New primitives for secure function evaluations using quantum communication

by

Timothé Bramas

to obtain the degree of Master of Science
at the Delft University of Technology

Thesis defense:
July 3rd 2025

Student Number: 6081436
Master Track: Computer Science, Cybersecurity Specialization
Project duration: November 2024 - July 2025
Thesis Committee: Dr. Zeki Erkin
Dr. Stephanie Wehner
Dr. Tim Coopmans (external member)

Abstract

Cryptography is used everywhere in our society, from simple internet searches to providing security and privacy for our banking systems. A key research area in this field is secure function evaluation, where multiple parties compute a function of their inputs, without revealing them to each other. However, as most cryptographic tasks, current implementations often rely on computational assumptions, which may become insecure in the future. Researchers have explored quantum communications to eliminate such computational assumptions since the 80s, but still challenges remain. For instance, many theoretical protocols using quantum communications rely on perfect single-photon sources. However, in practice, photon sources have a small probability of emitting multiple photons in one pulse, potentially leaking information to a dishonest party. Furthermore, a dishonest party could have secretly tempered the measurement device of the other party and potentially introduced a backdoor in it. The so-called "measurement device independent" setting has then been described, to provide security against this kind of attacks.

In this work, we investigate the possibility of achieving two secure function evaluation primitives - oblivious transfer and bit commitment - in the measurement device independent setting, using imperfect single-photon sources. We already know that under this setting, bit commitment is possible to achieve but oblivious transfer seems hard to achieve. It is still an open question if there exist a protocol to achieve oblivious transfer under this setting. If not, it would be interesting to find new achievable primitives other than oblivious transfer. Here, we study the existing protocols and provide some results towards answering these questions. We start by extending an existing result on the difficulty of achieving oblivious transfer by proving that even a weaker version of this primitive is difficult to achieve under such setting. We also shortly explore the possibility of using an existing reduction from oblivious transfer to bit commitment to see whether we can achieve oblivious transfer from the existing bit commitment protocol. Finally, we show that an existing bit commitment protocol can perform at a better rate by giving a slightly modified security proof.

Acknowledgment

This thesis project serves as the conclusion of my experience as a Master's student at TU Delft. I have spent two amazing years studying computer science and cybersecurity, for which I will forever be grateful. I would like to first express my gratitude towards Zeki and Stephanie, who have been two great supervisors, as well as Kaushik for his truly helpful daily supervision and support. I also want to thank Prof. Tim Coopmans for being part of my thesis committee. Thanks also to Juliette, who has done her master thesis on a similar topic, for helping me out with her knowledge in physics and for the interesting discussions we had regarding this difficult topic. I am also grateful towards Dr. Romain Alléaume and Guillaume Ricard, who gave me an entry point in quantum cryptography, during my research internship back in Télécom Paris. I would also like to thank every person in the Wehner group for their help and the really nice and safe working environment they built. I also want to express my gratitude to Antoine, Apolline, Camille, Franck, Nadine, Léo, Thibault and Laura for their support throughout this project, my studies and in my overall life.

Contents

Chapter 1

Introduction

1.1 Secure Function Evaluation

Secure Function Evaluation (SFE) tasks are crucial in our society, as they allow several (untrusted) parties, each holding an input, to jointly compute functions of these inputs without revealing their own inputs to other parties.

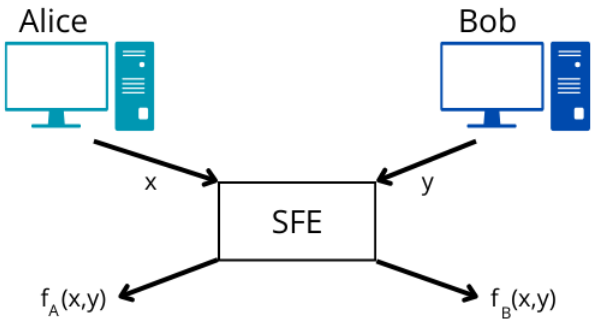


Figure 1.1: *A general two-party Secure Function Evaluation (SFE). At the start of the protocol, Alice holds the value x and Bob holds the value y. At the end of the SFE, Alice knows $f_A(x, y)$ and Bob knows $f_B(x, y)$. Alice does not learn more about y than what $f_A(x, y)$ reveals and Bob does not learn more about x than what $f(x, y)$ reveals.*

Oblivious Transfer (OT) and Bit Commitment (BC) are two central cryptographic primitives that can allow us to build more advanced SFEs. It has been shown [1] that oblivious transfer is universal, in the sense that if one has access to an oblivious transfer protocol, they can build a protocol to implement any given two-party SFE (including BC), using only classical communication. In addition, it is known that using quantum communications, one can produce an OT protocol given a BC protocol [2]. With this and the fact the OT is universal, the two primitives are then in a quantum communication regime: we can go from one to another.

However, OT and BC are both impossible to achieve using only classical communication. Assumptions regarding the computational power of the opponent have to be made to obtain a secure protocol [3]. This protocol makes the so-called Diffie-Hellman assumption, which is based on the complexity of computing discrete logarithms in cyclic groups. This assumption holds very well against attackers with classical computers, but things get trickier when the adversary is allowed to use quantum computers. For example, Shor's algorithm [4] is a period-finding algorithm which can be used to compute discrete logarithms in polynomial time [5], which is not possible using classical computers.

The use of quantum computers to break classical cryptosystems has been thought of theoretically for decades, which encouraged the development of Quantum Key Distribution (QKD) [6] - a primitive that allows to securely

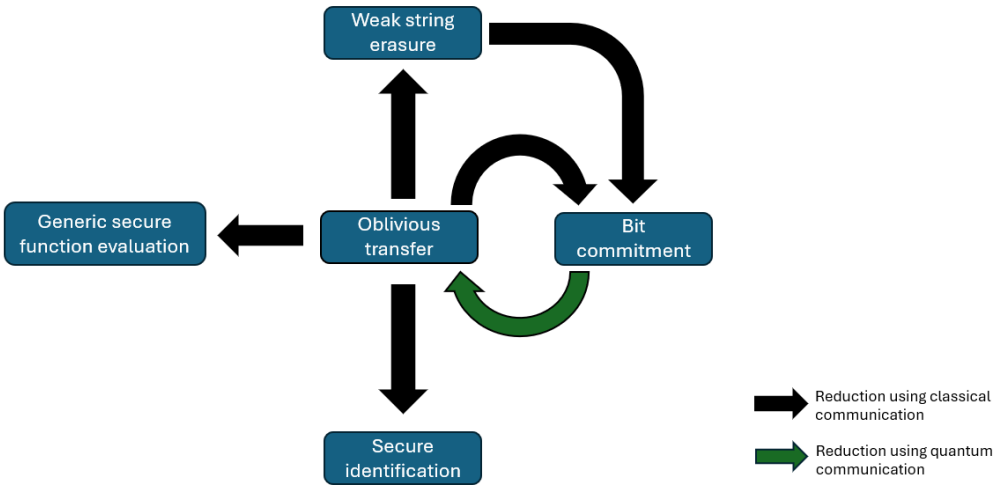


Figure 1.2: *Reductions between various secure function evaluation primitives*

distribute keys later used for one-time pad encryption between two parties - without making the same computational assumptions as for instance the Diffie-Hellman key exchange algorithm. One difference between QKD and two-party SFEs is that in a QKD protocol we evaluate the security against a malicious man-in-the-middle attacker - Eve - who can listen and interfere over the communications, whereas for SFE we consider that one party is honest and evaluate the security of the protocol assuming that the other party is malicious.

1.2 Quantum protocols for SFE

Instead of only using classical communication, protocols for OT and BC using quantum communication have been studied for a few decades [2, 7, 8]. Unfortunately, information theoretically secure BC is shown to be impossible using quantum communication without any assumptions [9]. This also implies the impossibility of OT. In order to build safe protocols, researchers have been trying to limit the capabilities of a malicious party with realistic assumptions. One model that stands out regarding this issue is the limited quantum storage model. This model can be derived in two variants: bounded-storage initiated by Damgård, Fehr, Salvail and Schaffner [10] and the noisy storage introduced by Wehner, Schaffner and Terhal [11]. A bounded-storage means that malicious Bob can perfectly store a limited amount of qubits. The noisy storage means that malicious Bob can store his qubits only with a high noise, resulting in the loss of some qubits after a period of time. In a noisy storage model the adversary will loose some of their stored qubits, and in the bounded-storage model they have to choose which qubits they store. It is shown in [12] that one can first prove the security of a protocol in the bounded-storage model to then extend it to the more general noisy storage model. The bounded/noisy storage setting provides everlasting security, meaning that the assumptions made only have to be true during the protocol, and gaining more power after the protocol does not allow to retroactively decipher the communications. This is an advantage compared to computational assumptions, where giving more power to the dishonest party after the protocol can harm the security of the protocol.

1.3 MDI setting and multiphoton emissions

The protocols proposed in the noisy or bounded storage [10, 13, 11] implicitly make an assumption that the quantum devices will always work as intended. However, some attacks can be made by tampering the quantum devices of one party [14]. In order to overcome these types of attacks, the Device Independent (DI) setting has been used to provide OT and BC protocols, which are secure even if the quantum devices (sources and measurement devices)

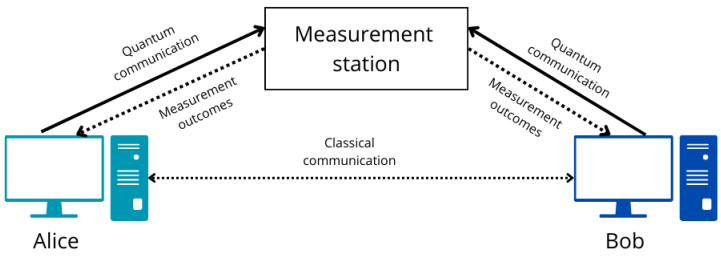


Figure 1.3: *Schematic of an Measurement Device Independent (MDI) protocol*

used are compromised [15]. A protocol for DI-OT in the bounded quantum storage model has been proposed by Broadbent and Yuen in [8]. Their work is based on a technique called self-testing [16, 17] which relies on a post-quantum computational assumption named the hardness of Learning With Errors (LWE) [18]. However, most of the attacks against devices are directed toward the measurement ones [19], which makes relevant the looser notion of Measurement Device Independence [20]. In this setting, only the measurement devices of both parties are treated as black boxes. They can be seen as a joint measurement station between Alice and Bob. Under the MDI setting, a dishonest party will have total control over the measurement station. Ribeiro et al. gave an MDI-BC protocol [21, Protocol II.1] and an MDI-OT protocol [21, Protocol II.2] in the bounded/noisy quantum storage model.

Ribeiro et al. initially consider the use of perfect single photon sources for their protocols. In a real world protocol, photon sources will have a small probability of emitting multiple photons in one pulse [22, 23], potentially leaking information to a dishonest party. For example, one commonly used photon source is Weak Coherent laser Pulses (WCP), which are cost efficient but have multi-photon emissions. Usually, the decoy states technique is used to construct quantum cryptographic protocols under multiphoton emissions [24]. Combining decoy states technique with [21, Protocol II.1] gives an MDI-BC protocol under multiphoton emissions [21, Protocol II.3]. However, problems arise while trying to find a similar protocol for MDI-OT which works with multiphoton emissions. Indeed, having imperfect sources which sometimes send multiple photons seems to leak too much information to allow for building a secure MDI-OT protocol.

1.4 Research goals

During this project, we are exploring the following research questions.

1. To what extent do multiphoton emissions harm the security of an MDI-OT protocol? Can some other OT-like primitive be securely implemented under the MDI setting with multiphoton emissions?
2. How can we reduce the negative impact of multiphoton emissions in the existing MDI-BC protocol from [21, Protocol II.3]?
3. What prevents us from using existing reduction from OT to BC [25] to build MDI-OT with imperfect photon sources from the MDI-BC protocol in [21, Protocol II.3]?

1.5 Contribution

Ribeiro et al. showed that the protocol obtained by combining decoy states technique with [21, Protocol II.2] does not securely implement OT under the MDI setting and multiphoton emissions, letting Alice (the sender) win with a probability strictly greater than $\frac{1}{2}$. However, this reasoning may suggest that it could be possible to use this protocol to build a weaker form of OT, where Alice can cheat with a probability bounded by a known value (for

instance 0.65). We then show that such a protocol can neither be used to implement such a variant of the OT primitive under the MDI setting and multiphoton emissions.

There is a known reduction from OT to BC [2], which could be used to obtain MDI-OT under multiphoton emissions from the secure MDI-BC protocol. We give a modified version of this reduction and prove its security under the MDI setting with perfect single photon sources. We show that multiphoton emissions does also harm the security of this protocol. We also give another version of this protocol to deal with bit flips during the quantum communications, but we do not prove its security here.

There is an assumption made in [21] which is that Alice guesses Bob's encoding basis (see Section 2.3.2) with probability 1 whenever Bob sends multiple photons at once. We show that we can find an upper bound on this probability which is strictly smaller than 1, allowing us not to make this assumption. We are currently looking into how can this analysis be used to reduce the number of photon transmissions needed in the MDI-BC protocol [21, Protocol II.3], by being less conservative.

1.6 Outline

Chapter 2 gives the notations and definitions required to understand the rest of the report, as well as some common concepts regarding quantum cryptography protocols. Chapter 3 is a review of related work which includes definitions of Weak String Erasure and BC primitives, as well as protocols to implement them under the MDI setting with perfect photon sources. This chapter also includes a review of the different variants of OT presented in the literature. In Chapter 4, the results obtained in this project are listed and Chapter 5 lists the potential approaches that could be explored later on.

Chapter 2

Background

This chapter should give the reader the required knowledge and definitions to understand the rest of the thesis.

2.1 Notations

We note by $\mathbb{N}$ the set of all non-negative integers, and $\mathbb{N}^* := \mathbb{N}\backslash\{0\}$ the set of all positive integers. Given $\epsilon > 0$, we note by $\log(\epsilon)$ the binary logarithm $\log_2(\epsilon) = \frac{\ln(\epsilon)}{\ln(2)}$. For a given set E, we will write $X \subseteq_U E$ if the random variable X is randomly and uniformly sampled from E.

Given a positive integer $n \geq 1$, we consider the following notations:
we note by $[n]$ the set of integers from 1 to n: $[n] := \{1, \ldots, n\}$, we write an n-bit string $X \in \{0,1\}^n$ as X_1^n, we note by $2^{[n]}$ the set of all subsets of $[n]$, we note by $\mathcal{M}_n(\mathbb{C})$ the set of all n by n matrices with complex values, and we call $\mathbb{1}_n$ the n by n identity matrix.

2.2 Definitions

Classical states The protocols that are described in this report rely on quantum communications but will also involve classical states, which can be seen as follows.

A quantum register of $m \in \mathbb{N}^*$ qubits can be described using a density matrix ρ. If a state A is classical, it can be described using the probability distribution $\{p_a(x), x \in \{0,1\}^m\}$ which is such that for any bit string $x \in \{0,1\}^m$ $p_a(x)$ is the probability that the string contained in the register A is equal to x. We can also represent bit strings from $\{0,1\}^m$ as decimal positive integers that range from 0 to $2^m - 1$. In the usual quantum bra-ket notation, the corresponding density matrix ρ_A is written as

$$\rho_A = \sum_{x=0}^{2^m-1} p_a(x)|x\rangle\langle x|. \tag{2.1}$$

We can see here that we can fully describe a classical state using either its probability distribution or its quantum density matrix.

Classical quantum states This definition comes from [26, Section 2.2.8].

If $m \in \mathbb{N}^*$ and we have two registers X_1^m and Q in which X_1^m corresponds to a classical state as defined above and Q is a generic quantum register, we call the joint state of X_1^m and Q a classical-quantum (cq) state, and its density matrix has the following form:

$$\rho_{XQ} = \sum_{x=0}^{2^m-1} \left(p_X(x)|x\rangle\langle x| \otimes \rho_x^Q\right). \tag{2.2}$$

Uniform distribution A classical register X_1^m that has a uniform probability distribution (meaning that $\forall x \in \{0,1\}^m, p_X(x) = \frac{1}{2^m}$) is in a maximally mixed state. We will call such a state τ_X, and it has the corresponding density matrix $\tau_X = \frac{1}{2^m}\sum_{x=0}^{2^m-1}|x\rangle\langle x|$.

Hermitian matrix A matrix $M \in \mathcal{M}_n(\mathbb{C})$ is called hermitian if $M^\dagger = M$, where $M^\dagger := \left(\bar{M}^T\right)$ is the conjugate transpose of M. A hermitian matrix is always diagonalizable with real eigenvalues.

Trace distance For quantum registers B and B' that have density matrices ρ_0 and ρ_1, the trace distance between them is equal to $D(B,B') = \max_{0\leq M\leq \mathbb{1}}(\mathrm{tr}(M(\rho_0-\rho_1)))$. A more suitable definition for calculations is

$$D(B,B') = \frac{1}{2}\left\|(\rho_0-\rho_1)\right\|_1 = \frac{1}{2}\mathrm{tr}\left(\sqrt{(\rho_0-\rho_1)^\dagger(\rho_0-\rho_1)}\right). \tag{2.3}$$

It is equal to half of the Schatten 1-norm of the matrix $(\rho_0-\rho_1)$, so half of the sum of its singular values.

POVM measurement A POVM measurement on an n-qubit state is given by a set of POVM elements $\{M_1, M_2, \ldots, M_\ell\}$ which satisfy the following properties:

- $\forall i$, M_i has to be hermitian and satisfy $0 \leq M_i \leq \mathbb{1}_{2^n}$
- $\sum_i M_i = \mathbb{1}_{2^n}$

ε-closeness

Let ρ, σ be two arbitrary quantum states and let $\varepsilon > 0$. We say that the two states are ε-close (in trace distance), and we note $\rho \approx_\varepsilon \sigma$, when $D(\rho,\sigma) = \frac{1}{2}\left\|(\rho-\sigma)\right\|_1 \leq \varepsilon$.

Conditional min-entropy Consider a cq state $X_1^n B$ where X_1^n is a classical register. The conditional min-entropy of the joint state $X_1^n B$ is defined as

$$\mathrm{H}_{\min}(X_1^n|B) = -\log(\mathrm{P}_{\mathrm{guess}}(X_1^n|B)), \tag{2.4}$$

where $\mathrm{P}_{\mathrm{guess}}(X_1^n|B)$ is the maximum probability that Bob who holds B guesses Alice's string X_1^n correctly.

We can see here that the more Bob knows about Alice's string, the smaller the min-entropy is. For instance, if Bob knows perfectly 10% of the string and has no information about the remaining bits, we have $\mathrm{P}_{\mathrm{guess}}(X_1^n|B) = \frac{1}{2^{0.9n}}$, and then $\mathrm{H}_{\min}(X_1^n|B) = 0.9n$.

However, min-entropy as described above is used to measure uncertainty when Bob has perfect (without errors) states, which are almost impossible in a real-world application. We then need to introduce a so-called smoothed

min-entropy, which is described in [11, 13]. In fact, instead of Bob having the ideal state B, he will have a state B' such that the trace distance (sometimes other distance metrics are used) between B and B' is smaller than a given parameter ε.

In an imperfect protocol, Bob therefore has a state $B' \in \mathscr{B}^\varepsilon(B)$ where $\mathscr{B}^\varepsilon(B)$ is defined as the set of all states B' such that $D(B, B') \leq \varepsilon$. We can now define the smooth min-entropy of Alice and Bob's state.

Smooth min-entropy Consider a cq state $X_1^n B$ where X_1^n is classical. The ε-smoothed (conditional) min-entropy of the joint state $X^n B$ is defined as

$$\mathrm{H}_{\min}^{\varepsilon}(X^n|B) = \max_{B' \in \mathscr{B}^\varepsilon(B)} \mathrm{H}_{\min}(X^n|B'). \tag{2.5}$$

Intuitively, this is the maximum min-entropy among every joint states $X^n B'$ such that B' is at most at a trace distance ε from Bob's perfect state B.

2-universal family of hash functions A family of hash functions $\mathcal{R}_\ell^n = \{r : \{0,1\}^n \to \{0,1\}^\ell\}$ is called 2-universal if for every two strings $x, x' \in \{0,1\}^n$ with $x \neq x'$ and any two $c, c' \in \{0,1\}^\ell$, we have

$$\Pr_{r \in \mathcal{R}} \left((r(x) = c) \wedge (r(x') = c')\right) = \frac{1}{2^{2\ell}}. \tag{2.6}$$

For any $r \in \mathcal{R}_\ell^n$, we refer to $r(x)$ also as $\mathrm{Ext}(x, r)$.

2.3 Ideas to understand quantum SFE protocols

This section explains a common building block for quantum cryptographic protocols called BB84 coding. There is also a small discussion on the impact of using imperfect single photon sources, especially under the Measurement Device Independent setting, and the different attack strategies that the dishonest party can use.

2.3.1 BB84 coding

This technique is called BB84 coding in reference to the quantum key distribution protocol in which it was first used [6]. In this technique, Alice and Bob are sending states encoded in two orthogonal bases, the computational basis $\{|0\rangle, |1\rangle\}$ and the Hadamard basis $\{|+\rangle, |-\rangle\} := \left\{ \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right), \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right) \right\}$. Encoding the bit $x \in \{0,1\}$ in the basis $\theta \in \{0,1\}$ then corresponds to preparing the state $|x\rangle_\theta$, where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$, $|1\rangle_1 = |-\rangle$. Measuring in one basis destroys the information on the other basis, which implies that measuring a single qubit in any basis does not allow the party to find the encoding basis: If Bob uses the first basis, from Alice's perspective it is equivalent to Bob sending $\rho_0 = \frac{1}{2}(\{|0\rangle\langle 0| + |1\rangle\langle 1|\})$, and in the second basis he sends $\rho_1 = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$ and we have $\rho_0 = \rho_1$. Therefore Alice can not know which basis Bob was chosen by Bob.

2.3.2 Multiphoton emissions under the MDI setting

The main consequence of multiphoton emissions is that they can leak to Alice information about Bob's encoding bases (and vice-versa). If only one photon was emitted, Bob can encode his random bit either in $\{|0\rangle, |1\rangle\}$ or in $\{|+\rangle, |-\rangle\}$.

If two photons are emitted, from Alice's perspective, Bob will send either $\rho_0 = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ or $\rho_1 = \frac{1}{2}(|++\rangle\langle ++| + |--\rangle\langle --|)$ which are not equal. For instance, if Alice measures two different outcomes on Bob's qubits, she will know that he did not choose the same base as her. The same happens for any number of photons emitted greater than 2.

When we are under the MDI setting, we assume that a malicious party has total control over the measurement station. Dishonest Alice or Bob could then announce every single photon emission as lost to only keep the rounds in which they have information about the other person's basis.

One technique used in quantum key distribution to deal with imperfect photon sources is the use of decoy states [24]. The aim of this technique is to allow both Alice and Bob to estimate how many multiphoton rounds have been kept compared to single photon rounds. If this number seems suspicious (too many single photon emission discarded by the measurement station), they assume that the other party tried to gain an advantage and abort the protocol. Using the decoy states technique, Alice and Bob can each choose the intensities (average number of photons sent) of a number q of decoy state intensities and the intensity of their signal states. Alice knows the value $n_1^A + n_{\geq 2}^A$ which is the number of rounds in which she used her signal intensity and the measurement station reported a successful measurement (same for Bob with $n_1^B + n_{\geq 2}^B$) but she does not know the individual values n_1^A and $n_{\geq 2}^A$, where the subscript corresponds to the number of photons sent. The decoy states technique will allow Alice and Bob to estimate lower bounds on n_1^A and n_1^B respectively using the decoy states (which gives them upper bounds on $n_{\geq 2}^A$ and $n_{\geq 2}^B$). Alice and Bob will abort the protocol if these lower bounds are below a certain threshold value. These bounds are functions of the intensities, the corresponding probabilities, and the number of rounds that were not discarded when they used each intensity. Lemma [21, Lemma IV.15] gives the analytical expressions of these lower bounds in the case where Alice and Bob use 2 different decoy intensities ($q = 2$), and [21, appendix B] gives a numerical way of computing them if $q > 2$.

2.3.3 Attacks against quantum protocols

In a typical attack strategy, the dishonest party (Alice or Bob) attaches an ancilla system to a quantum state sent by the honest party. They will then perform a unitary on the system composed of the sent state and the ancilla, to finally measure the ancilla system. When Alice and Bob are performing several quantum communication rounds, there exist 3 families of attack strategies: individual, collective and coherent attacks. A detailed description of these attacks is given for the context of quantum key distribution (where the malicious attacker is a third party Eve performing a man-in-the-middle attack) in [27, Section 5.3.1].

1. Individual attacks are the ones which give the dishonest party the least power. In this kind of attacks, the dishonest party is forced to attack every transmission individually and in the same way, they will attach the ancilla system to each state sent and measure them one by one after applying the same unitary for each round.
2. In collective attacks, the dishonest party still has to apply the same unitary to every round and they have the same ancilla state. However, they can perform a joint measurement on the ancillas obtained from all the rounds.
3. Finally, when considering coherent attacks the dishonest party is allowed to attach one ancilla system on the joint state composed of every transmission sent, to then apply a global unitary and perform a measurement on the ancilla system.

The following table (from [27, Table 5.1]) gives the ancilla state ρ_D^i (or ρ_D for coherent attacks) corresponding to each type of attacks performed by the dishonest party (Alice or Bob) $D \in \{A, B\}$ against the honest party $H = \{A, B\} \setminus D$, where we write $\mathcal{M}^1$ a POVM measurement for one system, and $\mathcal{M}^n$ a POVM over the global state. Here U denotes the unitary operating over each round and U_G is the global unitary applied to the whole system (for coherent attacks).

	Ancilla State	Probability Distribution
Individual	$\rho_D^i = \mathrm{Tr}_H \left(U^\dagger \left(\rho_H^i \otimes \lvert 0 \rangle\langle 0 \rvert_D \right) U \right)$	$P_{\mathcal{M}^1}^{\rho_D^1} \ldots P_{\mathcal{M}^1}^{\rho_D^n}$
Collective	$\rho_D^i = \mathrm{Tr}_H \left(U^\dagger \left(\rho_H^i \otimes \lvert 0 \rangle\langle 0 \rvert_D \right) U \right)$	$P_{\mathcal{M}^n}^{\rho_D^1 \otimes \rho_D^2 \otimes \ldots \otimes \rho_D^n}$
Coherent	$\rho_D = \mathrm{Tr}_H \left(U_G^\dagger \left(\left(\rho_H^1 \otimes \rho_H^2 \otimes \ldots \otimes \rho_H^n \right) \otimes \lvert 0 \rangle\langle 0 \rvert_D \right) U_G \right)$	$P_{\mathcal{M}^n}^{\rho_D}$

Table 2.1: Attacks against quantum *protocols [27, Table 5.1]*

Chapter 3

Related work

This chapter describes the current state of the art regarding quantum OT and BC protocols which provide information-theoretic security under the bounded/noisy storage assumption. In this report, we study the primitive of $\binom{2}{1}$-randomized oblivious string transfer, which we will refer to as Oblivious Transfer (OT). Similarly, we refer to Randomized String Commitment (or RSC) when we say Bit Commitment (BC).

We first provide the reader understanding of two quantum functionalities: Weak String Erasure with Errors (WSEE) introduced in [11] and Randomized String Commitment (RSC), studied in [21]. RSC is a primitive where Alice will commit to multiple bits (a string) at once toward Bob, and if she is honest this string will be randomly generated. In a second phase, Alice will open her string and reveal it to Bob. If Bob is honest, he should be able to detect whether Alice has changed her committed value between the two steps. We will give a protocol to implement MDI-WSEE with perfect single photon sources, and a classical reduction protocol that allows to build MDI-RSC from any MDI-WSEE protocol, along with the corresponding security proofs. While the two protocols given are parts of [21, Protocol II.1], we have chosen to split this MDI-RSC protocol into a WSEE part and a classical reduction part to make the security proof clearer for the reader. This also allows the use of the reduction part with other potential MDI-WSEE protocols, where the authors of [21] chose to directly build an RSC protocol and prove its security in one go.

We then define oblivious string transfer and we show the existing protocol for MDI-OT with perfect single photon sources. However, this protocol is proven by the authors to be unsafe against a dishonest Alice whenever Bob uses imperfect single photon sources, giving to a cheating Alice a probability of winning higher than if she performs random guesses. We then describe weaker variants of OT shown in the literature and make an overview of the existing protocols for implementing OT-like primitives.

3.1 Weak String Erasure with Errors (WSEE)

3.1.1 Definition

In Weak String Erasure (formally defined in [13]), Alice wants to send a bit string to Bob, who will obtain a part of this string (about 50% of it) with the indices corresponding to the bits he correctly received. A WSE protocol can therefore be informally viewed as an erasure channel in which each bit has been erased with probability $\frac{1}{2}$.

We consider here a modified version of this primitive presented in [11], called Weak String Erasure with Errors. In this protocol, apart from the erasure, there is for each bit a probability p_{err} for it to become flipped (a 0 bit becomes a 1 and vice versa). This is equivalent to adding a bit-flipping channel $E_{p_{err}}$ such that every bit has a probability p_{err} of being flipped. We can then write the channel $E_{p_{err}}$ for a bit $b \in \{0, 1\}$:

$$E_{p_{err}}(b) = \begin{cases} 1-b & \text{With probability } p_{err} \\ b & \text{With probability } 1-p_{err} \end{cases} \tag{3.1}$$

We give here an informal definition of WSEE, a formal definition can be found in Appendix A.

Definition 3.1. Weak String Erasure with errors (informal):

We define an $(n, \lambda, \varepsilon, p_{err})$-WSEE primitive as in [11] with the following parameters:

- $n \in \mathbb{N}$ the length of Alice's string
- λn the minimal uncertainty (in terms of smoothed min-entropy) that Bob has about Alice's string
- ε the smoothing parameter that defines the smoothed min-entropy.
- $p_{err} \in]0, 0.5[$ the probability of having a bit flip in the channel due to noise

A protocol is a secure $(n, \lambda, \varepsilon, p_{err})$-WSEE protocol if the following properties hold.

Correctness: If both Alice and Bob are honest, at the end of the protocol Alice has a randomly chosen bit string $X_1^n \in \{0,1\}^n$. Bob has a randomly chosen subset of indices $\mathcal{I} \subseteq [n]$ with the corresponding bit string $\hat{X_{\mathcal{I}}} = E_{p_{err}}(X_{\mathcal{I}})$ with $\forall i \in [n], \Pr(i \in \mathcal{I}) = \frac{1}{2}$.

Security for Alice: If Alice is honest, Bob's knowledge about X_1^n is limited to

$$\frac{1}{n} \mathrm{H}_{\min}^{\varepsilon}(X_1^n | B) \geq \lambda \tag{3.2}$$

where B is Bob's state and $\mathrm{H}_{\min}^{\varepsilon}$ is the smoothed min-entropy as defined in equation (2.5). This means that Bob is only allowed to have a certain amount of information about Alice's entire string.

Security for Bob: If Bob is honest, Alice must not learn anything about $\mathcal{I}$.

3.1.2 An MDI-WSEE protocol

We present here and prove the security of a protocol that implements WSEE under the MDI setting. We define for this protocol the following parameters:

$$\zeta := \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{2n}}, \ \zeta_{\mathcal{I}} := \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{2(\frac{1}{2} - \zeta)n}} \tag{3.3}$$

$$\lambda := f\left(\frac{-D}{n}\right) - \frac{1}{n} - \left(\frac{\log\left(\frac{2}{\varepsilon^2}\right)}{n}\right) \tag{3.4}$$

$$\delta := 2p_{err} + 4\zeta_{\mathcal{I}}, \tag{3.5}$$

where n is the length of Alice's string, D is an upper bound on the size of dishonest Bob's quantum memory (in number of qubits), p_{err} is the expected error rate between Alice's and Bob's strings $X_{\mathcal{I}}$ and $\hat{X_{\mathcal{I}}}$ and ε is a given

security parameter. We call h the Shannon's binary entropy such that $\forall x \in]0,1[, h(x) = -x\log(x) - (1-x)\log(1-x)$ and we define the functions g as $g(x) = h(x) + x - 1$ and f as follows.

$$f(x) := \begin{cases} 0 & \text{if } x < -1 \\ g^{-1}(x) & \text{if } -1 \leq x < \frac{1}{2} \\ x & \text{if } \frac{1}{2} \leq x < 1 \end{cases} \tag{3.6}$$

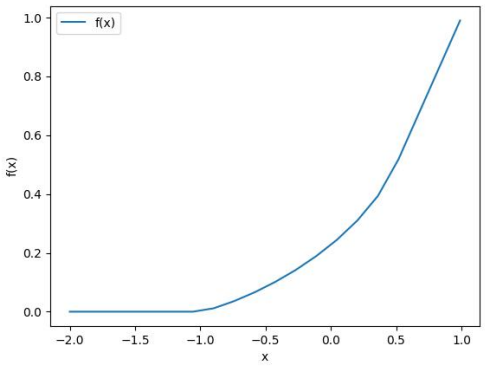


Figure 3.1: *Graph representing the function f*

Protocol 1: MDI-WSEE (from [21, Protocol II.1])

Inputs: The security parameter $\varepsilon > 0$, the length $n > 0$ of the string, D an upper bound on the size of dishonest Bob's quantum memory (in number of qubits), p_{err} the expected error rate between Alice's and Bob's strings $X_{\mathcal{I}}$ and $\hat{X}_{\mathcal{I}}$ due to noise.

Here, ζ and $\zeta_{\mathcal{I}}$ are defined as in (3.3), λ as in (3.4) and δ as in (3.5).

1. For round i until the total number of successful measurements is equal to n:
   - Alice chooses $(X_i, \Theta_i) \in_U \{0,1\}^2$ uniformly at random. She prepares and sends $|X_i\rangle_{\Theta_i}$ (where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$) to the measurement station.
   - Bob chooses $(\hat{X}_i, \hat{\Theta}_i) \in_U \{0,1\}^2$ uniformly at random. He prepares and sends $|\hat{X}_i\rangle_{\hat{\Theta}_i}$ (where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$) to the measurement station.
   - The measurement station performs a Bell state measurement on the two states it receives and publicly reveals the outcome (or reveals that the measurement failed). Bob decides based on the output of a successful measurement whether he should flip his bit $\hat{X}_i$ or not.
2. Alice and Bob discard all the rounds in which a failure has been announced. Now Alice has the two strings (X_1^n, Θ_1^n) and Bob has $(\hat{X}_1^n, \hat{\Theta}_1^n)$.
3. Both parties wait for a time Δt.
4. Alice sends Θ_1^n over to Bob.
5. Bob computes the set $\mathcal{I} \subseteq [1, n]$ of rounds where $\Theta_i = \hat{\Theta}_i$ and discards the rounds $i \notin I$. We now call $\hat{X}_{\mathcal{I}}$ the string formed by all the remaining bits $\hat{X}_i$ with $i \in \mathcal{I}$.

The measurement station performs a measurement that is sometimes referred to as "probabilistic Bell measurement". These measurements measure two qubits which are projected onto orthogonal maximally entangled states. The

outcome of such projections indicates to Bob whether he has to flip his bit x_i in order to have the same than Alice if they used the same encoding basis. The outcomes corresponding to operators that are not projections onto maximally entangled states are considered as "failures", just as when a qubit is lost before arriving to the station.

In order to perform the security proof, we need the following Lemmas:

Lemma 3.1. *Leftover hash lemma with smooth min-entropy (as used in [13, Theorem II.3]).*

Let $\rho_{A_1^n,B}$ be a cq-state, R be a randomness extractor chosen from a 2-universal hash functions family $\mathcal{R}_\ell^n$ uniformly and independently from $A_1^n B$. Let K_A be the classical register containing $Ext(A_1^n, R)$. Then, $\forall \varepsilon > 0$,

$$\frac{1}{2}\left\|\rho_{K_A,R,B} - \tau_{K_A} \otimes \rho_{R,B}\right\|_1 \leq 2^{-\frac{1}{2}(H_{\min}^{\varepsilon}(A_1^n|B)-\ell)-1} + 2\varepsilon.$$

Intuitively, this lemma shows that the state obtained after the randomness extraction is $\left(2^{-\frac{1}{2}(\mathrm{H}_{\min}^{\varepsilon}(A_1^n|B)-\ell)-1} + 2\varepsilon\right)$-close to a state in which K_A is chosen uniformly and independent of R and B. If we choose a small enough ℓ, these two states can be made to be 3ε-close. Note that this lemma corrects the mistake in the leftover hash lemma given in [21, Lemma IV.1] by adding the missing factor of $\frac{1}{2}$.

Lemma 3.2. *Chain rule for the min-entropy (as used in [21, Theorem IV.2] and [13, Equation 16]).*

If A, B are 2 classical registers and Q is a quantum register, we have

$$H_{\min}^{\varepsilon}(A|BQ) \geq H_{\min}^{\varepsilon}(A|B) - \log\left(\dim\left(Q\right)\right).$$

This means that by additionally obtaining the state in Q, a party holding B can reduce the entropy about the state in A by at most the number of qubits in Q.

Lemma 3.3. *Distance of a randomly generated code [21, Theorem IV.3].*

Let $\mathcal{C}$ be a randomly generated $[n, k]$ linear code. Then the distance d of the code satisfies, $\forall \delta \in [0, 1]$

$$\Pr(d \leq \delta n) \leq 2^{(\frac{k}{n}-1+h(\delta))n}.$$

This lemma will be used as the reduction protocol requires to create a random $[n, k, d]$ linear code $\mathcal{C}$ with d the distance of the code such that

$$d \geq \left(2p_{err} + 4\zeta_{\mathcal{I}}\right) n \tag{3.7}$$

Lemma 3.4. *Hoeffding's inequalities (A specific case of [21, Theorem IV.5]).*

Let $X_1, \ldots, X_n$ be n identically and independently distributed random variables such that $\forall i \in [1, n]$,

$$X_i = \begin{cases} 0 & \text{with probability } 1-p \\ 1 & \text{with probability } p \end{cases}.$$

Then, $\forall \varepsilon \in]0, 1[$

$$\Pr\left(\frac{1}{n}\sum_{i=1}^{n} X_i - p \geq \sqrt{\frac{\ln(\varepsilon^{-1})}{2n}}\right) \leq \varepsilon \tag{3.8}$$

$$\Pr\left(p - \frac{1}{n}\sum_{i=1}^{n} X_i \geq \sqrt{\frac{(\ln(\varepsilon^{-1})}{2n}}\right) \leq \varepsilon \tag{3.9}$$

which gives us

$$\Pr\left(\left|p-\frac{1}{n}\sum_{i=1}^{n}X_i\right|\geq\sqrt{\frac{\ln(\varepsilon^{-1})}{2n}}\right)\leq 2\varepsilon. \tag{3.10}$$

From equation (3.8), we obtain, $\forall t>0$

$$\Pr\left(p-\frac{1}{n}\sum_{i=1}^{n}X_i\geq t\right)\leq e^{\left(-2t^2n\right)}. \tag{3.11}$$

Theorem 3.1. *Security proof of the MDI-WSEE protocol*

Protocol 1 gives a secure MDI $(n,\lambda,\varepsilon,p_{err})$*-WSEE protocol, given that Bob's quantum memory* Q *(in terms of qubits) is such that* $\log\left(\dim\left(Q\right)\right)\leq D$*.*

Proof. Let us start with the correctness:

If the two parties are honest, they both choose at each round $X_i,\hat{X}_i,\Theta_i$ and $\hat{\Theta}_i$ uniformly at random. This directly results in X_1^n being randomly distributed. In addition, Bob will have the same bit than Alice at each round in which they chose the same basis $(\Theta_i=\hat{\Theta}_i)$, as he can flip his bit depending on the measurement station if $X_i\neq\hat{X}_i$. Honest Alice and Bob will have the same basis with probability $\frac{1}{2}$, which ensures that $\forall i\in[n]\,,\Pr\left(i\in\mathcal{I}\right)=\frac{1}{2}$.

Finally, considering p_{err} as an input allows us to see that $\hat{X}_{\mathcal{I}}$ that Bob receives is actually $\hat{X}_{\mathcal{I}}=E_{p_{err}}(X_{\mathcal{I}})$, as if a bit flip happens before a qubit reaches the measurement station Bob will incorrectly flip (not flip) his bit if $X_i=\hat{X}_i$ (if $X_i\neq\hat{X}_i$).

Lemma 3.5 gives the proof for the security for Alice, and Lemma 3.6 shows the security for Bob. □

Lemma 3.5. *Security for Alice for the MDI-WSEE protocol:*

If Alice is honest and Bob's quantum memory Q *is such that* $\log\left(\dim\left(Q\right)\right)\leq D$*, then at the end of Protocol 1, Bob's uncertainty about Alice's string* X_1^n *is such that* $\frac{1}{n}H_{\min}^{\varepsilon}(X_1^n|B)\geq\lambda$*.*

Proof. If Alice is honest, the MDI situation is equivalent to the one where Alice sends her states directly to Bob who performs the measurement. We can then adapt proofs for the non-MDI case. We can then use [28, Corollary 13] combined with [28, Lemma 23] to obtain

$$\mathrm{H}_{\min}^{\varepsilon}\left(X_1^n|B\right)_{\rho}\geq\lambda n, \tag{3.12}$$

with λ defined in equation (3.4). □

Lemma 3.6. *Security for Bob for the MDI-WSEE protocol:*

If Bob is honest, Alice does not learn anything about $\mathcal{I}$*.*

Proof. As explained in [21, Lemma IV.8] that the scenario in which a dishonest Alice would send half of an EPR pair to Bob is equivalent to the first step of the MDI-WSEE protocol when Alice is dishonest. The proof of the security for Bob from [13, Theorem III.5] can then used here and adapted to the presence of noise as in [21, Lemma IV.9]. This gives us that $\mathcal{I}$ is uniformly distributed and independent of Alice's register. □

3.2 Randomized String Commitment (RSC)

3.2.1 Definition

Randomized String Commitment is a protocol in which Alice wants to commit a randomly generated bit string to Bob. We want Alice to send some information to Bob during a so-called *commit* phase. At this point, Alice knows the string she is going to commit to, but Bob does not. Later - during the *open* phase - Bob receives the string Alice claims to have committed to, and he can use the information obtained in the previous phase to check that she indeed committed to this string, and he accordingly either accepts or rejects the commitment. The essential requirement is that Alice cannot change the string she commits to between the commit and the open phases without Bob noticing, with a high probability. This protocol is a more general version of Bit Commitment (BC), because Alice commits multiple bits at once.

The term *randomized* means that Alice does not get to choose the string she is going to commit to, it must be a randomly generated string. In an RSC protocol, Alice receives a random string she commits to, and Bob receives the fact that Alice committed to it both from the protocol. In the open phase, Alice reveals the string to Bob and he can check the correctness of the commitment and learn whether Alice cheated.

We give here an informal definition of RSC, a formal definition can be found in Appendix A.

Definition 3.2. Randomized string commitment (informal):

We define a RSC protocol as in [21] with the following parameters:

- ℓ is the length of the string that Alice will commit to
- ε is the parameter indicating the failure probability

A protocol implements an (ℓ, ε)-randomized string commitment if it ensures the following properties:

Correctness: If both Alice and Bob are honest, Alice's string C_1^ℓ is chosen randomly and Bob accepts, with a probability higher than $1 - \varepsilon$. .

Security for Alice: If Alice is honest, Bob cannot guess Alice's string C_1^ℓ before the open phase, except with a probability smaller than ε. Such a protocol is said to be ε-hiding.

Security for Bob: If Bob is honest, there exist a string C_1^ℓ of length ℓ after the commit phase, such that the probability that Alice opens to another string $C_1^{\ell\,\prime} \neq C_1^\ell$ and Bob accepts it is smaller than ε. Such a protocol is said to be ε-binding.

3.2.2 An MDI-RSC protocol: from WSEE to RSC

In this section, we show that the RSC primitive can be reduced to the WSEE primitive. We assume that we have a black box that performs a correct $(n, \lambda, \varepsilon, p_{err})$-WSEE protocol and explain how one can obtain a correct $(\ell, 3\varepsilon)$-RSC protocol from it, as described in [11, Protocol II.C]. By using the MDI-WSEE protocol described in Section 3.1, this reduction gives a secure MDI-RSC protocol.

With h the Shannon binary entropy, we take k to be the largest integer such that

$$\frac{k}{n} \leq 1 - h(\delta) + \frac{\log(\varepsilon)}{n} \tag{3.13}$$

where δ is defined in equation (3.5). Note that this definition slightly differs from the one in [21], where they take $\ln(\varepsilon)$ instead of $\log(\varepsilon)$. This change has been made to correct the proof of the security for Bob, in equation (3.18).

In the following protocol, C_1^ℓ represents the string Alice will commit to, where ℓ satisfies

$$\ell \leq (\lambda - h(\delta))n - 2\log(\frac{1}{2\varepsilon}) - \ln(\frac{1}{\varepsilon}), \tag{3.14}$$

where λ is defined as in equation (3.4).

Protocol 2: Going from $(n(\ell,\varepsilon), \lambda(\ell,\varepsilon), \varepsilon, p_{err}))$WSEE to (ℓ,ε)RSC

Inputs: The security parameter $\varepsilon > 0$, the length $\ell > 0$ of the string to be committed, D an upper bound on the size of dishonest Bob's quantum memory (in number of qubits), p_{err} the expected error rate between Alice's and Bob's strings $X_{\mathcal{I}}$ and $\hat{X}_{\mathcal{I}}$.

Preparation phase

1. Alice and Bob choose a number of rounds n such that $n(\lambda - h(\delta)) \geq \ell + 2\log(\frac{1}{2\varepsilon}) + \ln(\frac{1}{\varepsilon})$, where λ and δ are defined in equations (3.4) and (3.5).
2. Alice and Bob perform an $(n, \lambda, \varepsilon, p_{err})$-WSEE protocol. At the end, Alice obtains X_1^n and Bob obtains $(X_{\mathcal{I}}, \mathcal{I})$.

Commit phase

1. Bob checks that the length m of I is such that $m \geq \frac{n}{2} - n\zeta$, otherwise he aborts the protocol.
2. Alice chooses a random $[n,k]$ linear code $\mathcal{C}$ (with k defined in equation (3.13)) and computes the syndrome of X_1^n given by $w := \mathrm{Syn}_{\mathcal{C}}(X_1^n) \in \{0,1\}^{n-k}$.
3. Alice picks a random r from the 2-universal family of hash functions $\mathcal{R}_\ell^n$ and computes $C_1^\ell := \mathrm{Ext}(X_1^n, r)$.
4. Alice sends w and r to Bob.

Open phase

1. Alice sends X_1^n to Bob.
2. Bob computes the syndrome of X_1^n with the code $\mathcal{C}$ and check that it is indeed equal to w. If it is not the case, Bob aborts the protocol.
3. Bob finally checks that the proportion of indices in which $X_{\mathcal{I}}$ and $\hat{X}_{\mathcal{I}}$ do not agree lies in the interval $]p_{\mathrm{err}} - \zeta_{\mathcal{I}}, p_{\mathrm{err}} + \zeta_{\mathcal{I}}[$. If it is the case, Bob accepts and outputs $C_1^\ell := \mathrm{Ext}(X_1^n, r)$, otherwise Bob aborts the protocol.

The expression of the parameter $\zeta_{\mathcal{I}}$ is the same than the one for ζ except with a string of length m, as $(\frac{1}{2} - \zeta)n$ is a lower-bound for $|\mathcal{I}|$ during the protocol.

We will now prove that the protocol described allows to perform a secure RSC protocol given that the WSEE protocol can be securely implemented. This proof is an adaptation of the proof in IV-B of [21] and the Theorem IV.2 from [13].

After the WSEE protocol, we call n the length of Alice's string, and we define ζ and $\zeta_{\mathcal{I}}$ as in formula 3.3. We take $\mathcal{C}$ a random $[n,k]$ linear code with fixed k that satisfies 3.13.

If $\ell \in \mathbb{N}$ is such that the equation (3.14) is satisfied, we are going to prove that the protocol described implements a $(\ell, 3\varepsilon)$-RSC. In fact, the protocol will be 3ε-hiding, 2ε-binding and if both Alice and Bob are honest, the protocol will be correct and accepted with a probability greater than $1-3\varepsilon$.

Regarding the security for Alice, we want to make sure that, with high probability, a dishonest Bob does not learn C_1^ℓ before the open phase. Intuitively, this will be ensured through the correctness of the WSEE protocol - where the security for Alice criterion bounds the knowledge of Bob about X_1^n - and by showing that giving $\mathrm{Syn}(X_1^n)$ to Bob does not increase Bob's knowledge too much.

The security for Bob consists in ensuring that Alice cannot change her string C_1^ℓ between the commit and the open phases without Bob noticing it with high probability. Intuitively, Bob has two strings that help him detect whether Alice has cheated: the syndrome $\mathrm{Syn}(X_1^n)$ which indicates to him if Alice changed a small number of bits in X_1^n and his substring $\hat{X}_{\mathcal{I}}$ obtained during WSEE which indicates to him if Alice changed a lot of bits. Indeed, a dishonest Alice would have to find a string $\tilde{X_1^n}$ that has the same syndrome as X_1^n and matches with X_1^n (except at about $p_{err}|\mathcal{I}|$ locations). We choose a random linear code (having a sufficiently large distance with high probability) such that this happens with probability at most 2ε.

Theorem 3.2. *The reduction shown in Protocol 2 implements a secure MDI $(\ell, 3\varepsilon)$-RSC protocol, given that the MDI-WSEE protocol used in the preparation phase is secure, the total number of rounds n is chosen to satisfy equation (3.14) and the parameters of the $[n,k]$ error-correcting code are chosen to satisfy (3.13).*

Proof. Let us start with the correctness. If both parties are honest and Bob does not abort, the protocol is such that the final joint state held by Alice and Bob is $\rho_{C_1^\ell \tilde{C_1^\ell}} = \rho_{C_1^\ell C_1^\ell}$, i.e.$\tilde{C_1^\ell} = C_1^\ell$. The WSEE ensures that Alice's string X_1^n is uniformly chosen, just like the hash function r. The output of randomness extraction C_1^ℓ is then uniformly random, and we have $\rho_{C_1^\ell \tilde{C_1^\ell}} = \tau_{C_1^\ell C_1^\ell}$.

We are now going to show that if both parties are honest, the protocol will be accepted with probability higher than $1-3\varepsilon$. Bob can decide to abort the protocol at one of the three places: in the commit phase if $m < \frac{n}{2} - n\zeta$, in the open phase if the error rate between $X_{\mathcal{I}}$ and $\hat{X_{\mathcal{I}}}$ does not lie within $]p_{\mathrm{err}} - \zeta_{\mathcal{I}}, p_{\mathrm{err}} + \zeta_{\mathcal{I}}[$ or if the syndrome of X_1^n is different than w.

We can use the Hoeffding's inequality (Lemma 3.4) of equation (3.9) by seeing the sampling of I as n independent Bernoulli variables equal to 1 with probability $p = \frac{1}{2}$ to show that Bob will abort in the first case with a probability smaller than ε. In the second case, we can similarly show that Bob will abort with probability smaller than 2ε using equation (3.10). Finally, as the classical communication channel is assumed to be perfect, the last case will never happen if Alice and Bob are both honest.

This gives us that Bob will incorrectly abort the protocol with probability at most 3ε, and the protocol is 3ε-correct.

Lemma 3.7 gives the proof of the security for Alice, and Lemma 3.8 shows security for Bob. □

Lemma 3.7. *Security for Alice for the reduction protocol:*

Protocol 2 is 3ε-hiding, as long as $\lambda - 1 + \frac{k}{n} > 0$ and $n \geq \frac{\ell + 2\log(\frac{1}{2\varepsilon})}{\lambda - 1 + \frac{k}{n}}$, which is ensured by the conditions on k and ℓ given in equations (3.13) and (3.14).

Proof. Using these two equations we find that $k + 1 \geq n - nh(\delta) + \log(\varepsilon)$ (as k is the largest integer that satisfies equation (3.13)), therefore $\lambda - 1 + \frac{k}{n} \geq \ell - 1 + \log(\frac{1}{2\varepsilon}) + \ln(\frac{1}{\varepsilon}) > \ell - 1 > 0$ if $\ell \geq 2$.

After the preparation phase, the security for Alice criterion of the WSEE gives us that there exist an ideal state $\sigma_{X_1^n B'}$ such that $\mathrm{H}_{\min}(X_1^n|B')_\sigma \geq \lambda n$, and the real state $\rho_{X_1^n B}$ produced by the protocol is at a distance smaller

than ε from $\sigma_{X_1^n B'}$. This directly gives us that $\mathrm{H}_{\min}^{\varepsilon}(X_1^n|B)_\rho \geq \lambda n$ after the preparation phase. We can now use the chain rule of Lemma 3.2 to have that after the commit phase,

$$\mathrm{H}_{\min}^{\varepsilon}(X_1^n|Bw) \geq \lambda n - (n-k) \tag{3.15}$$

because of the length of the syndrome of an $[n,k]$ error correcting code is $n-k$. Bob learning $w = \mathrm{Syn}_{\mathcal{C}}(X_1^n)$ can then only reduce his entropy about X_1^n by $n-k$. We can rewrite it to have

$$\mathrm{H}_{\min}^{\varepsilon}(X_1^n|Bw) \geq n(\lambda - 1 + \frac{k}{n}). \tag{3.16}$$

We can now use the leftover hash lemma (Lemma 3.1) to obtain

$$\frac{1}{2}\left\|\rho_{C_1^\ell,\mathcal{R},Bw} - \tau_{C_1^\ell} \otimes \rho_{\mathcal{R},Bw}\right\|_1 \leq 2\varepsilon + 2^{-\frac{1}{2}(\mathrm{H}_{\min}^{\varepsilon}(X_1^n|Bw)-\ell)-1} = 2\varepsilon + 2^{-\frac{1}{2}(n(\lambda-1+\frac{k}{n})-\ell)-1} \tag{3.17}$$

The protocol is then $2\varepsilon+\varepsilon'$-binding where $\varepsilon' = 2^{-\frac{1}{2}(n(\lambda-1+\frac{k}{n})-\ell)-1}$. However, as $n \geq \frac{\ell+2\log(\frac{1}{2\varepsilon})}{\lambda-1+\frac{k}{n}}$ we have $\varepsilon' \leq \varepsilon$ and therefore the protocol becomes 3ε-binding. □

Lemma 3.8. *Security for Bob for the reduction protocol.*

We show here that the protocol is 2ε-binding, which means that if Alice changes her string before the open phase, Bob will notice it with probability greater than $1-2\varepsilon$. This proof is mostly an adaptation to a WSEE protocol of the proof in Lemma IV.4 of [13].

Proof. We will first prove that the randomly generated $[n,k]$-code has a distance d which satisfies equation (3.7) with probability greater than $1-\varepsilon$ as long as k was chosen to satisfy equation (3.13). □

Using Lemma 3.3 with $\delta = 2(p_{err} + 2\zeta_{\mathcal{I}})$, we find that

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

From equation (3.13), we have $(\frac{k}{n} - 1 + h(\delta))n = \log(\varepsilon)$.

We finally have

$$\Pr(d \leq (2(p_{err}+2\zeta_{\mathcal{I}}))n) \leq 2^{\log(\varepsilon)} = \varepsilon, \tag{3.18}$$

therefore, $\Pr(d \geq (2(p_{err}+2\zeta_{\mathcal{I}}))n) \geq 1-\varepsilon$.

We can now recall that after the WSEE protocol, Alice has absolutely no information about the set of indices I that Bob knows about her string. there exist a random string X_1^n such that Bob has a set of indices I and the substring (with errors) $\hat{X}_I$ of length $m \approx \frac{n}{2}$. Let us call $\bar{X}_1^n$ the closest string from X_1^n such that $w = \mathrm{Syn}_{\mathcal{C}}(\bar{X}_1^n)$, $\tilde{X}_1^n$ the string that Alice sends to Bob during the open phase, $w = \mathrm{Syn}_{\mathcal{C}}(X_1^n)$, and $C_1^\ell = \mathrm{Ext}(X_1^n, r)$ with r a randomly chosen 2-universal hash function.

First, if Alice sends $\tilde{X}_1^n = \bar{X}_1^n = X_1^n$, Bob will accept the protocol and output the commitment $\hat{C}_1^\ell = C_1^\ell$ which corresponds to a correct protocol, we will then analyze the case in which $X_1^n \neq \bar{X}_1^n$. For this we want to evaluate the probability of the event in which $\hat{C}_1^\ell \neq C_1^\ell$ and Bob accepts the protocol. We can split this situation in two cases: if $\mathrm{Syn}_{\mathcal{C}}(\bar{X}_1^n) = w$ and if $\mathrm{Syn}_{\mathcal{C}}(\bar{X}_1^n) \neq w$. The second case has probability 0 to occur as Bob will never accept the protocol if the syndrome he computes from Alice's string is different than the syndrome w he received during the *commit* phase. We can then write:

$$\Pr(\hat{C}_1^\ell \neq C_1^\ell \text{ and Bob accepts}) = \Pr(\mathrm{Ext}(\bar{X}_1^n, r) \neq \mathrm{Ext}(\bar{X}_1^n, r) \text{ and Bob accepts}|\mathrm{Syn}_{\mathcal{C}}(\bar{X}_1^n) = w)$$

Note that due to the properties of the error-correcting code $\mathcal{C}$, $\text{Syn}_{\mathcal{C}}(\bar{X_1^n}) = w$ means that the distance between $\bar{X_1^n}$ and X_1^n is at least $\frac{d}{2}$, and due to our choice of $\hat{X}_1^n$ the distance between $\hat{X_1^n}$ and $\bar{X_1^n}$ is smaller than $\frac{d}{2}$. Alice then has to modify at least $\frac{d}{2}$ bits of her string, and in order to not be detected by Bob during the open phase, she must do it in such a way that $\hat{X}_{\mathcal{I}}$ and $X_{\mathcal{I}}$ (the strings $\hat{X}_1^n$ and X_1^n sampled on the indices of $\mathcal{I}$) have at most $(p_{err} + \zeta_{\mathcal{I}})m$ distinct bits. We then want to have an idea of the number W of bits of $X_{\mathcal{I}}$ that Alice will flip. If Alice has randomly flipped $\frac{d}{2}$ bits among the n bits in X_1^n, a randomly chosen bit has a probability $\frac{d}{2n}$ to have been flipped, and a random number $m = |\mathcal{I}|$ of the n bits will be sampled by Bob.

We can now use the Hoeffding's inequality of equation (3.11): If we call $X_1, \ldots, X_m$ m random Bernoulli variables that are equal to 1 with probability $\frac{d}{2n}$ then W can be seen as the sum these random variables, and we have $\mathbb{E}(W) = \frac{md}{2n}$. Note that as Bob is assumed to be honest, conditioned on not aborting we have $m \geq \left(\frac{1}{2} - \zeta\right) n$. This gives us:

$$\begin{aligned}
\Pr(W \leq m(\frac{d}{2n} - \zeta_{\mathcal{I}})) &= \Pr\left(\mathbb{E}\left(\sum_{i=1}^{m} X_i\right) - \sum_{i=1}^{m} X_i \geq m\zeta_{\mathcal{I}}\right) \\
&\leq \Pr\left(\mathbb{E}\left(\frac{1}{\left(\frac{1}{2} - \zeta\right) n} \sum_{i=1}^{m} X_i\right) - \frac{1}{\left(\frac{1}{2} - \zeta\right) n} \sum_{i=1}^{m} X_i \geq \zeta_{\mathcal{I}}\right) \\
&\leq e^{-2\left(\frac{1}{2} - \zeta\right) n \zeta_{\mathcal{I}}^2} \\
&\leq e^{\left(-2\left(\frac{1}{2} - \zeta\right) n \sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{2\left(\frac{1}{2} - \zeta\right) n}}^2\right)} \\
&\leq e^{-\ln\left(\frac{1}{\varepsilon}\right)} \\
&\leq e^{\ln(\varepsilon)} \\
&\leq \varepsilon
\end{aligned}$$

In addition, if $d \geq 2\left(p_{err} + 2\zeta_{\mathcal{I}}\right) n$ as required in equation (3.7), we have $m\left(\frac{d}{2n} - \zeta_{\mathcal{I}}\right) \geq \left(p_{err} + \zeta_{\mathcal{I}}\right) m$. This then gives us that $\Pr(W \leq (p_{err} + \zeta_{\mathcal{I}})m) \leq \varepsilon$.

We can put this together with equation (3.18), to find that the event of Alice cheating without Bob detecting it will occur either if $W \leq (p_{err} + \zeta_{\mathcal{I}})m$ or if $d \leq 2\left(p_{err} + 2\zeta_{\mathcal{I}}\right) n$. Each event has a probability ε of occurring, therefore either of the events will happen with a probability smaller than 2ε. We can then say that the protocol is 2ε-binding.

3.3 Oblivious Transfer (OT)

As mentioned by the authors in [21], MDI-OT with imperfect photon sources is "difficult", meaning that they could not find a secure protocol to implement it. However, they give a lower-bound on Alice's probability of cheating which tends to $\frac{1}{2}$ when the length n of the strings gets large. This could indicate that weaker primitives than OT could be possible to do. After defining what is an OT primitive, this section therefore aims to present a review of existing weaker OT-like primitives and summarize how they compare to each other. The work of Santos et al. [29] helped us to perform this review.

3.3.1 Definition

We give here an informal definition of a randomized version of an OT primitive. A formal definition can be found in Appendix A.

Definition 3.3. Randomized 1-out-2 string Oblivious Transfer (informal):

We define an $\binom{2}{1}$-Randomized String Transfer protocol as in [21] with the following parameters:

- ℓ is the length of the two strings obtained by Alice
- ε is the parameter indicating the failure probability

A protocol implements an (ℓ, ε)-Randomized 1-out-2 Oblivious String Transfer if it ensures the following properties:

Correctness: If both Alice and Bob are honest, Alice's strings S_1 and S_0 are chosen randomly and Bob learns only one of the two strings (the string he learns is chosen randomly), while Bob accepts with a probability higher than $1 - \varepsilon$.

Security for Alice: If Alice is honest, she obtains two strings S_1 and S_0 such that there is at least one of the two strings that Bob is ε-ignorant about. Such a protocol is said to be ε-hiding.

Security for Bob: If Bob is honest, he receives after the protocol a randomly generated choice bit c and an ℓ-bit string $\hat{S}_c$, such that Alice is ε-ignorant about c. Such a protocol is said to be ε-binding.

3.3.2 An MDI-OT protocol

A protocol that implements MDI-OT with perfect single photon sources is given with its security proof in [21, Protocol II.2]. Let S_0 and S_1 represent the strings of length ℓ Alice will send, where

$$\ell \leq \frac{\left(\lambda - h(p_{err}) - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right) n}{2} - D - 1 + 2\log\left(1 - \sqrt{1-\varepsilon^2}\right) \tag{3.19}$$

and λ is defined as

$$\lambda := \frac{1}{2} - \delta' \tag{3.20}$$

with

$$\delta' := \left(2 - \log\left(\sqrt{\frac{32\ln\left(\frac{1}{\varepsilon}\right)}{n}}\right)\right)\sqrt{\frac{32\ln\left(\frac{1}{\varepsilon}\right)}{n}}. \tag{3.21}$$

Protocol 3, from [21, Protocol II.2]:

Inputs: The security parameter $\varepsilon > 0$, the length $\ell > 0$ of the string to be transferred, D an upper bound on the size of dishonest Bob's quantum memory (in number of qubits), p_{err} the expected error rate between Alice's and Bob's strings $X_{\mathcal{I}}$ and $\hat{X_{\mathcal{I}}}$.

Preparation phase

1. Alice and Bob choose a number of rounds n such that $n \geq 2\frac{\ell + D + 1 - 2\log\left(1-\sqrt{1-\varepsilon^2}\right)}{\lambda - h(p_{err}) - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)}$, where λ is defined in equation (3.20) and (3.21).

2. Alice and Bob perform the $(n, \lambda, \varepsilon, p_{err})$-WSEE protocol given by Protocol 3.1.2. At the end, Alice obtains X_1^n and Bob obtains $(X_{\mathcal{I}}, \mathcal{I})$.

Classical post processing

1. Bob checks that the length of $\mathcal{I}$ is such that $m \geq \frac{n}{2} - n\zeta$, otherwise he aborts the protocol. Bob then randomly truncates the string $\mathcal{I}$ for it to be exactly of length $m := \frac{n}{2} - n\zeta$.
2. Bob picks a random subset of $\mathcal{I}^c := [n] \setminus \mathcal{I}$ of size m called $\mathcal{I}_{bad}$ and picks his random bit c uniformly. He then renames $(\mathcal{I}, \mathcal{I}_{bad})$ into $(\mathcal{I}_c, \mathcal{I}_{1-c})$ and sends $(\mathcal{I}_0, \mathcal{I}_1)$ in this order to Alice.
3. Alice sends to Bob error correction information of length leak_O for the strings $X_{\mathcal{I}_0}$ and $X_{\mathcal{I}_1}$.
4. Bob uses the right syndrome to correct his string $\hat{X_{\mathcal{I}}}$. He aborts the protocol in case of a failure in the error correction.
5. Alice picks two random function r_0 and r_1 from the 2-universal family of hash functions $\mathcal{R}_\ell^m$ and sends them to Bob
6. Alice outputs $(S_0 S_1) := (\text{Ext}(X_{\mathcal{I}_0}, r_0), \text{Ext}(X_{\mathcal{I}_1}, r_1))$ and bob outputs $\hat{S}_c := \text{Ext}(X_{\mathcal{I}_c}, r_c)$ and c.

In order to satisfy the security definition for OT, when an honest party aborts the protocol, the aborting party will continue the protocol as if they were not aborting – in particular, they do not announce the abort event until the end of the protocol – except that in the end, when the abort event is announced all honest parties assign to their outputs uniformly random values

3.3.3 Impossibility result under the MDI setting with imperfect single photon sources

Protocol 3 was proven to be secure under the MDI setting with perfect single photon sources, however the authors showed in [21, Theorem IV.20] that this protocol is not secure when Bob uses an imperfect single photon source. We show here the attack strategy given in [21, Protocol II.4] for a semi-honest Alice. Let M be the classical information exchanged between Alice and Bob during the post processing of Protocol 3, and we call f_0 and f_1 the functions such that $S_0 = f_0(X_1^n, M)$ and $S_1 = f_1(X_1^n, M)$. These functions correspond to the computations that a honest Alice will do to compute the output strings S_0 and S_1. A dishonest Alice will in addition create two sets $\mathcal{I}_G$ and $\mathcal{I}_B$ using the leakage of information due to multiphoton emissions. For Protocol 3, $\mathcal{I}_G$ ($\mathcal{I}_B$) corresponds to the rounds where Bob emitted multiple photons and Alice and Bob used the same basis (different bases). The following assumption [21, Assumption II.1] is made by the authors: we assume that there exist a function F such that $(\mathcal{I}_0, \mathcal{I}_1) = F(X_1^n, M)$, on which f_0 and f_1 depends. We also assume that the event $[(\mathcal{I}_G \cup \mathcal{I}_B) \cap (\mathcal{I}_0 \setminus \mathcal{I}_1) \neq \emptyset \text{ and } (\mathcal{I}_G \cup \mathcal{I}_B) \cap (\mathcal{I}_1 \setminus \mathcal{I}_0) \neq \emptyset]$ happens with non negligible probability, which is the case in Protocol 3.

Protocol 4: Alice's attack strategy against Protocol 3 [21, Protocol II.4]:

Inputs: $X_1^n, M, \mathcal{I}_G, \mathcal{I}_B$

1. Alice computes $(\mathcal{I}_0, \mathcal{I}_1) = F(X_1^n, M)$
2. Alice checks that $(\mathcal{I}_G \cup \mathcal{I}_B) \cap (\mathcal{I}_0 \setminus \mathcal{I}_1) \neq \emptyset$ and $(\mathcal{I}_G \cup \mathcal{I}_B) \cap (\mathcal{I}_1 \setminus \mathcal{I}_0) \neq \emptyset$. If this is not the case, Alice outputs $\hat{c} \in_U \{0, 1\}$.
3. Alice randomly generates $r \in_U \{0, 1\}$, and chooses the index $i_r \in_U \mathcal{I}_r \setminus \mathcal{I}_{1-r} \cap (\mathcal{I}_G \cup \mathcal{I}_B)$
4. Alice outputs $\hat{c} := \begin{cases} r & \text{if } i_r \in \mathcal{I}_G \\ 1 - r & \text{if } i_r \in \mathcal{I}_B \end{cases}$

From [21, Theorem IV.20], using this attack strategy on Protocol 3 allows Alice to cheat with probability P_{guess} such that

$$P_{guess} \geq \frac{1}{2} + \left[1 - (1-\gamma)^{2m}\right] \times \frac{2\nu - 1}{n}, \tag{3.22}$$

where γ is the proportions of rounds where Bob emits 2 or more photons, and ν is the probability that Alice guesses Bob's encoding basis when he does so. This gives a lower-bound on Alice's probability of cheating greater than $\frac{1}{2}$. However, this lower bound approaches $\frac{1}{2}$ when the number n of communication rounds grows large. This could indicate that weaker primitives than OT which lets Alice cheats with a bounded advantage (say $P_{guess} \leq 0.6$) may be achievable. In the following section, we describe some weaker variants of OT to explore this possibility.

3.3.4 Weak OTs

3.3.4.1 Weakening the definitions

Since unconditionally secure OT is impossible without assumptions, research has been made to try to relax the definition of OT in different ways. We will write $\binom{n}{1}$-OT to denote a primitive in which Alice sends n bits and Bob receives 1 of them, and $\binom{2}{1}$-OT^k a protocol in which Alice has two k-bit strings and Bob receives only one of the strings. $\binom{2}{1}$-OT^k is also called string commitment, and we can see that $\binom{2}{1}$-OT is the same primitive as $\binom{2}{1}$-OT$^{k=1}$.

A $\binom{2}{1}$-XOR OT is a primitive in which Alice will still send 2 bits b_0 and b_1 but Bob can now receive one bit from $\{b_0, b_1, b_0 \oplus b_1\}$ without knowing the other values, and without Alice knowing what did Bob received. A generalized $\binom{2}{1}$-OT is a primitive in which Bob will choose one function $f : \{0,1\}^2 \to \{0,1\}$ and receive $f(b_0, b_1)$, without learning anything about b_0 and b_1 other than $f(b_0, b_1)$ and without Alice knowing f. We can see that the usual $\binom{2}{1}$-OT primitive is a special case of generalized OT in which the set of functions f is restricted to choosing one of the bits. Is has been shown in [7] that $\binom{2}{1}$-OT^k can be reduced to slightly more than $4.8188k$ instances of generalized $\binom{2}{1}$-OT. Finally, one more general (weaker) variant of OT is called universal $\binom{2}{1}$-OT. Here, Bob can choose any type of information about the bits sent by Alice (including probabilistic information). Bob can for instance choose to obtain noisy versions of the two bits (with some error probability ε).

Another work [10] defines the security of OT probabilistically by the means of information leakage, and they give a $\binom{2}{1}$-OT protocol that is secure in the bounded storage model.

3.3.4.2 Weakening the bounds

We recall that in a $\binom{2}{1}$-OT^{k}protocol, a dishonest Alice will try to cheat by guessing the value of Bob's choice bit, and a dishonest Bob will try to cheat by guessing the string which does not correspond to his choice bit. We call $p_A^\star$ and $p_B^\star$ the probabilities of winning for Alice and Bob in a given protocol. The aim of a safe OT protocol is to have $p_A^\star$ and $p_B^\star$ corresponding to random guesses with a probability of $\frac{1}{2}$ for each bit of secret information. For a secure $\binom{2}{1}$-OT^k scheme, $p_B^\star$ should be $\frac{1}{2^k}$ (the probability of correctly randomly guessing a k-bit) and $p_A^\star$ should be $\frac{1}{2}$.

Some researchers have then tried to find protocols in which $\max(p_A^\star, p_B^\star)$ is not $\frac{1}{2}$ but some constant between $\frac{1}{2}$ and 1 (for a length of $k = 1$ bit). This means that a dishonest party has some known advantage which translates to a greater chance of winning compared to performing random guesses. Several values of lower bound for the maximum probability of cheating have been given in different protocols.

First, in 2013, the authors of [30] show that by noting the bias ε of a protocol as $\varepsilon = \max(p_A^\star - \frac{1}{2}, p_B^\star - \frac{1}{2})$, OT and randomized-OT are equivalent: we can build a randomized-OT with bias ε from an OT protocol with bias ε, and vice-versa. The authors also show that for any quantum $\binom{2}{1}$-OT protocol that does not make assumptions on the storage of malicious parties, the probability of cheating of both Alice and Bob is greater than 0.5852, i.e. $\max(p_A^\star, p_B^\star) \geq 0.5852$.

In [31], it is shown that for any $\binom{2}{1}$-OT^k protocol that does not make assumptions on the storage of malicious parties, $\max(p_A^\star, p_B^\star) \geq 0.61$, which gives a lower bound for string oblivious transfer that is independent of the length k.

In [32], the authors introduce a framework for semi-random OT and show that the minimum achievable bound is $\max(p_A^\star, p_B^\star) \geq \frac{2}{3} \approx 0.67$, and they give a protocol that achieves cheating probabilities of $\frac{3}{4}$ for Alice and 0.729 for Bob.

Later, in 2022, it is shown in [33] that under a more general setting, for any quantum $\binom{2}{1}$-OT protocol $\max(p_A^\star, p_B^\star) \geq 0.5242$. This is a looser bound than the one previously presented in [30]. However, the authors explain the difference by the fact that the bound given is much more general compared to the other bounds restricted to certain OT protocols.s

Below is a table that gives an overview of several OT and weak OT protocols proposed in the literature.

Protocol	Conditions/assumptions	Techniques used	Alice security	Bob Security
BBCS[2]	Bob not allowed to store any qubit	BB84 coding	Bob has no information about S_{1-c}	Alice has no information about c
BBCS with commitment[29]	Perfect storage Assumes that BC is possible	Bit commitment on a fraction of Bob's encoded bits and bases for Alice to check	Bob has no information about S_{1-c}	Alice has no information about c
ε-OT[11]	Noisy storage with perfect photon sources	WSEE Interactive hashing	Bob is ε-ignorant about S_{1-c}	Alice has no information about c
ε-OT [34]	Noisy storage (for Bob), imperfect single photon sources	WSEE	Bob is ε-ignorant about S_{1-c}	Alice has no information about c
ε-OT[21]	MDI, bounded storage with perfect photon sources	WSEE	Bob is ε-ignorant about S_{1-c}	Alice has no information about c
ε-OT [8]	DI, Bounded storage LWE assumption	Self testing	Bob is ε-ignorant about S_{1-c}	Alice has no information about c
Weak OT [32]	Unbounded memory, perfect single photon sources	Unambiguous quantum state elimination	$p_B^* \geq 0.729$	$p_A^* \geq \frac{3}{4}$

Table 3.1: *Overview of various OT-like primitives*

3.3.5 $p_A^\star$-weak OT

Here, we give the definition of a particular weak variant of OT where the probability for Alice to guess Bob's choice bit is given by $p_A^\star \in \left]\frac{1}{2}, 1\right[$ and $p_B^\star = \frac{1}{2^k}$. For convenience, we refer to this primitive as $p_A^\star$-weak OT. This is a weak OT primitive that can be useful when there is a protocol that gives an advantage for Alice but not for Bob, and that advantage can be proven to be strictly smaller than $\frac{1}{2}$. In the next chapter, we will study the possibility of implementing this primitive using Protocol 3 under the MDI setting with multiphoton emissions.

Definition 3.4. Randomized 1-out-2 string $p_A^\star$-weak Oblivious Transfer (informal):

We define an OT protocol with the following parameters:

- ℓ is the length of the two strings obtained by Alice
- ε is the parameter indicating the failure probability
- $p_A^\star - \frac{1}{2}$ is the advantage for Alice in predicting Bob's choice bit

A protocol implements an (ℓ, ε)-Randomized 1-out-2 String $p_A^\star$-weak Oblivious Transfer if it ensures the following properties:

Correctness: If both Alice and Bob are honest, Alice's strings S_1 and S_0 are chosen randomly and Bob learns only one of the two strings (the string he learns is chosen randomly), while Bob accepts with a probability higher than $1 - \varepsilon$.

Security for Alice: If Alice is honest, she obtains two strings S_1 and S_0 such that there is at least one of the two strings that Bob cannot learn anything about except with probability ε. Such a protocol is said to be ε-hiding.

Security for Bob: If Bob is honest, he receives after the protocol a randomly generated choice bit c and an ℓ-bit string $\hat{S}_c$, such that Alice cannot guess c except with probability $p_A^\star$.

Chapter 4

Contributions

This chapter describes the contributions made during this project.

1. Ribeiro et al. showed that using the decoy states technique in [21, Protocol II.2] does not implement a secure OT protocol. We extend this result by showing that even $p_A^\star$-weak OT is not achievable by using the decoy states technique in [21, Protocol II.2] under the MDI setting and multiphoton emissions.
2. We are currently working to show that our analysis can be used to improve the rate of the MDI-BC protocol in [21, Protocol II.3]. By rate we mean the number of random bits generated per round of quantum communication.
3. We are also showing that the BBCS reduction from OT to BC [2] cannot be used to achieve a secure OT protocol under MDI setting with multiphoton emissions.

4.1 On the impossibility of $p_A^\star$-weak OT primitives from [21, Protocol II.2]

As mentioned above, the protocol [21, Protocol II.2] comes with a discussion on why this protocol will not allow to perform MDI-OT when using imperfect single photon sources. The authors give a lower bound on the probability for Alice to cheat, which may let us think that one could find a $p_A^\star$-weak OT protocol (Section 3.3.5) which allows Alice to cheat with a probability strictly smaller than $\frac{1}{2} + \text{adv}$, where $\text{adv} < \frac{1}{2}$. However, as we are going to see in this section, this is not possible to do with [21, Protocol II.2]. We are going to give here a cheating strategy for Alice and show that this strategy gives her a probability of cheating that exponentially grows to 1 as the number of communication rounds gets large.

4.1.1 Probability that Alice guesses Bob's basis when he sends a given number of photon

Theorem 4.1. *Probability that Alice correctly guess Bob's basis when he sends $m > 1$ photons*

If Alice and Bob are in a protocol where Bob uses Weak Coherent laser Pulses as an imperfect single photon source to send BB84 states and sends a number $n > 1$ of photons during one round, Alice has a probability of at most $p_{succ,m}^{\max} := \frac{1}{2} + \frac{1}{4} \left\| \rho_{\theta=0,m}^B - \rho_{\theta=1,m}^B \right\|_1 < 1$ to guess Bob's basis, where $\rho_{\theta=0,m}^B$ and $\rho_{\theta=1,m}^B$ are defined in equations (4.9,4.10).

Proof. We are deriving here the probability that on a given round, Alice correctly guess Bob's basis based on the number of photons he sent. Note that only in this section, we note n the number of photons sent during one round, instead of the total number of rounds. From Section 4.1.2, n will denote the number of rounds in the preparation phase of the OT protocol. Using Weak Coherent laser Pulses (WCP), if Bob chooses to encode his bits in the basis θ, he will send a state equal to

$$\rho^B_{\theta,x} = \sum_{n=0}^{\infty} p_m \rho_{\theta,x,m}, \tag{4.1}$$

where p_n denotes the probability that Bob's source sends n photons, and

$$\rho_{\theta=0,x=0,m} = |0\rangle^{\otimes m}\langle 0|^{\otimes m} \tag{4.2}$$
$$\rho_{\theta=0,x=1,m} = |1\rangle^{\otimes m}\langle 1|^{\otimes m} \tag{4.3}$$
$$\rho_{\theta=1,x=0,m} = |+\rangle^{\otimes m}\langle +|^{\otimes m} \tag{4.4}$$
$$\rho_{\theta=1,x=1,m} = |-\rangle^{\otimes m}\langle -|^{\otimes m}. \tag{4.5}$$

□

If we note χ the intensity (the average number of photons) of the WCP source, we have

$$p_m = e^{-\chi}\frac{\chi^m}{m!}. \tag{4.6}$$

Dishonest Alice's goal is to be able to distinguish, for a fixed number of photons n, whether the state is in $\{\rho^B_{\theta=0,x=0,m}, \rho^B_{\theta=0,x=1,m}\}$ or in $\{\rho^B_{\theta=1,x=0,m}, \rho^B_{\theta=1,x=1,m}\}$. Alice will try to find the pair of measurement operators $\left\{M^A_{0,n}, M^A_{1,n}\right\}$ such that measuring Bob's state $\rho^B \in \{\rho^B_{\theta=0,x=0,m}, \rho^B_{\theta=0,x=1,m}, \rho^B_{\theta=1,x=0,m}, \rho^B_{\theta=1,x=1,m}\}$ will give her the best guess about θ.

From [26, page 5.1.1], the probability of being able to correctly distinguishing between $\theta = 0$ and $\theta = 1$ is given by

$$p_{succ,m} := \frac{1}{4}\mathrm{tr}\left(M^A_{0,m}\rho^B_{\theta=0,x=0,m}\right) + \frac{1}{4}\mathrm{tr}\left(M^A_{0,m}\rho^B_{\theta=0,x=1,m}\right) + \frac{1}{4}\mathrm{tr}\left(M^A_{1,m}\rho^B_{\theta=1,x=0,m}\right) + \frac{1}{4}\mathrm{tr}\left(M^A_{1,m}\rho^B_{\theta=1,x=1,m}\right). \tag{4.7}$$

We have from the properties of POVM operators $M^A_{1,m} = \mathbb{1}_{2^m} - M^A_{0,m}$, which gives us

$$p_{succ,m} = \frac{1}{2} + \frac{1}{2}\mathrm{tr}\left(M^A_{0,m}\left(\rho^B_{\theta=0,m} - \rho^B_{\theta=1,m}\right)\right), \tag{4.8}$$

where

$$\rho^B_{\theta=0,m} = \frac{1}{2}\left(\rho^B_{\theta=0,x=0,m} + \rho^B_{\theta=0,x=1,m}\right) = \frac{1}{2}\left(|0\rangle^{\otimes m}\langle 0|^{\otimes m} + |1\rangle^{\otimes m}\langle 1|^{\otimes m}\right) \tag{4.9}$$

and

$$\rho^B_{\theta=1,m} = \frac{1}{2}\left(\rho^B_{\theta=1,x=0,m} + \rho^B_{\theta=1,x=1,m}\right) = \frac{1}{2}\left(|+\rangle^{\otimes m}\langle +|^{\otimes m} + |-\rangle^{\otimes m}\langle -|^{\otimes m}\right). \tag{4.10}$$

The maximum probability for Alice to distinguish the two states is then given by

$$p^{\max}_{succ,m} = \frac{1}{2} + \frac{1}{2}\max_{0\leq M\leq \mathbb{1}_{2^m}} \mathrm{tr}\left(M\left(\rho^B_{\theta=0,m} - \rho^B_{\theta=1,m}\right)\right). \tag{4.11}$$

From the definition of the trace distance (definition 1), this term can be written as

$$p^{\max}_{succ,m} = \frac{1}{2} + \frac{1}{4}\left\|\rho^B_{\theta=0,m} - \rho^B_{\theta=1,m}\right\|_1. \tag{4.12}$$

Computing the maximum probability of winning for Alice for various values of m gives the following graph:

We can put these numbers in a table, where we chose an intensity of $\chi = 0.1$:

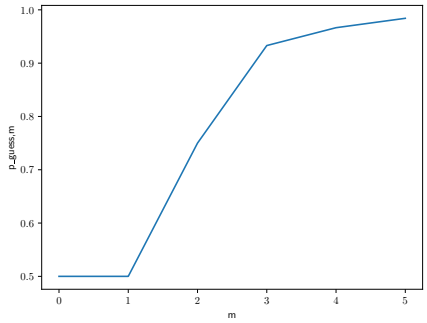


Figure 4.1: $p^{\max}_{succ,m}$ *as a function of* m

Number m of photons	0	1	2	3	4	5	6
p_m	0.905	0.090	0.004	0.00015	3.7×10^{-6}	7.5×10^{-8}	1.26×10^{-9}
$p^{\max}_{succ,m}$	0.5	0.5	0.75	0.933	0.967	0.984	0.992

We can see from this table that even if $p^{\max}_{succ,m}$ gets close to one quickly, the probability of sending m photons when $m \geq 5$ is really small, so most of the correct guesses from Alice will happen with a relatively small number of photons emitted. This is why we do not consider $m \geq 7$ for the numerical calculations below.

Corollary 4.1. *Probability that Bob emits 2 photons or more, and probability that Alice correctly guesses his base when he does so.*

If Alice and Bob are in a round of a protocol where Bob emits BB84 states using Weak Coherent laser Pulses as an imperfect single photon source with intensity χ*, then he has a probability* $\gamma := \frac{\sum_{m=2}^{\infty} p_m}{1-p_0}$ *to send multiple photons and Alice has a probability* $\nu := \frac{\sum_{m=2}^{\infty} p_m p^{\max}_{succ,m}}{\sum_{m=2}^{\infty} p_m}$ *of correctly guessing his encoding basis if he did so, where the values* $\{p_m, m \geq 0\}$ *are given in equation (4.6) and* $p^{\max}_{succ,m}$ *is given in equation (4.12).*

Proof. For a given intensity χ used by Bob, we can evaluate γ, the expected proportion of multiphoton emissions (excluding zero-photon emissions) and ν, the probability of predicting the basis choice correctly during a multiphoton emission.

$$\gamma := \frac{\sum_{m=2}^{\infty} p_m}{1 - p_0} \tag{4.13}$$

$$\nu := p^{\max}_{succ,m\geq 2} = \frac{\sum_{m=2}^{\infty} p_m p^{\max}_{succ,m}}{\sum_{m=2}^{\infty} p_m} \tag{4.14}$$

□

We can do the calculation, taking $\chi = 0.1$ and ranging the number of photons emitted up to 6, to find that $\nu \approx 0.756$ and $\gamma \approx 0.049$.
In order to compare the values obtained here with the work of Ribeiro et al, in which it is assumed that whenever a multiphoton emission occurs Alice can guess Bob's basis with probability 1, the following figure shows the value of ν as a function of the source intensity $\chi > 0$.

4.1.2 Estimating Alice's cheating probability in [21, Protocol II.2]

Let us recall that [21, Theorem IV.20] gives a lower bound on the probability that Alice has to cheat during Protocol 3 when Bob uses an imperfect single photon source which is strictly greater than $\frac{1}{2}$, as described in Section 3.3.3. However, this is not a lower bound which clearly tends to 1 when the number of rounds gets large, and this may

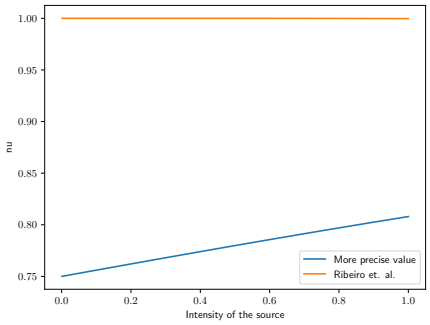


Figure 4.2: ν *as a function of* χ*. We can see that the value of* ν *is always far from* 1*.*

suggest that $p_A^\star$-weak OT is possible to achieve from this protocol, if one manages to find an upper bound on the probability that Alice has to cheat which is strictly smaller than 1. However, Theorem 4.2 states that this is not the case, by showing a new attack strategy for Alice.

Theorem 4.2. *Impossibility of* $p_A^\star$*-weak OT from [21, Protocol II.2] under multiphoton emissions*

When Alice and Bob perform the protocol [21, Protocol II.2] and Bob has access to an imperfect single photon source which sends 2 photons or more with probability γ *and Alice has a probability* ν *of correctly guessing his encoding basis when he does so, Alice can guess Bob's choice bit with a probability* $P_{guess} \geq 1 - e^{-n\frac{\gamma^2(2\nu-1)^2}{2}}$*, where* n *is the number of quantum communication rounds, using the attack strategy described in Protocol 5. This gives a better strategy for Alice to cheat against Protocol 3 compared to the attack described in Protocol 4 given by [21].*

Proof. We define here a cheating strategy for Alice and show that this cheating strategy gives her a winning probability that grows to 1 as the number of rounds n gets large. □

Let's first recall the key elements of the MDI-OT protocol [21, Protocol II.2]. Alice and Bob will start performing a WSEE-like protocol in a so-called "preparation phase" which outputs to honest Alice a bit string $X_1^n \in_U \{0,1\}^n$, while honest Bob receives a subset of indices $\mathcal{I} \subseteq_U [n]$ of length approximately $\frac{n}{2}$, as well as the string $X_{\mathcal{I}} = \{E_{p_{err}}(X_i), i \in \mathcal{I}\}$. However, the fact that Bob uses imperfect photon sources will leak information to a dishonest Alice, and she will try to guess for certain indices whether they are in $\mathcal{I}$ or not. We can say that a dishonest Alice will build two sets $\mathcal{I}_G, \mathcal{I}_B \subseteq [n]$ of combined length $|\mathcal{I}_G \cup \mathcal{I}_B| \approx \gamma n$ such that $\mathcal{I}_G \cap \mathcal{I}_B = \emptyset$, and $\forall i \in \mathcal{I}_G \cup \mathcal{I}_B$:

$$\text{if } i \in \mathcal{I} \text{ then } i \in \mathcal{I}_G \text{ with probability } \nu \text{ or } i \in \mathcal{I}_B \text{ with probability } 1-\nu$$

$$\text{if } i \notin \mathcal{I} \text{ then } i \in \mathcal{I}_G \text{ with probability } 1-\nu \text{ or } i \in \mathcal{I}_B \text{ with probability } \nu$$

After the preparation phase, Bob will create a set of indices $\mathcal{I}' := [n] \backslash \mathcal{I}$, randomly choose a bit $c \in \{0,1\}$, and rename $(\mathcal{I}, \mathcal{I}')$ into $(\mathcal{I}_c, \mathcal{I}_{1-c})$ before sending $(\mathcal{I}_0, \mathcal{I}_1)$ over to Alice through a classical channel. The aim of dishonest Alice is to correctly guess Bob's choice bit c.

One strategy for a dishonest Alice to cheat is to compute the numbers $|\mathcal{I}_G \cap \mathcal{I}_0|$, $|\mathcal{I}_G \cap \mathcal{I}_1|$, $|\mathcal{I}_B \cap \mathcal{I}_0|$ and $|\mathcal{I}_B \cap \mathcal{I}_1|$. We can see that from the definition of $\mathcal{I}_G$ and $\mathcal{I}_B$, if ν is large we expect $|\mathcal{I}_G \cap \mathcal{I}_c|$ and $|\mathcal{I}_B \cap \mathcal{I}_{1-c}|$ to be greater than the two other values, which will allow Alice to guess c with a high probability. We then give the following strategy for Alice, where the function F is described in Section 3.3.3:

Protocol 5: New Alice's attack strategy against Protocol 3:

Inputs: $X_1^n, M, \mathcal{I}_G, \mathcal{I}_B$

1. Alice computes $(\mathcal{I}_0, \mathcal{I}_1) = F\left(X_1^n, M\right)$
2. Alice outputs
$$\hat{c} := \begin{cases} 0 & \text{if } |\mathcal{I}_G \cap \mathcal{I}_0| + |\mathcal{I}_B \cap \mathcal{I}_1| - |\mathcal{I}_G \cap \mathcal{I}_1| - |\mathcal{I}_B \cap \mathcal{I}_0| > 0 \\ 1 & \text{otherwise} \end{cases} \tag{4.15}$$

In order to compute a lower bound on Alice's probability to cheat, we call Z the random variable such that

$$Z := |\mathcal{I}_G \cap \mathcal{I}_0| + |\mathcal{I}_B \cap \mathcal{I}_1| - |\mathcal{I}_G \cap \mathcal{I}_1| - |\mathcal{I}_B \cap \mathcal{I}_0| . \tag{4.16}$$

If we restrict ourselves in the case where $c = 0$ (the result holds when $c = 1$ for symmetry reasons), we can see that

$$P_{guess} = \Pr\left(\hat{c} = 0\right) = \Pr\left(Z > 0\right). \tag{4.17}$$

We will use a more general version of the Hoeffding's inequality: if $X_1, X_2, \ldots, X_m$ are m identically and independently distributed random variables such that $\forall i \in [m], X_i \in [a, b]$, then $\forall t > 0$,

$$\Pr\left(\sum_{i=1}^{m} X_i - \mathbb{E}\left(\sum_{i=1}^{m} X_i\right) \leq -t\right) \leq e^{-\frac{2t^2}{m(b-a)^2}} \tag{4.18}$$

We can now see that Z is a sum of n independent variables: $Z = \sum_{i=1}^{n} Z_i$, where

$$Z_i := \begin{cases} 0 & \text{if Bob sent 1 or 0 photons} \\ +1 & \text{if Bob sent more than one photon and } i \in (\mathcal{I}_G \cap \mathcal{I}_0) \cup (\mathcal{I}_B \cap \mathcal{I}_1) \\ -1 & \text{if Bob sent more than one photon and } i \in (\mathcal{I}_B \cap \mathcal{I}_0) \cup (\mathcal{I}_G \cap \mathcal{I}_1) , \end{cases}$$

$\forall i \in [n]$. We can see that the probability distribution of Z_i is given by

$$Z_i := \begin{cases} 0 & \text{with probability } 1 - \gamma \\ +1 & \text{with probability } \gamma\nu \\ -1 & \text{with probability } \gamma\left(1 - \nu\right), \end{cases}$$

$\forall i \in [n]$. We then have using Hoeffding's inequality, for $t > 0, a = -1, b = 1$,

$$\Pr\left(Z - \mathbb{E}\left(Z\right) \leq -t\right) \leq e^{-\frac{2t^2}{4n}},$$

we can take $t = \mathbb{E}\left(Z\right) = \gamma n\left(2\nu - 1\right)$, and we are left with

$$\Pr\left(Z \leq 0\right) \leq e^{-\frac{2[\gamma n(2\nu-1)]^2}{4n}} \tag{4.19}$$

$$\Pr\left(Z \leq 0\right) \leq e^{-n\frac{\gamma^2(2\nu-1)^2}{2}}. \tag{4.20}$$

Having $P_{guess} = \Pr(Z > 0)$, we finally have

$$P_{guess} \geq 1 - e^{-n\frac{\gamma^2(2\nu-1)^2}{2}}. \tag{4.21}$$

This gives us a lower bound on the probability that Alice has to guess Bob's bit correctly which tends to 1 when n gets large (as $\nu > \frac{1}{2}$), which indicates that not any form of weak OT can be achieved using [21, Protocol II.2].

4.2 Investigating a reduction from OT to BC under the MDI setting with imperfect sources

The authors in [25] show a reduction which allows to obtain a secure OT protocol from a BC black box, this reduction is called the BBCS protocol. We will assume here that we have a secure MDI-BC protocol safe under multiphoton emissions (for instance, the MDI-RSC protocol from [21, Protocol II.3]) and investigate whether such a reduction allows to build an MDI-OT protocol secure under multiphoton emissions. Note that if one has access to a secure protocol for randomized string commitment, they can build a secure non-randomized string commitment protocol, as explained in [13, Section IV.A]: if Alice wants to commit to an input string Y_1^ℓ and receives a random committed sting C_1^ℓ during the commit phase of the protocol, she can send $M_1^\ell := Y_1^\ell \oplus C_1^\ell$ to Bob at the end of this phase, who can discover Y_1^ℓ at the end of the open phase (where he receives C_1^ℓ) by computing $M_1^\ell \oplus C_1^\ell = Y_1^\ell$. If the original randomized string commitment is secure for Alice, Bob has no information about C_1^ℓ in the commit phase and M_1^ℓ can be seen as a one-time pad encryption of Alice's string, proving security for Alice. Nothing changes regarding the security for Bob as the string on which Alice and Bob perform the commitment is still actually C_1^ℓ.

4.2.1 BBCS MDI-OT protocol with perfect single photon sources

The BBCS protocol can be found in [25] and allows to build safe Oblivious Bit Transfer from Bit commitment, with non-MDI settings and assuming no bit flips in the quantum communication channel. The security proof for this protocol can be separately found in [35] (security for Alice) and [2] (security for Bob). A proof was later provided using a framework for analyzing sampling strategies by Bouman [36], on a slightly modified version of this protocol. In [37, Section 6.1], a protocol is given to implement oblivious string transfer from the BBCS protocol, using hash functions instead of parity values.

We now present an altered version of this protocol to provide security under the MDI setting with the bounded storage assumption. This version also outputs a randomized string in order to match with Ribeiro's protocol for Randomized Oblivious String Transfer [21, Protocol II.2]. Similarly to [21, Protocol II.2], we make use of an intermediate measurement station to construct a secure protocol under the MDI setting.

We define for this protocol the parameter

$$\zeta := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{2n}} \tag{4.22}$$

and we note $\lambda := \frac{\ell}{n}$ the rate of the protocol, where ℓ is the length of the strings S_0 and S_1 and $2n$ is the total number of quantum communication rounds.

Protocol 6: Modified BBCS for $\binom{2}{1}$-Randomized Oblivious String Transfer from Bit Commitment (MDI)

Inputs: The security parameter ε, the length ℓ of the strings Alice will receive, a bound $D < n$ on the size of Bob's quantum memory (in number of qubits).

1. For round $i \in [1, 2n]$, where $n > 8\ell + 4D$:
   (a) Alice chooses $(X_i, \Theta_i) \in_U \{0,1\}^2$ uniformly at random. She prepares and send $|X_i\rangle_{\Theta_i}$ to the measurement station.
   (b) Bob chooses $(\hat{X}_i, \hat{\Theta}_i) \in_U \{0,1\}^2$ uniformly at random. He prepares and send $|\hat{X}_i\rangle_{\hat{\Theta}_i}$ to the measurement station.
   (c) The measurement station performs a Bell measurement on the two states it receives and publicly reveals the outcome (or reveals that the measurement failed). Bob decides based on the output of a successful measurement whether he should flip his bit $\hat{X}_i$ or not.
2. For $i \in [1, n]$:

(a) Bob commits to $\left(\hat{X}_i, \hat{\Theta}_i\right)$ and $\left(\hat{X}_{n+i}, \hat{\Theta}_{n+i}\right)$.

(b) Alice chooses $f_i \in_U \{0,1\}$ and announces it to Bob.

(c) Bob opens his value $\left(\hat{X}_{n\times f_i+i}, \hat{\Theta}_{n\times f_i+i}\right)$.

(d) Alice checks that $\Theta_{n\times f_i+i} = \hat{\Theta}_{n\times f_i+i} \implies X_{n\times f_i+i} = \hat{X}_{n\times f_i+i}$, otherwise she aborts the protocol.

(e) if $f_i = 0$ then Alice sets $\Theta_i \leftarrow \Theta_{n+i}$ and $X_i \leftarrow X_{n+i}$, and Bob sets $\hat{\Theta}_i \leftarrow \hat{\Theta}_{n+i}$ and $\hat{X}_i \leftarrow \hat{X}_{n+i}$.

3. Alice announces $\Theta_1^n = (\Theta_1, \ldots, \Theta_n)$ to Bob, who computes the set $\mathcal{I}$ of rounds where $\Theta_i = \hat{\Theta}_i$.
4. Bob checks that $|\mathcal{I}| \geq n\left(\frac{1}{2} - \zeta\right) =: m$. If this is the case, he randomly truncates $\mathcal{I}$ so that $|\mathcal{I}| = m$, otherwise he aborts the protocol.
5. Bob randomly generates his choice bit $C \in_U \{0,1\}$
6. Bob picks a random subset $\mathcal{I}'$ of $[n] \setminus \mathcal{I}$ of size m, and he renames $(\mathcal{I}, \mathcal{I}')$ into $(\mathcal{I}_C, \mathcal{I}_{1-C})$ before sending $(\mathcal{I}_0, \mathcal{I}_1)$ to Alice.
7. Alice chooses two 2-universal hash functions $r_0, r_1 \in_U \mathcal{R}$ and sends them over to Bob.
8. Alice outputs $(S_1, S_0) = (\mathrm{Ext}\left(X_{\mathcal{I}_0}, r_0\right), \mathrm{Ext}\left(X_{\mathcal{I}_1}, r_1\right))$.
9. Bob outputs $\hat{S}_C = \mathrm{Ext}\left(X_{\mathcal{I}_C}, r_C\right)$.

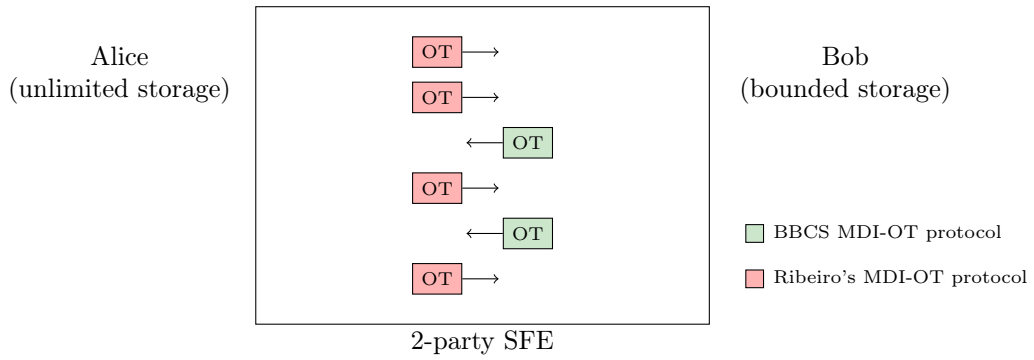
Note that this protocol assumes that there are no bit flips in the protocol ($p_{err} = 0$). For a protocol which accounts for bit flips ($p_{err} > 0$), see Section 4.2.3.

4.2.1.1 Differences between the two MDI-OT protocols

The steps 1 to 4 of Protocol 6 can be seen as giving the same output state as the preparation phase of [21, Protocol II.2], and we follow the same classical post processing. This classical post processing is also close to the one done in the original BBCS protocol (the major changes being the size of $\mathcal{I}_0$ and $\mathcal{I}_1$, and the output of strings using hash functions). We make sure that Bob does not keep qubits without measuring them using bit commitment. The $2n$ rounds then correspond to n code bits (which will be used in X_1^n) and n check bits (which are used for Alice to know whether Bob has tried to cheat by not measuring the qubits).

One important difference between these two protocols is with respect to the party for which we make the bounded/noisy quantum storage assumption. If we use [21, Protocol II.3] for implementing the bit commitment in Protocol 6 for MDI-OT, the bounded/noisy storage assumption has to be made on Alice's quantum memory. In Ribeiro's protocol for MDI-OT [21, Protocol II.2], the assumption is made on Bob's storage. According to [37, Corollary 6.2], the protocol is computationally secure against a dishonest Bob, as long as $\ell < \frac{n}{8}$, without making the bounded/noisy quantum storage assumption on Bob.

Knowing this, as reductions of secure function evaluation to OT can involve oblivious transfers from Alice to Bob and from Bob to Alice, one could design reductions which only imply the bounded storage assumption on one of the two parties (for instance the client in a client-server scenario) using one or the other of these two OT implementations to ensure that the same party is assumed to have bounded storage.



4.2.1.2 Security of the BBCS MDI-OT protocol with perfect single photon sources

We prove here the security of Protocol 3 in the bounded storage model. Note that we make here the assumption that Bob has a bounded storage, and using an MDI-BC protocol for Bob to commit his measurements to Alice will likely require to make the bounded storage assumption on Alice as well.

Theorem 4.3. *Security of the BBCS MDI-OT protocol*

We prove here that the protocol is ε-secure, if $n > 8\ell + 4D$, where D is an upper bound on the size of Bob's quantum storage. In particular, the protocol is ε-correct, $(\varepsilon = 0)$-hiding, and $(\varepsilon = 0)$-binding.

Proof. Let us start with the correctness: if both Alice and Bob are honest and Bob does not abort the protocol, the protocol runs correctly. Indeed, if Bob is honest, Alice will not abort the protocol. Bob can abort in step 4 if $|\mathcal{I}|$ is too small, which happens with probability at most ε using Hoeffding's inequality.

Regarding the security for Alice, if Bob is dishonest, we can use a similar argument as in [21, Figure 7] to see that the MDI situation is equivalent to the one where Alice sends her states directly to Bob who performs the measurement. We can then use the proof regarding the non-MDI case [37, Corollary 6.2], where Protocol 3 can be seen as the compilation $\mathcal{C}^{\alpha}$ of a BBCS protocol without commitment, where $\alpha = \frac{1}{2}$ is the proportion of the rounds used for the verification of the commitments. This theorem then tells us that the protocol is unconditionally secure against a dishonest Bob as if $\gamma = \frac{D}{n}$, we have $\gamma < \frac{1}{4} - 2\lambda$.

For the security for Bob, during the steps 1 to 4 and assuming that Bob uses a perfect single photon source, Alice does not get any information about the bases $\hat{\Theta}_i$ that he did not commit to due to the BB84 encoding. As Alice and Bob will later use the rounds to which Bob did not commit to, even an imperfect bit commitment scheme does not allow Alice to gain information. Alice then has no information about $\mathcal{I}$ and has no way of distinguishing between $\mathcal{I}_c$ and $\mathcal{I}_{1-c}$. Alice can then only randomly guess C, and the protocol is $(\varepsilon = 0)$-binding. □

4.2.2 Attack strategy against the BBCS MDI-OT protocol with multiphoton emissions

We recall here that in order to cheat, a dishonest Alice will try to guess Bob's choice bit c. We will adapt here the cheating strategy for Alice from the one described against the protocol [21, Protocol II.2]. As in this proof, Bob will use an imperfect single photon source (for instance weak coherent laser pulses) which emits 2 photons or more with probability γ. For a round where Bob emitted multiple photons, a dishonest Alice controlling the measurement station has an average probability $\nu \leq 1$ to guess Bob's encoding basis.

In the BBCS MDI-OT protocol, dishonest Alice is able to arbitrary choose the value f_i in the step 2, allowing her to choose between the rounds n and $n + i$ if one of them represents a multiphoton emission. We will then consider that after step 2, a round $i \in [n]$ represents a multiphoton emission with probability $\gamma' = 1 - (1 - \gamma)^2 \geq \gamma$, and for each of these rounds, Alice will in average guess the basis with probability ν.

Alice can then use the same attack strategy as the one given to attack [21, Protocol II.2], and she will obtain an overall cheating probability

$$P_{guess} \geq 1 - e^{-n\frac{\gamma'^2(2\nu-1)^2}{2}}.$$

Claim 4.1. This result suggests that any protocol for OT using a Weak String Erasure-like protocol as part of it with a classical post-processing similar to the one done in [21, Protocol II.2] will be vulnerable for Bob under the MDI setting if he uses an imperfect single photon source. Indeed, the multiphoton emissions will leak information about $\mathcal{I}$ (the set of rounds where Alice and Bob used the same basis), allowing her to guess which of the two sets $\mathcal{I}_0$ and $\mathcal{I}_1$ contains rounds that corresponds to Bob's set $\mathcal{I}$, letting her guess C with a high probability.

4.2.3 BBCS MDI-OT protocol to deal with bit flips

We now present an altered version of this protocol to provide security under the MDI setting and account for bit flips using error correction and an accumulator which aims to help Alice detecting whether Bob has likely tried to cheat by wrongly committing to too many measurements. We do not give here a security proof but we let this protocol as a potential lead for future work.

We define for this protocol the parameter $\zeta := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{2n}}$

Protocol 7: Modified BBCS for $\binom{2}{1}$-Randomized Oblivious String Transfer from Bit Commitment (MDI) accounting for bit flips

Inputs: The security parameter ε, the length ℓ of the strings Alice will receive, a bound $D < n$ on the size of Bob's quantum memory (in number of qubits).

1. For round $i \in [1, 2n]$, where $n > 8\ell + 4D$:
   (a) Alice chooses $(X_i, \Theta_i) \in_U \{0,1\}^2$ uniformly at random. She prepares and send $|X_i\rangle_{\Theta_i}$ to the measurement station.
   (b) Bob chooses $(\hat{X}_i, \hat{\Theta}_i) \in_U \{0,1\}^2$ uniformly at random. He prepares and send $|\hat{X}_i\rangle_{\hat{\Theta}_i}$ to the measurement station.
   (c) The measurement station performs a Bell measurement on the two states it receives and publicly reveals the outcome (or reveals that the measurement failed). Bob decides based on the output of a successful measurement whether he should flip his bit $\hat{X}_i$ or not.
2. Alice initializes her accumulator A to 0.
3. For $i \in [1, n]$:
   (a) Bob commits to $\left(\hat{X}_i, \hat{\Theta}_i\right)$ and $\left(\hat{X}_{n+i}, \hat{\Theta}_{n+i}\right)$.
   (b) Alice chooses $f_i \in_U \{0,1\}$ and announces it to Bob.
   (c) Bob opens his value $\left(\hat{X}_{n\times f_i+i}, \hat{\Theta}_{n\times f_i+i}\right)$.
   (d) Alice checks that $\Theta_{n\times f_i+i} = \hat{\Theta}_{n\times f_i+i} \implies X_{n\times f_i+i} = \hat{X}_{n\times f_i+i}$, otherwise she adds 1 to A.
   (e) if $f_i = 0$ then Alice sets $\Theta_i \leftarrow \Theta_{n+i}$ and $X_i \leftarrow X_{n+i}$, and Bob sets $\hat{\Theta}_i \leftarrow \hat{\Theta}_{n+i}$ and $\hat{X}_i \leftarrow \hat{X}_{n+i}$.
4. Alice verifies that the value A lies in the interval $](p_{err} - \zeta)\, n; (p_{err} + \zeta)\, n[$, otherwise she aborts the protocol.
5. Alice announces $\Theta_1^n = (\Theta_1, \ldots, \Theta_n)$ to Bob, who computes the set $\mathcal{I}$ of rounds where $\Theta_i = \hat{\Theta}_i$.
6. Bob checks that $|\mathcal{I}| \geq n\left(\frac{1}{2} - \zeta\right) =: m$. If this is the case, he randomly truncates $\mathcal{I}$ so that $|\mathcal{I}| = m$, otherwise he aborts the protocol.

7. Bob randomly generates his choice bit $c \in_U \{0,1\}$
8. Bob picks a random subset $\mathcal{I}'$ of $[n] \setminus \mathcal{I}$ of size m, and he renames $(\mathcal{I}, \mathcal{I}')$ into $(\mathcal{I}_c, \mathcal{I}_{1-c})$ before sending $(\mathcal{I}_0, \mathcal{I}_1)$ to Alice.
9. Alice sends Bob error correction information for the strings $X_{\mathcal{I}_0}$ and $X_{\mathcal{I}_1}$.
10. Bob uses the error correction information to correct his string $X_{\mathcal{I}_c}$.
11. Alice chooses two 2-universal hash functions $r_0, r_1 \in_U \mathcal{R}$ and sends them over to Bob.
12. Alice outputs $(S_1, S_0) = (\mathrm{Ext}(X_{\mathcal{I}_0}, r_0), \mathrm{Ext}(X_{\mathcal{I}_1}, r_1))$.
13. Bob outputs $\hat{S}_c = \mathrm{Ext}(X_{\mathcal{I}_c}, r_c)$.

4.3 Improving the rate of protocol [21, Protocol II.3]

This section was motivated by our calculation of ν in equation (4.14) that shows that we do not have to make the assumption that $\nu = 1$ i.e. Alice correctly knows Bob's basis whenever a multiphoton emission occurs. The aim to show that not making the assumption $\nu = 1$ gives a smaller lower bound on the minimum distance of the code d from equation (4.46), which will then allow to use [21, Protocol II.3] with less quantum communication rounds while keeping the same length of committed string ℓ.

We start by removing a circularity error in the parameters defined in [21, Lemma IV.19], using the work of Juliette van Mil, who is currently working on her master thesis project in order to give protocol [21, Protocol II.3] without these circular parameters (Section 4.3.1). We also rewrite one lemma which gives the security for Bob for this protocol ([21, Lemma IV.19]) to correct the derivation and more easily adapt it to the case $\nu < 1$, and we finally take $\nu < 1$ to provide a tighter lower bound on the rate of the protocol without affecting its overall security.

4.3.1 Corrections on the MDI-RSC protocol [21, Lemma IV.19]

Let us first recall the parameters of the protocol: Alice and Bob will use imperfect single photon sources which emits 2 photons or more with probability $\gamma \in \left[0, \frac{1}{2}\right[$. We assume that bit flips can happen in the quantum communication channel with probability p_{err}, and Alice and Bob give in input the security parameter ϵ as well as D an upper bound on the size of Bob's memory (in qubits). In order to circumvent the information leakage from multiphoton emissions, Alice and Bob will use decoy states. They chose a number $q \geq 2$ of decoy states intensities, and they chose 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 $\{b_s, b_{d_1}, \ldots, b_{d_q}\}$, where a_s and b_s are the signal intensities. For instance, if $i \in [q]$, Alice will use the intensity a_{d_i} with probability $p_{a_{d_i}}$. If n is the number of quantum communication rounds which have not been discarded at the end of the preparation phase of Protocol 8, we define the following parameter:

$$\zeta := \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2n}}. \tag{4.23}$$

The parameter α_4^B defined in [21] is used at the beginning of the protocol [21, Protocol II.3] but its value depends on parameters that are obtained during the execution protocol, which causes circularity issues. According to van Mil's work, we can use instead another parameter $\hat{\alpha}^B := (\gamma + 1)\frac{2\zeta}{p_{a_s}}$ such that $\alpha_4^B \leq \hat{\alpha}^B$ in the beginning of the protocol to fix the circular definitions. We can also define the parameter $\hat{\alpha}^A := (\gamma + 1)\frac{2\zeta}{p_{b_s}}$. We can then use these non-circular parameters at the beginning of the protocol (to define $n^\star$), and keep the values from the original paper for the rest of the computations. From this, we define the following parameters:

$$\zeta_{\bar{\Gamma}} := \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(1-\gamma-\hat{\alpha}^B\right)n}} \tag{4.24}$$

$$\zeta_{\bar{\mathcal{I}}} := \min\left[\frac{1}{2}; \frac{\zeta + \left(1-\gamma-\hat{\alpha}^B\right)\zeta_{\bar{\Gamma}}}{\gamma+\hat{\alpha}^B}\right] \tag{4.25}$$

$$\zeta_{\mathcal{I}} := \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(\frac{1}{2}-\zeta\right)n}} \tag{4.26}$$

$$\zeta_{\mathcal{I}\cap\bar{\Gamma}} := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{2\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\hat{\alpha}^B\right)n}} \tag{4.27}$$

$$\delta := 2\left[\left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\hat{\alpha}^B\right) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1-\gamma-\alpha^B\right) + \frac{\left(p_{err}+\zeta_{\mathcal{I}}\right)\left(\frac{1}{2}+\zeta\right)}{\frac{1}{2}+\zeta_{\bar{\Gamma}}}\right] \tag{4.28}$$

$$\lambda := f\left(-\frac{D}{n}\right) - \left(\gamma+\hat{\alpha}^B\right) - \frac{1}{n}, \tag{4.29}$$

where the function f is defined in equation (3.6).

Van Mil and I decided to introduce new notations that are hopefully more intuitive than the ones in the original paper. Following the notations in [11], we call every parameter that comes from a concentration bound with the letter ζ. Here is a table showing the equivalence between our notations:

Ribeiro's notation [21]	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	$\zeta_{\mathcal{I}}$	$\zeta_{\bar{\Gamma}}$	$\zeta_{\bar{\mathcal{I}}}$	β	ζ^A, ζ^B	α^A, α^B

Table 4.1: *Summary of our notations*

We give here the MDI-BC protocol from Ribeiro's paper:

Protocol 8: Corrected MDI-RSC protocol [21, Protocol II-3]

Inputs: Security parameters ϵ and ϵ_1 (ϵ_1 is used to compute the bounds using the decoy states technique, see [21, Lemma IV.15]), ℓ the length of the committed string, the parameter $\gamma \in \left[0, \frac{1}{2}\right[$ which is the probability of multiphoton emissions, the maximum size D of Bob's quantum memory, the expected proportion of bit flips 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 $\{b_s, b_{d_1}, \ldots, b_{d_q}\}$.

Preparation phase

1. Alice and Bob start by agreeing on the total number of round N. N is such that

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n^\star, \tag{4.30}$$

where p is the probability that a round i is not discarded if both parties are honest and $n^\star$ is the smallest integer solution to

$$n \geq \frac{\ell + 2\log\left(\frac{1}{2\epsilon}\right) + \ln\left(\frac{1}{\epsilon}\right)}{\lambda - h\left(\delta\right)}, \tag{4.31}$$

where λ and δ are in equations (4.28) and (4.29). We have $p = p_{a_s} \times p_{b_s} \times (1 - p_{fail|a_s b_s})$.

2. For round $i \in [N]$:

- Alice chooses $(X_i, \Theta_i) \in_R \{0,1\}^2$ uniformly at random and chooses $a \in \{a_s, a_{d_1}, \ldots, a_{d_q}\}$ according to her probability distribution. She prepares a signal of intensity a encoding X_i in the basis Θ_i and sends $|X_i\rangle_{\Theta_i}$ (where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$) to the measurement station.
- Bob chooses $(\hat{X}_i, \hat{\Theta}_i) \in_R \{0,1\}^2$ uniformly at random and chooses $b \in \{b_s, b_{d_1}, \ldots, b_{d_q}\}$ according to his probability distribution. He prepares a signal of intensity b encoding $\hat{X}_i$ in the basis $\hat{\Theta}_i$ and sends $|\hat{X}_i\rangle_{\hat{\Theta}_i}$ (where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$) to the measurement station.
- The measurement station performs a measurement on the two states it receives and publicly reveals the outcome (or reveals that the measurement failed). Bob decides based on the output of a successful measurement whether he should flip his bit $\hat{X}_i$ or not.

3. Alice and Bob publicly announce the intensities they have used for every round $i \in [N]$. We call f_{a_s} and f_{b_s} the fractions of rounds in which respectively Alice and Bob used their signal intensity when the measurement succeeded and the other party also used their signal intensity.

4. Alice computes $\beta^A := \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2(n^A)}}$ where n^A denotes the number of rounds where she used her signal intensity and the measurement succeeded. She checks that $f_{b_s} \geq p_{b_s} - \beta^A$, otherwise she aborts the protocol.

5. Bob computes $\beta^B := \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2(n^B)}}$ where n^B denotes the number of rounds where he used his signal intensity and the measurement succeeded. He checks that $f_{a_s} \geq p_{a_s} - \beta^B$, otherwise he aborts the protocol.

6. The number of round in which both Alice and Bob used their signal intensities is denoted as $n = f_{b_s} \times (n^A) = f_{a_s} \times (n^B)$. Using the decoy states Alice estimates a lower-bound L_{A1} for n_1^A (as given in [21, Lemma IV.15]) which is the number of rounds where the Bell measurement succeeded and Alice emitted exactly one photon with intensity a_s. If $U_{A2} := n - L_{A1} \geq (\gamma + \alpha^A)n$, Alice aborts the protocol.

7. Using the decoy states Bob estimates a lower-bound L_{B1} for n_1^B (as given in [21, Lemma IV.15]) which is the number of rounds where the Bell measurement succeeded and Bob emitted exactly one photon with intensity b_s. If $U_{B2} := n - L_{B1} \geq (\gamma + \alpha^B)n$, Bob aborts the protocol.

8. Alice and Bob discard all the rounds where a failure has been announced, and where the intensities used by Alice and Bob are not a_s and b_s. Alice and Bob check that $n \geq \frac{\ell + 2\log\left(\frac{1}{2\epsilon}\right) + \ln\left(\frac{1}{\epsilon}\right)}{\lambda - h(\delta)}$ and abort the protocol otherwise. Now Alice has the strings X_1^n and Θ_1^n and Bob has the strings $\hat{X}_1^n$ and $\hat{\Theta}_1^n$.

9. Both parties wait for a time Δt.

10. Alice sends Θ_1^n to Bob through a classical channel.

11. Bob computes the set of rounds $\mathcal{I}$ where $\Theta_i = \hat{\Theta}_i$. He discard every rounds which are not in $\mathcal{I}$.

Commit phase

1. Bob checks that the length m of $\mathcal{I}$ is such that $m \in \left[\frac{n}{2} - n\zeta, \frac{n}{2} + n\zeta\right]$, otherwise he aborts the protocol.
2. Alice chooses a random $[n,k]$ linear code $\mathcal{C}$ with k the largest integer such that $\frac{k}{n} \leq 1 - h(\delta) + \frac{\log(\varepsilon)}{n}$ and computes the syndrome of X_1^n given by $w := \mathrm{Syn}_{\mathcal{C}}(X_1^n) \in \{0,1\}^{n-k}$.
3. Alice picks a random r from the 2-universal family of hash functions $\mathcal{R}_\ell^n$ and computes $C_1^\ell := \mathrm{Ext}(X_1^n, r)$.
4. Alice sends w and r to Bob.

Open phase

1. Alice sends X_1^n to Bob.
2. Bob computes the syndrome of X_1^n with the code $\mathcal{C}$ and check that it is indeed equal to w. If it is not the case, Bob aborts the protocol.
3. Bob finally checks that the proportion of indices in which $X_{\mathcal{I}}$ 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 it is the case, Bob accepts and outputs $C_1^\ell := \text{Ext}(X_1^n, r)$, otherwise Bob aborts the protocol.

Lemma 4.1. *Decoy states technique (from [21, Lemma IV.15])*

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 [21, Lemma IV.15]. Then, if $n_1^H \geq L_{H1}$ in step 2 of Protocol 8, the proportion of multiphoton emissions from Bob is at most $\gamma + \alpha^H$, except with probability $16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1$.

Theorem 4.4. *Security proof for Protocol 8.*

Let $\epsilon, \epsilon_1, \varepsilon, \hat{\varepsilon}$ be as defined in Lemma 4.1. If the sources used by the two parties are sufficiently good, i.e,

$$\frac{p_{\geq 2|a_s}}{(1 - p_{0|a_s})} \leq p_{b_s}\gamma, \quad \frac{p_{\geq 2|b_s}}{(1 - p_{0|a_s})} \leq p_{a_s}\gamma. \tag{4.32}$$

then Protocol 8 gives a secure MDI $(\ell, 9\epsilon + 32(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1)$-RSC protocol.

Proof. The correctness and security for Alice are respectively proven in [21, Lemma IV.14] and [21, Lemma IV.17]. In particular, the protocol is $(9\epsilon + 32(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1)$-correct and $(3\epsilon + 16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1)$-secure for Alice. Lemma 4.2 shows that the protocol is $(2\epsilon + 16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1)$-secure for Bob. □

Lemma 4.2. *Security for Bob in Protocol 8*

In order to help the derivations of the improved rate and correct potential derivation errors, we rewrite here the proof of [21, Lemma IV.19], which corresponds to the proof of the security for Bob, to detail the calculation steps. The difference between this lemma and the derivation with perfect single photon sources (Section 3.8) is that Alice now has some information about Bob's set of indices $\mathcal{I}$ due to multiphoton emissions. The aim of this lemma is to show that we can still take a code with a sufficiently high distance d so that a dishonest Alice will cause Bob to abort the protocol (i.e. she flips a proportion higher than $(p_{err} + \zeta_{\mathcal{I}})$ of the bits in $\mathcal{I}$) with high probability, when trying to flip at least $\frac{d}{2}$ bits of her bit string X_1^n.

Let $\Gamma \subseteq [n]$ denote the set of all transmissions for which Bob has emitted multiple photons. We assume here that $\nu = 1$ (this is the assumption made in [21, Lemma IV.19]), which implies that Alice knows the sets $\mathcal{I}_G := \mathcal{I} \cap \Gamma$ and $\mathcal{I}_B := \bar{\mathcal{I}} \cap \Gamma$. Note that we obtain different values for δ and β (α_3) compared to Ribeiro et al, as we believe this is the correct derivation.

We want to estimate an upper bound on $\left|\bar{\mathcal{I}} \cap \Gamma\right|$, which is the number of bits that Alice can flip safely in X_1^n. In order to give this upper bound, we have from 4.1 that after the protocol and using the decoy state technique, the upper bound U_{B2} that Bob computes is greater than $n_{\geq 2}^B$ except with probability $16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1$. If Bob does not abort in the step 7 of the protocol, there are then at most $\left(\gamma + \alpha^B\right) n$ rounds in which Bob emitted 2 or more photons, except with probability $16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1$. This means that

$$|\Gamma| \leq \left(\gamma + \alpha^B\right) n \tag{4.33}$$

$$\left|\bar{\Gamma}\right| \geq \left(1 - \gamma - \alpha^B\right) n, \tag{4.34}$$

except with a small probability.

We can then use Hoeffding's inequality and the fact that $\mathcal{I}$ is randomly and uniformly sampled from $[n]$ to see that

$$\left|\mathcal{I}\cap\bar{\Gamma}\right| \leq \left(\frac{1}{2}+\sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left|\bar{\Gamma}\right|}}\right)\left|\bar{\Gamma}\right| \leq \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left|\bar{\Gamma}\right| \tag{4.35}$$

except with probability $\epsilon + 16\left(\epsilon+\varepsilon+\hat{\varepsilon}\right)+8\epsilon_1$, where

$$\zeta_{\bar{\Gamma}} := \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(1-\gamma-\alpha^B\right)n}}. \tag{4.36}$$

In addition, if the protocol does not abort then the total number of rounds in $\mathcal{I}$ is $|\mathcal{I}| \geq \left(\frac{1}{2}-\zeta\right)n$. We can directly see that

$$\begin{aligned}
\left|\bar{\mathcal{I}}\cap\Gamma\right| &= |\Gamma| + \left|\mathcal{I}\cap\bar{\Gamma}\right| - |\mathcal{I}| \\
&\leq |\Gamma| + \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left|\bar{\Gamma}\right| - |\mathcal{I}| \\
&= |\Gamma| + \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)(n-|\Gamma|) - |\mathcal{I}| \\
&= \left(\frac{1}{2}-\zeta_{\bar{\Gamma}}\right)|\Gamma| + \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)n - |\mathcal{I}| \\
&\leq \left(\frac{1}{2}-\zeta_{\bar{\Gamma}}\right)\left(\gamma+\alpha^B\right)n + \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)n - \left(\frac{1}{2}-\zeta\right)n \\
&\leq \left(\frac{\gamma+\alpha^B}{2} + \left(1-\gamma-\alpha^B\right)\zeta_{\bar{\Gamma}} + \zeta\right)n,
\end{aligned} \tag{4.37}$$

except with probability $\epsilon + 16\left(\epsilon+\varepsilon+\hat{\varepsilon}\right)+8\epsilon_1$.

We can rewrite this upper bound as

$$\left|\bar{\mathcal{I}}\cap\Gamma\right| \leq \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)n, \tag{4.38}$$

except with probability $\epsilon + 16\left(\epsilon+\varepsilon+\hat{\varepsilon}\right)+8\epsilon_1$, where $\zeta_{\bar{\mathcal{I}}} = \min\left[\frac{1}{2}, \frac{\zeta+\left(1-\gamma-\alpha^B\right)\zeta_{\bar{\Gamma}}}{\gamma+\alpha^B}\right]$. We will then use equation (4.38) as an upper bound on $\left|\bar{\mathcal{I}}\cap\Gamma\right|$, except with probability $\epsilon + 16\left(\epsilon+\varepsilon+\hat{\varepsilon}\right)+8\epsilon_1$.

Dishonest Alice still has to flip at least $\frac{d}{2} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)n$ bits outside of $\bar{\mathcal{I}}\cap\Gamma$. However, Alice knows that any flip in $\mathcal{I}\cap\Gamma$ will be detected by Bob, so she will probabilistically only flip bits from $\bar{\Gamma}$, which has at least $\left(1-\gamma-\alpha^B\right)n$ rounds. The choice of the bits to flip within $\bar{\Gamma}$ is then equivalent to uniformly sampling without replacement at least $\frac{d}{2} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)n$ bits out of at least $\left(1-\gamma-\alpha^B\right)n$ positions.

Let us denote by $W_{\bar{\Gamma}}$ the number of rounds belonging to $\mathcal{I}\cap\bar{\Gamma}$ that Alice will flip her bits when she flips $\frac{d}{2} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)n$ bits within $\bar{\Gamma}$. Let us note that the probability that a given round $i\in\bar{\Gamma}$ gets flipped by Alice is given by

$$p \leq \frac{1}{\left(1-\gamma-\alpha^B\right)n}\left(\frac{d}{2} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)n\right). \tag{4.39}$$

We can then write $W_{\bar{\Gamma}}$ as the sum of $\left|\mathcal{I}\cap\bar{\Gamma}\right|$ Bernoulli variables which are equal to 1 with probability p, and we know that $\left|\mathcal{I}\cap\bar{\Gamma}\right| \leq \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n$. The expected value for $W_{\bar{\Gamma}}$ can then be given by

$$\mathbb{E}\left(W_{\bar{\Gamma}}\right) \leq p\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n \tag{4.40}$$

$$\leq \left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(\frac{d}{2} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)n\right) \tag{4.41}$$

$$\leq n\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(\frac{d}{2n} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)\right), \tag{4.42}$$

except with probability $\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$.

We can once again use Hoeffding's inequality to see that

$$\Pr\left(\mathbb{E}\left(W_{\bar{\Gamma}}\right) - W_{\bar{\Gamma}} \geq \sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{2\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n}}\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n\right)$$

$$= \Pr\left(n\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(\frac{d}{2n} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)\right) - W_{\bar{\Gamma}} \geq \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n\right) \tag{4.43}$$

$$= \Pr\left(W_{\bar{\Gamma}} \leq n\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(\frac{d}{2n} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right)\right) - \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n\right) \tag{4.44}$$

$$= \Pr\left(W_{\bar{\Gamma}} \leq n\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(\frac{d}{2n} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right) - \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1-\gamma-\alpha^B\right)\right)\right) \tag{4.45}$$

$$\leq \epsilon$$

where $\zeta_{\mathcal{I}\cap\bar{\Gamma}} := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{2\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(1-\gamma-\alpha^B\right)n}}$.

This gives us that if we take the distance d of the code to satisfy

$$d \geq 2\left[\left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1-\gamma-\alpha^B\right) + \frac{\left(p_{err}+\zeta_{\mathcal{I}}\right)\left(\frac{1}{2}+\zeta\right)}{\frac{1}{2}+\zeta_{\bar{\Gamma}}}\right]n =: \delta n, \tag{4.46}$$

we have

$$W_{\bar{\Gamma}} > n\left(\frac{1}{2}+\zeta_{\bar{\Gamma}}\right)\left(\frac{d}{2n} - \left(\frac{1}{2}+\zeta_{\bar{\mathcal{I}}}\right)\left(\gamma+\alpha^B\right) - \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1-\gamma-\alpha^B\right)\right)$$

$$W_{\bar{\Gamma}} > \left(p_{err}+\zeta_{\mathcal{I}}\right)\left(\frac{1}{2}+\zeta\right)n \geq \left(p_{err}+\zeta_{\mathcal{I}}\right)\left|\mathcal{I}\right|,$$

except with probability $2\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$.

This means that if equation (4.46) is satisfied, a cheating Alice will be detected by Bob, except with probability $1 - 2\epsilon - 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) - 8\epsilon_1$.

4.3.2 Improving the rate of the protocol [21, Protocol II.3]

The aim is now to show that not making the assumption $\nu = 1$ gives security using a smaller lower bound on the minimum distance of the code d from equation (4.46), which will then allow to use [21, Protocol II.3] with less quantum communication rounds for the same length of committed string ℓ.

This assumption was implicitly made in [21] and not making it can intuitively allow us to use the value of ν from equation (4.14) by saying that for every multiphoton emission round (which represent a fraction γ of the total number of rounds), Alice has a probability ν of correctly guessing Bob's basis. However, a dishonest Alice can have access to a photon counter in the measurement station, and we then cannot assume that she will act the same on every round, she can have a strategy which depends on the number of photons sent by Bob. Let us recall that for any round, the probability $p^{\max}_{succ,m}$ that Alice correctly guess Bob's basis when he sends $m \geq 1$ photons is given by equation (4.12) in Section 4.1.1. This is an increasing function with respect to the number m.

Assumption 1. Note that we are here proving security against a semi-honest Alice i.e. we assume that Alice will try to gain advantage over Bob without changing her execution of the protocol during the preparation phase of Protocol 8. However, she is allowed to store the extra photons Bob transmits during multiphoton emissions and can use it after the preparation phase.

If a semi-honest Alice wants to open to a different string other than her committed string X_1^n without being detected by Bob, she will have to flip a suitable set of bits in X_1^n. Whether Bob detects a bit flip at position i depends on whether $\hat{\Theta}_i = \Theta_i$ or $\hat{\Theta}_i \neq \Theta_i$. In order to consider the most general kind of collective attacks that Alice can perform, we can assume that she makes a measurement on the extra photons in each round i of the transmission from Bob to predict $\hat{\Theta}_i$. She can predict Bob's choice of basis $\hat{\Theta}_i$ when Bob emits m photons with probability at most $p^{\max}_{succ,m}$. If Alice's predicts that $\hat{\Theta}_i \neq \Theta_i$ and she flips the bit i, Bob will detect this flip with probability $1 - p^{\max}_{succ,m}$. Similarly, if Alice predicts $\hat{\Theta}_i = \Theta_i$ and she flips the bit i, Bob will detect this flip with probability $p^{\max}_{succ,m}$. Note that $p^{\max}_{succ,m} = \frac{1}{2}$ when $m = 1$, $p^{\max}_{succ,m} > \frac{1}{2}$ for any $m \geq 2$ and $p^{\max}_{succ,m}$ increases with respect to m. Therefore, the best possible cheating strategy for Alice is to flip a suitable number of bits starting with rounds having high m and where she predicts $\hat{\Theta}_i \neq \Theta_i$. We can represent such an attack strategy using a set of fractions $\{f_m, m \geq 1\}$ such that whenever Bob sent m photons and Alice predicts $\hat{\Theta}_i \neq \Theta_i$, she flips the corresponding bit with probability f_m. One intuitive distribution of $\{f_m\}$ would be to say that there is an $m_{\text{th}} \geq 1$ and $f \in [0, 1]$ such that

$$f_m := \begin{cases} 0 & \text{if } m < m_{\text{th}} \\ f & \text{if } m = m_{\text{th}} \\ 1 & \text{if } m > m_{\text{th}}. \end{cases} \tag{4.47}$$

Note that if Alice uses any other attack strategy, Bob will have a higher probability of detecting her cheating compared to using f_m from equation (4.47) for some m_{th} and f.

For every $i \in [n]$, there are 4 cases: i can be in in $\mathcal{I} \cap \Gamma$, in $\mathcal{I} \cap \bar{\Gamma}$, in $\bar{\mathcal{I}} \cap \Gamma$ or in $\bar{\mathcal{I}} \cap \bar{\Gamma}$. For $m \geq 2$, we define Γ_m as the set of rounds where Bob sent exactly m photons, we then have $\Gamma := \Gamma_2 \cup \Gamma_3 \cup \Gamma_4 \cup \ldots$. . We are interested in the number of bits that Alice will flip at indices which are in $\mathcal{I} = (\mathcal{I} \cap \Gamma) \cup \left(\mathcal{I} \cap \bar{\Gamma}\right)$. As Alice has access to a photon counter, we assume that she will first only flip bits corresponding to rounds in Γ (where she has information about $\mathcal{I}$), and then try to randomly flip bits in $\bar{\Gamma}$ until she flipped $\frac{d}{2}$ bits in total. For a round where Bob sent $m \geq 2$ photons, Alice will flip it with probability f_m if she guessed (correctly or not) that the bit is not in $\mathcal{I}$, and her guess will be correct with probability $p^{\max}_{succ,m}$. For Alice to flip a round in $\mathcal{I} \cap \Gamma$, the round needs to be in $\mathcal{I}$ (which happens with probability $\frac{1}{2}$), and Alice has to incorrectly think that it is not in $\mathcal{I}$ and to flip it, which happens with probability

$$\Pr\left(\text{Alice flips } X_i | i \in \mathcal{I} \cap \Gamma_m\right) = f_m \left(1 - p^{\max}_{succ,m}\right). \tag{4.48}$$

As we know the value of p_m, the probability that Bob emits m photons during a given round, Alice will in average incorrectly flip a bit in $\mathcal{I} \cap \Gamma$ with probability

$$\begin{aligned} \Pr\left(\text{Alice flips } X_i | i \in \mathcal{I} \cap \Gamma\right) &= \sum_{m \geq 2} \Pr\left(\text{Alice flips } X_i | i \in \mathcal{I} \cap \Gamma_m\right) \Pr\left(i \in \mathcal{I} \cap \Gamma_m | i \in \mathcal{I} \cap \Gamma\right) \\ &= \sum_{m \geq 2} f_m \left(1 - p^{\max}_{succ,m}\right) \frac{p_m}{1 - p_0} \end{aligned} \tag{4.49}$$

When Alice uses $m_{\text{th}} = 1$, we have $\forall m \geq 2,\ f_m = 1$. The probability from (4.49) when $m_{\text{th}} = 1$ is given by

$$g := \sum_{m \geq 2} \left(1 - p^{\max}_{succ,m}\right) \frac{p_m}{1 - p_0}. \tag{4.50}$$

Since $\forall m \geq 2, p^{\max}_{succ,m} > \frac{1}{2}$, we have $g \leq \frac{p_{\geq 2}}{2(1-p_0)}$, with $p_{\geq 2} := \sum_{m \geq 2} p_m$.

Theorem 4.5. *Security for Protocol 8 with improved rate.*

Protocol 8 with parameters as defined in Theorem 4.4 and δ replaced with

$$\begin{aligned} \delta' := 2 \Bigg[&\left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) + \zeta_{\mathcal{I} \cap \bar{\Gamma}}\left(1 - \gamma - \alpha^B\right) + \frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} \\ &- \left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\left(g - \zeta_{\mathcal{I} \cap \Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right)\Bigg] \end{aligned} \tag{4.51}$$

and p_{err} satisfying

$$p_{err} > \frac{1}{2}\left(\frac{p_{\geq 2}}{1 - p_0}\right)^2 + \frac{3}{4}\frac{p_{\geq 2}}{1 - p_0} \tag{4.52}$$

gives an MDI $(\ell, 9\epsilon + 32\,(\epsilon + \varepsilon + \hat{\varepsilon}) + 16\epsilon_1)$*-RSC protocol which is correct, secure against dishonest Bob and secure against any collective attack by a semi-honest Alice, which improves the rate of the protocol, as presented numerically in Figure 4.3.*

Proof. We know that $|\mathcal{I}| \geq \left(\frac{1}{2} - \zeta\right) n$ except with probability ϵ. If we call $p_{\geq 2} := \sum_{m \geq 2} p_m$ the probability to send 2 photons or more (this is then the probability of a given round to be in Γ), we can once again use Hoeffding's inequality to find that

$$|\mathcal{I} \cap \Gamma| \geq \left(\frac{p_{\geq 2}}{1 - p_0} - \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\,|\mathcal{I}|}}\right) |\mathcal{I}| \tag{4.53}$$

$$\geq \left(\frac{p_{\geq 2}}{1 - p_0} - \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(\frac{1}{2} - \zeta\right) n}}\right) \left(\frac{1}{2} - \zeta\right) n \tag{4.54}$$

$$|\mathcal{I} \cap \Gamma| \geq \left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right) \left(\frac{1}{2} - \zeta\right) n, \tag{4.55}$$

except with probability 2ϵ, where

$$\zeta_{\mathcal{I}} = \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(\frac{1}{2} - \zeta\right) n}}. \tag{4.56}$$

Case 1: $m_{\text{th}} = 1$.

Let U_Γ be the number of bits Alice flips within $\bar{\mathcal{I}} \cap \Gamma$ and W_Γ be the number of bits Alice flips within $\mathcal{I} \cap \Gamma$. We then have, using Hoeffding's inequality, that W_Γ is bounded by

$$W_\Gamma \geq \left(g - \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\,|\mathcal{I} \cap \Gamma|}}\right) |\mathcal{I} \cap \Gamma| \tag{4.57}$$

$$\geq \left(g - \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(\frac{p_{\geq 2}}{1-p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right) n}}\right) \left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right) \left(\frac{1}{2} - \zeta\right) n \tag{4.58}$$

$$\geq \left(g - \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(\frac{p_{\geq 2}}{1-p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right) n}}\right) \left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right) \left(\frac{1}{2} - \zeta\right) n, \tag{4.59}$$

except with probability 3ϵ. If we define

$$\zeta_{\mathcal{I}\cap\Gamma} := \sqrt{\frac{\ln\left(\frac{1}{\epsilon}\right)}{2\left(\frac{p_{\geq 2}}{1-p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right) n}}. \tag{4.60}$$

we have

$$W_\Gamma \geq (g - \zeta_{\mathcal{I}\cap\Gamma}) \left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right) \left(\frac{1}{2} - \zeta\right) n, \tag{4.61}$$

except with probability 3ϵ. Similarly, we can define an upper bound on W_Γ as

$$W_\Gamma \leq (g + \zeta_{\mathcal{I}\cap\Gamma}) \left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right) \left(\frac{1}{2} + \zeta\right) n, \tag{4.62}$$

except with probability 3ϵ.

After flipping U_Γ bits in $\bar{\mathcal{I}} \cap \Gamma$ and W_Γ bits in $\mathcal{I} \cap \Gamma$, Alice still needs to flip $\frac{d}{2} - U_\Gamma - W_\Gamma$ bits in $\bar{\Gamma}$. Since

$$U_\Gamma \leq \left|\bar{\mathcal{I}} \cap \Gamma\right| \leq \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right) \left(\gamma + \alpha^B\right) n, \tag{4.63}$$

except with probability $\epsilon+$ Alice still needs to flip at least $\frac{d}{2} - \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n - W_\Gamma$ bits within $\bar{\Gamma}$, which has at least $\left(1 - \gamma - \alpha^B\right) n$ rounds. The choice of the bits to flip within $\bar{\Gamma}$ is then equivalent to uniformly sampling without replacement at least $\frac{d}{2} - \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n - W_\Gamma$ bits out of at least $\left(1 - \gamma - \alpha^B\right) n$ positions. Alice then has less margin of error, as she will have already wrongly flipped W_Γ bits in $\mathcal{I} \cap \Gamma$ (which will be detected by Bob). Bob will detect a cheating by Alice if the number of flips in $\bar{\Gamma}$ exceeds $\left(p_{err} + \zeta_{\mathcal{I}}\right)|\mathcal{I}| - W_\Gamma$.

We can then reuse equation (4.46) from Lemma 4.2, replacing

$$\frac{d}{2} - \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n \text{ with } \frac{d}{2} - \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n - W_\Gamma \text{ and}$$
$$\left(p_{err} + \zeta_{\mathcal{I}}\right)|\mathcal{I}| \text{ with } \left(p_{err} + \zeta_{\mathcal{I}}\right)|\mathcal{I}| - W_\Gamma$$

This gives us that if we take the distance d of the code to satisfy

$$d \geq 2\left[\left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1 - \gamma - \alpha^B\right) + \frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right) - \frac{W_\Gamma}{n}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} + \frac{W_\Gamma}{n}\right] n \tag{4.64}$$

$$\geq 2\left[\left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1 - \gamma - \alpha^B\right) + \frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} - \frac{W_\Gamma}{n}\left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\right] n \tag{4.65}$$

we have $W_{\bar{\Gamma}} + W_\Gamma \geq \left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right) n \geq \left(p_{err} + \zeta_{\mathcal{I}}\right)|\mathcal{I}|$, except with a probability less than $5\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$.

Using the lower bound on W_Γ from equation (4.35), if d satisfies

$$d \geq 2\left[\left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1 - \gamma - \alpha^B\right) + \frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right.$$
$$\left. - \left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\left(g - \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right)\right] n \tag{4.66}$$

$$=: \delta' n, \tag{4.67}$$

then Bob will detect more than $\left(p_{err} + \zeta_{\mathcal{I}}\right)|\mathcal{I}|$ *, except with probability* $5\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$.

Case 2: $m_{\text{th}} \geq 2$.

Similar to the case where $m_{th} = 1$, let U_Γ be the number of bits Alice flips within $\bar{\mathcal{I}} \cap \Gamma$ and W_Γ be the number of bits Alice flips within $\mathcal{I} \cap \Gamma$. Note that upper bounds for U_Γ and W_Γ when $m_{th} = 1$ are also upper bounds for U_Γ and W_Γ when $m_{th} \geq 2$. This implies that

$$U_\Gamma \leq \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n \tag{4.68}$$

except with probability $\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$, and

$$W_\Gamma \leq \left(g + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right) n \tag{4.69}$$

except with probability 3ϵ.

The total number of flips made by Alice in Γ, given by $U_\Gamma + W_\Gamma$, is bounded as

$$U_\Gamma + W_\Gamma \leq \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n + \left(g + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right) n \tag{4.70}$$

$$\leq \left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) n + \left(\frac{1}{2}\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right) n \tag{4.71}$$

except with probability $4\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$. We know that

$$\frac{d}{2} \geq \left[\left(\frac{1}{2} + \zeta_{\bar{\mathcal{I}}}\right)\left(\gamma + \alpha^B\right) + \zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1 - \gamma - \alpha^B\right) + \frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} - \left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\left(g - \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right)\right] n. \tag{4.72}$$

Using the two bounds from equations (4.72) and (4.71), we get that

$$\begin{aligned}
\frac{d}{2} - U_\Gamma - W_\Gamma &\geq \left[\zeta_{\mathcal{I}\cap\bar{\Gamma}}\left(1 - \gamma - \alpha^B\right) + \frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} - \left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\left(g - \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} - \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} - \zeta\right)\right. \\
&\qquad \left. - \left(\frac{1}{2}\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)\right] n && (4.73) \\
&\geq \left[\frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} - \left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\left(g + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)\right. \\
&\qquad \left. - \left(\frac{1}{2}\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\left(\frac{1}{2} + \zeta\right)\right] n && (4.74) \\
&\geq \left(\frac{1}{2} + \zeta\right)\left[\frac{\left(p_{err} + \zeta_{\mathcal{I}}\right)}{\frac{1}{2} + \zeta_{\bar{\Gamma}}} - \left(\frac{\frac{1}{2} - \zeta_{\bar{\Gamma}}}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\right)\left(\frac{1}{2}\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\right. \\
&\qquad \left. - \left(\frac{1}{2}\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1 - p_0} + \zeta_{\mathcal{I}}\right)\right] n && (4.75) \\
&= \frac{\frac{1}{2} + \zeta}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\left[p_{err} - \frac{1}{2}\left(\frac{p_{\geq 2}}{1 - p_0}\right)^2 - \frac{p_{\geq 2}}{1 - p_0}\left(\frac{\zeta_{\mathcal{I}}}{2} + \zeta_{\mathcal{I}\cap\Gamma}\right) + \zeta_{\mathcal{I}} - \zeta_{\mathcal{I}}\zeta_{\mathcal{I}\cap\Gamma}\right] n && (4.76) \\
&\geq \frac{\frac{1}{2} + \zeta}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\left[p_{err} - \frac{1}{2}\left(\frac{p_{\geq 2}}{1 - p_0}\right)^2 - \frac{p_{\geq 2}}{1 - p_0}\left(\frac{\zeta_{\mathcal{I}}}{2} + \zeta_{\mathcal{I}\cap\Gamma}\right)\right] n && (4.77) \\
&\geq \frac{\frac{1}{2} + \zeta}{\frac{1}{2} + \zeta_{\bar{\Gamma}}}\left[p_{err} - \frac{1}{2}\left(\frac{p_{\geq 2}}{1 - p_0}\right)^2 - \frac{3}{4}\frac{p_{\geq 2}}{1 - p_0}\right] n && (4.78) \\
&> 0 && (4.79)
\end{aligned}$$

except with probability $4\epsilon + 16\left(\epsilon + \varepsilon + \hat{\varepsilon}\right) + 8\epsilon_1$. This implies that Alice will not be able to flip $\frac{d}{2}$ or more bits by taking $m_{th} \geq 2$, except with a small probability. We can then assume that Alice will use $m_{th} = 1$. □

Note that in the case 1, $\delta' < \delta$. The value δ is crucial as it is used in the equation (37) of [21] to give the rate $\frac{\ell}{n}$ of the protocol

$$n \geq \frac{\ell + 2\log\left(\frac{1}{2\epsilon}\right) + \ln\left(\frac{1}{\epsilon}\right)}{\lambda - h\left(\delta\right)}, \tag{4.80}$$

and in the equation for the $[n, k]$-error correcting code used by Alice and Bob

$$\frac{k}{n} \leq 1 - h\left(\delta\right) + \frac{\log\left(\frac{1}{\epsilon}\right)}{n}. \tag{4.81}$$

Considering the values of $\zeta_{\mathcal{I}}$, $\zeta_{\mathcal{I}\cap\Gamma}$, γ , α^B, p_{err}, $\zeta_{\mathcal{I}}$ and ζ are all very small compared to 1 in a realistic context, we will have $\delta < \frac{1}{2}$, and then $h\left(\delta'\right) < h\left(\delta\right)$. This will then allow to decrease the number of successful rounds $n^\star$ which is the smallest integer satisfying equation (4.80), which then improves the rate of the protocol. The new value δ' also allows to reduce the size of the syndrome $w \in \{0,1\}^{n-k}$ that Alice sends to Bob, reducing the classical communication needed.

If Alice's attack strategy is to have $m_{\text{th}} \geq 1$ and $f \in [0, 1]$ such that

$$f_m := \begin{cases} 0 & \text{if } m = 0 \\ f & \text{if } m = 1 \\ 1 & \text{if } m \geq 2, \end{cases}$$

we then reduce the value δ by

$$\frac{2W_\Gamma}{n}\left(\frac{\frac{1}{2}-\zeta_{\bar{\Gamma}}}{\frac{1}{2}+\zeta_{\bar{\Gamma}}}\right)=\left(\frac{\frac{1}{2}-\zeta_{\bar{\Gamma}}}{\frac{1}{2}+\zeta_{\bar{\Gamma}}}\right)\left(\left(f\left(1-p^{\max}_{succ,m_{\text{th}}}\right)\frac{p_{m_{\text{th}}}}{1-p_0}+\sum_{m\geq m_{\text{th}}}\left(1-p^{\max}_{succ,m}\right)\frac{p_m}{1-p_0}\right)-\zeta_{\mathcal{I}\cap\Gamma}\right)\left(\frac{p_{\geq 2}}{1-p_0}-\zeta_{\mathcal{I}}\right)\left(\frac{1}{2}-\zeta\right).$$

The relevence of this improvement is shown in Figure 4.3.

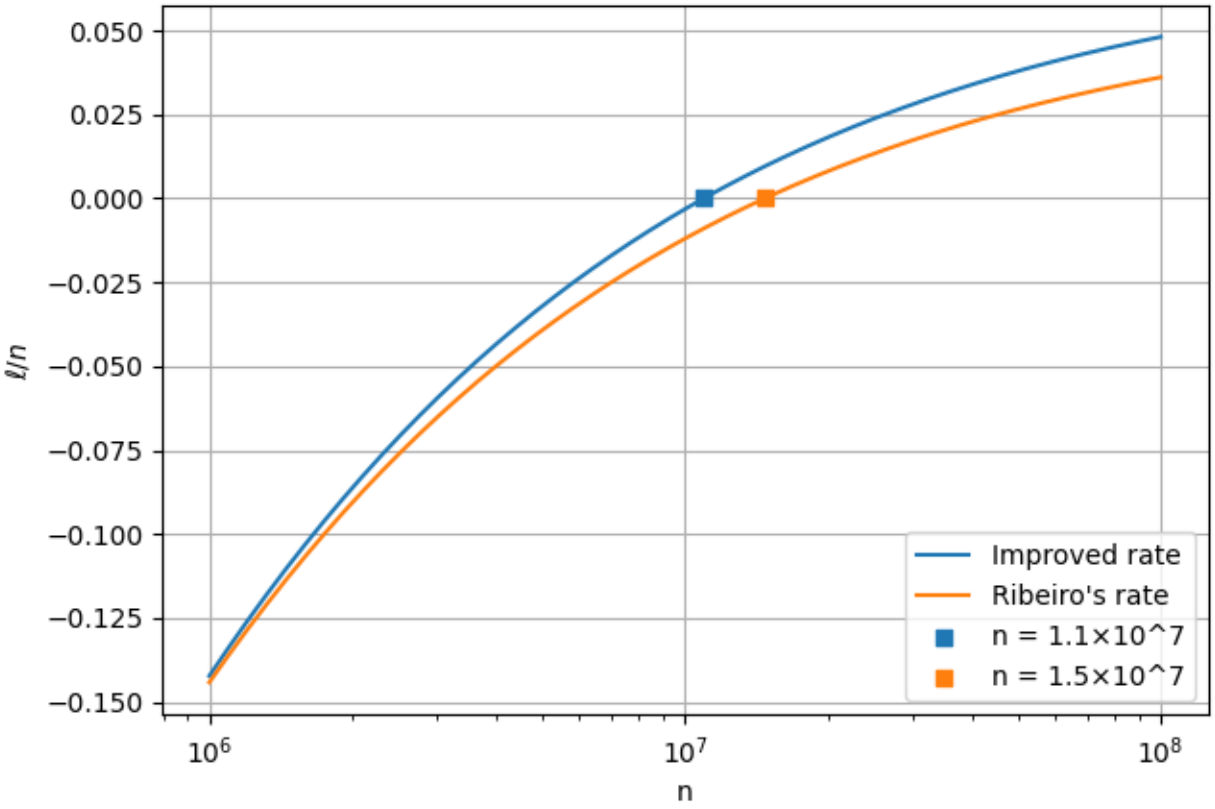


Figure 4.3: *Simulation to show the change of the rate provided with our improvement. We took an intensity* $\chi = 0.01$*, a probability of bit flips in the channel* $p_{err} = 0.0035$*, a security parameter* $\epsilon = 10^{-6}$*. This image was obtained thanks to help from Van Mil in writing the simulation code.*

Chapter 5

Discussion and future work

This chapter gives a summary of the contributions made in this thesis while discussing the impact of these results, and lists other possible approaches that can be taken to make further progress on the topic.

5.1 Discussion

During this thesis, we have discussed the possibility of achieving oblivious transfer under the measurement device independent setting, using imperfect single-photon sources. We defined a new attack strategy to show that the MDI-OT protocol given in [21, Protocol II.2] does not allow implementing $p_A^\star-$weak OT, a weaker version of oblivious transfer, when using imperfect single-photon sources. However, we have not investigated other possible weaker forms of OT, such as the ones described in Section 3.3.4.
We have defined a modified version of the BBCS OT protocol which is secure under the MDI setting with perfect single-photon sources. We proved the security of this protocol when making the bounded storage assumption on Bob, but according to [29], it is likely that a security result stronger than computational security can be obtained without this assumption, reinforcing the observation made in Section 4.2.1.1 regarding the party we assume to have bounded storage. We proved that this reduction is vulnerable to the same kind of attack when trying to implement oblivious transfer under the MDI setting with multiphoton emissions. While it remains an open question whether OT can be securely implemented under the MDI setting using imperfect single-photon sources, these results reinforce the intuition that this is a difficult challenge.
We have also shown that when assuming that Alice is semi-honest, we can improve the rate of the protocol [21, Protocol II.3], which reduces the negative impact of multiphoton emissions. One could try to obtain a stronger statement proving security when assuming that Alice is fully dishonest.

Overall, this work paves the way for further exploration of the OT and BC primitives, under a realistic setting. In the next section, we also propose a new protocol that aims to implement a new primitive we decided to call "Weak String Erasure with Errors and Leaks", but we do not give security proofs. Defining such a primitive could be useful under the setting of this thesis where basis information is leaked to Alice. It could also help to deal with the basis-dependent flaw [38], where basis information can also be leaked.

5.2 Proposing a WSEEL protocol

We know that RSC can be reduced to WSEE in the case of perfect single photon sources (Section 3.2). In order to see how much power the quantum state of the MDI-RSC protocol [21, Protocol II.3] gives after the preparation phase, we have been interested in describing a new primitive which could be called Weak String Erasure with Errors and Leaks (WSEEL). This primitive would be a WSEE-like primitive which adds the parameter γ to characterize the information brought to Alice by multiphoton emissions under the MDI setting.

5.2.1 Definition

The aim of this section is to define a Weak String Erasure-like protocol that takes into account the use of imperfect photon sources under the MDI setting. This is a lead that was left behind after discussion, but it may still be interesting for someone to try to push into this direction.

We are defining here a WSEE-like protocol that holds when Alice and Bob are using multiphoton emissions, which leads to dishonest Alice being able to guess whether some bits of her string are known or not by Bob. A formal definition can be found in B.

Definition 5.1. Weak String Erasure with Errors and Leaks:

We define a $(n, \lambda, \varepsilon, p_{err}, \gamma)$-WSEEL protocol similar to the $(n, \lambda, \varepsilon, p_{err})$-WSEE protocol [11] but adding the "leaks" part required to deal with imperfect sources like in [21, Protocol II.3.] with the following parameters:

- $n \in \mathbb{N}$ the length of Alice's string X_1^n
- $\lambda \in [0, 1]$ which indicates the Bob's uncertainty about Alice's string.
- $\varepsilon \in [0, 1]$ the smoothing parameter used to define the smooth min-entropy $\mathrm{H}_{\min}^{\varepsilon}$.
- $p_{err} \in]0, 0.5[$ the probability of bit flip in the bits from X_1^n received by Bob from Alice.
- $\gamma \in \left]0, \frac{1}{2}\right[$ indicates the proportion of multiphoton emissions during the protocol.

An $(n, \lambda, \varepsilon, p_{err}, \gamma)$-WSEEL is a protocol between Alice and Bob satisfying the following properties.

Correctness: If both Alice and Bob are honest, at the end of the protocol Alice obtains a bit string $X_1^n \in_U \{0,1\}^n$. Bob has a bit string $\mathcal{I}_1^n \in_U \{0,1\}^n$ as well as the corresponding bit string $\hat{X}_{\mathcal{I}} = \{E_{p_{err}}(X_j) | \mathcal{I}_j = 1\}$.

Security for Alice: If Alice is honest, Bob's knowledge about X_1^n is limited to

$$\frac{1}{n}\mathrm{H}_{\min}^{\varepsilon}\left(X_1^n | B'\right) \geq \lambda, \tag{5.1}$$

where B' is the state held by a dishonest Bob.

Security for Bob: If Bob is honest, Alice's knowledge about $\mathcal{I}_1^n$ is limited to

$$\frac{1}{n}\mathrm{H}_{\min}^{\varepsilon}\left(\mathcal{I}_1^n | A'\right) \geq 1 - \gamma, \tag{5.2}$$

where A' is the state held by a dishonest Alice.

5.2.2 An MDI-WSEEL protocol [21, Protocol II.3.]

The following protocol was provided in [11] without MDI settings, and a version under the MDI setting is described in the preparation phase of [21, Protocol II-3]. This performs a WSE protocol which contains errors (bit flips) and which allows Alice to have some information about Bob's string. This protocol is given in the bounded storage assumption, we therefore require the size of Bob's quantum register Q to be upper-bounded by some value D.

Alice and Bob each have probability distributions $(p_{a_s}, p_{a_{d_1}}, \ldots, p_{a_{d_q}})$ and $(p_{b_s}, p_{b_{d_1}}, \ldots, p_{b_{d_q}})$ that give the probability that they use their intensities $\{a_s, a_{d_1}, \ldots, a_{d_q}\}$ and $\{b_s, b_{d_1}, \ldots, b_{d_q}\}$. The parameter λ is defined as $\lambda = f(\frac{-D}{n}) - (\gamma + \alpha_4^A) - \frac{1}{n}$, if we define the function f as in equation (3.6).

Protocol 9: MDI-WSEEL protocol (from the preparation phase of [21, Protocol II-3])

Inputs: n the number of rounds, a security parameter ϵ, 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 $\{b_s, b_{d_1}, \ldots, b_{d_q}\}$.

1. Alice and Bob start by agreeing on a target number of round N. N is such that

$$\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n \tag{5.3}$$

where p is the probability that a round i is not discarded if both parties are honest and n is the target number of rounds, given as an input of the protocol. We have $p = p_{a_s} \times p_{b_s} \times (1 - p_{fail|a_s b_s})$.

2. For round $i \in [N]$:

- Alice chooses $(X_i, \Theta_i) \in_R \{0,1\}^2$ uniformly at random and chooses $a \in \{a_s, a_{d_1}, \ldots, a_{d_q}\}$ according to her probability distribution. She prepares a signal of intensity a encoding X_i in the basis Θ_i and sends $|X_i\rangle_{\Theta_i}$ (where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$) to the measurement station.
- Bob chooses $(\hat{X}_i, \hat{\Theta}_i) \in_R \{0,1\}^2$ uniformly at random and chooses $b \in \{b_s, b_{d_1}, \ldots, b_{d_q}\}$ according to his probability distribution. He prepares a signal of intensity b encoding $\hat{X}_i$ in the basis $\hat{\Theta}_i$ and sends $|\hat{X}_i\rangle_{\hat{\Theta}_i}$ (where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$ and $|1\rangle_1 = |-\rangle$) to the measurement station.
- The measurement station performs a measurement on the two states it receives and publicly reveals the outcome (or reveals that the measurement failed). Bob decides based on the output of a successful measurement whether he should flip his bit $\hat{X}_i$ or not.

3. Alice and Bob publicly announce the intensities they have used for every round $i \in [N]$. We call f_{a_s} and f_{b_s} the fractions of rounds in which respectively Alice and Bob used their signal intensity when the measurement succeeded and the other party also used their signal intensity.

4. Alice computes $\beta^A := \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2(n^A)}}$ where n^A denotes the number of rounds where she used her signal intensity and the measurement succeeded. She checks that $f_{b_s} \geq p_{b_s} - \beta^A$, otherwise she aborts the protocol.

5. Bob computes $\beta^B := \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2(n^B)}}$ where n^B denotes the number of rounds where he used his signal intensity and the measurement succeeded. He checks that $f_{a_s} \geq p_{a_s} - \beta^B$, otherwise he aborts the protocol.

6. The number of round in which both Alice and Bob used their signal intensities is denoted as $n' = f_{b_s} \times (n^A) = f_{a_s} \times (n^B)$. Using the decoy states Alice estimates a lower-bound L_{A1} for n_1^A which is the number of rounds where the Bell measurement succeeded and Alice emitted exactly one photon with intensity a_s. If $U_{A2} \geq (\gamma + \alpha^A)n'$, Alice aborts the protocol.

7. Using the decoy states Bob estimates a lower-bound L_{B1} for n_1^B which is the number of rounds where the Bell measurement succeeded and Bob emitted exactly one photon with intensity b_s. If $U_{B2} \geq (\gamma + \alpha^B)n'$, Bob aborts the protocol.

8. Alice and Bob discard all the rounds where a failure has been announced, and where the intensities used by Alice and Bob are not a_s and b_s. Alice and Bob check that $n' \geq n$ and abort the protocol otherwise. They randomly choose to drop $n' - n$ rounds. Alice then has strings X_1^n and Θ_1^n and Bob has the strings $\hat{X}_1^n$ and $\hat{\Theta}_1^n$.

9. Both parties wait for a time Δt.

10. Alice sends Θ_1^n to Bob through a classical channel.

11. Bob computes the string $\mathcal{I}_1^n = 1 \oplus \Theta_1^n \oplus \hat{\Theta}_1^n$ and $\hat{X}_{\mathcal{I}}$ the string formed by all the bits where $\mathcal{I}_i = 1$.

We require the condition $\left(p - \sqrt{\frac{\ln(\frac{1}{\epsilon})}{2N}}\right) N \geq n$ in order to make sure that Alice and Bob end up with a string of length at least n with probability at least $1 - \epsilon$ using the Hoeffding inequality.

Bibliography

[1] J. Kilian. Founding cryptography on oblivious transfer. *Theory of Computing*, 1988. DOI: 10.1145/62212.62215. URL: https://dl.acm.org/doi/pdf/10.1145/62212.62215.

[2] Charles Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In volume 576, pages 351–366, January 1991.

[3] Mihir Bellare and Silvio Micali. Non-interactive oblivious transfer and applications. In *Proceedings on Advances in Cryptology*, CRYPTO '89, 547–557, Santa Barbara, California, USA. Springer-Verlag, 1989. ISBN: 0387973176.

[4] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. DOI: 10.1109/SFCS.1994.365700.

[5] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

[6] Charles H. Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 1984. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025.

[7] Gilles Brassard and Claude Crépeau. Oblivious transfers and privacy amplification. In pages 334–347, May 1997. ISBN: 978-3-540-62975-7. DOI: 10.1007/3-540-69053-0_23.

[8] Anne Broadbent and Peter Yuen. Device-independent oblivious transfer from the bounded-quantum-storage-model and computational assumptions. *New Journal of Physics*, 25(5):053019, May 2023. ISSN: 1367-2630. DOI: 10.1088/1367-2630/accf32. URL: http://dx.doi.org/10.1088/1367-2630/accf32.

[9] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997. ISSN: 1079-7114. DOI: 10.1103/physrevlett.78.3414. URL: http://dx.doi.org/10.1103/PhysRevLett.78.3414.

[10] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model, 2006. arXiv: quant-ph/0508222 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/0508222.

[11] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. Implementation of two-party protocols in the noisy-storage model. *Physical Review A*, 81(5), May 2010. ISSN: 1094-1622. DOI: 10.1103/physreva.81.052336. URL: http://dx.doi.org/10.1103/PhysRevA.81.052336.

[12] Jérémy Ribeiro, Le Phuc Thinh, Jędrzej Kaniewski, Jonas Helsen, and Stephanie Wehner. Device independence for two-party cryptography and position verification with memoryless devices. *Physical Review A*, 97(6), June 2018. ISSN: 2469-9934. DOI: 10.1103/physreva.97.062307. URL: http://dx.doi.org/10.1103/PhysRevA.97.062307.

[13] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, March 2012. ISSN: 1557-9654. DOI: 10.1109/tit.2011.2177772. URL: http://dx.doi.org/10.1109/TIT.2011.2177772.

[14] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2), August 2006. ISSN: 1094-1622. DOI: 10.1103/physreva.74.022313. URL: http://dx.doi.org/10.1103/PhysRevA.74.022313.

[15] Jędrzej Kaniewski and Stephanie Wehner. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics*, 18(5):055004, 2016. DOI: 10.1088/1367-2630/18/5/055004. URL: https://dx.doi.org/10.1088/1367-2630/18/5/055004.

[16] Tony Metger, Yfke Dulek, Andrea Coladangelo, and Rotem Arnon-Friedman. Device-independent quantum key distribution from computational assumptions. *New Journal of Physics*, 23(12):123021, December 2021. ISSN: 1367-2630. DOI: 10.1088/1367-2630/ac304b. URL: http://dx.doi.org/10.1088/1367-2630/ac304b.

[17] Tony Metger and Thomas Vidick. Self-testing of a single quantum device under computational assumptions. *Quantum*, 5:544, September 2021. ISSN: 2521-327X. DOI: 10.22331/q-2021-09-16-544. URL: http://dx.doi.org/10.22331/q-2021-09-16-544.

[18] Chris Peikert. 2016. DOI: 10.1561/0400000074.

[19] Shihan Sajeed, Igor Radchenko, Sarah Kaiser, Jean-Philippe Bourgoin, Anna Pappa, Laurent Monat, Matthieu Legré, and Vadim Makarov. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A*, 91:032326, 3, 2015. DOI: 10.1103/PhysRevA.91.032326. URL: https://link.aps.org/doi/10.1103/PhysRevA.91.032326.

[20] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13), March 2012. ISSN: 1079-7114. DOI: 10.1103/physrevlett.108.130503. URL: http://dx.doi.org/10.1103/PhysRevLett.108.130503.

[21] Jeremy Ribeiro and Stephanie Wehner. On bit commitment and oblivious transfer in measurement-device independent settings, 2020. arXiv: 2004.10515 [quant-ph]. URL: https://arxiv.org/abs/2004.10515.

[22] Fumihiro Kaneda, Karina Garay-Palmett, Alfred U'Ren, and Paul Kwiat. Heralded single-photon source utilizing highly nondegenerate, spectrally factorable spontaneous parametric downconversion. *Optics Express*, 24:10733–10747, May 2016. DOI: 10.1364/OE.24.010733.

[23] M. Eisaman, Jingwen Fan, Alan Migdall, and Sergey Polyakov. Invited review article: single-photon sources and detectors. *The Review of scientific instruments*, 82:071101, July 2011. DOI: 10.1063/1.3610677.

[24] Xiongfeng Ma, Chi-Hang Fred Fung, Frédéric Dupuis, Kai Chen, Kiyoshi Tamaki, and Hoi-Kwong Lo. Decoy-state quantum key distribution with two-way classical postprocessing. *Physical Review A*, 74(3), September 2006. ISSN: 1094-1622. DOI: 10.1103/physreva.74.032330. URL: http://dx.doi.org/10.1103/PhysRevA.74.032330.

[25] Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In volume 7, pages 60–77, May 2001. ISBN: 978-3-540-42070-5. DOI: 10.1007/3-540-44987-6_5.

[26] T. Vidick and S. Wehner. *Introduction to Quantum Cryptography*. Cambridge University Press, 2023.

[27] Ramona Wolf. Quantum key distribution. *Lecture notes in physics*, 988, 2021.

[28] Frederic Dupuis, Omar Fawzi, and Stephanie Wehner. Entanglement sampling and applications. *IEEE Transactions on Information Theory*, 61(2):1093–1112, February 2015. ISSN: 1557-9654. DOI: 10.1109/tit.2014.2371464. URL: http://dx.doi.org/10.1109/TIT.2014.2371464.

[29] Manuel B. Santos, Paulo Mateus, and Armando N. Pinto. Quantum oblivious transfer: a short review. *Entropy*, 24(7):945, July 2022. ISSN: 1099-4300. DOI: 10.3390/e24070945. URL: http://dx.doi.org/10.3390/e24070945.

[30] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer, 2013. arXiv: 1007.1875 [quant-ph]. URL: https://arxiv.org/abs/1007.1875.

[31] Gus Gutoski, Ansis Rosmanis, and Jamie Sikora. Fidelity of quantum strategies with applications to cryptography, 2018. arXiv: 1704.04033 [quant-ph]. URL: https://arxiv.org/abs/1704.04033.

[32] Ryan Amiri, Robert Stárek, David Reichmuth, Ittoop V. Puthoor, Michal Mičuda, Ladislav Mišta Jr., Miloslav Dušek, Petros Wallden, and Erika Andersson. Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation. *PRX Quantum*, 2(1), March 2021. ISSN: 2691-3399. DOI: 10.1103/prxquantum.2.010335. URL: http://dx.doi.org/10.1103/PRXQuantum.2.010335.

[33] Sarah Osborn and Jamie Sikora. A constant lower bound for any quantum protocol for secure function evaluation, 2022. arXiv: 2203.08268 [quant-ph]. URL: https://arxiv.org/abs/2203.08268.

[34] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs. An experimental implementation of oblivious transfer in the noisy storage model. *Nature Communications*, 5(1), March 2014. ISSN: 2041-1723. DOI: 10.1038/ncomms4418. URL: http://dx.doi.org/10.1038/ncomms4418.

[35] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '95, 67–75, Las Vegas, Nevada, USA. Association for Computing Machinery, 1995. ISBN: 0897917189. DOI: 10.1145/225058.225085. URL: https://doi.org/10.1145/225058.225085.

[36] Niek Johannes Bouman. *Cryptography from quantum uncertainty in the presence of quantum side information.* Leiden University, 2012.

[37] Ivan Damgaard, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open, 2009. arXiv: 0902.3918 [quant-ph]. URL: https://arxiv.org/abs/0902.3918.

[38] Kiyoshi Tamaki, Hoi-Kwong Lo, Chi-Hang Fred Fung, and Bing Qi. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A*, 85:042307, 4, 2012. DOI: 10.1103/PhysRevA.85.042307. URL: https://link.aps.org/doi/10.1103/PhysRevA.85.042307.

Appendix A

Formal definitions of WSEE, RSC and OT

Definition A.1. Weak String Erasure with errors (formal) [11, Appendix A]:

An $(n, \lambda, \varepsilon, p_{err})$-WSEE scheme is a protocol between Alice and Bob that satisfies the following three properties.

Correctness:

If both parties are honest, the ideal state $\sigma_{X_1^n I \hat{X}_I}$ is defined with $\hat{X}_I = E_{p_{err}}(X_I)$ such that

1. The joint distribution of the n-bit string X_1^n and the subset I is uniform:

$$\sigma_{X_1^n I} = \tau_{\{0,1\}^n} \otimes \tau_{2^{[n]}}$$

2. The joint state ρ_{AB} created by the real protocol is ε-close to the ideal state:

$$\rho_{X_1^n I \hat{X}_I} \approx_\varepsilon \sigma_{X_1^n I \hat{X}_I}$$

Security for Alice:

If Alice is honest, then there exist an ideal state $\sigma_{X_1^n B'}$ such that

1. The amount of information that B' gives Bob about X_1^n is limited:

$$\frac{1}{n} \mathrm{H}_{\min}(X_1^n | B')_\sigma \geq \lambda$$

2. The joint state $\rho_{X_1^n B}$ created by the real protocol is ε-close to the ideal state:

$$\rho_{X_1^n B} \approx_\varepsilon \sigma_{X_1^n B'}$$

Security for Bob:

If Bob is honest, then there exist an ideal state $\sigma_{A'\hat{X_1^n}I}$, where $\hat{X_1^n} \in \{0,1\}^n$ and $I \subseteq [n]$ such that

1. The random variable I is independent of $A'\hat{X_1^n}$ and uniformly distributed over $2^{[n]}$:

$$\sigma_{A'\hat{X_1^n}I} = \sigma_{A'\hat{X_1^n}} \otimes \tau_{2^{[n]}}$$

2. The joint state $\rho_{A'\hat{X_1^n}I}$ created by the real protocol is ε-close to the ideal state:

$$\rho_{A'\hat{X_1^n}I} \approx_\varepsilon \sigma_{A'\hat{X_1^n}I}$$

Definition A.2. Randomized string commitment (formal) [21, Appendix C]:

An (ℓ, ε)-RSC scheme is a protocol between Alice and Bob that satisfies the following three properties.

Correctness:

If both parties are honest, the ideal state $\sigma_{C_1^\ell C_1^\ell F}$ is defined such that

1. C_1^ℓ is uniformly distributed over $\{0,1\}^\ell$ and the protocol is accepted:

$$\sigma_{C_1^\ell F} = \tau_{C_1^\ell} \otimes |accept\rangle\langle accept|_F$$

2. The joint state $\rho_{C_1^\ell \tilde{C_1^\ell} F}$ created by the real protocol is ε-close to the ideal state:

$$\rho_{C_1^\ell \tilde{C_1^\ell} F} \approx_\varepsilon \sigma_{C_1^\ell C_1^\ell F}$$

Security for Alice:

If Alice is honest, Bob is ignorant about C_1^ℓ before the open phase:

$$\rho_{C_1^\ell B} \approx_\varepsilon \tau_{C_1^\ell} \otimes \rho_B.$$

Security for Bob:

If Bob is honest, then there exist between the commit and the open phases an ideal state $\sigma_{C_1^\ell AB}$ such that for any Open algorithm described by the CPTP map $\mathcal{O}_{\mathcal{AB}}$, in which Bob is honest, we have:

1. Bob almost never accepts $\tilde{C_1^\ell} \neq C_1^\ell$:

$$\text{for } (\mathbb{1}_{C_1^\ell} \otimes \mathcal{O}_{\mathcal{AB}})(\sigma_{C_1^\ell AB}) \text{ we have } \Pr(\tilde{C_1^\ell} \neq C_1^\ell \text{ and } F = accept) \leq \varepsilon.$$

2. The joint state ρ_{AB} produced by the real commitment is ε-close to the ideal state:

$$\rho_{AB} \approx_\varepsilon \sigma_{AB}$$

Definition A.3. Randomized 1-out-2 string Oblivious Transfer (formal) [21, Appendix C]:

An (ℓ, ε)-Randomized 1-out-2 Oblivious String Transfer scheme is a protocol between Alice and Bob that satisfies the following three properties:

Correctness:

If both parties are honest, the ideal state $\sigma_{S_0S_1CS_C}$ is defined such that

1. S_0, S_1 and C are uniformly and independently distributed:

$$\sigma_{S_0S_1C} = \tau_{S_0} \otimes \tau_{S_1} \otimes \tau_C$$

2. The joint state $\rho_{S_0S_1C\hat{S}_C}$ created by the real protocol is ε-close to the ideal state:

$$\rho_{S_0S_1C\hat{S}_C} \approx_\varepsilon \sigma_{S_0S_1CS_C}$$

Security for Alice:

If Alice is honest, there exist a binary variable $\tilde{C} \in \{0, 1\}$ such that Bob is ε-ignorant about $S_{1-\tilde{C}}$:

$$\rho_{S_0S_1BC} \approx_\varepsilon \sigma_{S_CBC} \otimes \tau_{S_{1-\tilde{C}}}.$$

Security for Bob:

If Bob is honest, then Alice is ε-ignorant about C:

$$\rho_{AC} \approx_\varepsilon \sigma_{S_0S_1} \otimes \tau_C$$

Appendix B

Formal definition of WSEEL

Definition 7. Weak String Erasure with errors and leaks (formal):

An $(n, \lambda, \varepsilon, p_{err}, \gamma)$-WSEEL scheme is a protocol between Alice and Bob that satisfies the following three properties.

Correctness:

If both parties are honest, the ideal state $\sigma_{X_1^n J_1^n \hat{X}_I I_1^n}$ is defined with $\hat{X}_I = \{E_{p_{err}}(X_i) | i \in [n] \cap I_i = 1\}$ such that

1. The joint distribution of the strings X_1^n, I_1^n and J_1^n are independent and uniform:
$$\sigma_{X_1^n J_1^n I_1^n} = \tau_{\{0,1\}^n} \otimes \tau_{\{-1,0,1\}^n} \otimes \tau_{\{0,1\}^n}$$
2. The joint state ρ_{AB} created by the real protocol is ε-close to the ideal state:
$$\rho_{AB} = \rho_{X_1^n J_1^n \hat{X}_I I_1^n} \approx_\varepsilon \sigma_{X_1^n J_1^n \hat{X}_I I_1^n}$$

Security for Alice:

If Alice is honest, then there exist an ideal state $\sigma_{X_1^n I_1^n B'}$ such that

1. The amount of information that B' gives Bob about X_1^n is limited:
$$\frac{1}{n} \mathrm{H}_{\min}\left(X_1^n | B'\right)_\sigma \geq \lambda$$
2. The joint state $\rho_{X_1^n I_1^n B}$ created by the real protocol is ε-close to the ideal state:
$$\rho_{X_1^n I_1^n B} \approx_\varepsilon \sigma_{X_1^n I_1^n B'}$$

Security for Bob:

If Bob is honest, then there exist an ideal state $\sigma_{A' \hat{X}_1^n I_1^n}$, where $\hat{X}_1^n \in \{0,1\}^n$ and $I_1^n \in \{0,1\}^n$ such that

1. The amount of information that A' gives Alice about I_1^n is limited:
$$\frac{1}{n} \mathrm{H}_{\min}\left(I_1^n | A'\right)_\sigma \geq 1 - \gamma$$
2. The joint state $\rho_{A \hat{X}_1^n I_1^n}$ created by the real protocol is ε-close to the ideal state:
$$\rho_{A \hat{X}_1^n I_1^n} \approx_\varepsilon \sigma_{A' \hat{X}_1^n I_1^n}$$