pulses with a joined systems state. In this protocol Eve has full control and knowledge of the whole system, creating a worst case scenario. Then we will try to give an equation that can approximately calculate the SKR of such protocol.

$$\begin{aligned}|\Psi'\rangle = \frac{1}{2}(&|0_z\rangle_E|0_z\rangle_B|0_z\rangle_A \left|\Phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\right\rangle \left|\Phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\right\rangle \\ &+|0_z\rangle_E|0_z\rangle_B|1_z\rangle_A \left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_A}\right\rangle)\right\rangle \left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_B}\right\rangle)\right\rangle \\ &+|1_z\rangle_E|1_z\rangle_B|0_z\rangle_A \left|\Phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\right\rangle \left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_B}\right\rangle)\right\rangle \\ &+|1_z\rangle_E|1_z\rangle_B|1_z\rangle_A \left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_A}\right\rangle)\right\rangle \left|\Phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\right\rangle).\end{aligned} \tag{6.1}$$

Below, we will explain what each parameter in the above state means.

- The first system denoted by E ($|K\rangle_E$) is used to inform Eve if Alice and Bob have used the same base. If Alice and Bob used the same base then the system is $|0_z\rangle_E$ and if they used different bases the system is $|1_z\rangle_E$.
- The second system denoted by B ($|K\rangle_B$) is used to inform Bob if he used the same base as Alice. As before, if Bob used the same base as Alice then the system is $|0_z\rangle_B$ and if he used different a base the system is $|1_z\rangle_B$.
- The third system denoted by A ($|K\rangle_A$) is used by Alice. She measure it to determine the base to use. If the system is $|0_z\rangle_A$ then Alice used the X base and if it $|1_z\rangle_A$ she used the Y base. The outcome of the measurement is sent to Eve after she announces the measurement outcome at the MU.
- The systems $\left|\Phi_x^{(+)}(\left|\sqrt{\alpha_A}\right\rangle)\right\rangle$, $\left|\Phi_x^{(+)}(\left|\sqrt{\alpha_B}\right\rangle)\right\rangle$, $\left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_A}\right\rangle)\right\rangle$ and $\left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_B}\right\rangle)\right\rangle$ are sent to Eve and contain the valuable information for the key generation.

Eve then post-selects the pulses that will be used for the key generation. As described before the key generation process is accomplished only when Bob and Alice use the same base. Following this assumption we will write again the state for the virtual protocol (Equation 6.1), focusing only on the systems that Bob and Alice used the same base.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle_A \left|\Phi_x^{(+)}(|\sqrt{\alpha_A}\rangle)\right\rangle \left|\Phi_x^{(+)}(|\sqrt{\alpha_B}\rangle)\right\rangle + |1_z\rangle_A \left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_A}\right\rangle)\right\rangle \left|\Phi_y^{(+)}(\left|\sqrt{-i\alpha_B}\right\rangle)\right\rangle). \tag{6.2}$$

To be able to calculate the key generation rate, we need to focus on the approximation of the Phase error rate, as this can not be experimentally calculated. The Phase error rate is the rate of errors on the bits when we measure a state with the wrong base. To give an example, in this protocol we have a Phase error rate on the Y basis, denoted as $\delta_{ph,y}$, if Charlie chose to measure on the Y basis when Bob and Alice prepared and sent pulses in the X basis.

We are going to bound the phase and bit error rates. Let $\gamma(t|\alpha)$ be the number of events that a measurement was accomplished and "t", "α" be two variables that indicate the existence of an error and the base that was used, respectively. "t" and "α" can take the value of 0 and 1.

- To find the value of "t", Bob measures his system ($|K\rangle_B$) using the X base. If there is an error "t" is 1 and if there is not t is 0.
- To find α, Alice measures her system ($|K\rangle_A$). If $\alpha = 0$ then Charlie uses the wrong base for the measurement and we have a Phase error rate. If $\alpha = 1$ Charlie uses the same base and we have a Bit error rate.

Following this assumption, the number of events that we have a phase error denoted as δ_{ph}, is equal to $\delta_{ph} = \gamma(t = 1|\alpha = 0)$. Similarly, the number of events we have bit errors are $\delta_{bit} = \gamma(t = 1|\alpha = 1)$. Below, there is going to be an analysis on some equations that we need in order to bound the bit and phase error rates, using the help of [15, 16].

Easily we can assume that as the protocol uses only two bases, the number of measurement events with phase error is going to be approximately half of the total.

$$\gamma(\alpha = 0) \approx 1/2 \ .$$

Another useful equation can be found if we try to find the total number of events that Bobs measurement gives an error (t=1). And can be approximately assumed that it is the half of the total bit and phase error rates.

$$\gamma(t = 1) \approx \frac{\delta_{bit} + \delta_{ph}}{2} \ . \tag{6.3}$$

Two more useful equations are:

$$\gamma(a = 1|t = 1) \approx \frac{\delta_{bit}}{\delta_{bit} + \delta_{ph}}$$
$$\gamma(a = 0|t = 0) \approx \frac{1 - \delta_{bit}}{2 - \delta_{bit} - \delta_{ph}} \ . \tag{6.4}$$

Before we continue, it is essential to bound the total number of successful events in base X (γ_x) and Y (γ_y). At first let us write the possibility ρ as:

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

Now we can write that:

$$\begin{aligned}\langle X\rangle &= Tr(\rho X) = \gamma_x \\ \langle Y\rangle &= Tr(\rho Y) = \gamma_y \\ \langle Z\rangle &= Tr(\rho Z) = \gamma_z \ .\end{aligned}$$

And we know that:

$$\begin{aligned}&\gamma_x^2 + \gamma_y^2 + \gamma_z^2 \leq 1 \\ &\Rightarrow \gamma_x^2 + \gamma_y^2 \leq 1 - \gamma_z^2 \ .\end{aligned}$$

We also know that $\gamma_z^2 \leq 1$ and we conclude that:

$$\gamma_x^2 + \gamma_y^2 \leq 1 \ .$$

Another way to write the above equation is:

$$\langle X\rangle^2 + \langle Y\rangle^2 \leq 1 \ .$$

Keeping in mind that $\langle X\rangle$ can take values of either 1 or -1, we have:

$$\begin{aligned}&\langle X\rangle = 1Prob(-1) - 1Prob(1) \\ \Rightarrow &\langle X\rangle = (1 - Prob(1)) - 1Prob(1) \\ \Rightarrow &\langle X\rangle = 1 - 2Prob(1) \\ \Rightarrow &\langle X\rangle = 1 - 2\gamma \ ,\end{aligned}$$

when $Prob(1) = \gamma$ and:

$$Prob(1) + Prob(-1) = 1 \Rightarrow Prob(-1) = 1 - Prob(1) \ .$$

Combining all the above equations we get that:

$$(1 - 2\gamma_x)^2 + (1 - 2\gamma_y)^2 \leq 1 \ . \tag{6.5}$$

Last, we'll assume a parameter "Δ" that can be described as the possibility the measurement of the Quantum coin to be $|1_x\rangle$. The Quantum coin is measured along the X Base. What proposed before, can be written as $\| \langle 1_x|\Psi\rangle \|^2 = \Delta$. Knowing that, we can write:

$$\gamma(t=0)\gamma_x(a=1|t=0) + \gamma(t=1)\gamma_x(a=1|t=1) \approx \Delta \ . \tag{6.6}$$

If we use the equations 6.3, 6.4, 6.5 and 6.6, we conclude to the final equation that bounds the bit and phase error rates, of either the X or the Y base.

$$\sqrt{(1-\delta_{bit})(1-\delta_{ph})} + \sqrt{\delta_{bit}\cdot\delta_{ph}} \geq 1 - 2\Delta \ . \tag{6.7}$$

Finally, we have everything we need to write the equation of the Key Generation Rate (G) along the X basis.

$$G_x = \gamma_{x,suc} \cdot (1 - f(\delta_{x,bit})h(\delta_{x,bit}) - h(\delta_{y,ph})) \ . \tag{6.8}$$

Similarly we can write the Key Generation Rate along the Y basis, all we need to do is interchange the X base with the Y base parameters.

$$G_y = \gamma_{y,suc} \cdot (1 - f(\delta_{y,bit})h(\delta_{y,bit}) - h(\delta_{x,ph})) \ , \tag{6.9}$$

where γ_{suc} is the number of successful events, $h(\delta_{bit})$ is the rate of the sifted key that has to be sacrificed, in order to perform the error correcting code (in order to match Bob's key with Alice's), $f(\delta_{bit})$ is the inefficiency of the error correcting code and $h(\delta_p h)$ is the cost of performing privacy amplification.

7. PROPOSAL FOR A THREE USER MDI-QKD PROTOCOL

In this chapter, we'll propose an extension on the basic protocol, that allows a communication between a three member party. There is going to be a mention on its security and on the fact that a connection (between at least two members) can be established regardless of the base that the members use. First, we are going to focus our attention on the architecture of the protocol. The architecture of this protocol and the layout of Beam splitters that the Interference Unit needs, is displayed in figure 7.1.

As we now have three users that send pulses to Charlie, we need three detectors to satisfy all the different combinations on the MU. In accordance with the typical protocol these combinations denote the type of the detection.

7.1 Steps of a 3-party protocol

The steps that need to take place don't differ from the typical approach that was presented before and are shown below. As we have three members now, we'll name the first two members as Bob_1 and Bob_2 and the third as Alice.

1. As with the typical protocol, the three users prepare two different categories of pulses, the reference and the signal pulse. Then they randomly apply phase modulation on the signal pulse, choosing from four different phases (0, $\pi/2$, π, $3\pi/2$). These phases can be grouped into pairs, defining the two bases X (0, π) and Y ($\pi/2$, $3\pi/2$).
2. The party members send their pulses to Charlie that has a Measuring Unit (MU). Charlie performs measurements onto the pulses and announces if the measurements were successful or not. Also, if the measurement was successful, he announces the type of detection (0, 1, 2 or 3). In table 7.1 we color:
    - with light orange when we have a detection on detectors 2 and 3 (detection type 0).
    - with light red when we have a detection on detector 1 (detection type 1).
    - with light green when we have a detection on detector 2 (detection type 2).
    - with light blue when we have a detection on detector 3 (detection type 3).
3. In a scenario that the measurement was not successful the members discard their data and begin the process from step 1. If it was successful, they keep them and broadcast the bases they used. If their bases don't match, they discard them and begin from step 1 again. If their bases match, depending on the detection type and their bit value, they check if they need to perform a bit flip. The bit flip is done in regards to the bits of Alice (see table 7.1 for more information). After the bit flip procedure they create the sifted key.

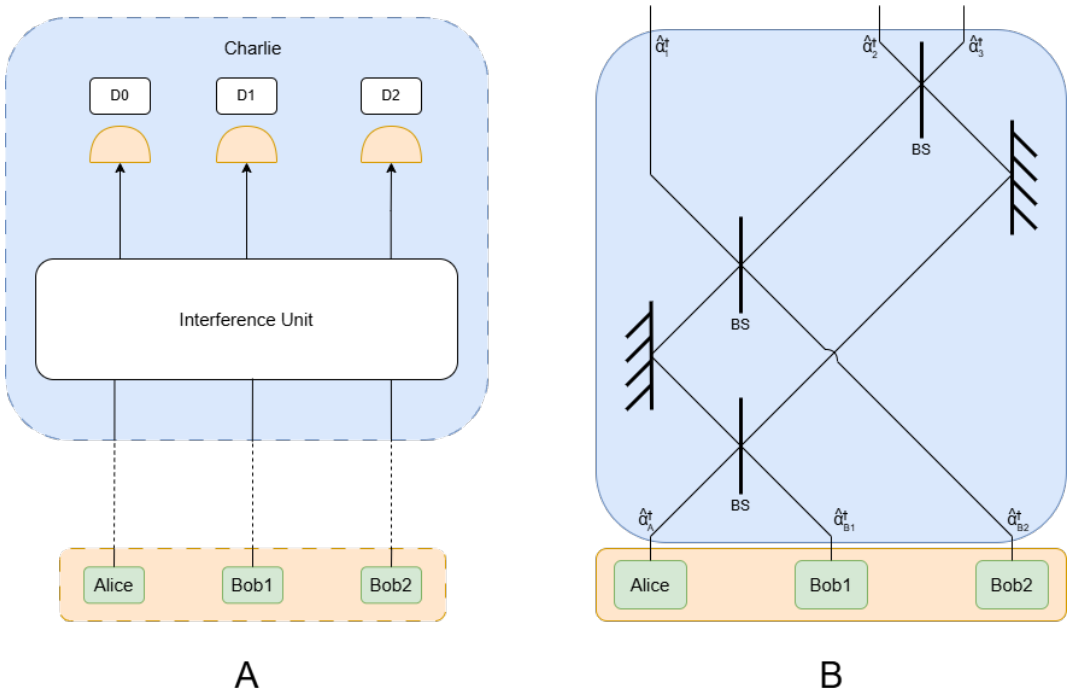

Figure 7.1: The architecture of the 3-Party Phase Encoding Scheme (A) and the structure of the Interference Unit (B).

4. The members continue to follow these three first steps until they create a sifted key that's large enough for their needs.

5. When they create the sifted key, they proceed to estimate two parameters of the channel, the Bit Error Rate (BER) and the Phase Error Rate with respect to Alice, as we explain in section 7.3. To achieve that, they use a piece of the sifted key and use it as the test bits for the BER estimation and estimate the phase error rate using the remaining bits. If these two parameters are too high, the party members abort the protocol.

In the pair-wise case (see section 7.4) the party members perform one last step. They choose on an error correcting code and a hash function that they will both use, depending on the values of the two parameters (BER and Phase Error Rate). Then, they perform error correction and privacy amplification before they finally share the key. In the case where all three users use the same base, this step can not be performed as we will explain in section 7.3.

7.2 Interference Unit and Bell State Measurement

One major component that had to be changed was the BS, as now we don't have two light pulses but three. For that reason, we need to replace it for an "Interference Unit". The

”Interference Unit” has to perform a three dimensional rotation on the three beams. The rotation matrix (R) that is used, is a rotation on each of the three axis in a three dimensional space. We use the Lie algebra orthogonal group as our rotation matrices.

$$L_x = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}, \quad L_y = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \quad L_z = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$R = e^X \cdot e^Y \cdot e^Z \tag{7.1}$$

,where e^X, e^Y, e^Z are the exponential matrices and $X = \pi/4L_x, Y = \pi/4L_y, Z = \pi/4L_z$

After the ”Interference Unit”, the three input pulses are rotated and give three output pulses. These output pulses can be easily found using the following equation.

$$\begin{pmatrix} \hat{\alpha}^\dagger_{B1} \\ \hat{\alpha}^\dagger_{B2} \\ \hat{\alpha}^\dagger_{A} \end{pmatrix} = R^T \cdot \begin{pmatrix} \hat{\alpha}^\dagger_{1} \\ \hat{\alpha}^\dagger_{2} \\ \hat{\alpha}^\dagger_{3} \end{pmatrix} \tag{7.2}$$

In Appendix B we give a detailed explanation on how to find the output beam equations using equation 7.2.

When the three pulses interfere in the BS, they create the state that follows:

$$|\alpha_{BS}\rangle = e^K e^{\sqrt{\mu}\hat{\Lambda}} |000\rangle \ , \tag{7.3}$$

where $K = -\frac{3\mu}{2}$ and $\hat{\Lambda} = e^{i\theta_{B1}}\hat{\alpha}^\dagger_{B1} + e^{i\theta_{B2}}\hat{\alpha}^\dagger_{B2} + e^{i\theta_A}\hat{\alpha}^\dagger_{A}$. Then Charlie performs a measurement onto the above state.

If all users send pulses in the same base, we have the table 7.1, that follows. In the table 7.1 we assumed that the users chose the base X (0, π) for their pulses. The results are exactly the same, if they had chosen base Y ($\frac{\pi}{2}$, $\frac{3\pi}{2}$). Also, by examining the table 7.1 we notice that the results do not disclose the value of the bit that was used during the making of the pulses by the users. A detailed analysis on the calculations of the table can be found in Appendix A.2.1.

7.3 Security of the three party protocol

At first, we wanted to prove the security of our proposed protocol taking into consideration and following the methodology that was presented in the previous section. Unfortunately, we faced some serious obstacles. The main reason was the lack of CSS codes for a three member QKD scheme. As explained in a previous chapter, without the help of CSS codes we are not able to perform the procedures of error correction and privacy amplification. And furthermore, the theory of entanglement distillation for three-partite entangled states is not fully developed.

Table 7.1: Results of the Bell State Measurements for three users, using the same base. Due to the small value of μ, we can only assume that in the results of the table, a detection can take place when the intensity of the pulse that arrives at the detector has a factor greater than 1.

User			Detector			Detection Type
B_1	B_2	A	D1	D2	D3	
0	0	0	$0.71\sqrt{\mu}$	$0.5\sqrt{\mu}$	$1.5\sqrt{\mu}$	**Type 3**
0	0	π	$0.71\sqrt{\mu}$	$1.5\sqrt{\mu}$	$0.5\sqrt{\mu}$	**Type 2**
0	π	0	$1.70\sqrt{\mu}$	$0.22\sqrt{\mu}$	$0.22\sqrt{\mu}$	**Type 1**
0	π	π	$0.32\sqrt{\mu}$	$1.20\sqrt{\mu}$	$1.20\sqrt{\mu}$	**Type 0**
π	0	0	$0.32\sqrt{\mu}$	$1.20\sqrt{\mu}$	$1.20\sqrt{\mu}$	**Type 0**
π	0	π	$1.70\sqrt{\mu}$	$0.22\sqrt{\mu}$	$0.22\sqrt{\mu}$	**Type 1**
π	π	0	$0.71\sqrt{\mu}$	$1.5\sqrt{\mu}$	$0.5\sqrt{\mu}$	**Type 2**
π	π	π	$0.71\sqrt{\mu}$	$0.5\sqrt{\mu}$	$1.5\sqrt{\mu}$	**Type 3**

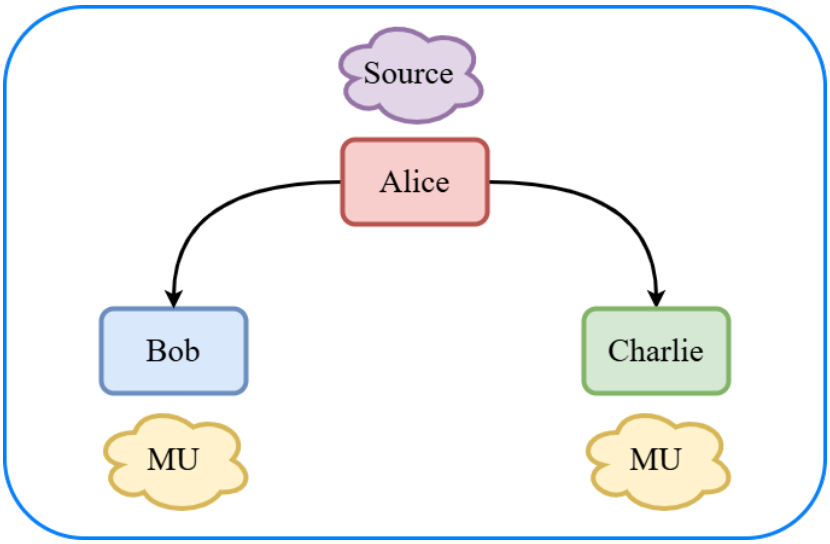

Figure 7.2: The architecture of the protocol [2], based on whom we prove the security of our 3-Party Phase Encoding protocol.

Due to the limitations that were described above we'll prove the security of our protocol using the method in Ref. [2]. Let us first perform a quick review on how this protocol works and how its security was proven. To begin with, we present the architecture of this protocol in figure 7.2.

This protocol is a typical prepare and measure CKA protocol. Below we present the steps.

1. Alice prepares the same sequence of 2n qubits and sends it to Bob and Charlie. This sequence can contain states from two bases ($|0\rangle$, $|1\rangle$) and ($|+\rangle$, $|-\rangle$) in a random manner.

2. Bob and Charlie receive the sequence and choose a basis ($|0\rangle, |1\rangle$) or ($|+\rangle, |-\rangle$) for the measurement. They do this process for each qubit independently. And the choice of the basis is independent between them.

3. Alice announces which basis she used for each qubit. Then, Bob and Charlie announce which basis they used for the measurement of that qubit. At the end of this process only the qubits that were prepared and measured with the same base are kept.

4. If the preparation and measurement of a qubit was in the basis ($|0\rangle, |1\rangle$), then Alice assigns:

   - bit 0 ($a_i = 0$) in the bit-stream when the qubit was $|0\rangle$
   - bit 1 ($a_i = 1$) when the qubit was $|1\rangle$

   Following the same method we can create Bob's bits:

   - bit 0 ($b_i = 0$) when we have the qubit $|0\rangle$

- bit 1 ($b_i = 1$) when we have the qubit $|1\rangle$

and Charlie's bits:

- bit 0 ($c_i = 0$) when we have the qubit $|0\rangle$
- bit 1 ($c_i = 1$) when we have the qubit $|1\rangle$

5. If the preparation and measurement of a qubit was in the basis ($|+\rangle, |-\rangle$), then Alice assigns:

   - bit 0 ($\alpha_i = 0$) in the bit-stream when the qubit was $|+\rangle$
   - bit 1 ($\alpha_i = 1$) when the qubit was $|-\rangle$.

   Exactly as before, we create Bob's bits:

   - bit 0 ($\beta_i = 0$) when we have the qubit $|+\rangle$
   - bit 1 ($\beta_i = 1$) when we have the qubit $|-\rangle$

   and Charlie's bits:

   - bit 0 ($\gamma_i = 0$) when we have the qubit $|+\rangle$
   - bit 1 ($\gamma_i = 1$) when we have the qubit $|-\rangle$.

   From this point forward we are going to describe the key generation process, using the bit-streams a, b and c of the base ($|0\rangle, |1\rangle$).

6. Alice randomly chooses half of the qubits that were transmitted on base ($|0\rangle, |1\rangle$), creating a subset denoted with S. Then, Alice, Bob and Charlie publicly announce their bits (a_i, b_i, c_i) and calculate their bit error rate using the following equation.

$$q_1 = max\left(\frac{B\_E_{(A-B)}}{S}, \frac{B\_E_{(A-C)}}{S}\right) , \tag{7.4}$$

   where $B\_E_{(A-B)}$ is the number of bit errors between Alice and Bob and $B\_E_{(A-C)}$ is the number of bit errors between Alice and Charlie.

7. Alice randomly chooses half of the qubits that were transmitted on base ($|+\rangle, |-\rangle$), creating a subset denoted with S'. Then, Alice, Bob and Charlie publicly announce their bits ($\alpha_i, \beta_i, \gamma_i$) and calculate their bit error rate using the following equation.

$$q_2 = \frac{B\_E_{(\alpha,\beta,\gamma)}}{S'} , \tag{7.5}$$

   where $B\_E_{(\alpha,\beta,\gamma)}$ is the number of bit errors that only two out of three users have a bit disagreement. Practically the total number of errors between the users.

8. Alice, Bob and Charlie agree on an error correcting (linear) code C_1.

9. Using a parity check matrix H_1 for the linear code C_1, a syndrome is created ($H_1\vec{a}$) and publicly announced by Alice. This syndrome can be used to find the position of the errors in the bit-stream. $\vec{a}$ is the vector containing the second half of the bits from step 4.

10. Bob and Charlie calculate their error vectors $\vec{f}$ and $\vec{f'}$ such that:

$$H_1\vec{f} = H_1\vec{b} - H_1\vec{a} \Rightarrow (\vec{b} - \vec{f} = \vec{a})$$
$$H_1\vec{f'} = H_1\vec{c} - H_1\vec{a} \Rightarrow (\vec{c} - \vec{f'} = \vec{a})$$

11. Finally, Alice chooses a subspace (C_2) of C_1, with dimensions nh(q_2), where h(...) is the binary entropy. Finding and using this subspace C_2 is crucial for the secret key generation rate.

Before we present the final equation for the key generation rate, we need to perform a quick review on the CSS code. As with the Ref. [2], we'll define the quantum state vector

$$|\vec{v}\rangle = |v_1\rangle \otimes |v_2\rangle \otimes ... \otimes |v_n\rangle$$

We have two binary linear codes C_1 and C_2, so we can write that:

$$\frac{1}{\sqrt{|C_2|}} \sum |\vec{v} + \vec{w}\rangle \ ,$$

where $\vec{v} \in C_1$, $\vec{w} \in C_2$ and $C_2 \subset C_1 \subset F_2^n$. F_2^n is the binary vector space on n bits.

If we parametrize the CSS code for $\vec{x}$ and $\vec{z}$, we have:

$$\frac{1}{\sqrt{|C_2|}} \sum (-1)^{(\vec{z}\cdot\vec{x})} |\vec{x} + \vec{v} + \vec{w}\rangle$$

We assume that a linear code has a length of n. In our protocol the bit-stream is of length 2n. For that reason we need a linear code CC of length 2n. So, now the parametrized CSS code is written as:

$$\frac{1}{\sqrt{|C_2|}} \sum (-1)^{(\vec{z}\cdot\vec{x})} |\vec{x} + \vec{v} + \vec{w}\rangle |\vec{x} + \vec{v} + \vec{w}\rangle$$

For a random $\vec{z}$ the above equation is written as:

$$\frac{1}{2^n|C_2|} \sum_{\vec{z}\in F_2^n} \left(\sum_{\vec{w_1}\in C_2} (-1)^{(\vec{z}\cdot\vec{w_1})} |\vec{x} + \vec{v} + \vec{w_1}\rangle |\vec{x} + \vec{v} + \vec{w_1}\rangle \right)$$
$$\times \left(\sum_{\vec{w_2}\in C_2} (-1)^{(\vec{z}\cdot\vec{w_2})} |\vec{x} + \vec{v} + \vec{w_2}\rangle |\vec{x} + \vec{v} + \vec{w_2}\rangle \right)$$
$$= \frac{1}{|C_2|} \sum_{\vec{w}\in C_2} |\vec{x} + \vec{v} + \vec{w}\rangle |\vec{x} + \vec{v} + \vec{w}\rangle \langle\vec{x} + \vec{v} + \vec{w}| \langle\vec{x} + \vec{v} + \vec{w}| \ ,$$

which is exactly the same argument as with reference [17]. We can easily write the above equation as:

$$\frac{1}{4^n}\sum_{\vec{x}\in F_2^n}\sum_{\vec{v}\in F_2^n}\rho(\vec{x},\vec{v}) = \frac{1}{2^n}\sum_{\vec{\alpha}\in F_2^n}|\vec{\alpha}\vec{\alpha}\rangle\langle\vec{\alpha}\vec{\alpha}| \ .$$

The second part of the above equation shows that the states $|00\rangle$ or $|11\rangle$ if we send them n times, have the same probability. And this is how Alice works in this protocol.

Here we conclude the theoretical analysis on the bit error rate and we'll proceed on the calculation of the phase error rate. We assume an H_2 parity check matrix for $C_2^{\perp}$ and then an H_2' parity check matrix for $(C_2C_2)^{\perp}$. Both H_2 and H_2' have dimensions of n-dim(C_2). Also, we assume a phase error:

$$Z^{z_1}\otimes Z^{z_2}\otimes ...\otimes Z^{z_{2n}} \ .$$

After the phase error correction process we know the quantity ($\vec{h_i}\vec{h_i},\vec{e}$), for i=1,...,$n-dim(C_2)$, where $\vec{e}=(z_1,z_2,...,z_{2n})\in F_2^n$. Now, we can consider a new phase error:

$$Z^{z_1'}\otimes Z^{z_2'}\otimes ...\otimes Z^{z_{2n}'}$$

that has the same effect onto the state if:

$$z_i+z_{n+i}=z_i'+z_{n+i}' \ .$$

Following this assumption, in order to correct the phase errors we need to find the binary vector:

$$\vec{e'}=(e_i+e_{n+i},...,e_n+e_{2n}) \ .$$

We can easily observe that:

$$(\vec{h_i}\vec{h_i},\vec{e})=(\vec{h_i},\vec{e'}) \ .$$

And as we know, finding $\vec{e'}$ from ($\vec{h_i},\vec{e'}$) is the decoding process of the linear code $C_2^{\perp}$. Also, the probability $e_i+e_{n+i}=1$ can be calculated from q_2.

Considering all of the above, we conclude that the SKR can be calculated from the below equation:

$$G=1-h(q_1)-h(q_2) \ , \tag{7.6}$$

where h() is the binary entropy, $h(q_1)$ is the amount of bits that we need for the error correction and $h(q_2)$ is the amount of bits for the privacy amplification.

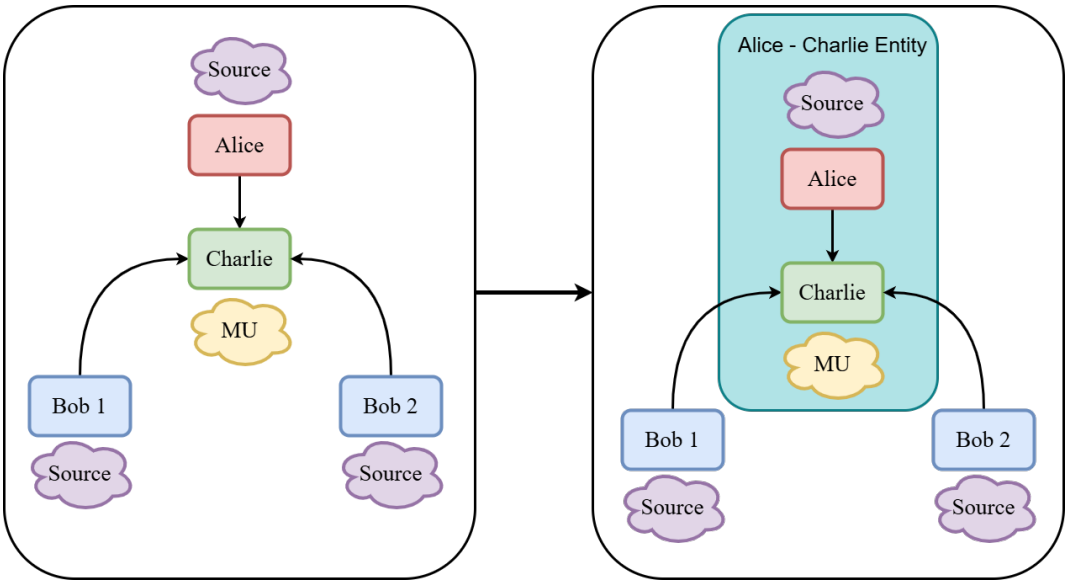

Figure 7.3: First assumption in order for our protocol to match with that of [2].

Having completed the review of the protocol Ref. [2], we are ready to apply this proof to the three-party MDI phase encoding protocol. Before we proceed, will have to take some assumptions so that there is a matching for the two protocols.

1. First, we take the assumption that the channel between Alice and Charlie has no errors. One way we can come close to this assumption is if we place Alice close enough to the MU (Charlie). Another way, would be if we placed Alice on the MU, this move though would transformed our protocol from an MDI, to a typical multiparty QKD protocol. Using this assumption, we can say that Alice and Charlie are virtually one entity, as shown in figure 7.3. This assumption was introduced to make every user perform error correction on the bit-stream of Alice, as was described in step 6 of the protocol.

2. Second, we have to reverse the way that the states are transmitted. Instead of going from the users (Bob_1 and Bob_2) to the MU (Charlie-Alice entity), they are transmitted the other way (from the Charlie-Alice entity to the users), as shown in figure 7.4.

3. Lastly, we need to make the bases (X and Y) indistinguishable from each other, in order to reduce the basis flaw. This can be quantified by a simple measure of distance between density matrices of the same degree of mixedness. A detailed analysis on the subject, is presented in appendix C that shows the relation of the basis flow and the intensity of the photons (μ). A graph on this relation is presented in figure 7.5.

Now that our protocol matches that of Ref. [2], we can easily implement the security proof that was described in this subsection and calculate the SKR using the equations 7.4, 7.5 and 7.6. Finally, we conclude that our protocol is indeed secure.

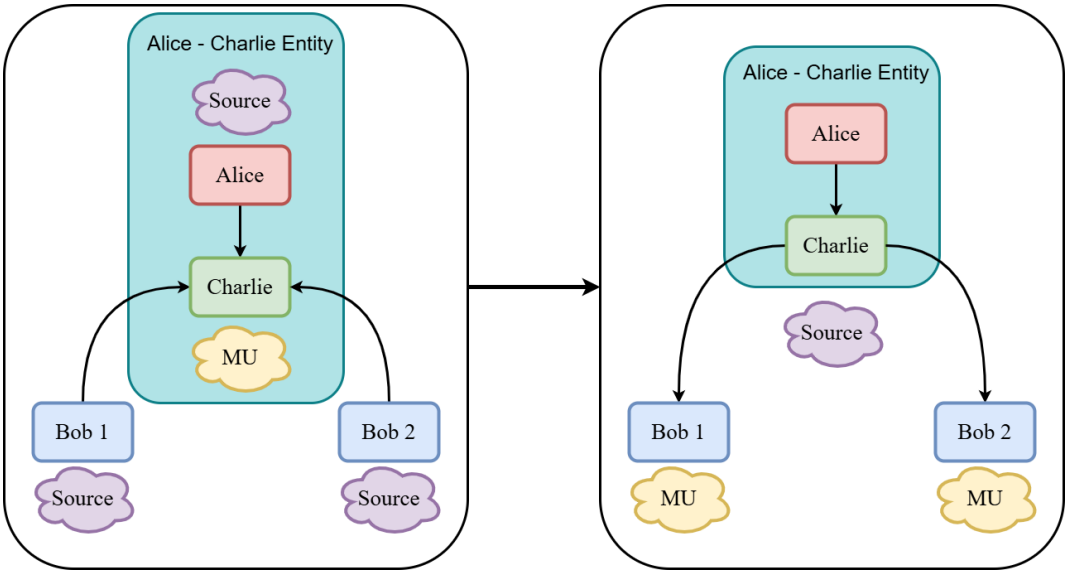

Figure 7.4: Second assumption in order for our protocol to match with that of [2].

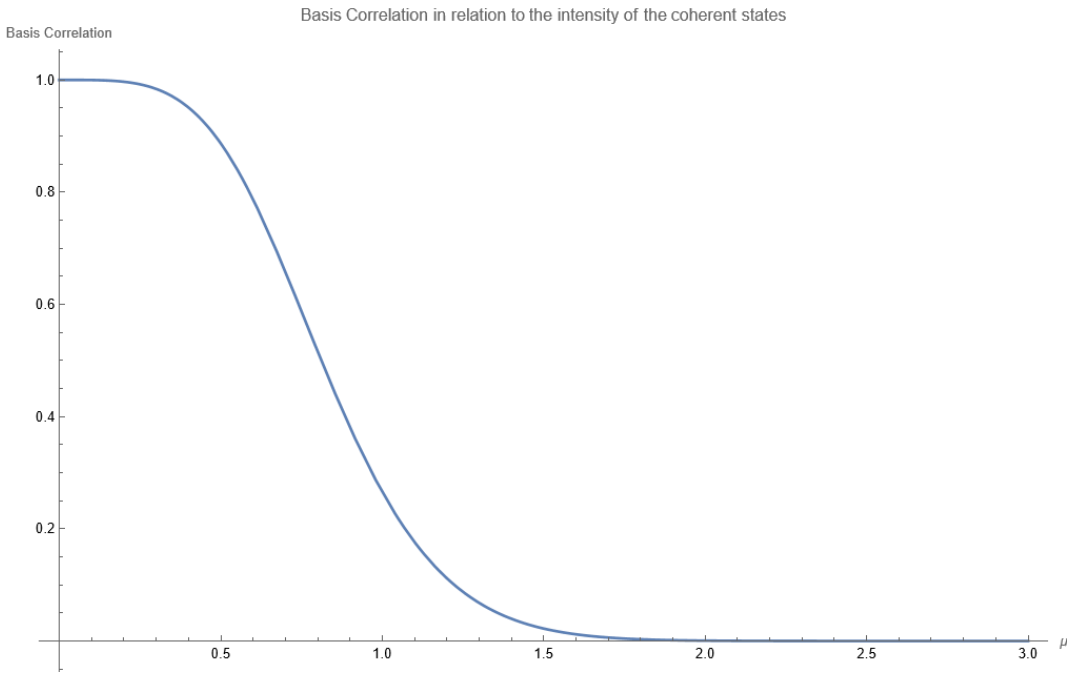

Figure 7.5: Presentation of the Basis correlation in relation to the intensity of the coherent states.

7.4 Pair-wise QKD with the proposed setting

In case we have two users transmitting in the same base and a third transmitting in a different one, this protocol can establish a connection between those two with the same base. Using the Equation 7.3, as before, we present a table that underlines a pairwise QKD scheme. We present in the table (7.2) below, the results when two users transmit in the base X and one in the base Y (left table) and when two users transmit in the base Y and one in the base X (right table).

Table 7.2: Results of the Bell State Measurements for three users, in the pair-wise case.

User			Detector			User			Detector		
B_1	B_2	A	D1	D2	D3	B_1	B_2	A	D1	D2	D3
0	0	$\frac{\pi}{2}$	$0.71\sqrt{\mu}$	$1.12\sqrt{\mu}$	$1.12\sqrt{\mu}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	$0.55\sqrt{\mu}$	$0.92\sqrt{\mu}$	$1.36\sqrt{\mu}$
0	π	$\frac{\pi}{2}$	$1.22\sqrt{\mu}$	$0.87\sqrt{\mu}$	$0.87\sqrt{\mu}$	$\frac{\pi}{2}$	$\frac{3\pi}{2}$	0	$1.3\sqrt{\mu}$	$1.1\sqrt{\mu}$	$0.39\sqrt{\mu}$
π	0	$\frac{\pi}{2}$	$1.22\sqrt{\mu}$	$0.87\sqrt{\mu}$	$0.87\sqrt{\mu}$	$\frac{3\pi}{2}$	$\frac{\pi}{2}$	0	$1.3\sqrt{\mu}$	$1.1\sqrt{\mu}$	$0.39\sqrt{\mu}$
π	π	$\frac{\pi}{2}$	$0.71\sqrt{\mu}$	$1.12\sqrt{\mu}$	$1.12\sqrt{\mu}$	$\frac{3\pi}{2}$	$\frac{3\pi}{2}$	0	$0.55\sqrt{\mu}$	$0.92\sqrt{\mu}$	$1.36\sqrt{\mu}$
0	0	$\frac{3\pi}{2}$	$0.71\sqrt{\mu}$	$1.12\sqrt{\mu}$	$1.12\sqrt{\mu}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	π	$0.55\sqrt{\mu}$	$0.92\sqrt{\mu}$	$1.36\sqrt{\mu}$
0	π	$\frac{3\pi}{2}$	$1.22\sqrt{\mu}$	$0.87\sqrt{\mu}$	$0.87\sqrt{\mu}$	$\frac{\pi}{2}$	$\frac{3\pi}{2}$	π	$1.3\sqrt{\mu}$	$1.1\sqrt{\mu}$	$0.39\sqrt{\mu}$
π	0	$\frac{3\pi}{2}$	$1.22\sqrt{\mu}$	$0.87\sqrt{\mu}$	$0.87\sqrt{\mu}$	$\frac{3\pi}{2}$	$\frac{\pi}{2}$	π	$1.3\sqrt{\mu}$	$1.1\sqrt{\mu}$	$0.39\sqrt{\mu}$
π	π	$\frac{3\pi}{2}$	$0.71\sqrt{\mu}$	$1.12\sqrt{\mu}$	$1.12\sqrt{\mu}$	$\frac{3\pi}{2}$	$\frac{3\pi}{2}$	π	$0.55\sqrt{\mu}$	$0.92\sqrt{\mu}$	$1.36\sqrt{\mu}$

In table 7.2 when two users transmit in base X we have the following two types of detection:

1. **Detection type 0**: When we have a detection on detectors 2 and 3 (colored with blue).
2. **Detection type 1**: When we have a detection on detector 1 (colored with light blue).

If the users transmit in base Y we have the following two types of detection:

1. **Detection type 0**: When we have a detection on detector 3 (colored with blue).
2. **Detection type 1**: When we have a detection on detectors 1 and 2 (colored with light blue).

The above results are the same regardless of which two users use the same base. It can be Bob_1 and Bob_2, Bob_1 and Alice or Bob_2 and Alice.

7.5 Security in the pair-wise case

To prove the security of the pair-wise scenario of our protocol, we can easily compare it to the proof of the typical MDI protocol (Section 6.3.3). As we can observe that both protocols are exactly the same, from the number of members that will create a secret key to the implementation of the key generation procedure.

8. CONCLUSIONS

In this thesis, we have introduced and analyzed a multi-user MDI-QKD phase encoding protocol. Our work extends the current understanding and capabilities of QKD by addressing the complexities associated with multi-user scenarios and providing a robust framework for secure key distribution among three parties.

Firstly, we proposed an innovative phase encoding protocol designed to distribute a common key among three users. This protocol was constructed with the goal of maintaining high security standards while accommodating the practical constraints of multi-user QKD systems.

Our analysis demonstrated that the proposed protocol functions effectively when all users employ the same basis. We further extended our investigation to scenarios where only two of the three users use the same basis, showing that the protocol remains functional and secure under these conditions. This flexibility is crucial for practical implementations where synchronization and coordination among multiple users can pose significant challenges.

For the scenario where all three users use the same basis, we established security by comparing and transforming our protocol to another multiparty MDI-QKD protocol [2] without entanglement that fitted our needs. This comparative analysis underscored the robustness of our approach, confirming that it provides the expected security guarantees.

In the case where only two users use the same basis, we demonstrated security by drawing parallels with the typical phase encoding protocol [5]. By leveraging well-established security principles from typical QKD, we ensured that our multi-user protocol inherits the strong security properties necessary for reliable key distribution.

The contributions of this thesis are multifaceted: we not only introduced a new protocol but also provided comprehensive security proofs for different operational scenarios, thereby paving the way for practical and secure multi-user QKD implementations. Our work addresses key challenges in the field and sets the stage for future research to build upon these foundations, exploring further expansion on the number of users, while keeping the communication secure.

ABBREVIATIONS - ACRONYMS

QKD	Quantum Key Distribution
DD	Device Dependent
SDI	Source Device Independent
MDI	Measurement Device Independent
MU	Measurement Unit
TF	Twin Field
QCKA	Quantum Conference Key Agreement
SKR	Secure Key Rate
HOM	Hong-Ou-Mandel
BSM	Bell State Measurement
BS	Beam Splitter
APDs	Avalanche Photodiodes
WCS	Weak Coherent State
PM	Phase Modulator
IM	Intensity Modulator
SPDs	Single Photon Detectors
PBSs	Polarizing Beam Splitters
PolM	Polarization Modulator
BER	Bit Error Rate

APPENDIX A. DETAILED CALCULATIONS ON MEASUREMENT OUTCOMES

In this Appendix, we will write in depth the calculations of the BSMs in the cases of a two member and three member phase encoding MDI-QKD protocol. Before we continue we'll introduce the Euler's formula, as it will be very useful in the calculations below. The Euler's formula is written as:

$$e^{i\theta} = \cos\theta + i\sin\theta$$

For the various values of θ, we have:

$$\begin{aligned}
\theta = 0 &\Rightarrow e^{i\theta} = 1 \\
\theta = \pi &\Rightarrow e^{i\theta} = -1 \\
\theta = \frac{\pi}{2} &\Rightarrow e^{i\theta} = i \\
\theta = \frac{3\pi}{2} &\Rightarrow e^{i\theta} = -i
\end{aligned}$$

A.1 Two member phase encoding MDI-QKD

In this section we'll give the equations that produce the results of Table 6.1. First, we'll use the equation 4.7, that gives the state that Charlie has after the pulses of Bob and Alice interfere. The first we'll explore what happens if both Alice and Bob sent pulses in the same basis.

1. Base X ($0, \pi$):
   - If Alice and Bob chose phase 0 ($\theta_A = 0$, $\theta_B = 0$):

$$\begin{aligned}
|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(1\cdot(\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger) + 1\cdot(-\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger))} |00\rangle \\
&= e^{-\mu} e^{\sqrt{2\mu}\hat{\alpha}_1^\dagger} |00\rangle
\end{aligned}$$

     - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{2\mu}$.
     - No signal arriving at Detector 0.
   - If Alice and Bob chose phase π ($\theta_A = \pi$, $\theta_B = \pi$):

$$\begin{aligned}
|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-1)\cdot(\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger) + (-1)\cdot(-\hat{\alpha}_0^\dagger + \hat{\alpha}_1^\dagger))} |00\rangle \\
&= e^{-\mu} e^{\sqrt{2\mu}\hat{\alpha}_1^\dagger} |00\rangle
\end{aligned}$$

    - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{2\mu}$.
    - No signal arriving at Detector 0.
- If Alice chose phase 0 ($\theta_A = 0$) and Bob chose phase π ($\theta_B = \pi$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(1\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-1)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{2\mu}\hat{\alpha}_0^\dagger}|00\rangle\end{aligned}$$

    - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{2\mu}$.
    - No signal arriving at Detector 1.
- If Alice chose phase π ($\theta_A = \pi$) and Bob chose phase 0 ($\theta_B = 0$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-1)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+1\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{2\mu}\hat{\alpha}_0^\dagger}|00\rangle\end{aligned}$$

    - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{2\mu}$.
    - No signal arriving at Detector 1.

2. Base Y ($\frac{\pi}{2}$, $\frac{3\pi}{2}$):

- If Alice and Bob chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$, $\theta_B = \frac{\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(i\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+i\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{i\sqrt{2\mu}\hat{\alpha}_1^\dagger}|00\rangle\end{aligned}$$

    - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{2\mu}$.
    - No signal arriving at Detector 0.
- If Alice and Bob chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$, $\theta_B = \frac{3\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-i)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-i)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{i\sqrt{2\mu}\hat{\alpha}_1^\dagger}|00\rangle\end{aligned}$$

    - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{2\mu}$.
    - No signal arriving at Detector 0.
- If Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$) and Bob chose phase $\frac{3\pi}{2}$ ($\theta_B = \frac{3\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(i\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-i)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{2\mu}\hat{\alpha}_0^\dagger}|00\rangle\end{aligned}$$

    - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{2\mu}$.
    - No signal arriving at Detector 1.

- If Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$) and Bob chose phase $\frac{\pi}{2}$ ($\theta_B = \frac{\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-i)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+i\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))} |00\rangle \\ &= e^{-\mu} e^{\sqrt{2\mu}\hat{\alpha}_0^\dagger} |00\rangle\end{aligned}$$

  - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{2\mu}$.
  - No signal arriving at Detector 1.

Now, we'll write the equations if the two users chose different bases:

1. Alice in base X (0, π) and Bob in base Y ($\frac{\pi}{2}$, $\frac{3\pi}{2}$):

   - If Alice chose phase 0 ($\theta_A = 0$) and Bob chose phase $\frac{\pi}{2}$ ($\theta_B = \frac{\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(1\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+i\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))} |00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(\hat{\alpha}_0^\dagger(1-i)+\hat{\alpha}_1^\dagger(1+i))} |00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}(1-i)\hat{\alpha}_0^\dagger+\frac{\sqrt{2}}{2}(1+i)\hat{\alpha}_1^\dagger)} |00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.
   - If Alice chose phase 0 ($\theta_A = 0$) and Bob chose phase $\frac{3\pi}{2}$ ($\theta_B = \frac{3\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(1\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-i)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))} |00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(\hat{\alpha}_0^\dagger(1+i)+\hat{\alpha}_1^\dagger(1-i))} |00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}(1+i)\hat{\alpha}_0^\dagger+\frac{\sqrt{2}}{2}(1-i)\hat{\alpha}_1^\dagger)} |00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.
   - If Alice chose phase π ($\theta_A = \pi$) and Bob chose phase $\frac{\pi}{2}$ ($\theta_B = \frac{\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-1)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+i\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))} |00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(-\hat{\alpha}_0^\dagger(i+1)+\hat{\alpha}_1^\dagger(i-1))} |00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(-\frac{\sqrt{2}}{2}(i+1)\hat{\alpha}_0^\dagger+\frac{\sqrt{2}}{2}(i-1)\hat{\alpha}_1^\dagger)} |00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.
   - If Alice chose phase π ($\theta_A = \pi$) and Bob chose phase $\frac{3\pi}{2}$ ($\theta_B = \frac{3\pi}{2}$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-1)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-i)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))} |00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(\hat{\alpha}_0^\dagger(i-1)-\hat{\alpha}_1^\dagger(i+1))} |00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}(i-1)\hat{\alpha}_0^\dagger-\frac{\sqrt{2}}{2}(i+1)\hat{\alpha}_1^\dagger)} |00\rangle\end{aligned}$$

- A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
- A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.

2. Alice in base Y ($\frac{\pi}{2}$, $\frac{3\pi}{2}$) and Bob in base X (0, π):

   - If Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$) and Bob chose phase 0 ($\theta_B = 0$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(i\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+1\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(\hat{\alpha}_0^\dagger(i-1)+\hat{\alpha}_1^\dagger(i+1))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}(i-1)\hat{\alpha}_0^\dagger+\frac{\sqrt{2}}{2}(i+1)\hat{\alpha}_1^\dagger)}|00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.
   - If Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$) and Bob chose phase π ($\theta_B = \pi$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(i\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-1)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(\hat{\alpha}_0^\dagger(i+1)+\hat{\alpha}_1^\dagger(i-1))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}(i+1)\hat{\alpha}_0^\dagger+\frac{\sqrt{2}}{2}(i-1)\hat{\alpha}_1^\dagger)}|00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.
   - If Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$) and Bob chose phase 0 ($\theta_B = 0$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-i)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+1\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(-\hat{\alpha}_0^\dagger(1+i)+\hat{\alpha}_1^\dagger(1-i))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(-\frac{\sqrt{2}}{2}(1+i)\hat{\alpha}_0^\dagger+\frac{\sqrt{2}}{2}(1-i)\hat{\alpha}_1^\dagger)}|00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.
   - If Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$) and Bob chose phase π ($\theta_B = \pi$):

$$\begin{aligned}|\alpha_C\rangle &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}((-i)\cdot(\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger)+(-1)\cdot(-\hat{\alpha}_0^\dagger+\hat{\alpha}_1^\dagger))}|00\rangle \\ &= e^{-\mu} e^{\frac{\sqrt{2\mu}}{2}(\hat{\alpha}_0^\dagger(1-i)-\hat{\alpha}_1^\dagger(1+i))}|00\rangle \\ &= e^{-\mu} e^{\sqrt{\mu}(\frac{\sqrt{2}}{2}(1-i)\hat{\alpha}_0^\dagger-\frac{\sqrt{2}}{2}(1+i)\hat{\alpha}_1^\dagger)}|00\rangle\end{aligned}$$

     - A signal arriving at Detector 0 ($\hat{\alpha}_0^\dagger$) with intensity $\sqrt{\mu}$.
     - A signal arriving at Detector 0 ($\hat{\alpha}_1^\dagger$) with intensity $\sqrt{\mu}$.

A.2 Three member phase encoding MDI-QKD

Using equation 7.3 and those of Appendix B we will calculate the parameter $\hat{\Lambda}$, for the various phases, to find the intensity on each detector.

A.2.1 Three user communication

If all three users chose the same base, for example Base X (0, π), we have:

- If Alice, Bob$_1$, Bob$_2$ chose phase 0 ($\theta_A = \theta_{B_1} = \theta_{B_2} = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} - \frac{1}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(1 - \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(1 + \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \frac{\sqrt{2}}{2}\hat{\alpha}_1^\dagger + \frac{1}{2}\hat{\alpha}_2^\dagger + \frac{3}{2}\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.5\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.5\sqrt{\mu}$.

- If Alice chose phase π ($\theta_A = \pi$) and Bob$_1$, Bob$_2$ chose phase 0 ($\theta_{B_1} = \theta_{B_2} = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} - \frac{1}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(1 + \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(1 - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\frac{1}{\sqrt{2}}\hat{\alpha}_1^\dagger + \frac{3}{2}\hat{\alpha}_2^\dagger + \frac{1}{2}\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.5\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.5\sqrt{\mu}$.

- If Alice and Bob$_1$ chose phase 0 ($\theta_A = \theta_{B_1} = 0$) and Bob$_2$ chose phase π ($\theta_{B_2} = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} + \frac{1}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(1 - \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{1}{2} - 1\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}+1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{2-\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger - \left(\frac{2-\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

- ∗ A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.70\sqrt{\mu}$.
- ∗ A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.222\sqrt{\mu}$.
- ∗ A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.22\sqrt{\mu}$.

- If Alice and Bob$_2$ chose phase π ($\theta_A = \theta_{B_2} = \pi$) and Bob$_1$ chose phase 0 ($\theta_{B_1} = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} + \frac{1}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{1}{\sqrt{2}} + \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(-\frac{1}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}-1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{2+\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger - \left(\frac{2+\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - ∗ A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.32\sqrt{\mu}$.
  - ∗ A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.20\sqrt{\mu}$.
  - ∗ A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.20\sqrt{\mu}$.

- If Alice and Bob$_2$ chose phase 0 ($\theta_A = \theta_{B_2} = 0$) and Bob$_1$ chose phase π ($\theta_{B_1} = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} - \frac{1}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(-\frac{1}{\sqrt{2}} + \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{1-\sqrt{2}}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{2+\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{2+\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - ∗ A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.32\sqrt{\mu}$.
  - ∗ A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.20\sqrt{\mu}$.
  - ∗ A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.20\sqrt{\mu}$.

- If Alice and Bob$_1$ chose phase π ($\theta_A = \theta_{B_1} = \pi$) and Bob$_2$ chose phase 0 ($\theta_{B_2} = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} - \frac{1}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{1}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}+1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{\sqrt{2}-2}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{2-\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - ∗ A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.70\sqrt{\mu}$.
  - ∗ A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.22\sqrt{\mu}$.
  - ∗ A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.22\sqrt{\mu}$.

- If Alice chose phase 0 ($\theta_A = 0$) and Bob$_1$, Bob$_2$ chose phase π ($\theta_{B_1} = \theta_{B_2} = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} + \frac{1}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(1 + \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{1}{2} - 1\right)\hat{\alpha}_3^\dagger \\ &= \frac{1}{\sqrt{2}}\hat{\alpha}_1^\dagger - \frac{3}{2}\hat{\alpha}_2^\dagger + \frac{1}{2}\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.5\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.5\sqrt{\mu}$.

- If Alice, Bob$_1$, Bob$_2$ chose phase π ($\theta_A = \theta_{B_1} = \theta_{B_2} = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} + \frac{1}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(1 - \frac{1}{2}\right)\hat{\alpha}_2^\dagger - \left(1 + \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\frac{\sqrt{2}}{2}\hat{\alpha}_1^\dagger - \frac{1}{2}\hat{\alpha}_2^\dagger - \frac{3}{2}\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.5\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.5\sqrt{\mu}$.

It can be easily proven that the results in the Y base are exactly the same as in the X base, if we add the imaginary i before each $\hat{\alpha}^\dagger$.

A.2.2 Pair-wise case

In the pair-wise case, we follow the same procedure as before, with the difference that one of the users is in the ”wrong” base. Starting with two users in base X and one in base Y, we have:

- If Bob$_1$ and Bob$_2$ chose phase 0 ($\theta_{B_1} = \theta_{B_2} = 0$) and Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} - \frac{1}{2} + \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(1 - \frac{i}{2}\right)\hat{\alpha}_2^\dagger + \left(1 + \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= \frac{i}{\sqrt{2}}\hat{\alpha}_1^\dagger + \left(\frac{2-i}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{2+i}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.12\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.12\sqrt{\mu}$.

- If Bob$_1$ chose phase 0 ($\theta_{B_1} = 0$), Bob$_2$ chose phase π ($\theta_{B_2} = \pi$) and Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} + \frac{1}{2} + \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{1}{\sqrt{2}} - \frac{i}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{1}{\sqrt{2}} + \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}+i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{2-i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger - \left(\frac{2-i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.22\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.87\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.87\sqrt{\mu}$.

- If Bob$_1$ chose phase π ($\theta_{B_1} = \pi$), Bob$_2$ chose phase 0 ($\theta_{B_2} = 0$) and Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} - \frac{1}{2} + \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{1}{\sqrt{2}} + \frac{i}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{1}{\sqrt{2}} + \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{i-\sqrt{2}}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{2+i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{2+i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.22\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.87\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.87\sqrt{\mu}$.

- If Bob$_1$ and Bob$_2$ chose phase π ($\theta_{B_1} = \theta_{B_2} = \pi$) and Alice chose phase $\frac{\pi}{2}$ ($\theta_A = \frac{\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} + \frac{1}{2} + \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(1 + \frac{i}{2}\right)\hat{\alpha}_2^\dagger - \left(1 - \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= \frac{i}{\sqrt{2}}\hat{\alpha}_1^\dagger - \left(\frac{2+i}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{2-i}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.

- A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.12\sqrt{\mu}$.
- A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.12\sqrt{\mu}$.

- If Bob$_1$ and Bob$_2$ chose phase 0 ($\theta_{B_1} = \theta_{B_2} = 0$) and Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} - \frac{1}{2} - \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(1 + \frac{i}{2}\right)\hat{\alpha}_2^\dagger + \left(1 - \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\frac{i}{\sqrt{2}}\hat{\alpha}_1^\dagger + \left(\frac{2+i}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{2-i}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.12\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.12\sqrt{\mu}$.

- If Bob$_1$ chose phase 0 ($\theta_{B_1} = 0$), Bob$_2$ chose phase π ($\theta_{B_2} = \pi$) and Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{1}{2} + \frac{1}{2} - \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{1}{\sqrt{2}} + \frac{i}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{1}{\sqrt{2}} + \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}-i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{2+i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger - \left(\frac{2+i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.22\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.87\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.87\sqrt{\mu}$.

- If Bob$_1$ chose phase π ($\theta_{B_1} = \pi$), Bob$_2$ chose phase 0 ($\theta_{B_2} = 0$) and Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} - \frac{1}{2} - \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{1}{\sqrt{2}} - \frac{i}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{1}{\sqrt{2}} - \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\left(\frac{\sqrt{2}+i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{2-i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{2-i\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.22\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.87\sqrt{\mu}$.

    - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.87\sqrt{\mu}$.

- If Bob$_1$ and Bob$_2$ chose phase π ($\theta_{B_1} = \theta_{B_2} = \pi$) and Alice chose phase $\frac{3\pi}{2}$ ($\theta_A = \frac{3\pi}{2}$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{1}{2} + \frac{1}{2} - \frac{i}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(1 - \frac{i}{2}\right)\hat{\alpha}_2^\dagger - \left(1 + \frac{i}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\frac{i}{\sqrt{2}}\hat{\alpha}_1^\dagger - \left(\frac{2-i}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{2+i}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

    - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.71\sqrt{\mu}$.
    - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.12\sqrt{\mu}$.
    - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.12\sqrt{\mu}$.

If we study the case where we have two users in base Y and one in base X, we have:

- If Bob$_1$ and Bob$_2$ chose phase $\frac{\pi}{2}$ ($\theta_{B_1} = \theta_{B_2} = \frac{\pi}{2}$) and Alice chose phase 0 ($\theta_A = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{i}{2} - \frac{i}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(i - \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(i + \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \frac{1}{\sqrt{2}}\hat{\alpha}_1^\dagger + \left(\frac{2i-1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{2i+1}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

    - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.55\sqrt{\mu}$.
    - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.92\sqrt{\mu}$.
    - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.36\sqrt{\mu}$.

- If Bob$_1$ chose phase $\frac{\pi}{2}$ ($\theta_{B_1} = \frac{\pi}{2}$), Bob$_2$ chose phase $\frac{3\pi}{2}$ ($\theta_{B_2} = \frac{3\pi}{2}$) and Alice chose phase 0 ($\theta_A = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{i}{2} + \frac{i}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{i}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{i}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}i+1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{2i-\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger - \left(\frac{2i-\sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

    - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.3\sqrt{\mu}$.
    - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.1\sqrt{\mu}$.
    - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.39\sqrt{\mu}$.

- If Bob$_1$ chose phase $\frac{3\pi}{2}$ ($\theta_{B_1} = \frac{3\pi}{2}$), Bob$_2$ chose phase $\frac{\pi}{2}$ ($\theta_{B_2} = \frac{\pi}{2}$) and Alice chose phase 0 ($\theta_A = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{i}{2} - \frac{i}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{i}{\sqrt{2}} + \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{i}{\sqrt{2}} + \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{1 - i\sqrt{2}}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{2i - \sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{2i - \sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.3\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.1\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.39\sqrt{\mu}$.

- If Bob$_1$ and Bob$_2$ chose phase $\frac{3\pi}{2}$ ($\theta_{B_1} = \theta_{B_2} = \frac{3\pi}{2}$) and Alice chose phase 0 ($\theta_A = 0$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{i}{2} + \frac{i}{2} + \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(i + \frac{1}{2}\right)\hat{\alpha}_2^\dagger - \left(i - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \frac{1}{\sqrt{2}}\hat{\alpha}_1^\dagger - \left(\frac{2i + 1}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{2i - 1}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.55\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.92\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.36\sqrt{\mu}$.

- If Bob$_1$ and Bob$_2$ chose phase $\frac{\pi}{2}$ ($\theta_{B_1} = \theta_{B_2} = \frac{\pi}{2}$) and Alice chose phase π ($\theta_A = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{i}{2} - \frac{i}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(i + \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(i - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\frac{1}{\sqrt{2}}\hat{\alpha}_1^\dagger + \left(\frac{2i + 1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{2i - 1}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  - A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.55\sqrt{\mu}$.
  - A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.92\sqrt{\mu}$.
  - A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.36\sqrt{\mu}$.

- If Bob$_1$ chose phase $\frac{\pi}{2}$ ($\theta_{B_1} = \frac{\pi}{2}$), Bob$_2$ chose phase $\frac{3\pi}{2}$ ($\theta_{B_2} = \frac{3\pi}{2}$) and Alice chose phase π ($\theta_A = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(\frac{i}{2} + \frac{i}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{i}{\sqrt{2}} + \frac{1}{2}\right)\hat{\alpha}_2^\dagger - \left(\frac{i}{\sqrt{2}} + \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= \left(\frac{\sqrt{2}i - 1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger + \left(\frac{2i + \sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger - \left(\frac{2i + \sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  * A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.3\sqrt{\mu}$.
  * A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.1\sqrt{\mu}$.
  * A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.39\sqrt{\mu}$.

- If Bob$_1$ chose phase $\frac{3\pi}{2}$ ($\theta_{B_1} = \frac{3\pi}{2}$), Bob$_2$ chose phase $\frac{\pi}{2}$ ($\theta_{B_2} = \frac{\pi}{2}$) and Alice chose phase π ($\theta_A = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{i}{2} - \frac{i}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{i}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{i}{\sqrt{2}} - \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\left(\frac{\sqrt{2}i + 1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(\frac{2i - \sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_2^\dagger + \left(\frac{2i - \sqrt{2}}{2\sqrt{2}}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  * A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $1.3\sqrt{\mu}$.
  * A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $1.1\sqrt{\mu}$.
  * A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $0.39\sqrt{\mu}$.

- If Bob$_1$ and Bob$_2$ chose phase $\frac{3\pi}{2}$ ($\theta_{B_1} = \theta_{B_2} = \frac{3\pi}{2}$) and Alice chose phase π ($\theta_A = \pi$):

$$\begin{aligned}\hat{\Lambda} &= \left(-\frac{i}{2} + \frac{i}{2} - \frac{1}{\sqrt{2}}\right)\hat{\alpha}_1^\dagger - \left(i - \frac{1}{2}\right)\hat{\alpha}_2^\dagger - \left(i + \frac{1}{2}\right)\hat{\alpha}_3^\dagger \\ &= -\frac{1}{\sqrt{2}}\hat{\alpha}_1^\dagger - \left(\frac{2i - 1}{2}\right)\hat{\alpha}_2^\dagger + \left(\frac{2i + 1}{2}\right)\hat{\alpha}_3^\dagger\end{aligned}$$

  If we replace this $\hat{\Lambda}$ in equation 7.3 we get:

  * A signal arriving at Detector 1 ($\hat{\alpha}_1^\dagger$) with intensity $0.55\sqrt{\mu}$.
  * A signal arriving at Detector 2 ($\hat{\alpha}_2^\dagger$) with intensity $0.92\sqrt{\mu}$.
  * A signal arriving at Detector 3 ($\hat{\alpha}_3^\dagger$) with intensity $1.36\sqrt{\mu}$.

APPENDIX B. CALCULATIONS FOR THE DESIGN OF THE INTERFERENCE UNIT

Using the rotation matrix that was proposed in section 7.2, we will present the necessary calculation, in order to find the output beam coefficients of the interference unit. First, we'll start with equation 7.1:

$$R = e^X \cdot e^Y \cdot e^Z$$

,where e^X, e^Y, e^Z are the exponential matrices and $X = \pi/4L_x, Y = \pi/4L_y, Z = \pi/4L_z$

If we do the calculations the rotation matrix (R) is:

$$R = \begin{bmatrix} \left(\frac{1}{2}\right) & \left(-\frac{1}{2}\right) & \left(\frac{1}{\sqrt{2}}\right) \\ \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right) & \left(-\frac{1}{2}\right) \\ \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right) & \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \left(\frac{1}{2}\right) \end{bmatrix} \tag{B.1}$$

Then, we have to check if this matrix is unitary. Easily we can prove that:

$$R \cdot R^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Using the equations 7.2 and B.1 we get:

$$\begin{pmatrix} \hat{\alpha}^\dagger_{B_1} \\ \hat{\alpha}^\dagger_{B_2} \\ \hat{\alpha}^\dagger_{A} \end{pmatrix} = \begin{bmatrix} \left(\frac{1}{2}\right) & \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right) \\ \left(-\frac{1}{2}\right) & \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right) & \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \\ \left(\frac{1}{\sqrt{2}}\right) & \left(-\frac{1}{2}\right) & \left(\frac{1}{2}\right) \end{bmatrix} \cdot \begin{pmatrix} \hat{\alpha}^\dagger_1 \\ \hat{\alpha}^\dagger_2 \\ \hat{\alpha}^\dagger_3 \end{pmatrix} \tag{B.2}$$

And finally we can calculate the output beam equations as:

$$\begin{aligned} \hat{\alpha}^\dagger_{B_1} &= \frac{\hat{\alpha}^\dagger_1}{2} + \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)\hat{\alpha}^\dagger_2 + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)\hat{\alpha}^\dagger_3 \\ \hat{\alpha}^\dagger_{B_2} &= -\frac{\hat{\alpha}^\dagger_1}{2} + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)\hat{\alpha}^\dagger_2 + \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)\hat{\alpha}^\dagger_3 \\ \hat{\alpha}^\dagger_{A} &= \frac{\hat{\alpha}^\dagger_1}{\sqrt{2}} - \frac{\hat{\alpha}^\dagger_2}{2} + \frac{\hat{\alpha}^\dagger_3}{2} \end{aligned} \tag{B.3}$$

APPENDIX C. QUANTIFICATION OF THE BASIS FLAW

In order to find the correlation of the two bases (X and Y), we'll start from relating the amplitude α of a coherent state $|\alpha\rangle$ with the displacement in position q_0 and the displacement in momentum p_0 of an electromagnetic oscillator in the phase space [9] as:

$$\alpha = \frac{1}{\sqrt{2}}(q_0 + ip_0) \ . \tag{C.1}$$

If we are in the base X we have one of coherent states $|\pm\alpha\rangle$ with $\alpha > 0$ and according to the equation C.1 we need $p_0 = 0$ and $q_0 = \pm\sqrt{2}\alpha$. Using the same idea, if we are in the base Y, we have a coherent state $|\pm i\alpha\rangle$ and respectively $q_0 = 0$ and $p_0 = \pm\sqrt{2}\alpha$.

Let us also write the wave function of a coherent state $|\alpha\rangle$ in the position representation using formula C.1:

$$\Psi_\alpha(q) = \langle q|a\rangle = \frac{1}{\pi^{-\frac{1}{4}}} \exp\left\{-\frac{(q-q_0)^2}{2} + ip_0q - \frac{ip_0q_0}{2}\right\} \tag{C.2}$$

as well as its conjugate:

$$\overline{\Psi}_\alpha(q) = \langle a|q\rangle = \frac{1}{\pi^{-\frac{1}{4}}} \exp\left\{-\frac{(q-q_0)^2}{2} - ip_0q + \frac{ip_0q_0}{2}\right\} \ . \tag{C.3}$$

The situation when a user sends two states $|\psi_1\rangle$ and $|\psi_2\rangle$ with the same probability can be described by the density matrix:

$$\hat{\rho} = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2| \tag{C.4}$$

In our case we have two density matrices, one for the base X and one for the base Y. For the X base we have:

$$\hat{\rho}_X = \frac{1}{2}|\alpha\rangle\langle\alpha| + \frac{1}{2}|-\alpha\rangle\langle-\alpha| \tag{C.5}$$

and for the Y base:

$$\hat{\rho}_Y = \frac{1}{2}|i\alpha\rangle\langle i\alpha| + \frac{1}{2}|-i\alpha\rangle\langle-i\alpha| \ . \tag{C.6}$$

To represent the operators $\hat{\rho}_X$ and $\hat{\rho}_Y$ as a function, we project it in the position basis $|q\rangle$. Doing that we have:

$$\hat{\rho}_X \rightarrow \langle q'| \hat{\rho}_X |q\rangle = \rho_X(q', q) = \frac{1}{2} \langle q'|\alpha\rangle \langle\alpha|q\rangle + \frac{1}{2} \langle q'|-\alpha\rangle \langle-\alpha|q\rangle \tag{C.7}$$

$$\hat{\rho}_Y \rightarrow \langle q'| \hat{\rho}_Y |q\rangle = \rho_Y(q', q) = \frac{1}{2} \langle q'|i\alpha\rangle \langle i\alpha|q\rangle + \frac{1}{2} \langle q'|-i\alpha\rangle \langle-i\alpha|q\rangle \ . \tag{C.8}$$

In an ideal protocol, where there is no basis flaw, these above two operators have max fidelity and they satisfy the following equation:

$$\hat{\rho}_X \equiv \hat{\rho}_Y \ .$$

One way to quantify the overlap (fidelity) of the two bases (X and Y), and therefore the basis flaw between them, is by the equation:

$$B\_F = \frac{\mathsf{Tr}\{\hat{\rho}_X \cdot \hat{\rho}_Y\}}{\mathsf{Tr}\{\hat{\rho}_X \cdot \hat{\rho}_X\}} \tag{C.9}$$

,where the $\mathsf{Tr}\{\hat{\rho}_X \cdot \hat{\rho}_X\}$ is the normalization factor and we know that:

$$\mathsf{Tr}\{\hat{\rho}_X^2\} = \mathsf{Tr}\{\hat{\rho}_Y^2\} \tag{C.10}$$

We proceed with the calculation of equation C.9:

$$\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_y}\} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \rho_x(q', q) \rho_y(q, q') \, dq' \, dq \tag{C.11}$$

Using equations C.7 ,C.8 and C.11 we can calculate the quantity $\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_y}\}$:

$$\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_y}\} = e^{-2^{\alpha^2}} \tag{C.12}$$

Also, we can calculate the quantity $\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_x}\}$:

$$\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_x}\} = \frac{1 + e^{-4^{\alpha^2}}}{2} \tag{C.13}$$

Using equations C.12 and C.13, we can calculate the basis correlation from equation C.9 as:

$$B\_F = \frac{\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_y}\}}{\mathsf{Tr}\{\hat{\rho_x} \cdot \hat{\rho_x}\}} = \frac{2e^{-2^{\alpha^2}}}{1 + e^{-4^{\alpha^2}}} \tag{C.14}$$

We can simplify this equation as follows:

$$\begin{aligned} B\_F &= \frac{2e^{-2^{\alpha^2}}}{1+e^{-4^{\alpha^2}}} \\ &= \frac{2e^{-2^{\alpha^2}}}{1+e^{-4^{\alpha^2}}} \times \frac{e^{2^{\alpha^2}}}{e^{2^{\alpha^2}}} \\ &= \frac{2}{e^{2^{\alpha^2}}+e^{-2^{\alpha^2}}} \end{aligned}$$

We know though that:

$$\cosh x = \frac{e^x + e^{-x}}{2} \Rightarrow 2\cosh x = e^x + e^{-x}$$

Using this exponential definition we can write that:

$$B\_F = \frac{1}{\cosh 2\alpha^2}$$

And if we include that $\alpha = \sqrt{\mu}$, we get:

$$B\_F = \frac{1}{\cosh 2\mu} \tag{C.15}$$

REFERENCES

[1] Z. Pei, Z. Hongyi, W. Weijie, and M. Xiongfeng, “Mode-pairing quantum key distribution,” *Nature Communications*, vol. 13, no. 23, 2022. [Online]. Available: https://doi.org/10.1038/s41467-022-31534-7

[2] R. Matsumoto, “Multiparty quantum-key-distribution protocol without use of entanglement,” *Physical Review A*, vol. 76, 2007.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, 1984.

[4] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.130503

[5] K. Tamaki, H. K. Lo, C. H. F. Fung, and B. Qi, “Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw,” *Physical Review A*, vol. 85, no. 4, 2012.

[6] G. Carrara, G. Murta, and F. Grasselli, “Overcoming fundamental bounds on quantum conference key agreement,” *Physical Review Applied*, vol. 19, no. 6, Jun. 2023. [Online]. Available: http://dx.doi.org/10.1103/PhysRevApplied.19.064017

[7] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, “Quantum conference key agreement: A review,” *Advanced Quantum Technologies*, vol. 3, no. 11, Sep. 2020. [Online]. Available: http://dx.doi.org/10.1002/qute.202000025

[8] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi, “Conference key agreement in a quantum network,” *npj Quantum Inf 9*, vol. 82, 2023. [Online]. Available: https://doi.org/10.1038/s41534-023-00750-4

[9] U. Leonhardt, *Measuring the Quantum State of Light*, 1st ed. Cambridge University Press, 1997.

[10] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*, 1st ed. Springer Cham, 2019.

[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” 2004. [Online]. Available: https://arxiv.org/abs/quant-ph/0212066

[12] A. Steane, “Multiple particle interference and quantum error correction,” *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 452, no. 1954, p. 2551–2577, 1996. [Online]. Available: http://dx.doi.org/10.1098/rspa.1996.0136

[13] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.54.1098

[14] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters*, vol. 94, no. 23, Jun. 2005. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.94.230504

[15] M. Koashi, “Simple security proof of quantum key distribution based on complementarity,” *New Journal of Physics*, vol. 11, 2009. [Online]. Available: https://doi.org/10.1088/1367-2630/11/4/045018

[16] K. Tamaki, M. Koashi, and N. Imoto, “Unconditionally secure key distribution based on two nonorthogonal states,” *Phys. Rev. Lett.*, vol. 90, p. 167904, Apr 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.90.167904

[17] P. W. Shor and J. Preskill, “Simple proof of security of the bb84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.85.441