



Scientific Education Division
Master Dissertation

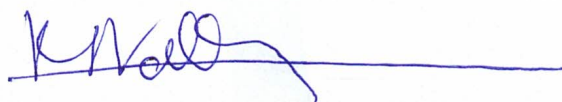
A Security Analysis for the Rio Quantum Network

Mario Augusto Curvo Tavares Ribeiro

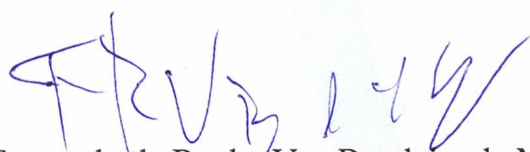
"SECURITY ANALYSIS FOR THE RIO QUANTUM NETWORK"

MARIO AUGUSTO CURVO TAVARES RIBEIRO

Dissertação de Mestrado em Física apresentada no
Centro Brasileiro de Pesquisas Físicas do
Ministério da Ciência Tecnologia e Inovação.
Fazendo parte da banca examinadora os seguintes
professores:



Raúl Oscar Vallejos - Orientador/CBPF



Fernando da Rocha Vaz Bandeira de Melo – Coorientador/ CBPF



Malena Osorio Hor-Meyll - UFRJ



Rafael Chaves Souto Araújo – UFRN

Rio de Janeiro, 28 de abril de 2025.

Acknowledgements

I would like to thank each person who made this work possible. This dissertation has only been achievable thanks to the amazing people in my life, and this is the perfect moment to express how grateful I am for their help in forging my path.

First, my two supervisors, Raul Vallejos and Fernando de Melo, who not only did an excellent job of convincing me to study quantum cryptography but also taught me and showed me the ropes so I could take my first steps toward becoming a researcher in this field. Your support and inspiration have made me look forward to the future with confidence and high expectations. I am very grateful to have two amazing professors guiding me through this master's degree.

I would also like to thank my colleagues, João, Nina, and Isadora, who have inspired and motivated me to become a better student. Our discussions and time together, especially during Paraty, will always stay with me, and I am sure we will build many more memories and collaborations in the future.

My family, of course, for always supporting me no matter what. I am very lucky to have a place to call home whenever I need it. My parents, Marilia and Luiz, whom I constantly miss with all my heart; my brother, Gabriel, whom I miss even more; and my grandparents, Nilza, Guto, Sônia, and Mariano, who have always taken care of me when needed, along with my aunts, Lilian, Eloisa, Luciana, and Ana. I love you all, and I am grateful for the best upbringing you could have possibly given me.

My chosen family—my very dear and amazing friends. I don't know where I would be without you. Betânia, Daniela, Danielle, Ilana, Matheus, and Vitória, you know how much I love you and what you mean to me. I would also like to thank my carioca friends, Lucas, Ranner, and Yasmin, for always keeping me company and being there for me whenever I needed it. My childhood friends, Angelo and Yago, still managing to make me laugh the moment we meet.

I want to thank my life partner, Marina. We have been together since the moment I started this journey in physics, and I hope we will be together until the very end. Thank you for your unconditional love and support, always.

Finally, the most special thanks go to my cat, Shitake, for showing me the purest form of love there is and for never letting a day in my life be boring—even though I doubt he will read this dissertation.

There is a theory which states that if ever anyone discovers exactly what the Universe is for and why it is here, it will instantly disappear and be replaced by something even more bizarre and inexplicable. There is another theory which states that this has already happened.

Douglas Adams

Resumo

A Distribuição Quântica de Chaves (QKD, do inglês Quantum Key Distribution) é uma das aplicações mais relevantes da teoria da informação quântica, especialmente no contexto dos computadores quânticos, que podem, no futuro, comprometer os esquemas de criptografia utilizados no dia a dia. A QKD utiliza os princípios fundamentais da mecânica quântica para permitir que duas ou mais partes compartilhem uma sequência de bits, denominada chave, que é secreta e segura—ou seja, as partes podem verificar que apenas elas conhecem o valor dessa chave. Esse campo tem despertado o interesse de prestigiadas instituições de pesquisa ao redor do mundo e amadureceu a ponto de permitir aplicações em um futuro próximo, utilizando configurações de baixo custo relativo.

O objetivo desta dissertação é introduzir o leitor ao funcionamento da QKD, explicando por que e quando ela pode ser considerada segura, além de abordar os principais protocolos de QKD que impactaram a área. Por fim, apresentamos a primeira tentativa do Brasil de implementar uma rede quântica em escala metropolitana, denominada Rede Rio Quântica.

A Rede Rio Quântica é uma rede multiusuário que interliga diversas instituições de pesquisa na cidade do Rio de Janeiro. O protocolo analisado é uma variante do protocolo Twin Field QKD (TF-QKD), classificado como Measurement Device Independent QKD (MDI-QKD), o que elimina a necessidade de suposições de segurança sobre os dispositivos de medição. Em vez de Alice e Bob possuírem fontes de fótons em seus laboratórios, eles realizam modulações de fase e amplitude em um sinal enviado pelo nó central, Charlie, para executar o protocolo. Devido à topologia em anel da rede, essa implementação funciona como um protocolo Twin Field QKD baseado em Interferômetro de Sagnac. Demonstraremos como a comunicação é estabelecida entre as partes, os detalhes da geração de chaves seguras e uma análise de segurança com a expressão da taxa de chave secreta para essa variante do protocolo.

Palavras-chave: Distribuição Quântica de Chaves, Criptografia Quântica, Informação Quântica

Abstract

Quantum Key Distribution (QKD) is one of the most relevant applications of quantum information theory, especially on the verge of quantum computers potentially breaking our day-to-day encryption schemes. QKD uses the foundations of quantum mechanics to allow two or more parties to exchange a shared string of bits, called a key, which is secret and secure, meaning the parties can verify that only they know the value of this exchanged key. This field has gotten the interest of prestigious research institutions all over the world, and has matured to the point of near-term applications using relative low budget set ups.

The scope of this thesis is to introduce the reader on how QKD works, why and when it can be called secure, while talking about the main QKD protocols that have impacted the field. Finally, we present Brazil's first attempt at making a metropolitan-wide quantum network, called Rio Quantum Network (RQN).

The RQN is a multi-user network involving multiple research institutions in the city of Rio de Janeiro. The protocol we will be analyzing is a variant of a Twin Field QKD protocol, which is a type of a Measurement Device Independent QKD protocol. This means that no safety assumptions are needed for the measurement devices. Instead of Alice and Bob each having a source in their lab, they will perform phase and amplitude modulations on a signal sent by the central-node, Charlie, in order to execute the protocol. Since the network has a ring topology, this protocol works as a Sagnac Based Twin Field QKD. We will show how exactly communication will be established between the parties, the details of how the parties can create a secure key and provide a security analysis with a secret key rate expression for this variant protocol.

Keywords: Quantum Key Distribution, Quantum Cryptography, Quantum Information

Contents

	Resumo	7
	Abstract	9
1	INTRODUCTION AND MOTIVATION	19
2	INTRODUCTION TO QUANTUM INFORMATION THEORY . . .	23
2.1	Linear Algebra and Quantum Mechanics	23
2.2	Density Operator	25
2.3	POVMs	25
2.4	Entanglement	26
2.4.1	Partial Trace and Purification	27
2.4.2	State Distinguishability	27
2.5	Quantum Operations	29
2.6	Qubits and Bell States	29
2.6.1	Pauli Matrices	30
2.6.2	Depolarizing Channel	31
2.6.3	Bell States	32
2.6.4	No-cloning Theorem	32
2.7	Entropy	33
2.7.1	Shannon Entropy	33
2.7.2	Von Neumann Entropy	34
2.7.3	Min- and Max-Entropy	36
2.7.4	Smooth Min- and Max-Entropy	37
3	QUANTUM KEY DISTRIBUTION	39
3.1	The One-Time Pad	39
3.2	The Framework of a QKD protocol	41
3.3	The BB84 Protocol	43
3.3.1	Security Analysis	46
4	QKD PROTOCOLS WITH IMPERFECT DEVICES	53
4.1	Practical Implementations of Light Sources	53
4.1.1	Decoy States Strategy	55
4.2	Device Independent QKD	57
4.2.1	Bell Inequalities	57
4.2.2	DI-QKD Protocol Based on the CHSH Inequality	59

4.3	Measurement-Device-Independent QKD	61
4.4	Fundamental Limits of Quantum Communication	64
4.5	Twin-Field QKD	65
4.5.1	Ideal Protocol	65
4.5.2	Practical Protocol	69
5	THE RIO QUANTUM NETWORK	73
5.1	Motivation	73
5.2	Sagnac-based TF-QKD: Ideal Scenario	74
5.3	Equivalence to EB-BB84: Virtual scenario	77
5.4	The practical protocol	79
5.5	Security analysis and secret key rate estimation	80
5.6	Upper bound estimation for the yields	83
5.7	Secret key rate estimation	85
6	CONCLUSIONS	87
	Appendix A	89
	Appendix B	91
	BIBLIOGRAPHY	93

List of Figures

- Figure 1 – Entanglement-Based BB84 protocol schematic. An untrusted source distributes entangled states to Alice and Bob via a quantum channel. In each round, Alice and Bob randomly choose measurement bases (Z or X) and record outcomes. After transmission, they publicly compare a subset of bases to perform parameter estimation: mismatched bases test for eavesdropping (via error rates), while matched bases generate raw key bits. Final key distillation uses classical post-processing (error correction and privacy amplification) to eliminate Eve’s information. Security relies on certifying entanglement through observed correlations. 45
- Figure 2 – Photon number splitting (PNS) attack strategy. Eve replaces the quantum channel with a lossless link and uses quantum non-demolition (QND) measurements to sort pulses by photon number: vacuum states ($n = 0$) are forwarded to Bob (no detection); single-photon pulses ($n = 1$) are selectively blocked to mimic channel loss; multiphoton pulses ($n \geq 2$) are split, with one photon stored in Eve’s quantum memory and the rest sent to Bob. After basis reconciliation, Eve measures stored photons to deduce the key, while unblocked single photons may trigger errors via intercept-resend attacks. 54
- Figure 3 – Example of the decoy-state strategy. Alice uses two weak laser sources: a signal source with low photon number (e.g., $\mu_S = 0.1$) and a decoy source with higher photon number (e.g., $\mu_D = 0.8$). She mixes decoy states (e.g., 5% of pulses) randomly with signal states. After transmission, Alice tells Bob which pulses were decoys. Bob then checks the loss in the signal states—if Eve tried a PNS attack, the signal loss will be much higher than expected, exposing the attack. 56
- Figure 4 – Characterizing black boxes without internal assumptions. Alice and Bob interact with their devices by selecting inputs (e.g., pressing buttons labeled x or y) and recording outputs a and b . Repeated trials reveal the input-output statistics $\{p(a, b|x, y)\}$, which describe how the boxes behave—without requiring knowledge of their internal mechanisms. . . 58

Figure 5 – Experimental scheme for MDI-QKD [Lo, Curty e Qi 2012]. Alice and Bob encode random bits in polarization states of phase-randomized WCPs, with amplitude modulators implementing decoy intensities. Their pulses interfere at an untrusted relay containing a 50:50 beam splitter (BS) and PBSs directing photons to four single-photon detectors (D_{CH} , D_{CV} , D_{DH} , D_{DV}). Detector clicks herald Bell-state measurement outcomes, which the relay broadcasts. 62

Figure 6 – Experimental setup for practical Twin-Field QKD (CAL-19 protocol) [Curty, Azuma e Lo 2019]. Alice and Bob independently select the X basis (probability p_X) or Z basis (probability p_Z). In X -basis rounds, Alice encodes a random bit b_A in the phase of a weak coherent pulse (WCP) with intensity α_A , while Bob encodes b_B in a WCP of intensity α_B . For Z -basis rounds, they prepare phase-randomized WCPs with decoy intensities μ_i and ν_i , respectively. Signals traverse lossy channels (transmittance $\sqrt{\eta_A}$, $\sqrt{\eta_B}$) to a central relay, where a 50:50 beam splitter (BS) interferes them. Threshold detectors at the BS outputs (D_c , D_d) record clicks $k_c, k_d \in \{0, 1\}$, which the relay broadcasts. Rounds with $k_c \oplus k_d \neq 1$ or mismatched bases are discarded. The raw key is formed by bits b_A and $b_B \oplus k_d$ 67

Figure 7 – Basic overview of the Rio Quantum Network’s structure and the institutes connected by it. The distances are measured in a straight line. The bold lines represent connection by optical fibers, while the dotted line represents a free-space link. 74

Figure 8 – Two-parties QKD in Rio Quantum Network using a Sagnac-based topology: experimental setup. Charlie prepares a optical signal and sends it to the network. A 50:50 BS acts on the signal creating a uniform superposition between the clockwise and anti-clockwise modes. Alice and Bob independently apply a phase shift on the anti-clockwise mode randomly sampling the phase value from four possible settings. The signal then goes back to Charlie’s lab, where it interferes back at the BS, and it is followed by two detectors D_\odot and D_\ominus . The relay announces detection results k_\odot and k_\ominus . The parties keep the rounds in which they choose the same basis and $k_\odot \oplus k_\ominus = 1$, all the other rounds are discarded. The network has optical switches that can be used to allow other users to communicate. 76

Figure 9 – Secret key rate per pulse in logarithmic scale for the Rio Quantum Network as a function of the overall loss of the network. The solid line represents the secret key rate for the RQN protocol. We compare it to the PLOB-bound [Pirandola et al. 2017], and to the GLLP secret key rate for a BB84 protocol using WCPs [Gottesman et al. 2004]. 86

List of Tables

Table 1 – Possible phase values and their respective sets, as well as the bit value associated with each phase value.	76
Table 2 – Different phase and amplitude modulations depending on the set chosen by Alice (Bob).	80

1 Introduction and Motivation

Cryptography has been a topic of great interest in human society since ancient Greece, particularly in the context of exchanging secret messages during times of war [Singh 2000]. Throughout history, the primary goal of encryption schemes has been to achieve unconditional security. This means ensuring that even if a malicious third party intercepts an encrypted message, it would remain indecipherable, even under the assumption of infinite computational power and resources. However, achieving this level of security has proven to be a formidable challenge.

Numerous cryptographic schemes have been developed—and subsequently broken—over the years. One of the earliest known methods is the *Caesar Cipher*, which encrypts a message by substituting each letter with another letter of the alphabet, shifted by a fixed number of positions [Singh 2000]. Later, the *Vigenère Cipher* introduced a refinement by assigning a distinct shift to each letter in the message, based on a repeating keyword, or cryptographic key. Despite these advancements, both ciphers can eventually be cracked with sufficient time and resources; once the underlying shifting rule is discovered, the encrypted message can be deciphered.

In the modern era of information and technology, the need for robust privacy and security has become more critical than ever. Most of our digital communication relies on the RSA (Rivest-Shamir-Adleman) protocol [Rivest, Shamir e Adleman 1978], which is based on the mathematical properties of one-way functions, such as the difficulty of factoring the product of two large prime numbers. In this scheme, two parties, commonly referred to as Alice and Bob, each possess a secret prime number as their individual private keys. A public key is generated by performing operations with their private keys and is used to encrypt the parties' original message. This public key is shared openly, however, only the private keys of Alice and Bob can be used to recover the original message. This allows secure communication while ensuring that, given sufficiently large prime numbers, the public key remains computationally infeasible to factor and recover their private keys. Although the most powerful classical computers would take years to break RSA encryption, the protocol's security is inherently tied to the limitations of current computational power. As computing technology advances, this security assumption weakens. Moreover, the advent of quantum computers poses an even greater threat, as algorithms such as Shor's algorithm [Shor 1994] enable efficient factorization of large integers, effectively breaking RSA and similar protocols.

In the 1920s, Vernam proposed one of the first encryption schemes to achieve information-theoretic security: the *Vernam Cipher*, commonly known as the *one-time*

pad [Vernam 1926]. In this scheme, two parties possessing identical bit strings, referred to as the *key*, can encrypt and decrypt messages by performing a binary sum (XOR operation) between the key and the message, both of which must have at least the same length. While the one-time pad is theoretically unbreakable [Shannon 1948], its security depends on two stringent conditions: the key must be shared in complete secrecy, and a new key must be used for every communication. Meeting these conditions in practice remains a significant challenge.

Quantum Key Distribution (QKD) has emerged as a promising solution to the challenges faced by classical cryptographic protocols. By leveraging the fundamental principles of quantum mechanics, QKD enables two distant parties to perform experiments and securely generate a shared *key*, even in the presence of potential eavesdroppers. The first QKD protocol, known as BB84, was proposed by [Bennett e Brassard 1984]. This protocol encodes classical bits into quantum bits (*qubits*), which are physical realizations of two-level quantum systems, such as the polarization states of photons. For instance, the parties can exchange photons, measure their polarizations, and thereby establish a shared string of bits, known only to them.

This development not only addresses the impending obsolescence of RSA encryption and alike, but also marks a fundamental paradigm shift in cryptography. While post-quantum cryptography is often regarded as a viable replacement for RSA schemes [Bernstein, Buchmann e Dahmen 2009], it ultimately relies on the same underlying principle—the security depends on current computational capabilities and existing algorithms. As history has shown, any cryptographic scheme might eventually be compromised by future scientific breakthroughs. In contrast, QKD represents an entirely different approach. Rather than engaging in the centuries-old cat-and-mouse game of algorithmic updates, QKD uses the principles of quantum mechanics—nature itself—to ensure security. In this context, potential vulnerabilities arise not from the protocol but from the physical devices used in communication. Moreover, certain QKD protocols, such as Device-Independent QKD, first proposed by [Ekert 1991], eliminate reliance on assumptions about device safety, offering an even higher level of security.

Since the advent of BB84, numerous QKD protocols have been developed. Advances in research have significantly enhanced their security and efficiency, leading to practical implementations over increasing distances. Research institutions worldwide are actively conducting long-distance QKD experiments, but these efforts also highlight practical challenges such as quantum signal loss and high implementation costs. Consequently, experimental adaptations are necessary to develop more accessible and cost-effective QKD solutions. The successful deployment of metropolitan-scale quantum networks capable of performing QKD protocols is a significant step toward making secure communication both feasible and widespread. The Rio Quantum Network stands as an ambitious initiative to

establish a metropolitan quantum communication network connecting research institutions in Rio de Janeiro. This network faces high urban signal loss, cost constraints, and hybrid quantum-classical integration. These hurdles highlight the need for protocol optimizations tailored to practical environments.

This thesis is organized as follows: In chapter 2, we introduce the foundational concepts of information theory, encompassing both classical and quantum domains, and explain the criteria for secure communication. Chapter 3 provides an introduction to QKD, focusing on the BB84 protocol as a fundamental and robust example of quantum cryptography. Chapter 4 explores advancements in QKD theory, with an emphasis on protocols that eliminate the need for trusted measurement devices, known as Measurement Device Independent (MDI) QKD protocols. Finally, chapter 5 presents a theoretical security analysis of a QKD protocol adapted for the Rio Quantum Network based on a Sagnac interferometer structure.

2 Introduction to Quantum Information Theory

In order to properly discuss Quantum Key Distribution, we need to understand a few concepts of Quantum Mechanics and Quantum Information Theory. We will briefly discuss those concepts and mathematical tools in this chapter, focusing on the concept of Entropy and how it is fundamental to Information Theory (both classical and quantum). This chapter is mainly based on [Nielsen e Chuang 2000] and [Wilde 2013].

2.1 Linear Algebra and Quantum Mechanics

Using the *Dirac notation*, a quantum state is described by a *ket* $|\psi\rangle$, which is a normalized vector of a *Hilbert space* \mathcal{H} with dimension d . A Hilbert space is by definition a complete complex vector space equipped with an inner product. To every ket $|\psi\rangle$ in a finite-dimension Hilbert space \mathcal{H} , there is a corresponding dual vector $\langle\psi|$, called *bra*, in the also finite-dimension dual Hilbert space \mathcal{H}^* .

A ket $|\psi\rangle$ defines a linear map $\langle\psi| \in \mathcal{H}^*$ that maps any other ket $|\phi\rangle \in \mathcal{H}$ to a complex number through the inner product $\langle\psi|\phi\rangle$ or *bra-ket*, meaning \mathcal{H}^* is the space of linear maps from \mathcal{H} to \mathbb{C} . Two kets $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if their inner product is zero. Also, the inner product induces a *norm* in the Hilbert space, so for every $|\psi\rangle \in \mathcal{H}$, the norm is defined by $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$. A $|\psi\rangle$ is a *normalized* vector if $\| |\psi\rangle \| = 1$ and a set of vectors $\{|\psi_i\rangle\}$ is called *orthonormal* if $\langle\psi_i|\psi_j\rangle = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta.

The *outer-product*, or *ket-bra*, between two vectors $|\psi\rangle$ and $|\phi\rangle$ is defined by $|\psi\rangle \langle\phi|$. We can use it to define a linear operation $|\psi\rangle \langle\phi| : \mathcal{H} \rightarrow \mathcal{H}$. For example, given a ket $|\xi\rangle \in \mathcal{H}$, the outer product $|\psi\rangle \langle\phi|$ maps it to the vector $\langle\phi|\xi\rangle |\psi\rangle$, meaning $(|\psi\rangle \langle\phi|) |\xi\rangle$ is simply the ket $|\psi\rangle$ multiplied by the complex number $\langle\phi|\xi\rangle$. In other words, $|\psi\rangle \langle\phi|$ is an operator acting on a Hilbert space.

An orthonormal basis for a d -dimensional Hilbert Space is composed of a set of linearly independent and orthonormal vectors $\{|\psi_i\rangle\}_{i=1}^d$ that span the whole dimension of the space. Given an orthonormal basis $\{|\psi_i\rangle\}_{i=1}^d$, any vector $|\phi\rangle$ can be written as a linear combination called *superposition*, such as $|\phi\rangle = \sum_{i=1}^d \psi_i |\psi_i\rangle$, where ψ_i is the resulting complex number of the inner product $\langle\psi_i|\phi\rangle$. Since this is true for all vectors $|\phi\rangle \in \mathcal{H}$, it

follows that

$$\sum_{i=1}^d |\psi_i\rangle \langle \psi_i| = \mathbb{I}, \quad (2.1)$$

where \mathbb{I} is the *identity operator*. This is called the *completeness relation*.

Given an orthonormal set of vectors $\{|\psi_i\rangle\}_{i=1}^d$, we can also use the outer product to represent any linear operator A acting on \mathcal{H} as:

$$A = \sum_{i,j=1}^d \langle \psi_i | A | \psi_j \rangle |\psi_i\rangle \langle \psi_j|. \quad (2.2)$$

A linear operator A can be written as a $d \times d$ matrix, and the term $\langle \psi_i | A | \psi_j \rangle$ represents the element $A_{i,j}$ of that matrix, with respect to the basis $\{|\psi_i\rangle\}_{i=1}^d$. The *adjoint* operator of A is called A^\dagger and by definition:

$$(\langle \phi | A^\dagger | \psi \rangle)^* = \langle \psi | A | \phi \rangle \quad (2.3)$$

for any $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. The operator A is called *self-adjoint* if $A = A^\dagger$; in finite-dimensional Hilbert spaces, A is also Hermitian. One of its properties are that its eigenvalues a_i are real numbers and its eigenvectors $\{|\alpha_i\rangle\}_{i=1}^d$ form an orthonormal basis. It follows that we can write A in its spectral decomposition:

$$A = \sum_{i=1}^d a_i |\alpha_i\rangle \langle \alpha_i| \quad (2.4)$$

The evolution of a quantum system is described by the action of a unitary operator U . An operator is said to be unitary if $UU^\dagger = U^\dagger U = \mathbb{I}$. The unitary operator preserves the inner product:

$$\langle \psi | \phi \rangle = \langle \psi | U^\dagger U | \phi \rangle = \langle \psi' | \phi' \rangle \quad (2.5)$$

where $|\psi'\rangle = U |\psi\rangle$ and $|\phi'\rangle = U |\phi\rangle$. Unitary operators also map one orthonormal basis $\{|\psi_i\rangle\}_{i=1}^d$ into another orthonormal basis $\{|\psi'_i\rangle\}_{i=1}^d$ in \mathcal{H} , so we can write $|\psi'_i\rangle = U |\psi_i\rangle$.

An operator P is called a *projector* if $P^2 = P$, and given an orthonormal basis $\{|\psi_i\rangle\}_{i=1}^d$:

$$P = \sum_{i \in S} |\psi_i\rangle \langle \psi_i| \quad (2.6)$$

where $S \subseteq \{1, \dots, d\}$. It projects any vector of the Hilbert space into the subspace spanned by the vectors $\{|\psi_i\rangle\}_{i \in S}$. Finally, given an orthonormal basis for \mathcal{H} , $\{|\psi_i\rangle\}_{i=1}^d$, we define the *trace* of an operator A as:

$$\text{Tr}(A) = \sum_{i=1}^d \langle \psi_i | A | \psi_i \rangle. \quad (2.7)$$

One of the main properties is that the trace of a product of operators is invariant under cyclic permutations: $\text{Tr}(ABC) = \text{Tr}(CAB) = \text{Tr}(BCA)$ and therefore its definition

does not depend on the orthonormal basis chosen, since the change of basis is represented by the action of a unitary operator:

$$\mathrm{Tr}(A) = \sum_{i=1}^d \langle \psi_i | A | \psi_i \rangle = \sum_{i=1}^d \langle \phi_i | U^\dagger A U | \phi_i \rangle = \mathrm{Tr}(U^\dagger A U) = \mathrm{Tr}(A U U^\dagger) = \mathrm{Tr}(A). \quad (2.8)$$

2.2 Density Operator

A quantum state fully characterized by a single state vector $|\psi\rangle$ is termed a *pure state*. For cases where a system's state cannot be described by a single state vector—such as statistical mixtures of states—a more general framework is required. The *density operator formalism* provides a unified description for both *mixed states* and pure states. For a pure state $|\psi\rangle$, the density operator is defined as:

$$\rho = |\psi\rangle \langle \psi|. \quad (2.9)$$

A mixed state arises when the state of a quantum system is described by an ensemble of vector states $\{|\psi_i\rangle\}_{i=1}^n$, each occurring with probability p_i . The density operator generalizes to:

$$\rho = \sum_{i=1}^n p_i |\psi_i\rangle \langle \psi_i|, \quad (2.10)$$

where $\sum_{i=1}^n p_i = 1$, $p_i \geq 0$. Like all quantum operators, the density operator can be expressed as a matrix. To represent a valid physical description of the quantum state of a system, the density matrix must satisfy two conditions: it must be *positive semi-definite* (all eigenvalues are non-negative) and its trace must equal unity ($\mathrm{Tr}[\rho] = 1$), as this is a direct consequence of the normalization and positivity of the probability distribution p_i . These properties ensure the matrix corresponds to a physically realizable quantum state, encapsulating both probabilistic mixtures and coherent superpositions. Finally, note that if a quantum state ρ is pure, it follows that $\rho^2 = \rho$ and thus $\mathrm{Tr}[\rho^2] = 1$. Consequently, ρ is a mixed state if $\mathrm{Tr}[\rho^2] < 1$.

2.3 POVMs

A Positive Operator-Valued Measurement (POVM) is a form of quantum measurement that uses a set of positive operators $\{E_m\}_{m=1}^n$ that satisfy $\sum_{m=1}^n E_m = \mathbb{I}$, where each operator E_m corresponds to a possible measurement outcome. The probability of obtaining outcome $m \in \mathcal{M}$ for a state described by density operator ρ is:

$$p(m) = \mathrm{Tr}[E_m \rho]. \quad (2.11)$$

POVMs are particularly useful when analyzing measurement statistics without requiring knowledge of the post-measurement state. When it is not the case, any measurement described by operators $\{M_m\}$ can be expressed as a POVM with $E_m = M_m^\dagger M_m$. The

probability of obtaining an outcome m from a measurement of the state ρ is defined by:

$$p(m) = \text{Tr}[M_m^\dagger M_m \rho] \quad (2.12)$$

and the state after the measurement reads:

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\text{Tr}[M_m^\dagger M_m \rho]}. \quad (2.13)$$

A special case is the *projective measurement*, where the POVM elements E_m are orthogonal projectors ($E_m = M_m = P_m$) described in (2.6). When all P_m are rank-one projectors (i.e., $P_m = |\psi_m\rangle\langle\psi_m|$), the measurement is termed a *von Neumann measurement*. Finally, the average outcome of a POVM is defined by the expectation value of the observable $E = \sum_m \lambda_m E_m$:

$$\langle E \rangle_\rho = \text{Tr}[E \rho]. \quad (2.14)$$

2.4 Entanglement

Given two different quantum states in different quantum systems, $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$, we use the *tensor product* to represent a *composite* or *bipartite* state as:

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B \quad (2.15)$$

with $|\Psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. Another possible notation for $|\psi\rangle_A \otimes |\phi\rangle_B$ is $|\psi_A \phi_B\rangle$. Any state that can be written as (2.15), or is a mixture of states of this form, is called a *separable state*. If a state cannot be written that way, meaning it is not *separable*, it is called an *entangled state*. A pure state $|\Psi\rangle_{AB}$ is entangled if it cannot be written as a product state $|\psi\rangle_A \otimes |\phi\rangle_B$ for any choice of states $|\psi\rangle_A$ and $|\phi\rangle_B$.

If two parties, Alice and Bob prepare their local states $|\psi_i\rangle_A$ and $|\psi_i\rangle_B$ using a shared classical probability distribution $\{p_i\}$, their joint state is a separable state and takes the form:

$$\rho_{AB} = \sum_{i=1}^n p_i |\psi_i\rangle\langle\psi_i|_A \otimes |\psi_i\rangle\langle\psi_i|_B. \quad (2.16)$$

Here, all correlations between Alice and Bob arise *classically* from the shared probabilities $\{p_i\}$, which can be established via LOCC (Local Operations and Classical Communication). LOCC refers to protocols where Alice and Bob perform quantum operations on their individual subsystems and exchange classical information, but cannot share quantum resources (e.g., entangled particles). Crucially, LOCC cannot create entanglement.

By contrast, entangled states (e.g., $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$) cannot be decomposed into such a mixture. Their correlations cannot be explained by classical statistics alone, as demonstrated by violations of Bell inequalities [Bell 1964]. This type of quantum correlation is fundamental to quantum cryptography.

2.4.1 Partial Trace and Purification

Given a composite state ρ_{AB} on \mathcal{H}_{AB} , one can find the *reduced density operator* ρ_A by taking the *partial trace* of ρ_{AB} over the subsystem B :

$$\rho_A = \text{Tr}_B[\rho_{AB}]. \quad (2.17)$$

The partial trace is defined by:

$$\text{Tr}_B[|\psi\rangle\langle\psi|_A \otimes |\phi\rangle\langle\phi|_B] = |\psi\rangle\langle\psi|_A \text{Tr}[|\phi\rangle\langle\phi|_B]. \quad (2.18)$$

In a similar manner, the reduced density operator ρ_B can be found by taking the partial trace of ρ_{AB} over the subsystem A .

Given two orthonormal basis $\{|a_i\rangle\}_i$ and $\{|b_k\rangle\}_k$ for the two subsystems A and B , the action of the partial trace can be computed as follows:

$$\begin{aligned} \text{Tr}_B[\rho_{AB}] &= \text{Tr}_B \left[\sum_{i,j,k,l} \lambda_{i,j,k,l} |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l| \right] = \sum_{i,j,k,l} \lambda_{i,j,k,l} |a_i\rangle\langle a_j| \otimes \text{Tr}[|b_k\rangle\langle b_l|] \\ &= \sum_{i,j,k,l} \lambda_{i,j,k,l} |a_i\rangle\langle a_j| \langle b_k|b_l\rangle = \sum_{i,j,k,l} \lambda_{i,j,k,l} |a_i\rangle\langle a_j| \delta_{k,l} = \rho_A, \end{aligned} \quad (2.19)$$

where $\lambda_{i,j,k,l} = \langle a_i b_k | \rho_{AB} | a_j b_l \rangle$ are the matrix elements of ρ_{AB} .

Given a quantum state ρ_A of a system A , it is always possible to introduce a second system E and define a pure state $|\Psi\rangle_{AE} \in \mathcal{H}_{AE}$, called *purification* of ρ_A , such that:

$$\rho_A = \text{Tr}_E[|\Psi\rangle\langle\Psi|_{AE}]. \quad (2.20)$$

This procedure is called *purification*. Without making any assumption about ρ_A , we can define the pure state of the composite system as:

$$|\Psi\rangle_{AE} = \sum_i \sqrt{\lambda_i} |\psi_i\rangle_A \otimes |\xi_i\rangle_E. \quad (2.21)$$

With this, it follows that

$$\begin{aligned} \text{Tr}_E[|\Psi\rangle\langle\Psi|_{AE}] &= \sum_{i,j} \sqrt{\lambda_i \lambda_j} |\psi_i\rangle\langle\psi_j|_A \text{Tr}[|\xi_i\rangle\langle\xi_j|_E] \\ &= \sum_{i,j} \sqrt{\lambda_i \lambda_j} |\psi_i\rangle\langle\psi_j|_A \delta_{i,j} = \rho_A. \end{aligned} \quad (2.22)$$

2.4.2 State Distinguishability

The *trace norm* of an operator ρ is defined by the sum of its singular values:

$$\|\rho\|_1 = \text{Tr}[\sqrt{\rho\rho^\dagger}]. \quad (2.23)$$

This norm introduces a natural distance measure for quantum states, called the *trace distance*. The trace distance between two density operators ρ and τ is:

$$T(\rho, \tau) = \frac{1}{2} \|\rho - \tau\|_1 = \frac{1}{2} \text{Tr} \left[\sqrt{(\rho - \tau)^2} \right] = \frac{1}{2} \sum_i |\lambda_i|. \quad (2.24)$$

where $\{\lambda_i\}_i$ are the eigenvalues of the operator $(\rho - \tau)$.

Two quantum states ρ and τ are ε -close if $T(\rho, \tau) \leq \varepsilon$, and we say $\rho \approx_\varepsilon \tau$ (i.e. those states are indistinguishable except for a probability at most $\varepsilon/2$). It is also useful to define an ε -ball around ρ . It is the set of all states ρ' which are ε -close to ρ :

$$\mathcal{B}^\varepsilon(\rho) := \{\rho' | \rho' \geq 0, \text{Tr}(\rho') = 1, T(\rho, \rho') \leq \varepsilon\}. \quad (2.25)$$

Finally, the *fidelity* is another common measure for closeness of quantum states. For two states ρ and τ , it is defined as:

$$F(\rho, \tau) = \text{Tr} \left[\sqrt{\sqrt{\rho} \tau \sqrt{\rho}} \right]^2. \quad (2.26)$$

If $\rho = |\psi\rangle \langle \psi|$ and $\tau = |\phi\rangle \langle \phi|$ are pure states, the fidelity between them can be simplified to

$$F(\rho, \tau) = |\langle \psi | \phi \rangle|^2. \quad (2.27)$$

The fidelity by itself is not considered a metric on the space of density operators since its role is to quantify similarity rather than distance. By introducing the *purified distance*, one can use the fidelity in order to find a distance measure. The purified distance between two quantum states ρ, τ is defined as:

$$P(\rho, \tau) = \sqrt{1 - F(\rho, \tau)}. \quad (2.28)$$

In order to establish the relationship between the fidelity and the trace distance, we recur to the following theorem:

Theorem 2.1. *The following relationship holds for the fidelity and the trace distance between two quantum states ρ, τ :*

$$1 - \sqrt{F(\rho, \tau)} \leq \frac{1}{2} \|\rho - \tau\|_1 \leq \sqrt{1 - F(\rho, \tau)}. \quad (2.29)$$

Finally, we can use *Uhlmann's Theorem* to define the fidelity using the purification of states.

Theorem 2.2 (Uhlmann's Theorem). *Suppose ρ_A and τ_A are states of a quantum system A and let R be a second quantum system which is a copy of A . Then:*

$$F(\rho_A, \tau_A) = \max_{|\psi_\rho\rangle, |\varphi_\tau\rangle} |\langle \psi_\rho | \varphi_\tau \rangle|^2 \quad (2.30)$$

where the maximization is over all purifications $|\psi_\rho\rangle$ of ρ_A and $|\varphi_\tau\rangle$ of τ_A into system $A \otimes R$.

The proof for both of the above theorems can be found in [Wilde 2013].

2.5 Quantum Operations

A physical process acting on a system in a given state ρ is generally described by a quantum operation, or quantum *channel* \mathcal{E} , with $\mathcal{E}(\rho)$ being the final state of the system after the process. However, a map \mathcal{E} is only considered a quantum channel if it obeys the following properties:

1. A map \mathcal{E} acting on the state ρ must preserve the hermicity and positivity of ρ . It also must be trace preserving: $\text{Tr}[\rho] = \text{Tr}[\mathcal{E}(\rho)]$.
2. \mathcal{E} must be convex-linear on the set of density operators, or $\mathcal{E}\left(\sum_i p_i \rho^{(i)}\right) = \sum_i p_i \mathcal{E}(\rho^{(i)})$ for any probability distribution $p_i \geq 0 \ \forall i$ and $\sum_i p_i = 1$.
3. \mathcal{E} must be completely positive, meaning it must be a positive operator for every input state ρ . Also, for every composite state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, the operator $(\mathbb{I}_A \otimes \mathcal{E})\rho_{AB}$ is positive on $\mathcal{H}_A \otimes \mathcal{H}_B$.

Properties 1 and 3 are needed to ensure that the output of a quantum channel acting on a density operator is also a density operator, even when it acts on a subsystem of a composite system.

We can use the *Choi-Kraus Theorem* to give a better characterization of quantum operations. It states:

Theorem 2.3 (Choi-Kraus Theorem). *A map $\mathcal{E} : \mathcal{H}_A \rightarrow \mathcal{H}_B$ is linear, completely positive and trace-preserving if and only if there exists a set of operators called Kraus operators $\{K_i\}$ such that:*

$$\mathcal{E}(\rho_A) = \sum_{i=1}^d K_i \rho_A K_i^\dagger \quad (2.31)$$

with $K_i : \mathcal{H}_A \rightarrow \mathcal{H}_B$ for all $i \in \{1, \dots, d\}$ and

$$\sum_{i=1}^d K_i^\dagger K_i = \mathbb{I}_A, \quad (2.32)$$

and d need not be any larger than $\dim(\mathcal{H}_A) \dim(\mathcal{H}_B)$.

The proof for this theorem can be read in [Wilde 2013].

2.6 Qubits and Bell States

Quantum bits or *qubits*, are a type of quantum system represented by any two-level system, such as photon polarization or the state of particles with spin $\frac{1}{2}$. Qubits can be written as vectors in a bi-dimensional Hilbert space and are described by the superposition of kets:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.33)$$

with $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\alpha, \beta \in \mathbb{C}$. Note that in order to be a valid qubit state, $|\psi\rangle$ needs to be normalized, or $|\alpha|^2 + |\beta|^2 = 1$. The numbers α and β are called amplitudes of $|\psi\rangle$ and represent the probability of obtaining outcomes "0" or "1", respectively, when measuring with respect to that basis, which is called the *computational basis* consisting of $\{|0\rangle, |1\rangle\}$. Another very useful basis, is the *Hadamard basis*, which consists of $\{|+\rangle, |-\rangle\}$ with:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (2.34)$$

Those two bases form mutually unbiased bases (MUBs) and are commonly used in set ups for Quantum Key Distribution protocols, and the fact that they are not orthogonal in respect to one another is crucial in order for two parties to exchange secure information—when a system is prepared in an eigenstate of one of the bases, all outcomes of the measurement with respect to the other basis are predicted to occur with an equal probability of $1/2$.

2.6.1 Pauli Matrices

There is a very notable set of operators called *Pauli operators* that are important in the description of qubits. They are called X , Z and Y , or in some notations σ_X , σ_Z , σ_Y . Their matrix representation is as follows:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (2.35)$$

They are Hermitian operators, with null trace and eigenvalues ± 1 . Also, $X^2 = Z^2 = Y^2 = \mathbb{I}$. They also respect the following relation:

$$\sigma_i \sigma_j = \delta_{i,j} \mathbb{I} + \sum_{k=1}^3 \epsilon_{ijk} \sigma_k \quad (2.36)$$

where $\sigma_1 = \sigma_X = X$, $\sigma_2 = \sigma_Y = Y$ and $\sigma_3 = \sigma_Z = Z$ and ϵ_{ijk} is the Levi-Civita symbol. Another very interesting property of the Pauli operators is that their action on a qubit represents possible errors that can happen in qubit operations. In the computational basis, the X operator produces a *bit flip*:

$$X |0\rangle = |1\rangle, \quad X |1\rangle = |0\rangle \quad (2.37)$$

Z produces a *phase flip*:

$$Z |0\rangle = |0\rangle, \quad Z |1\rangle = -|1\rangle \quad (2.38)$$

and Y produces both a phase and a bit flip, since $Y = iXZ$:

$$Y |0\rangle = i |1\rangle, \quad Y |1\rangle = -i |0\rangle. \quad (2.39)$$

However, when the Pauli operators act on a qubit in the Haddamard basis, Z produces a bit flip: $Z |+\rangle = |-\rangle$ and $Z |-\rangle = |+\rangle$, and X produces a phase flip: $X |+\rangle = |+\rangle$ and $X |-\rangle = -|-\rangle$. The computational basis is also called the Z-basis and the Haddamard basis is also called the X-basis.

Finally, any mixed qubit state can be described by a density operator ρ in terms of the identity and Pauli operators:

$$\rho = \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} \quad (2.40)$$

with $\vec{r} \in \mathbb{R}^3$, $||\vec{r}|| \leq 1$ and where $\vec{\sigma} = (X, Y, Z)^T$. The purity of a qubit state is $\text{Tr}[\rho^2] = (1 + ||\vec{r}||^2)/2$, and therefore the state is pure if the norm of \vec{r} equals to 1 and is mixed if it less than 1. The case where the norm of \vec{r} is zero is called the maximally mixed state.

2.6.2 Depolarizing Channel

One of the main characterizations of quantum loss, or noise, is described by the Depolarizing Channel. It is defined by the channel:

$$\mathcal{E}(\rho) = (1 - p)\rho + \frac{p}{3} \sum_{i=1}^3 \sigma_i \rho \sigma_i^\dagger. \quad (2.41)$$

The Kraus operators, in this case, are:

$$K_0 = \sqrt{1 - p} \mathbb{I}, \quad K_i = \sqrt{\frac{p}{3}} \sigma_i \quad (2.42)$$

with $i = (1, 2, 3)$. Meaning that with probability $1 - p$ the state remains unchanged, but with probability $p/3$ it is affected by one of the Pauli operators. This channel is useful in testing the robustness of a given quantum information protocol against quantum noise. However, given the properties of Pauli operators, we can calculate

$$\rho + \sum_{i=1}^3 \sigma_i \rho \sigma_i = 2\mathbb{I} \quad (2.43)$$

and substituting in (2.41) we can write the channel as:

$$\mathcal{E}(\rho) = (1 - q)\rho + q \frac{\mathbb{I}}{2}, \quad (2.44)$$

where $q = 3p/4$. In practice, the action of the Depolarizing Channel is that, with probability q , it replaces any given qubit state ρ with the maximally mixed state $\mathbb{I}/2$.

2.6.3 Bell States

A very useful and important set of states are the so called Bell states. Given two qubit systems A and B, we can define the Bell states acting on \mathcal{H}_{AB} as:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), & |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \quad (2.45)$$

These four states can be written in the compact form:

$$|\psi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0, j\rangle + (-1)^i |1, 1-j\rangle) \quad (2.46)$$

with $i, j \in \{0, 1\}$. Note that they form a basis, called Bell basis $\{|\psi_{ij}\rangle\}_{i,j=0}^1$, and thus we can express a bi-partite state in terms of Bell states.

2.6.4 No-cloning Theorem

One of the key factors of quantum mechanics that allows QKD to exist is what is called the *No-Cloning Theorem*. This theorem states that pure qubit states cannot be universally copied. Therefore, there is no operation that an eavesdropper that intercepts a message can make in order to universally copy any quantum state, keep the copy for future measurements and send the original state back along the intended path. This is a fundamental difference between classical information theory and quantum information theory, and it is crucial for the security of QKD protocols.

This theorem was first formulated in [Wootters e Zurek 1982], and its proof is quite simple. Say that, by the way of contradiction, exists and unitary U that can copy any state, meaning that:

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle. \quad (2.47)$$

Then, assuming this cloning machine works for any state, it should also follow that $U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$, and since U is unitary, we have $U^\dagger U = \mathbb{I}$, thus:

$$\begin{aligned} \langle\psi|\phi\rangle &= \langle\psi|\phi\rangle \langle 0|0\rangle \\ &= (\langle\psi| \otimes \langle 0|)U^\dagger U(|\phi\rangle \otimes |0\rangle) \\ &= (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) = (\langle\psi|\phi\rangle)^2 \end{aligned} \quad (2.48)$$

and therefore it is only valid when $|\psi\rangle$ and $|\phi\rangle$ are either orthogonal, meaning $\langle\psi|\phi\rangle = 0$, or they are equal to each other. Therefore, whenever $0 < |\langle\psi|\phi\rangle| < 1$, a copying unitary U cannot exist.

Additionally, any information gain by Eve introduces disturbance on the system [Nielsen e Chuang 2000]—in the attempt to distinguish non-orthogonal quantum states in a quantum signal, any information gain is accompanied by a disturbance on the signal.

Let $|\psi\rangle$ and $|\phi\rangle$ be two non-orthogonal quantum states. We can use a generic quantum operation (i.e. a unitary acting on one of the states and an ancilla $|u\rangle$) to represent Eve's action on a signal. Let us assume, by contradiction, that Eve's action leaves the signal states unchanged:

$$U(|\psi\rangle \otimes |u\rangle) = |\psi\rangle \otimes |v\rangle, \quad (2.49)$$

$$U(|\phi\rangle \otimes |u\rangle) = |\phi\rangle \otimes |v'\rangle. \quad (2.50)$$

Eve's goal is to distinguish $|\psi\rangle$ and $|\phi\rangle$ via the outcomes of this operation, $|v\rangle$ and $|v'\rangle$. By trying to distinguish them, we obtain:

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle \langle v'|v\rangle, \quad (2.51)$$

which implies that $|v\rangle = |v'\rangle$. This means that any successful attempt to distinguish two non-orthogonal states implies the disturbance of at least one of them.

2.7 Entropy

A good method of quantifying information is by measuring entropies. Those quantities are very important in information theory, as they generally are used to measure the amount of uncertainty about the state of a system, be it classical or quantum. Therefore it is a tool required to prove security of a cryptographic protocol. In this section we will go through some of the most important entropies for QKD as well as their physical and operational meaning.

2.7.1 Shannon Entropy

The *Shannon entropy* was defined by Shannon [Shannon 1948] and it quantifies the uncertainty about a classical random variable.

Definition 2.4 (Shannon entropy). Let X be a random variable whose outcome x is drawn from an alphabet \mathcal{X} with probability p_x . The Shannon entropy of X is given by:

$$H(X) = H(\{p_x\}) = - \sum_{x \in \mathcal{X}} p_x \log(p_x), \quad (2.52)$$

where here \log is referring to the base-2 logarithm. For convenience, this is the case for the rest of the thesis. Also, by convention, we take $0 \log 0 = 0$.

The *binary entropy* is useful when studying binary systems, and can be written in the form:

$$h(p) := -p \log(p) - (1 - p) \log(1 - p). \quad (2.53)$$

The Shannon entropy can be used to describe the joint information of two random variables X and Y , as well as the *conditional* and *mutual* information between the two. The joint Shannon entropy of X and Y distributed according to a probability distribution $p(x, y)$ is:

$$H(XY) = - \sum_{x,y} p_{x,y} \log(p_{x,y}) \quad (2.54)$$

and it describes the joint uncertainty about those variables. The *conditional entropy* is given by the quantity:

$$H(X|Y) = H(XY) - H(Y) \quad (2.55)$$

and it quantifies the uncertainty about the variable X given the known information about Y . Note that the Shannon conditional entropy cannot assume negative values, since the joint uncertainty about both variables is always going to be greater than the uncertainty about one of them. The *mutual information* $H(X : Y)$ is given by:

$$H(X : Y) = H(X) - H(X|Y) = H(X) + H(Y) - H(XY) \quad (2.56)$$

and it measures the amount of information gained on X when knowing the value of Y . In other words, it is the total information of X minus the uncertainty we have about X after knowing the outcome of Y .

2.7.2 Von Neumann Entropy

In quantum information theory, a system's uncertainty is quantified by the *von Neumann entropy*, which is defined by:

Definition 2.5 (von Neumann entropy). Given a quantum state ρ with eigenvalues $\{\lambda_i\}$, the von Neumann entropy of the state is:

$$H(\rho) = - \text{Tr}[\rho \log(\rho)] = - \sum_i \lambda_i \log(\lambda_i). \quad (2.57)$$

Note that the von Neumann entropy of a quantum state can be written as the Shannon entropy of its eigenvalues, which by themselves describe a probability distribution associated with the state. An important property that the von Neumann entropy has is that $0 \leq H(\rho) \leq \log(d)$, for every state ρ on a d -dimensional Hilbert space. Note that $H(\rho) = 0$ when ρ is a pure state and $H(\rho) = \log(d)$ when it is maximally mixed: of course, the pure state has no uncertainty about it and the maximally mixed state is the most uncertain one.

The von Neumann entropy also can be extended to bipartate state with the *joint quantum entropy*:

$$H(\rho_{AB}) = H(AB)_\rho = - \text{Tr}[\rho_{AB} \log(\rho_{AB})]. \quad (2.58)$$

The *conditional quantum entropy* of the state ρ_A of subsystem A conditioned on state ρ_B of subsystem B is:

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho, \quad (2.59)$$

where $H(B)_\rho = H(\rho_B)$ is the von Neumann entropy of the reduced state from subsystem B . If ρ_{AB} is a product state, then $H(A|B)_\rho = H(A)_\rho$, meaning that the known information of subsystem B is completely uncorrelated with subsystem A . A useful entropy property is the following:

Theorem 2.6. *Conditioning does not increase the entropy of a quantum state. For a bipartite quantum state ρ_{AB} , the following holds for the marginal entropy $H(A)_\rho$ and the conditional quantum entropy $H(A|B)_\rho$:*

$$H(A)_\rho \geq H(A|B)_\rho \quad (2.60)$$

with equality if and only if ρ_{AB} is a separable state.

The proof of this theorem can be found in [Wolf 2021]. Given a tripartite state, ρ_{ABC} , it follows that:

$$H(A|BC)_\rho \leq H(A|B)_\rho, \quad (2.61)$$

where $H(A|B)_\rho$ is evaluated by taking the partial trace on the state ρ_{ABC} and calculating its conditional entropy. This is particularly useful when talking about classical-quantum states, which play a very important role in the security analysis of QKD protocols.

A classical-quantum state (c-q state) is defined by:

$$\rho_{XQ} = \sum_x p(x) |x\rangle \langle x|_X \otimes \rho_Q^x, \quad (2.62)$$

where X is a random variable that can assume a value x with probability $p(x)$ and Q is a quantum system whose state ρ_Q^x depends on the outcome of X . Such states are foundational in quantum key distribution (QKD) because they model scenarios where classical information (e.g., Alice's key bits) is correlated with quantum systems accessible to an eavesdropper (Eve). Specifically, in QKD protocols, Eve's potential knowledge is encoded in a purification of the shared quantum state, making c-q states essential for analyzing adversarial information. The entropy of Q conditioned on X can be expressed as:

$$H(Q|X)_\rho = \sum_x p(x) H(\rho_Q^x). \quad (2.63)$$

and quantifies the average uncertainty about the quantum system Q given knowledge of the classical variable X . In QKD, this entropy directly bounds Eve's information about the key: a lower $H(Q|X)_\rho$ implies greater information leakage to Eve, while a higher value signifies stronger secrecy.

Finally, the conditional von Neumann entropy can assume negative values and this is observed to happen in entangled states [Wilde 2013]. Thus, the von Neumann entropy of a subsystem can be larger than the entropy of the composite system, and therefore it does not hold in general that $H(AB)_\rho \geq H(A)_\rho$.

We can use one of the Bell states described in (2.45) as an example: $\rho_{AB} = |\phi_+\rangle\langle\phi_+|_{AB}$. Since it is a pure state, it follows that $H(AB)_\rho = 0$, but we can see that $H(A)_\rho = H(B)_\rho = 1$, since $\rho_A = \rho_B = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{\mathbb{I}}{2}$. Therefore, $H(A|B)_\rho = -1$. This is unique to quantum systems, and if the conditional entropy of a state ρ_{AB} is negative, we know that it is entangled.

2.7.3 Min- and Max-Entropy

The entropies previously discussed are very useful when studying the case in which the probabilities are independently and identically distributed (i.i.d.). Under the i.i.d. assumption, repeated trials of an experiment are statistically independent and governed by the same probability distribution. This guarantees that the experimental repetitions yield well-defined and stable probabilities, enabling precise asymptotic predictions. However, practical QKD protocols run experiments a limited number of times, and in order to properly quantify information, other forms of entropy are needed. First, we will discuss the *conditional min-entropy* and the *conditional max-entropy* [Konig, Renner e Schaffner 2009]. These entropies are also called "one-shot entropies" and play a crucial role when talking about *privacy amplification*, one of the steps present in most QKD protocols. During this step, Alice and Bob need to transform their classical bit strings, which are correlated with Eve's quantum system, into a uniformly random string that is independent of Eve's knowledge.

Definition 2.7 (Conditional min-entropy). For a bipartite quantum state ρ_{AB} , the min-entropy of system A conditioned on B is defined via the optimization:

$$H_{\min}(A|B)_\rho = -\log \min_{\sigma_B} \{ \text{Tr}(\sigma_B) : \sigma_B \geq 0, (\mathbb{I}_A \otimes \sigma_B) - \rho_{AB} \geq 0 \}, \quad (2.64)$$

where the minimization is over all positive semi-definite operators σ_B on subsystem B .

Definition 2.8 (Conditional max-entropy). Let ρ_{ABC} be a purification of a bipartite quantum state ρ_{AB} . The max-entropy of A conditioned on B of the state ρ_{AB} is defined as:

$$H_{\max}(A|B)_\rho = -H_{\min}(A|C)_\rho. \quad (2.65)$$

The above definitions are also valid for classical probability distributions p_X , one needs only to evaluate the min- or max- entropy on the state $\rho_X = \sum_x p_X(x) |x\rangle\langle x|$ for some orthonormal basis $\{|x\rangle\}_x$. The conditional min- and max-entropy are related to the

conditional von Neumann entropy as follows [Tomamichel, Colbeck e Renner 2009]:

$$H_{\min}(A|B) \leq H(A|B) \leq H_{\max}(A|B). \quad (2.66)$$

In privacy amplification, the min-entropy of a cq-state quantifies the amount of nearly uniform random bits that can be reliably extracted from a classical source—even when it is correlated with a quantum system—ensuring that the extracted key is independent of any quantum side information. Conversely, the max-entropy measures the minimal number of bits into which the original classical data can be compressed, while still allowing the original data to be reconstructed perfectly when given access to the correlated quantum system.

We can use the following operational interpretation to further visualize the importance of those entropy measures for quantum cryptography. Consider the case in which Alice possesses a random key K that she intends to keep secret from an adversary, Eve. We say Eve has a state ρ_E^k on a quantum system E that is correlated with the value of Alice's key K . The cq state representing this scenario is:

$$\rho_{KE} = \sum_{k \in K} p_K(k) |k\rangle \langle k| \otimes \rho_E^k \quad (2.67)$$

where $\{|k\rangle\}_k$ is an orthonormal basis representing Alice's possible keys with probability distribution $\{p_k\}_k$. Min-entropy of classical distribution can be viewed as a guessing probability [Konig, Renner e Schaffner 2009], called P_{guess} . It can be interpreted as the probability of Eve correctly guessing K while using the best possible strategy at her disposal (i.e. an optimal measurement strategy on her state ρ_E^k). We can describe this scenario by defining this probability that Eve correctly guesses K when using an optimal measurement strategy as:

$$P_{\text{guess}}(K|E) = \max_{\{E_k\}} \sum_{k \in K} p_K(k) \text{Tr}[E_k \rho_E^k] \quad (2.68)$$

with $\{E_k\}$ being the POVM elements of a generic quantum measurement on system E . Eve's guessing probability on Alice's key can then be related to the min-entropy of the state (2.67) [Konig, Renner e Schaffner 2009]:

$$H_{\min}(K|E)_\rho = -\log P_{\text{guess}}(K|E) \quad (2.69)$$

Thus, higher min-entropy implies greater secrecy, as Eve's probability of guessing K diminishes exponentially.

2.7.4 Smooth Min- and Max-Entropy

A powerful generalization of the Shannon and von Neumann entropies is in the form of the smooth min- and max- entropies. They are optimizations of their corresponding non-smooth versions over a region of states surrounding ρ_{AB} and are useful in order to account for errors and imperfections on a given protocol.

Definition 2.9 (Smooth entropies). Let ρ_{AB} be a bipartite quantum state. The smooth min- and max- entropy of A conditioned on B of that state are given by:

$$H_{\min}^{\varepsilon}(A|B)_{\rho} = \max_{\sigma \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\sigma} \quad (2.70)$$

$$H_{\max}^{\varepsilon}(A|B)_{\rho} = \min_{\sigma \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\max}(A|B)_{\sigma} \quad (2.71)$$

where $\mathcal{B}^{\varepsilon}(\rho_{AB})$ is a ball of ε -close states centered in ρ_{AB} .

The smooth min- and max- entropies have a particularly notable property, called the *quantum asymptotic equipartition property*, shown in [Tomamichel, Colbeck e Renner 2009]:

$$H(A|B)_{\rho} = \lim_{\substack{\varepsilon \rightarrow 0 \\ n \rightarrow \infty}} \frac{1}{n} H_{\min}^{\varepsilon}(A^n|B^n)_{\rho^{\otimes n}} \quad (2.72)$$

$$H(A|B)_{\rho} = \lim_{\substack{\varepsilon \rightarrow 0 \\ n \rightarrow \infty}} \frac{1}{n} H_{\max}^{\varepsilon}(A^n|B^n)_{\rho^{\otimes n}}. \quad (2.73)$$

This property provides a rigorous link between the smooth min- and max-entropies and the von Neumann entropy. In the limit of large, i.i.d. states, the one-shot entropies converge to the von Neumann entropy, thereby extending its applicability to practical, finite-key scenarios. This connection is crucial in QKD as it bridges the gap between idealized, asymptotic security proofs and the realistic, error-prone conditions encountered in experiments.

3 Quantum Key Distribution

In this chapter, we delve into the foundations of Quantum Key Distribution (QKD). The primary objective of a QKD protocol is to enable two distant parties to establish a shared secret key, with its secrecy quantified by the secret key rate. The secret key rate represents the fraction of the key that is provably secure from eavesdropping.

We begin by introducing the one-time pad, an encryption scheme known for its theoretically-perfect security, provided the parties can securely generate and share a random secret key—the task addressed by QKD. We then discuss the basic structure of QKD protocols, which typically consist of two main phases: quantum transmission and classical post-processing. As a concrete example, we examine the BB84 protocol [Bennett e Brassard 1984], widely regarded as the most fundamental and robust QKD protocol, and demonstrate its security in the asymptotic regime.

3.1 The One-Time Pad

The *Vernam cipher*, or *one-time pad* [Vernam 1926], is one of the earliest encryption schemes proven to be unconditionally secure. In this scheme, two parties, Alice and Bob, communicate a message m securely, provided they share a secret key k . The message can be any type of information that the parties could exchange and the key is anything that can be used to encrypt the message. For simplicity, we assume both the message and the key are represented as bit strings (sequences of 0s and 1s).

Suppose Alice and Bob previously met in person and secretly shared a key $k \in \{0, 1\}^l$ of length l before returning to their distant locations. To send a message $m \in \{0, 1\}^l$ of the same length in secrecy, Alice uses the one-time pad encryption scheme, applying a binary XOR operation between the message and her key:

$$e = (e_1, e_2, \dots, e_l) = (m_1 \oplus k_1, m_2 \oplus k_2, \dots, m_l \oplus k_l) = m \oplus k. \quad (3.1)$$

The resulting ciphertext e is transmitted to Bob over a public channel accessible to eavesdroppers. Upon receiving e , Bob decrypts it using his copy of the key k by applying XOR to the ciphertext, $e \oplus k$. Since XOR is its own inverse, Bob recovers the original message as long as they have matching keys:

$$e \oplus k = (m \oplus k) \oplus k = m. \quad (3.2)$$

This demonstrates that the one-time pad is *correct*: it allows the intended recipient to retrieve the original message. However, an encryption scheme also needs to be *secure*.

Definition 3.1 (Security). An encryption scheme is *secure* or *secret* if for all prior distributions $p(m)$ over messages and all messages m , we have

$$p(m) = p(m|e), \quad (3.3)$$

where e is the cipher text.

In other words, an encryption scheme is called secure if the probability of obtaining the message is completely uncorrelated from the publicly transmitted cyphertext. To show that the one-time pad is secure, we will assume that the key k is uniformly random over all l -bit strings. Since for each bit e_l the probability of correctly guessing m_l is $1/2$, we have:

$$p(e|m) = p(m \oplus k|m) = p(k|m) = p(k) = \frac{1}{2^l}. \quad (3.4)$$

Consequently, for all prior distributions over m , the probability of e is:

$$p(e) = \sum_m p(m)p(e|m) = \frac{1}{2^l}. \quad (3.5)$$

We can apply the Bayes rule to find:

$$p(m|e) = \frac{p(m, e)}{p(e)} = \frac{p(e|m)p(m)}{p(e)} = p(m), \quad (3.6)$$

and thus it is secure.

Despite its theoretical appeal, the one-time pad has significant practical limitations. For the scheme to remain secure, the following assumptions must hold:

- The key needs to be truly random, meaning the bits that compose it are not correlated with each other (i.e. knowing the n -first bits does not reveal any information about the $n + 1$ -th bit).
- The key must be at least as long as the message.
- Each key can only be used once. Reusing keys compromises security, as an eavesdropper could eventually infer information about the messages.
- The keys must remain confidential and inaccessible to potential eavesdroppers.

These requirements make the one-time pad impractical for most real-world applications, as securely generating and sharing long random keys between distant parties is challenging. This is where Quantum Key Distribution provides a compelling solution. By leveraging the inherent randomness of quantum mechanics, the no-cloning theorem (discussed in Section 2.6.4) and other quantum properties, QKD enables the secure generation of random keys at a distance, overcoming the practical hurdles of the one-time pad.

3.2 The Framework of a QKD protocol

As mentioned earlier, the goal of a generic Quantum Key Distribution (QKD) protocol is to enable two distant parties, typically referred to as Alice and Bob, to establish a shared secret key, secure from a potential adversary, commonly named Eve. For any QKD protocol, Alice and Bob are assumed to have two communication channels at their disposal: a quantum channel, used to exchange quantum states with bits of information encoded in them (e.g., via photon polarization), and a classical channel, which is authenticated—meaning Alice and Bob can verify each other’s identities—but which is also accessible to Eve. The general structure of a QKD protocol can be outlined as follows:

1. **Quantum transmission.** Alice and Bob exchange quantum information via the quantum channel, which is vulnerable to eavesdropping since Eve is assumed to have full access to it. This step can involve either a *Prepare-and-Measure* (PM) strategy, where one party sends quantum states to the other, or an *Entanglement-Based* (EB) strategy, where both parties receive subsystems of an entangled state generated by an untrusted source. The equivalence of these two approaches will be demonstrated in the next section.
2. **Quantum measurement.** In each round, Bob (and Alice, in the EB strategy) performs measurements on the incoming quantum signal in order to retrieve the encoded information. After M rounds of the protocol, Alice and Bob should share a key of length M , which contain errors that may be caused by Eve’s tampering.
3. **Sifting.** Alice and Bob communicate via the authenticated classical channel to compare their chosen basis for preparations and measurements (or only measurements, in the EB strategy). They will discard the rounds in which their chosen basis differ, obtaining a raw key each.
4. **Classical parameter estimation.** Using the authenticated classical channel, Alice and Bob exchange partial information to align their data. They disclose a subset of their raw keys to estimate the error rate and detect potential eavesdropping. If the error rate exceeds a predefined threshold, they abort the protocol.
5. **Information reconciliation.** Alice and Bob apply error-correction protocols to reconcile their raw keys. After the protocol is done, they use information reconciliation protocols in order to verify that the keys match.
6. **Privacy amplification.** To eliminate any information Eve might have gained, Alice and Bob apply *randomness extractors* on their keys. This process compresses the reconciled key into a shorter, secure key. The final keys K_A and K_B should

be identical with a small probability of mismatch, ensuring high confidence in the protocol's security and correctness.

While many QKD protocols follow this general framework, several key assumptions are necessary for efficient key generation:

- **Quantum Mechanics is a correct theory.** The correctness of quantum information theory underpins QKD. If quantum states behaved differently in practice (e.g., violating the no-cloning theorem), the protocol would not be safe.
- **Alice and Bob have isolated labs.** Alice's and Bob's laboratories must be secure from external interference. If Eve could access their preparations and measurements, the protocol's security would be compromised.
- **Alice and Bob have trusted devices.** The devices used, such as detectors or photon sources in PM setups, must function reliably and be free from Eve's tampering. Some protocols relax this assumption, as discussed in the next chapter.
- **Classical communication is authenticated.** Alice and Bob must confirm they are communicating directly with each other, even if Eve intercepts the classical messages. Authentication ensures that error correction and privacy amplification are performed correctly.

QKD protocols generally comprise two phases: quantum transmission and classical post-processing. The first phase involves quantum experiments to generate raw keys. In an ideal scenario without loss or errors, these keys should be identical. The second phase uses classical algorithms to correct errors and minimize information leakage. Even with the above assumptions, Eve is assumed to have full access to both quantum and classical channels, enabling her to correlate her system with the transmitted information. However, QKD protocols are designed to detect Eve's presence through measurable parameters such as the error rate and to quantify security via the secret key rate, which reflects the amount of key material uncorrelated with Eve's information.

In the next section, we will introduce the foundational QKD protocol, BB84 [[Bennett e Brassard 1984](#)], and use it as a case study to explore potential attacks by Eve and the strategies Alice and Bob can employ to ensure the protocol's security.

3.3 The BB84 Protocol

The BB84 protocol [Bennett e Brassard 1984], named after its inventors Charles Bennet and Gilles Brassard, was the first Quantum Key Distribution (QKD) protocol to be conceptualized. It remains the most fundamental and widely studied QKD protocol due to its simplicity and robust theoretical security. The protocol can be implemented using either a Prepare-and-Measure (PM) strategy or an Entanglement-Based (EB) strategy.

In the PM version, Alice has a source of single photons in her lab, using the photon's polarization to encode bits of information. Alice and Bob will then agree on using two sets of bases for the experiment: the Z basis, defined by the horizontal (0°) and the vertical (90°) directions, and the X basis, defined by the diagonal (45°) and anti-diagonal (-45°) directions. These bases correspond to the eigenstates of a two-dimensional Hilbert space, and the bits of information are encoded in qubits representing states in those bases. The Z basis consists in $\{|0\rangle, |1\rangle\}$ and the X basis consists in $\{|+\rangle, |-\rangle\}$, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. These states are not orthogonal between bases, as $\langle 0|\pm\rangle = 1/\sqrt{2}$ and $\langle 1|\pm\rangle = \pm 1/\sqrt{2}$.

The steps of the protocol are as follows:

1. **Quantum transmission.** Alice randomly selects a basis (Z or X) then randomly prepare a state in the selected basis. She encodes the bits a by associating the bit value $a = 0$ with the states $|0\rangle$ and $|+\rangle$ and the bit value $a = 1$ with the states $|1\rangle$ and $|-\rangle$. Alice then sends the prepared quantum state to Bob via a quantum channel.
2. **Quantum measurement.** Bob randomly selects a basis (Z or X) for each incoming state and measures it accordingly. He records the outcome b using the same bit encoding as Alice. This process is repeated M times, resulting in bit strings A_M for Alice and B_M for Bob.
3. **Sifting.** Alice and Bob communicate via an authenticated classical channel to reveal their chosen basis for each round. They discard the rounds where their basis choice differ. If Bob's measurement basis matches Alice's preparation basis in a given round, he (in principle) correctly learns the encoded bit. If his basis differs, his result is random with a 50% probability for each bit value. By the end of this step, they retain sifted bit strings A_m and B_m , with length $m \approx M/2$.
4. **Parameter estimation.** Alice and Bob reveal a subset of their bit strings in order to estimate the quantum bit error rates (QBERs). They calculate the QBER for the Z basis as $E_Z = p_{ZZ}(a \neq b)$ and for the X basis as $E_X = p_{XX}(a \neq b)$. The QBERs are the probabilities of bit disagreements in rounds where the same basis was used.

After discarding the revealed subset, Alice and Bob are left with their *raw keys*, R_A and R_B .

5. **Information reconciliation.** Alice and Bob perform error correction protocols. We will discuss the case in which they use a one-way error correction process, where Alice sends information to Bob to help him correct his raw key R_B . This ensures that Bob's corrected key \tilde{R}_B matches Alice's raw key: $R_B \rightarrow \tilde{R}_B = R_A$. They need to verify if the procedure was successful, so Alice applies a randomly chosen two-universal hash function (further discussed in the security analysis) to her key with output h_A . Bob then applies the same function to his key, obtaining output h_B . They compare the outputs of this procedure, and if $h_A \neq h_B$, they don't have the same keys and the protocol is aborted.
6. **Privacy amplification.** Alice and Bob compress their key by removing the information leaked to Eve in the previous steps of the protocol via a randomness extractor. In the end, $R_A \rightarrow k_a \in \{0, 1\}^\ell$ and $\tilde{R}_B \rightarrow k_b \in \{0, 1\}^\ell$, with k_a and k_b secret and ℓ is the length of the secret key.

At the protocol's conclusion, Alice and Bob must share identical keys $k_a = k_b$. The protocol satisfies *correctness* if the probability of key mismatch is bounded by:

$$p(k_a \neq k_b) \leq \epsilon_{\text{cor}}, \quad (3.7)$$

where ϵ_{cor} is the pre-agreed correctness error tolerance. For *secrecy*, the final key must be statistically independent of Eve's quantum system E . This is quantified by the trace distance between the real protocol state $\rho_{k_a E}$: a c.q. state consisting of Alice's final key, k_a , and Eve's quantum side information E , and an ideal scenario where Eve's state ρ_E is uncorrelated with Alice's uniform key τ_{k_a} :

$$\|\rho_{k_a E} - \tau_{k_a} \otimes \rho_E\|_1 \leq \epsilon_{\text{sec}}, \quad (3.8)$$

where ϵ_{sec} is the secrecy error tolerance, and τ_{k_a} represents the maximally mixed state over all possible ℓ -bit keys:

$$\tau_{k_a} = \frac{1}{2^\ell} \sum_{k \in \{0, 1\}^\ell} |k\rangle \langle k|_A. \quad (3.9)$$

The protocol is deemed *secure* if the total security parameter $\epsilon = \epsilon_{\text{cor}} + \epsilon_{\text{sec}}$ remains within acceptable bounds. A key performance metric is the *secret key rate*—the number of secure key bits ℓ generated per protocol round M :

$$r = \frac{\ell}{M} \quad (3.10)$$

For simplicity, we compute this rate in the asymptotic regime ($M \rightarrow \infty$), where finite-size effects vanish. While unrealistic, this regime provides a fundamental performance benchmark for QKD protocols.

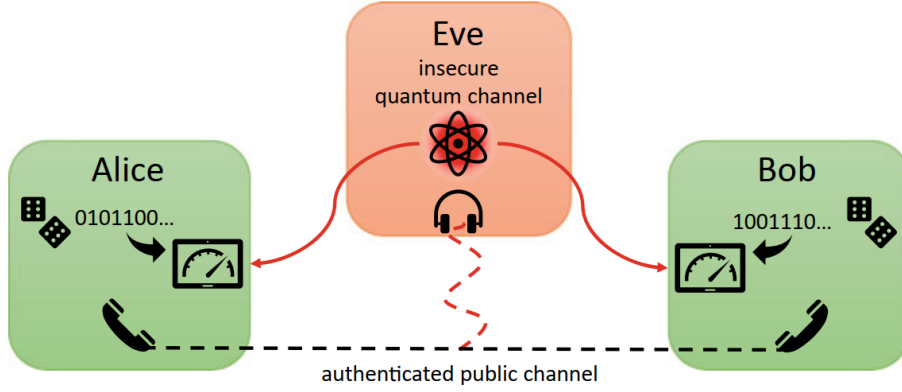


Figure 1 – Entanglement-Based BB84 protocol schematic. An untrusted source distributes entangled states to Alice and Bob via a quantum channel. In each round, Alice and Bob randomly choose measurement bases (Z or X) and record outcomes. After transmission, they publicly compare a subset of bases to perform parameter estimation: mismatched bases test for eavesdropping (via error rates), while matched bases generate raw key bits. Final key distillation uses classical post-processing (error correction and privacy amplification) to eliminate Eve’s information. Security relies on certifying entanglement through observed correlations.

Source: [Grasseli 2021]

We analyze the entanglement-based (EB) variant of BB84, described in Fig. (1), where Eve prepares one of the Bell states

$$|\psi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0, j\rangle + (-1)^i |1, 1 - j\rangle), \quad (3.11)$$

with $i, j \in \{0, 1\}$, and distributes qubits to Alice and Bob via the quantum channel. Both parties randomly measure their qubits in the Z- or X-basis, mirroring the prepare-and-measure (PM) protocol’s outcomes. Note that those strategies are equivalent: since the state Bob receives is conditioned on Alice’s measurement, they will obtain perfectly correlated outcomes if they measure in the same basis and random outcomes otherwise. However, the EB framework strengthens security claims by granting Eve full control over the distributed quantum state.

Finally, we assume Eve performs *collective attacks*, where she prepares identical mixed states ρ_{AB} for each round while holding the purifying system E . The global state $|\phi_{ABE}\rangle$ remains pure, and Alice and Bob’s shared state across M rounds is i.i.d. as $\rho_{AB}^{\otimes M}$. Eve’s presence manifests as errors in Alice and Bob’s correlated measurement outcomes, which are detected during parameter estimation.

We can extend the security proof done in the next section to a more general case where Eve directly distributes the state ρ_{AB}^M while holding the purified state ρ_{ABE}^M . In this case, Eve executes a *coherent attack*, a stronger adversarial strategy where she correlates her actions across all rounds (i.e., the states in each round are not necessarily *i.i.d.*). This

extension can be done using the *postselection technique* [Christandl, König e Renner 2009], as long as the dimension $d = \dim(\mathcal{H}_A \otimes \mathcal{H}_B)$ of Alice’s and Bob’s quantum system is known. Specifically, if an M -round QKD protocol is ϵ -secure against collective attacks, it remains $(M + 1)^{d^2-1}\epsilon$ -secure against coherent attacks, provided the final key length ℓ is reduced by $2(d^2 - 1)\log(M + 1)$ bits.

In the asymptotic regime, coherent attacks can be reduced to collective attacks because the parameters $M \rightarrow \infty$ and $\epsilon \rightarrow 0$ exponentially fast, making the corrections to the secret key rate due to PST negligible. Furthermore, the *Quantum de Finetti theorem* [Renner 2008] states that any symmetric quantum state can be approximated to a mixture of i.i.d. states. Since statistical fluctuations vanish in the asymptotic limit, the state ρ_{ABE}^M is symmetric, thus implying that coherent and collective attacks become effectively equivalent when $M \rightarrow \infty$.

3.3.1 Security Analysis

In order to provide a security analysis for the BB84 protocol, we first need to define some of the post-processing used in the information reconciliation and privacy amplification steps of the protocol. First, the correctness condition (3.7) needs to be verified at the end of the information reconciliation step. In order to do so, Alice and Bob apply a two-universal hash function f_{IR} to their raw keys R_A and \tilde{R}_B , obtaining outcomes h_A and h_B of length $l = \lceil \log(1/\epsilon_{\text{cor}}) \rceil$, where $\lceil x \rceil$ denotes the smallest integer $\geq x$. They randomly select f_{IR} from a family of *two-universal hashing functions* \mathcal{F}_{IR} .

A family $\mathcal{F} = \{f : \{0, 1\}^m \rightarrow \{0, 1\}^l\}$ is defined as two-universal if for all distinct $x, x' \in \{0, 1\}^m$,

$$\Pr_{f \in \mathcal{F}}(f(x) = f(x')) \leq \frac{1}{2^l}. \quad (3.12)$$

This means that the probability that the two outputs $f_{\text{IR}}(R_A) = h_A$ and $f_{\text{IR}}(\tilde{R}_B) = h_B$ coincide given that the inputs R_A and \tilde{R}_B are different is given by $2^{-\lceil \log(1/\epsilon_{\text{cor}}) \rceil}$:

$$p(h_A = h_B | R_A \neq \tilde{R}_B) \leq 2^{-\lceil \log(1/\epsilon_{\text{cor}}) \rceil} = \epsilon_{\text{cor}}. \quad (3.13)$$

The subsequent post-processing steps are identically applied to both Alice and Bob’s raw keys. Therefore, if $h_A = h_B$, they have matching raw keys (except for probability ϵ_{cor}) and their final keys k_a and k_b are ϵ_{cor} -correct, as described in (3.7). Note that this process leaks information to Eve, which can be denoted by $\Gamma = \text{leak}_{\text{IR}} + \log(1/\epsilon_{\text{cor}}) \leq \text{leak}_{\text{IR}} + \log(2/\epsilon_{\text{cor}})$.

To verify the secrecy condition, we need to look into the privacy amplification step. Let us assume that Alice and Bob apply a different hashing function $f_{\text{PA}} : \{0, 1\}^m \rightarrow \{0, 1\}^\ell$ to their raw keys R_A and \tilde{R}_B , producing final keys $k_a = f_{\text{PA}}(R_A)$ and $k_b = f_{\text{PA}}(\tilde{R}_B)$. Here, the hash function is used for its randomness extraction property—the goal is to transform

Alice and Bob's raw keys into a smaller, uniformly random bit string that is independent of Eve's system.

The *Quantum Leftover Hash Lemma* [Tomamichel et al. 2011] provides an upper bound for the trace distance between the final key state and an ideal uniform key. Let $\rho_{R_A E}$ denote the classical-quantum (c.q.) state comprising Alice's raw key R_A and Eve's quantum side information E . Applying a random $f_{PA} \in \mathcal{F}_{PA}$ to Alice's raw key in $\rho_{R_A E}$ generates the final state $\rho_{k_a E}$.

Lemma 3.1 (Quantum Leftover Hash Lemma). For a c.q. state $\rho_{R_A E}$ and a randomly selected two-universal hash function $f \in \mathcal{F}$, the following inequality holds:

$$\|\rho_{k_a F E} - \tau_{k_a} \otimes \rho_{F E}\|_1 \leq 2\varepsilon + \frac{1}{2} \sqrt{2^{\ell - H_{\min}^\varepsilon(R_A|E)}}, \quad (3.14)$$

where τ_{k_a} is the maximally mixed state on Alice's key, k_a , and F represents the subsystem storing the chosen hash function f .

Note that during the information reconciliation and privacy amplification steps, Eve gains classical information on the key. Therefore, her subsystem E_{total} could be described by a subsystem which is quantum in E and classical in C , and the smooth min-entropy $H_{\min}^\varepsilon(R_A|EC)_\rho$ satisfies:

$$H_{\min}^\varepsilon(R_A|EC)_\rho \geq H_{\min}^\varepsilon(R_A|E)_\rho - \log |C|. \quad (3.15)$$

Here, C comprises the information leaked during PE and IR steps, namely $\log |C| = \text{leak}_{PE} + \text{leak}_{IR} + \log(2/\epsilon_{\text{cor}})$. In the asymptotic limit, the leakage for PE, which consists mostly on the fraction of the key revealed to estimate QBERs, becomes negligible compared to the total number of rounds, and therefore vanishes.

By the end of the PA step, Alice and Bob can set the key length ℓ as:

$$\ell = H_{\min}^\varepsilon(R_A|E)_\rho - \text{leak}_{IR} - \log \frac{2}{\epsilon_{\text{cor}}} - 2 \log \frac{1}{2\epsilon_{\text{pa}}}. \quad (3.16)$$

To obtain a secrecy parameter, we can rewrite (3.14) with the secrecy condition (3.8) and substitute ℓ :

$$\begin{aligned} \|\rho_{k_a F E} - \tau_{k_a} \otimes \rho_{F E}\|_1 &\leq \epsilon_{\text{sec}} \leq 2\varepsilon + \frac{1}{2} \sqrt{2^{\ell - H_{\min}^\varepsilon(R_A|E)_\rho + \text{leak}_{IR} + \log 2/\epsilon_{\text{cor}}}} \\ &\leq 2\varepsilon + \frac{1}{2} \sqrt{2^{\log(2\epsilon_{\text{pa}})^2}} = 2\varepsilon + \epsilon_{\text{PA}}. \end{aligned} \quad (3.17)$$

Thus, the protocol is ϵ_{sec} -secret, with $\epsilon_{\text{sec}} \leq 2\varepsilon + \epsilon_{\text{PA}}$. Combining this with the correctness condition, this protocol is ϵ -secure, with $\epsilon \leq 2\varepsilon + \epsilon_{\text{PA}} + \epsilon_{\text{cor}}$.

The asymptotic secret key rate r_∞ , defined as secret bits per round, is:

$$r_\infty = \lim_{M \rightarrow \infty} \frac{\ell}{M}. \quad (3.18)$$

Over many rounds, the size of the key is such that the terms related to the parameters ϵ_{cor} and ϵ_{PA} vanish, resulting in:

$$r_{\infty} = \lim_{M \rightarrow \infty} \frac{H_{\min}^{\epsilon}(R_A|E)_{\rho} - \text{leak}_{\text{IR}}}{M}. \quad (3.19)$$

Considering an one-way error correction protocol, the leakage term referring to the IR step can be interpreted as the minimal amount of information Alice sends to Bob that allows him to correct his key given his noisy bit string. This can be quantified by the smooth max-entropy between Alice's and Bob's raw keys: $\text{leak}_{\text{IR}} \approx H_{\max}^{\epsilon}(R_A|R_B)_{\rho}$, neglecting finite-key terms. Also, the entropies are computed on the i.i.d. states $\rho_{R_A R_B E}^{\otimes M}$ shared across M rounds, which allows us to use the quantum asymptotic equipartition property defined in (2.72) and (2.73) to obtain:

$$r_{\infty} = \lim_{\substack{\epsilon \rightarrow 0 \\ M \rightarrow \infty}} \frac{1}{M} (H_{\min}^{\epsilon}(R_A|E)_{\rho} - H_{\max}^{\epsilon}(R_A|R_B)_{\rho}) = H(R_A|E)_{\rho} - H(R_A|R_B)_{\rho}. \quad (3.20)$$

We can use the definition of mutual information to recover the *Devetak-Winter rate* [Devetak e Winter 2005] for protocols with one-way error correction:

$$r_{\text{DW}} = H(R_A : R_B) - H(R_A : E), \quad (3.21)$$

where $H(R_A : R_B)$ and $H(R_A : E)$ quantifies the mutual information shared between Alice and Bob and Alice and Eve, respectively. Thus, the secret key rate is, in essence, the amount of information that Alice and Bob's raw keys bits have in common minus the amount of information that Eve has gained on Alice's key bit. From here, we will omit the subscript ρ and use the following description for the secret key rate:

$$r = H(R_A|E) - H(R_A|R_B). \quad (3.22)$$

Our goal is to express (3.22) in terms of the quantum bit error rates (QBERs) E_Z and E_X , enabling a direct link between observed errors and achievable secrecy.

For efficiency, we consider an asymmetric protocol where the Z -basis is used for both key generation and PE, while the X -basis is reserved for PE. By choosing a small probability of X basis rounds, p_X , the probability of key-generating Z -basis rounds $p_Z = 1 - p_X$ dominates, maximizing the usable key fraction.

The classical-quantum-classical (c.c.q.) state $\rho_{R_A R_B E}$ governing the entropy calculations in (3.22) arises from Alice and Bob's Z -basis measurements on the tripartite pure state $|\Phi_{ABE}\rangle$ distributed by Eve. Let $\{|a\rangle\}_{a=0}^1$ and $\{|b\rangle\}_{b=0}^1$ denote the computational basis states. The state after the quantum measurement step is:

$$\rho_{R_A R_B E} = \sum_{a,b=0}^1 (|a\rangle \langle a| \otimes |b\rangle \langle b| \otimes \mathbb{I}_E) |\Phi_{ABE}\rangle \langle \Phi_{ABE}| (|a\rangle \langle a| \otimes |b\rangle \langle b| \otimes \mathbb{I}_E). \quad (3.23)$$

Without loss of generality, we assume Eve prepares a *Bell-diagonal state* $\tilde{\rho}_{AB}$ for Alice and Bob:

$$\tilde{\rho}_{AB} = \sum_{i,j=0}^1 \lambda_{ij} |\psi_{ij}\rangle \langle \psi_{ij}|, \quad (3.24)$$

where $\{|\psi_{ij}\rangle\}$ are Bell states defined in (2.46):

$$|\psi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0, j\rangle + (-1)^i |1, 1-j\rangle) \quad (3.25)$$

with $i, j \in \{0, 1\}$ and λ_{ij} satisfy $0 \leq \lambda_{ij} \leq 1$ with $\sum_{ij} \lambda_{ij} = 1$. This can be done via symmetrization maps \mathcal{E}_X and \mathcal{E}_Z , defined as:

$$\mathcal{E}_X(\rho_{AB}) = \frac{1}{2} (\mathbb{I} \otimes \mathbb{I}) \rho_{AB} (\mathbb{I} \otimes \mathbb{I}) + \frac{1}{2} (X \otimes X) \rho_{AB} (X \otimes X), \quad (3.26)$$

$$\mathcal{E}_Z(\rho_{AB}) = \frac{1}{2} (\mathbb{I} \otimes \mathbb{I}) \rho_{AB} (\mathbb{I} \otimes \mathbb{I}) + \frac{1}{2} (Z \otimes Z) \rho_{AB} (Z \otimes Z). \quad (3.27)$$

The combined operation $(\mathcal{E}_X \circ \mathcal{E}_Z)$ symmetrizes the state into:

$$\begin{aligned} \tilde{\rho}_{AB} = \frac{1}{4} & \left[\rho_{AB} + (Z \otimes Z) \rho_{AB} (Z \otimes Z) \right. \\ & \left. + (X \otimes X) \rho_{AB} (X \otimes X) + (Y \otimes Y) \rho_{AB} (Y \otimes Y) \right], \end{aligned} \quad (3.28)$$

This can be done because, from the parties' point of view, the only observing effect of this operation is the symmetrization of the marginals: the action of the map $(\mathcal{E}_X \circ \mathcal{E}_Z)$ is equivalent to a simultaneous bit flip of both Alice's and Bob's bits, thus not affecting the QBERs or their raw keys correlations. This operation is also not disadvantageous to Eve: since she is preparing the state $\tilde{\rho}_{AB}$, she also holds its purification and her uncertainty on Alice's (or Bob's) key does not increase with this symmetrization. In other words, $H(R_A|E)_\rho \geq H(R_A|E)_{\tilde{\rho}}$. The proof for this argument can be found in the Appendix Section A.

Since the QBERs are defined by the probability of Alice and Bob obtaining different measurement outcomes when choosing the same basis, we can write that:

$$E_Z = \text{Tr} [(|0\rangle \langle 0| \otimes |1\rangle \langle 1| + |1\rangle \langle 1| \otimes |0\rangle \langle 0|) \tilde{\rho}_{AB}] = \lambda_{01} + \lambda_{11}, \quad (3.29)$$

$$E_X = \text{Tr} [(|+\rangle \langle +| \otimes |-\rangle \langle -| + |-\rangle \langle -| \otimes |+\rangle \langle +|) \tilde{\rho}_{AB}] = \lambda_{10} + \lambda_{11}. \quad (3.30)$$

First, we compute the conditional entropy $H(R_A|E)$ appearing in (3.22), which quantifies Eve's uncertainty about Alice's raw key R_A . Since Eve holds the purifying system of the symmetrized Bell-diagonal state $\tilde{\rho}_{AB}$, the global state shared between Alice, Bob, and Eve is pure and can be expressed as:

$$|\Phi_{ABE}\rangle = \sum_{i,j=0}^1 \sqrt{\lambda_{ij}} |\psi_{ij}\rangle_{AB} \otimes |\varphi_{ij}\rangle_E, \quad (3.31)$$

where $\{|\varphi_{ij}\rangle\}_{i,j=0}^1 \in \mathcal{H}_E$ forms an orthonormal basis for Eve's subsystem.

To derive $\rho_{R_A E}$, we trace out Alice and Bob's subsystems after Alice performs her Z -basis measurement:

$$\begin{aligned}
\rho_{R_A E} &= \sum_{a=0}^1 |a\rangle \langle a|_{R_A} \otimes \text{Tr}_{AB} [(|a\rangle \langle a| \otimes \mathbb{I}_{BE}) |\Phi_{ABE}\rangle \langle \Phi_{ABE}|] \\
&= \sum_{a=0}^1 |a\rangle \langle a|_{R_A} \otimes \sum_{i,j,k,l=0}^1 \sqrt{\lambda_{ij}\lambda_{kl}} \text{Tr}_{AB} [(|a\rangle \langle a| \otimes \mathbb{I}_B) |\psi_{ij}\rangle \langle \psi_{kl}|_{AB}] \otimes |\varphi_{ij}\rangle \langle \varphi_{kl}|_E \\
&= \sum_{a=0}^1 p(a) |a\rangle \langle a|_{R_A} \otimes \sum_{i,j,k=0}^1 \sqrt{\lambda_{ij}\lambda_{kj}} (-1)^{(i+k)a} |\varphi_{ij}\rangle \langle \varphi_{kj}|_E.
\end{aligned} \tag{3.32}$$

where $p(a) = 1/2$ is the probability of obtaining outcome a on Alice's Z -basis measurement.

This allows us to define Eve's conditional state ρ_E^a for each outcome a :

$$\rho_E^a = \sum_{i,j,k=0}^1 \sqrt{\lambda_{ij}\lambda_{kj}} (-1)^{(i+k)a} |\varphi_{ij}\rangle \langle \varphi_{kj}|_E. \tag{3.33}$$

The non-zero eigenvalues of ρ_E^a are $\{\lambda_{00} + \lambda_{10}, \lambda_{01} + \lambda_{11}\}$, which remain independent of a . This can be shown if we divide ρ_E^a into two parts ($j = 0$ and $j = 1$) and take their respective eigenvalues:

$$\rho_E^a = \sum_{i,k=0}^1 \sqrt{\lambda_{i0}\lambda_{k0}} (-1)^{(i+k)a} |\varphi_{i0}\rangle \langle \varphi_{k0}| + \sqrt{\lambda_{i1}\lambda_{k1}} (-1)^{(i+k)a} |\varphi_{i1}\rangle \langle \varphi_{k1}|. \tag{3.34}$$

For the first term,

$$\gamma^2 - (\lambda_{00} + \lambda_{10})\gamma + \lambda_{00}\lambda_{10} - \lambda_{00}\lambda_{10} = \gamma(\gamma - (\lambda_{00} + \lambda_{10})) = 0 \tag{3.35}$$

and thus the eigenvalues are $\gamma = 0$ and $\gamma = \lambda_{00} + \lambda_{10}$. The same logic applies for $j = 1$, yielding eigenvalues 0 and $\lambda_{01} + \lambda_{11}$. Note that the phase factor $(-1)^a$ squares to 1 when computing the eigenvalues of ρ_E^a .

To compute $H(R_A|E)$, we use the entropy chain rule:

$$H(R_A|E) = H(E|R_A) + H(R_A) - H(E). \tag{3.36}$$

The first term is calculated for the state (3.32) while using the expression for the conditional entropy of a c.q. state (2.63), and it reads:

$$H(E|R_A) = \sum_{a=0}^1 p(a) H(\rho_E^a) = H(\{\lambda_{00} + \lambda_{10}, \lambda_{01} + \lambda_{11}\}). \tag{3.37}$$

Since $E_Z = \lambda_{01} + \lambda_{11}$ and $\sum_{i,j=0}^1 \lambda_{ij} = 1$, we can write:

$$H(E|R_A) = -E_Z \log(E_Z) - (1 - E_Z) \log(1 - E_Z) = h(E_Z). \tag{3.38}$$

The symmetry of Alice's raw key ensures

$$H(R_A) = - \sum_{a=0}^1 p(a) \log(p(a)) = -(\frac{1}{2} \log \frac{1}{2} + \frac{1}{2} \log \frac{1}{2}) = 1. \quad (3.39)$$

Since $|\Phi_{ABE}\rangle$ is pure, $H(ABE) = 0$. Moreover, the reduced density matrixes derived from $|\Phi_{ABE}\rangle$, $\tilde{\rho}_{AB}$ and ρ_E , have the same eigenvalues $\{\lambda_{ij}\}_{i,j=0}^1$ and we can write $H(E) = H(AB) = H(\{\lambda_{ij}\})$. Thus,

$$H(R_A|E) = 1 + h(E_Z) - H(\{\lambda_{ij}\}). \quad (3.40)$$

The observed error rates E_Z and E_X only partially constrain the eigenvalues $\{\lambda_{ij}\}$, leaving residual freedom in their values. To account for Eve's maximal possible knowledge of the key, we adopt a worst-case security analysis by minimizing $H(R_A|E)$ over all valid eigenvalue configurations. These configurations must satisfy the QBER definitions in (3.29) and (3.30), along with the normalization condition $\sum_{i,j=0}^1 \lambda_{ij} = 1$. This minimization results in [Scarani et al. 2009]:

$$H(R_A|E) = 1 + h(E_Z) - (h(E_X) + h(E_Z)) = 1 - h(E_X). \quad (3.41)$$

The conditional Shannon entropy $H(R_A|R_B)$ is computed on the probability distributions represented by Alice and Bob's Z-basis outcomes, mainly $E_Z = p(a \neq b) = p(a = 0, b = 1) + p(a = 1, b = 0)$, and since those probabilities are symmetrized, it follows that:

$$\begin{aligned} H(R_A|R_B) &= H(R_A, R_B) - H(R_B) = - \sum_{a,b=0}^1 p(a, b) \log p(a, b) - 1 \\ &= -(1 - E_Z) \log \frac{1 - E_Z}{2} - E_Z \log \frac{E_Z}{2} - 1 \\ &= -(1 - E_Z) \log(1 - E_Z) - E_Z \log E_Z + 1 - E_Z + E_Z - 1 \\ &= h(E_Z) \end{aligned} \quad (3.42)$$

where we used the fact that analogously to $H(R_A)$, $H(R_B) = 1$ and $p(a = b) = 1 - E_Z$.

Combining these results, the asymptotic secret key rate for the asymmetric BB84 protocol becomes:

$$r_\infty = p_{ZZ} (1 - h(E_X) - h(E_Z)), \quad (3.43)$$

where p_{ZZ} represents the probability of both parties selecting the Z-basis for measurement.

4 QKD Protocols With Imperfect Devices

This chapter addresses the physical and operational challenges inherent in real-world QKD implementations. While these challenges can often be mitigated, such adaptations risk introducing vulnerabilities that adversaries might exploit to compromise security. We begin by analyzing practical implementations based on attenuated laser pulses—so-called *weak coherent pulses*—and strategies to ensure robustness against specific attacks. Next, we examine *Device-Independent QKD* (DI-QKD), which eliminates trust assumptions on both light sources and detectors but faces severe experimental barriers despite its theoretical security. Finally, we explore two protocols—*Measurement-Device-Independent QKD* (MDI-QKD) and its enhanced variant, *Twin-Field QKD* (TF-QKD)—that retain trusted source assumptions while relaxing security requirements on detectors, thereby offering improved practicality without sacrificing security.

4.1 Practical Implementations of Light Sources

Implementing ideal single-photon sources remains experimentally challenging [Scarani et al. 2009], prompting most QKD protocols to adopt *weak coherent pulses* (WCPs) as a practical alternative. These pulses can be represented by coherent states of the form:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (4.1)$$

where $|n\rangle$ denotes a Fock state with n photons, and $|\alpha|^2 \ll 1$ represents the average photon number per pulse. The photon number follows a Poisson distribution:

$$p(n) = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}, \quad (4.2)$$

resulting in a non-negligible probability of multiphoton emissions:

$$p_{\text{multi}} = 1 - e^{-|\alpha|^2} - |\alpha|^2 e^{-|\alpha|^2} > 0. \quad (4.3)$$

This practical implementation turns into a vulnerability, enabling attacks such as the *photon number splitting* (PNS) attack. Considering a PM scenario, Eve substitutes the lossy quantum channel with a lossless one and performs nondestructive quantum non-demolition (QND) measurements to probe the photon number in each pulse without disturbing their polarizations. For single-photon pulses, she probabilistically blocks them

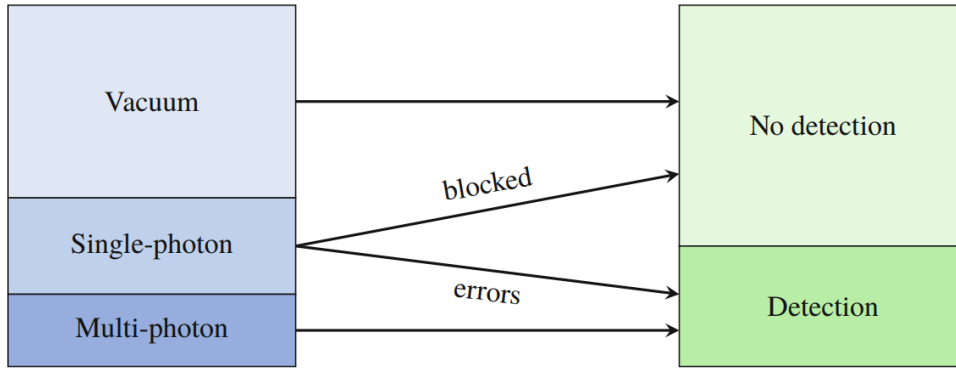


Figure 2 – Photon number splitting (PNS) attack strategy. Eve replaces the quantum channel with a lossless link and uses quantum non-demolition (QND) measurements to sort pulses by photon number: vacuum states ($n = 0$) are forwarded to Bob (no detection); single-photon pulses ($n = 1$) are selectively blocked to mimic channel loss; multiphoton pulses ($n \geq 2$) are split, with one photon stored in Eve’s quantum memory and the rest sent to Bob. After basis reconciliation, Eve measures stored photons to deduce the key, while unblocked single photons may trigger errors via intercept-resend attacks.

Source: [Wolf 2021]

according to the loss probability of the network, so Alice and Bob still observe the network’s regular loss statistics and Eve’s tampering goes unnoticed. For multiphoton pulses, she extracts and stores one photon in a quantum memory while forwarding the remainder to Bob. This way, Bob still receives a signal and Eve can wait until the bases chosen are revealed to perform her measurements. After basis reconciliation, Eve measures her retained photons in the correct basis, thereby gaining exact information on the key bits for each multiphoton round while remaining undetected.

This analysis implies that security hinges on single-photon pulses. In practice, weak coherent pulses (WCPs) with average photon number $|\alpha|^2 = 0.1$ predominantly emit vacuum states, as the vacuum probability $p(0) = e^{-|\alpha|^2} \approx 90.5\%$ dominates. Single-photon events occur with $p(1) \approx 9\%$, while multiphoton events remain rare ($p_{\text{multi}} \approx 0.5\%$). Although further laser attenuation could suppress multiphoton emissions, it severely compromises the protocol’s efficiency. This motivates the use of the *decoy-state* strategy to mitigate risks without sacrificing performance.

While PNS attacks provide a challenge to PM setups in QKD protocols using WCPs, they are not a threat to QKD protocols based on distribution of entangled states from an untrusted source. The security proof shown in section 3.3.1 allows Eve to be in control of the light source as well as the channel, thus allowing her to extract photons and perform PNS attacks. In this context, a PNS attack is equivalent to a collective attack where Eve attaches ancilla photons to entangled states intended for Alice and Bob, already accounted for in the security proof.

4.1.1 Decoy States Strategy

The decoy-state method was first proposed by [Lo 2004], then further developed by [Lo, Ma e Chen 2005]. By randomly varying the intensity of transmitted laser pulses, legitimate users introduce "decoy" signals that mimic ordinary signals but serve a critical diagnostic role. Decoy states allow Alice and Bob to statistically detect eavesdropping attempts, even if the attacker targets multi-photon pulses. The core insight is that Eve cannot distinguish decoy pulses from true signal pulses, forcing any attack to perturb both types equally. By comparing detection rates and errors across different intensities, Alice and Bob can isolate the contribution of single-photon pulses—the only ones trusted for key generation—and bound the eavesdropper's knowledge.

In order to eliminate phase coherence, Alice prepares a phase-randomized WCP. Assuming that the phase θ of a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ is randomized for all signals, the coherent state transforms into a statistical mixture of Fock states with a Poisson photon-number distribution:

$$\rho_\mu = \frac{1}{2\pi} \int_0^{2\pi} d\theta |\sqrt{\mu}e^{i\theta}\rangle \langle \sqrt{\mu}e^{i\theta}| = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} |n\rangle \langle n|, \quad (4.4)$$

where $\mu = |\alpha|^2$ is the average photon number per pulse, and $p(n) = e^{-\mu}\mu^n/n!$ gives the probability of the source emitting n photons. The probability $P^{(n)}$ of Alice sending n photons and Bob registering a detection is:

$$P^{(n)} = e^{-\mu} \frac{\mu^n}{n!} Y^{(n)}, \quad (4.5)$$

where $Y^{(n)}$, the n -photon yield, represents the conditional probability that Bob has a detection event given that Alice sent n photons. These yields cannot be directly observed but are critical for security analysis.

In a typical PM QKD protocol using decoy-states, Alice transmits two types of pulses: *signal states* (ρ_μ), used for key generation, and *decoy states* (ρ_{μ_i}), used for parameter estimation. The decoy states will have their intensity values randomly drawn from a set $\{\mu_i\}_i$ with $\mu_i \neq \mu$ being the only property that differs the signal states from the decoy states. Therefore, Eve cannot distinguish a decoy state from a signal state—to Eve, this is the same scenario as Alice picking a Fock state $|n\rangle \langle n|$ according to a unknown probability distribution and sending it through the quantum channel.

The total gains P_{μ_i} (probability of Bob detecting a signal) and error rate E_{μ_i} for intensities μ_i are expressed as:

$$P_{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y^{(n)} \quad (4.6)$$

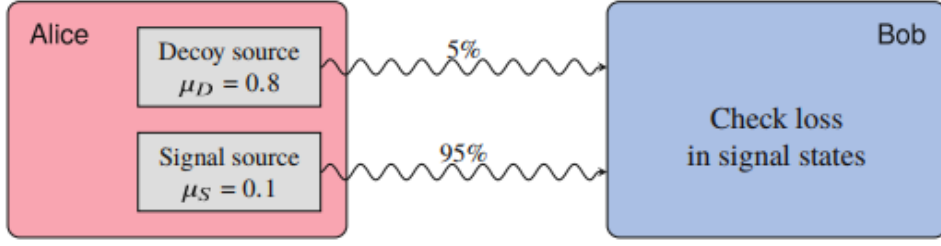


Figure 3 – Example of the decoy-state strategy. Alice uses two weak laser sources: a signal source with low photon number (e.g., $\mu_S = 0.1$) and a decoy source with higher photon number (e.g., $\mu_D = 0.8$). She mixes decoy states (e.g., 5% of pulses) randomly with signal states. After transmission, Alice tells Bob which pulses were decoys. Bob then checks the loss in the signal states—if Eve tried a PNS attack, the signal loss will be much higher than expected, exposing the attack.

Source: [Wolf 2021]

$$E_{\mu_i} P_{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y^{(n)} e^{(n)}, \quad (4.7)$$

where $e^{(n)}$ is the QBER of an n -photon signal. The gains P_{μ_i} and error rates E_{μ_i} can be experimentally measured by Alice and Bob, and since the relations between the variables are linear, they can solve equations (4.6) and (4.7) to derive bounds for $Y^{(n)}$ and $e^{(n)}$ according to the number of different intensities μ_i used. Thus, the more number of decoy intensities μ_i used, the tighter those bounds are.

Prior knowledge of the channel's expected behavior (e.g., baseline loss and noise levels) allows Alice and Bob to define plausible ranges for $Y^{(n)}$ and $e^{(n)}$, which are the quantities that reflect Eve's action on the quantum channel. Therefore, an attack performed by Eve that changes the value of those parameters will be caught with high probability.

For example, the Prepare-Measure BB84 with the decoy-state strategy works with Alice preparing the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ encoded in the polarization of phase randomized WCPs (4.4). It is generally more practical to use an asymmetric version of this strategy. Here, Alice uses the Z basis (key generation) with probability p_Z , where she modulates the pulse intensity to μ (signal state) with probability q or to a decoy intensity μ_i with probability $1 - q$. In the X-basis rounds, chosen with probability $1 - p_Z$, she only generates decoy states. Bob will then choose to measure the incoming pulses in the Z basis with probability p_Z or in the X basis with probability $1 - p_Z$. In the end of transmission, Alice reveals the intensity setting as well as the basis chosen every round. Bob instead reveals all the X-basis outcomes (since they are not used for key generation) to estimate the QBERs $E_X^{\mu_i}$ and some of the Z-basis outcomes to estimate E_Z^μ . The rest of the protocol remains unchanged, and the secret key rate becomes [Wei et al. 2013]:

$$r_{\text{decoy}} \geq p_Z^2 q \left[P_Z^{(0\downarrow)} + P_Z^{(1\downarrow)} (1 - h(e_X^{(1\uparrow)})) - P_Z^\mu h(E_Z^\mu) \right], \quad (4.8)$$

where P_Z^μ and E_Z^μ are the gain and QBER of the signal state, while $P_Z^{(0\downarrow)}$ ($P_Z^{(1\downarrow)}$) is a lower

bound on the probability that Alice sent 0 (1) photon and Bob had a detection event, given that Alice sent a signal state: $P^{(0\downarrow)} = e^{-\mu}Y^{(0\downarrow)}$ and $P_Z^{(1\downarrow)} = e^{-\mu}\mu Y_Z^{(1\downarrow)}$. Here, the yields $Y^{(0\downarrow)}$ and $Y_Z^{(1\downarrow)}$ are estimated from the set of equations in (4.6). Finally, $e_X^{(1\uparrow)}$ is an upper bound on the X -basis error rate on single-photon signals, estimated via (4.7). Note that by considering the ideal case, we recover the secret key rate in (3.43): all states are signal states $q = 1$ and all detection events are caused by single-photons $P^{(0\downarrow)} = 0$, $P_Z^{(1\downarrow)} = P_Z^\mu = 1$ and $e_X^{(1\uparrow)} = E_X$.

4.2 Device Independent QKD

One of the assumptions previously discussed when talking about QKD protocols is that the honest parties, Alice and Bob, have trusted devices. We have also seen those assumptions relaxed in the case of quantum light sources in the Entanglement-Based BB84. Initially proposed in [Ekert 1991], Device-Independent QKD (DI-QKD) relies on "black boxes" (Fig. 4) that perform unknown measurements on an entangled state and give outcomes based on different inputs performed by the parties. By performing *test rounds*, the parties estimate violations of *Bell inequalities* [Bell 1964]—statistical bounds satisfied by classical systems but violated by strong quantum correlations. A Bell violation certifies that their outputs are intrinsically quantum and possibly uncorrelated with any external system (including an eavesdropper). To contextualize DI-QKD security, we first outline Bell inequalities.

4.2.1 Bell Inequalities

Bell's theorem [Bell 1964] demonstrates that quantum mechanics cannot be described by local hidden variable theories. A Bell inequality is usually given by a linear constraint on measurement correlators that holds for classical systems but fails for entangled quantum states.

The *Clauser–Horne–Shimony–Holt (CHSH) inequality* [Clauser et al. 1969] is a canonical example. Consider Alice and Bob each with a black box (Fig. 4) accepting inputs $x, y \in \{0, 1\}$ and producing outputs $a, b \in \{-1, 1\}$. Their joint statistics $p(a, b|x, y)$ define the CHSH polynomial:

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle, \quad (4.9)$$

where $\langle a_x b_y \rangle = \sum_{a,b=\pm 1} ab p(a, b|x, y)$. For classical systems, $S \leq 2$. To see this, note that any classical assignment gives $a_0(b_0 + b_1) + a_1(b_0 - b_1) = \pm 2$. Averaging over all assignments preserves $|\langle S \rangle| \leq 2$.

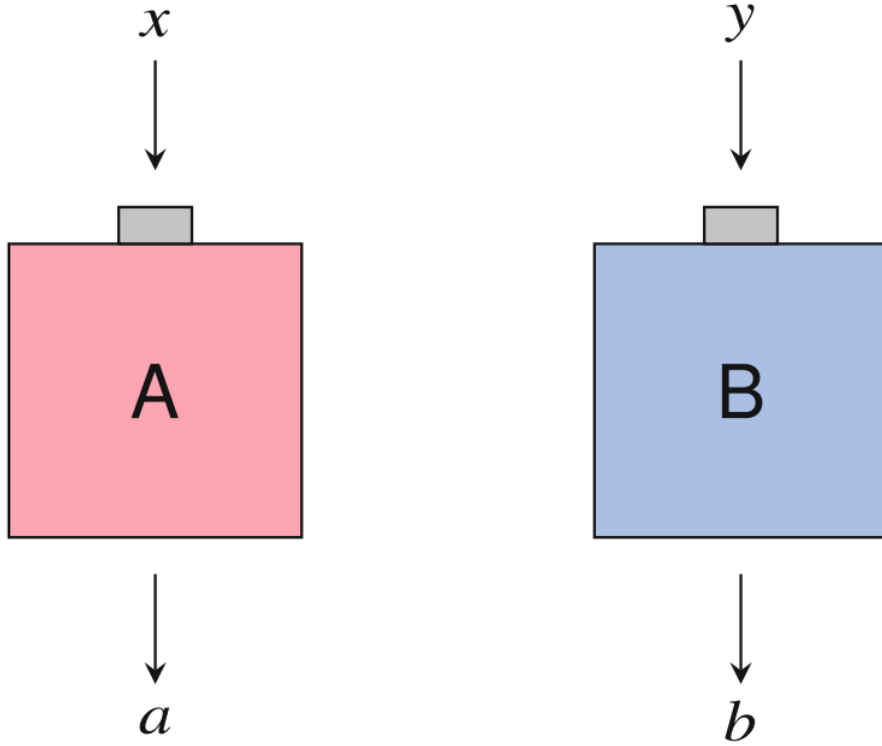


Figure 4 – Characterizing black boxes without internal assumptions. Alice and Bob interact with their devices by selecting inputs (e.g., pressing buttons labeled x or y) and recording outputs a and b . Repeated trials reveal the input-output statistics $\{p(a, b|x, y)\}$, which describe how the boxes behave—without requiring knowledge of their internal mechanisms.

Source: [Wolf 2021]

Quantum mechanics can violate this bound. Suppose Alice and Bob share the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, rewritten using the Pauli operators:

$$|\phi^+\rangle\langle\phi^+| = \frac{1}{4}(\mathbb{I} \otimes \mathbb{I} + X \otimes X + Z \otimes Z - Y \otimes Y). \quad (4.10)$$

Let Alice's measurements be $A_0 = X$, $A_1 = Z$, and Bob's be $B_0 = (X + Z)/\sqrt{2}$, $B_1 = (X - Z)/\sqrt{2}$. The correlators $\langle A_i B_j \rangle = \text{Tr}(A_i \otimes B_j \rho)$ yield:

$$\begin{aligned} S &= \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \\ &= \sqrt{2} \langle \phi^+ | X \otimes X | \phi^+ \rangle + \sqrt{2} \langle \phi^+ | X \otimes X | \phi^+ \rangle \\ &= 2\sqrt{2}, \end{aligned} \quad (4.11)$$

violating the CHSH inequality. This maximal violation ($S = 2\sqrt{2}$) certifies their shared state is maximally entangled. This maximal entanglement is crucial because of the monogamy of entanglement: if Alice and Bob share a maximally entangled state, Eve cannot be significantly correlated with their state without reducing the degree of entanglement between them. In the context of DI-QKD protocols, this means that any attempt by Eve to gain information about the key would necessarily disturb the quantum correlations,

leading to a lower CHSH violation that Alice and Bob could detect. Thus, Alice and Bob need not know their devices' internal workings—they verify Bell inequality violations through observed statistics to guarantee security.

4.2.2 DI-QKD Protocol Based on the CHSH Inequality

In the Ekert-91 (E91) protocol [Ekert 1991], the users can verify the potential action of an eavesdropper by testing the CHSH inequality, and aborting the protocol if needed. Later, [Acín et al. 2007] developed a security proof for this type of protocol by using the CHSH inequality as a parameter in the secret key rate.

Eve distributes possibly entangled states to Alice and Bob, which in turn can perform measurements on these states using uncharacterized measurement devices. Alice's measurement device has three inputs, A_x , $x \in \{0, 1, 2\}$, each with possible outcomes $a \in \{-1, +1\}$ while Bob's device has two inputs, B_y , $y \in \{1, 2\}$, with $b \in \{-1, +1\}$. Before initiating the protocol, Alice and Bob agree on a set of parameters: the total number of rounds M , the probability in which they perform a test round $0 < p_t < 1$, the expected CHSH value $2 < S_{\text{exp}} \leq 2\sqrt{2}$, and its tolerance $0 < \delta < (2\sqrt{2} - 2)$. The step-by-step can be described as:

1. **Quantum transmission.** For each round, Alice and Bob receive a quantum state from an untrusted source. With probability p_t , they perform a test round; otherwise, they execute a key-generation (KG) round.
2. **Quantum measurement.** KG rounds use the input pair (A_0, B_1) to generate raw keys R_A and R_B . Test rounds utilize inputs (A_1, A_2, B_1, B_2) to compute the CHSH polynomial S (Eq. 4.9).
3. **Parameter estimation.** Alice and Bob disclose all test-round inputs and outputs to evaluate S . If $S < S_{\text{exp}} - \delta$, the protocol aborts. They also reveal a few of their raw keys to estimate the quantum bit error rate (QBER) $E_{01} = p(a \neq b | x = 0, y = 1)$.
4. **Classical post-processing.** They proceed with error correction and privacy amplification on R_A and R_B .

In the ideal scenario, Alice and Bob share a maximally entangled state (such as $|\phi^+\rangle$) and achieve $S = 2\sqrt{2}$. For the parties to have perfectly correlated raw key bits, they must measure the same observable in the KG rounds. This can be done, for example, given that they are expected to receive the state $|\phi^+\rangle$, by having $A_0 = B_1 = Z$.

The secret key rate of this protocol against collective attacks [Acín et al. 2007] is given from the Devetak-Winter rate [Devetak e Winter 2005]:

$$r_{DI} = I(A_0 : B_1) - \chi(B_1 : E) \geq r_{DW}. \quad (4.12)$$

Here, we consider the mutual information between Alice and Bob’s measurements used in KG rounds, as well as the Holevo quantity given by:

$$\chi(B_1 : E) = H(E)_\rho - \frac{1}{2} \sum_{b_1=\pm 1} H(\rho_E|b_1) \geq I(B_1 : E) \quad (4.13)$$

The usage of Bob’s measurements statistics instead of Alice’s is because $\chi(A_0 : E) \geq \chi(B_1 : E)$ [Acín, Massar e Pironio 2006], and therefore it is more beneficial for the communication of post-processing to be made from Bob to Alice (i.e. reversal reconciliation).

The first term of (4.12) is calculated in a similar manner as the BB84. Since Alice and Bob can assume uniform marginals in their probability distributions ($\langle a_i \rangle = \langle b_i \rangle = 0$), we can write:

$$I(A_0 : B_1) = 1 - h(E). \quad (4.14)$$

The second term is calculated in [Acín et al. 2007] and is bounded in terms of the CHSH polynomial:

$$\chi(B_1 : E) \leq h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right), \quad (4.15)$$

and therefore:

$$r_{DI} \geq 1 - h(E_{01}) - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right). \quad (4.16)$$

Differently from the BB84, the generalization of this result to coherent attacks is a challenging task. However, the *Entropy Accumulation Theorem (EAT)* [Dupuis e Fawzi 2019, Arnon-Friedman et al. 2018, Dupuis, Fawzi e Renner 2020] has allowed the reduction of the whole protocol to that of a single round, thus allowing the generalization to coherent attacks. A detailed security proof using the EAT can be found in [Arnon-Friedman, Renner e Vidick 2019].

DI-QKD protocols represent a profound achievement in quantum cryptography. By eliminating the need to trust measurement devices as well as light sources, DI-QKD essentially bypasses critical vulnerabilities that QKD protocols often face with imperfect devices. This further represents quantum cryptography’s shift in paradigm from regular cryptography—the security relies on the properties of nature itself. However, the theoretical elegance of DI-QKD contrasts sharply with its experimental demands. First, closing the “detection loophole” requires near-perfect detection efficiency, as missed detections artificially suppress Bell violations [Pearle 1970]. Second, DI-QKD suffers from drastically reduced key rates compared to device-dependent protocols. The need to sacrifice rounds for Bell tests, coupled with finite-size effects and statistical estimation, often results in rates orders of magnitude lower than BB84 or decoy-state protocols. Third, generating high-fidelity entanglement over long distances remains challenging, as channel losses degrade correlations and amplify errors. The groundbreaking effort to overcome the challenges of achieving loophole-free Bell tests earned Alain Aspect, John Clauser, and Anton Zeilinger

the 2022 Nobel Prize in Physics, highlighting the role of such experiments in advancing quantum information theory.

In the following section, we will discuss a type of protocol that relaxes the assumptions on measurement devices only, maintaining the need of secure light sources. This is still a great argument towards universal security—imperfect measurement devices are often exploited for eavesdropping attacks [Zhao et al. 2008].

4.3 Measurement-Device-Independent QKD

Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) addresses critical detector-side vulnerabilities in quantum cryptography by eliminating the need to trust measurement devices. In MDI-QKD, Alice and Bob independently prepare and transmit encoded quantum states to an untrusted relay, which performs a measurements and publicly broadcasts its outcomes. These announcements reveal only the parity between Alice and Bob’s key bits according to the measurement results, without disclosing their private encoding choices to anyone, including Eve. By post-selecting events where the relay reports a successful Bell-state measurement and their bases align, Alice and Bob distill a secret key through classical error correction and privacy amplification. The security analysis of MDI-QKD relies on the quantum correlations intrinsic to entanglement-based protocols, while the protocol itself retains the practicality of prepare-and-measure architectures.

A practical implementation first idealized in [Lo, Curty e Qi 2012] uses linear optics to perform Bell-state measurements and the decoy states strategy discussed in (4.1.1) to guarantee security against PNS attacks, as shown in Fig.5.

- **Quantum transmission.** In each round, Alice and Bob independently prepare phase-randomized WCPs, encoding random bits in the polarization state of the pulses. Each party randomly select the horizontal/vertical (Z) basis or the $45^\circ/-45^\circ$ (X) basis and encode bits 0/1 accordingly. The two pulses are sent to the central, untrusted relay.
- **Quantum measurement.** The relay’s 50:50 BS interferes incoming pulses. Polarizing beam-splitters at each output port separate horizontal (D_{CH} , D_{DH}) and vertical (D_{CV} , D_{DV}) polarizations for detection.
- **Sifting.** The parties compare their basis chosen in each round and discard the rounds in which they chose different basis. Additionally, the central relay publicly announces

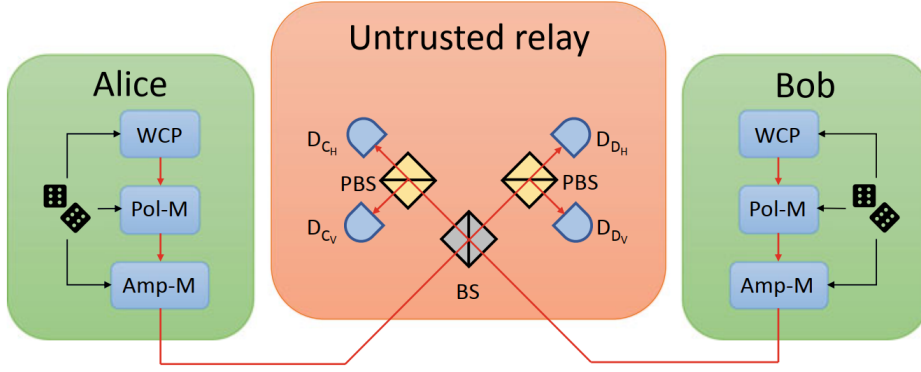


Figure 5 – Experimental scheme for MDI-QKD [Lo, Curty e Qi 2012]. Alice and Bob encode random bits in polarization states of phase-randomized WCPs, with amplitude modulators implementing decoy intensities. Their pulses interfere at an untrusted relay containing a 50:50 beam splitter (BS) and PBSs directing photons to four single-photon detectors (D_{CH} , D_{CV} , D_{DH} , D_{DV}). Detector clicks herald Bell-state measurement outcomes, which the relay broadcasts.

Source: [Grasseli 2021]

the detection events and the parties discard the rounds in which only one detector clicked.

- **Parameter estimation and classical post-processing.** Alice and Bob reveal a part of their bit strings in order to estimate QBERs. They can proceed with the usual error correction and privacy amplification steps on their raw keys.

Discarding single-detector events is critical, as these reveal polarization encodings to Eve. An important characteristic of MDI-QKD is that the events in which both detectors D_{CH} and D_{DH} or detectors D_{CV} and D_{DV} simultaneously click cannot happen due to the *Hong-Ou-Mandel (HOM) effect* [Hong, Ou e Mandel 1987]. When two indistinguishable photons simultaneously enter the input ports of a 50:50 beam splitter, they must exit together through the same output port. The other possible rounds are caused by a projection of the pulses in Bell states. This can be visualized by using a *virtual qubit* scenario, where Alice and Bob each have a virtual qubit entangled with the polarization state of the photons they are sending.

Say Alice and Bob each prepare an entangled state between a virtual qubit they store in their respective labs and a single photon polarized either horizontally or vertically.

$$\begin{aligned} |\psi_A\rangle &= \frac{1}{\sqrt{2}}(|H\rangle_A |1\rangle_{AH} + |V\rangle_A |1\rangle_{AV}), \\ |\psi_B\rangle &= \frac{1}{\sqrt{2}}(|H\rangle_B |1\rangle_{BH} + |V\rangle_B |1\rangle_{BV}), \end{aligned} \quad (4.17)$$

where the kets $|H\rangle_{A(B)}$ and $|V\rangle_{A(B)}$ denote Alice's (Bob's) qubit in the computational basis according to the polarization state of the single photon, while the Fock states $|1\rangle_{AH(BH)}$

and $|1\rangle_{A_V(B_V)}$ describe Alice's (Bob's) single photon polarized horizontally or vertically. Note that Alice and Bob measuring their qubits in the Z or X basis is equivalent to them preparing the single-photon signal in a random polarization state of the corresponding basis, which is exactly the protocol described without the virtual qubits.

After they send the signals through the network, the global quantum state right before interference at the 50:50 BS reads:

$$|\psi_A\rangle \otimes |\psi_B\rangle = \frac{1}{2} \left[|HH\rangle_{AB} |11\rangle_{A_H B_H} + |HV\rangle_{AB} |11\rangle_{A_H B_V} + |VH\rangle_{AB} |11\rangle_{A_V B_H} + |VV\rangle_{AB} |11\rangle_{A_V B_V} \right]. \quad (4.18)$$

We can rewrite the Fock states in terms of the creation operators a^\dagger and b^\dagger acting on the vacuum state $|0\rangle$ (e.g. $|1\rangle_{A_H}$ as $a_H^\dagger |0\rangle$) and represent the action of the 50:50 BS by labelling c^\dagger and d^\dagger as the creation operators of the photons exiting the left and right outputs, respectively. The unitary action of the 50:50 BS on the signal consists of $a^\dagger \rightarrow (c^\dagger + d^\dagger)/\sqrt{2}$ and $b^\dagger \rightarrow (c^\dagger - d^\dagger)/\sqrt{2}$. Since the creation operators relative to different optical paths or different polarizations commute, the final state after exiting the BS is:

$$|\Psi_{BS}\rangle = \frac{1}{2} \left[|HH\rangle_{AB} \left(\frac{|2\rangle_{C_H} - |2\rangle_{D_H}}{2} \right) + |VV\rangle_{AB} \left(\frac{|2\rangle_{C_V} - |2\rangle_{D_V}}{2} \right) + \left(\frac{|HV\rangle + |VH\rangle}{\sqrt{2}} \right)_{AB} \left(\frac{|1\rangle_{C_H} |1\rangle_{C_V} - |1\rangle_{D_H} |1\rangle_{D_V}}{\sqrt{2}} \right) - \left(\frac{|HV\rangle - |VH\rangle}{\sqrt{2}} \right)_{AB} \left(\frac{|1\rangle_{C_H} |1\rangle_{D_V} - |1\rangle_{C_V} |1\rangle_{D_H}}{\sqrt{2}} \right) \right], \quad (4.19)$$

where $|n\rangle_{C(D)_{H(V)}}$ denotes n photons polarized horizontally (vertically) on the left (right) output port of the BS. It can also be written as:

$$|\Psi_{BS}\rangle = \frac{1}{2} \left[|HH\rangle_{AB} \left(\frac{|2\rangle_{C_H} - |2\rangle_{D_H}}{2} \right) + |VV\rangle_{AB} \left(\frac{|2\rangle_{C_V} - |2\rangle_{D_V}}{2} \right) + |\psi^+\rangle_{AB} \left(\frac{|1\rangle_{C_H} |1\rangle_{C_V} - |1\rangle_{D_H} |1\rangle_{D_V}}{\sqrt{2}} \right) - |\psi^-\rangle_{AB} \left(\frac{|1\rangle_{C_H} |1\rangle_{D_V} - |1\rangle_{C_V} |1\rangle_{D_H}}{\sqrt{2}} \right) \right]. \quad (4.20)$$

Note that the virtual qubit states become the Bell states $|\psi^+\rangle$ and $|\psi^-\rangle$ in two of the possible outcomes: the first with successful detections in detectors D_{C_H}, D_{C_V} or D_{D_H}, D_{D_V} , and the second with D_{C_H}, D_{D_V} or D_{C_V}, D_{D_H} . Those are used for key generation, since Alice and Bob will know that their bits are anti-correlated and they can perform bit flips in order to obtain the same raw key. Since Alice and Bob's measurements commute with the detection at the relay, they can be delayed until the photon detection has occurred. This virtual approach plays an important role in proving the security of MDI-QKD protocols. Specifically, after the relay performs its Bell-state measurement, Alice and Bob effectively share either a $|\psi^+\rangle$ or $|\psi^-\rangle$ Bell state, depending on the outcome. They can then independently measure their virtual qubits in the Z or X basis, just as in EB-BB84, and

proceed with sifting, parameter estimation, and classical post-processing. This equivalence enables the security proof of MDI-QKD to follow the same steps as the decoy-state BB84 protocol described earlier. The asymptotic secret key rate of the protocol described here is [Lo, Curty e Qi 2012]:

$$r_{\text{MDI}} = P_Z^{1,1}(1 - h(e_X^{1,1})) - P_Z h(E_Z), \quad (4.21)$$

where P_Z and E_Z are the gains and QBERs, respectively, of the signal state in the Z basis, $P_Z^{1,1}$ is the gain with both parties sending a single photon each in the Z basis and $e_X^{1,1}$ is the error rate in the X basis given that both parties sent one photon each. Similarly to the BB84 with decoys states, the later two quantities can be bounded. In the ideal setup and in the asymptotic limit for the key's length, the secret key rate is simply given by the probability that a useful detection event happened in the case where Alice and Bob both prepared a single photon in the Z basis:

$$r_{\text{MDI}}^{\text{ideal}} = P_Z^{1,1}. \quad (4.22)$$

Preparing indistinguishable photons from two independent and distant light sources and obtaining good HOM interference is crucial for this type of protocol. This is very hard to achieve [Lo, Curty e Qi 2012], especially accounting for long-distance and high-loss scenarios, rendering this type of protocol challenging to implement efficiently.

4.4 Fundamental Limits of Quantum Communication

In [Pirandola et al. 2017], the authors established a fundamental bound on the secret key rate achievable by any QKD protocol over a lossy channel with transmittance η . Termed the *Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound*, this limit is expressed as:

$$r_{\text{PLOB}} = -\log(1 - \eta), \quad (4.23)$$

where η quantifies the probability of a photon traversing the channel intact. For optical fiber links, η is determined by the attenuation coefficient γ (typically $\gamma \approx 0.2$ dB/km for modern fibers) and the transmission distance L via:

$$\eta = 10^{-\gamma L/10}. \quad (4.24)$$

In high-loss regimes ($\eta \ll 1$), the PLOB bound asymptotically simplifies to $r_{\text{PLOB}} \approx 1.44\eta$, revealing that the secret key rate scales linearly with η —and thus decays exponentially with distance L . This emphasizes the severe impact of channel loss on long-distance QKD.

The PLOB bound represents a critical benchmark for all QKD protocols. While numerous strategies aim to mitigate loss-induced rate reductions, none circumvent the

exponential dependence on distance inherent to η . For example, the MDI-QKD protocol discussed previously splits the total channel into two segments of transmittance $\sqrt{\eta}$, each linking Alice and Bob to an intermediate relay. However, successful detection requires both photons to survive their respective channels, yielding an overall success probability $(\sqrt{\eta})^2 = \eta$ —identical to the single-channel case. Quantum repeaters [Briegel et al. 1998] and memories [Panayi et al. 2014, Abruzzo, Kampermann e Bruß 2014] theoretically enable rate scaling with $\sqrt{\eta}$ or better, but their practical realization faces incredible challenges, including high-fidelity entanglement swapping and long-lived quantum storage.

In the following section, we analyze *Twin-Field QKD* (TF-QKD), a protocol that circumvents the PLOB bound by encoding key information in single-photon detection events at a remote relay. By exploiting phase correlations between Alice and Bob’s signals, TF-QKD achieves a secret key rate scaling as $\sqrt{\eta}$, dramatically outperforming conventional protocols in high-loss regimes. This breakthrough positions TF-QKD as a promising candidate for practical, long-distance quantum communication.

4.5 Twin-Field QKD

Twin-Field QKD (TF-QKD), initially proposed in [Lucamarini et al. 2018], is based on the same principles of MDI-QKD while re-imagining the role of the intermediate relay: instead of requiring simultaneous detection of photons from Alice and Bob, TF-QKD encodes key information in single-photon interference events at the relay, achieving a secret key rate scaling with $\sqrt{\eta}$. The initial versions of TF-QKD suffered the technical challenges of phase stabilization and synchronization between Alice and Bob’s independent lasers, which resulted in many rounds being discarded due to phase post-selection.

The protocol *CAL-19*, introduced in [Curty, Azuma e Lo 2019], removes the need for global phase tracking, significantly increasing the protocol’s performance and better aligning with existing laser technology. We will first outline an idealized version of the protocol involving single-photon states in order to properly show the intuition behind secret key generation. Then, we will describe a practical version of the protocol utilizing the decoy state strategy.

4.5.1 Ideal Protocol

In order to explain the protocol and show the intuition behind key generation, we first explain the protocol while using "virtual" qubits in Alice and Bob’s labs. The virtual, single-photon scenario of the CAL-19 protocol is as follows:

- **Quantum transmission.** In each round, Alice and Bob prepare an optical signal entangled with a qubit in their respective labs:

$$|\Phi\rangle_{Aa} = \sqrt{q}|00\rangle_{Aa} + \sqrt{1-q}|11\rangle_{Aa} \quad (4.25)$$

with $0 \leq q \leq 1$, $|0\rangle_a$ and $|1\rangle_a$ are the Fock states representing the vacuum and single-photon state while $\{|0\rangle_A, |1\rangle_A\}$ are qubit states on the Z -basis. Bob's state $|\Phi\rangle_{Bb}$ is described analogously. They then send their optical modes (a and b) through optical channels with transmittance $\sqrt{\eta}$.

- **Quantum measurement.** Upon arriving at the central node, Alice and Bob's signals interfere on a 50:50 beam splitter with output ports connected to detectors D_c and D_d , as shown in Figure 6. The relay broadcasts the outcomes $k_c, k_d \in \{0, 1\}$ of the respective detectors. Independently from each other, Alice and Bob perform measurements in their qubits. With probability p_X , they perform a measurement in the X basis, while with probability $p_Z = 1 - p_X$ they perform a measurement in the Z basis, recording the outcomes b_A and b_B , respectively, for each measurement.
- **Sifting.** Alice and Bob publicly compare their basis chosen in each round and discard the rounds in which they chose different basis for measurement. They only use the rounds in which only one of the relay's detectors clicked ($k_c \oplus k_d = 1$), discarding the rest. They can choose an asymmetric strategy, where they keep the X -basis rounds for key generation and use the Z -basis rounds for parameter estimation.
- **Parameter estimation.** Alice and Bob compare all of their Z -basis outcomes to estimate their QBER E_Z and some of the X -basis rounds to estimate E_X .
- **Classical post-processing** Alice and Bob can proceed with the usual error correction and privacy amplification steps on their raw keys.

In order to see how they are able to distill a secret key from this, we can calculate the final state of the protocol after the interference at the BS in the central relay (without considering the effect of losses). Right before interference, Alice and Bob's signal reads:

$$\begin{aligned} |\Phi\rangle_{Aa} \otimes |\Phi\rangle_{Bb} = & q|00\rangle_{AB}|00\rangle_{ab} + \sqrt{q(1-q)}|01\rangle_{AB}|0\rangle_a|1\rangle_b + \\ & \sqrt{q(1-q)}|10\rangle_{AB}|1\rangle_a|0\rangle_b + (1-q)|11\rangle_{AB}|1\rangle_a|1\rangle_b. \end{aligned} \quad (4.26)$$

We can describe the unitary action of the BS on the signal as $a^\dagger \rightarrow (c^\dagger + d^\dagger)/\sqrt{2}$ and $b^\dagger \rightarrow (c^\dagger - d^\dagger)/\sqrt{2}$. After the interference, the state reads:

$$\begin{aligned} |\Phi\rangle_{BS} = & q|00\rangle_{AB}|00\rangle_{cd} + \sqrt{q(1-q)}|\psi^+\rangle_{AB}|10\rangle_{cd} \\ & - \sqrt{q(1-q)}|\psi^-\rangle_{AB}|01\rangle_{cd} + (1-q)|11\rangle_{AB}\frac{1}{2}(|2,0\rangle_{cd} + |0,2\rangle_{cd}), \end{aligned} \quad (4.27)$$

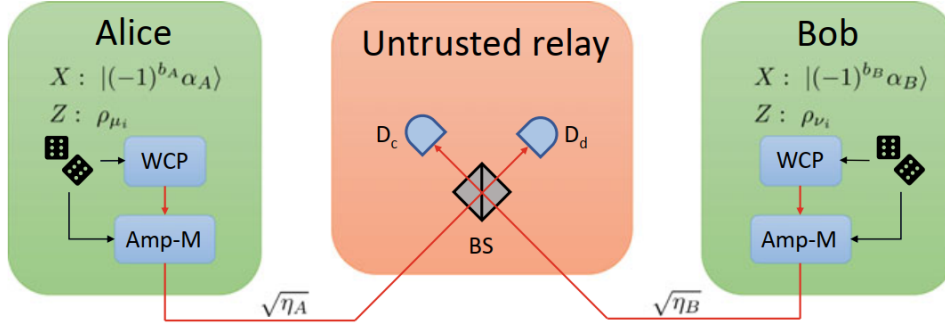


Figure 6 – Experimental setup for practical Twin-Field QKD (CAL-19 protocol) [Curty, Azuma e Lo 2019]. Alice and Bob independently select the X basis (probability p_X) or Z basis (probability p_Z). In X -basis rounds, Alice encodes a random bit b_A in the phase of a weak coherent pulse (WCP) with intensity α_A , while Bob encodes b_B in a WCP of intensity α_B . For Z -basis rounds, they prepare phase-randomized WCPs with decoy intensities μ_i and ν_i , respectively. Signals traverse lossy channels (transmittance $\sqrt{\eta_A}$, $\sqrt{\eta_B}$) to a central relay, where a 50:50 beam splitter (BS) interferes them. Threshold detectors at the BS outputs (D_c , D_d) record clicks $k_c, k_d \in \{0, 1\}$, which the relay broadcasts. Rounds with $k_c \oplus k_d \neq 1$ or mismatched bases are discarded. The raw key is formed by bits b_A and $b_B \oplus k_d$.

Source: [Grasseli 2021]

where $|\psi^\pm\rangle_{AB} = (|01\rangle \pm |10\rangle)/\sqrt{2}$. Here, we fully visualize how Alice and Bob generate their keys. The rounds in which they both sent vacuum states are discarded. In order to ensure that almost all the detection events are caused by single-photon events, Alice and Bob can choose $(1 - q) \ll 1$, meaning they are preparing mostly vacuum states. Thus, the probability of two-photon interference is minimal. In a detection event they most probably share a Bell state $|\psi^\pm\rangle_{AB}$, and their measurement outcomes (i.e. bit values) are correlated. However, just as in the MDI-QKD protocol described in Section 4.3, the detection outcomes reveal to Eve only that Alice and Bob have different bit values. Since the parties only use the rounds in which $k_c \oplus k_d = 1$, Eve cannot identify which of the two sent the signal—the beam splitter creates a coherent superposition of the states, and the information of who sent the photon is lost. They can then measure their qubit, choosing randomly between the X and Z basis, and the rest of the protocol follows an entanglement-based BB84 protocol with different error rates.

By rewriting $|\psi^+\rangle$ in the X basis, we obtain $(|++\rangle - |--\rangle)/\sqrt{2}$, therefore Alice and Bob's bits should be equal when $k_d = 0$ and different when $k_d = 1$, since $|\psi^-\rangle = -(|+-\rangle - |-+\rangle)/\sqrt{2}$. In the Z basis, they should ideally follow $b_A = b_B \oplus 1$. Thus, the QBERs E_X and E_Z are:

$$E_X = p_{XX}(b_A \neq b_B \oplus k_d | k_c \oplus k_d = 1), \quad (4.28)$$

$$E_Z = p_{ZZ}(b_A = b_B | k_c \oplus k_d = 1). \quad (4.29)$$

However, TF-QKD has intrinsic error rates, especially when accounting for the transmittance of the network. In this case, the detection events caused by single photons happen with probability

$$p_{\text{single}} = \sqrt{\eta}(1-q)q + (1-q)^2\sqrt{\eta}(1-\sqrt{\eta}), \quad (4.30)$$

in which the first term is the ideal case with one photon being emitted and successfully transmitted and the second term is the case when two photons are emitted but only one of them arrives at the BS. The detection events caused by two-photon signals happen with probability:

$$p_{\text{two}} = \frac{1}{2}(1-q)^2\eta. \quad (4.31)$$

Thus, the probability of a single detector (either D_c or D_d) clicking is given by $p_{\text{click}} = p_{\text{single}} + p_{\text{two}}$. It is clear that any two-photon emission followed by a detection event cannot be used for key generation (since Alice and Bob's bits will be revealed) but also cannot be distinguished from the ideal, useful case. By normalizing the probabilities in respect to a successful detection event, the intrinsic error probability of the protocol can be written as:

$$p_{\text{error}} = \frac{p_{\text{single}}}{p_{\text{click}}} \frac{(1-q)^2\sqrt{\eta}(1-\eta)}{p_{\text{single}}} + \frac{p_{\text{two}}}{p_{\text{click}}} = \frac{p_{\text{single}}}{p_{\text{click}}} \frac{(1-q)(1-\sqrt{\eta})}{q + (1-q)(1-\sqrt{\eta})} + \frac{p_{\text{two}}}{p_{\text{click}}} \quad (4.32)$$

The asymptotic secret key rate of the protocol is given by the BB84 protocol key rate weighted by the probability $2p_{\text{click}}$ of a successful detection event by D_c or D_d :

$$r_{\text{TF}} = 2p_{\text{click}}(1 - h(E_Z) - h(E_X)) \quad (4.33)$$

One thing to note is that the parties can optimize their error rates by adjusting the parameter q in their preparation for the protocol. A sufficient high value for q ensures that $p_{\text{error}} \approx 0$ and $2p_{\text{click}} \approx 2q(1-q)\sqrt{\eta}$, since we neglect the terms $(1-q)^2$. Thus, the secret key rate scales with $\sqrt{\eta}$ as predicted.

In practice, this protocol can be executed without the use of virtual entangled qubits, instead turning the protocol into a prepare-and-measure where Alice and Bob can randomly choose the value of their bits and encode the signal accordingly. First, since the measurements performed by Alice and Bob commute with all the other operations performed in the protocol, they can be done before sending the signal. This transforms the protocol into the following PM setup: Alice randomly selects the X or Z basis with probabilities p_X and p_Z . In X -basis rounds, she prepares an optical pulse:

$$|X\rangle_{b_A a} := \sqrt{q}|0\rangle_a + (-1)^{b_A}\sqrt{1-q}|1\rangle_a, \quad (4.34)$$

where b_A is her randomly chosen bit. For Z -basis rounds, she sends a Fock state:

$$|Z\rangle_{b_A a} := |b_A\rangle_a, \quad (4.35)$$

with $b_A = 0$ (vacuum) or $b_A = 1$ (single photon) chosen with probabilities q and $1 - q$, respectively. Bob prepares his states analogously. From Eve's perspective, this prepare-and-measure protocol is indistinguishable from the virtual scenario version. Thus, this PM version is equivalent in terms of security and secret key rate.

4.5.2 Practical Protocol

The practical version of TF-QKD described in [Curty, Azuma e Lo 2019] employs the decoy state strategy in order to account for vulnerabilities caused by practical photon sources. Since the parameter q is chosen with high values suggests that the X -basis states can be replaced by WCPs $|(-1)^{b_A}\alpha_A\rangle$ and $|(-1)^{b_B}\alpha_B\rangle$ with $|\alpha|^2 \ll 1$. The decoy-state method can also be used in the Z -basis states in order to better estimate the phase-error rate E_Z , since they do not contribute to key generation. In this manner, Alice and Bob do not rely on single-photon states and can use practical laser sources to execute the protocol. The states sent by Alice in the X -basis rounds are:

$$|(-1)^{b_A}\alpha_A\rangle = e^{|\alpha_A|^2/2} \sum_{n=0}^{\infty} \frac{((-1)^{b_A}\alpha_A)^n}{\sqrt{n!}} |n\rangle, \quad (4.36)$$

while the states sent in the Z -basis are:

$$\rho_{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} |n\rangle \langle n|, \quad (4.37)$$

with intensity μ_i randomly drawn from a set $\{\mu_i\}$. Bob prepares his states analogously, with both bit values b_B and amplitude α_B not necessarily equal to Alice's, and phase-randomized WCPs ρ_{ν_j} with intensity ν_j randomly drawn from the set $\{\nu_j\}$, that also need not be equal to Alice's. The sets containing the possible decoy intensities are publicly agreed upon by the parties. When executing this protocol, the quantities observed by Alice and Bob are the gains:

- $p_{XX}(k_c, k_d | b_A, b_B)$: Probability that the relay announces the detection pattern k_c, k_d given that Alice and Bob prepared the coherent states $|(-1)^{b_A}\alpha_A\rangle$ and $|(-1)^{b_B}\alpha_B\rangle$.
- $p_{ZZ}(k_c, k_d | \mu_i, \nu_j)$: Probability that the relay announces the detection pattern k_c, k_d given that Alice and Bob prepared states ρ_{μ_i} and ρ_{ν_j} .

The QBERs E_X are observed by the parties and can be given by (4.28), just as with the ideal case. In order to estimate the error in the Z -basis, we note that Eve cannot distinguish the case in which Alice and Bob send decoy states ρ_{μ_i} and ρ_{ν_j} from the case in which they send number states $|n\rangle_a$ and $|m\rangle_b$ according to a Poissonian distribution P_{μ_i} and P_{ν_j} :

$$P_{\mu_i}(n) = e^{-\mu_i} \frac{\mu_i^n}{n!}, \quad P_{\nu_j}(m) = e^{-\nu_j} \frac{\nu_j^m}{m!} \quad (4.38)$$

This implies that Eve's announcement of k_c and k_d follows a probability distribution $p_{ZZ}(k_c, k_d|n, m)$, and:

$$p_{ZZ}(k_c, k_d|\mu_i, \nu_j) = \sum_{n,m=0}^{\infty} p_{ZZ}(k_c, k_d|n, m) P_{\mu_i}(n) P_{\nu_j}(m). \quad (4.39)$$

Once Alice and Bob know $p_{ZZ}(k_c, k_d|\mu_i, \nu_j)$ for any given μ_i and ν_j , they can use the decoy-state method of Section 4.1.1 to estimate $p_{ZZ}(k_c, k_d|n, m)$ based on their knowledge of $P_{\mu_i}(n)$ and $P_{\nu_j}(m)$.

Next, we remark that if Alice and Bob chose the X -basis, Eve cannot distinguish the practical scenario from the entanglement-based version of the protocol. In Eve's point of view, Alice (and Bob, analogously) could be preparing the following state

$$|\Phi\rangle_{Aa} = \frac{|+\rangle_A |\alpha\rangle_a + |-\rangle_A |-\alpha\rangle_a}{\sqrt{2}}, \quad (4.40)$$

while delaying the X measurement on the qubit until the detection event at the relay. Thus, the global state of the parties' qubits and signals after the announcement of k_c, k_d is:

$$|\chi^{k_c, k_d}\rangle_{Aa'Bb'} := \frac{M_{a,b}^{k_c, k_d} |\Phi\rangle_{Aa} |\Phi\rangle_{Bb}}{\sqrt{p_{XX}(k_c, k_d)}}, \quad (4.41)$$

where $M_{a,b}^{k_c, k_d}$ is the Kraus operator that describes the action of the relay on the signals. In order to prove security, we need to relate the conditional probabilities $p_{ZZ}(k_c, k_d|n, m)$ to the phase-error rate $e_Z^{k_c, k_d}$, which measures the coherence between the bit-error rates in the Z -basis and the incoming signal on the key generation rounds:

$$e_Z^{k_c, k_d} = \sum_{j=0,1} ||_{AB} \langle jj | \chi^{k_c, k_d} \rangle_{Aa'Bb'} ||^2. \quad (4.42)$$

The probability that the relay announces detection event k_c, k_d given that Alice and Bob sent n and m photons in Z -basis rounds is given by the yields $Y_{nm}^{k_c, k_d}$:

$$Y_{nm}^{k_c, k_d} := p_{ZZ}(k_c, k_d|n, m). \quad (4.43)$$

As seen before, the decoy state method allows us to estimate $Y_{nm}^{k_c, k_d}$ by observing the gains on the Z -basis, since they are constrained by the set of equations:

$$p_{ZZ}(k_c, k_d|\mu_i, \nu_j) = \sum_{n,m=0}^{\infty} e^{-\mu_i - \nu_j} \frac{\mu_i^n \nu_j^m}{n!m!} Y_{n,m}^{k_c, k_d}, \quad (4.44)$$

with $\mu_i \in \{\mu_i\}$ and $\nu_j \in \{\nu_j\}$. In the scenario where Alice and Bob use an infinite number decoy intensity settings, they can precisely estimate each yield value. The yields can be used to derive an upper bound on (4.42) and obtain (The calculations are detailed in the Appendix B):

$$\bar{e}_Z^{k_c, k_d} = \frac{1}{p_{XX}(k_c, k_d)} \left[\left(\sum_{n,m=0}^{\infty} C_{2n}^a C_{2m}^b \sqrt{Y_{2n,2m}^{k_c, k_d}} \right)^2 + \left(\sum_{n,m=0}^{\infty} C_{2n+1}^a C_{2m+1}^b \sqrt{Y_{2n+1,2m+1}^{k_c, k_d}} \right)^2 \right], \quad (4.45)$$

where $C_n^a = e^{\frac{-|\alpha_A|^2}{2}} \frac{\alpha_A^n}{\sqrt{n!}}$ and $C_m^b = e^{\frac{-|\alpha_B|^2}{2}} \frac{\alpha_B^m}{\sqrt{m!}}$. The asymptotic secret key rate of the practical CAL-19 protocol is given by [Curty, Azuma e Lo 2019]:

$$r_{\text{TF}} \geq r_{\text{TF}}^{1,0} + r_{\text{TF}}^{0,1}, \quad (4.46)$$

where $r_{\text{TF}}^{k_c, k_d}$ is the secret key rate for each detection event with $k_c \oplus k_d = 1$:

$$r_{\text{TF}}^{k_c, k_d} = p_{XX}(k_c, k_d)[1 - h(E_X^{k_c, k_d}) - h(\bar{e}_Z^{k_c, k_d})]. \quad (4.47)$$

The term $p_{XX}(k_c, k_d)$ is the probability of having a detection event k_c, k_d when Alice and Bob chose the X -basis; since those events are caused primarily by a single photon arriving, sent by either Alice or Bob, it scales with $\sqrt{\eta}$, and thus the secret key rate scales with $\sqrt{\eta}$ as in the ideal case. The secret key rate has a lower bound corresponding to the upper bounds on the yields. In the realistic finite-scenario, one can derive the upper bound for a subset of yields—typically the most likely cases in attenuated lasers (small n and m) and trivially upper-bound the remaining yields by 1.

TF-QKD has emerged as a transformative approach in quantum communication, overcoming the fundamental rate-distance limit of conventional QKD protocols by exploiting single-photon interference at a central relay. This paradigm shift enables a secret key rate scaling proportional to $\sqrt{\eta}$, which shows a promising result for QKD even in high-loss scenarios. However, practical implementations further grapple with the limitations of weak coherent photon sources, which necessitate decoy-state methods to bound multi-photon contributions. Advanced superconducting nanowire single-photon detectors (SNSPDs), with near-unity efficiency and ultralow dark counts, have proven indispensable in state-of-the-art experimental realizations [Boaron et al. 2018], yet their high cost and cryogenic requirements highlight the need for scalable alternatives.

In spite of this, recent experiments show promising practical results. Secure key distribution over 1000 km of ultralow-loss fiber has been achieved [Liu et al. 2023] using the metropolitan Beijing-Shanghai backbone, with key rates surpassing traditional QKD by orders of magnitude at comparable distances, while demonstrating compatibility with existing infrastructure. Very recent experiments also managed to execute free-space TF-QKD over 14km urban atmospheric channels [Li et al. 2025]. These achievements, however, mask unresolved challenges. Long-term phase stabilization in dynamic environments remains an open engineering problem, with current solutions relying on resource-intensive active feedback systems [Zhou et al. 2023]. Furthermore, the integration of TF-QKD into multi-user networks demands standardization of synchronization protocols and wavelength allocation to ensure interoperability with classical communication systems [Liu et al. 2023].

5 The Rio Quantum Network

The Rio Quantum Network (RQN) is a collaborative initiative designed to implement a metropolitan-scale quantum network connecting multiple research institutions across Rio de Janeiro, as shown in Figure 7. A primary objective of this project is to enable secure point-to-point communication between any two network nodes through quantum key distribution (QKD) protocols. The network’s operational conditions—characterized by high channel losses and extended transmission distances between nodes—pose significant technical challenges. Given the absence of quantum repeaters in the initial deployment phase, the network requires a QKD protocol capable of maintaining efficiency in high-loss environments.

5.1 Motivation

As demonstrated in previous chapters, Twin-Field QKD (TF-QKD) offers promising solutions in high loss scenarios by surpassing fundamental limits of conventional QKD, such as the PLOB bound. However, practical implementation of TF-QKD in the RQN faces several constraints. First, the original protocol proposed in [Lucamarini et al. 2018] necessitates a stable phase reference between communicating parties to enable interference at the central relay—a requirement that becomes increasingly difficult to satisfy in a metropolitan network with distributed nodes, leading to suboptimal secret key rates. Second, the RQN’s multi-user architecture generates asymmetric channel conditions between arbitrary node pairs, necessitating the introduction of compensatory fibers (and associated losses) to align channel parameters with the symmetric assumptions required by phase-stable frameworks such as [Curty, Azuma e Lo 2019]. Third, conventional TF-QKD implementations impose substantial operational costs, and this infrastructure burden complicates scalability and limits the feasibility of adding new users.

Recent advances in Sagnac interferometer-based TF-QKD protocols, as proposed by [Zhong et al. 2019], [Zhong et al. 2021] and [Zhong et al. 2022], present a viable framework for addressing common challenges. The Sagnac architecture inherently ensures phase stability between users by them having a shared laser source, thereby eliminating phase-reference mismatches. Additionally, the protocol’s tolerance for channel asymmetries—achieved through common-path signal propagation—aligns well with the RQN’s heterogeneous topology. Crucially, this approach centralizes critical components such as light sources

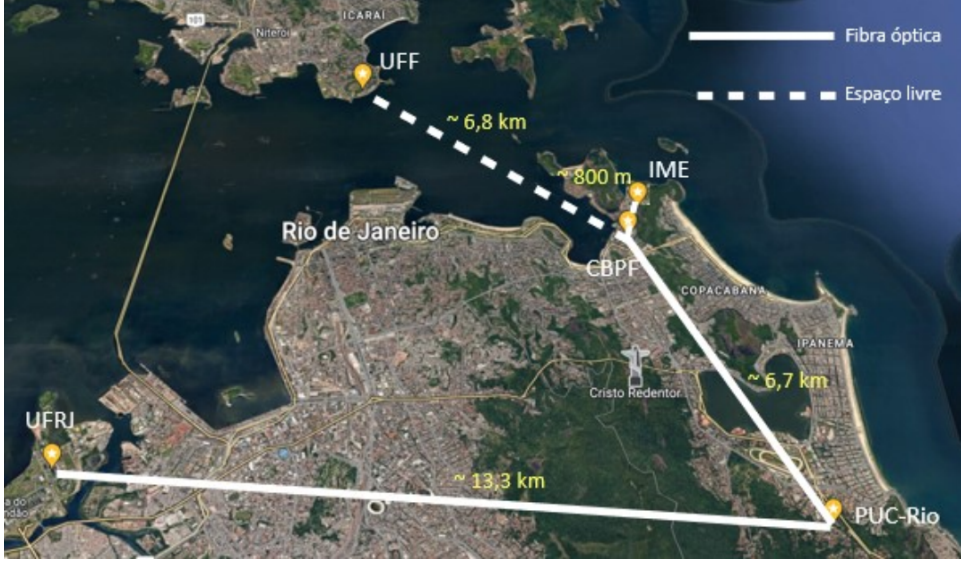


Figure 7 – Basic overview of the Rio Quantum Network’s structure and the institutes connected by it. The distances are measured in a straight line. The bold lines represent connection by optical fibers, while the dotted line represents a free-space link.

Source: Google Maps

and detectors, significantly reducing per-user infrastructure costs and simplifying network expansion. However, this improvement comes at the cost of a $\sqrt{\eta}$ scaling for the secret key rate. The signal must travel twice the distance compared to the original TF-QKD protocols, which results in a key rate that falls below the PLOB bound ¹. In the next sections, we will elaborate on the protocol’s operational principles, security analysis, and information exchange mechanisms for establishing secure communication between nodes.

5.2 Sagnac-based TF-QKD: Ideal Scenario

A untrusted central node, Charlie, is located outside the loop and is in possession of a light source and photon detectors. He is responsible for preparing and sending a signal through the network, as well as performing measurements upon the signal’s return. Alice and Bob will apply phase shifts to the signal, which will then affect the interference pattern and Charlie’s measurement’s results, as shown in Figure 8. When assuming single-photon emissions, the protocol is described as follows:

1. **Quantum Transmission.** In each round, the central node, Charlie, prepares a state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\odot\rangle + |\oslash\rangle) \quad (5.1)$$

¹ The authors in [Zhong et al. 2019, Zhong et al. 2021, Zhong et al. 2022] claim to have simulations with key rates that surpass the PLOB bound. Their model, however, is similar to the one in [Curty, Azuma e Lo 2019], which may have caused this key rate scaling.

by sending a photon through a 50:50 Beam Splitter. Each output port of the BS determines the direction the signal travels. Alice and Bob will act on the counter-clockwise mode of the signal by independently and randomly choosing between two different phases within two different sets and applying it to the signal. Each set corresponds to a choice of basis, and each phase is associated with a bit value. See table 1 for details.

This results in the following state:

$$|\psi\rangle_C = \frac{1}{\sqrt{2}}(|\circ\rangle + e^{i(\phi_A+\phi_B)} |\oslash\rangle). \quad (5.2)$$

2. **Quantum Measurement.** The two different modes interfere in the same BS back at Charlie's lab, which has a detector in each of the output ports, labeled D_\circ and D_\oslash . Just before detection, the state can be written as:

$$|\psi\rangle_{BS} = \frac{1}{2}[(1 + e^{i(\phi_A+\phi_B)}) |\circ\rangle + (1 - e^{i(\phi_A+\phi_B)}) |\oslash\rangle]. \quad (5.3)$$

Charlie performs a measurement and records the outcomes k_\circ and k_\oslash where $k_{\circ(\oslash)} = 0$ corresponds to a no-click event and $k_{\circ(\oslash)} = 1$ corresponds to a click event. This step is repeated until they complete a predetermined M number of rounds. Since there was a bit value associated with each possible phase applied by Alice and Bob, they each hold now a bit string of length M .

3. **Sifting.** Alice and Bob will publicly and classically communicate to each other which set they chose in each round and discard the rounds in which they chose different sets. The relay publicly announces the outcome of his measurements k_\circ and k_\oslash of detectors D_\circ and D_\oslash for each round to Alice and Bob, and they discard the rounds in which $k_\circ \oplus k_\oslash \neq 1$. After this step, Alice and Bob should each have a bit string of length $\approx M/2$.
4. **Parameter Estimation.** Alice and Bob will compare part of their bit strings, and consequently the phase values applied, for a part of the rounds. Meaning they will publicly share a random subset of their bit strings, $S \subset M$, and compare them bit-by-bit. They use this data to evaluate the quantum bit error rates (QBERs) E_Z and E_Y .
5. **Information Reconciliation.** Alice and Bob can then proceed with the usual error correction and privacy amplification protocols of their choice.

The phases Alice and Bob apply can assume values $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$, divided among two different sets. The values $\{0, \pi\}$ are assigned to the Z set and the values $\{\pi/2, 3\pi/2\}$ are assigned to the Y set. The 0 and 1 bit values are assigned for each set's first and second value, respectively, as shown in the table:

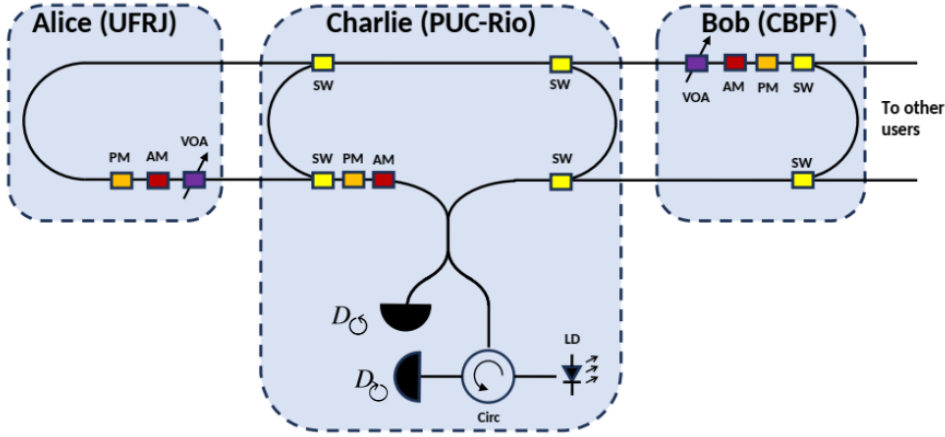


Figure 8 – Two-parties QKD in Rio Quantum Network using a Sagnac-based topology: experimental setup. Charlie prepares a optical signal and sends it to the network. A 50:50 BS acts on the signal creating a uniform superposition between the clockwise and anti-clockwise modes. Alice and Bob independently apply a phase shift on the anti-clockwise mode randomly sampling the phase value from four possible settings. The signal then goes back to Charlie’s lab, where it interferes back at the BS, and it is followed by two detectors D_0 and D_1 . The relay announces detection results k_0 and k_1 . The parties keep the rounds in which they choose the same basis and $k_0 \oplus k_1 = 1$, all the other rounds are discarded. The network has optical switches that can be used to allow other users to communicate.

bit	Z set	Y set
0	0	$\pi/2$
1	π	$3\pi/2$

Table 1 – Possible phase values and their respective sets, as well as the bit value associated with each phase value.

We can see from (5.3) that the probability of Charlie obtaining a particular outcome depends on the phase applied by the parties. If they apply phases from different sets, each detector in Charlie’s lab will have a 50% chance of clicking, and this is why those rounds are not used for QKD. More explicitly, by choosing from different sets, $\phi_A + \phi_B$ will be equal to $\pi/2$ or $3\pi/2$, and therefore $e^{i(\phi_A + \phi_B)} = \pm i$.

$$|\langle \psi | \psi \rangle_{BS}|^2 = \left| \frac{1}{2}(1 \pm i) \right|^2 = \frac{1}{2} \quad (5.4)$$

If they applied phases from the same set, $\phi_A + \phi_B$ will be equal to 0 or π , and therefore $e^{i(\phi_A + \phi_B)} = \pm 1$.

For instance, in the Z set, whenever they both apply 0 (π), $e^{i0} = 1$ ($e^{i(2\pi)} = 1$) and the D_0 detector will click with 100% probability. Whenever they apply different phases, $e^{i(\pi)} = -1$ and the D_1 detector will click 100% probability. The same goes for the Y set, but applying the same phase will result in a click on the D_1 detector and applying

different phases will result in a click on the D_{\odot} detector.

This is precisely why Alice and Bob are able to distill a secret key from this protocol. Essentially, the only information available to an eavesdropper (Eve) is the sum of phases applied on the signal. The information on each individual phase applied either by Alice or Bob is lost due to the interference, and therefore it is only available to them. However, since Alice knows which phase she applied in each round, as well as the detection pattern (i.e. the sum of phases), she automatically knows which phase Bob applied and vice-versa (as long as they chose the same set). Thus, they know each other's bit value for each round.

In order to properly distill a secret key rate for the protocol, we will use the following strategy: by introducing a "virtual" qubit in Alice's and Bob's labs and considering an infinite number of rounds, we can trace an equivalence to the entanglement-based BB84 protocol in the asymptotic scenario, and therefore use the Devetak-Winter rate for this protocol. As previously mentioned, this is the same strategy typically used in other MDI-QKD protocols to derive an expression for the secret key rate.

5.3 Equivalence to EB-BB84: Virtual scenario

In order to show that this protocol is equivalent to the Entanglement-Based BB84 protocol, we introduce a virtual qubit in Alice's and Bob's labs which they can perform measurements on. Also, instead of randomly selecting a phase and applying it to the signal, they will instead correlate their qubit with the signal by performing a conditional unitary operation on the joint state. Here, $|0\rangle_{A(B)}$ and $|1\rangle_{A(B)}$ denotes Alice's (Bob's) qubit state in the Z basis.

$$|\psi\rangle_{CAB} = \frac{1}{\sqrt{2}}(|\odot\rangle + |\oslash\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B). \quad (5.5)$$

The unitary for Alice can be written as:

$$U_A = (\mathbb{I}_C \otimes |0\rangle\langle 0|_A + Z_C \otimes |1\rangle\langle 1|_A) \otimes \mathbb{I}_B, \quad (5.6)$$

and for Bob:

$$U_B = \mathbb{I}_A \otimes (\mathbb{I}_C \otimes |0\rangle\langle 0|_B + Z_C \otimes |1\rangle\langle 1|_B), \quad (5.7)$$

where Z is the pauli matrix $Z = |\odot\rangle\langle\odot| - |\oslash\rangle\langle\oslash|$ and \mathbb{I} is the identity operator. This operation introduces a π phase on the counter-clockwise mode. This results in:

$$U_B U_A |\psi\rangle_{CAB} = \frac{1}{2\sqrt{2}} \left[(|\odot\rangle + |\oslash\rangle) |00\rangle_{AB} + (|\odot\rangle - |\oslash\rangle) |01\rangle_{AB} + (|\odot\rangle - |\oslash\rangle) |10\rangle_{AB} + (|\odot\rangle + |\oslash\rangle) |11\rangle_{AB} \right]. \quad (5.8)$$

After returning to the final BS, the state right before detection reads:

$$|\psi\rangle_{final} = \left(\frac{|00\rangle_{AB} + |11\rangle_{AB}}{2}\right) |\circ\rangle + \left(\frac{|01\rangle_{AB} + |10\rangle_{AB}}{2}\right) |\oslash\rangle. \quad (5.9)$$

Note that, after the application of the unitary operations, performing measurements on the qubit on the Z or Y basis introduces the corresponding phase onto the signal. As the measurement on the qubits commutes with the interferometer propagation, such measurements can be postponed. To clarify the phase difference between the Z and Y bases in the protocol, we outline the action of the unitary (5.6) on the signal:

$$\begin{aligned} U_A(|\psi\rangle_C \otimes |\psi\rangle_A) &= \frac{1}{2}(|\circ\rangle + |\oslash\rangle) |0\rangle_A + \frac{1}{2}(|\circ\rangle + e^{i\pi} |\oslash\rangle) |1\rangle_A \\ &= \frac{1}{2}(|\circ\rangle + |\oslash\rangle)_C |0\rangle_A + \frac{1}{2}(|\circ\rangle - |\oslash\rangle)_C |1\rangle_A. \end{aligned} \quad (5.10)$$

Here, we naturally see the Z set phases, $\{0, \pi\}$ applied to the counter-clockwise mode. If we rewrite Alice's qubits on the Y basis (i.e. Alice decides to her qubit on the Y basis), we have the following:

$$\begin{aligned} U_A(|\psi\rangle_C \otimes |\psi\rangle_A) &= \frac{1}{2}(|\circ\rangle + |\oslash\rangle) \left(\frac{|R\rangle_A + |L\rangle_A}{\sqrt{2}}\right) + \frac{1}{2}(|\circ\rangle - |\oslash\rangle) \left(\frac{|R\rangle_A - |L\rangle_A}{i\sqrt{2}}\right) \\ &= \frac{1}{2} \left[\frac{(1-i)}{\sqrt{2}} |\circ\rangle + \frac{(1+i)}{\sqrt{2}} |\oslash\rangle \right] |R\rangle_A + \frac{1}{2} \left[\frac{(1+i)}{\sqrt{2}} |\circ\rangle + \frac{(1-i)}{\sqrt{2}} |\oslash\rangle \right] |L\rangle_A. \\ &= \left(\frac{|\circ\rangle + e^{i\frac{\pi}{2}} |\oslash\rangle}{2}\right) e^{-i\frac{\pi}{4}} |R\rangle_A + \left(\frac{|\circ\rangle + e^{i\frac{3\pi}{2}} |\oslash\rangle}{2}\right) e^{i\frac{\pi}{4}} |L\rangle_A, \end{aligned} \quad (5.11)$$

where we see the Y -set phases, $\{\pi/2, 3\pi/2\}$, being applied to the counter-clockwise mode. Following this, the final state where Alice and Bob's qubits states are written on the Y basis:

$$|\psi\rangle_{final} = \left(\frac{|RL\rangle_{AB} + |LR\rangle_{AB}}{2}\right) |\circ\rangle + \left(\frac{|RR\rangle_{AB} + |LL\rangle_{AB}}{2}\right) |\oslash\rangle. \quad (5.12)$$

From here, Bob can perform bit flips accordingly such that they always have the $\frac{1}{2}(|00\rangle + |11\rangle)_{AB}$ state, which is also the final state of an EB-BB84 protocol. Now, we can consider the secret key rate described in (3.43) as the secret key rate to be used in the RQN protocol:

$$r_{ideal} = p_{\text{click}}(1 - h(E_Z) - h(E_Y)), \quad (5.13)$$

where E_Z and E_Y are the QBERs in the Z and Y basis, and p_{click} is the probability of a successful detection event, which in the ideal scenario is simply given by the transmittance of the network, η . In the RQN case, we can analyze equations (5.9) and (5.12) to define the QBERs as:

$$E_Z = p_{ZZ}[b_a \neq b_b \oplus k_{\circ} | k_{\circ} \oplus k_{\oslash} = 1], \quad (5.14)$$

$$E_Y = p_{YY}[b_a \neq b_b \oplus k_{\circ} | k_{\circ} \oplus k_{\oslash} = 1]. \quad (5.15)$$

We remark that only the rounds where $k_{\circ} \oplus k_{\circ} = 1$ (only one detector clicked) are considered for the protocol, since any other case can only happen due to multiple photons being sent or dark counts in detectors. When using single photon sources, the protocol's security analysis ends here. One can observe the results and easily estimate the QBERs on step 3, and therefore calculate the secret key rate for the protocol.

5.4 The practical protocol

As seen in Chapter 4, a more practical implementation of single-photon sources can be done via highly attenuated lasers producing Weak Coherent Pulses (WCPs), which can be represented by coherent states with $|\alpha|^2 \ll 1$:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (5.16)$$

In this practical scenario, Charlie will be sending WCPs into the network, with Alice and Bob performing phase shifts in a similar manner as the single-photon case. The action of the BS divides the signal into two different modes (clockwise and anti-clockwise) with amplitudes $\alpha/\sqrt{2}$:

$$|\Psi\rangle_C = \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\circ}} \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\circ}} = e^{-\frac{|\alpha|^2}{2}} \sum_{n,m=0}^{\infty} \left(\frac{\alpha}{\sqrt{2}} \right)^n \left(\frac{\alpha}{\sqrt{2}} \right)^m \frac{1}{\sqrt{n!m!}} |n,m\rangle_{C_{\circ}C_{\circ}}. \quad (5.17)$$

The unitaries Alice and Bob apply to the signal are changed to:

$$U'_A = (\mathbb{I}_C \otimes |0\rangle\langle 0|_A + e^{i\pi c_{\circ}^{\dagger} c_{\circ}} \otimes |1\rangle\langle 1|_A) \otimes \mathbb{I}_B \quad (5.18)$$

and

$$U'_B = \mathbb{I}_A \otimes (\mathbb{I}_C \otimes |0\rangle\langle 0|_B + e^{i\pi c_{\circ}^{\dagger} c_{\circ}} \otimes |1\rangle\langle 1|_B), \quad (5.19)$$

respectively. Here, c_{\circ}^{\dagger} and c_{\circ} are the creation and annihilation operators of the counter-clockwise mode. The operator $e^{i\pi c_{\circ}^{\dagger} c_{\circ}} = \Pi$ is called the parity operator, and its action on a coherent state reads $\Pi |\alpha\rangle = |-\alpha\rangle$.

However, protocols using WCPs are only secure when the parties can guarantee they are only using the rounds in which the detection event was caused by a single photon. This is very hard to achieve, especially since Alice and Bob do not have control of the light source. Besides, since Eve can be in control of the channel, she can perform PNS attacks on the stretch of the network in between Alice and Bob's labs, thus gaining the information of the individual phase (and therefore bit value) applied in some of the rounds. The decoy states strategy is used to ensure that Eve cannot perform this type of attack.

Here, when they choose the Z set, the protocol remains the same, however, when the Y set is chosen, Alice (Bob) will independently introduce a random phase $\Phi_{A(B)}$ with

$0 \leq \Phi_{A(B)} \leq 2\pi$ and modulate the amplitude with intensities μ_i (ν_j) drawn from a set $\{\mu_i\}$ ($\{\nu_j\}$), as shown in Table (2). Only the Z-set rounds are used for key generation, while the Y-set rounds are used for parameter estimation. Additionally, in step 4 of the protocol, Alice and Bob also publicly disclose their amplitude settings for each round. The remaining steps of the protocol are the same.

Set	Phases	Amplitude
Z	$\{0, \pi\}$	-
Y	$0 \leq \Phi_{A(B)} \leq 2\pi$	$\mu_i(\nu_j)$

Table 2 – Different phase and amplitude modulations depending on the set chosen by Alice (Bob).

5.5 Security analysis and secret key rate estimation

In order to distill the secret key rate for this protocol, we need to analyze the error rates in each given basis. The key generating rounds using the Z basis have the same error rates as previously mentioned in (5.14):

$$E_Z = p_{ZZ}[b_a \neq b_b \oplus k_{\odot} \oplus k_{\odot} = 1]. \quad (5.20)$$

However, since the Y basis rounds are not generating keys and have randomized phases and intensities, we will use the phase-error rate e_Y instead. In summary, we are measuring the coherence between the bit-error rates in the Y-basis and the incoming signal on the key generation rounds. The phase-error rate is essentially the Y-basis error that affects the Z-basis rounds, which is by definition:

$$e_Y^{k_{\odot}, k_{\odot}} = \sum_{j=0}^1 \left\| {}_{AB} \langle j, j \oplus k_{\odot} | Z^{k_{\odot}, k_{\odot}} \rangle_{C_{\odot} C_{\odot} AB} \right\|^2, \quad (5.21)$$

where here $|0\rangle$ ($|1\rangle$) are equal to Alice and Bob's $|R\rangle$ ($|L\rangle$) Y-basis state. $|Z^{k_{\odot}, k_{\odot}}\rangle_{C_{\odot} C_{\odot} AB}$ is the state after Charlie's untrusted relay's detection in the Z basis rounds, which is given by:

$$|Z^{k_{\odot}, k_{\odot}}\rangle_{C_{\odot} C_{\odot} AB} = \frac{1}{2\sqrt{p_{ZZ}(k_{\odot}, k_{\odot})}} M_{C_{\odot} C_{\odot}}^{k_{\odot}, k_{\odot}} |\psi\rangle_{C_{\odot} C_{\odot} AB}, \quad (5.22)$$

with $p_{ZZ}(k_{\odot}, k_{\odot})$ being the probability that both Alice and Bob chose the Z basis for a given round with a detection event and $M_{C_{\odot} C_{\odot}}^{k_{\odot}, k_{\odot}}$ is the Kraus operator representing the relay's action on the two incoming modes of the signal. We can write the $|\psi\rangle_{C_{\odot} C_{\odot} AB}$ state

as being the one right before returning to the central relay:

$$\begin{aligned}
|\psi\rangle_{ABC_{\odot}C_{\ominus}} &= U_B U_A \left(\left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}} \otimes \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B) \right) \\
&= \frac{1}{2} \left[\left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}} |00\rangle_{AB} + \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{(-1)}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}} |01\rangle_{AB} + \right. \\
&\quad \left. + \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{(-1)}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}} |10\rangle_{AB} + \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}} |11\rangle_{AB} \right].
\end{aligned} \tag{5.23}$$

The phase-error rate in (5.21) for each detection pattern in which $k_{\odot} \oplus k_{\ominus} = 1$ is:

$$e_Y^{1,0} = \frac{1}{4p_{ZZ}(1,0)} \left(\|_{AB} \langle RR | M_{C_{\odot}C_{\ominus}}^{1,0} |\psi\rangle_{C_{\odot}C_{\ominus}AB} \|^2 + \|_{AB} \langle LL | M_{C_{\odot}C_{\ominus}}^{1,0} |\psi\rangle_{C_{\odot}C_{\ominus}AB} \|^2 \right). \tag{5.24}$$

We then evaluate:

$$\begin{aligned}
{AB} \langle RR | M{C_{\odot}C_{\ominus}}^{1,0} |\psi\rangle_{C_{\odot}C_{\ominus}AB} &= M_{C_{\odot}C_{\ominus}}^{1,0} (_{AB} \langle RR | \psi \rangle_{C_{\odot}C_{\ominus}AB}) \\
&= M_{C_{\odot}C_{\ominus}}^{1,0} (-i) \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{(-1)}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}},
\end{aligned} \tag{5.25}$$

where we use $\langle RR| = \frac{1}{2}(\langle 00| - i\langle 01| - i\langle 10| - \langle 11|)$. Similarly for $\langle LL| = \frac{1}{2}(\langle 00| + i\langle 01| + i\langle 10| - \langle 11|)$, we have:

$$_{AB} \langle LL | M_{C_{\odot}C_{\ominus}}^{1,0} |\psi\rangle_{C_{\odot}C_{\ominus}AB} = M_{C_{\odot}C_{\ominus}}^{1,0} i \left| \frac{1}{\sqrt{2}}\alpha \right\rangle_{C_{\odot}} \left| \frac{(-1)}{\sqrt{2}}\alpha \right\rangle_{C_{\ominus}}. \tag{5.26}$$

Substituting in (5.24):

$$\begin{aligned}
e_Y^{1,0} &= \frac{1}{4p_{ZZ}(1,0)} \left(\|M_{C_{\odot}C_{\ominus}}^{1,0} (-i) \left| \frac{\alpha}{\sqrt{2}} \right\rangle_{C_{\odot}} \left| \frac{-\alpha}{\sqrt{2}} \right\rangle_{C_{\ominus}} \|^2 + \|M_{C_{\odot}C_{\ominus}}^{1,0} i \left| \frac{\alpha}{\sqrt{2}} \right\rangle_{C_{\odot}} \left| \frac{-\alpha}{\sqrt{2}} \right\rangle_{C_{\ominus}} \|^2 \right) \\
&= \frac{1}{4p_{ZZ}(1,0)} \left(\|M_{C_{\odot}C_{\ominus}}^{1,0} \sum_{n,m=0}^{\infty} (-i) C_n C_m^- |n, m\rangle_{C_{\odot}C_{\ominus}} \|^2 + \|M_{C_{\odot}C_{\ominus}}^{1,0} \sum_{n,m=0}^{\infty} i C_n C_m^- |n, m\rangle_{C_{\odot}C_{\ominus}} \|^2 \right) \\
&\leq \frac{1}{2p_{ZZ}(1,0)} \left(\sum_{n,m=0}^{\infty} (C_n C_m^-)^2 \|M_{C_{\odot}C_{\ominus}}^{1,0} |n, m\rangle_{C_{\odot}C_{\ominus}} \|^2 \right) \\
&= \frac{1}{2p_{ZZ}(1,0)} \left(\sum_{n,m=0}^{\infty} C_n C_m^- \sqrt{Y_{n,m}^{1,0}} \right)^2,
\end{aligned} \tag{5.27}$$

where $C_n = e^{\frac{-|\alpha|^2}{2}} (\frac{\alpha}{\sqrt{2}})^n / \sqrt{n!}$ and $C_m^- = e^{\frac{-|\alpha|^2}{2}} (\frac{-\alpha}{\sqrt{2}})^m / \sqrt{m!}$. Here, we considered $\alpha \in \mathbb{R}$. Note that the yields appear in the phase-error rate expression and are defined by:

$$Y_{n,m}^{k_{\odot}, k_{\ominus}} := \|M_{C_{\odot}C_{\ominus}}^{k_{\odot}, k_{\ominus}} |n, m\rangle_{C_{\odot}C_{\ominus}} \|^2 = p_{YY}(k_{\odot}, k_{\ominus} | n, m). \tag{5.28}$$

Similarly for $e_Y^{0,1}$ we have:

$$\begin{aligned}
e_Y^{0,1} &= \frac{1}{4p_{ZZ}(0,1)} \left(\|_{AB} \langle RL | M_{C_\odot C_\odot}^{0,1} |\psi\rangle_{C_\odot C_\odot AB} \|^2 + \|_{AB} \langle LR | M_{C_\odot C_\odot}^{0,1} |\psi\rangle_{C_\odot C_\odot AB} \|^2 \right) \\
&\leq \frac{1}{2p_{ZZ}(0,1)} \left(\sum_{n,m=0}^{\infty} (C_n C_m)^2 \|M_{C_\odot C_\odot}^{0,1} |n, m\rangle_{C_\odot C_\odot} \|^2 \right) \\
&= \frac{1}{2p_{ZZ}(0,1)} \left(\sum_{n,m=0}^{\infty} C_n C_m \sqrt{Y_{n,m}^{0,1}} \right)^2.
\end{aligned} \tag{5.29}$$

By defining $C_m^{k_\odot} = e^{\frac{-|\alpha|^2}{2}} ((-1)^{k_\odot} \alpha / \sqrt{2})^m / \sqrt{m!}$, we can write:

$$e_Y^{k_\odot, k_\odot} = \frac{1}{2p_{ZZ}(k_\odot, k_\odot)} \left(\sum_{n,m=0}^{\infty} C_n C_m^{k_\odot} \sqrt{Y_{n,m}^{k_\odot, k_\odot}} \right)^2. \tag{5.30}$$

These yields are constrained by the following set of equations, each one corresponding to the particular pair of decoy intensities (μ_i, ν_j) chosen by Alice and Bob:

$$p_{YY}(k_\odot, k_\odot | \mu_i \nu_j) = \sum_{n,m=0}^{\infty} e^{-\mu_i - \nu_j} \frac{\mu_i^n \nu_j^m}{n! m!} Y_{n,m}^{k_\odot, k_\odot}, \tag{5.31}$$

with $\mu_i \in \{\mu_i\}, \nu_j \in \{\nu_j\}$. One needs to derive upper bounds on the yields in (5.30) in order to achieve a lower bound on the key rate. The power of the decoy states strategy, as well as its necessity, is shown here. In a PNS attack, Eve needs to substitute the lossy channel for a lossless one and emulate the original loss in order to remain undetected by Alice and Bob. Alice and Bob will estimate upper bounds on the yields in (5.30), which depend on the intensity values as well as the gains observed experimentally. If Eve would attempt a PNS attack, Alice and Bob could verify that those upper bounds for the yields would be different and potentially broken—the loss Eve tries to recreate would result in different values for the gains and higher values for some yields, breaking the expected upper bound).

The phase-error rate (5.30) will be consequentially upper bounded by the yields' upper bounds, but will also contain the coefficients for the other yields trivially bounded by 1. This will result in a lower bound on the secret key rate. In summary, we upper bound the yields $Y_{nm}^{k_\odot, k_\odot}$ for $(n, m) \in \mathbb{S}$ where \mathbb{S} is a subset of $\{(n, m) | n, m \in \mathbb{N}_0\}$ which depends on the number of decoy settings used. The phase-error rate will be then bounded by:

$$e_Y^{k_\odot, k_\odot} \leq \frac{1}{2p_{ZZ}(k_\odot, k_\odot)} \left[\sum_{(n,m) \in \mathbb{S}} C_n C_m^{k_\odot} \sqrt{Y_{n,m}^{k_\odot, k_\odot}} + \sum_{(n,m) \notin \mathbb{S}} C_n C_m^{k_\odot} \right]^2. \tag{5.32}$$

The secret key rate can be written as:

$$r_{RQN} \geq r_{RQN}^{1,0} + r_{RQN}^{0,1}, \tag{5.33}$$

where $r_{RQN}^{k_\odot, k_\odot}$ is the key rate resulting of a detection event k_\odot, k_\odot with $k_\odot \oplus k_\odot = 1$ and is defined as:

$$r_{RQN}^{k_\odot, k_\odot} = p_{ZZ}(k_\odot, k_\odot) [1 - h(E_Z^{k_\odot, k_\odot}) - h(\bar{e}_Y^{k_\odot, k_\odot})]. \tag{5.34}$$

5.6 Upper bound estimation for the yields

In order to gain a better understanding of the average key rate, one can analytically obtain upper bounds for the yields according to different decoy settings used on the protocol. In this section, we will follow the same strategy used in [Grasselli e Curty 2019] to show how to obtain upper bounds for four different yields using two different possible decoy values. For simplicity, we assume that Alice and Bob both have the same set of two decoy intensities $\{\mu_0, \mu_1\}$ and apply them independently of one another. We will also omit the indices associated with detection (k_\odot, k_\ominus) since they do not affect the bounds estimations. We can then use (5.31) to write $p_{YY}(k_\odot, k_\ominus | \mu_i, \mu_j) := p^{i,j}$ and

$$\tilde{P}^{i,j} = e^{\mu_i + \mu_j} p^{i,j} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n \mu_j^m}{n!m!} Y_{n,m}. \quad (5.35)$$

We also constrain the yields on the fact that they represent a probability, such that for all n, m :

$$0 \leq Y_{n,m} \leq 1. \quad (5.36)$$

In order to derive the upper bounds on the yields, we can combine different gains (5.35) and maximize a specific yield while minimizing the others. For example, to obtain an upper bound on the yield Y_{11} , we evaluate

$$G_{11} = \tilde{P}^{0,0} + \tilde{P}^{1,1} - \tilde{P}^{0,1} - \tilde{P}^{1,0} = \sum_{n,m=0}^{\infty} \frac{1}{n!m!} Y_{n,m} (\mu_0^n - \mu_1^n) (\mu_0^m - \mu_1^m), \quad (5.37)$$

and it is clear to see that for $n = 0$ or $m = 0$, the coefficients for the yields are zero. So we can rewrite (5.37) as

$$G_{11} = Y_{11}(\mu_0 - \mu_1)^2 + \sum_{\substack{n,m=1 \\ n+m>2}}^{\infty} Y_{n,m} (\mu_0^n - \mu_1^n) (\mu_0^m - \mu_1^m). \quad (5.38)$$

Now, in order to estimate an upper bound on Y_{11} , we need to minimize all other $Y_{n,m}$ yields in each sum component of (5.38). Since the coefficients are always positive, we can do that by setting all other yields to zero, resulting in:

$$\bar{Y}_{11} \leq \frac{G_{11}}{(\mu_0 - \mu_1)^2} = \frac{\tilde{P}^{0,0} + \tilde{P}^{1,1} - \tilde{P}^{0,1} - \tilde{P}^{1,0}}{(\mu_0 - \mu_1)^2}. \quad (5.39)$$

Note that by combining the gains in (5.38) we eliminate the contributions of all the yields Y_{0m} and Y_{n0} , resulting in Y_{11} being the yield with the highest contribution (bigger coefficients) in the equation. We can use the same logic to find upper bounds on yields Y_{01} , Y_{10} and Y_{00} .

By writing

$$G_{01} = \mu_1 \tilde{P}^{0,0} + \mu_0 \tilde{P}^{1,1} - \mu_1 \tilde{P}^{0,1} - \mu_0 \tilde{P}^{1,0} = \sum_{n,m=0}^{\infty} \frac{1}{n!m!} Y_{n,m} (\mu_1 \mu_0^n - \mu_0 \mu_1^n) (\mu_0^m - \mu_1^m), \quad (5.40)$$

we can easily see that the coefficients of the yields when $n = 1$ or $m = 0$ are zero, and we can write:

$$\begin{aligned} G_{01} = & -Y_{01}(\mu_0 - \mu_1)^2 - \sum_{m=2}^{\infty} \frac{1}{m!} Y_{0m}(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m) \\ & + \sum_{\substack{n=2 \\ m=1}}^{\infty} \frac{\mu_0 \mu_1}{n! m!} Y_{nm}(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m - \mu_1^m). \end{aligned} \quad (5.41)$$

In order to obtain an upper bound for Y_{01} , we need to consider the minimal value for the remaining yields. In other words, Y_{01} is maximal when the yields with the same sign coefficients are minimal and the yields with opposite sign coefficients are maximal. We can do that by setting Y_{0m} with $m \geq 2$ to zero and Y_{nm} with $n \geq 2$ and $m \geq 1$ to 1, resulting in

$$\bar{Y}_{01} \leq \frac{1}{(\mu_0 - \mu_1)^2} \left[-G_{01} + \left(\sum_{m=1}^{\infty} \frac{\mu_0^m}{m!} - \frac{\mu_1^m}{m!} \right) \left(\sum_{n=2}^{\infty} \mu_1 \frac{\mu_0^n}{n!} - \mu_0 \frac{\mu_1^n}{n!} \right) \right], \quad (5.42)$$

and finally:

$$\bar{Y}_{01} \leq \frac{(e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1}) - G_{01}}{(\mu_0 - \mu_1)^2}. \quad (5.43)$$

For the yield Y_{10} , we can write:

$$G_{10} = \mu_1 \tilde{P}^{0,0} + \mu_0 \tilde{P}^{1,1} - \mu_0 \tilde{P}^{0,1} - \mu_1 \tilde{P}^{1,0} = \sum_{n,m=0}^{\infty} \frac{1}{n! m!} Y_{n,m}(\mu_0^n - \mu_1^n)(\mu_1 \mu_0^m - \mu_0 \mu_1^m). \quad (5.44)$$

The coefficients for the yields Y_{n1} and Y_{0m} are zero, therefore:

$$\begin{aligned} G_{10} = & -Y_{10}(\mu_0 - \mu_1)^2 - \sum_{n=2}^{\infty} \frac{1}{n!} Y_{n0}(\mu_0 - \mu_1)(\mu_0^n - \mu_1^n) \\ & + \sum_{\substack{n=1 \\ m=2}}^{\infty} \frac{\mu_0 \mu_1}{n! m!} Y_{nm}(\mu_0^n - \mu_1^n)(\mu_0^{m-1} - \mu_1^{m-1}). \end{aligned} \quad (5.45)$$

Following the same previous logic, in order to obtain \bar{Y}_{10} we can set Y_{n0} with $n \geq 2$ to zero and Y_{nm} with $n \geq 1$ and $m \geq 2$ to 1:

$$\bar{Y}_{10} \leq \frac{1}{(\mu_0 - \mu_1)^2} \left[-G_{10} + \left(\sum_{n=1}^{\infty} \frac{\mu_0^n}{n!} - \frac{\mu_1^n}{n!} \right) \left(\sum_{m=2}^{\infty} \mu_1 \frac{\mu_0^m}{m!} - \mu_0 \frac{\mu_1^m}{m!} \right) \right], \quad (5.46)$$

and finally:

$$\bar{Y}_{10} \leq \frac{(e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1}) - G_{10}}{(\mu_0 - \mu_1)^2}. \quad (5.47)$$

In order to calculate an upper bound on Y_{00} we write:

$$G_{00} = \mu_1^2 \tilde{P}^{0,0} + \mu_0^2 \tilde{P}^{1,1} - \mu_0 \mu_1 \tilde{P}^{0,1} - \mu_0 \mu_1 \tilde{P}^{1,0} = \sum_{n,m=0}^{\infty} \frac{1}{n! m!} Y_{n,m}(\mu_1 \mu_0^n - \mu_0 \mu_1^n)(\mu_1 \mu_0^m - \mu_0 \mu_1^m). \quad (5.48)$$

Since the coefficients for Y_{1m} and Y_{n1} are zero, we have:

$$G_{00} = Y_{00}(\mu_0 - \mu_1)^2 - \mu_0\mu_1(\mu_0 - \mu_1) \left[\sum_{m=2}^{\infty} \frac{1}{m!} Y_{0m}(\mu_0^{m-1} - \mu_1^{m-1}) + \sum_{n=2}^{\infty} \frac{1}{n!} Y_{n0}(\mu_0^{n-1} - \mu_1^{n-1}) \right] \\ + \sum_{n,m=2}^{\infty} \frac{\mu_0^2 \mu_1^2}{n!m!} Y_{nm}(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^{m-1} - \mu_1^{m-1}). \quad (5.49)$$

By setting to zero the yields with the same sign as Y_{00} , namely the yields Y_{nm} with $n, m \geq 2$, and setting the yields with opposite sign (Y_{0m} and Y_{n0}) to 1, we have:

$$\bar{Y}_{00} \leq \frac{\mu_0\mu_1}{(\mu_0 - \mu_1)} \left[\left(\sum_{m=2}^{\infty} \frac{\mu_0^{m-1}}{m!} - \frac{\mu_1^{m-1}}{m!} \right) \left(\sum_{n=2}^{\infty} \frac{\mu_0^{n-1}}{n!} - \frac{\mu_1^{n-1}}{n!} \right) \right] + \frac{G_{00}}{(\mu_0 - \mu_1)^2}. \quad (5.50)$$

And finally:

$$\bar{Y}_{00} \leq \frac{2(\mu_1 e^{\mu_0} - \mu_0 e^{\mu_1} + \mu_0 - \mu_1)}{(\mu_0 - \mu_1)} + \frac{G_{00}}{(\mu_0 - \mu_1)^2}. \quad (5.51)$$

5.7 Secret key rate estimation

Since we do not have experimental statistics for the gains of the protocol, and thus the quantities G_{ij} , we will estimate the yields directly. We remark that in a more realistic simulation or experimental scenario, the yields are calculated via those quantities. To approximate a near-optimal secret key rate for the Rio Quantum Network (RQN), we model quantum bit error rates (QBERs) and detection yields using generalized parameter values such as network loss, laser intensities and dark count probabilities. For preliminary estimations, errors in the Z basis are expressed as [Gisin et al. 2002]:

$$E_Z^{(1,0)} = E_Z^{(0,1)} = \frac{p_{\text{error}}}{p_{\text{click}}} = \frac{e_d \eta (1 - e^{-\mu_s}) + \frac{Y_{00}}{2}}{Y_{00} + \eta (1 - e^{-\mu_s})}, \quad (5.52)$$

where $Y_{00} \approx 10^{-6}$ corresponds to the vacuum yield from detector dark counts, $e_d \approx 0.01$ represents intrinsic device misalignment, and $\mu_s = |\alpha|^2 \approx 0.02$ is the signal intensity. The phase-error rate $e_Y^{k_{\odot}, k_{\odot}}$ in the decoy-state framework is derived using yields for up to two photons, assuming Poissonian photon statistics. Single-photon yields (Y_{01}, Y_{10}) and two-photon yields (Y_{11}, Y_{02}, Y_{20}) are approximated as $\mu_d e^{-\mu_d} \eta$ and $\frac{\mu_d^2}{2!} e^{-\mu_d} \eta$, respectively, where $\mu_d \approx 0.1$ denotes the decoy intensity. With Alice and Bob selecting the Z -basis 90% of the time, the joint probability p_{ZZ} becomes 0.81, while $p_{ZZ}(1,0)$ and $p_{ZZ}(0,1)$ are calculated as $(p_{ZZ}/2)p_{\text{click}}$. Here, $p_{\text{click}} = Y_{00} + \eta(1 - e^{-\mu_s})$ defines the total detection probability. This framework enables the computation of the secret key rate (Equation (5.33)) as a function of total channel loss.

Figure 9 plots the secret key rate per pulse (logarithmic scale) against total channel loss for the RQN protocol, benchmarked against the PLOB bound [Pirandola et al. 2017] and the Gottesman-Lo-Lütkenhaus-Preiskill (GLLP) analysis for BB84 with weak coherent

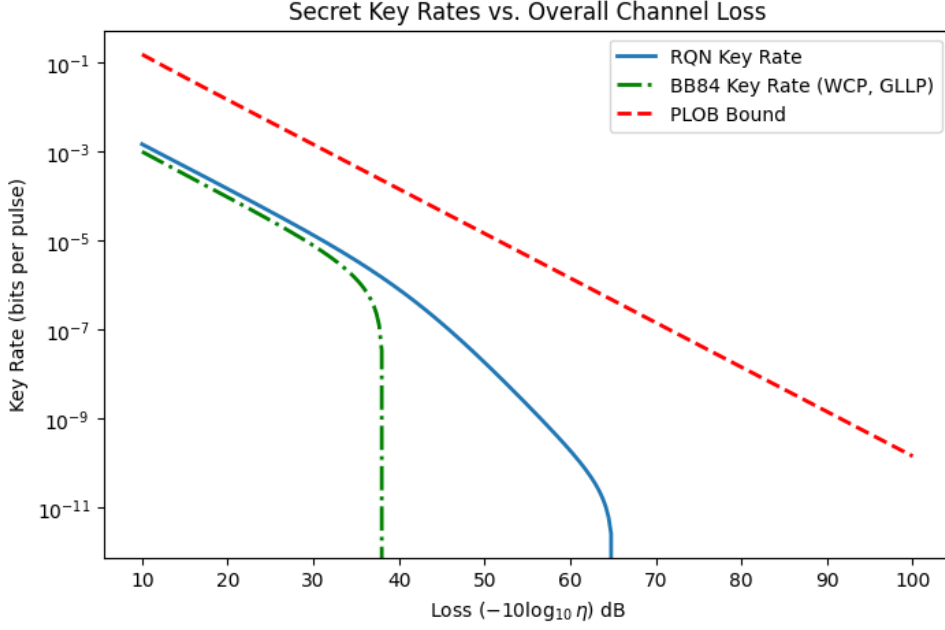


Figure 9 – Secret key rate per pulse in logarithmic scale for the Rio Quantum Network as a function of the overall loss of the network. The solid line represents the secret key rate for the RQN protocol. We compare it to the PLOB-bound [Pirandola et al. 2017], and to the GLLP secret key rate for a BB84 protocol using WCPs [Gottesman et al. 2004].

pulses (WCPs) [Gottesman et al. 2004]. The GLLP key rate vanishes at approximately 38.6 dB loss, whereas the RQN protocol sustains a non-zero rate up to around 65 dB, demonstrating superior resilience in high-loss regimes. While the RQN key rate does not surpass the PLOB bound—a fundamental limit for repeaterless quantum communication—it remains competitive, operating closer to this theoretical threshold than conventional protocols under high-loss conditions.

For a transmittance of $\eta = 0.5$, the model predicts a secret key rate of $r_{\text{RQN}} \approx 0.0072$ per round. At MHz pulse repetition rates, this corresponds to approximately 7200 secure bits per second—a promising result under idealized conditions. This simplified analysis assumes stable parameter values and neglects operational imperfections such as temporal phase drift or polarization misalignment. Future refinements could incorporate dynamic channel fluctuations and finite-key effects to better approximate real-world performance. The RQN’s ability to approach the PLOB bound while outperforming the GLLP benchmark aligns with the network’s design objectives of enabling secure communication in lossy, repeaterless environments. This preliminary analysis thus validates the protocol’s feasibility while highlighting the need for further experimental validation to address practical implementation constraints.

6 Conclusions

We have shown how quantum key distribution (QKD) represents a paradigm shift in secure communication, offering information-theoretic security rooted in the laws of quantum mechanics. This work has given an overview of the more prominent protocols in QKD, emphasizing on the foundational BB84, explicitly calculating its secret key rate while discussing its security assumptions, especially the need for trusted physical devices. The decoy-state strategy, introduced to mitigate vulnerabilities in laser-based sources, exemplifies how theoretical innovations can bridge the gap between idealized protocols and real-world constraints.

To address limitations imposed by device trust, we examined device-independent QKD (DI-QKD), which uses Bell inequality violations to ensure secure communication between two parties. While theoretically elegant, DI-QKD remains impractical for near-term deployment due to its extreme technical demands and high sensitivity to channel losses. Measurement-device-independent QKD (MDI-QKD) emerged as a pragmatic alternative, confining trust assumptions to photon sources while guaranteeing security in spite of untrusted devices. This framework gives way to one of the most promising protocols for high-loss security communication, twin-field QKD. In TF-QKD, the users are able to overcome the repeaterless secret key capacity bound (PLOB) through phase-encoding and remote single-photon interference. We have shown its security analysis and how it still faces challenges in real-world deployment, such as phase instability and asymmetric channel conditions, which are exacerbated in multi-user networks like the Rio Quantum Network (RQN).

Finally, we discussed the RQN project, which by itself poses as a major development landmark for Brazil in quantum technologies and quantum communication. Expected to operate in high-loss, asymmetric environments, the network demands a protocol that combines TF-QKD's resilience with practical scalability. We have shown how a Sagnac-Based TF-QKD can provide a similar security analysis while severely reducing implementation costs and easily allowing new users to join the network loop. This variation uses a shared laser source and common-path signal propagation to inherently synchronize phases across users, eliminating the need for individual light sources, and tolerating channel asymmetries—critical advantages for a heterogeneous network spanning multiple institutions in a metropolitan area. We used both TF-QKD and BB84 analysis to provide the reader with a secret key rate expression in an ideal single-photon scenario as well as in the practical scenario using the decoy state strategy. We have established a "near-ideal" model

for the secret key rate, achieving approximately 7200 bits per second at 0.5 transmittance under idealized conditions, sustaining communication up to 61.5dB loss. While this performance does not surpass the PLOB bound, it can outperform conventional imperfect-light-source BB84 (GLLP) and positions the RQN as a practical solution for high-loss, repeaterless environments. The deployment of TF-QKD marks a promising first step in implementing the Rio Quantum Network and thus contributing to Brazil's research field in quantum cryptography. Furthermore, studies such as [Donne et al. 2025] demonstrate the critical role of integrated quantum networks in enabling quantum computing and quantum communication, advancing us closer to realizing a quantum internet.

Future steps for this project include attempts to establish a Conference-Key-Agreement QKD protocol, given the network's multi-user structure. Also, more precise simulations and models can be made while the network is not fully operating, as well as using it as a "sandbox" for elaborating novel QKD protocols while accounting for its practical limitations.

In closing, this work reaffirms that quantum networks are not merely theoretical constructs but tangible infrastructures with transformative potential. The Rio Quantum Network protocol, by balancing theoretical rigor with practical feasibility, illustrates how tailored solutions can overcome global QKD challenges while addressing local priorities and financial limitations. As quantum technologies transition from labs to real-world applications, initiatives like the RQN will play a pivotal role in shaping Brazil's future in secure communication.

Appendix

A: Eve's uncertainty does not increase under symmetrization

This proof follows the steps detailed in [Grasseli 2021]. In the BB84 security proof, it is said that, without loss of generality, Eve's uncertainty on Alice's raw key bit $H(R_A|E)_\rho$ does not increase under symmetrization, i.e.:

$$H(R_A|E)_\rho \geq H(R_A|E)_{\tilde{\rho}} \quad (1)$$

where ρ is referring to the state ρ_{AB} distributed to Alice and Bob by Eve and $\tilde{\rho}_{AB}$ is the state after the symmetrization maps ($\mathcal{E}_X \circ \mathcal{E}_Z$):

$$\begin{aligned} \tilde{\rho}_{AB} = \frac{1}{4} & \left[\rho_{AB} + (Z \otimes Z)\rho_{AB}(Z \otimes Z) \right. \\ & \left. + (X \otimes X)\rho_{AB}(X \otimes X) + (Y \otimes Y)\rho_{AB}(Y \otimes Y) \right]. \end{aligned} \quad (2)$$

First, we argue that this is equivalent to Eve preparing one of four states depending on the outcome of a random variable $t \in \{0, 1, 2, 3\}$: $\rho_{AB}, (Z \otimes Z)\rho_{AB}(Z \otimes Z), (X \otimes X)\rho_{AB}(X \otimes X)$ and $(Y \otimes Y)\rho_{AB}(Y \otimes Y)$, respectively. The state prepared by Eve can be described as:

$$\tilde{\rho}_{ABET} = \frac{1}{4} \sum_t |\phi_{ABE}^t\rangle \langle \phi_{ABE}^t| \otimes |t\rangle \langle t|_T, \quad (3)$$

where $\{\phi_{ABE}^t\}_{t=1}^4$ are the pure, global states shared between Alice, Bob and Eve. The subsystem T is the classical register which stores the classical random variable t . Furthermore, we assume that Eve holds the purifying system T' of the state (3), with the purified global state being:

$$|\phi_{ABETT'}\rangle = \frac{1}{2} \sum_t |\phi_{ABE}^t\rangle \otimes |t\rangle_T \otimes |t\rangle_{T'}. \quad (4)$$

In summary, we need to verify that $H(R_A|E)_\rho \geq H(R_A|E_{\text{total}})_{\tilde{\rho}}$, where $E_{\text{total}} = ETT'$ consists of Eve's quantum side information E , the outcome of the random variable T and the purifying system T' . We start by using the strong subadditivity property (Theorem 2.6):

$$H(R_A|E_{\text{total}})_{\tilde{\rho}} \leq H(R_A|ET)_{\tilde{\rho}}. \quad (5)$$

Alice's raw key R_A is formed by the outcome of her measurement on state (3). We calculate the state $\tilde{\rho}_{R_AET}$ in which the entropies (5) are computed on by applying the map

$\mathcal{E}_{R_A}(\sigma) = \sum_{a=0}^1 |a\rangle \langle a| \sigma |a\rangle \langle a|$ and tracing out Bob's system on the state $\tilde{\rho}_{ABET}$:

$$\begin{aligned}\tilde{\rho}_{R_AET} &= (\mathcal{E}_{R_A} \otimes \mathbb{I}_{ET}) \text{Tr}_B[\tilde{\rho}_{ABET}] \\ &= \frac{1}{4} (\mathcal{E}_{R_A} \otimes \mathbb{I}_{ET}) \text{Tr}_B \left[\sum_t |\phi_{ABE}^t\rangle \langle \phi_{ABE}^t| \otimes |t\rangle \langle t|_T \right] \\ &:= \frac{1}{4} \sum_t \rho_{R_AE}^t \otimes |t\rangle \langle t|_T.\end{aligned}\tag{6}$$

Since the state $\rho_{R_AE}^t$ is a c.q. state, it follows that $H(\tilde{\rho}_{R_AET}) = \sum_t p(t) H(\tilde{\rho}_{R_AE})$. Thus,

$$H(R_A|ET)_{\tilde{\rho}} = \frac{1}{4} \sum_t H(R_A|E)_{\rho^t} \geq H(R_A|E_{\text{total}})_{\tilde{\rho}}.\tag{7}$$

Now, we explicitly compute $\rho_{R_AE}^t$ to show that $H(R_A|E)_{\rho^t} = H(R_A|E)_{\rho}$ (i.e. the entropy does not depend on the variable t). We have that:

$$\rho_{R_AE}^t = (\mathcal{E}_{R_A} \otimes \mathbb{I}_{ET}) \text{Tr}_B \left[|\phi_{ABE}^t\rangle \langle \phi_{ABE}^t| \right]\tag{8}$$

where $|\phi_{ABE}^t\rangle$ is the purification of one of the states prepared by Eve according to T . Let us fix $t = 2$ and let the state be $(X \otimes X)\rho_{AB}(X \otimes X)$, noting that this process can be done analogously in the other cases. We can write ρ_{AB} in terms of its eigenvalues λ :

$$\rho_{AB} = \sum_{\lambda} \lambda |\lambda\rangle \langle \lambda|.\tag{9}$$

Thus, the state $|\phi_{ABE}^t\rangle$ reads:

$$|\phi_{ABE}^t\rangle = \sum_{\lambda} \sqrt{\lambda} |\lambda^t\rangle_{AB} \otimes |\xi_{\lambda}\rangle_E.\tag{10}$$

where $|\lambda^t\rangle_{AB} = (X \otimes X) |\lambda\rangle$ are the eigenstates of the operator $(X \otimes X)\rho_{AB}(X \otimes X)$. We then compute:

$$\begin{aligned}\rho_{R_AE}^t &= (\mathcal{E}_{R_A} \otimes \mathbb{I}_{ET}) \text{Tr}_B \left[\sum_{\lambda\sigma} \sqrt{\lambda\sigma} |\lambda^t\rangle \langle \sigma^t|_{AB} \otimes |e_{\lambda}\rangle \langle e_{\sigma}|_E \right] \\ &= \sum_a^1 |a\rangle \langle a| \otimes \text{Tr}_B \left[\sum_{\lambda\sigma} \sqrt{\lambda\sigma} (\langle a|_A \otimes \mathbb{I}_B) |\lambda^t\rangle \langle \sigma^t|_{AB} (|a\rangle_A \otimes \mathbb{I}_B) \right] \otimes |e_{\lambda}\rangle \langle e_{\sigma}|_E \\ &= \sum_a^1 |a\rangle \langle a| \otimes \text{Tr}_B \left[\sum_{\lambda\sigma} \sqrt{\lambda\sigma} (\langle a|_A \otimes \mathbb{I}_B) (X \otimes X) |\lambda\rangle \langle \sigma|_{AB} (X \otimes X) (|a\rangle_A \otimes \mathbb{I}_B) \right] \otimes |e_{\lambda}\rangle \langle e_{\sigma}|_E \\ &= \sum_a^1 |a\rangle \langle a| \otimes \text{Tr}_B \left[\sum_{\lambda\sigma} \sqrt{\lambda\sigma} (\langle \bar{a}|_A \otimes \mathbb{I}_B) |\lambda\rangle \langle \sigma|_{AB} (|\bar{a}\rangle_A \otimes \mathbb{I}_B) \right] \otimes |e_{\lambda}\rangle \langle e_{\sigma}|_E \\ &= \sum_a^1 |a\rangle \langle a| \otimes \rho_E^{\bar{a}}.\end{aligned}\tag{11}$$

Here, we used the fact that since Alice's raw key bit is the result of a Z -basis measurement, the action of X flips its eigenstates: $X|a\rangle = |\bar{a}\rangle$. By relabeling the classical outcomes $a \leftrightarrow \bar{a}$, we obtain that

$$\rho_{R_AE}^t = \sum_a^1 |\bar{a}\rangle \langle \bar{a}| \otimes \rho_E^a\tag{12}$$

We can calculate the state ρ_{RAE} analogously:

$$\begin{aligned}
\rho_{RAE} &= (\mathcal{E}_{RA} \otimes \mathbb{I}_E) \text{Tr}_B \left[|\phi_{ABE}\rangle \langle \phi_{ABE}| \right] \\
&= \sum_a^1 |a\rangle \langle a| \otimes \text{Tr}_B \left[\sum_{\lambda\sigma} \sqrt{\lambda\sigma} (\langle a|_A \otimes \mathbb{I}_B) |\lambda\rangle \langle \sigma|_{AB} (|a\rangle_A \otimes \mathbb{I}_B) \right] \otimes |e_\lambda\rangle \langle e_\sigma|_E \\
&= \sum_a^1 |a\rangle \langle a| \otimes \rho_E^a
\end{aligned} \tag{13}$$

and conclude that the states ρ_{RAE}^t and ρ_{RAE} are the same state up to a classical permutation, thus we can write:

$$H(R_A|E)_{\rho^t} = H(R_A|E)_\rho \quad \forall t, \tag{14}$$

and finally:

$$H(R_A|E)_\rho \geq H(R_A|E_{\text{total}})_{\tilde{\rho}}. \tag{15}$$

B: Twin-Field protocol phase error-rate

The definition of the phase-error rate given in 4.42:

$$e_Z^{k_c, k_d} = \sum_{j=0,1} ||_{AB} \langle jj | \chi^{k_c, k_d} \rangle_{Aa'Bb'} ||^2, \tag{16}$$

with

$$|\chi^{k_c, k_d}\rangle_{Aa'Bb'} := \frac{M_{a,b}^{k_c, k_d} |\psi\rangle_{Aa} |\psi\rangle_{Bb}}{\sqrt{p_{XX}(k_c, k_d)}}, \tag{17}$$

where $M_{a,b}^{k_c, k_d}$ is the Kraus operator that describes the action of the relay on the signals and a' and b' are the modes of the signals after the relay's action. If we only look into Alice's part in the phase error rate, we can see that:

$${}_A \langle j | \psi_X \rangle_{Aa} = \frac{{}_A \langle j | + \rangle_A |\alpha_A\rangle_a + {}_A \langle j | - \rangle_A |-\alpha_A\rangle_a}{2} = e^{\frac{-|\alpha_A|^2}{2}} \sum_{n=0}^{\infty} \frac{1}{\sqrt{n!}} \frac{(\alpha_A^n + (-1)^j (-\alpha_A)^n)}{2} |n\rangle_a, \tag{18}$$

which results in

$${}_A \langle 0 | \psi_X \rangle_{Aa} = e^{\frac{-|\alpha_A|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha_A^{2n}}{\sqrt{2n!}} |2n\rangle_a = \sum_{n=0}^{\infty} C_{2n}^a |2n\rangle_a \tag{19}$$

and

$${}_A \langle 1 | \psi_X \rangle_{Aa} = e^{\frac{-|\alpha_A|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha_A^{2n+1}}{\sqrt{(2n+1)!}} |2n+1\rangle_a = \sum_{n=0}^{\infty} C_{2n+1}^a |2n+1\rangle_a, \tag{20}$$

with $C_n = e^{\frac{-|\alpha_A|^2}{2}} \frac{\alpha_A^n}{\sqrt{n!}}$. The same goes for Bob's part. Therefore, the phase error rate can be written as:

$$\begin{aligned}
e_Z^{k_c, k_d} &= \|_{AB} \langle 00 | \chi^{k_c, k_d} \rangle_{Aa'Bb'} \|^2 + \|_{AB} \langle 11 | \chi^{k_c, k_d} \rangle_{Aa'Bb'} \|^2 \\
&= \frac{1}{p_{XX}(k_c, k_d)} \left[\|M_{a,b}^{k_c, k_d} \sum_{n,m=0}^{\infty} C_{2n}^a C_{2m}^b |2n\rangle_a |2m\rangle_b \|^2 + \right. \\
&\quad \left. \|M_{a,b}^{k_c, k_d} \sum_{n,m=0}^{\infty} C_{2n+1}^a C_{2m+1}^b |2n+1\rangle_a |2m+1\rangle_b \|^2 \right] \\
&\leq \sum_{n,m=0}^{\infty} \frac{1}{p_{XX}(k_c, k_d)} \left[(C_{2n}^a C_{2m}^b)^2 \langle 2n, 2m | M_{a,b}^{k_c, k_d \dagger} M_{a,b}^{k_c, k_d} | 2n, 2m \rangle_{ab} + \right. \\
&\quad \left. + (C_{2n+1}^a C_{2m+1}^b)^2 \langle 2n+1, 2m+1 | M_{a,b}^{k_c, k_d \dagger} M_{a,b}^{k_c, k_d} | 2n+1, 2m+1 \rangle_{ab} \right]
\end{aligned} \tag{21}$$

We then have:

$$\begin{aligned}
e_Z^{k_c, k_d} &= \sum_{n,m=0}^{\infty} \frac{1}{p_{XX}(k_c, k_d)} \left[(C_{2n}^a C_{2m}^b)^2 \|M_{a,b}^{k_c, k_d} |2n, 2m\rangle_{ab} \|^2 \right. \\
&\quad \left. + (C_{2n+1}^a C_{2m+1}^b)^2 \|M_{a,b}^{k_c, k_d} |2n+1, 2m+1\rangle_{ab} \|^2 \right].
\end{aligned} \tag{22}$$

We can then define the yields as being

$$\|M_{a,b}^{k_c, k_d} |2n, 2m\rangle_{ab} \|^2 := p_{ZZ}(k_c, k_d | 2n, 2m) = Y_{2n, 2m}^{k_c, k_d} \tag{23}$$

and

$$\|M_{a,b}^{k_c, k_d} |2n+1, 2m+1\rangle_{ab} \|^2 := p_{ZZ}(k_c, k_d | 2n+1, 2m+1) = Y_{2n+1, 2m+1}^{k_c, k_d}. \tag{24}$$

Then, finally, the phase error rate is

$$e_Z^{k_c, k_d} = \frac{1}{p_{xx}(k_c, k_d)} \left[\left(\sum_{n,m=0}^{\infty} C_{2n}^a C_{2m}^b \sqrt{Y_{2n, 2m}^{k_c, k_d}} \right)^2 + \left(\sum_{n,m=0}^{\infty} C_{2n+1}^a C_{2m+1}^b \sqrt{Y_{2n+1, 2m+1}^{k_c, k_d}} \right)^2 \right]. \tag{25}$$

Bibliography

ABRUZZO, S.; KAMPERMANN, H.; BRUSS, D. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A*, American Physical Society, v. 89, p. 012301, Jan 2014. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevA.89.012301>>. Cited on page 65.

ACÍN, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, American Physical Society, v. 98, p. 230501, Jun 2007. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.98.230501>>. Cited 2 times on pages 59 and 60.

ACÍN, A.; MASSAR, S.; PIRONIO, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, v. 8, n. 8, p. 126, aug 2006. Disponível em: <<https://dx.doi.org/10.1088/1367-2630/8/8/126>>. Cited on page 60.

ARNON-FRIEDMAN, R. et al. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, v. 9, n. 1, p. 459, 01 2018. ISSN 2041-1723. Disponível em: <<https://doi.org/10.1038/s41467-017-02307-4>>. Cited on page 60.

ARNON-FRIEDMAN, R.; RENNER, R.; VIDICK, T. Simple and tight device-independent security proofs. *SIAM Journal on Computing*, v. 48, n. 1, p. 181–225, 2019. Disponível em: <<https://doi.org/10.1137/18M1174726>>. Cited on page 60.

BELL, J. S. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, American Physical Society, v. 1, p. 195–200, Nov 1964. Disponível em: <<https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195>>. Cited 2 times on pages 26 and 57.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, v. 560, p. 7–11, 1984. ISSN 0304-3975. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0304397514004241>>. Cited 4 times on pages 20, 39, 42, and 43.

BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. (Ed.). *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer, 2009. v. 5292. (Lecture Notes in Computer Science, v. 5292). ISBN 978-3-540-88701-0. Cited on page 20.

BOARON, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, American Physical Society, v. 121, p. 190502, Nov 2018. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.121.190502>>. Cited on page 71.

BRIEGEL, H.-J. et al. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, American Physical Society, v. 81, p. 5932–5935, Dec 1998. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.81.5932>>. Cited on page 65.

- CHRISTANDL, M.; KÖNIG, R.; RENNER, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, American Physical Society, v. 102, p. 020504, Jan 2009. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevLett.102.020504>. Cited on page 46.
- CLAUSER, J. F. et al. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, American Physical Society, v. 23, p. 880–884, Oct 1969. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevLett.23.880>. Cited on page 57.
- CURTY, M.; AZUMA, K.; LO, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information*, v. 5, n. 1, p. 64, Jul 2019. ISSN 2056-6387. Disponível em: <https://doi.org/10.1038/s41534-019-0175-6>. Cited 7 times on pages 14, 65, 67, 69, 71, 73, and 74.
- DEVETAK, I.; WINTER, A. Distillation of secret key and entanglement from quantum states. *Proc. Math. Phys. Eng. Sci.*, The Royal Society, v. 461, n. 2053, p. 207–235, jan. 2005. Cited 2 times on pages 48 and 59.
- DONNE, C. D. et al. An operating system for executing applications on quantum network nodes. *Nature*, v. 639, n. 8054, p. 321–328, mar 2025. Disponível em: <https://doi.org/10.1038/s41586-025-08704-w>. Cited on page 88.
- DUPUIS, F.; FAWZI, O. Entropy accumulation with improved second-order term. *IEEE Transactions on Information Theory*, v. 65, n. 11, p. 7596–7612, 2019. Cited on page 60.
- DUPUIS, F.; FAWZI, O.; RENNER, R. Entropy accumulation. *Communications in Mathematical Physics*, v. 379, n. 3, p. 867–913, 11 2020. ISSN 1432-0916. Disponível em: <https://doi.org/10.1007/s00220-020-03839-5>. Cited on page 60.
- EKERT, A. K. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, American Physical Society, v. 67, p. 661–663, Aug 1991. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>. Cited 3 times on pages 20, 57, and 59.
- GISIN, N. et al. Quantum cryptography. *Rev. Mod. Phys.*, American Physical Society, v. 74, p. 145–195, Mar 2002. Disponível em: <https://link.aps.org/doi/10.1103/RevModPhys.74.145>. Cited on page 85.
- GOTTESMAN, D. et al. Security of quantum key distribution with imperfect devices. In: *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*. [S.l.: s.n.], 2004. p. 136–. Cited 2 times on pages 15 and 86.
- GRASSELLI, F. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Springer, 2021. (Quantum Science and Technology). ISBN 978-3-030-64359-0. Disponível em: <https://link.springer.com/book/10.1007/978-3-030-64360-7>. Cited 4 times on pages 45, 62, 67, and 89.
- GRASSELLI, F.; CURTY, M. Practical decoy-state method for twin-field quantum key distribution. *New Journal of Physics*, IOP Publishing, v. 21, n. 7, p. 073001, jul 2019. Disponível em: <https://dx.doi.org/10.1088/1367-2630/ab2b00>. Cited on page 83.

HONG, C. K.; OU, Z. Y.; MANDEL, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, American Physical Society, v. 59, p. 2044–2046, Nov 1987. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.59.2044>>. Cited on page 62.

KONIG, R.; RENNER, R.; SCHAFFNER, C. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, v. 55, n. 9, p. 4337–4347, 2009. Cited 2 times on pages 36 and 37.

LI, Y.-H. et al. *Free-Space Twin-Field Quantum Key Distribution*. 2025. Disponível em: <<https://arxiv.org/abs/2503.17744>>. Cited on page 71.

LIU, Y. et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.*, American Physical Society, v. 130, p. 210801, May 2023. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.130.210801>>. Cited on page 71.

LO, H.-K. Quantum key distribution with vacua or dim pulses as decoy states. In: *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*. [S.l.: s.n.], 2004. p. 137–. Cited on page 55.

LO, H.-K.; CURTY, M.; QI, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, American Physical Society, v. 108, p. 130503, Mar 2012. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.108.130503>>. Cited 4 times on pages 14, 61, 62, and 64.

LO, H.-K.; MA, X.; CHEN, K. Decoy state quantum key distribution. *Physical Review Letters*, American Physical Society (APS), v. 94, n. 23, jun 2005. Disponível em: <<https://doi.org/10.1103/PhysRevLett.94.230504>>. Cited on page 55.

LUCAMARINI, M. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, v. 557, n. 7705, p. 400–403, 05 2018. ISSN 1476-4687. Disponível em: <<https://doi.org/10.1038/s41586-018-0066-6>>. Cited 2 times on pages 65 and 73.

NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. [S.l.]: Cambridge University Press, 2000. Cited 2 times on pages 23 and 32.

PANAYI, C. et al. Memory-assisted measurement-device-independent quantum key distribution. *New Journal of Physics*, IOP Publishing, v. 16, n. 4, p. 043005, apr 2014. Disponível em: <<https://dx.doi.org/10.1088/1367-2630/16/4/043005>>. Cited on page 65.

PEARLE, P. M. Hidden-variable example based upon data rejection. *Phys. Rev. D*, American Physical Society, v. 2, p. 1418–1425, Oct 1970. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevD.2.1418>>. Cited on page 60.

PIRANDOLA, S. et al. Fundamental limits of repeaterless quantum communications. *Nature Communications*, v. 8, n. 1, p. 15043, 04 2017. ISSN 2041-1723. Disponível em: <<https://doi.org/10.1038/ncomms15043>>. Cited 4 times on pages 15, 64, 85, and 86.

RENNER, R. Security of quantum key distribution. *International Journal of Quantum Information*, v. 06, n. 01, p. 1–127, 2008. Disponível em: <<https://doi.org/10.1142/S0219749908003256>>. Cited on page 46.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, Association for Computing Machinery, New York, NY, USA, v. 21, n. 2, p. 120–126, fev. 1978. ISSN 0001-0782. Disponível em: <https://doi.org/10.1145/359340.359342>. Cited on page 19.

SCARANI, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.*, American Physical Society, v. 81, p. 1301–1350, Sep 2009. Disponível em: <https://link.aps.org/doi/10.1103/RevModPhys.81.1301>. Cited 2 times on pages 51 and 53.

SHANNON, C. E. A mathematical theory of communication. *The Bell System Technical Journal*, v. 27, n. 3, p. 379–423, 1948. Cited 2 times on pages 20 and 33.

SHOR, P. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. [S.l.: s.n.], 1994. p. 124–134. Cited on page 19.

SINGH, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Knopf Doubleday Publishing Group, 2000. ISBN 9780385495325. Disponível em: <https://books.google.com.br/books?id=skt7TrLK5uYC>. Cited on page 19.

TOMAMICHEL, M.; COLBECK, R.; RENNER, R. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, v. 55, n. 12, p. 5840–5847, 2009. Cited 2 times on pages 37 and 38.

TOMAMICHEL, M. et al. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, v. 57, n. 8, p. 5524–5535, 2011. Cited on page 47.

VERNAM, G. S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, v. 45, n. 2, p. 109–115, 1926. Cited 2 times on pages 20 and 39.

WEI, Z. et al. Decoy-state quantum key distribution with biased basis choice. *Scientific Reports*, v. 3, n. 1, p. 2453, Aug 2013. ISSN 2045-2322. Disponível em: <https://doi.org/10.1038/srep02453>. Cited on page 56.

WILDE, M. M. *Quantum Information Theory*. [S.l.]: Cambridge University Press, 2013. Cited 4 times on pages 23, 28, 29, and 36.

WOLF, R. *Quantum key distribution: an introduction with exercises*. Cham: Springer, 2021. v. 988. 1 online resource (xi, 229 pages) : illustrations, diagrams p. (Lecture notes in physics, v. 988). ISBN 9783030739911. Disponível em: <https://bib-pubdb1.desy.de/record/470445>. Cited 4 times on pages 35, 54, 56, and 58.

WOOTTERS, W. K.; ZUREK, W. H. A single quantum cannot be cloned. *Nature*, v. 299, n. 5886, p. 802–803, Oct 1982. ISSN 1476-4687. Disponível em: <https://doi.org/10.1038/299802a0>. Cited on page 32.

ZHAO, Y. et al. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, American Physical Society, v. 78, p. 042333, Oct 2008. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevA.78.042333>. Cited on page 61.

ZHONG, X. et al. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.*, American Physical Society, v. 123, p. 100506, Sep 2019. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.123.100506>>. Cited 2 times on pages 73 and 74.

ZHONG, X. et al. Simple multiuser twin-field quantum key distribution network. *Phys. Rev. Appl.*, American Physical Society, v. 17, p. 014025, Jan 2022. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevApplied.17.014025>>. Cited 2 times on pages 73 and 74.

ZHONG, X. et al. Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses. *npj Quantum Information*, v. 7, n. 1, p. 8, Jan 2021. ISSN 2056-6387. Disponível em: <<https://doi.org/10.1038/s41534-020-00343-5>>. Cited 2 times on pages 73 and 74.

ZHOU, L. et al. Twin-field quantum key distribution without optical frequency dissemination. *Nature Communications*, v. 14, n. 1, p. 928, Feb 2023. ISSN 2041-1723. Disponível em: <<https://doi.org/10.1038/s41467-023-36573-2>>. Cited on page 71.