Quantum Secure Function Evaluations with Real-world Devices

by

Juliette van Mil

to obtain the degree of Master of Science in Applied Physics
at the Delft University of Technology,

Student number: 4775899
Project duration: October 1, 2024 – October 9, 2025
Thesis committee:

Prof. dr. S. Wehner,	QuTech, TU Delft, supervisor
Prof. dr. E. Greplova,	Kavli Institute, TU Delft
Dr. F. Ferreira da Silva,	TU Delft
Dr. K. Senthoor,	TU Delft, daily co-supervisor

TU Delft

Abstract

Cryptographic primitives such as Bit Commitment (BC) and Oblivious Transfer (OT) are foundational building blocks for two-party Secure Function Evaluations. While unconditional security for BC is impossible in the quantum setting, it can be realised under additional physical assumptions. In particular, the bounded- and noisy-storage models provide a framework where security is guaranteed against adversaries with limited quantum memory. Recent work by Ribeiro and Wehner [1] introduced the first Measurement-Device-Independent (MDI) protocols for BC and OT in the bounded storage model. For the BC protocols, they consider a variant of BC that is called Randomised String Commitment (RSC). They give two MDI-RSC protocols using polarisation-encoded photon sources: one with perfect single-photon emission and another with multi-photon emissions. They also give an MDI-OT protocol using sources with perfect single-photon emission. However, the MDI security for OT using sources with multi-photon emissions remains an open problem.

This thesis investigates the feasibility of MDI-RSC protocols using sources with multi-photon emissions, such as weak coherent pulses (WCP) and spontaneous parametric down-conversion (SPDC) sources. First, we correct a practical error in the existing MDI-RSC protocol by bounding the relevant parameters, ensuring the validity of the original security claims. Second, we analyse the achievable committed string rates while using WCP and SPDC sources. We further consider heralded SPDC sources, which in principle enable single-photon emission, and discuss the impact of imperfect local detectors on their performance and the consequences that has on the protocol implementation.

Finally, motivated by techniques from Twin-Field Quantum Key Distribution (TF-QKD), we give a phase-encoded MDI-RSC protocol using coherent states and provide a sketch of the security proof in the bounded-storage model. We also investigate extending the approach to OT. However, this is still a challenge due to the basis-dependent information leakage inherent in phase-encoded coherent states.

Preface

This thesis project concludes my Master's in Applied Physics at the TU Delft, and with that seven exciting, challenging and very valuable years of studying in Delft; starting from a double bachelor's in applied physics and mathematics, followed by a year at the Delft Hyperloop dreamteam, and ending with a double master's degree, concluding this thesis simultaneously with a Master's in Communication Design for Innovation. This research helped me develop on both a technical and personal level. On a technical level, I greatly expanded my conceptual understanding of quantum cryptographic protocols. I also improved my skills in writing mathematical proofs. On the personal level, this project gave me a lot of experience with planning a long and complex project and with the natural flow of scientific research, where things never go exactly as you planned them. I would like to thank Stephanie, for giving me the opportunity to do this thesis project and for providing me with sharp and valuable feedback when I needed it. I want to thank Kaushik for his daily supervision and support. I am very grateful for our frequent, pleasant and very helpful discussions. I also want to thank Prof. Eliška Greplová and Dr. Francisco Ferreira da Silva for being part of my thesis committee. Thanks also to Timothé, who has done his master thesis on a similar topic, for on occasions helping me out with the maths, but mostly for sharing our frustrations or interesting discussions regarding this topic. Thanks to everyone from the Wehner group for their support and the nice and safe working environment they built, especially Tzula, for the helpful discussions we had about quantum optics at the start of my project. Also thanks to my family for their patience and support over the past years. Lastly, I want to thank Jasper for his unwavering patience and support, always ready to listen, help, provide feedback and even proofread chapters for me on the train journey to your new full-time job.

Juliette van Mil
Delft, October 2025

Contents

1 Introduction

1.1. Context

Cryptography provides the foundation for secure communication and computation. We encounter it every day in secure online transactions, encrypted messaging apps and confidential data exchange. The emergence of quantum information has both challenged and extended classical cryptographic assumptions. In particular, Shor's algorithm illustrates that widely used hardness assumptions, such as factoring and discrete logarithms, are no longer secure in the presence of quantum computers [2]. This motivates the development of cryptographic protocols that are resistant to these quantum threats. One approach is to leverage the inherent properties of quantum mechanics to ensure security. This concept forms the basis of the field of quantum cryptography.

1.1.1. Secure function evaluations

The most well-known protocol of quantum cryptography is Quantum Key Distribution (QKD), which uses the fundamental principles of quantum mechanics to securely distribute a secret key between two trusted parties. QKD provides security that is guaranteed by the laws of physics, rather than computational assumptions. However, QKD is limited in scope. It enables secure key exchange, but it does not realise more general cryptographic tasks.

Two-party Secure Function Evaluation (SFE) protocols address a different problem. Instead of defending against an outside eavesdropper, they provide security when the two parties, Alice and Bob, themselves do not fully trust each other but still wish to jointly perform a cryptographic task. SFE allows the parties to compute a function of their private inputs while ensuring that no party learns more about the other's input than what can be inferred from the output of the function itself, see Figure 1.1. Two foundational examples of two-party SFE are Bit Commitment and Oblivious Transfer.

Figure 1.1: Schematic of a general two-party Secure Function Evaluation. At the start of the protocol Alice (left) has an input x and Bob (right) has an input y. At the end, Alice has $f_A(x,y)$ and Bob has $f_B(x,y)$. Alice does not know more about y than what $f_A(x,y)$ reveals and Bob does not know more about x than what $f_B(x,y)$ reveals.

Bit Commitment (BC) is a primitive in which one party, Alice, commits to a chosen bit while keeping it hidden from the other party, Bob. Later, Alice can "open" the commitment to reveal the bit, see Figure 1.2. The protocol must ensure both hiding (Bob cannot learn the bit before the opening) and binding (Alice cannot change the bit after committing).

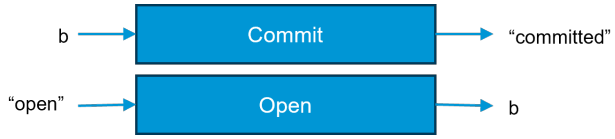

Figure 1.2: Schematic of Bit Commitment. In the Commit phase, Alice (left) commits a certain bit b to the protocol and this outputs a guarantee that she committed to Bob (right). In the Open phase, Alice gives the prompt to open her bit to Bob and the protocol output b to Bob.

An important variant of bit commitment that will be relevant later is Randomised String Commitment (RSC). In this primitive, Alice does not commit to an arbitrary string of her choice, but instead receives a random string from the protocol and commits to it. The security requirements mirror those of standard BC: the commitment must be hiding, so that Bob cannot learn anything about the string before the opening, and binding, so that Alice cannot change the string once she has committed. RSC is often easier to prove than BC, since it removes power from Alice by not letting her choose what she commits to. This means that the binding requirement reduces to binding given randomness.

1-out-of-2 Oblivious Transfer (OT) is a primitive where Alice has two messages, and Bob chooses one of them to receive, see Figure 1.3. The security of the protocol ensures that Bob learns only the message he selected, and Alice remains oblivious to which choice Bob made.

Figure 1.3: Schematic of 1-out-of-2 Oblivious Transfer. Alice (left) gives two messages s_0 and s_1 as input. Bob's (right) input is a choice $c \in \{0, 1\}$. The protocol outputs only the message of Bob's choice only to Bob.

OT and BC are central cryptographic primitives. OT is called universal, as any two-party SFE can be constructed from OT [3]. Furthermore, OT and BC are closely related: OT can be used to build BC, and conversely, BC can be used to build OT if quantum communication is available. In fact, with quantum communication, OT and BC are reducible to one another [4].

Nevertheless, neither OT nor BC is possible without restrictions on adversaries. The classical approach assumes computational hardness, which is vulnerable to quantum attacks such as Shor's algorithm. Similarly, unconditional approaches based on quantum mechanics, in analogy to QKD, fail for bit commitment: Mayers [5] and Lo and Chau [6, 7] prove that unconditionally secure quantum BC is impossible. This motivates alternative models that impose physical limits on adversaries, such as constraints on their ability to store quantum information.

1.1.2. Bounded storage model

The bounded-storage model offers a future-proof alternative. This model assumes that the adversary has access to a quantum memory, but can store only a limited number of qubits. Its key advantage is that security remains valid even if the adversary later gains improved storage capabilities, since the assumptions need only hold during the protocol execution. A generalisation, the noisy-storage model, links security to the imperfections of the adversary's memory, such as its classical capacity, entanglement cost, or quantum capacity. These settings provide everlasting security and do not require honest parties to have quantum memory themselves. Protocols developed under these models have established secure OT and BC, demonstrating the practical relevance of storage-based assumptions. Damgård et al. [8] show that two-party cryptographic primitives such as OT and BC can be securely implemented against adversaries with bounded quantum memory. Wehner et al. [9] provide practical security guidelines for implementing these protocols in the noisy-storage model, analysing real-world imperfections and proposing decoy-state modifications with explicit security pa-

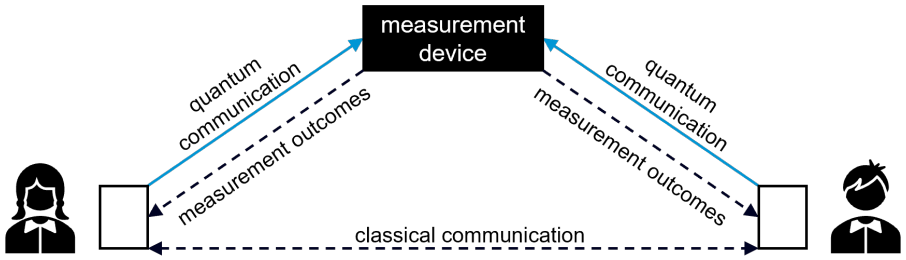

Figure 1.4: Schematic of a Measurement Device Independent setup with Alice on the left, Bob on the right and a central measurement station.

rameters. König, Wehner, and Wullschleger [10] additionally prove security against general attacks under realistic noise levels and show that these protocols can be implemented with current quantum key distribution technology without requiring quantum storage for honest parties. Ng et al. [11] demonstrate the practical feasibility of bit commitment in the noisy-storage model by experimentally implementing the protocol with entangled photons, providing a full security analysis under realistic errors and finite-size effects.

1.1.3. Measurement device independence

While storage-based models are powerful, they assume that devices behave as intended. In practice, adversaries can exploit device imperfections, for example by tampering with measurement devices. To address this, the device-independent (DI) framework can be used to enable two-party protocols that remain secure even when the quantum devices (both sources and measurement devices) are compromised [12]. A more practical relaxation is measurement-device independence (MDI), in which security is maintained even when measurement devices are untrusted [13]. A schematic of an MDI protocol is given in Figure 1.4. MDI assumes that Alice and Bob can fully trust and characterise their own devices, but that the central measurement device is fully controlled by the adversary.

Within MDI, two frameworks are typically considered: one with ideal sources and another with imperfect, realistic sources. Practical implementations must deal with imperfections such as weak coherent pulses that exhibit multi-photon emissions, in contrast to ideal single-photon sources. Bridging this gap between theory and experiment is crucial. This, in combination with the fact that MDI has been extensively studied in QKD but less so in the context of bit commitment, motivates the study of MDI-RSC under realistic conditions. We do this based on the work of Ribeiro and Wehner [1], who introduce the first MDI protocols for RSC and Random 1-out-of-2 OT. They prove the security of these protocols in the bounded quantum storage model with perfect photon sources and show that with imperfect sources BC remains possible, while secure OT is significantly harder. This is because the imperfect sources allow unavoidable multi-photon emissions, which leak information that a dishonest party can exploit. For OT, this means that security is no longer possible in the class of protocols studied by [1].

1.1.4. Twin-Field QKD

Twin-field quantum key distribution (TF-QKD) is a family of protocols that achieves secure key exchange at distances far beyond the fundamental rate-distance limit (the repeaterless bound) of traditional QKD schemes [14]. The central idea is that Alice and Bob each send weak quantum signals to a central measurement station, where interference between the two ”twin” fields enables the extraction of secret key information without requiring either party to send strong pulses directly over long distances.

TF-QKD possesses several interesting features. It overcomes the linear secret key rate scaling with channel transmittance, while at the same time remaining compatible with existing optical fiber infrastructure, and the protocols are MDI. We discuss TF-QKD here because it relies on a similar paradigm as the quantum SFE protocols studied in this work: both use a central node to perform interference-based measurements, while maintaining security even if this node is not trusted. TF-QKD illustrates how carefully designed protocols can enable strong cryptographic tasks under realistic assumptions, and it motivates our exploration of related techniques in the context of quantum SFE.

1.2. Research goals

This thesis focuses on protocols for MDI-RSC by Ribeiro and Wehner [1]. The goals of this work are:

1. To investigate the feasibility and security of MDI-RSC protocols implemented with realistic physical sources, such as weak coherent pulses (WCP) and spontaneous parametric down-conversion (SPDC) sources, by analysing the achievable committed string rates for different ranges of physical parameters.
2. To study the effect of heralding the idler photon in SPDC sources on protocol performance.
3. To explore the possibility of designing MDI-RSC protocols motivated from TF-QKD, specifically using phase-based encoding in weak coherent pulses.

1.3. Thesis outline

In Chapter 2, we present notation, mathematical and quantum preliminaries, and details of the physical sources, including photon number distributions. Chapter 3 reviews related work and introduces introduces the two MDI-RSC protocols from [1]. The first contribution of this thesis, described in Section 3.4, corrects a practical error in the existing protocols by bounding the relevant parameters, thereby maintaining security claims. In Chapter 4, we analyse the achievable committed string rates for the protocols introduced in Chapter 3, using the source models described in Chapter 2. In Chapter 5, we explore the potential for MDI-RSC protocols in the framework of TF-QKD. We focus on its characteristic phase-based encoding and propose a phase-encoded MDI-RSC protocol and give a sketch of its security proof. Our security proof of Alice still needs some improvement. We also find that the problem of extending this approach to an MDI-OT protocol, that [1] encountered, still exists for implementation with phase-based encoding. Finally in Chapter 6, we conclude this work and give recommendations for further research.

2

Background

2.1. Mathematical tools

We start with some general notations and definions. Given $\epsilon > 0$, we denote by $\log(\epsilon)$ the binary logarithm

$$\log(\epsilon) := \log_2(\epsilon) = \frac{\ln(\epsilon)}{\ln(2)}. \tag{2.1}$$

For a given set K, we write $k \in_R K$ if the random variable k is sampled uniformly at random from K, where a uniform distribution on a finite set K assigns equal probability $1/|K|$ to each element $k \in K$.

For a positive integer $N \geq 1$, we denote $[N] := \{1, 2, \ldots, N\}$.

The $n \times n$ identity matrix is denoted as $\mathbb{1}_n$.

States and Operators

We denote quantum states with the Greek letters ρ, σ, τ and use the bra-ket notation to denote pure states: $|\Psi\rangle$. The quantum protocols in this work also use classical information, which can be represented within the quantum formalism.

Definition 2.1.1. A register Y consisting of $m \in \mathbb{N}$ classical bits is described by a probability distribution $\{p_Y(y), y \in \{0,1\}^m\}$, where $p_Y(y)$ is the probability that the register contains the string y. In the bra–ket notation, the associated density matrix is

$$\rho_Y = \sum_{y \in \{0,1\}^m} p_Y(y) \, |y\rangle \langle y| \, . \tag{2.2}$$

Thus, a classical state can be fully specified either by its probability distribution or by its diagonal density matrix in the computational basis.

Definition 2.1.2. If Y is a classical register as above and Q is a quantum register, we define a classical–quantum (cq) state on YQ by

$$\rho_{YQ} = \sum_{y \in \{0,1\}^m} p_Y(y) \, |y\rangle\langle y| \otimes \rho_Q^y, \tag{2.3}$$

where ρ_Q^y is the quantum state of Q conditioned on $Y = y$. In this way, the register Y behaves classically, while Q can be in a general quantum state.

A classical register Y of size m is uniformly distributed if $p_Y(y) = 2^{-m}$ for all $y \in \{0,1\}^m$. The corresponding density matrix is the maximally mixed state

$$\tau_Y := \frac{1}{2^m} \sum_{y \in \{0,1\}^m} |y\rangle\langle y|. \tag{2.4}$$

An $n \times n$ complex valued matrix M is Hermitian if $M = M^\dagger$, where $M^\dagger = (M^\top)^*$ is the conjugate transpose of M. We describe quantum measurements as Positive Operator Valued Measures (POVMs) on a d-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^{\mathsf{d}}$. A POVM is a finite collection of positive semidefinite operators $\{M_x\}_{x\in\mathcal{X}}$ satisfying $\sum_x M_x = \mathbb{1}_d$, where $\mathcal{X}$ is a finite set of indices.

Definition 2.1.3. The trace norm of an operator M is defined as

$$\|M\|_1 := \mathsf{Tr}\sqrt{M^\dagger M}. \tag{2.5}$$

Definition 2.1.4. The trace distance between two quantum states ρ, σ is

$$\frac{1}{2}\|\rho - \sigma\|_1. \tag{2.6}$$

We say that ρ and σ are ϵ-close, denoted $\rho \approx_\epsilon \sigma$, if

$$\frac{1}{2}\|\rho - \sigma\|_1 \leq \epsilon. \tag{2.7}$$

Information-theoretic Tools

A family $\mathcal{R}$ of functions $h : \{0,1\}^n \to \{0,1\}^\ell$ is called 2-universal if, for all $x \neq x'$,

$$\Pr_{h\in_R\mathcal{R}}[h(x) = h(x')] \leq 2^{-\ell}. \tag{2.8}$$

Let $\mathsf{Ext}\colon \{0,1\}^n \times \mathcal{R} \to \{0,1\}^\ell$ be a randomness extractor from the 2-universal family of functions, where $\mathcal{R}$ is a family of 2-universal hash functions. It extracts nearly uniform random bits from a source that may be biased or weakly random, using an auxiliary random seed $r \in_R \mathcal{R}$. The input source needs, however, to have enough min-entropy.

Definition 2.1.5. The conditional min-entropy of X given a quantum system Q for a cq-state ρ_{XQ} is defined as

$$H_{\min}(X|Q)_\rho = -\log(P_{\mathsf{guess}}(X|Q)), \tag{2.9}$$

where P_{guess} is the maximum probability to guess X correctly given all information in Q.

We see from this definition that for a high conditional min-entropy, the system Q gives little information about X. The smooth conditional min-entropy $H^\epsilon_{\min}(X|Q)_\rho$ is obtained by maximizing $H_{\min}(X|Q)$ over all states ρ' that are ϵ-close to ρ. A useful property of the smooth min-entropy is a chain rule.

Lemma 2.1.1 (Chain Rule for min-entropy [10])**.** *For any classical-classical-quantum (ccq)-state ρ_{XYQ},*

$$H^\epsilon_{\min}(X|YQ)_\rho \geq H^\epsilon_{\min}(X|Q)_\rho - \log|\mathcal{Y}|, \tag{2.10}$$

where $|\mathcal{Y}|$ is the size of the support of Y, and

$$H^\epsilon_{\min}(X|YQ)_\rho \geq H^\epsilon_{\min}(X|Y)_\rho - \log\dim(Q), \tag{2.11}$$

where $\dim(Q)$ is the dimension of Q.

We will use this chain rule and the following lemma when we prove the security for Alice in Section 5.3.

Lemma 2.1.2 (Leftover Hash Lemma with min-entropy (adapted from [15, Corollary 5.6.1] and [10, Theorem II.3]))**.** *Let ρ_{XQ} be a cq-state, where X is an n-bit string, and let* $\mathsf{Ext} : \{0,1\}^n \times \mathcal{R} \to \{0,1\}^\ell$ *be an extractor based on a 2-universal family $\mathcal{R}$, that maps the classical n-bit string X into C. Then,*

$$\rho_{CRQ} \approx_{\epsilon'} \tau_{\{0,1\}^\ell} \otimes \rho_{RQ}, \tag{2.12}$$

where

$$\epsilon' = 2\epsilon + 2^{-\frac{1}{2}(H^\epsilon_{\min}(X^n|Q)-\ell)}. \tag{2.13}$$

In the MDI-RSC protocols that we present in this work, we use random linear codes to ensure that certain strings have a minimum Hamming distance. For this, we use the following lemma.

Lemma 2.1.3 (Distance of a randomly generated code [1])**.** *For a randomly generated* $[n, k, d]$ *binary linear code* C*, the minimum distance* d *satisfies*

$$\Pr[d \leq \delta n] \leq 2^{(k/n-(1-h(\delta)))n}, \quad 0 \leq \delta \leq 1, \tag{2.14}$$

where $h(x) := -x\log(x)-(1-x)\log(1-x)$ *is the binary entropy function, and the probability is taken uniformly over all codes with fixed* k *and* n*.*

Statistical Tools

Since the protocols in this work are defined in the finite regime, we need to deal with statistical fluctuations when we sample from sets with a certain probability p_x^y. Therefore, we introduce fluctuation parameters ζ_x^y associated with probabilities p_x^y. These allow us to bound deviations from expected values with high confidence using Hoeffding's inequality.

Lemma 2.1.4 (Hoeffding's Inequality [16])**.** *Let* $X_1, \ldots, X_n$ *be i.i.d. random variables with* $X_j \in \{0, 1\}$*, and let* $S_n = \sum_{i=1}^n X_i$*. Then, for* $\zeta = \sqrt{\frac{\ln(1/\epsilon)}{2n}}$*,*

$$\Pr(S_n \geq \mathbb{E}(S_n) + n\zeta) \leq \epsilon, \tag{2.15}$$
$$\Pr(S_n \leq \mathbb{E}(S_n) - n\zeta) \leq \epsilon, \tag{2.16}$$
$$\Pr(|S_n - \mathbb{E}(S_n)| \geq n\zeta) \leq 2\epsilon. \tag{2.17}$$

As an example, consider bounding the number of single-photon emissions over N rounds, where the emission probability is p^1_{src}. The expected number is $p^1_{\mathsf{src}}N$. With fluctuation parameter $\zeta^1_{\mathsf{src}} = \sqrt{\frac{\ln(1/\epsilon)}{2N}}$, we obtain

$$\Pr\left[\, |S - p^1_{\mathsf{src}}N| \geq \zeta^1_{\mathsf{src}}N \,\right] \leq 2\epsilon, \tag{2.18}$$

so that, except with probability 2ϵ, the number of emissions lies in

$$[(p^1_{\mathsf{src}} - \zeta^1_{\mathsf{src}})N,\ (p^1_{\mathsf{src}} + \zeta^1_{\mathsf{src}})N]. \tag{2.19}$$

We will frequently use this argument and denote such intervals by ζ_x^y.

2.2. Quantum physics preliminaries

In this section, we briefly review the basic quantum states and measurements that are relevant to the protocols discussed in this work. We describe the types of states that Alice and Bob prepare, the measurements performed at the central station, and the role of the decoy-state technique.

The computational basis of a qubit is given by $\{|0\rangle, |1\rangle\}$. Another important basis is the Hadamard (or diagonal) basis, defined as $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, so that the basis states are $\{|+\rangle, |-\rangle\}$.

The four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ are known as the BB84 states. They form the signal states of the BB84 quantum key distribution protocol and will also serve as the basic states in the protocols studied here.

Photon states in a single optical mode are described in the Fock basis $\{|n\rangle\}_{n=0}^{\infty}$, where $|n\rangle$ represents a number state containing exactly n photons.

Unless otherwise stated, the central measurement node in the measurement-device-independent (MDI) protocols we consider performs a probabilistic Bell state measurement (BSM). A BSM projects two incoming qubits onto maximally entangled Bell states, $X^a Z^b \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $(a, b) \in \{0, 1\}^2$, where X and Z denote the Pauli X and Z operators. Using only linear optics, however, one can reliably distinguish only a subset of these states [1]. The measurement station has two threshold detectors that click in the presence of a photon. These click patterns are the outcome of the measurement station. Outcomes that do not correspond with operators that are projections onto maximally entangled states are failure outcomes. These also include the events where it could be detected that the photons were lost before reaching the measurement device.

2.2.1. Multi-photon emissions

In a realistic setup, Alice and Bob do not have access to perfect single-photon sources. Pulses may contain instead zero, one or multiple photons. These multi-photon emissions endanger the security of the protocol, as they are vulnerable to attacks like photon number splitting, where a dishonest party could do projective measurements to determine the basis of the photon emission. A malicious player can then announce all of the single-photon emissions as lost and only keep the rounds where they have information about the bases. The decoy state method mitigates this vulnerability by allowing the parties to estimate the behaviour of the quantum channel (in terms of losses) for pulses of different photon numbers. This technique makes it possible to estimate an upper bound to the number of rounds that are kept and correspond to multi-photon emissions. Honest parties can then better control that the most rounds that are kept at the end correspond to single-photon emissions.

2.2.2. Decoy state technique

With the decoy state technique, Alice and Bob will randomly choose a setting of their photon source according to some probability distribution. Here we give the decoy state technique as described by Ribeiro and Wehner [1]. One of the settings is the signal setting, which will post-selectively be used for the protocol (a_s for Alice and b_s for Bob). The other settings are decoy settings, used to test the honesty of the other party. These are drawn from the set $\{a_{d1}, \ldots, a_{dq}\}$ and $\{b_{d1}, \ldots, b_{dq}\}$, respectively. We will use p_a (p_b) to denote the probability that Alice (Bob) prepares a signal with intensity $a \in \{a_s, a_{d1}, \ldots, a_{dq}\}$ ($b \in \{b_s, b_{d1}, \ldots, b_{dq}\}$). The probability that an emitter produces k photons will be written as p_k (e.g., for $k = 1$, we write p_1, etc.). Similarly, the probability that an emitter produces more than k photons will be denoted as $p_{\geq k}$. Furthermore, we will combine these notations for conditional events. For instance, the probability that Alice emits 1 photon given that she chooses a signal intensity a_s will be represented as $p_{1|a_s}$.

Let N be the total number of quantum communication rounds, let n_k^H be the number of quantum communication rounds in which party H's source ($H \in \{\text{A, B}\}$) has produced k photons, while using their signal setting, and in which the measurement station announced a successful measurement. Note that Alice and Bob can only know the quantities $n_1^A + n_{\geq 2}^A$ and $n_1^B + n_{\geq 2}^B$ from the announcements of the measurement station, but cannot individually distinguish n_1^A, n_1^B and $n_{\geq 2}^A, n_{\geq 2}^B$. However, using the decoy states, Alice (Bob) can estimate a lower bound L_{A1} (L_{B1}) on n_1^A (n_1^B) by estimating the yield of single-photon pulses, denoted as Y_1.

For a given intensity setting i, the total detection probability Q_i is:

$$Q_i = \sum_{k=0}^{\infty} p_{k|i} Y_k, \tag{2.20}$$

where $p_{k|i}$ is the probability of emitting k-photon pulses, Y_k is the yield for k-photon pulses. By comparing the detection probabilities Q_i for the signal state and various decoy states, the Alice (Bob) solves a system of equations to isolate Y_1, the yield for single-photon pulses [9]. Once Y_1 is estimated, the lower bound on the number of single-photon emissions in the rounds using the signal state is given by:

$$n_1^H = p_{1|i} Y_1 (n_1^H + n_{\geq 2}^H), \tag{2.21}$$

where $n_1^H + n_{\geq 2}^H$ is the total number of pulses sent by a honest party H using the signal setting.

2.3. Sources

In this section, we introduce two types of realistic quantum sources, which we will use to evaluate the MDI-RSC protocols in Chapter 4.

Phase-randomised Weak Coherent Pulses

A coherent state is a quantum state of light that most closely resembles classical light, for example, light from a laser. Coherent states can be written in the Fock basis of number states as follows:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle , \tag{2.22}$$

where α is a complex number, $|\alpha|^2$ is the intensity or the mean photon number and the phase $\arg(\alpha)$ represents the phase of the electromagnetic wave. $|n\rangle$ is the photon number state. In a weak coherent pulse source the

intensity is low, meaning that the mean photon number per pulse is also small. This allows for a probabilistic generation of single photons, that are useful in quantum cryptographic applications. For a weak coherent pulse source with low intensity, most pulses contain no photons, some are single photon pulses and very few contain more than one photon.

In the phase randomised version of a weak coherent pulse with $\alpha = |\alpha|e^{i\phi}$, the phase ϕ is chosen uniformly at random in $[0, 2\pi)$. When the phase of the state is not known, this state is equivalent to a mixed state and is represented as a statistical mixture of Fock (number) states

$$\rho = \sum_{n=0}^{\infty} p_{\text{WCP}}(n, \mu)|n\rangle\langle n|. \tag{2.23}$$

Here, $p_{\text{WCP}}(n, \mu)$ is the probability of having n photons per pulse, which follows a Poisson distribution

$$p_{\text{WCP}}(n, \mu) = \frac{\mu^n e^{-\mu}}{n!}, \tag{2.24}$$

where $\mu = |\alpha|^2$ is the average photon number (intensity) of the pulse.

Phase randomisation ensures that the state is diagonal in the photon number basis, removing phase coherence between different Fock states. This simplifies the analysis of security by reducing the state to a classical mixture of Fock states with a known photon number distribution. A dishonest party, in principle, gains no additional advantage by attempting to exploit coherence between different photon number states because the phase randomisation destroys such coherence. The best strategy for an adversary is then to perform a quantum non-demolition measurement of the photon number so as to not cause a disturbance. We can assume that a dishonest party will do this attack without loss of generality. This also simplifies the security analysis, as we can analyse single-photon emissions separately from multi-photon emissions [9].

Spontaneous Parametric Down Conversion

Spontaneous parametric down-conversion (SPDC) is a non-linear optical process used to generate entangled photon pairs. It occurs when a high-energy *pump* photon passes through a non-linear optical medium and spontaneously splits into two lower-energy photons: the *signal* and the *idler*. In the type of SPDC that we consider in this work, the signal and idler photons have orthogonal polarisations and emerge in an entangled state. A detailed derivation of the probability of having n photons per pulse for a SPDC source is given in Appendix A. The final statement is (as in Wehner et al. [9]):

$$p_{\text{PDC}}(n, \mu) = \frac{(n+1)(\mu/2)^n}{(1+\mu/2)^{n+2}} \tag{2.25}$$

where μ is the intensity of the pulse, which includes both the signal and idler beam.

2.3.1. Central measurement for an MDI setup

In the phase-encoded MDI setup that is used in Chapter 5, Alice and Bob have identical setups that send coherent states to a central node, which consists of a 50:50 beamsplitter (BS) with threshold detectors at its two output modes. In this section we give description of how coherent states move through a 50:50 beamsplitter and how they are measured in threshold detectors.

An ideal threshold detector clicks if it detects one or more photons, but does not resolve how many photons there were. The probability of there being no photons in coherent state $|\beta\rangle$ is $p(0) = e^{-|\beta|^2}$. Thus the probability that an ideal threshold detector clicks in the presence of the coherent state is

$$p_{\text{click}} = 1 - p(0) = 1 - e^{-|\beta|^2} \tag{2.26}$$

Now, we look at how coherent states move through a 50:50 beamsplitter. A detailed description of the beamsplitter transformations of single photon states and coherent states is given in Appendix B. First note that coherent states $|\alpha\rangle$ are defined as the eigenstates of the annihilation operator,

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.27}$$

We will analyse what happens when we input two arbitrary coherent states, by using the beamsplitters transformation on the annihilation operators. With the transformation of the creation operators given in Equation (B.2), the output annihilation operators are given by

$$\hat{a}_{\text{out}} = \tfrac{1}{\sqrt{2}}(\hat{a}_{\text{in}} + \hat{b}_{\text{in}}), \quad \hat{b}_{\text{out}} = \tfrac{1}{\sqrt{2}}(-\hat{a}_{\text{in}} + \hat{b}_{\text{in}}). \tag{2.28}$$

First consider putting two coherent states with the same amplitude and phase

$$|\Psi_{\text{in}}\rangle = |\alpha e^{i\theta}\rangle_a \otimes |\alpha e^{i\theta}\rangle_b . \tag{2.29}$$

Since coherent states are eigenstates of the annihilation operator, we have

$$\hat{a}_{\text{in}} |\alpha e^{i\theta}\rangle_a = \alpha e^{i\theta} |\alpha e^{i\theta}\rangle_a , \quad \hat{b}_{\text{in}} |\alpha e^{i\theta}\rangle_b = \alpha e^{i\theta} |\alpha e^{i\theta}\rangle_b , \tag{2.30}$$

To find the eigenvalues of the output modes, we use linearity of the transformation to write

$$\hat{a}_{\text{out}} |\Psi_{\text{in}}\rangle = \tfrac{1}{\sqrt{2}}(\hat{a}_{\text{in}} + \hat{b}_{\text{in}}) |\alpha e^{i\theta}\rangle_a \otimes |\alpha e^{i\theta}\rangle_b = \tfrac{1}{\sqrt{2}}(\alpha e^{i\theta} + \alpha e^{i\theta}) |\Psi_{\text{in}}\rangle = \sqrt{2}\alpha e^{i\theta} |\Psi_{\text{in}}\rangle . \tag{2.31}$$

Thus the state in output mode a becomes a coherent state with eigenvalue $\sqrt{2}\alpha e^{i\theta}$.

$$\hat{b}_{\text{out}} |\Psi_{\text{in}}\rangle = \tfrac{1}{\sqrt{2}}(-\hat{a}_{\text{in}} + \hat{b}_{\text{in}}) |\alpha e^{i\theta}\rangle_a \otimes |\alpha e^{i\theta}\rangle_b = \tfrac{1}{\sqrt{2}}(-\alpha e^{i\theta} + \alpha e^{i\theta}) |\Psi_{\text{in}}\rangle = 0. \tag{2.32}$$

So mode b ends up in the vacuum state. Since coherent states are uniquely determined by their eigenvalues, the output state is

$$|\Psi_{\text{out}}\rangle = |\sqrt{2}\alpha e^{i\theta}\rangle_a \otimes |0\rangle_b . \tag{2.33}$$

Now we consider two different coherent states in the input modes:

$$|\Psi_{\text{in}}\rangle = |\alpha e^{i\theta_a}\rangle_a \otimes |\beta e^{i\theta_b}\rangle_b . \tag{2.34}$$

We can simply use the same transformations of the annihilation operators given in Equation (2.28) and the fact that coherent states are eigenstates of the annihilation operators to write

$$|\Psi_{\text{out}}\rangle = |\tfrac{1}{\sqrt{2}}(\alpha e^{i\theta_a} + \beta e^{i\theta_b})\rangle_a \otimes |\tfrac{1}{\sqrt{2}}(-\alpha e^{i\theta_a} + \beta e^{i\theta_b})\rangle_b . \tag{2.35}$$

Thus we conclude that, when Alice and Bob send coherent states to the central node, this results in a deterministic click in output mode a when their states have the same amplitude and phase, and in a deterministic click in output mode b when their states have the same amplitude and a phase difference of $\Delta\theta = \pi$. For all other coherent input states, the click pattern of the output detectors is determined by some probability distribution that depends on the input states.

3

MDI Randomised String Commitment for multi-photon emissions

In this chapter, we describe the two protocols for MDI-RSC by Ribeiro and Wehner [1, Protocol II.1] and [1, Protocol II.3], on which this work is based, and their security proofs in Section 3.2 and Section 3.3. In Section 3.4 we remove a circularity error in some of the parameters of [1, Protocol II.3], which is the first contribution this work makes.

3.1. Randomised String Commitment

Randomised String Commitment is a generalisation of BC, since Alice does not commit only one bit b, but a whole string C. However, since the string is randomised, she cannot choose her string. The string will be produced uniformly at random by the protocol. The protocols for RSC that we show in this work consist of 3 phases: Preparation, Commit and Open.

In the Preparation phase, Alice and Bob do their quantum communication. Afterwards they each hold an n-bit string: Alice has X, and Bob has $\hat{X}$, which matches Alice's string in roughly half of the positions. Bob knows which positions match, but Alice does not. In the Commit phase, Alice creates a commitment to her string by applying a randomness extractor, which produces a shorter, nearly uniform random output C. This commitment hides almost all information about her original string, so that Bob cannot learn anything useful about it before Alice decides to reveal. To allow later verification, Alice sends Bob a different piece of auxiliary information derived from her string X. In the Open phase, Alice reveals her original string X. Bob can check that it matches what Alice committed to, using the auxiliary information she sent him and the positions he knows from $\hat{X}$ to confirm that Alice could not have changed her mind about the commitment. When he accepts he can recompute the commitment C on his own to complete the protocol.

We give an informal definition of RSC below. The formal definition can be found in Appendix C.

Definition 3.1.1 (Randomised String Commitment (informal, from [1, Definition II.1]))**.** A protocol implements an (ℓ, ϵ)-Randomised String Commitment if it satisfies the following three conditions.

Correctness: If both Alice an Bob are honest, the protocol outputs a classical state ρ_{CCF} such that ρ_{CF} is ϵ-close to $\tau_C \otimes |\textit{accept}\rangle\langle\textit{accept}|_F$, where $\tau_C := \frac{\mathbb{1}}{2^\ell}$ is maximally mixed and C is an ℓ-bit string.

Security for Alice: If Alice is honest, then after the Commit phase and before the Open phase Bob is "ϵ-ignorant" about the string C that Alice has received during the Commit phase. This property is called ϵ-hiding.

Security for Bob: If Bob is honest, then there exists a string C after the Commit phase, such that the probability that Alice opens to another string $C' \neq C$ and Bob accepts is smaller than ϵ. This property is called ϵ-binding.

3.2. MDI-RSC with perfect sources

In this section we present [1, Protocol II.1] that implements MDI-RSC for ideal single photon sources. First we define the following parameters, according to [17],

$$\zeta := \sqrt{\frac{\ln \epsilon^{-1}}{2n}}, \tag{3.1}$$

$$\zeta_{\mathcal{I}} := \sqrt{\frac{\ln \epsilon^{-1}}{2(\frac{1}{2}-\zeta)n}}, \tag{3.2}$$

$$\lambda := f\left(-\frac{D}{n}\right) - \frac{1}{n} - \frac{\log\left(\frac{2}{\epsilon^2}\right)}{n}, \tag{3.3}$$

$$\delta := 2p_{\text{err}} + 4\zeta_{\mathcal{I}} \tag{3.4}$$

where $0 < \epsilon < 1$ is a security parameter, n is the length of Alice's string, p_{err} is the expected bit-flip error probability on the quantum communication channel. Let Q be Bob's quantum register, then D is such that $\log \dim(Q) \leq D$, and $f(\cdot)$ is the following function.

$$f(x) := \begin{cases} 0 & \text{if } x < -1 \\ g^{-1}(x) & \text{if } -1 \leq x < \frac{1}{2} \\ x & \text{if } \frac{1}{2} \leq x \leq 1, \end{cases} \tag{3.5}$$

where $g(x) := h(x) + x - 1$ and $h(x) := -x\log(x) - (1-x)\log(1-x)$ is the binary entropy for all $x \in (0,1)$. A plot of the function f is given in Figure 3.1.

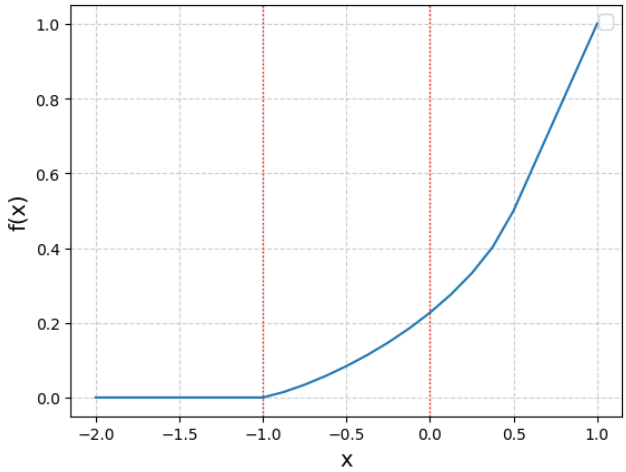

Figure 3.1: Plot of function f given in Equation (3.5). The part in between the dotted lines is the part of the function that is relevant for the input $x = -D/n$ when $n \in \{D, kD\}$, for $k > 0$.

We will further use a randomly generated binary $[n, k, d]$-linear code $\mathsf{C} \subseteq \{0,1\}^n$ with a fixed rate $\frac{k}{n}$. The use of this code requires that two strings with the same syndrome have Hamming distance at least d. We denote the function that outputs the parity-check syndrome of C, by $\text{Syn} : \{0,1\}^n \mapsto \{0,1\}^{n-k}$. We further take k to be the largest integer such that

$$\frac{k}{n} \leq 1 - h(\delta) + \frac{\log(\epsilon)}{n}. \tag{3.6}$$

We give below the MDI-RSC protocol [1, Protocol II.1]. The security proof for this protocol can be found in [1, Theorem IV.6].

Protocol 3.2.1 (Randomised String Commitment [1, Protocol II.1])**.** *Alice and Bob agree on the input parameters ϵ, the length of the committed string ℓ, D and p_{err}. Then they do the following steps.*

Preparation phase:

1. *Alice and Bob agree on a number N of rounds satisfying*

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n^*, \tag{3.7}$$

where p is the probability that a round j is not discarded if both parties are honest and n^* is the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}, \tag{3.8}$$

where λ and δ are in Equations (3.3) *and* (3.4)*.*

2. *For each round $j \in [N]$:*
   - *Alice chooses $X_j \in_R \{0,1\}$ and $\Theta_j \in_R \{0,1\}$, prepares and sends $|X_j\rangle_{\Theta_j}$ to the measurement station.*
   - *Bob chooses $\hat{X}_j \in_R \{0,1\}$ and $\hat{\Theta}_j \in_R \{0,1\}$, prepares and sends $|\hat{X}_j\rangle_{\hat{\Theta}_j}$ to the measurement station.*
   - *The measurement station performs a probabilistic Bell measurement on the two states it receives and broadcasts if the outcome is of type 0 or 1, or whether the measurement failed. If the outcome is of type 1, Bob flips his bit.*
3. *Alice and Bob discard all rounds with failure outcomes. Let n be the number of remaining rounds. Alice has strings X and $\Theta \in \{0,1\}^n$ and Bob has strings $\hat{X}$ and $\hat{\Theta} \in \{0,1\}^n$.*
4. *Both parties wait for a time Δt.*
5. *Alice sends Θ to Bob.*
6. *Bob computes the set of indices $\mathcal{I} := \{j \in [n] : \Theta_j = \hat{\Theta}_j\}$. He discards all the rounds $j \notin \mathcal{I}$. We call $\hat{X}_{\mathcal{I}}$ the string that is formed by the remaining bits $\hat{X}_j$ with $j \in \mathcal{I}$.*

Commit phase:

1. *Bob checks if $m := |\mathcal{I}| \geq \frac{n}{2} - n\zeta$. If not, he aborts.*
2. *Alice chooses a random $[n,k,d]$-linear code* C *(for fixed n and k) and computes the syndrome of X given by $w := \mathsf{Syn}(X)$ and sends it to Bob.*
3. *Alice picks a random 2-universal hash function r from a family of hash functions $\mathcal{R}$ and sends it to Bob.*
4. *Alice outputs $C := \mathsf{Ext}(X, r)$ where $\mathsf{Ext}(\cdot,\cdot)$ is a randomness extractor from the 2-universal family of functions.*

Open phase:

1. *Alice sends X to Bob.*
2. *Bob computes its syndrome and checks if it agrees with w he received from Alice in the Commit phase. If they disagree Bob aborts.*
3. *Bob checks that the fraction of rounds $j \in \mathcal{I}$ where X and $\hat{X}_{\mathcal{I}}$ do not agree lies in the interval $(p_{err} - \zeta_{\mathcal{I}}, p_{err} + \zeta_{\mathcal{I}})$. If not, Bob aborts the protocol, otherwise he accepts and outputs $C = \mathsf{Ext}(X, r)$.*

If the protocol aborts, the honest parties proceed as if it did not, but at the end:

- *Honest Bob rejects the commitment and outputs a uniformly random value $\tilde{C}$*
- *Honest Alice outputs a uniformly random value for C*

3.3. MDI-RSC with imperfect sources

In this section, we present the protocol and security proof of a protocol for MDI-RSC with decoy states, given in [1, Protocol II.3] and corrected by the author and Bramas [17]. Together we also gave some parameters a different symbol. Table 3.1 gives an overview of the differences between our notation and Ribeiro's notation.

Ribeiro's notation	e_{err}	α_1	α_2	α_1''	α_1'	α_3	β^A, β^B	α_4^A, α_4^B
Our notation	p_{err}	ζ	$\zeta_{\mathcal{I}}$	$\zeta_{\bar{\Gamma}}$	$\zeta_{\bar{\mathcal{I}}}$	$\zeta_{\mathcal{I}\cap\bar{\Gamma}}$	ζ^A, ζ^B	α^A, α^B

Table 3.1: Summary of our notations compared to [1].

For this protocol, Alice and Bob use imperfect single photon sources with a quality parameter $\gamma \in [0, \frac{1}{2})$, which is the probability that the sources emit two or more photons, given that at least one was emitted. Alice and Bob use decoy states to deal with multi-photon states, as described in Section 2.2.1. Let N be total number of quantum communication rounds of protocol 3.3.1, let n_H^k be the number of these rounds in which party H's source ($H \in \{\text{Alice, Bob}\}$) has produced k photons and in which the measurement station has clicked, and let n is the length of Alice's string that is kept in the preparation of the protocol. Besides Equation (3.1) and Equation (3.2) we define the following parameters.

$$\zeta_{\bar{\Gamma}} = \sqrt{\frac{\ln \epsilon^{-1}}{2(1-\gamma-\alpha^B)n}}, \tag{3.9}$$

$$\zeta_{\bar{\mathcal{I}}} = \min\left[\tfrac{1}{2}; \frac{\zeta + (1-\gamma-\alpha^B)\zeta_{\bar{\Gamma}}}{\gamma+\alpha^B}\right], \tag{3.10}$$

$$\zeta_{\mathcal{I}\cap\bar{\Gamma}} = \sqrt{\frac{\ln \epsilon^{-1}}{2(\frac{1}{2}+\zeta_{\bar{\Gamma}})(1-\gamma-\alpha^B)n}}. \tag{3.11}$$

$$\zeta^A = \sqrt{\frac{\ln \epsilon^{-1}}{2(n_1^A + n_{\geq 2}^A)}}, \quad \text{assuming } \zeta^A \leq p_{b_s}/2, \tag{3.12}$$

$$\zeta^B = \sqrt{\frac{\ln \epsilon^{-1}}{2(n_1^B + n_{\geq 2}^B)}}, \quad \text{assuming } \zeta^B \leq p_{a_s}/2, \tag{3.13}$$

$$\alpha^A = \left(\frac{2\gamma}{p_{b_s}} + \frac{1}{f_{b_s}}\right)\zeta^A, \tag{3.14}$$

$$\alpha^B = \left(\frac{2\gamma}{p_{a_s}} + \frac{1}{f_{a_s}}\right)\zeta^B. \tag{3.15}$$

Next to these fluctuation parameters we define

$$\delta := 2\left[\left(\tfrac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)(\gamma+\alpha^B) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}(1-\gamma-\alpha^B) + \frac{(p_{\text{err}}+\zeta_{\mathcal{I}})(\frac{1}{2}+\zeta)}{\frac{1}{2}+\zeta_{\bar{\Gamma}}}\right]. \tag{3.16}$$

$$\lambda := f(-D/n) - (\gamma+\alpha^A) - 1/n \tag{3.17}$$

where f is defined as in Equation (3.5).

Next is stated the MDI-RSC protocol with decoy states from Ribeiro and Wehner [1, Protocol II.3]. An error in the expression for δ was corrected by Bramas [17]. Note that λ and δ depend on $\alpha^A, \alpha^B, \zeta^A$ and ζ^B, which can be evaluated only after step 2 of the Preparation phase. However, the original protocol uses λ and δ in step 1 of the Preparation phase. We remove this inconsistency by replacing these parameters with $\hat{\lambda}$ and $\hat{\delta}$ (see Section 3.4 for further explanation).

Protocol 3.3.1 (MDI-RSC with decoy states [17, Protocol 8] (adapted from [1, Protocol II.3]))**.** *Alice and Bob agree on the following inputs: security parameters ϵ and ϵ_1 (ϵ_1 is used to compute the bounds using the decoy states technique, see Lemma 3.3.1), ℓ the length of the committed string, the source quality parameter $\gamma \in [0, \frac{1}{2})$, the maximum size of D of Bob's quantum memory, the expected probability of*

bit-flip errors p_{err}, the probability distributions $(p_{a_s}, p_{a_{d_1}}, \ldots, p_{a_{d_q}})$ and $(p_{b_s}, p_{b_{d_1}}, \ldots, p_{b_{d_q}})$ as well as the intensities $\{a_s, a_{d_1}, \ldots, a_{d_q}\}$ and $\{b_s, b_{d_1}, \ldots, b_{d_q}\}$. Then they do the following steps.

Preparation phase:

1. *Alice and Bob agree on a number N of rounds satisfying*

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq \hat{n}^*, \tag{3.18}$$

   where p is the probability that a round j is not discarded if both parties are honest and $\hat{n}^*$ is the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\hat{\lambda} - h(\hat{\delta})}, \tag{3.19}$$

   where $\hat{\lambda}$ and $\hat{\delta}$ are defined as in Equations (3.45) *and* (3.46)*.*

2. *For round $j \in [N]$:*
   - *Alice chooses $X_j \in_R \{0,1\}$ and $\Theta_j \in_R \{0,1\}$ uniformly at random, and chooses intensity $a \in \{a_s, a_{d_1}, ..., a_{d_q}\}$ according to her probability distribution p_a. Alice prepares a quantum signal of intensity a, encoding X_j in the basis Θ_j, and sends $|X_j\rangle_{\Theta_j}$ to the measurement station (where $|0\rangle_0 = |0\rangle, |1\rangle_0 = |1\rangle, |0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$).*
   - *Bob chooses $\hat{X}_j \in_R \{0,1\}$ and $\hat{\Theta}_j \in_R \{0,1\}$ uniformly at random, and chooses intensity $b \in \{b_s, b_{d_1}, ..., b_{d_q}\}$ according to his probability distribution p_b. Bob prepares a quantum signal of intensity b, encoding $\hat{X}_j$ in the basis $\hat{\Theta}_j$, and sends $|\hat{X}_j\rangle_{\hat{\Theta}_j}$ to the measurement station.*
   - *The measurement station performs a probabilistic Bell measurement on the two states it receives and broadcasts if the outcome is of type 0 or 1, or whether the measurement failed. If the outcome is of type 1, Bob flips his bit.*
3. *Alice and Bob publicly announce the intensities they have used for all the rounds $j \in [N]$. They check if the amount of rounds where the other party used the signal setting matches the probability distribution for this setting, to check if there are f.e. not too much reported measurement failures.*
   - *Alice checks that among the rounds where she has used intensity a_s and the measurement succeeded, the fraction f_{b_s} of rounds where Bob has used intensity b_s is higher than $p_{b_s} - \zeta^A$. If not, she aborts.*
   - *Bob checks that among the rounds where he has used intensity b_s and the measurement succeeded, the fraction f_{a_s} of rounds where Alice has used intensity a_s is higher than $p_{a_s} - \zeta^B$. If not, he aborts.*

   Alice and Bob discard all the rounds where a failure has been announced, and all the rounds where the intensities used by Alice and Bob are not a_s and b_s. We call the remaining number of rounds n. Note that $n = f_{b_s} \times (n_1^A + n_{\geq 2}^A) = f_{a_s} \times (n_1^B + n_{\geq 2}^B)$.
4. *Alice and Bob check separately that the number of single photon rounds that were not reported as failure, is sufficiently high.*
   - *Using the decoy state technique, Alice estimates a lower-bound L_{A1} for n_1^A (given in [1, Lemma IV.15]), the number of rounds where the Bell measurement has not been announced as a failure and where Alice emitted 1 photon with intensity a_s. If $U_{A2} := n - L_{A1} \geq (\gamma + \alpha^A)n$ Alice aborts the protocol.*
   - *Using the decoy state technique, Bob estimates a lower-bound L_{B1} for n_1^B (given in [1, Lemma IV.15]), the number of rounds where the Bell measurement has not been announced as a failure and where Bob emitted 1 photon with intensity b_s. If $U_{B2} := n - L_{B1} \geq (\gamma + \alpha^B)n$ Bob aborts the protocol.*
5. *Alice and Bob check that $n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}$, and otherwise they abort the protocol.*

6. *Both parties wait for a time Δt.*
7. *Alice sends Θ over to Bob.*
8. *Bob computes the set of rounds $\mathcal{I} \subseteq [n]$ where $\Theta_j = \hat{\Theta}_j$. Bob discards all the rounds $j \notin \mathcal{I}$. Let's then call $\hat{X}_{\mathcal{I}}$ the string formed by all the remaining bits $\hat{X}_j$ with $j \in \mathcal{I}$.*

   When there is no noise, we have that $\forall j \in \mathcal{I}\ X_j = \hat{X}_j$. In practice there is noise and we call p_{err} the expected error rate between $\hat{X}_{\mathcal{I}}$ and X with $j \in \mathcal{I}$.

Commit phase:

1. *Bob checks whether $m := |\mathcal{I}| \in [n/2 - n\zeta, n/2 + n\zeta]$. If this is not the case, Bob aborts.*
2. *Alice chooses a random $[n, k, d]$-linear code C (for fixed n and k) and computes $w := \mathsf{Syn}(X)$ and sends it to Bob.*
3. *Alice picks a random 2-universal hash function $r \in_R \mathcal{R}$ and sends it to Bob.*
4. *Alice outputs $C := \mathsf{Ext}(X, r)$ where $\mathsf{Ext}(\cdot, \cdot)$ is a randomness extractor from the 2-universal family of functions.*

Open phase:

1. *Alice sends X to Bob.*
2. *Bob computes its syndrome and checks if it agrees with w he received from Alice in the Commit phase. If they disagree Bob aborts.*
3. *Bob checks that the fraction of rounds $j \in \mathcal{I}$ where X and $\hat{X}_{\mathcal{I}}$ do not agree lies in the interval $(p_{\text{err}} - \zeta_{\mathcal{I}}, p_{\text{err}} + \zeta_{\mathcal{I}})$. If not, Bob aborts the protocol, otherwise he accepts and outputs $C := \mathsf{Ext}(X, r)$.*

If the protocol aborts, the honest parties proceed as if it did not, but at the end:

- *Honest Bob rejects the commitment and outputs a uniformly random value $\tilde{C}$*
- *Honest Alice outputs a uniformly random value for C*

The requirement on N in the inputs is to make sure that there are enough quantum communication rounds N to securely produce ℓ-bits of final string, by making sure there will be enough successful rounds n. With these three parameter we can define the committed string rate $R := \frac{\ell}{n}$ and the effective committed string rate $R_{\text{eff}} := \frac{\ell}{N}$, which we will evaluate in Chapter 4.

Taking a closer look at p, the probability that a round is not discarded in the honest scenario, this means that both parties sent a signal state for this round, with probability $p_{a_s} \times p_{b_s}$, and the measurement station did not report a failure. this happens with probability $1 - p_{\text{fail}|a_s b_s}$. Thus $p = p_{a_s} \times p_{b_s} \times p_{\text{fail}|a_s b_s}$ [1].

If Alice and Bob are dishonest, the output for Alice is an n-bit string $X \in \{0,1\}^n$, the n-bit string Θ that specifies the basis she used for qubit encryption and a substring of Bob's bases $\hat{\Theta}_{\mathcal{J}_A}$. The output for Bob is a random set of indices $\mathcal{I} = \{j \mid \Theta_j = \hat{\Theta}_j\}$, the substring $\mathcal{E}_{p_{\text{err}}}(X_{\mathcal{I}})$ of X and his basis-specifying string $\hat{\Theta}$ and some of Alice's bases $\Theta_{\mathcal{J}_B}$. He then also has a slightly larger set for $\mathcal{I}$ supplied with what he could intercept from Alice's basis information: $\tilde{\mathcal{I}} = \mathcal{I} \cup \mathcal{J}_B$.

Because of the imperfect photon sources, a dishonest Alice and Bob both have more information about the other, consisting of the basis information of the rounds in $\mathcal{J}_A$ and $\mathcal{J}_B$ respectively. When one of the parties is dishonest, we assume that they also control the measurement station. If a dishonest party controls the measurement station, they can also decide to announce extra failures when they notice that the other sent a single state. To prevent this, honest Alice and Bob want to bound from above the fraction of multi-photon states that they sent, that will be used for the protocol. To estimate this fraction, they use q additional decoy states in the preparation phase. In [1, Lemma IV.15] the security analysis is done for $q = 2$.

Lemma 3.3.1 (Decoy states technique (from [1, Lemma IV.15] adapted in [17, Lemma 4.1]))**.** *Take $\epsilon, \epsilon_1 > 0$. Let $H \in \{A, B\}$ denote one of the two parties, Alice and Bob. Let $\varepsilon, \hat{\varepsilon}$ and L_{H1} be parameters whose values are as defined in [1, Lemma IV.15]. Then, if $n_1^H \geq L_{H1}$ in step 4 of Protocol 3.3.1, the proportion of multi-photon emissions from one of the parties is at most $\gamma + \alpha^H$, except with probability $16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1$.*

The security of Protocol 3.3.1 is stated and proved in [1, Theorem IV.14]. The correctness proof of [1] contains some errors, therefore, we rewrite the correctness proof here.

Theorem 3.3.2 (Security of Protocol 3.3.1 [17, Theorem 4.4] (adapted from [1, Theorem IV.14]))**.** *With $\epsilon, \epsilon_1, \varepsilon, \hat{\varepsilon}$ defined as in Lemma 3.3.1 and if the sources are sufficiently good, i.e.,*

$$\begin{cases} \frac{p_{\geq 2|a_s}}{(1-p_{0|a_s})} \leq p_{b_s}\gamma, \\ \textit{and} \\ \frac{p_{\geq 2|b_s}}{(1-p_{0|b_s})} \leq p_{a_s}\gamma. \end{cases} \tag{3.20}$$

then Protocol 3.3.1 gives a secure MDI $(\ell, 9\epsilon + 32(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1)$-RSC protocol.

Proof. The security for Alice is proved in [1, Theorem IV.17]. In particular, the protocol is $(3\epsilon + 16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1)$-secure for Alice. The security for Bob is given in [17, Lemma 4.2] and proves that the protocol is $(2\epsilon + 16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1)$-secure for Bob.

For the proof of correctness, note that conditioned on not aborting, the protocol is correct. We check for each part of the protocol with which probability at most an honest party would abort and show that when both parties are honest, the protocol aborts with probability at most $9\epsilon + 32(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1$.

In step 3 of the protocol, the honest parties abort with probability at most 2ϵ, as we can check with Hoeffding's inequality (see Lemma 2.1.4). $\Pr[f_{b_s} \leq p_{b_s} - \zeta^A] \leq \epsilon$. So Alice aborts with probability at most ϵ. The same holds for Bob, the total probability of aborting in this step is 2ϵ.

In step 4 of the protocol, note that the expectation of $n^A_{\geq 2}$ can be written as

$$\mathbb{E}(n^A_{\geq 2}) = p_{\geq 2|a_s,\text{no vacuum}}(n^A_1 + n^A_{\geq 2}), \tag{3.21}$$

where $p_{\geq 2|a_s,\text{no vacuum}}$ is the probability that Alice sends a multi-photon state, given that she used the signal setting and sent at least one photon. We can write this probability, according to conditional probability rules,

$$\Pr[\geq 2 \text{ photons sent} \mid 1 \cup \geq 2 \text{ photons sent}] = \frac{\Pr[\geq 2 \text{ photons sent} \cap (1 \cup \geq 2 \text{ photons sent}]}{\Pr[1 \cup \geq 2 \text{ photons sent}]}, \tag{3.22}$$

so we have

$$p_{\geq 2|a_s,\text{no vacuum}} = \frac{p_{\geq 2|a_s}}{(1 - p_{0|a_s})} \tag{3.23}$$

and

$$\mathbb{E}(n^A_{\geq 2}) = \frac{p_{\geq 2|a_s}}{(1 - p_{0|a_s})}(n^A_1 + n^A_{\geq 2}). \tag{3.24}$$

Using Hoeffding's inequality,

$$\Pr\left(n^A_{\geq 2} \geq \frac{p_{\geq 2|a_s}}{(1 - p_{0|a_s})}(n^A_1 + n^A_{\geq 2}) + \zeta^A(n^A_1 + n^A_{\geq 2})\right) \leq \epsilon \tag{3.25}$$

$$\Pr\left(\frac{n^A_{\geq 2}}{(n^A_1 + n^A_{\geq 2})} \geq \frac{p_{\geq 2|a_s}}{(1 - p_{0|a_s})} + \zeta^A\right) \leq \epsilon, \tag{3.26}$$

where we used the same fluctuation parameter ζ^A as in step 3, since the probability both intervals relate to are equivalent. Using equation (3.20) we can now derive that Alice has, except with probability at most ϵ,

$$\frac{n^A_{\geq 2}}{n^A_1 + n^A_{\geq 2}} \leq \frac{p_{\geq 2|a_s}}{(1 - p_{0|a_s})} + \zeta^A \leq p_{b_s}\gamma + \zeta^A. \tag{3.27}$$

If we divide this expression by f_{b_s} and use that, conditioned on not aborting up to this point, $f_{b_s} \geq p_{b_s} - \zeta^A$ from step 2, we get

$$\frac{n^A_{\geq 2}}{f_{b_s}(n^A_1 + n^A_{\geq 2})} \leq \frac{p_{b_s}\gamma}{p_{b_s} - \zeta^A} + \frac{\zeta^A}{f_{b_s}}. \tag{3.28}$$

If we assume that $\zeta^A/p_{b_s} \leq \frac{1}{2}$ like in Equation (3.12), we have that $\frac{1}{1-\zeta^A/p_{b_s}} \leq 1 + \frac{2\zeta^A}{p_{b_s}}$. Substituting this into equation (3.28) and using that $n = f_{b_s}(n_1^A + n_{\geq 2}^A)$ we get

$$\frac{n_{\geq 2}^A}{n} \leq \gamma\left(1 + \frac{2\zeta^A}{p_{b_s}}\right) + \frac{\zeta^A}{f_{b_s}} = \gamma + \left(\frac{2\gamma}{p_{b_s}} + \frac{1}{f_{b_s}}\right)\zeta^A \tag{3.29}$$

except with probability at most ϵ. Use from [1, Lemma IV.15], that the honest party can always find a lower bound L_{H1} on n_1^H, except with probability $16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$. Then, except with that same probability, $U_{A2} \geq n_{\geq 2}^A$. With this, we get the desired result and the probability that Alice aborts is at most $\epsilon + 16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1$. A similar proof holds for Bob. The total probability of aborting in step 4 is at most $2\epsilon + 32(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1$.

In step 5 of the protocol, Alice and Bob check for the number of remaining rounds $n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}$. Since p is the probability that any given round $j \in [N]$ is not discarded, we have by Hoeffding's inequality in Lemma 2.1.4

$$\Pr\left(n \leq \left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N\right) \leq \epsilon. \tag{3.30}$$

So except with probability ϵ we have that $n > \left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N$. At the start of the protocol we required that N must satisfy $\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n^* \geq \hat{n}^*$, where $\hat{n}^*$ is the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\hat{\lambda} - h(\hat{\delta})}. \tag{3.31}$$

So we have that except with probability at most ϵ

$$n > \left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq \hat{n}^* \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\hat{\lambda} - h(\hat{\delta})} \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}. \tag{3.32}$$

Thus while checking if $n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}$ Alice and Bob will abort the protocol with probability at most ϵ.

Again using Hoeffding's inequality we can check that Bob will abort the protocol at step 1 of the Commit phase, with probability at most 2ϵ, since he checks a double interval. We can similarly check that he aborts at step 3 of the Open phase of the protocol with probability at most 2ϵ. Thus overall, when both parties are honest, the protocol aborts with probability at most $9\epsilon + 32(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1$. □

3.4. Bounds on parameter definitions of [1, Protocol II.3]

In this section, we address a mistake in the MDI-RSC protocol with decoy states from Ribeiro and Wehner [1]. The variables λ and δ rely on experimental values that are not determinable a priori, but are used at the beginning step of the protocol. This dependence poses a challenge for the security analysis. To overcome this issue, we introduce a set of upper and lower bounds as replacements for these variables, using terms that can be determined in advance.

In step 1 of the Preparation phase of the original protocol, Alice and Bob agree on a number N of rounds satisfying

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n^*, \tag{3.33}$$

where p is the probability that a round j is not discarded if both parties are honest and n^* is the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}, \tag{3.34}$$

where λ and δ are in Equations (3.16) and (3.17). The problem is that λ depends on α^A and δ depends on α^B, where

$$\alpha^A = \left(\frac{2\gamma}{p_{b_s}} + \frac{1}{f_{b_s}}\right)\zeta^A, \tag{3.35}$$

$$\alpha^B = \left(\frac{2\gamma}{p_{a_s}} + \frac{1}{f_{a_s}}\right)\zeta^B, \tag{3.36}$$

$$\zeta^A = \sqrt{\frac{\ln \epsilon^{-1}}{2(n_1^A + n_{\geq 2}^A)}}, \tag{3.37}$$

$$\zeta^B = \sqrt{\frac{\ln \epsilon^{-1}}{2(n_1^B + n_{\geq 2}^B)}}. \tag{3.38}$$

The variables $\zeta^A, \zeta^B, \alpha^A, \alpha^B$ depend on parameters $n_1^A + n_{\geq 2}^A, n_1^B + n_{\geq 2}^B, f_{a_s}$ and f_{b_s} which are in the protocol determined after the quantum communication rounds are executed. To still analyse the rate of the secure committed strings produced by the protocol, we will bound these four parameters so that they no longer depend on $n_1^A + n_{\geq 2}^A, n_1^B + n_{\geq 2}^B, f_{a_s}$ and f_{b_s}. With that we can also give a bound on λ and δ. Bounding these parameters makes sure that all the intermediate steps in the security proof from Ribeiro and Wehner [1] hold. The committed string rate is slightly reduced. However, in the asymptotic case ($N \to \infty$), the committed string rate remains the same.

Note that since f_{a_s} and f_{b_s} are fractions and n is defined as $n = f_{b_s} \times (n_1^A + n_{\geq 2}^A) = f_{a_s} \times (n_1^B + n_{\geq 2}^B)$, $n \leq n_1^A + n_{\geq 2}^A$ and $n \leq n_1^B + n_{\geq 2}^B$. Thus we can bound $\zeta^A \leq \zeta$ and $\zeta^B \leq \zeta$. Then in the definitions of α^A and α^B, we replace these fractions f_{a_s} and f_{b_s} using that, conditioned on not aborting in step 2 of the protocol $f_{b_s} \geq p_{b_s} - \zeta^A$ and using the assumption $\zeta^A / p_{b_s} \leq \frac{1}{2}$ to get $\frac{\zeta^A/p_{b_s}}{1-\zeta^A/p_{b_s}} \leq \frac{2\zeta^A}{p_{b_s}}$,

$$\alpha^A = \left(\frac{2\gamma}{p_{b_s}} + \frac{1}{f_{b_s}}\right)\zeta^A \leq \left(\frac{2\gamma}{p_{b_s}} + \frac{1}{p_{b_s} - \zeta^A}\right)\zeta^A \tag{3.39}$$

$$\leq \left(\frac{2\gamma}{p_{b_s}} + \frac{1/p_{b_s}}{1 - \frac{1}{2}}\right)\zeta^A = \left(\frac{2\gamma}{p_{b_s}} + \frac{2}{p_{b_s}}\right)\zeta^A \tag{3.40}$$

$$\leq \left(\frac{2\gamma}{p_{b_s}} + \frac{2}{p_{b_s}}\right)\zeta = (\gamma + 1)\frac{2\zeta}{p_{b_s}} =: \hat{\alpha}^A, \tag{3.41}$$

where we used in the last inequality the bound on ζ^A. A similar argument holds for $\alpha^B \leq \hat{\alpha}^B := (\gamma + 1)\frac{2\zeta}{p_{a_s}}$.

Define then the statistical fluctuation variables as in Equations (3.9) to (3.11) respectively, but with $\hat{\alpha}^B$ instead of α^B:

$$\hat{\zeta}_{\bar{\Gamma}} = \sqrt{\frac{\ln \epsilon^{-1}}{2(1 - \gamma - \hat{\alpha}^B)n}}, \tag{3.42}$$

$$\hat{\zeta}_{\bar{\mathcal{I}}} = \min\left[\tfrac{1}{2}; \frac{\zeta + (1 - \gamma - \hat{\alpha}^B)\hat{\zeta}_{\bar{\Gamma}}}{\gamma + \hat{\alpha}^B}\right], \tag{3.43}$$

$$\hat{\zeta}_{\mathcal{I}\cap\bar{\Gamma}} = \sqrt{\frac{\ln \epsilon^{-1}}{2(\frac{1}{2} + \hat{\zeta}_{\bar{\Gamma}})(1 - \gamma - \hat{\alpha}^B)n}}. \tag{3.44}$$

Define $\hat{\delta}$ as in Equation (3.16) but with the variables with hats:

$$\hat{\delta} = 2\left[(\tfrac{1}{2} + \hat{\zeta}_{\bar{\mathcal{I}}})(\gamma + \hat{\alpha}^B) + \hat{\zeta}_{\mathcal{I}\cap\bar{\Gamma}}(1 - \gamma - \hat{\alpha}^B) + \frac{(p_{\text{err}} + \zeta_{\mathcal{I}})(\frac{1}{2} + \zeta)}{\frac{1}{2} + \hat{\zeta}_{\bar{\Gamma}}(x)}\right], \tag{3.45}$$

and similarly for $\hat{\lambda}$ defined as in Equation (3.17)

$$\hat{\lambda} = f\left(-\frac{D}{n}\right) - (\gamma + \hat{\alpha}^A) - \frac{1}{n}. \tag{3.46}$$

Then define $\hat{n}^*$ to be the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2}\epsilon) + \ln(\epsilon^{-1})}{\hat{\lambda} - h(\hat{\delta})}, \tag{3.47}$$

just as in Equation (3.34). To find if $\hat{n}^* \geq n^*$, we need to check that the denominator of Equation (3.47) is smaller than the original, $\hat{\lambda} - h(\hat{\delta}) \leq \lambda - h(\delta)$. Since α^A or α^B always appears in these expressions as a sum with γ, and γ does not depend on α^A or α^B, we define $x_A = \gamma + \alpha^A$ and $x_B = \gamma + \alpha^B$. Note that $x_A, x_B < 1$.

First, we check the derivative of λ to see if it is increasing or decreasing with x_A.

$$\lambda(x_A) = f\left(-\frac{D}{n}\right) - x_A - \frac{1}{n}, \tag{3.48}$$

gives

$$\frac{d\lambda}{dx_A} = -1 < 0. \tag{3.49}$$

For the binary entropy function we know

$$h'(\delta) = \frac{d}{d\delta}\left[-\delta\ln\delta - (1-\delta)\ln(1-\delta)\right] = \ln\left(\frac{1-\delta}{\delta}\right). \tag{3.50}$$

For δ in the interval $(0, \frac{1}{2})$ one finds $h'(\delta) > 0$. Thus this is increasing. If we can find that $\hat{\delta} \geq \delta$, we are done. We have

$$\delta(x_B) = 2\left[\left(\tfrac{1}{2} + \zeta_{\bar{\mathcal{I}}}(x_B)\right)x_B + \zeta_{\mathcal{I}\cap\bar{\Gamma}}(x_B)(1-x_B) + \frac{(p_{\text{err}} + \zeta_{\mathcal{I}})(\frac{1}{2}+\zeta)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}(x_B)}\right]. \tag{3.51}$$

Note that increasing α^B in x_b while γ remains constant is the same as increasing γ in x_b while α^B remains constant, in the expression for δ. Increasing γ implies that there is more information leakage due to multi-photon states. This implies that we will need a code with a higher distance to detect a dishonest party. Then by Lemma 2.1.3 $\hat{\delta}$ can only be higher than δ. Thus we conclude $\hat{\lambda} - h(\hat{\delta}) \leq \lambda - h(\delta)$. This means that $\hat{n}^* \geq n^*$, and it automatically obeys the bound of Equation (3.34), meaning that we can use the variables with hats in an analysis while maintaining the integrity and validity of the original security analysis of Ribeiro and Wehner [1].

4

Implementations of MDI Randomised String Commitment

In this chapter we will analyse the achievable committed string rates of the MDI-RSC protocols of Chapter 3, when they would be implemented with realistic sources that emit multi-photon states.

In Section 4.1 we analyse the achievable committed string rate of Protocol 3.2.1 implemented with a heralded SPDC source, which heralds whenever a single photon was emitted, using perfect, fully trusted local detectors.

In Section 4.2 we analyse the achievable committed string rate of Protocol 3.3.1 with two different source implementations: WCP sources in Section 4.2.1, and the signal output of an SPDC source in Section 4.2.2.

4.1. Using heralded SPDC sources with ideal local detectors

In this section, we evaluate Protocol 3.2.1, which implements randomised string commitment using perfect single-photon sources. In this analysis we use heralded single-photon sources based on the SPDC source described in Section 2.3 with ideal local detectors. We will evaluate the maximum achievable committed string rate over varying average photon number μ and error rate p_{err}.

When the idler photon of the SPDC source is successfully detected, this ”heralds” the presence of a signal photon, resulting in a heralded single-photon source. This enables Alice and Bob to verify the existence of a single photon before transmission, allowing them to discard rounds with vacuum or multi-photon emissions and eliminating the need for decoy states.

In this protocol, the maximum committed string rate over the accepted rounds is given by

$$R := \frac{\ell}{n} = \lambda - h(\delta) - \frac{2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{n}, \tag{4.1}$$

with

$$\lambda = f\left(-\frac{D}{n}\right) - \frac{1}{n} - \frac{\log(\frac{2}{\epsilon^2})}{n}, \quad \text{and} \quad \delta = 2p_{\text{err}} + 4\zeta_{\mathcal{I}}, \tag{4.2}$$

and n is the number of rounds that are not discarded during the protocol. To account for all rounds that were sent during the protocol, we define the effective committed string rate as

$$R_{\text{eff}} := \frac{\ell}{N} = \frac{\ell}{n} \cdot \frac{n}{N}, \tag{4.3}$$

where N is the total number of quantum rounds, including discarded ones. The value of N must satisfy the input condition

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n^*, \tag{4.4}$$

with n^* being the smallest integer satisfying Equation (3.8). For practicality, we use the relaxed criterion $\left(p - \sqrt{\frac{\ln(1/\epsilon)}{2N}}\right) N \geq n$ in this analysis, where p is the probability that a round is not discarded.

To determine the range of average photon numbers per beam μ and error rates p_{err} for which a positive effective string rate is achievable, we look at the asymptotic limit $N \to \infty$. In this regime, the square root term in Equation (4.4) vanishes, implying $n \to \infty$ as well. Then, λ and δ simplify to

$$\lambda \to f(0), \quad \delta \to h(2p_{\text{err}}) \tag{4.5}$$

and the committed string rate becomes

$$R_{n\to\infty} = f(0) - h(2p_{\text{err}}). \tag{4.6}$$

Note that this does not depend on μ. This dependence comes up when we look at the fraction of rounds that are not discarded, as discarding happens based on the outcome of the heralding. We have that

$$\frac{n}{N}\Big|_{N\to\infty} = p \tag{4.7}$$

and the effective committed string rate for this protocol with heralded SPDC sources and ideal local detectors, becomes

$$R_{\text{eff},N\to\infty} = (f(0) - h(2p_{\text{err}})) \cdot p. \tag{4.8}$$

The probability p that a round is not discarded is

$$p = p^1_{\text{A,sent}} \cdot p^1_{\text{B,sent}} \cdot (1 - p_{\text{fail}}), \tag{4.9}$$

where $p^1_{\text{A,sent}}(p^1_{\text{B,sent}})$ is the probability that Alice (Bob) successfully prepares and sends a single-photon state, and p_{fail} is the failure probability of the central Bell-state measurement.

Under ideal conditions, perfect detector efficiency and no dark counts , heralding ensures that only genuine single-photon emissions are accepted. In this idealised case

$$p^1_{\text{A,sent}} = p^1_{\text{B,sent}} = p_{\text{PDC}}(1, \mu),$$

where $p_{\text{PDC}}(1, \mu)$ is the probability that the SPDC source emits exactly one photon pair at intensity μ [9]. From Equation (2.25) we find that this is

$$p_{\text{PDC}}(1, \mu) = \frac{\mu}{(1 - \mu/2)^3}. \tag{4.10}$$

Now, p_{fail} is the failure probability of the BSM given that Alice and Bob sent their single photon. This is equal to the yield Y_{11}. When we assume that there are no losses on the transmission channels and the measurement station also has a perfect detector efficiency and no dark counts, this is equal to $Y_{11} = \frac{1}{2}$, [18]. Thus we find

$$p(\mu) = \tfrac{1}{2}\frac{\mu^2}{(1 - \mu/2)^6} \tag{4.11}$$

For $\epsilon = 10^{-6}$ and $D = 1000$ qubits, the effective committed string rates that can be achieved in the asymptotic case with this protocol and source, for different settings of μ and p_{err} are given in Figure 4.1. Indeed, as expected the region with the best effective committed string rates lies around $\mu = 1$, as for this setting the component of single photons will be the highest.

4.2. Using imperfect single photon sources

In this section, we evaluate the performance of Protocol 3.3.1 which implements randomised string commitment with decoy states. If we use a non-heralded source, or even a heralded source with non-ideal local detectors, there will be a possibility that we send multi-photon states. The decoy state technique deals with this.

In Protocol 3.3.1 the committed string rate over rounds that are not discarded is given by

$$R := \frac{\ell}{n} = \hat{\lambda} - h(\hat{\delta}) - \frac{2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{n}, \tag{4.12}$$

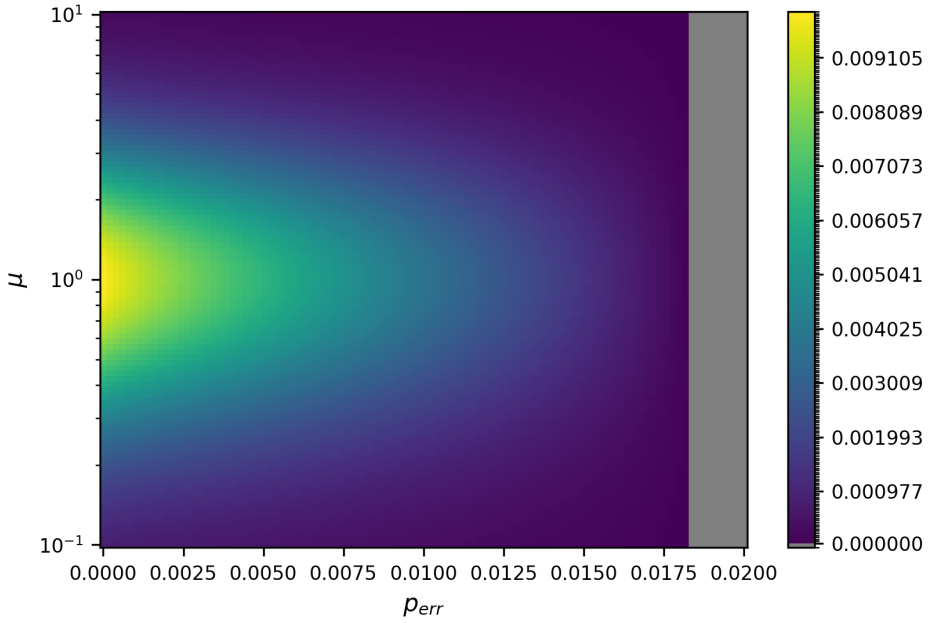

Figure 4.1: The effective committed string rate $R_{\text{eff},N\to\infty}$ of Protocol 3.2.1 with heralded SPDC sources and ideal local detectors for different values of μ and p_{err}. The infeasible region, where $R_{\text{eff},N\to\infty} < 0$ is coloured grey. The highest rates are indicated by the yellow region.

where $\hat{\lambda}$ and $\hat{\delta}$ are defined in Section 3.4 and n is the number of rounds that are not discarded during the protocol. To account for all rounds that were sent during the protocol, we examine again the effective committed string rate

$$R_{\text{eff}} = \frac{\ell}{N} = \frac{\ell}{n} \cdot \frac{n}{N}, \tag{4.13}$$

where N is the total number of quantum rounds, including discarded ones. The value of N must satisfy the input condition

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq \hat{n}^*, \tag{4.14}$$

with $\hat{n}^*$ being the smallest integer satisfying Equation (3.47). For practicality, we use the relaxed criterion $\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n$ in this analysis. Here, p is the probability that a round is not discarded, given by [1]

$$p = p_{a_s} p_{b_s} (1 - p_{\text{fail}|a_s b_s}), \tag{4.15}$$

where $p_{\text{fail}|a_s b_s}$ is the failure probability of the central Bell state measurement conditioned on both parties having sent signal states.

The values $\hat{\lambda}$ and $\hat{\delta}$ both depend on the parameter γ, which captures the proportion of multi-photon events. This parameter is a function of the source intensity μ and the probabilities p_{a_s} and p_{b_s} that Alice and Bob choose the signal setting. Following Wehner et al. [9], we assume a system with two decoy states and uniform random choice of intensity settings, so $p_{a_s} = p_{b_s} = 1/3$. We also assume both parties use the same signal intensity μ, i.e., $a_s = b_s = \mu$. The parameter gamma is defined in Equation (3.20) and has a value such that

$$\gamma \geq \max\left\{\frac{p_{\geq 2|a_s}}{p_{b_s}(1 - p_{0|a_s})}, \frac{p_{\geq 2|b_s}}{p_{a_s}(1 - p_{0|b_s})}\right\} = 3 \cdot \frac{p_{\geq 2|\mu}}{1 - p_{0|\mu}}. \tag{4.16}$$

Here, $p_{\geq 2|\mu}$ and $p_{0|\mu}$ come from the photon number distributions of the different sources.

To determine the range of source intensities μ and error rates p_{err} for which a positive effective string rate is achievable, we look at the asymptotic limit $N \to \infty$. In this regime, the statistical fluctuation term in Equation (4.14) vanishes, implying $n \to \infty$ as well. This means that $\hat{\lambda}$ and $\hat{\delta}$ simplify to

$$\hat{\lambda} \to f(0) - \gamma(\mu), \quad \hat{\delta} \to h(\gamma(\mu) + 2p_{\text{err}}), \tag{4.17}$$

and thus the committed string rate becomes:

$$R_{n\to\infty} = \hat{\lambda} - h(\hat{\delta}) = f(0) - \gamma(\mu) - h(\gamma(\mu) + 2p_{\text{err}}). \tag{4.18}$$

The fraction of rounds that are not discarded, converges to

$$\frac{n}{N}\Big|_{N\to\infty} = p. \tag{4.19}$$

Therefore, the effective committed string rate becomes

$$R_{\text{eff},N\to\infty} = (f(0) - \gamma(\mu) - h(\gamma(\mu) + 2p_{\text{err}})) \cdot p. \tag{4.20}$$

To estimate the probability p that rounds are kept, we use

$$p_{\text{fail}|a_s b_s} = p_{\text{fail}|\mu\mu} = 1 - Q_{\mu\mu}, \tag{4.21}$$

where $Q_{\mu\mu}$ is the gain, the probability that the BSM yields a successful outcome when both Alice and Bob send signal states of intensity μ. The gain is determined by the probability that both signals contain exactly one photon ($p^2_{1|\mu}$) and the yield Y_{11}, which is the success probability of the BSM given two single-photon inputs. It is given by [13, Equation B9] for WCPs, but it can be generalised to the following definition for photon number distributions for our sources.

$$Q_{\mu\mu} = (p_{1|\mu})^2 Y_{11}. \tag{4.22}$$

Using the decoy-state method, the honest parties can estimate Y_{11}. For the probabilistic BSM, that is assumed for this protocol by Ribeiro and Wehner [1], the maximum probability of success of the BSM is $\frac{1}{2}$ [19]. Under idealised assumptions, this yield is indeed $Y_{11} = \frac{1}{2}$ [18, Equation A9].

In the following sections, we evaluate R_{eff} for two different sources: phase-randomised WCP and SPDC. For every source we give the definition of the source dependent γ and p, find the regions of the source intensity μ and error rate p_{err} for which it is possible to get a positive committed string rate in the asymptotic case. Then we give the committed string rate as a function of the quantum communication rounds N for a few settings, to compare with which source to get a high rate in the finite regime.

4.2.1. Phase-randomised WCP source

The photon number distribution for a phase-randomised WCP with intensity μ is given by Equation (2.24), from which we find the specific values

$$p_{0|\mu} = e^{-\mu}, \tag{4.23}$$
$$p_{1|\mu} = \mu e^{-\mu}, \tag{4.24}$$
$$p_{\geq 2|\mu} = 1 - p_{0|\mu} - p_{1|\mu}. \tag{4.25}$$

Using this and Equation (4.16), we find that γ has a value such that

$$\gamma(\mu) = 3 \cdot \frac{1 - e^{-\mu} - \mu e^{-\mu}}{1 - e^{-\mu}}. \tag{4.26}$$

To find the expression for p we calculate

$$Q_{\mu\mu} = \mu^2 e^{-2\mu} Y_{11} \tag{4.27}$$

and find

$$p(\mu) = p_{a_s} p_{b_s} Q_{\mu,\mu} = \tfrac{1}{3} \cdot \tfrac{1}{3} \cdot \tfrac{1}{2} \mu^2 e^{-2\mu} = \tfrac{1}{18} \mu^2 e^{-2\mu}. \tag{4.28}$$

For $\epsilon = 10^{-6}$ and $D = 1000$ qubits, the effective committed string rates that can be achieved in the asymptotic case with this protocol and source, for different settings of μ and p_{err} are given in Figure 4.2.

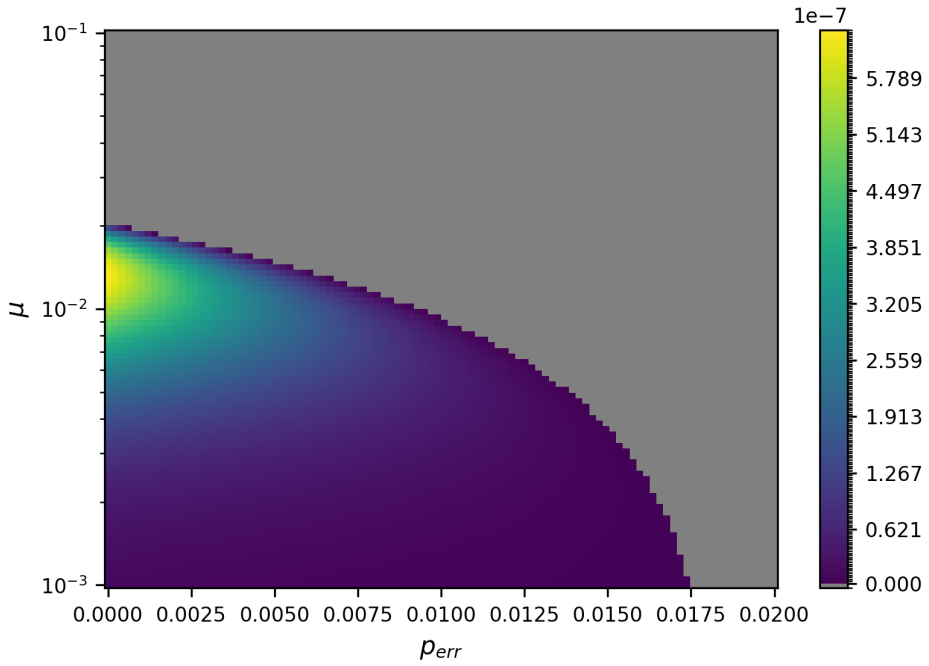

Figure 4.2: The effective committed string rate $R_{\text{eff},N\to\infty}$ of Protocol 3.3.1 with WCP sources for different values of μ and p_{err}. The infeasible region, where $R_{\text{eff},N\to\infty} < 0$ is coloured grey. The highest rates are indicated by the yellow region.

4.2.2. SPDC source

The photon number distribution for the signal beam of the SPDC is given by Equation (2.25), from which we find the specific values

$$p_{0|\mu} = \frac{1}{(1+\mu/2)^2}, \tag{4.29}$$

$$p_{1|\mu} = \frac{\mu}{(1+\mu/2)^3}, \tag{4.30}$$

$$p_{\geq 2|\mu} = 1 - p_{0|\mu} - p_{1|\mu}. \tag{4.31}$$

Then γ becomes

$$\gamma = 3\frac{1 - \frac{1}{(1-\mu/2)^2} - \frac{\mu}{(1-\mu/2)^3}}{1 - \frac{1}{(1-\mu/2)^2}} = 3\frac{(1-\mu/2)^3 - (1-\mu/2) - \mu}{(1-\mu/2)\left((1-\mu/2)^2 - 1\right)} = 3\frac{(1-\mu/2)^3 - (1-\mu/2) - \mu}{(1-\mu/2)^3 - (1-\mu/2)}. \tag{4.32}$$

For the gain of the BSM we get

$$Q_{\mu\mu} = p_{1|\mu}^2 Y_{1,1} = \frac{\mu^2}{(1+\mu/2)^6} \cdot \tfrac{1}{2}. \tag{4.33}$$

Therefore,

$$p(\mu) = \tfrac{1}{18}\frac{\mu^2}{(1+\mu/2)^6} \tag{4.34}$$

For $\epsilon = 10^{-6}$ and $D = 1000$ qubits, the effective committed string rates that can be achieved in the asymptotic case with this protocol and source, for different settings of μ and p_{err} are given in Figure 4.3.

4.3. Discussion

In Section 4.2, we evaluated the achievable effective committed string rate of implementations of the MDI-RSC Protocol 3.3.1 with decoy states. Two different sources were considered: WCP and SPDC. For both sources, there is a clear region around an optimal intensity setting μ with $p_{\text{err}} = 0$, as shown in Figures 4.2 and 4.3. In

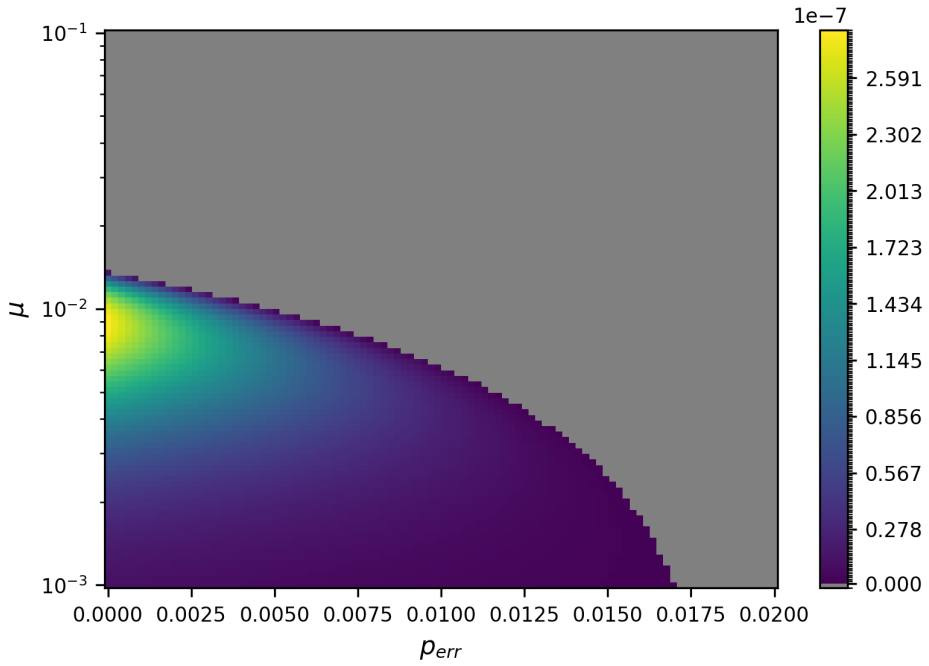

Figure 4.3: The effective committed string rate $R_{\text{eff},N\to\infty}$ of Protocol 3.3.1 with SPDC sources for different values of μ and p_{err}. The infeasible region, where $R_{\text{eff},N\to\infty} < 0$ is coloured grey. The highest rates are indicated by the yellow region.

this regime, the effective committed string rates achieved by the two implementations are comparable. Both are of the order of 10^{-7} secure committed string bits per quantum communication round.

For values of μ and p_{err} that are too high, it is no longer possible to generate a committed string with Protocol 3.3.1. These cases correspond to the grey regions in the plots. Here, the effective committed string rate becomes negative, meaning that the protocol will abort already during the Preparation phase.

In practice, these results can serve as a guideline for choosing between the two sources. The trade-off depends on the available intensity settings, since the optimal regions differ slightly for WCP and SPDC.

The true advantage of the SPDC source lies in the fact that it emits two entangled states. These can be used to build a heralded single-photon source, as we explored in Section 4.1. In that implementation, we assumed ideal local detectors that perfectly identify single photons. A real implementation, however, is more challenging. With non-ideal local detectors, multi-photon states may still be sent, even when heralding announces a single photon. In this case, the MDI-RSC protocol with decoy states must again be applied.

For general local detector settings, with efficiency $\eta \in [0,1]$ and dark count probability $p_{\text{dark}} \in [0,1]$, the probability of a single photon being emitted conditioned on heralding can be modelled using [9, Eq. C21]. With this model, one could perform an analysis similar to that in Section 4.2, to determine the achievable committed string rate of a heralded SPDC source with non-ideal detectors. This, however, lies outside the scope of the present work.

Finally, we note that in this chapter we assumed that the central measurement of the MDI setup succeeded with maximum probability. This is a best-case scenario. In practice, the performance will also depend on the quality of the measurement devices. For a realistic evaluation of Protocol 3.3.1, imperfections of the central measurement station must be taken into account in addition to the bit-flip errors from transmission which we modelled by p_{err}

5

Phase-encoded MDI Randomised String Commitment

In the previous chapter we analysed the rates of the MDI-RSC protocols 3.2.1 and 3.3.1 when implemented with different sources. In this chapter we take a step further and explore an alternative way for Alice and Bob to exchange quantum states in the Preparation phase of the RSC protocol. For this purpose, we draw inspiration from ideas developed in different QKD regimes.

Initially, the Twin-Field QKD (TF-QKD) regime appeared promising, since its central goal is to overcome the distance limitations of conventional QKD, which could in turn improve the performance of an RSC protocol. However, the intricacies of TF-QKD make it difficult to adapt directly to our setting. Instead, we adopt a coherent-state, phase-encoded MDI scheme, which shares some features with TF-QKD while remaining more accessible for protocol design and security analysis.

In what follows, we first review the basic principles of TF-QKD in Section 5.1, before moving on in Section 5.2 to the simplified phase-encoded MDI regime that we will use as the quantum exchange phase of our new protocol. In Section 5.3 we give a phase-encoded MDI-RSC protocol and give a sketch of a security proof. Finally in Section 5.4 we discuss the implications and limitations of this new protocol.

5.1. Twin-Field QKD

Twin-Field QKD (TF-QKD) is a scheme in which weak coherent states prepared by two remote parties interfere at a central, potentially untrusted, measurement station. It was proposed by Lucamarini et al. [14] as a means to overcome the rate–distance limit of conventional QKD by exploiting single-photon interference. A key insight is that the secure key rate can scale with the square root of the channel transmittance, rather than linearly, thereby surpassing the traditional repeaterless bound.

The central advantage of TF-QKD is its reliance on single-photon interference, in contrast to the two-photon interference underlying MDI-QKD. Interference can occur even when Alice and Bob each send indistinguishable weak coherent states that together contain, with some probability, only a single photon. This avoids the exponential loss associated with direct single-photon transmission. The indistinguishability of the optical pulses ensures that interference outcomes depend solely on their relative phase.

Security against an adversary controlling the central station is guaranteed because detection events are indistinguishable with respect to which party emitted the optical field. Any attempt at eavesdropping disturbs the interference pattern, creating errors that Alice and Bob can identify during post-processing.

Conceptually, TF-QKD can be regarded as an ”unfolded” phase-encoded protocol, in which both parties send optical fields to a central station (see Figure 5.1). The bit and basis choices are encoded in the phase of coherent states, while single-photon interference at the relay reveals only their relative phase. Next to the three main features of TF-QKD that

1. it is measurement-device independent,

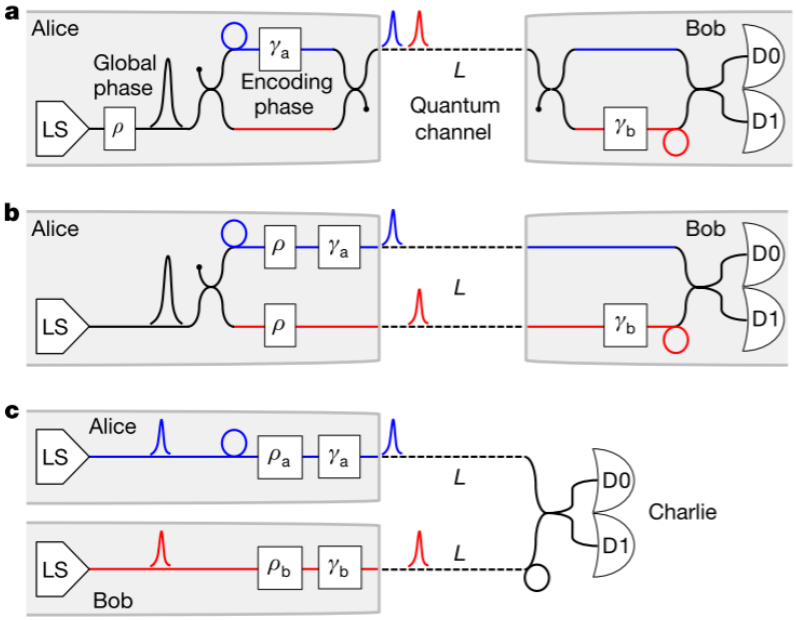

Figure 5.1: Schematics of phase-based QKD unfolded into TF-QKD from [14]. The shaded regions are inaccessible to an eavesdropper. **a.** Standard setup: a light source emits optical pulses with random global phase ρ. At the input of an asymmetric Mach–Zehnder interferometer, the pulse is split; the longer path acquires a relative phase γ_a. The two pulses travel through a quantum channel of length L to Bob, who applies a phase γ_b in his interferometer and measures the interference with detectors D_0 and D_1. **b.** Unfolded setup: the common path of length L is replaced by two equal-length channels, with the secondary pulses travelling separately before interfering at Bob's detectors. **c.** Twin Field setup: both Alice and Bob act as transmitters, each with a laser and one interferometer arm. Alice (Bob) prepares a pulse with random phase ρ_a (ρ_b) and encoding phase γ_a (γ_b). Their pulses are overlapped at Charlie's beamsplitter and detected. After Charlie announces the detection result, Alice and Bob reveal the basis choices $\gamma_{a,b}$ and the phase slices containing $\rho_{a,b}$.

2. it relies on single-photon interference, and
3. it uses phase-encoded coherent quantum states,

two further ingredients are essential. First, information is encoded in the relative phase of the coherent states, while the global phase is chosen uniformly at random from $[0, 2\pi)$. Phase randomisation ensures the prepared signals are effectively mixtures of photon-number states, enabling the decoy-state method. Second, because measurements depend only on relative phase, Alice and Bob must align their global phases. To increase the probability of alignment, Lucamarini et al. [14] proposed discretising the phase space into M slices and post-selecting rounds where their global phases fall within the same slice. This ensures a maximum misalignment of $2\pi/M$, at the cost of a trade-off between error rate and data yield.

An alternative approach, suggested by Curty, Azuma, and Lo [20], fixes the global phase in the key-generation basis while applying randomisation only in the parameter-estimation basis. While suitable for QKD, this strategy does not translate to RSC. In RSC, Alice and Bob must generate correlated strings that agree roughly half of the time, while the remaining positions stay random and unknown to Bob, and which positions are correlated remains unknown to Alice. A single deterministic basis cannot achieve this: if Alice and Bob were to perform parameter estimation in only one basis, Alice would always know which basis Bob used for his *string* generation, and therefore she could determine exactly which parts of their strings coincide. For RSC, it is essential that the committed strings are generated using two complementary bases. This ensures that Alice can later reveal her basis information to Bob, and as a result, Bob learns about half of the bits in Alice's string, while Alice herself remains ignorant of which subset Bob knows.

A similar strategy is adopted by Liu et al. [21], who employ heralded single-photon sources based on SPDC in the parameter-estimation basis. Since we also analysed heralded SPDC sources in Chapter 4, their approach initially appeared promising. However, for the purpose of designing an RSC protocol, it was ultimately set aside for the same reasons discussed above.

Although TF-QKD is conceptually appealing, its technical demands in mainly the last two features make it

challenging to adapt directly to an MDI-RSC setting. For this reason, we introduce in Section 5.3 a simplified alternative: a phase-encoded MDI-RSC protocol and give its security proof. This keeps the essential first three features while omitting the additional complexities of phase randomisation and decoy-state analysis.

5.2. Phase-encoded MDI-RSC

Alice and Bob prepare a signal pulse and a reference pulse. Then a phase modulation is applied to the signal pulse, randomly chosen from $\{0, \pi/2, \pi, 3\pi/2\}$ where $\{0, \pi\}$ is the X basis and $\{\pi/2, 3\pi/2\}$ is the Y basis. The pulses are sent to a central measurement station that aligns their global phase and establishes a quantum correlation between the signal pulses sent by Alice and Bob, and it is announced whether the measurement was successful and in that case, if the outcome is of type 0 or 1. The correlation measurement is done by having Alice and Bob's signal pulses as input to a 50:50 beamsplitter which is followed by two single-photon threshold detectors D_0 and D_1 (see for example the experimental setup of [22], given in Figure 5.2).

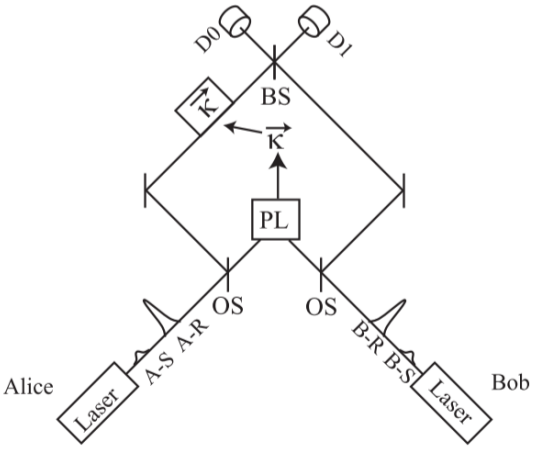

Figure 5.2: Schematic of the experimental setup of [22, phase-encoding scheme I]. Alice and Bob each prepare a pair of pulses: signal (A-S, B-S) and reference (A-R, B-R). The signal pulses are phase-modulated according to their choices. An optical switch (OS) transmits the reference pulses while reflecting the signal pulses. A phase-locking unit (PL) measures the relative phase between two polarization modes and applies the corresponding phase shift κ to one of the signal pulses. Finally, the signal pulses interfere at a 50:50 beamsplitter (BS) and are detected by detectors D_0 and D_1.

When we assume that Alice and Bob use the same amplitudes α for their signal pulses and also that their global phases are aligned due to the reference pulse, their inputs look like

$$|e^{i\phi_A}\alpha\rangle\,, \quad |e^{i\phi_B}\alpha\rangle \tag{5.1}$$

respectively, where ϕ_A and ϕ_B are randomly chosen from the set $\{0, \pi/2, \pi, 3\pi/2\}$. Using Equations (2.34) and (2.35) we can find for all possible inputs of Alice and Bob the outputs in D_0 and D_1.

Whenever Alice and Bob use a different basis, there will be non-vacuum states in both detectors. For example, for $\phi_A = 0$ and $\phi_B = \frac{\pi}{2}$ we get the states $|\frac{1}{\sqrt{2}}(1+i)\alpha\rangle_{D_0}$ and $|\frac{1}{\sqrt{2}}(-1+i)\alpha\rangle_{D_1}$. Whenever they use the same basis, one detector has a state that is amplified by $\sqrt{2}$ compared to one of the inputs, and the other has the vacuum state. For example, for $\phi_A = 0$ and $\phi_B = \pi$ we get the states $|0\rangle_{D_0}$ and $|-\sqrt{2}\alpha\rangle_{D_1}$. Using Equation (2.26), we can find the probabilities that the detectors click for each input state of Alice and Bob. When they use a different basis

$$p_{\text{click}}(D_0|\phi_A = 0, \phi_B = \tfrac{\pi}{2}) = 1 - e^{-\left|\frac{1}{\sqrt{2}}(1+i)\alpha\right|^2} = 1 - e^{-|\alpha|^2} \tag{5.2}$$

$$p_{\text{click}}(D_1|\phi_A = 0, \phi_B = \tfrac{\pi}{2}) = 1 - e^{-\left|\frac{1}{\sqrt{2}}(-1+i)\alpha\right|^2} = 1 - e^{-|\alpha|^2} \tag{5.3}$$

and when they use the same basis

$$p_{\text{click}}(D_0|\phi_A = 0, \phi_B = \pi) = 1 - e^{-|0|^2} = 0 \tag{5.4}$$

$$p_{\text{click}}(D_1|\phi_A = 0, \phi_B = \pi) = 1 - e^{-|-\sqrt{2}\alpha|^2} = 1 - e^{-2|\alpha|^2} \tag{5.5}$$

This can be summarised in the probabilities a certain click pattern is observed, given Alice and Bob used the same bases or not. These probabilities are given in Table 5.1. In this table, we mean by a single click that only one of the detectors clicked, and by a double click that there has been a click in both detectors D_0 and D_1.

	no click	single click	double click
same basis	$e^{-2\|\alpha\|^2}$	$1 - e^{-2\|\alpha\|^2}$	0
different basis	$e^{-2\|\alpha\|^2}$	$2e^{-\|\alpha\|^2}(1 - e^{-\|\alpha\|^2})$	$(1 - e^{-\|\alpha\|^2})^2$
average	$p_{\text{fail}} = e^{-2\|\alpha\|^2}$	$p_1 = \frac{1}{2} - \frac{3}{2}e^{-2\|\alpha\|^2} + e^{-\|\alpha\|^2}$	$p_2 = \frac{1}{2}(1 - e^{-\|\alpha\|^2})^2$

Table 5.1: Probabilities for the tree different click patterns in detectors D_0 and D_1, given Alice and Bob either used the same basis, different bases, or on average. Note that the probabilities per row sum up to 1.

In the phase-encoded MDI-RSC Protocol 5.3.1, all single- and double-click events are regarded as successful events. The total probability of a successful event is given by

$$\Pr[\text{succ event}] = \Pr[\text{single click} \cup \text{double click}] = 1 - e^{-2|\alpha|^2} \tag{5.6}$$

From Table 5.1 we see that the probability of a certain click event depends on whether Alice and Bob used the same basis. When Alice and Bob choose their basis uniformly at random, they will have a probability of $p = \frac{1}{2}$ to use the same basis. For Bob to check the size of set $\mathcal{I}$ it is useful to know what the probability is that the two parties used the same basis, given that the central measurement station announced a successful event. When Alice and Bob are both honest, this is

$$\Pr[\text{same basis}|\text{succ event}] = \frac{\Pr[\text{succ event}|\text{same basis}] \cdot \Pr[\text{same basis}]}{\Pr[\text{succ event}]} \tag{5.7}$$

$$= \frac{(1 - e^{-2|\alpha|^2}) \cdot \frac{1}{2}}{1 - e^{-2|\alpha|^2}} = \frac{1}{2} \tag{5.8}$$

This is in the ideal case. In reality $\Pr[\text{same basis}|\text{succ event}]$ also depends on noise and imperfections in the channels and beamsplitter which might have different effects depending on the intensity of the coherent state. For simplicity, these imperfections are disregarded.

5.3. Phase-encoded MDI-RSC Protocol

Here, we present a protocol for MDI-RSC with phase-encoded coherent states and give its security proof. For measuring the incoming coherent states of Alice and Bob, the central measurement station uses a beamsplitter and two threshold detectors D_0 and D_1. We define successful events where exactly one detector clicks as type 0 when only detector D_0 clicks, and type 1 when only detector D_1 clicks. In the successful event where both detectors click, the measurement station will announce a successful event of type 0 or type 1 uniformly at random. The measurement station only reveals if the measurement was a failure (no click) or if it was a successful event of type 0 or type 1. On a successful event, it does not reveal if it was a single click or a double click.

Define the following parameters.

$$\zeta := \sqrt{\frac{\ln \epsilon^{-1}}{2n}} \tag{5.9}$$

$$\zeta_{\mathcal{I}} := \sqrt{\frac{\ln \epsilon^{-1}}{2(\frac{1}{2} - \zeta)n}} \tag{5.10}$$

$$\zeta_{\text{fail}} := \sqrt{\frac{\ln(\epsilon^{-1})}{2(1 - p_{\text{fail}})n}} \tag{5.11}$$

$$\mathcal{F} := \frac{1 - p_{\text{fail}}}{(1 + \zeta_{\text{fail}})^2} \tag{5.12}$$

$$\lambda := -\frac{1}{\mathcal{F}} \log(2\Omega) - \frac{D}{n} + 1 \tag{5.13}$$

$$\delta := p_{\text{err}} + 2\zeta_{\mathcal{I}} + e_2(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}}) \tag{5.14}$$

$$e_2 := \frac{p_2 + \zeta}{\mathcal{F}} \tag{5.15}$$

Here $0 < \epsilon < 1$ is a security parameter, n is the length of the bit string with successful measurement outcomes, $p_{\text{err}} \in [0, \frac{1}{2})$ is the expected bit-flip error probability on the quantum communication channel, p_{fail} is the probability that a round j is not announced as successful if both parties are honest, e_2 is an upper bound on the fraction of rounds for which the measurement station observes a double click, p_2 is the probability that the measurement station observes a double click (for ideal conditions, this probability can be found in Table 5.1), and Ω is an upper bound on Bob's guessing probability of one of Alice's bits, defined in Theorem 5.3.5. Take k to be the largest integer such that

$$\frac{k}{n} \leq 1 - h(\delta) + \frac{\log \epsilon}{n}. \tag{5.16}$$

Protocol 5.3.1 (Phase-encoded MDI randomised string commitment)**.** *After having agreed upon the input parameters, Alice and Bob execute the following steps.*

Preparation phase:

1. *Alice and Bob agree on a number N of rounds satisfying*

$$\left((1 - p_{\textit{fail}}) - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}} \right) N \geq n^*, \tag{5.17}$$

   where $p_{\textit{fail}}$ is the probability that a round j is not announced as successful if both parties are honest and n^* is the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}, \tag{5.18}$$

   where λ and δ are in Equations (5.13) *and* (5.14)*.*

2. *For round $j \in [N]$:*
   - *Alice chooses $X_j \in_R \{0,1\}$ and $\Theta_j \in_R \{0,1\}$ uniformly at random. She prepares a signal and a reference pulse and applies a phase shift to the signal pulse of $\phi_j = \pi X_j + \frac{\pi}{2}\Theta_j$. Here, X_j is the bit she encodes in the X-basis when $\Theta_j = 0$ and in the Y-basis when $\Theta_j = 1$. She sends the signal pulse and reference pulse to the central measurement station.*
   - *Bob chooses $\hat{X}_j \in_R \{0,1\}$ and $\hat{\Theta}_j \in_R \{0,1\}$ uniformly at random. He prepares a signal and a reference pulse and applies a phase shift to the signal pulse of $\hat{\phi}_j = \pi \hat{X}_j + \frac{\pi}{2}\hat{\Theta}_j$. He sends the signal pulse and reference pulse to the central measurement station.*
   - *The measurement station performs a beamsplitter based measurement and announces whether the outcome is successful or not. If the outcome was successful, they announce whether it was of type 0 or type 1.*
3. *Alice and Bob keep their data for the rounds in which the measurement outcomes were successful. We call this set of indices $\mathcal{S} \subseteq [N]$, $|\mathcal{S}| = n$. Bob flips his bit if the outcome was of type 1. Alice has strings $X_{\mathcal{S}}, \Theta_{\mathcal{S}} \in \{0,1\}^n$ and Bob has strings $\hat{X}_{\mathcal{S}}, \hat{\Theta}_{\mathcal{S}} \in \{0,1\}^n$.*
4. *Alice and Bob check if the fraction of measurement failures exceeds $p_{\textit{fail}} + \sqrt{\frac{\ln(\epsilon^{-1})}{2N}}$. If so, they abort.*
5. *Both parties wait for a time Δt.*

6. *Alice sends $\Theta_{\mathcal{S}}$ to Bob.*
7. *Bob computes the set of indices $\mathcal{I} = \{\, j \in [n] : (\Theta_{\mathcal{S}})_j = (\hat{\Theta}_{\mathcal{S}})_j \,\}$. He discards all the rounds $j \notin \mathcal{I}$. We call $\hat{X}_{\mathcal{I}}$ the string formed by the remaining bits $\hat{X}_j$ with $j \in \mathcal{I}$. Accounting for errors that occur during transmission, we call p_{err} the expected error rate between X_j and $\hat{X}_j$ for $j \in \mathcal{I}$, thus p_{err} is the expected fraction of error between $X_{\mathcal{I}}$ and $\hat{X}_{\mathcal{I}}$.*

Commit phase:

1. *Bob checks if $m := |\mathcal{I}| \geq (\frac{1}{2} - \zeta) \cdot n$. If not, he aborts.*
2. *Alice chooses a random $[n, k, d]$-linear code C (for fixed n and k) and computes $w := \mathsf{Syn}(X)$ and sends it to Bob.*
3. *Alice picks a random 2-universal hash function $r \in_R \mathcal{R}$ and sends it to Bob.*
4. *Alice outputs $C := \mathsf{Ext}(X_{\mathcal{S}}, r)$ where $\mathsf{Ext}(\cdot, \cdot)$ is a randomness extractor from the 2-universal family of functions.*

Open phase:

1. *Alice sends $X_{\mathcal{S}}$ to Bob.*
2. *Bob computes its syndrome and checks if it agrees with w he received from Alice in the Commit phase. If they disagree Bob aborts.*
3. *Bob checks that the fraction of rounds $j \in \mathcal{I}$ where $X_{\mathcal{S}}$ and $\hat{X}_{\mathcal{I}}$ do not agree lies in the interval $[p_{\text{err}} - \zeta_{\mathcal{I}}, p_{\text{err}} + \zeta_{\mathcal{I}}]$. If not, Bob aborts the protocol, otherwise he outputs $C := \mathsf{Ext}(X_{\mathcal{S}}, r)$.*

If the protocol aborts, the honest parties proceed as if it did not, but at the end:

- *Honest Bob rejects the commitment and outputs a uniformly random value $\tilde{C}$*
- *Honest Alice outputs a uniformly random value for C*

We now present the security proof of Protocol 5.3.1, in particular we prove Theorem 5.3.1. Note that for the theorem to hold true, λ has to be positive. In the later half of Section 5.3.2 we derive a lower bound on λ. However, our lower bound is still negative.

Note that we prove the security for Bob only against a semi-honest Alice, who will only start to try to cheat from the Open phase. This means that Alice has full control over the central measurement station, but will act honestly during the Preparation phase and the Commit phase. In the Open phase, she will try to let Bob accept a different string $X'_{\mathcal{S}}$ instead of the string $X_{\mathcal{S}}$ that she committed to.

Theorem 5.3.1 (Security of Protocol 5.3.1)**.** *Let $\epsilon > 0$ and let λ and δ be defined as in Equations* (5.13) *and* (5.14)*. If*

$$\left((1 - p_{\text{fail}}) - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n^*, \tag{5.19}$$

where n^* is the smallest positive integer solution to the inequality

$$n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon}) + \ln(\frac{1}{\epsilon})}{\lambda - h(\delta)}, \tag{5.20}$$

and p_{fail} is the probability that a round $j \in [N]$ is not announced as successful if both parties are honest, then Protocol 5.3.1 implements a $(\ell, 4\epsilon)$-Randomised String Commitment.

Proof. When Alice and Bob are honest and conditioned on not aborting, the protocol is correct, since X and r are chosen at random. When the two parties are honest, they can abort the protocol in three places: in the fourth step of the Preparation phase, in the first step of the Commit phase or in the third step of the Open phase. Alice and Bob abort the protocol in the preparation phase whe the fraction of measurement failures exceeds $p_{\text{fail}} + \sqrt{\frac{\ln(\epsilon^{-1})}{2N}}$. By Hoeffding's inequality 2.15 this happens with probability at most ϵ. In the Commit phase, Bob aborts if $|\mathcal{I}| < (\frac{1}{2} - \zeta)n$. By the definition of ζ and Hoeffding's inequality 2.16, this happens with

probability at most ϵ. Similarly, in the Open phase, Bob aborts the protocol if he observes an error rate that does not lie in the interval $[p_{\text{err}} - \zeta_{\mathcal{I}}, p_{\text{err}} + \zeta_{\mathcal{I}}]$. By the Hoeffding's inequality 2.17, this happens with probability at most 2ϵ. Putting the three potential abort events together, the honest parties have a probability at most 4ϵ to abort, which proves correctness of a $(\ell, 4\epsilon)$-Randomised String Commitment. Lemma 5.3.3 proves that Protocol 5.3.1 is 4ϵ-binding. Lemma 5.3.4 proves that Protocol 5.3.1 is 3ϵ-hiding. □

To derive bounds for the proofs of security for Alice and Bob, we need the following lemma.

Lemma 5.3.2. *When honest Alice did not abort the protocol during the Preparation phase, the fraction of successful rounds is at least $\mathcal{F}$, i.e.*

$$\frac{n}{N} \geq \mathcal{F}, \tag{5.21}$$

except with probability at most ϵ.

The proof of this lemma can be found in Appendix D.

5.3.1. Security for Bob against a semi-honest Alice

After the Preparation phase, a semi-honest Alice has some information about $\mathcal{I}$. Assume that Alice has full control of the measurement station, so that she knows which of the successful rounds were double-click events. Call the set of indices for which rounds there was a double-click event $\mathcal{C}_2$. Whenever there is a double click, Alice knows that she and Bob did not use the same basis. She can flip any bit in this set $X_{\mathcal{C}_2}$ without detection.

Lemma 5.3.3 (Security against semi-honest Alice (based on [17, Lemma 3.8])**.** *Protocol 5.3.1 is 4ϵ-binding, which means that if semi-honest Alice opens a different string in the Open phase than she committed to, the probability that Bob accepts a commitment $\hat{C} \neq C$ is less than 4ϵ, i.e.,*

$$\Pr[\textit{Bob accepts and } \hat{C} \neq C] \leq 4\epsilon. \tag{5.22}$$

Proof. First, we show that the randomly generated $[n, k, d]$-code C has a distance d which satisfies $d \geq \delta n$, where δ is given in Equation (5.14), except with probability at most ϵ, given that k satisfies Equation (5.16).

Using Lemma 2.1.3 with $\delta = p_{\text{err}} + 2\zeta_{\mathcal{I}} + e_2(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}})$, we find

$$\Pr[d \leq (p_{\text{err}} + 2\zeta_{\mathcal{I}} + e_2(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}}))n] \leq 2^{(\frac{k}{n} - 1 + h(\delta))n}. \tag{5.23}$$

From Equation (5.16) we have $(\frac{k}{n} - 1 + h(\delta))n = \log \epsilon$, thus

$$\Pr[d \leq (p_{\text{err}} + 2\zeta_{\mathcal{I}} + e_2(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}}))n] \leq 2^{\log \epsilon} = \epsilon. \tag{5.24}$$

There exists a string $X_{\mathcal{S}}$ such that $w = \mathsf{Syn}(X_{\mathcal{S}})$ and Bob has a set of indices $\mathcal{I}$ and the substring $\hat{X}_{\mathcal{I}}$, containing errors with probability p_{err}. Let's call $X'_{\mathcal{S}}$ the string that Alice sends to Bob during the Open phase.

If Alice sends $X'_{\mathcal{S}} = X_{\mathcal{S}}$, Bob will accept the protocol and output the commitment $\hat{C} = C$. This is the correct protocol in the case of an honest Alice.

If Alice wants to cheat, she has to open a string $X'_{\mathcal{S}} \neq X_{\mathcal{S}}$. In this case, we want to know the probability that $\hat{C} \neq C$ and Bob accepts the protocol. There are two possibilities: $\mathsf{Syn}(X'_{\mathcal{S}}) \neq w$ or $\mathsf{Syn}(X'_{\mathcal{S}}) = w$. For the former, the probability is 0, since Bob always rejects if $\mathsf{Syn}(X'_{\mathcal{S}}) \neq w$. Thus

$$\begin{aligned} \Pr[\text{Bob accepts and } \hat{C} \neq C] &= \Pr[\text{Bob accepts and } \mathsf{Ext}(X'_{\mathcal{S}}, r) \neq \mathsf{Ext}(X_{\mathcal{S}}, r) \mid \mathsf{Syn}(X'_{\mathcal{S}}) = w] && (5.25) \\ &\leq \Pr[\text{Bob accepts and } X'_{\mathcal{S}} \neq X_{\mathcal{S}} \mid \mathsf{Syn}(X'_{\mathcal{S}}) = w] && (5.26) \end{aligned}$$

Due to the properties of the error-correcting code C, $X'_{\mathcal{S}} \neq X_{\mathcal{S}}$ and $\mathsf{Syn}(X'_{\mathcal{S}}) = w$ means that the distance between $X_{\mathcal{S}}$ and $X'_{\mathcal{S}}$ is at least d. So Alice has to flip at least d bits in her string $X_{\mathcal{S}}$ in such a way that $\hat{X}_{\mathcal{I}}$ and $X_{\mathcal{I}}$ differ by at most $(p_{\text{err}} + \zeta_{\mathcal{I}})m$ bits. Alice can flip the bits X_j for $j \in \mathcal{C}_2$ for free, since she knows that these are not in $X_{\mathcal{I}}$. Let $c_2 := |\mathcal{C}_2|$. Among the $n - c_2$ remaining bits, she will flip a number W of bits of $X_{\mathcal{I}}$. If she

randomly flips $d - c_2$ bits among the $n - c_2$ bits in $X_{\mathcal{S}\setminus\mathcal{C}_2} = X_{\mathcal{C}_1}$, any bit has a probability of at least $\frac{d-c_2}{n-c_2}$ to have been flipped, and a random number $m = |\mathcal{I}|$ of the $n - c_2$ bits will be sampled by Bob.

We can use Hoeffding's inequality from Equation (2.16). Call $Y_1, \ldots, Y_m$ m random Bernoulli variables that have value 1 with probability at least $\frac{d-c_2}{n-c_2}$, indicating flipped bits in $X_{\mathcal{I}}$. Then $W = \sum_{j=1}^{m} Y_j$ and $\mathbb{E}(W) \geq \frac{m(d-c_2)}{n-c_2}$. As Bob is assumed to be honest, conditioned on not aborting, we have $m \geq (\frac{1}{2} - \zeta)n$. This gives

$$\Pr\left[W \leq m\left(\frac{d-c_2}{n-c_2} - \zeta_{\mathcal{I}}\right)\right] \leq \Pr\left[\mathbb{E}\left(\sum_{j=1}^{m} Y_j\right) - \sum_{j=1}^{m} Y_j \geq m\zeta_{\mathcal{I}}\right] \tag{5.27}$$

$$\leq \Pr\left[\mathbb{E}\left(\frac{1}{(\frac{1}{2}-\zeta)n}\sum_{j=1}^{m} Y_j\right) - \frac{1}{(\frac{1}{2}-\zeta)n}\sum_{j=1}^{m} Y_j \geq \zeta_{\mathcal{I}}\right] \tag{5.28}$$

$$\leq e^{-2(\frac{1}{2}-\zeta)n\zeta_{\mathcal{I}}^2} \tag{5.29}$$

$$= \exp\left[-2(\tfrac{1}{2}-\zeta)n\left(\frac{\ln\epsilon^{-1}}{2\left(\frac{1}{2}-\zeta\right)n}\right)\right] \tag{5.30}$$

$$= e^{-\ln(\frac{1}{\epsilon})} = \epsilon. \tag{5.31}$$

Now, we know that $\frac{d}{n} \geq p_{\text{err}} + 2\zeta_{\mathcal{I}} + e_2(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}})$ except with probability at most ϵ from Equation (5.24).

By Hoeffding's inequality 2.15

$$c_2 \leq \left(p_2 + \sqrt{\frac{\ln(\epsilon^{-1})}{2N}}\right)N \leq \left(p_2 + \sqrt{\frac{\ln(\epsilon^{-1})}{2n}}\right)N, \tag{5.32}$$

except with probability at most ϵ, where we used that $N \geq n$ in the second inequality. From Lemma 5.3.2, we know $n \geq \mathcal{F}N$ except with probability at most ϵ.

Thus, except with probability at most 2ϵ,

$$e_2 \geq \frac{c_2}{n}. \tag{5.33}$$

Combining this we find that except with probability at most 3ϵ

$$\frac{d}{n} \geq p_{\text{err}} + 2\zeta_{\mathcal{I}} + \frac{c_2}{n}(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}}). \tag{5.34}$$

With this, we can write that $m\left(\frac{d-c}{n-c} - \zeta_{\mathcal{I}}\right) \geq (p_{\text{err}} + \zeta_{\mathcal{I}})m$. Thus $\Pr[W \leq (p_{\text{err}} + \zeta_{\mathcal{I}})m] \leq \epsilon$.

The event that Alice cheats without Bob detecting it, happens either if $W \leq (p_{\text{err}} + \zeta_{\mathcal{I}})m$ or if $\frac{d}{n} < p_{\text{err}} + 2\zeta_{\mathcal{I}} + \frac{c_2}{n}(1 - p_{\text{err}} - 2\zeta_{\mathcal{I}})$. The first event occurs with probability at most ϵ and the second event occurs with probability at most 3ϵ. Thus the protocol is 4ϵ-binding. □

5.3.2. Sketch for security for Alice

When Bob is dishonest, we assume that he controls the measurement station and thus that Alice sends her states directly to him. Following the proof for security for Alice by Ribeiro and Wehner [1], we first try to derive a bound on Bob's min-entropy of Alice's string $X_{\mathcal{S}}$ given the coherent state sent by Alice and the basis choices she used, which she reveals after step 4 in the Preparation phase of the protocol.

To bound the min-entropy, we will first derive a bound on the probability that Bob can guess Alice's bit X_j, given the coherent state from Alice in round $j \in [N]$ and her basis choice Θ_j. Alice can send one of the four different states given in Table 5.2.

A dishonest Bob without any quantum memory has to perform a measurement on the coherent state that Alice sends before he receives Θ_j. There are four distinct measurement outcomes Bob can obtain, which can be used to make a prediction of X_j (denoted as $\hat{X}_j$), after receiving Θ_j. This measurement can be

	X_j	Θ_j
$\|\alpha\rangle$	0	0
$\|-\alpha\rangle$	1	0
$\|i\alpha\rangle$	0	1
$\|-i\alpha\rangle$	1	1

Table 5.2: The four different coherent states Alice can send, given her bit X_j and basis Θ_j.

$\hat{X}_j$	$\Theta_j = 0$	$\Theta_j = 1$
M_0	0	0
M_1	1	0
M_2	0	1
M_3	1	1

Table 5.3: Bob's guess $\hat{X}_j$ of Alice's bit X_j given his measurement outcome and the corresponding basis that Alice reveals afterwards.

described as $\mathcal{M} = \{M_0, M_1, M_2, M_3\}$, where M_0, M_1, M_2, M_3 are positive semidefinite operators, such that $M_0 + M_1 + M_2 + M_3 = \mathbb{1}_4$. Bob prediction $\hat{X}_j$ for each possible measurement outcome is given in Table 5.3.

Bob's probability of correctly guessing Alice's bit X_j (i.e. when $\hat{X}_j = X_j$) is

$$\begin{aligned} P_{\text{guess}}(X_j) &= \tfrac{1}{4}\mathsf{Tr}[(M_0 + M_2)|\alpha\rangle\langle\alpha| + (M_1 + M_3)|-\alpha\rangle\langle-\alpha| \\ &\quad + (M_0 + M_1)|i\alpha\rangle\langle i\alpha| + (M_2 + M_3)|-i\alpha\rangle\langle-i\alpha|] \qquad (5.35) \\ &= \tfrac{1}{4}\mathsf{Tr}[M_0(|\alpha\rangle\langle\alpha| + |i\alpha\rangle\langle i\alpha|) + M_1(|-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha|) \\ &\quad + M_2(|\alpha\rangle\langle\alpha| + |-i\alpha\rangle\langle-i\alpha|) + M_3(|-\alpha\rangle\langle-\alpha| + |-i\alpha\rangle\langle-i\alpha|)] \qquad (5.36) \end{aligned}$$

We define the maximum guessing probability for X_j to be

$$\begin{aligned} \Omega := \max_{\substack{0\leq M_0,M_1,M_2,M_3\leq\mathbb{1} \\ M_0+M_1+M_2+M_3=\mathbb{1}}} & \tfrac{1}{4}\mathsf{Tr}[M_0(|\alpha\rangle\langle\alpha| + |i\alpha\rangle\langle i\alpha|) + M_1(|-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha|) \\ & + M_2(|\alpha\rangle\langle\alpha| + |-i\alpha\rangle\langle-i\alpha|) + M_3(|-\alpha\rangle\langle-\alpha| + |-i\alpha\rangle\langle-i\alpha|)] \qquad (5.37) \end{aligned}$$

Since each round of transmission in the Preparation phase is statistically i.i.d.,

$$P_{\text{guess}}(X)_{\max} = \prod_{i=1}^{N} P_{\text{guess}}(X_j)_{\max} = \Omega^N. \qquad (5.38)$$

What Bob is interested to know, however, is the string $X_{\mathcal{S}}$ that Alice keeps after the Preparation phase.

Let $\mathcal{G}$ be the guessing strategy with which dishonest Bob (with no quantum memory) guesses $X_{\mathcal{S}}$ with the maximum probability. Define Bob's strategy $\mathcal{G}'$ to guess X as follows. Bob will use strategy $\mathcal{G}$ to predict $X_{\mathcal{S}}$, and use coin tosses to predict the $N - n$ bits in $X_{[N]\setminus\mathcal{S}}$. Thus we have that

$$\begin{aligned} P_{\text{guess}}(X)_{\mathcal{G}'} &\leq P_{\text{guess}}(X)_{\max} = \Omega^N \qquad (5.39) \\ P_{\text{guess}}(X_{\mathcal{S}})_{\mathcal{G}}\ (\tfrac{1}{2})^{N-n} &\leq \Omega^N \qquad (5.40) \\ P_{\text{guess}}(X_{\mathcal{S}})_{\mathcal{G}} &\leq \Omega^N\ 2^{N-n}. \qquad (5.41) \\ & \qquad (5.42) \end{aligned}$$

We can now write Bob's min-entropy per bit on Alice's string $X_{\mathcal{S}}$.

$$\begin{aligned} \frac{1}{n}H_{\min}(X_{\mathcal{S}}|B\Theta) &= -\frac{1}{n}\log P_{\text{guess}}(X_{\mathcal{S}})_{\max} \qquad (5.43) \\ &\geq -\frac{1}{n}\log[\Omega^N\ 2^{N-n}] \qquad (5.44) \\ &= -\frac{1}{n}\log\left[(2\Omega)^{\frac{n}{f}}\ 2^{-n}\right] \qquad (5.45) \end{aligned}$$

$$= -\frac{1}{n}\left[\frac{n}{f}\log(2\Omega) - n\log 2\right] \tag{5.46}$$

$$= -\frac{1}{f}\log(2\Omega) + 1 \tag{5.47}$$

$$\geq -\frac{1}{\mathcal{F}}\log(2\Omega) + 1 \tag{5.48}$$

In Equation (5.45) we used the fraction of successful measurements $f := \frac{n}{N}$ to substitute $N = n/f$ and in Equation (5.48) we used Lemma 5.3.2 to bound $f \geq \mathcal{F}$.

Up until now, we assumed that Bob has no quantum memory. Let Q be Bob's quantum memory such that $\log\dim(Q) \leq D$. Then we can use the min-entropy chain rule to write

$$\frac{1}{n}H_{\min}(X_{\mathcal{S}}|QB\Theta) = \frac{1}{n}H_{\min}(X_{\mathcal{S}}|B\Theta) - \frac{1}{n}\log\dim(Q) \tag{5.49}$$

$$\geq -\frac{1}{\mathcal{F}}\log(2\Omega) + 1 - \frac{1}{n}\log\dim(Q) \tag{5.50}$$

$$\geq -\frac{1}{\mathcal{F}}\log(2\Omega) - \frac{D}{n} + 1 = \lambda \tag{5.51}$$

Lemma 5.3.4 (Security for Alice against dishonest Bob (based on [1, Lemma IV.8]))**.** *Let $0 < \epsilon < 1$. Let Q be Bob's quantum memory such that $\log\dim(Q) \leq D$. Let* C *be a random $[n, k, d]$-linear code. If n satisfies*

$$\lambda - 1 + \frac{k}{n} > 0 \quad \textit{and} \quad n \geq \frac{\ell + 2\log(\frac{1}{2\epsilon})}{\lambda - 1 + \frac{k}{n}}. \tag{5.52}$$

If Alice is honest, then the protocol is 3ϵ-hiding.

Proof. Using Equation (5.51) and Equation (2.10) we find that after the Commit phase, Bob's entropy on Alice's string $X_{\mathcal{S}}$ is

$$H_{\min}(X_{\mathcal{S}}|QB\Theta\mathsf{Syn}(X_{\mathcal{S}})) \geq -\frac{1}{\mathcal{F}}\log(2\Omega) - \frac{D}{n} + 1 - n + k, \tag{5.53}$$

where the length of the syndrome $\mathsf{Syn}(X_{\mathcal{S}})$ is $n-k$. Combining this with the Leftover Hash Lemma 2.1.2 gives

$$\rho_{C,QB\Theta\mathsf{Syn}(X_{\mathcal{S}})} \approx_{\epsilon'} \tau_C \otimes \rho_{QB\Theta\mathsf{Syn}(X_{\mathcal{S}})}, \tag{5.54}$$

where τ_C is the maximally mixed state on C, and

$$\epsilon' = 2\epsilon + \tfrac{1}{2}2^{-\frac{1}{2}(H_{\min}(X_{\mathcal{S}}|QB\Theta\mathsf{Syn}(X_{\mathcal{S}}))-\ell)}. \tag{5.55}$$

If $\lambda - 1 + \frac{k}{n} > 0$, then by choosing n sufficiently large we can have $\epsilon' \leq 3\epsilon$, meaning that Protocol 5.3.1 is 3ϵ-hiding. □

Finding a lower bound on λ

Note that λ is a function of Ω. Hence, we first find an upper bound on Ω (as a function of the intensity $|\alpha|^2$).

Theorem 5.3.5. *Assume Alice transmits a coherent state $|\alpha\rangle, |-\alpha\rangle, |i\alpha\rangle$ or $|-i\alpha\rangle$ as in step 1 of the Preparation phase of Protocol 5.3.1 for each round $j \in [N]$. Then the maximum probability that Bob, with no quantum memory, predicts X_j (after receiving Θ_j from Alice) correctly is bounded as*

$$\Omega \leq \Omega_u := \min\left[1, \frac{1}{2} + \frac{1}{\sqrt{2}}(A_0A_1 + A_1A_2 + A_0A_3 + A_2A_3)\right], \tag{5.56}$$

where A_0, A_1, A_2 and A_3 are functions of α given by

$$A_0 = e^{-\frac{|\alpha|^2}{2}}\sqrt{\frac{\cosh|\alpha|^2 + \cos|\alpha|^2}{2}}, \tag{5.57}$$

$$A_1 = e^{-\frac{|\alpha|^2}{2}}\sqrt{\frac{\sinh|\alpha|^2 + \sin|\alpha|^2}{2}}, \tag{5.58}$$

$$A_2 = e^{-\frac{|\alpha|^2}{2}} \sqrt{\frac{\cosh|\alpha|^2 - \cos|\alpha|^2}{2}}, \tag{5.59}$$

$$A_3 = e^{-\frac{|\alpha|^2}{2}} \sqrt{\frac{\sinh|\alpha|^2 - \sin|\alpha|^2}{2}}. \tag{5.60}$$

The proof of this theorem is given in Appendix D. The plot of Ω as a function of $|\alpha|^2$ is given in Figure 5.3.

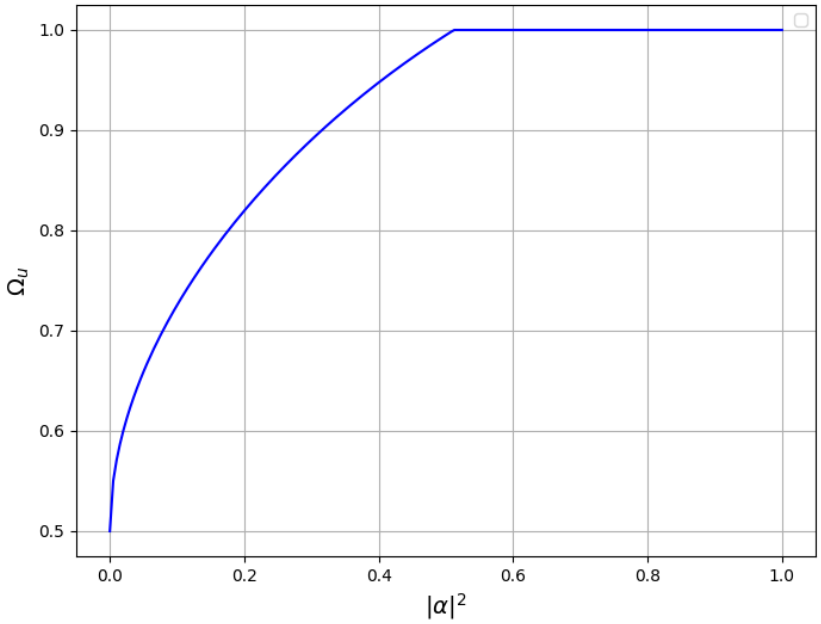

Figure 5.3: Plot of the bound Ω_u on Bob's $P_{\text{guess}}(X_i)$ as a function of the amplitude of Alice's coherent pulses α

We use this bound on Ω to get a bound on λ,

$$\lambda = -\frac{1}{\mathcal{F}}\log(2\Omega) - \frac{D}{n} + 1 \tag{5.61}$$

$$\geq -\frac{1}{\mathcal{F}}\log(2\Omega_u) - \frac{D}{n} + 1 \tag{5.62}$$

$$=: \lambda_L. \tag{5.63}$$

We plot λ_L in the asymptotic case ($N \to \infty$) as a function of $|\alpha|^2$ (with $p_{\text{fail}} = e^{-2|\alpha|^2}$) in Figure 5.4. Note that λ_L is negative for any $|\alpha|^2$. If we can find a better bound on Ω, which leads to a positive lower bound on λ, this will give us a secure phase-encoded MDI-RSC protocol. However, this is still an open challenge.

5.4. Discussion

In this chapter we presented a phase-encoded MDI-RSC protocol along with a sketch of a security proof. However, the security for Alice depends upon the parameter Ω. Finding a good upper bound on Ω which completes the security proof is still an open challenge.

It is also important to note that the security proof for Bob relies on the assumption that Alice is only semi-honest. Specifically, this means that during the Preparation and Commit phases of the protocol, she will act like an honest party, and only in the Open phase she will use the extra knowledge she has from controlling the measurement station, to convince Bob to accept a different string than the one she initially committed to.

If Alice is fully dishonest, however, she can act strategically during the Preparation and Commit phases. Similar to dishonest Bob in the security proof for Alice, she can perform different measurements to gain knowledge

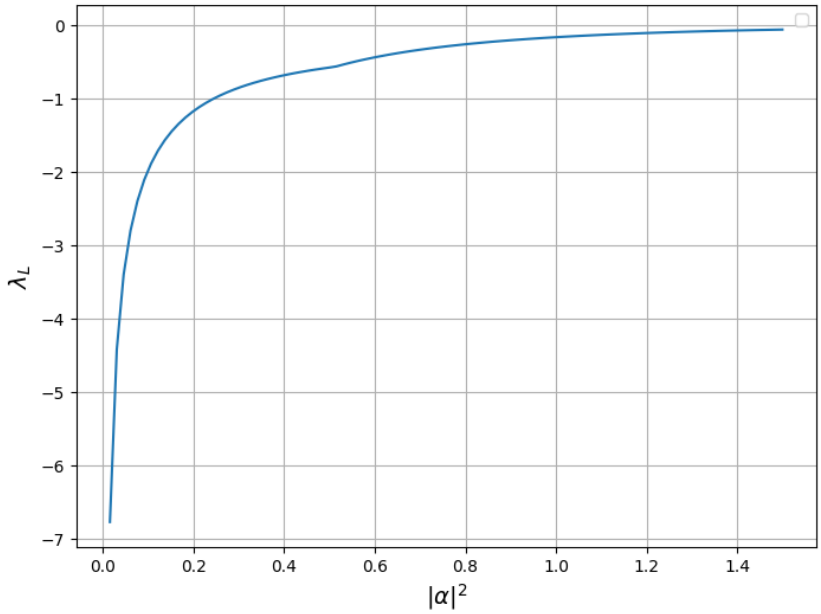

Figure 5.4: Plot of λ_L in the asymptotic case ($N \to \infty$) as a function of $|\alpha|^2$.

about the bases Bob used and his string $\hat{X}$. Security proofs for Bob in other works [10, 1] use a virtual scenario where dishonest Alice instead sends half of an EPR pair to Bob and use this to give the security proof. For a full security proof for Bob for phase-encoded MDI-RSC, this approach can also be explored.

5.4.1. Application to OT

A key challenge in implementing MDI-OT with realistic physical sources comes from the unavoidable multi-photon states that will occur. As highlighted in [1], protocols that rely on non-ideal single-photon sources are vulnerable to attack where a dishonest party can extract additional information from the quantum communication rounds, thereby violating the security guarantees of OT.

Phase-encoded MDI protocols, inspired by TF-QKD, offer several practical advantages that have been discussed in this chapter. However, phase encoding introduces an inherent basis-dependent flaw [22]. The value of a phase-encoded state is directly tied to the choice of basis. Physical imperfections in the source, such as small variations in intensity or phase modulation errors, can also leak partial information about which basis was used. Unlike polarisation-encoded states, phase-encoded weak coherent pulses naturally encode some basis information in their physical degrees of freedom. An adversary capable of exploiting this leakage could probabilistically distinguish rounds that were encoded in different phases and gain partial knowledge about the transmitted string. These two effects of multi-photon leakage in weak coherent pulses and the unavoidable basis-dependent information in phase encoding, create the same challenges for implementing secure OT.

6

Conclusions and recommendations for future work

This thesis investigated the feasibility and security of Measurement-Device-Independent Randomised String Commitment (MDI-RSC) protocols under realistic assumptions, motivated by the work of Ribeiro and Wehner [1]. The three main research goals of this study were:

1. to analyse achievable committed string rates when implementing MDI-RSC with realistic sources such as weak coherent pulses (WCP) and spontaneous parametric down-conversion (SPDC) sources,
2. to evaluate the impact of heralding in SPDC-based implementations, and
3. to explore the design and security of a phase-encoded MDI-RSC protocol inspired by Twin-Field QKD.

The contributions of this thesis are summarised here and their limitations discussed.

First, we identified and corrected a practical error in the existing MDI-RSC protocols by properly bounding the relevant variables. This bound ensures that the original security claims remain valid, while removing the error.

Secondly, we quantitatively analysed achievable committed string rates for WCP and SPDC sources using decoy states. Both sources achieve comparable performance, with effective committed string rates on the order of 10^{-7} bits per communication round in optimal regimes. We also explored the potential of heralded SPDC sources, showing that they could in principle provide advantages, though realistic imperfections in local detectors must be considered. These imperfections in the local detectors can still cause heralded single photon sources to emit multi-photon states and require the use of a protocol that deals with this, for example via the decoy states technique. A realistic implementation of heralded SPDC with non-ideal local detectors and the use of decoy states was not considered in this thesis.

Furthermore, the assumption of perfect central measurement devices was adopted in this thesis to focus on source imperfections. In practice, detector efficiency, dark counts, and alignment errors in the measurement station will also affect protocol performance and must be incorporated into a full implementation analysis.

Finally, we designed and analysed a phase-encoded MDI-RSC protocol using coherent states, motivated by techniques from Twin-Field QKD. A sketch for security proof for Alice was established in the bounded-storage model. The full proof of security for Alice is still an open problem. We further discussed why extending this approach to Oblivious Transfer (OT) remains difficult due to multi-photon leakage and inherent basis dependence in phase-encoded coherent states. This suggests that the challenges identified in Ribeiro and Wehner [1] persist in this new setting.

Building on the contributions and limitations identified in this thesis, several directions for future research can be identified.

- Min-entropy with phase-encoding: A positive lower bound for the min-entropy still needs to be obtained for a full security proof. We can study the various approaches from [23, 24, 25, 26, 27] to find a bound which works for our protocol.

- Incorporating imperfect measurement devices: A full performance and security analysis of MDI-RSC protocols should include realistic imperfections of the central measurement station, extending beyond the idealised assumptions made here.
- Heralded SPDC with non-ideal detectors: The analysis of heralded SPDC sources should be extended to account for detector efficiency and dark counts, building on models such as those of Wehner et al. [9]. This would clarify whether heralding can provide a genuine practical advantage.
- Towards Twin-Field RSC: It will be interesting to investigate whether the full Twin-Field regime can be adapted to Randomised String Commitment. A key challenge will be to incorporate phase randomisation without introducing a separation between parameter-estimation and key-generation rounds.
- Extending security proof for Bob: For phase-encoded MDI-RSC, completing the full security proof for Bob without the semi-honest assumption remains an important problem. Exploring the virtual-entanglement-based proof techniques that are applied in related works, is recommended as an initial direction.

In conclusion, this thesis demonstrates that Measurement-Device-Independent Randomised String Commitment is feasible under realistic source assumptions and highlights both the promise and the challenges of adapting Twin-Field-QKD-inspired techniques to two-party cryptography. This work contributes to bridging the gap between theoretical constructions and realistic implementations, by identifying practical parameter regimes and proposing a novel phase-encoded MDI-RSC protocol using coherent states.

References

[1] Jérémy Ribeiro and Stephanie Wehner. *On Bit Commitment and Oblivious Transfer in Measurement-Device Independent settings*. Use of Bell measurements for MDI communications. Apr. 2020.

[2] Peter W Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *AT&T Research* (1996), pp. 124–134.

[3] Joe Kilian. "Founding Cryptography on Oblivious Transfer". In: *Proceedings of the twentieth annual ACM Symposium on Theory of Computing* (Jan. 1988), pp. 20–31. doi: https://doi.org/10.1145/62212.62215.

[4] Charles H. Bennett et al. "Practical Quantum Oblivious Transfer". In: *Advances in Cryptology — CRYPTO '91*. Ed. by Joan Feigenbaum. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 351–366. isbn: 978-3-540-46766-3.

[5] Dominic Mayers. "Unconditionally Secure Quantum Bit Commitment is Impossible". In: *Phys. Rev. Lett.* 78 (17 Apr. 1997), pp. 3414–3417. doi: 10.1103/PhysRevLett.78.3414. url: https://link.aps.org/doi/10.1103/PhysRevLett.78.3414.

[6] Hoi-Kwong Lo and H. F. Chau. "Is Quantum Bit Commitment Really Possible?" In: *Phys. Rev. Lett.* 78 (17 Apr. 1997), pp. 3410–3413. doi: 10.1103/PhysRevLett.78.3410. url: https://link.aps.org/doi/10.1103/PhysRevLett.78.3410.

[7] Hoi-Kwong Lo and H.F. Chau. "Why quantum bit commitment and ideal quantum coin tossing are impossible". In: *Physica D: Nonlinear Phenomena* 120.1 (1998). Proceedings of the Fourth Workshop on Physics and Consumption, pp. 177–187. issn: 0167-2789. doi: https://doi.org/10.1016/S0167-2789(98)00053-0. url: https://www.sciencedirect.com/science/article/pii/S0167278998000530.

[8] Ivan B Damgård et al. "Cryptography In the Bounded Quantum-Storage Model". In: *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science - FOCS 2005* (2005), pp. 449–458. url: https://doi.org/10.48550/arXiv.quant-ph/0508222.

[9] Stephanie Wehner et al. "Implementation of two-party protocols in the noisy-storage model". In: *Physical Review A - Atomic, Molecular, and Optical Physics* 81 (5 May 2010). Use of BB84 states, Alice sends, Bob measures. issn: 10941622. doi: 10.1103/PhysRevA.81.052336.

[10] Robert König, Stephanie Wehner, and Jürg Wullschleger. *Unconditional security from noisy quantum storage*. 2011.

[11] Nelly Huei Ying Ng et al. "Experimental implementation of bit commitment in the noisy-storage model". In: *Nature Communications* 3 (2012), p. 1326. issn: 20411723. doi: 10.1038/ncomms2268.

[12] Jędrzej Kaniewski and Stephanie Wehner. "Device-independent two-party cryptography secure against sequential attacks". In: *New Journal of Physics* 18.5 (May 2016), p. 055004. doi: 10.1088/1367-2630/18/5/055004. url: https://dx.doi.org/10.1088/1367-2630/18/5/055004.

[13] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution". In: (May 2012). doi: 10.1103/PhysRevLett.108.130503. url: http://arxiv.org/abs/1109.1473%20http://dx.doi.org/10.1103/PhysRevLett.108.130503.

[14] M. Lucamarini et al. "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters". In: *Nature* 557 (7705 May 2018), pp. 400–403. issn: 14764687. doi: 10.1038/s41586-018-0066-6.

[15] Renato Renner. "Security of Quantum Key Distribution". PhD thesis. Swiss Federal Institute of Technology, 2006.

[16] Wassily Hoeffding. "Probability Inequalities for Sums of Bounded Random Variables". In: *Journal of the American Statistical Association* 58.301 (1963), pp. 13–30. doi: 10.1080/01621459.1963.10500830. eprint: https://www.tandfonline.com/doi/pdf/10.1080/01621459.1963.10500830. url: https://www.tandfonline.com/doi/abs/10.1080/01621459.1963.10500830.

[17] Timothé Bramas. “New primitives for secure function evaluations using quantum communication”. MSc thesis. TU Delft, 2025.

[18] Xiongfeng Ma and Mohsen Razavi. “Alternative schemes for measurement-device-independent quantum key distribution”. In: (Dec. 2012). doi: 10.1103/PhysRevA.86.062319. url: http://arxiv.org/abs/1204.4856%20http://dx.doi.org/10.1103/PhysRevA.86.062319.

[19] J. Calsamiglia and N. Lütkenhaus. “Maximum efficiency of a linear-optical Bell-state analyzer”. In: *Applied Physics B: Lasers and Optics* 72 (1 2001), pp. 67–71. issn: 09462171. doi: 10.1007/s003400000484.

[20] Marcos Curty, Koji Azuma, and Hoi Kwong Lo. “Simple security proof of twin-field type quantum key distribution protocol”. In: *npj Quantum Information* 5 (1 Dec. 2019). issn: 20566387. doi: 10.1038/s41534-019-0175-6.

[21] Xiao Peng Liu et al. “Efficient twin-field quantum key distribution with heralded single-photon source”. In: *Physica A: Statistical Mechanics and its Applications* 608 (Dec. 2022). issn: 03784371. doi: 10.1016/j.physa.2022.128228.

[22] Kiyoshi Tamaki et al. “Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw”. In: *Physical Review A - Atomic, Molecular, and Optical Physics* 85 (4 Apr. 2012). issn: 10502947. doi: 10.1103/PhysRevA.85.042307.

[23] Manuel A Ballester, Stephanie Wehner, and Andreas Winter. “State discrimination with post-measurement information”. In: *IEEE Transactions on Information Theory* 54.9 (2008), pp. 4183–4198.

[24] Nelly Huei Ying Ng, Mario Berta, and Stephanie Wehner. “A min-entropy uncertainty relation for finite size cryptography”. In: (May 2014). doi: 10.1103/PhysRevA.86.042315. url: http://arxiv.org/abs/1205.0842%20http://dx.doi.org/10.1103/PhysRevA.86.042315.

[25] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner. “Entanglement sampling and applications”. In: (June 2015). doi: 10.1109/TIT.2014.2371464. url: http://arxiv.org/abs/1305.1316%20http://dx.doi.org/10.1109/TIT.2014.2371464.

[26] Fabian Furrer, Christian Schaffner, and Stephanie Wehner. “Continuous-Variable Protocols in the Noisy-Storage Model”. In: (Sept. 2015). url: http://arxiv.org/abs/1509.09123.

[27] Ioannis Petrongonas and Erika Andersson. “Optimal Discrimination of Mixed Symmetric Multi-mode Coherent States”. In: (Oct. 2024). url: http://arxiv.org/abs/2410.11632.

[28] Leonard Mandel and Emil Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.

[29] Pieter Kok and Samuel L Braunstein. *Postselected versus nonpostselected quantum teleportation using parametric down-conversion*. Derivation of probability to create n entangled pairs from a PDC source. 2000.

[30] Michael A. Nielsen, Isaac Chuang, and Lov K. Grover. *Quantum Computation and Quantum Information*. 2002, pp. 287–297. isbn: 9781107002173. doi: 10.1119/1.1463744.

[31] Dmitry Makarov. *Theory for the Beam Splitter in Quantum Optics: Quantum Entanglement of Photons and Their Statistics, HOM Effect*. Dec. 2022. doi: 10.3390/math10244794.

[32] Carl D. Meyer. *Matrix analysis and applied linear algebra*. Siam, Society for industrial and applied mathematics, 2000, pp. 566–567.

A

Spontaneous Parametric Down Conversion

Spontaneous parametric down-conversion (SPDC) is a non-linear optical process used to generate entangled photon pairs. It occurs when a high-energy *pump* photon passes through a non-linear optical medium and spontaneously splits into two lower-energy photons: the *signal* and the *idler*. This process conserves both energy and momentum, expressed as:

$$E_p = E_s + E_i, \tag{A.1}$$
$$\vec{p}_p = \vec{p}_s + \vec{p}_i, \tag{A.2}$$

where $E = \hbar\omega$ is the photon energy and $\vec{p} = \hbar\vec{k}$ is the photon momentum, with ω the angular frequency and $\vec{k}$ the wave vector. The emission angles of the signal and idler photons are determined by the conservation of momentum.

There are several types of SPDC, distinguished by the polarisation of the output photons. In type-0 SPDC, the signal, idler and pump photon have the same polarisation. In type-I SPDC, the signal and idler photon share polarisation that is orthogonal to the pump photon. In type-II SPDC, the signal and idler photons have orthogonal polarisations and emerge in an entangled state. This the type that we are interested in. The resulting quantum state is a two-mode squeezed vacuum state, which can be written in the Fock basis as:

$$|\psi\rangle = \sqrt{1-\xi^2}\sum_{n=0}^{\infty} \xi^n \left|n\right\rangle_s \left|n\right\rangle_i ,$$

where $\xi := \tanh r$, with r being the squeezing parameter related to the pump amplitude. The Fock states $\left|n\right\rangle_s$ and $\left|n\right\rangle_i$ represent n photons in the signal and idler modes, respectively. This expression shows that the signal and idler modes are perfectly photon-number correlated.

The probability of having n photons per mode is

$$P(n) = (1-\xi^2)\xi^{2n}. \tag{A.3}$$

Using that $|\xi^2| < 1$ and the sum $\sum_{n=0}^{\infty} nx^n = \frac{x}{(1-x)^2}$ for $|x| < 1$, the mean photon number per mode is

$$\bar{n} = \sum_{n=0}^{\infty} nP(n) = \frac{\xi^2}{1-\xi^2}, \tag{A.4}$$

which can be rewritten to express ξ in terms of $\bar{n}$, i.e.,

$$\xi^2 = \frac{\bar{n}}{1+\bar{n}}. \tag{A.5}$$

Substituting this into the expression for $P(n)$, we find

$$P(n) = \frac{\bar{n}^n}{(1+\bar{n})^{n+1}}, \tag{A.6}$$

which corresponds to a Bose-Einstein distribution, common for thermal photon statistics [28].

Now consider the detailed structure of the quantum state produced in type-II SPDC. When post-selecting on events where exactly n photon pairs are created, the shared signal-idler state can be written in the computational basis as [29, 9]:

$$|\Phi_n\rangle = \sum_{m=0}^{n} \frac{(-1)^m}{\sqrt{n+1}} |n-m, m\rangle_s |m, n-m\rangle_i . \tag{A.7}$$

This state includes all possible symmetric arrangements of the n photons in each of the polarization modes, and reflects the entangled nature of the type-II PDC process.

Since each n-photon-pair state $|\Phi_n\rangle$ has $(n+1)$ possible mode arrangements, the total probability $P(n)$ of observing n photons per mode in the output must incorporate this multiplicity. Therefore the probability becomes:

$$P(n) = N_{\bar{n}} \frac{(n+1)\bar{n}^n}{(1+\bar{n})^{n+1}}, \tag{A.8}$$

where $N_{\bar{n}}$ is a normalisation constant to make sure that the probabilities sum to 1. To compute $N_{\bar{n}}$, we evaluate the sum:

$$\begin{aligned}\sum_{n=0}^{\infty} P(n) &= \sum_{n=0}^{\infty} N_{\bar{n}} \frac{(n+1)\bar{n}^n}{(\bar{n}+1)^{n+1}} = \frac{1}{1+\bar{n}} N_{\bar{n}} \sum_{n=0}^{\infty} (n+1) \left(\frac{\bar{n}}{1+\bar{n}}\right)^n \\ &= \frac{1}{1+\bar{n}} N_{\bar{n}} \sum_{n=0}^{\infty} (n+1)(\xi^2)^n.\end{aligned}$$

Since $\xi^2 < 1$, this final sum is a standard power series:

$$\sum_{n=0}^{\infty} (n+1)x^n = \frac{1}{(1-x)^2}, \quad |x| < 1. \tag{A.9}$$

Setting $x = \xi^2 = \frac{\bar{n}}{1+\bar{n}}$, we get

$$\sum_{n=0}^{\infty} P(n) = \frac{N_{\bar{n}}}{1+\bar{n}} \frac{1}{(1-\xi^2)^2}. \tag{A.10}$$

Since $1 - \xi^2 = \frac{1}{1+\bar{n}}$, this simplifies to

$$\sum_{n=0}^{\infty} P(n) = N_{\bar{n}}(1+\bar{n}) \tag{A.11}$$

Thus, the normalisation constant must be $N_{\bar{n}} = \frac{1}{1+\bar{n}}$ and the final expression for the photon number distribution per modes becomes:

$$p_{\text{PDC}}(n, \bar{n}) = \frac{(n+1)\bar{n}^n}{(1+\bar{n})^{n+2}}, \tag{A.12}$$

or expressed in the intensity of the pulse μ, we define $\mu = 2\bar{n}$ to write (as in Wehner et al. [9]):

$$p_{\text{PDC}}(n, \mu) = \frac{(n+1)(\mu/2)^n}{(1+\mu/2)^{n+2}}. \tag{A.13}$$

B

Beamsplitter transformations

In TF-QKD and in the phase-encoded MDI-RSC discussed in this work, Alice and Bob have identical setups that send photon states to a central node, which consists of a beamsplitter (BS) with threshold detectors at its two output modes. A lossless BS is represented by a unitary operator $\hat{B}$ characterised by its angle θ, which relates to the orientation of the half-silvered mirror in the physical BS. The BS acts on the two input modes and, in the Heisenberg picture, the annihilation operators transform as (e.g. [30]):

$$\hat{B}a\hat{B}^\dagger = a\cos\theta + b\sin\theta, \quad \hat{B}b\hat{B}^\dagger = -a\sin\theta + b\cos\theta. \tag{B.1}$$

The unitary transformation of the BS on the two input and two output modes is given [31]:

$$\begin{pmatrix} \hat{a}_{\text{out}} \\ \hat{b}_{\text{out}} \end{pmatrix} = \hat{B} \begin{pmatrix} \hat{a}_{\text{in}} \\ \hat{b}_{\text{in}} \end{pmatrix}.$$

Conservation of photon number (and thus the bosonic commutation relations) requires that the transformation matrix $\hat{B}$ be unitary. A general form for the beamsplitter matrix is given by

$$\hat{B} = \begin{pmatrix} \sqrt{T} & e^{i\phi}\sqrt{R} \\ -e^{-i\phi}\sqrt{R} & \sqrt{T} \end{pmatrix},$$

where $T = \cos^2\theta$ and $R = \sin^2\theta$ are the transmission and reflection coefficients satisfying $T + R = 1$, and ϕ is a phase shift.

For a 50:50 beamsplitter we have $\theta = \pi/4$, so that $T = R = \frac{1}{2}$. If we choose the phase $\phi = 0$ (a common convention [31]), the matrix simplifies to

$$\hat{B} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

This matrix explicitly shows that the two input modes are mixed equally. The minus sign in the lower left element ensures the unitarity of $\hat{B}$ and reflects the phase difference between the two outputs. One output port corresponds to constructive interference, while the other corresponds to destructive interference. The transformation of the creation operators through a 50:50 BS are given as

$$\hat{B}\,\hat{a}^\dagger\hat{B}^\dagger = \tfrac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{b}^\dagger), \quad \hat{B}\,\hat{b}^\dagger\hat{B}^\dagger = \tfrac{1}{\sqrt{2}}(-\hat{a}^\dagger + \hat{b}^\dagger). \tag{B.2}$$

Alternate representations are possible (e.g., setting $\phi = \pi/2$ may lead to factors of i in the matrix elements), but the physical content remains the same as long as unitarity and the relation $T + R = 1$ are maintained [31].

We will analyse the action of a 50:50 beamsplitter on different input quantum states. First, we look at single-photon and two-photon interference in the BS. Then we consider the case of a Fock state with n photons in one mode and vacuum in the other. Then, we present a theorem with proof showing that a coherent state input results in coherent state outputs with appropriately scaled amplitudes.

Single-photon interference Suppose we have a single photon in input mode a and vacuum states in all other modes. We analyse the single photon interference of this photon in the 50:50 BS. The state is $|\psi\rangle_{\text{in}} = \hat{a}^\dagger |00\rangle$ and becomes

$$|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{b}^\dagger) |00\rangle .$$

The single photon is after the 50:50 BS in equal superposition of being at the a or b mode.

Two-photon interference Suppose we have a single photon in input mode a and in input mode b. We analyse the two-photon interference of these photons in the 50:50 BS. The state is $|\psi\rangle_{\text{in}} = \hat{a}^\dagger \hat{b}^\dagger |00\rangle$ and becomes

$$\begin{aligned} |\psi\rangle_{\text{out}} &= \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{b}^\dagger)\frac{1}{\sqrt{2}}(-\hat{a}^\dagger + \hat{b}^\dagger) |00\rangle \\ &= \frac{1}{2}(-\hat{a}^\dagger\hat{a}^\dagger - \hat{b}^\dagger\hat{a}^\dagger + \hat{a}^\dagger\hat{b}^\dagger + \hat{b}^\dagger\hat{b}^\dagger) |00\rangle \\ &= \frac{1}{2}(-\hat{a}^\dagger\hat{a}^\dagger + \hat{b}^\dagger\hat{b}^\dagger) |00\rangle , \end{aligned}$$

a superposition of both photons emerging together at the a or b mode. Here we used that creation operators of different modes commute.

Fock state transformation Let $\hat{B}$ be the unitary beamsplitter operator (with inverse $\hat{B}^\dagger$) and consider the input state where mode a contains a Fock state $|n\rangle$ and mode b is in the vacuum state:

$$|\Psi_{\text{in}}\rangle = |n, 0\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}} |0, 0\rangle .$$

The output state is given by

$$|\Psi_{\text{out}}\rangle = \hat{B} |n, 0\rangle .$$

Under the beamsplitter transformation the creation operator in mode a transforms as

$$\hat{B}\hat{a}^\dagger\hat{B}^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{b}^\dagger\right) .$$

Thus, one may write

$$\hat{B}(\hat{a}^\dagger)^n |0, 0\rangle = \left[\frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{b}^\dagger\right)\right]^n |0, 0\rangle .$$

Expanding via the binomial theorem, we have

$$\begin{aligned} \hat{B}(\hat{a}^\dagger)^n |0, 0\rangle &= \frac{1}{2^{n/2}} \sum_{k=0}^{n} \binom{n}{k} (\hat{a}^\dagger)^k (\hat{b}^\dagger)^{n-k} |0, 0\rangle \\ &= \frac{1}{2^{n/2}} \sum_{k=0}^{n} \binom{n}{k} |k, n-k\rangle . \end{aligned}$$

The output state becomes then, with normalisation factor $N = \sqrt{\frac{n!2^n}{\binom{2n}{n}}}$,

$$\begin{aligned} |\Psi_{\text{out}}\rangle &= N\frac{1}{\sqrt{n!}}\frac{1}{2^{n/2}} \sum_{k=0}^{n} \binom{n}{k} |k, n-k\rangle \\ &= \sqrt{\frac{1}{\binom{2n}{n}}} \sum_{k=0}^{n} \binom{n}{k} |k, n-k\rangle \end{aligned}$$

Thus, Fock states are divided over the two outputs, by the 50:50 BS.

Transformation of coherent states Coherent states $|\alpha\rangle$ are defined as the eigenstates of the annihilation operator,

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

and can be expanded in the Fock basis as

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

We now assume that the coherent state is input in mode a while mode b is in the vacuum:

$$|\Psi_{\text{in}}\rangle = |\alpha, 0\rangle .$$

Lemma B.0.1. *A coherent state input $|\alpha, 0\rangle$ to a 50:50 beamsplitter yields coherent state outputs in both output modes with amplitudes scaled by a factor of $1/\sqrt{2}$.*

Proof. Starting with the coherent state in mode a,

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

the beamsplitter transformation gives

$$|\Psi_{\text{out}}\rangle = \hat{B} |\alpha, 0\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} \left[\frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{b}^\dagger)\right]^n |0, 0\rangle .$$

Expanding the nth power by the binomial theorem,

$$|\Psi_{\text{out}}\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{1}{n!} \left(\frac{\alpha}{\sqrt{2}}\right)^n \sum_{k=0}^{n} \binom{n}{k} (\hat{a}^\dagger)^k (\hat{b}^\dagger)^{n-k} |0, 0\rangle .$$

Changing the summation index by letting $m = n - k$, the double sum can be rearranged as

$$|\Psi_{\text{out}}\rangle = \left[e^{-|\alpha|^2/2} \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{\alpha}{\sqrt{2}} \hat{a}^\dagger\right)^k\right] \left[e^{-|\alpha|^2/2} \sum_{m=0}^{\infty} \frac{1}{m!} \left(\frac{\alpha}{\sqrt{2}} \hat{b}^\dagger\right)^m\right] |0, 0\rangle .$$

Recognizing each bracket as the expansion of a coherent state, we obtain

$$|\Psi_{\text{out}}\rangle = |\alpha/\sqrt{2}\rangle_a \otimes |\alpha/\sqrt{2}\rangle_b ,$$

which shows that the output modes are in coherent states with amplitudes $\alpha/\sqrt{2}$. □

Thus a coherent state at one input is divided equally by the 50:50 BS, like classical light. We will now analyse what happens when we input two arbitrary coherent states, by using the beamsplitters transformation on the annihilation operators. With the transformation of the creation operators given in Equation (B.2), the output annihilation operators are given by

$$\hat{a}_{\text{out}} = \tfrac{1}{\sqrt{2}}(\hat{a}_{\text{in}} + \hat{b}_{\text{in}}), \quad \hat{b}_{\text{out}} = \tfrac{1}{\sqrt{2}}(-\hat{a}_{\text{in}} + \hat{b}_{\text{in}}). \tag{B.3}$$

First consider putting two coherent states with the same amplitude and phase

$$|\Psi_{\text{in}}\rangle = |\alpha e^{i\theta}\rangle_a \otimes |\alpha e^{i\theta}\rangle_b .$$

Since coherent states are eigenstates of the annihilation operator, we have

$$\hat{a}_{\text{in}} |\alpha e^{i\theta}\rangle_a = \alpha e^{i\theta} |\alpha e^{i\theta}\rangle_a , \quad \hat{b}_{\text{in}} |\alpha e^{i\theta}\rangle_b = \alpha e^{i\theta} |\alpha e^{i\theta}\rangle_b ,$$

To find the eigenvalues of the output modes, we use linearity of the transformation to write

$$\hat{a}_{\text{out}} |\Psi_{\text{in}}\rangle = \tfrac{1}{\sqrt{2}}(\hat{a}_{\text{in}} + \hat{b}_{\text{in}}) |\alpha e^{i\theta}\rangle_a \otimes |\alpha e^{i\theta}\rangle_b = \tfrac{1}{\sqrt{2}}(\alpha e^{i\theta} + \alpha e^{i\theta}) |\Psi_{\text{in}}\rangle = \sqrt{2}\alpha e^{i\theta} |\Psi_{\text{in}}\rangle .$$

Thus the state in output mode a becomes a coherent state with eigenvalue $\sqrt{2}\alpha e^{i\theta}$.

$$\hat{b}_{\text{out}} |\Psi_{\text{in}}\rangle = \tfrac{1}{\sqrt{2}}(-\hat{a}_{\text{in}} + \hat{b}_{\text{in}}) |\alpha e^{i\theta}\rangle_a \otimes |\alpha e^{i\theta}\rangle_b = \tfrac{1}{\sqrt{2}}(-\alpha e^{i\theta} + \alpha e^{i\theta}) |\Psi_{\text{in}}\rangle = 0.$$

So mode b ends up in the vacuum state. Since coherent states are uniquely determined by their eigenvalues, the output state is

$$|\Psi_{\text{out}}\rangle = |\sqrt{2}\alpha e^{i\theta}\rangle_a \otimes |0\rangle_b \,.$$

Now we consider two different coherent states in the input modes:

$$|\Psi_{\text{in}}\rangle = |\alpha e^{i\theta_a}\rangle_a \otimes |\beta e^{i\theta_b}\rangle_b \,.$$

We can simply use the same transformations of the annihilation operators given in Equation (B.3) and the fact that coherent states are eigenstates of the annihilation operators to write

$$|\Psi_{\text{out}}\rangle = |\tfrac{1}{\sqrt{2}}(\alpha e^{i\theta_a} + \beta e^{i\theta_b})\rangle_a \otimes |\tfrac{1}{\sqrt{2}}(-\alpha e^{i\theta_a} + \beta e^{i\theta_b})\rangle_b \,.$$

Thus we conclude that, when Alice and Bob send coherent states to the central node, this results in a deterministic click in output mode a when their states have the same amplitude and phase, and in a deterministic click in output mode b when their states have the same amplitude and a phase difference of $\Delta\theta = \pi$. For all other coherent input states, the click pattern of the output detectors is determined by some probability distribution that depends on the input states.

Threshold detection and coherent states

An ideal single-photon threshold detector clicks if it detects one or more photons, but does not resolve how many photons there were. It is assumed to have efficiency $\eta = 1$ and no dark counts, $p_{\text{dark}} = 0$

The probability of there being no photons in coherent state $|\beta\rangle$ is $p(0) = e^{-|\beta|^2}$. Thus the probability that an ideal threshold detector clicks in the presence of the coherent state is

$$p_{\text{click}} = 1 - p(0) = 1 - e^{-|\beta|^2} \tag{B.4}$$

C

Formal definition of Randomised String Commitment

The protocols for RSC that we show in this work consist of 3 phases: Preparation, Commit and Open. In the Preparation phase, Alice and Bob do their quantum communication. After that, they only need to perform classical computations and communications with the information they have to do RSC. This happens in the Commit and Open phase of the protocol. We may write the Commit and the Open protocol as CPTPMs $\mathcal{C}_{AB}$ and $\mathcal{O}_{AB}$ respectively, consisting of the local actions of honest Alice and Bob, together with any operations they may perform on messages that are exchanged. When both parties are honest, the output of the Commit protocol will be a state

$$\mathcal{C}_{AB}(\rho_{\mathsf{in}}) = \rho_{CAB} \tag{C.1}$$

for some fixed input state ρ_{in}, where the committed string $C \in \{0,1\}^\ell$ is, the classical output of Alice, and A and B are the internal states of Alice and Bob respectively. If Alice is dishonest, she may not follow the protocol, and we use $\mathcal{C}_{A'B}$ to denote the resulting map. Note that $\mathcal{C}_{A'B}$ may not have output C, and we hence simply write $\rho_{A'B}$ for the resulting output state, where A' denotes the register of a dishonest Alice. Similarly, we use $\mathcal{C}_{AB'}$ to denote the CPTPM corresponding to the case where Bob is dishonest, and write $\rho_{CAB'}$ for the resulting output state, where B' denotes the register of a dishonest Bob.

The Open protocol can be described similarly. If both parties are honest, the map $\mathcal{O}_{AB} : \mathcal{B}(\mathcal{H}_{AB}) \to \mathcal{B}(\mathcal{H}_{\hat{C}F})$ creates the state

$$\rho_{C\hat{C}F} := (\mathbb{1}_C \otimes \mathcal{O}_{AB})(\rho_{CAB}), \tag{C.2}$$

where $\hat{C} \in \{0,1\}^\ell$ and $F \in \{\mathsf{accept}, \mathsf{reject}\}$ is the classical output of Bob. Again, if Alice is dishonest, we write $\mathcal{O}_{A'B}$ to denote the resulting CPTPM with output $\rho_{A''\hat{C}F}$, and if Bob is dishonest, we write $\mathcal{O}_{AB'}$ for the resulting CPTPM with output $\rho_{CB''}$.

We formalise the RSC introduced above in the following definition.

Definition C.0.1 (Randomised string commitment [10])**.** Let τ_R denote the maximally mixed state on a register R. An (ℓ, ϵ)-Randomised String Commitment scheme is a protocol between Alice and Bob that satisfies the following three properties.
Correctness: When both parties are honest, then there exists an ideal state σ_{CCF} such that

- The distribution of C is uniform and Bob accepts the commitment:

$$\sigma_{CF} := \tau_{\{0,1\}^\ell} \otimes |\mathit{accept}\rangle\langle\mathit{accept}|_F, \tag{C.3}$$

- The real state produced by the protocol $\rho_{C\hat{C}F}$ is ϵ-close to the ideal state:

$$\rho_{C\hat{C}F} \approx_\epsilon \sigma_{CCF}, \tag{C.4}$$

  where we identify (A, B) with $(C, \hat{C}F)$.

Security for Alice: When Alice is honest, for any joint state $\rho_{CB'}$ created in the Commit phase, Bob is ignorant about C before the Open phase:

$$\rho_{CB'} \approx_\epsilon \tau_{\{0,1\}^\ell} \otimes \rho_{B'}. \tag{C.5}$$

The protocol is then said to be ϵ-hiding.

Security for Bob: After the Commit phase and before the Open phase, there exists an ideal state σ_{CAB} such that for any Open algorithm, described by $\mathcal{O}_{AB}$, in which Bob is honest, we have:

- Bob almost never accepts $\hat{C} \neq C$:
  for $\rho_{CA''\hat{C}F} = (\mathbb{1}_C \otimes \mathcal{O}_{A'B})(\sigma_{CA'B})$ we have $\Pr[\hat{C} \neq C \text{ and } F = \text{ accept}] \leq \epsilon$.
- The real state produced by the commitment phase is ϵ-close to the ideal state:

$$\rho_{A'B} \approx_\epsilon \sigma_{A'B}. \tag{C.6}$$

The protocol is then said to be ϵ-binding.

D

Auxiliary proofs for Section 5.3

Proof of Lemma 5.3.2

Proof. Given that Alice did not abort the protocol in step 4 of the Preparation phase, we know that $f \leq p_{\text{fail}} + \sqrt{\frac{\ln(\epsilon^{-1})}{2N}}$ except with probability at most ϵ. This gives then

$$N - n - p_{\text{fail}} N - \sqrt{\frac{\ln(\epsilon^{-1})}{2}}\sqrt{N} \leq 0 \tag{D.1}$$

$$(1 - p_{\text{fail}})N - \sqrt{\frac{\ln(\epsilon^{-1})}{2}}\sqrt{N} - n \leq 0 \tag{D.2}$$

$$(1 - p_{\text{fail}})\frac{N}{n} - \sqrt{\frac{\ln(\epsilon^{-1})}{2n}}\sqrt{\frac{N}{n}} - 1 \leq 0. \tag{D.3}$$

Using the quadratic equation, we find

$$\sqrt{\frac{N}{n}} \leq \frac{\sqrt{\frac{\ln(\epsilon^{-1})}{2n}} + \sqrt{\frac{\ln(\epsilon^{-1})}{2n} + 4(1 - p_{\text{fail}})}}{2(1 - p_{\text{fail}})} \tag{D.4}$$

$$\leq \frac{\sqrt{\frac{\ln(\epsilon^{-1})}{2n}} + \sqrt{\frac{\ln(\epsilon^{-1})}{2n} + 4(1 - p_{\text{fail}}) + 2\sqrt{\frac{\ln(\epsilon^{-1})}{2n}}\left(2\sqrt{1 - p_{\text{fail}}}\right)}}{2(1 - p_{\text{fail}})} \tag{D.5}$$

$$= \frac{\sqrt{\frac{\ln(\epsilon^{-1})}{2n}} + \sqrt{\left(\sqrt{\frac{\ln(\epsilon^{-1})}{2n}} + 2\sqrt{1 - p_{\text{fail}}}\right)^2}}{2(1 - p_{\text{fail}})} \tag{D.6}$$

$$= \frac{\sqrt{\frac{\ln(\epsilon^{-1})}{2n}} + \sqrt{1 - p_{\text{fail}}}}{1 - p_{\text{fail}}}. \tag{D.7}$$

Invert this fraction to find

$$\sqrt{\frac{n}{N}} \geq \frac{1 - p_{\text{fail}}}{\sqrt{1 - p_{\text{fail}}} + \sqrt{\frac{\ln(\epsilon^{-1})}{2n}}} \tag{D.8}$$

$$= \frac{\sqrt{1 - p_{\text{fail}}}}{1 + \sqrt{\frac{\ln(\epsilon^{-1})}{2(1-p_{\text{fail}})n}}} \tag{D.9}$$

$$\frac{n}{N} \geq \frac{1 - p_{\text{fail}}}{(1 + \zeta_{\text{fail}})^2}. \tag{D.10}$$

□

Proof of Theorem 5.3.5

Proof. We can express, for $\omega \in \{1, -1, i, -1\}$,

$$|\omega\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{j=0}^{\infty} \frac{\omega^j \alpha^j}{\sqrt{j!}} |j\rangle \tag{D.11}$$

$$= e^{-\frac{|\alpha|^2}{2}} \left(\sum_{j=0,4,8,\ldots}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle + \omega \sum_{j=1,5,9,\ldots}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle + \omega^2 \sum_{j=2,6,10,\ldots}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle + \omega^3 \sum_{j=3,7,11,\ldots}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle \right) \tag{D.12}$$

$$= A_0 |\varphi_0\rangle + \omega A_1 |\varphi_1\rangle + \omega^2 A_2 |\varphi_2\rangle + \omega^3 A_3 |\varphi_3\rangle \tag{D.13}$$

where $A_k |\varphi_k\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{j=0}^{\infty} \frac{\alpha^{4j+k}}{(4j+k)!} |4j+k\rangle$, with $\{|\varphi_k\rangle\}_{k=0}^{3}$ a set of orthonormal pure states and A_k given by

$$A_0 = e^{-\frac{|\alpha|^2}{2}} \sqrt{\sum_{j=0}^{\infty} \frac{(|\alpha|^2)^{4j}}{(4j)!}} = e^{-\frac{|\alpha|^2}{2}} \sqrt{\frac{\cosh|\alpha|^2 + \cos|\alpha|^2}{2}} \tag{D.14}$$

$$A_1 = e^{-\frac{|\alpha|^2}{2}} \sqrt{\sum_{j=0}^{\infty} \frac{(|\alpha|^2)^{4j+1}}{(4j+1)!}} = e^{-\frac{|\alpha|^2}{2}} \sqrt{\frac{\sinh|\alpha|^2 + \sin|\alpha|^2}{2}} \tag{D.15}$$

$$A_2 = e^{-\frac{|\alpha|^2}{2}} \sqrt{\sum_{j=0}^{\infty} \frac{(|\alpha|^2)^{4j+2}}{(4j+2)!}} = e^{-\frac{|\alpha|^2}{2}} \sqrt{\frac{\cosh|\alpha|^2 - \cos|\alpha|^2}{2}} \tag{D.16}$$

$$A_3 = e^{-\frac{|\alpha|^2}{2}} \sqrt{\sum_{j=0}^{\infty} \frac{(|\alpha|^2)^{4j+3}}{(4j+3)!}} = e^{-\frac{|\alpha|^2}{2}} \sqrt{\frac{\sinh|\alpha|^2 - \sin|\alpha|^2}{2}} \tag{D.17}$$

The expression of the four coherent states in this manner is similar to that in Petrongonas and Andersson [27, Equation D.21]. Simply, we can express Alice's states in the basis $\{|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_2\rangle, |\varphi_3\rangle\}$.

$$|\alpha\rangle = A_0 |\varphi_0\rangle + A_1 |\varphi_1\rangle + A_2 |\varphi_2\rangle + A_3 |\varphi_3\rangle \tag{D.18}$$

$$|-\alpha\rangle = A_0 |\varphi_0\rangle - A_1 |\varphi_1\rangle + A_2 |\varphi_2\rangle - A_3 |\varphi_3\rangle \tag{D.19}$$

$$|i\alpha\rangle = A_0 |\varphi_0\rangle + iA_1 |\varphi_1\rangle - A_2 |\varphi_2\rangle - iA_3 |\varphi_3\rangle \tag{D.20}$$

$$|-i\alpha\rangle = A_0 |\varphi_0\rangle - iA_1 |\varphi_1\rangle - A_2 |\varphi_2\rangle + iA_3 |\varphi_3\rangle \tag{D.21}$$

and we can also express

$$\rho_\omega = |\omega\alpha\rangle\langle\omega\alpha| = \sum_{k,m=0}^{3} \omega^k (\omega^m)^* A_k A_m |\varphi_k\rangle \langle\varphi_m| \tag{D.22}$$

$$= \sum_{k,m=0}^{3} \omega^{k-m} A_k A_m |\varphi_k\rangle \langle\varphi_m| \tag{D.23}$$

$$= \begin{bmatrix} A_0^2 & A_0 A_1 \omega^{-1} & A_0 A_2 \omega^{-2} & A_0 A_3 \omega^{-3} \\ A_1 A_0 \omega & A_1^2 & A_1 A_2 \omega^{-1} & A_1 A_3 \omega^{-2} \\ A_2 A_0 \omega^2 & A_2 A_1 \omega^1 & A_2^2 & A_2 A_3 \omega^{-1} \\ A_3 A_0 \omega^3 & A_3 A_1 \omega^2 & A_3 A_2 \omega^1 & A_3^2 \end{bmatrix} \tag{D.24}$$

and, for any $\omega \in \{1, -1, i, -i\}$,

$$(\rho_\omega + \rho_{i\omega}) = \begin{bmatrix} 2A_0^2 & A_0 A_1 (\omega - i\omega) & 0 & A_0 A_3 (\omega + i\omega) \\ A_1 A_0 (\omega + i\omega) & 2A_1^2 & A_1 A_2 (\omega - i\omega) & 0 \\ 0 & A_2 A_1 (\omega + i\omega) & 2A_2^2 & A_2 A_3 (\omega - i\omega) \\ A_3 A_0 (\omega - i\omega) & 0 & A_3 A_2 (\omega + i\omega) & 2A_3^2 \end{bmatrix}. \tag{D.25}$$

Since M_k are positive semidefinite $M_k^{(nm)} = (M_k^{(nm)})^*$, we can write,

$$
\begin{aligned}
&\mathsf{Tr}[M_k(\rho_{\omega_k}+\rho_{i\omega_k})]\\
&= M_k^{(00)}2A_0^2 + M_k^{(01)}A_1A_0(\omega_k+i\omega_k) + M_k^{(02)}A_2A_0(\omega_k^2+(i\omega_k)^2) + M_k^{(03)}A_3A_0(\omega_k^3+(i\omega_k)^3)\\
&\quad + M_k^{(10)}A_0A_1(\omega_k^{-1}+(i\omega_k)^{-1}) + M_k^{(11)}2A_1^2 + M_k^{(12)}A_2A_1(\omega_k+i\omega_k) + M_k^{(13)}A_3A_1(\omega_k^2+(i\omega_k)^2)\\
&\quad + M_k^{(20)}A_0A_2(\omega_k^{-2}+(i\omega_k)^{-2}) + M_k^{(21)}A_1A_2(\omega_k^{-1}+(i\omega_k)^{-1}) + M_k^{(22)}2A_2^2 + M_k^{(23)}A_3A_2(\omega_k+i\omega_k)\\
&\quad + M_k^{(30)}A_0A_3(\omega_k^{-3}+(i\omega_k)^{-3}) + M_k^{(31)}A_1A_3(\omega_k^{-2}+(i\omega_k)^{-2}) + M_k^{(32)}A_2A_3(\omega_k^{-1}+(i\omega_k)^{-1}) + M_k^{(33)}2A_3^2
\end{aligned}
\tag{D.26}
$$

$$
\begin{aligned}
&= 2A_0^2M_k^{(00)} + 2A_1^2M_k^{(11)} + 2A_2^2M_k^{(22)} + 2A_3^2M_k^{(33)}\\
&\quad + 2A_0A_1\Re(M_k^{(01)}(\omega_k+i\omega_k)) + 2A_1A_2\Re(M_k^{(12)}(\omega_k+i\omega_k))\\
&\quad + 2A_0A_3\Re(M_k^{(03)}(\omega_k+i\omega_k)) + 2A_2A_3\Re(M_k^{(23)}(\omega_k+i\omega_k))
\end{aligned}
\tag{D.27}
$$

$$
\begin{aligned}
&\leq 2A_0^2M_k^{(00)} + 2A_1^2M_k^{(11)} + 2A_2^2M_k^{(22)} + 2A_3^2M_k^{(33)}\\
&\quad + 2A_0A_1\sqrt{2}|M_k^{(01)}| + 2A_1A_2\sqrt{2}|M_k^{(12)}| + 2A_0A_3\sqrt{2}|M_k^{(03)}| + 2A_2A_3\sqrt{2}|M_k^{(23)}|
\end{aligned}
\tag{D.28}
$$

$$
\begin{aligned}
&\leq 2A_0^2M_k^{(00)} + 2A_1^2M_k^{(11)} + 2A_2^2M_k^{(22)} + 2A_3^2M_k^{(33)}\\
&\quad + 2A_0A_1\sqrt{2}\sqrt{M_k^{(00)}M_k^{(11)}} + 2A_1A_2\sqrt{2}\sqrt{M_k^{(11)}M_k^{(22)}}\\
&\quad + 2A_0A_3\sqrt{2}\sqrt{M_k^{(00)}M_k^{(33)}} + 2A_2A_3\sqrt{2}\sqrt{M_k^{(22)}M_k^{(33)}}
\end{aligned}
\tag{D.29}
$$

For the inequality in Equation (D.28) we used that the last four terms can be simplified as follows, for example,

$$
\Re(M_0^{(01)}(1+i)) \leq |M_0^{(01)}(1+i)| = |M_0^{(01)}||1+i| = \sqrt{2}|M_0^{(01)}|, \tag{D.30}
$$

and similarly for the other terms. For the inequality in Equation (D.29) we used the fact that for positive semidefinite matrices $M_k^{(nn)}M_k^{(mm)} - |M_k^{(nm)}|^2 \geq 0$ and thus $|M_k^{(nm)}| \leq \sqrt{M_k^{(nn)}M_k^{(mm)}}$ [32, property 7.6.12]. Note that $M_0^{(nn)} + M_1^{(nn)} + M_2^{(nn)} + M_3^{(nn)} = 1$ by the definition of the POVM.

The total guessing probability becomes

$$
P_{\mathsf{guess}}(X_j) = \tfrac{1}{4}\mathsf{Tr}[M_0(\rho_1+\rho_i) + M_1(\rho_{-1}+\rho_i) + M_2(\rho_1+\rho_{-i}) + M_3(\rho_{-1}+\rho_{-i})] \tag{D.31}
$$

$$
\begin{aligned}
&\leq \tfrac{1}{2}\Big(A_0^2 + A_1^2 + A_2^2 + A_3^2\\
&\quad + A_0A_1\sqrt{2}\sum_{k=0}^{3}\sqrt{M_k^{(00)}M_k^{(11)}} + A_1A_2\sqrt{2}\sum_{k=0}^{3}\sqrt{M_k^{(11)}M_k^{(22)}}\\
&\quad + A_0A_3\sqrt{2}\sum_{k=0}^{3}\sqrt{M_k^{(00)}M_k^{(33)}} + A_2A_3\sqrt{2}\sum_{k=0}^{3}\sqrt{M_k^{(22)}M_k^{(33)}}\Big)
\end{aligned}
\tag{D.32}
$$

$$
\begin{aligned}
&\leq \tfrac{1}{2}\Big[A_0^2 + A_1^2 + A_2^2 + A_3^2\\
&\quad + A_0A_1\sqrt{2}\sqrt{\sum_{k=0}^{3}M_k^{(00)}}\sqrt{\sum_{k=0}^{3}M_k^{(11)}} + A_1A_2\sqrt{2}\sqrt{\sum_{k=0}^{3}M_k^{(11)}}\sqrt{\sum_{k=0}^{3}M_k^{(22)}}\\
&\quad + A_0A_3\sqrt{2}\sqrt{\sum_{k=0}^{3}M_k^{(00)}}\sqrt{\sum_{k=0}^{3}M_k^{(33)}} + A_2A_3\sqrt{2}\sqrt{\sum_{k=0}^{3}M_k^{(22)}}\sqrt{\sum_{k=0}^{3}M_k^{(33)}}\Big]
\end{aligned}
\tag{D.33}
$$

$$
= \tfrac{1}{2}\Big[A_0^2 + A_1^2 + A_2^2 + A_3^2 + \sqrt{2}(A_0A_1 + A_1A_2 + A_0A_3 + A_2A_3)\Big] \tag{D.34}
$$

$$
= \frac{1}{2} + \frac{1}{\sqrt{2}}(A_0A_1 + A_1A_2 + A_0A_3 + A_2A_3) \tag{D.35}
$$

In the second inequality, we used the Cauchy-Schwarz inequality for the last four terms. Since this bound holds for any choice of M_0, M_1, M_2 and M_3, it also holds for the optimal choice. This gives the bound on the

maximum guessing probability

$$P_{\mathsf{guess}}(X_j)_{\max} \leq \frac{1}{2} + \frac{1}{\sqrt{2}}(A_0A_1 + A_1A_2 + A_0A_3 + A_2A_3). \tag{D.36}$$

□