A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions

Eleni Diamanti[1], Alex B. Grilo[1], Adriano Innocenzi[1], Pascal Lefebvre[1,2], Verena Yacoub[1], and Álvaro Yángüez[1] ⋆

[1] *Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France*
[2] *KTH Royal Institute of Technology, Stockholm, Sweden*

Abstract. We present a new simulation-secure quantum oblivious transfer (QOT) protocol based on one-way functions in the plain model. With a focus on practical implementation, our protocol surpasses prior works in efficiency, promising feasible experimental realization. We address potential experimental errors and their correction, offering analytical expressions to facilitate the analysis of the required quantum resources. Technically, we achieve simulation security for QOT through an *equivocal* and *relaxed-extractable* quantum bit commitment.

⋆ Corresponding author: alvaro.yanguez@lip6.fr

1 Introduction

Since the early stages of quantum cryptography, quantum protocols that achieve information-theoretical security (i.e., security against unbounded adversaries) have been known for primitives that are impossible in the classical setting [BB84]. However, it was soon realized that even quantumly, a very limited family of cryptographic primitives can achieve such level of security [LC97,May97], and therefore, the use of computational assumptions is necessary to reach quantum advantage.

Multi-party computation (MPC) is a very versatile primitive that plays a central role in classical cryptography. In MPC, many parties want to collectively compute a function that depends on their private inputs, while maintaining the inputs secret (even if many of these parties are malicious and deviate from the original protocol). This functionality can be constructed from another primitive: oblivious transfer (OT) [DFL$^+$09]. However, it is not expected that OT (and thus MPC) can be constructed only from one-way functions (OWFs)[1][2].

On the other hand, [GLSV21,BCKM21] showed that OT *can* be built from OWFs and quantum resources. More precisely, [GLSV21,BCKM21] showed how to build equivocal and extractable commitment schemes, which were known to be sufficient to build quantum protocols for OT [DFL$^+$09] and MPC [IPS08,Kil88] [3].

One important feature of [GLSV21,BCKM21] is that the quantum resources required for such protocols are exactly the same as the ones used in some quantum key distribution (QKD) protocols: they only need to prepare, communicate, and measure one-qubit states in conjugate bases. Given the huge progress in the implementation of QKD in very different setups [AAB$^+$23,GBR$^+$23,PSC$^+$23] [ZMM$^+$24], it would be expected that one could easily implement such quantum protocols with current technology.

Unfortunately, this is not the case. While the protocols proposed by [GLSV21] [BCKM21] are important to theoretically understand the power of quantum resources, their building blocks put serious barriers in their experimental implementation. More concretely, they pose the following difficulties:

- **Fragility against errors.** The protocols proposed by [GLSV21] and [BCKM21] do not tolerate experimental errors such as bit flips during the state distribution steps.
- **Practical hash functions and zero knowledge proofs.** Zero knowledge proofs used in [GLSV21] do not make black-box use of OWFs, and the practical implementation of the protocol would require the arithmetical description of the inner functioning of the one-way functions. It is currently

[1] One-way functions are functions that are easy to compute and hard to invert. These are considered the minimal computational assumption in classical cryptography.

[2] More formally, [IR90] shows that no MPC protocol can be built from OWF in a black-box way.

[3] We notice that later, it was shown that MPC can be built even from weaker computation assumptions such as pseudo-random states [MY22,AQY22].

unclear how to achieve such descriptions for widespread heuristic implementations of post-quantum OWFs like the secure hash standard (SHA), making their integration in the [GLSV21] scheme non-trivial.
- **Inefficiency.** The iterative structure of the protocol proposed by [BCKM21] allows the protocol to make a black-box use of the underlying components but requires a very large quantity of quantum states, which prevents it from being practically implementable. For example, one run of that protocol requires an order of 10^{13} BB84 states [BB84], which are provided by days of transmission given a state-of-the-art discrete-variable QKD setup.

The main contribution of this work is to provide a noise-tolerant protocol for OT, based on the structure from [BCKM21], while avoiding some of its bottlenecks and while making it efficiently implementable. In particular, with this new protocol, we expect that around 10^6 BB84 states would be sufficient instead of 10^{13}, improving the transmission time to the order of seconds. Moreover, we notice that with this amount of quantum resources, we can distil more than one OT at once, which will be crucial in future uses of this protocol to implement MPC.

1.1 Background and our results

As previously mentioned, the goal of [GLSV21,BCKM21] is to achieve a quantum protocol for oblivious transfer, since it can be used to construct MPC in a generic way [IPS08]. Oblivious transfer is a cryptographic primitive where Alice chooses two messages, m_0 and m_1, Bob chooses a bit $b \in \{0,1\}$, and Bob learns m_b (notice that Bob should not learn $m_{\bar{b}}$ and Alice should not learn b).

In the quantum protocol for OT proposed in [CK88,BBCS92], Alice sends BB84 states to Bob. The encoded states are $\left(\left|x_i^{OT}\right\rangle_{\theta_i^{OT}}\right)_{i\in[2\lambda_{OT}]}$, where $x_i^{OT} \in \{0,1\}$ is the value of the bit, $\theta_i^{OT} \in \{+,\times\}$ is the choice of encoding bases and λ_{OT} is a security parameter. Bob chooses measurement bases $\hat{\theta}_i^{OT} \in \{+,\times\}$ and obtains measurement results $\hat{x}_i^{OT} \in \{0,1\}$. However, since we cannot guarantee that a malicious Bob will follow the protocol (in particular, that he keeps these qubits in a quantum memory instead of measuring them), Alice and Bob perform a sub-protocol that will give guarantees to Alice that Bob did measure the quantum state. However, this sub-protocol comes with a cost, since it adds the need for bit commitment, and requires the added cost of cryptographic assumptions. More concretely, to ensure Bob's measurement, Bob *commits* to the measurement basis that he chose and the outcomes resulting from the measurement. Alice can then choose a subset of these pairs of measurements/outcomes, and she asks Bob to *open* the corresponding commitments. Then, she can check if the outcomes are consistent with the BB84 states that she sent. If they are, it can be shown that there are strong guarantees that Bob measured (most of) the qubits sent by Alice [BF12]. The bit commitment sub-protocol is finished when Alice sends the basis of her original BB84 states. Bob then divides his indices into two different subsets $I_b = \{i : \theta_i^{OT} = \hat{\theta}_i^{OT}\}$ and $I_{\bar{b}} = \{i : \theta_i^{OT} \neq \hat{\theta}_i^{OT}\}$,

which depend on the bit choice bit b. Bob sends the two sets I_0 and I_1 to Alice who can encode the messages m_0 and m_1 using $\mathbf{x_0}^{OT} = \{x_i^{OT} : i \in I_0\}$ and $\mathbf{x_1}^{OT} = \{x_i^{OT} : i \in I_1\}$ as encrypting keys. Bob receives the encoded messages and decodes m_b.

The subtleties here are the properties needed in the commitments to prove that the protocol is secure. In standard bit commitment schemes, there are two properties of interest: *hiding*, meaning that the receiver cannot learn the committed message before the opening, and *binding*, meaning that after committing, there is only one value that can be opened by the committer. However, these properties alone do not allow us to prove the security of the quantum OT protocol in the simulation-based setting (which is needed to use this building block in MPC protocols). To prove the simulation-security of the QOT protocol, a strengthening of these properties is needed, namely:

Equivocality: A bit commitment protocol is called equivocal if there is a simulator (also called equivocator) that can perform a "dummy commitment" that can be opened to any desired value. Moreover, such a dummy commitment cannot be distinguished from the real ones by any polynomial-time distinguisher. [4]
Extractability: A bit commitment protocol is called extractable if there is a simulator (also called extractor) that is able to extract the commitment message in the commitment phase of the protocol. [5]

In [DFL+09], they show that equivocation and extraction of the quantum bit commitment are sufficient properties to prove the simulation-security of the QOT protocols of [CK88,BBCS92]. Moreover, the technical contribution of [GLSV21,BCKM21] was to show a quantum protocol bit commitment that is equivocal and extractable. The main observation that allowed us to improve the parameters of such a protocol is that full extraction is not needed in order to prove the security of the QOT protocol. Instead, we show that *relaxed extractability* is sufficient, and we show a more efficient bit commitment protocol that achieves this property (and is still equivocal). We describe the details of our contributions in the next section.

1.2 Technical overview

We explain now the approach of [BCKM21] to achieve extractable and equivocal commitment, and discuss how we modify it. In their result, they propose two compilers: in the first one, they propose an equivocal commitment scheme based on any bit commitment scheme that satisfies only "vanilla" binding and hiding. Moreover, the resulting commitment is extractable if the original commitment was also extractable. In the second commitment, they show how to turn an equivocal commitment into an extractable one (while losing equivocality). We notice that in this second step, even if the original bit commitment scheme

[4] We notice that for this to be true, the simulator has to have some leverage (e.g., a trapdoor, or the ability to rewind), otherwise the protocol would not be secure.
[5] We have here the same considerations as in Footnote 4.

is classical, the resulting one would be a quantum protocol. They achieve the equivocal and extractable bit commitment scheme by starting with a standard bit commitment scheme, and then applying the equivocal compiler, followed by the extractable compiler, and then finally the equivocal compiler again.

In the equivocal compiler, *EqCommitment*, the committer generates λ pairs of random bits (u_i^0, u_i^1). For each i, the commuter and the receiver proceed as follows, sequentially: the committer commits, using the base bit commitment scheme, to each one of them twice leading to the commitments $(c_{i,0}^0, c_{i,1}^0, c_{i,0}^1, c_{i,1}^1)$. Then, the receiver chooses a random bit γ_i and the committer opens $c_{i,0}^{\gamma_i}, c_{i,1}^{\gamma_i}$. The verifier aborts if such pairs of commitments open to different values. At the end of this interaction, the committer sends $e_i = b \oplus u^{\gamma_i}$ for every i. In the opening phase, the committer chooses bits d_i and opens $c_{i,d_i}^{\gamma_i}$ and the receiver accepts if all the e_i's decommit to the same value b.

In the equivocality proof, the equivocator guesses γ_i, and then commits to two different values on $c_{i,0}^{\overline{\gamma_i}}, c_{i,1}^{\overline{\gamma_i}}$. At each step, the equivocator uses Watrous' rewinding [Wat06] to amplify the success probability to $1 - negl(\lambda)$. In this case, in the opening phase, the equivocator can choose which $c_{i,d_i}^{\overline{\gamma_i}}$ to open, so that the decommitment will be the desired bit. The binding/extractable property follows from the fact that, if many of the checks on γ_i's passed, then most of the pairs $c_{i,0}^{\overline{\gamma_i}}, c_{i,1}^{\overline{\gamma_i}}$ commit to the same value, and therefore the decommitted bit is fixed.

The modification that we propose to the equivocal compiler is simple but impactful. Instead of repeating the commitment/checking λ times sequentially, our protocol only performs it once. The proof of equivocality follows exactly as in [BCKM21], but the binding property completely breaks. In particular, a malicious committer can guess γ, and commit to two different values of $c_0^{\overline{\gamma}}, c_1^{\overline{\gamma}}$, and therefore, with probability $\frac{1}{2}$, the receiver's checks pass and the committer can open to any value of their choice. However, we show that this protocol satisfies what we call *relaxed binding*. We defer the formal definition of this property to Section 3.1, but, intuitively, it says that, if we commit to m bits using our bit commitment scheme and all of the tests pass, then, with overwhelming probability, only a logarithmic small fraction of these bits are non-binding. As we discuss next, we show that this property is sufficient in the extractable compiler. Moreover, since this sub-protocol is repeated many times in later parts of the protocol, reducing its complexity has a big impact in the runtime of the classical post-processing of our final protocol.

We switch gears now to the extractable compiler of [BCKM21]. This compiler is heavily inspired by the structure of the quantum OT protocol of [CK88,BBCS92]. In this compiler, the committer generates 2λ BB84 states and sends them to the receiver. As in the quantum OT protocol, the receiver equivocally commits to measurement basis and outcomes, then the committer challenges the receiver to open a subset of size λ of such commitments and verify the consistency of the opened values with the committer's original encoded states. If such a test passes, the committer divides the remaining encoded states into $\sqrt{\lambda}$ strings $x_1, ..., x_{\sqrt{\lambda}}$ of size $\sqrt{\lambda}$, and using $\sqrt{\lambda}$ hashes from a 2-universal hash function $h_1, ..., h_{\sqrt{\lambda}}$, the committer sends $\hat{h}_i = h_i(x_i) \oplus b$

The opening in [BCKM21] is followed by the committer sending $x_1, ..., x_{\sqrt{\lambda}}, b$, which is followed by the receiver checking if these values are consistent with their measurement outcomes and if $\hat{h}_i = h_i(x_i) \oplus b$.

The hiding property of the commitment comes from the properties of 2-universal hash functions along with the entropy of x_i from the receiver's perspective due to the uncertainty relations of measurement outcomes that we can achieve with the binding property of the commitment scheme. We notice that the relaxed binding of the base commitment instead of a full binding preserves the overall proof of hiding with minimal losses.

The extraction property is (roughly) proved as follows. Using the equivocality of the base bit commitment scheme, the extractor can delay the measurement until the committer reveals which subset of positions they will check. At this point, the extractor measures those positions on random basis, and then equivocates the opening to these values. Later in the protocol, whenever the committer sends the basis, the extractor is able to measure *all* of the qubits in the correct basis and find the (purported) values of $x_1, ..., x_{\sqrt{\lambda}}$, and then extract the committed values from $\hat{h}_i$.

The first problem of this compiler is that it assumes that all of the parties have access to perfect (noiseless) devices. In particular, noise will make it impossible for the extractor to extract the correct values. A second problem appears while splitting the string in $\sqrt{\lambda}$ blocks, since it causes a quadratic loss in the security of the protocol. Finally, we notice that, in [BCKM21], this protocol is repeated multiple times: firstly in the equivocal compiler, and then to commit to many values in the final quantum OT protocol. This causes the huge overhead needed in the total number of qubits required for their protocol.

In our work, we solve all of these problems at once. First, in order to enable extraction even in the presence of noise, we send the syndrome of the encoded values according to a linear error correcting code, and, as in the QKD setting, this allows the extractor to correct the faulty positions. Second, we replace the use of hashes so that, with the same number of BB84 states, we can commit to many qubits with equivocality and some extraction properties. Our proposed Equivocal and Relaxed-Extractable commitment scheme (*ERE-Commitment*), can be divided into two main different subroutines: the generation of a set of random seeds that are relaxed-extractable and the use of these seeds as "keys" in a set of equivocal commitments. We show that the keys of almost all the equivocal commitments are extractable, which is sufficient for a simulator to open most of the messages. We notice that the structure of our scheme is conceptually different from the one proposed by [BCKM21], allowing the drastic reductions of the needed quantum resources.

The challenge is to generate random seeds that are relaxed-extractable. To do so, we make use of quantum resources again. Given the distribution of BB84 states, the sender can distill random seeds from the encoded states. By using an equivocal commitment subroutine, these seeds cannot be distilled by a receiver that is forced to measure. However, an efficient simulator is able to extract them.

More concretely, we split the encoded string $\boldsymbol{x}_{EX}$ into $\left(\tilde{\boldsymbol{x}}^{\boldsymbol{j}}\right)_{j\in[2k]}$ subsets of size m. Using privacy amplification techniques found in QKD [Ren08], we distill uniformly random strings $\boldsymbol{s}^j$ which are used as seeds of pseudo-random generators, i.e., we expand them to the pseudo-random strings $\left(\boldsymbol{p}^{\boldsymbol{j}}\right)_{j\in[2k]}$. Each $\boldsymbol{p}^j$ represents a concatenation of $2w$ values $\boldsymbol{p}_i^j$ that are used for their randomness as needed in statistically binding bit commitment schemes used for equivocation.

ERE-Commitment allows us to achieve the independence of seeds required to open the different commitments, while avoiding the modular composition proposed by [BCKM21]. The reason is that we consider that the $2k$ seed families $(\boldsymbol{p}^j)_{j\in[2k]}$ are grouped in k pairs $(\boldsymbol{p}^1,\boldsymbol{p}^2),...(\boldsymbol{p}^{2k-1},\boldsymbol{p}^{2k})$, so each of the $r\in[k]$ pairs can be used for parallel commitment of w values. For the r-th pair, each of the $q\in[w]$ instances makes use of two seeds $\boldsymbol{p}_i^j$ from each family of the pair, in such a way that the final set of seeds for the q-th EqCommitment instance of the r-th family pair is $\left(\left(\boldsymbol{p}_{i_{q,0}}^{j^{r,0}},\boldsymbol{p}_{i_{q,1}}^{j^{r,0}},\boldsymbol{p}_{i_{q,0}}^{j^{r,1}},\boldsymbol{p}_{i_{q,1}}^{j^{r,1}}\right)_{q\in[w]}\right)_{r\in[k]}$. Afterwards, Bob sends Alice the corresponding x_i^{EX} and θ_i^{EX}, then Alice checks that $x_i^{EX}=\hat{x}_i^{EX}$ whenever $\theta_i^{EX}=\hat{\theta}_i^{EX}$ and that the p^j were generated in an honest way. This ensures that the seeds $\boldsymbol{p}_i^j$ originate from the proper $\mathbf{x}^{EX}$ with probability $1-negl(k)$. Bob can then commit to $\left((\hat{x}_i^{OT},\hat{\theta}_i^{OT})\right)_{i\in[2\lambda_{OT}]}$ using $\boldsymbol{p}_i^j$.

To prove that ERE-Commitment is relaxed extractable, we make use of equivocality and quantum rewinding. A simulator commits to dummy values instead of $\left((\hat{x}_i^{EX},\hat{\theta}_i^{EX})\right)_{i\in[8\lambda_{EX}]}$. After learning the challenged subset E, the simulator measures the corresponding states $\left(\left|x_i^{EX}\right\rangle_{\theta_i^{EX}}\right)_{i\in E}$, and, applying Watrous' quantum rewinding, opens to the measured values. Once the simulator has passed the decommitment check, Bob announces the bases. The simulator will then measure $\left(\left|x_i^{EX}\right\rangle_{\theta_i^{EX}}\right)_{i\in\bar{E}}$ in the correct bases obtaining $\mathbf{x}^{EX}$. It is in this step in which the simulator has to make use of the error correction code for obtaining the correct seeds $(\boldsymbol{p}^{\boldsymbol{j}})_{j\in[2k]}$ given the syndromes $(Synd_j)_{j\in[2k]}$. The simulator will obtain the seeds of the equivocal commitments, and thus extracts $\left|\bar{T}\right|-\omega(\log^2(k))$ of the non-challenged committed values $\left((\hat{x}_i^{OT},\hat{\theta}_i^{OT})\right)_{i\in\bar{T}}$ with probability $1-negl(k)$.

Despite these changes, we prove that the OT functionality is simulation-based secure given an equivocal and a χ-relaxed extractable bit commitment. Having a practical implementation as our final goal, we take into account the possible experimental errors as well as their correction, and we provide analytical expressions based on [BF12] that facilitates the bench-marking of the needed quantum resources. Moreover, we propose a method to distill a number of n_{OT} QOT keys from a single run of the protocol. This could be done if a large number of BB84 states was required to reach a desired smaller sampling error (thus a tighter Δ-security bound).

1.3 Related works

In [ABKK22], the authors also focus on reducing round complexity by leveraging the Quantum Random Oracle Model (QROM). In the QROM model, equivocality and extractability are achieved for most common constructions of commitments, so no further resources are needed. While, based on our estimations, the number of BB84 states sent in their protool is comparable [6], this number does not account for practical errors such as as bit-flips, photon loss or multi-photon events. Therefore, we see their result and ours as complementary, since each protocol focus on minimizing a different resource. Moreover, we also highlight that our security proof is in the plain model, and it does not depend on heuristic implementations of the random oracle.

Further proposals, such as [CCLY23], consider relaxed version of simulations, where the run-time of the simulator depends polynomially on the desired security level. In our work, we can achieve negligible distinguishing probability with polynomial-time simulators.

1.4 Paper Organisation

Section 1 contains important background information and the technical overview of the paper. Section 2 contains preliminary information such as a description of the notation used throughout the paper, and useful definitions. Section 3 contains the proposed equivocal commitment. Section 4 presents the equivocal and relaxed-extractable commitment. Section 5 contains the proof that the QOT protocol we propose is simulation-based secure given relaxed-extractable and equivocal bit commitment.

2 Preliminaries and Definitions

2.1 Notation

Throughout this paper, we represent classical random variables with capital letters (e.g., X) while the value they take is represented by lower case letters (e.g., x). Bold characters (e.g., $\mathbf{x}$) are strings of values. Quantum states are represented as density matrices $\rho \in \mathcal{B}_1(\mathcal{H})$. The probability of distinguishing two density matrices is upper-bounded by $\frac{1}{2}(1 + \Delta(\rho^1, \rho^2))$, where $\Delta(\rho^1, \rho^2)$ is the trace distance. When a negligible function $\mu(\lambda)$ exists such that $\Delta(\rho^1, \rho^2) \leq \mu(\lambda)$, ρ^1 and ρ^2 are said to be statistically close. $\mu(\lambda)$ is negligible if, for every fixed c, $\mu(\lambda) = o(1/\lambda^c)$, where λ is the *security parameter*. Throughout the paper, the security parameters of the different steps are written as λ_{OT} and λ_{EX}, for example. When using the symbol $\perp$, it means to abort.

[6] Assuming a security level of 256 bits and that the random oracle is instantiated using SHA3, the maximum number of oracle queries by the adversary would be approximately $2^{128}/(1.2 \cdot 10^6)$. Based on these parameters, we estimate that around $2 \cdot 10^6$ BB84 states would be required in their protocol to achieve a security distance of 2^{-80} due to privacy amplification.

We define a *classical-quantum hybrid state* as a bipartite state of the subsystems XE such that $\rho_{XE} = \sum_{x\in\mathcal{X}} p_x(x) \left|x\right\rangle \left\langle x\right| \otimes \sigma_E^x$, where subsystem X is classical. $\mathcal{X}$ is a finite set with $|\mathcal{X}| = dim(\mathcal{H}_X)$, $p_x : \mathcal{X} \to [0,1]$ is a probability distribution and $\{|x\rangle\}_{x\in\mathcal{X}}$ an orthonormal basis of $\mathcal{H}_x$. $\sigma_E^x \in \mathcal{H}_E$ is the density matrix correlated with the value $x \in \mathcal{X}$. When we treat a collection of qubits as a single unit, we refer to it as a *quantum register*.

A function $h : \mathcal{X} \times \mathcal{S} \to \mathcal{Y}$ is called *2-universal hash* function if, for every two strings $x \neq x' \in \mathcal{X}$, we have that $\Pr[h(x,S) = h(x',S)] \leq \frac{1}{|\mathcal{Y}|}$. In the same way, a function $G : \{0,1\}^\ell \to \{0,1\}^n$ with seed length $\ell < n$ is a *pseudorandom generator* (PRG) if, given a non-uniform quantum polynomial time distinguisher $\mathcal{D}^* = \{\mathcal{D}_\lambda^*, \sigma_\lambda\}$, there exists a negligible function $\nu(\cdot)$ such that $\left|\mathbb{P}_{s\in\{0,1\}^n}[\mathcal{D}^*(1^\lambda, G(s)) = 1] - \mathbb{P}_{r\in\{0,1\}^\ell}[\mathcal{D}^*(1^\lambda, r) = 1]\right| \leq \nu(\lambda)$ with r chosen uniformly at random.

A *non-uniform quantum polynomial time distinguisher* $\mathcal{D}^* = \{\mathcal{D}_\lambda^*, \sigma_\lambda\}$ is composed of a λ-size quantum circuit $\mathcal{D}_\lambda^*$ and a non-uniform λ-size quantum advice $\sigma_\lambda \in \mathcal{B}(\mathcal{H}_\mathcal{D})$.

2.2 Bit commitment

A bit commitment is a two-party interactive functionality between a quantum committer $\mathcal{C}$ and a quantum receiver $\mathcal{R}$. A commitment protocol is composed of two phases: the committing phase and the decommitting phase, where $\mathcal{C} = \{\mathcal{C}_{com}, \mathcal{C}_{dec}\}$ and $\mathcal{R} = \{\mathcal{R}_{com}, \mathcal{R}_{dec}\}$. During the committing phase, the committer $\mathcal{C}$ commits to a bit $b \in \{0,1\}$, with $\mathcal{C}_{com}(1^\lambda, b)$ representing this step for the committer and $\mathcal{R}_{com}(1^\lambda)$, for the receiver. After the interaction, $\mathcal{C}_{com}$ outputs a state $\rho_{com}^\mathcal{C} \in \mathcal{B}_1(\mathcal{H}_\mathcal{C})$ and $\mathcal{R}_{com}$, $\rho_{com}^\mathcal{R} \in \mathcal{B}_1(\mathcal{H}_\mathcal{R})$. All in all, the commitment phase is written as $(\rho_{com}^\mathcal{C}, \rho_{com}^\mathcal{R}) \leftarrow\!\!\!\rightarrow \langle \mathcal{C}_{com}(1^\lambda, b), \mathcal{R}_{com}(1^\lambda)\rangle$. Additionally, $\rho_{com}^\mathcal{C}$ and $\rho_{com}^\mathcal{R}$ may be entangled. During the decommitment phase, the interaction between $\mathcal{C}_{dec}(\rho_{com}^\mathcal{C})$ and $\mathcal{R}_{dec}(\rho_{com}^\mathcal{R})$ leads to an output of $\mathcal{R}_{dec}$ that is either b' or $\perp$.

Security against malicious receiver. The two notions of security that we use against malicious receivers are as follows:

Definition 2.1 (Computational hiding). *A bit commitment protocol $(\mathcal{C}, \mathcal{R})$ is computationally hiding if, given any polynomial-size interactive receiver $\mathcal{R}_{com}^* = \{\mathcal{R}_{com,\lambda}^*, \rho_\lambda\}$ with $OUT_\mathcal{R}\langle \mathcal{C}(1^\lambda, b), \mathcal{R}_{com,\lambda}^*(\rho_\lambda)\rangle$ being the output of the receiver after the commitment phase, there exists a negligible function $\nu(\cdot)$ such that:*

$$\Big|I\!P[OUT_\mathcal{R}\langle \mathcal{C}_{com}(1^\lambda, 0), \mathcal{R}_{com}^*(\rho_\lambda)\rangle = 1] - I\!P[OUT_\mathcal{R}\langle \mathcal{C}_{com}(1^\lambda, 1), \mathcal{R}_{com}^*(\rho_\lambda)\rangle = 1]\Big| = \nu(\lambda).$$

Definition 2.2 (Equivocality). *Given a set of auxiliary states $\{\rho_\lambda, \sigma_\lambda\}_{\lambda\in\mathbb{N}}$ with $\rho_\lambda, \sigma_\lambda \in \mathcal{B}_1(\mathbb{C}^n)$, a bit commitment protocol $(\mathcal{C}, \mathcal{R})$ is equivocal if, for any poly-size receiver $\mathcal{R}^* = \{\mathcal{R}^*_{com,\lambda}, \mathcal{R}^*_{dec,\lambda}, \rho_\lambda\}$, there exists a non-uniform quantum polynomial time equivocator $\mathcal{Q}_{\mathcal{R}^*} = \{\mathcal{Q}_{\mathcal{R}^*,com}, \mathcal{Q}_{\mathcal{R}^*,dec}\}$ such that, for any poly-size distinguisher $\mathcal{D} = \{\mathcal{D}_\lambda, \sigma_\lambda\}$, there exists a negligible function $\nu(\lambda) > 0$ for the committed bit $b \in \{0,1\}$:*

$$|I\!P[\mathcal{D}^*(\sigma_\lambda, Real_b) = 1] - I\!P[\mathcal{D}^*(\sigma_\lambda, Ideal_b) = 1| = \nu(\lambda),$$

provided that:

***Real**$_b$: Interaction between $\mathcal{R}^*_{com}(\rho)$ and $\mathcal{C}_{com}(1^\lambda, b)$ such that $(\rho^{\mathcal{C}}_{com}, \rho^{\mathcal{R}^*}_{com}) \leftarrow\!\!\shortmid \langle \mathcal{C}_{com}(b), \mathcal{R}^*_{com}(\rho)\rangle$ and $\rho^{\mathcal{R}^*}_{final} \leftarrow\!\!\shortmid \langle \mathcal{C}_{dec}(\rho^{\mathcal{C}}_{com}), \mathcal{R}^*_{dec}(\rho^{\mathcal{R}^*}_{com})\rangle$.*

***Ideal**$_b$: The quantum simulator outputs $(\rho^{\mathcal{C}}_{com}, \rho^{\mathcal{R}^*}_{com}) \leftarrow\!\!\shortmid \mathcal{Q}_{\mathcal{R}^*,com}(\rho)$.*
Then, $\rho^{\mathcal{R}^*}_{final} \leftarrow\!\!\shortmid \langle \mathcal{Q}_{\mathcal{R}^*,dec}(\rho^{\mathcal{C}}_{com}, b), \mathcal{R}^*_{dec}(\rho^{\mathcal{R}^*}_{com})\rangle$.

Security against malicious sender. The security definitions of bit commitment against malicious sender are written as:

Definition 2.3 (Statistical binding). *A bit commitment protocol $(\mathcal{C}, \mathcal{R})$ is statistical-binding if, for every unbounded-size committer $\mathcal{C}^* = \{\mathcal{C}^*_{com}, \mathcal{C}^*_{dec}\}$ and $\lambda \in \mathbb{N}$, such that:*

$$\left(\rho^{\mathcal{C}^*}_{com}, \rho^{\mathcal{R}}_{com}\right) \leftarrow\!\!\shortmid \left(\langle \mathcal{C}^*_{com}(1^\lambda, b), \mathcal{R}_{com}(1^\lambda)\rangle\right),$$

there exists a bit $b \in \{0,1\}$ and a negligible function $\nu(\cdot)$ such that with probability at least $1 - \nu(\lambda)$,

$$I\!P[OUT_{\mathcal{R}}\langle \mathcal{C}^*_{dec}(1^\lambda, \rho^{\mathcal{C}^*}_{com}(\lambda)), \mathcal{R}_{dec}(1^\lambda, \rho^{\mathcal{R}}_{com}((\lambda))\rangle \neq b] \leq \nu(\lambda).$$

In this work, we use a weaker notion of binding that we call relaxed statistical binding. Unlike the general definition of statistically binding bit commitment, each individual commitment is not statistically binding by itself. However, committing to a collection of bits binds for a fraction $1 - \eta$ of the bits.

Definition 2.4 (η-relaxed statistical binding). *Let $(\mathcal{C}, \mathcal{R})$ be a bit commitment protocol. For a sequence of m commitments $\left(\mathcal{C}^*_i = (\mathcal{C}^*_{com,i}, \mathcal{C}^*_{dec,i})\right)_{i\in m}$ with $\lambda \in \mathbb{N}$ such that:*

$$\left(\boldsymbol{\rho}^{\mathcal{C}^*}_{com}(\lambda), \boldsymbol{\rho}^{\mathcal{R}}_{com}(\lambda)\right) \leftarrow\!\!\shortmid \left(\langle \mathcal{C}^*_{com,i}(1^\lambda, b_i), \mathcal{R}_{com,i}(1^\lambda)\rangle\right)_{i\in m}.$$

$(\mathcal{C}, \mathcal{R})$ is η-relaxed-binding if given the commitment there exists a set $I \subseteq [m]$, where $I \geq (1-\eta)m$ and a negligible function $\nu(\cdot)$ such that with probability at least $1 - \nu(\lambda)$ over $\left(\boldsymbol{\rho}^{\mathcal{C}^*}_{com}(\lambda), \boldsymbol{\rho}^{\mathcal{R}}_{com}(\lambda)\right)$, there exists a string $\boldsymbol{b} \in \{0,1\}^{|I|}$ such that,

$$I\!P[OUT_{\mathcal{R}}\langle \mathcal{C}^*_{dec}(1^\lambda, \boldsymbol{\rho}^{\mathcal{C}^*}_{com}(\lambda)), \mathcal{R}_{dec}(1^\lambda, \boldsymbol{\rho}^{\mathcal{R}}_{com}((\lambda))\rangle|_I \neq \boldsymbol{b}(\lambda)] \leq \nu(\eta).$$

Relaxed extractability works similarly to relaxed binding: after committing to many bits, most of them can be extracted.

Definition 2.5 (χ-relaxed extractability). *Let $(\mathcal{C}, \mathcal{R})$ be a bit commitment protocol. Given a sequence of auxiliary states $(\rho_i, \sigma_i)_{i\in m}$ where $\rho_i, \sigma_i \in \mathcal{B}_1(\mathbb{C}^\lambda)$ and $\lambda \in \mathbb{N}$, m sequential repetitions of commitments $(\rho^{\mathcal{C}^*}_{com,1}, \rho^{\mathcal{R}}_{com,1})$, ..., $(\rho^{\mathcal{C}^*}_{com,m}, \rho^{\mathcal{R}}_{com,m})$ are χ-relaxed-extractable if, for any poly-size quantum malicious committer $\mathcal{C}^* = \{(\mathcal{C}^*_{com,i}(1^\lambda))_{i\in m},\ (\rho_i)_{i\in m}\}$, there exists a quantum polynomial time extractor $\mathcal{Q}_{\mathcal{C}^*} = \{\mathcal{Q}_{\mathcal{C}^*,com}, \mathcal{Q}_{\mathcal{C}^*,dec}\}$ such that, for any poly-size distinguisher $\mathcal{D}^* = \{(\mathcal{D}^*_i)_{i\in m}, (\sigma_i)_{i\in m}\}$ and for every polynomial-size opening strategy $\left(\mathcal{C}^*_{dec,i}\right)_{i\in m}$, there is a negligible function $\nu(\chi) > 0$ that obeys:*

$$|I\!P[\mathcal{D}^*(\sigma_\lambda, Real) = 1] - I\!P[\mathcal{D}^*(\sigma_\lambda, Ideal) = 1]| = \nu(\chi),$$

with:

***Real**: Interaction between $\mathcal{R}_{dec}(\rho^{\mathcal{R}}_{com})$ and $\mathcal{C}^*_{dec}(\rho^{\mathcal{C}^*}_{com})$ such that $(\rho^{\mathcal{C}^*}_{final}, b_i) \leftarrow\!\!\shortmid \langle \mathcal{C}^*_{dec}(\rho^{\mathcal{C}^*}_{com}), \mathcal{R}_{dec}(\rho^{\mathcal{R}}_{com})\rangle_i$, with $b_i \in \{0, 1, \perp\}$. Then, the output after m sequential repetitions is given by $\left(\boldsymbol{\rho}^{\mathcal{C}^*}_{final}(m), \boldsymbol{b}(m)\right) \leftarrow\!\!\shortmid \left(\langle \mathcal{C}^*_{com,i}(1^\lambda, b_i), \mathcal{R}_{com,i}(1^\lambda)\rangle\right)_{i\in m}$, where $\boldsymbol{b} \in \{0, 1\}^m$.*

***Ideal**: The simulator computes $(\boldsymbol{\rho}^{\mathcal{C}}_{com}(m), \boldsymbol{\rho}^{\mathcal{R}}_{com}(m), \boldsymbol{b^*}(m)) \leftarrow\!\!\shortmid (\mathcal{Q}_{\mathcal{C}^*,com}(\rho_i))_{i\in\lambda}$, where $\boldsymbol{b}^* \in \{0, 1, ?\}^m$. Then, $(\boldsymbol{\rho}^{\mathcal{C}}_{final}(m), \boldsymbol{b}(m)) \leftarrow\!\!\shortmid \langle \mathcal{C}^*_{dec}(\boldsymbol{\rho}^{\mathcal{C}}_{com}(m)), \mathcal{R}_{dec}(\boldsymbol{\rho}^{\mathcal{R}}_{com}(m))\rangle$. The simulator outputs FAIL if :*

- $|\{i : b^*_i = ?\}| \geq \chi m$, *or*
- *if for any i such that $b^*_i \in \{0, 1\}$, $b_i \neq b^*_i$.*

If the simulator does not output FAIL, it outputs $(\boldsymbol{\rho}^{\mathcal{C}}_{final}(m), \boldsymbol{b}_S(m))$, where $\boldsymbol{b}_S(j) = \boldsymbol{b^*}(j)$ every time $b^*_i \neq ?$, and replaces the $?$ cases by the values $\boldsymbol{b}(j)$ opened by $\mathcal{C}^*_{dec}(\boldsymbol{\rho}^{\mathcal{C}}_{com}(j))$.

2.3 Leftover hash lemma

Definition 2.6 (Quantum conditional min-entropy [Ren08]). *Given a classical-quantum hybrid state $\rho_{XE} = \sum_{x\in\mathcal{X}} p_x(x) |x\rangle\langle x| \otimes \sigma^x_E$, the conditional min-entropy $H_{min}(X|E)$ is defined as:*

$$H_{min}(X|E) = H_{min}(\rho_{XE}|E) = \sup_{\sigma_E} \max\{h \in \mathbb{R} : 2^{-h}\, \mathbb{I} \otimes \sigma_E - \rho_{XE} \geq 0\}.$$

Lemma 2.7 (Leftover Hash Lemma with Quantum Side Information [Ren08]). *Let ρ_{XE} be a hybrid state and $h(r, x) : \{0, 1\}^m \times \{0, 1\}^n \to \{0, 1\}^\ell$ a two-universal hash function, with r uniformly distributed over $\mathcal{R}$. Then, $K = h(r, x)$ satisfies:*

$$\Delta(\rho_{K_{\bar{b}} K_b E}, \frac{1}{2^\ell}\mathbb{I} \otimes \rho_{K_b E}) \leq \frac{1}{2}\sqrt{2^{\ell - H_{min}(X|E)}}.$$

Lemma 2.8 (Conditional min-entropy [BF12]). *Given an n-qubit system A, let the state $|\psi_{AE}\rangle = \sum_{\substack{\boldsymbol{b}\in\{0,1\}^n \\ |w(\boldsymbol{b})-\alpha|\leq\delta}} |b\rangle \otimes |\psi_E^b\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E$ have a relative Hamming weight δ-close to α, with $\delta + \alpha \leq 1/2$. Let X be the random variable obtained by measuring A in the bases $H^{\boldsymbol{\theta}}\{|0\rangle, |1\rangle\}^{\otimes n}$ for $\boldsymbol{\theta} \in \{0,1\}^n$. Then:*

$$H_{min}(X|E) \geq d_H(\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}) - h_2(\delta + \alpha)n, \tag{2.1}$$

where $\hat{\boldsymbol{\theta}} \in \{0,1\}^n$ denotes the measurement bases committed by Bob, $h_2(\cdot) : [0,1] \to [0,1]$, the binary entropy function and $d_H(\cdot,\cdot) : \{0,1\}^n \times \{0,1\}^n \to \mathbb{N}$, the Hamming distance function.

2.4 Watrous Rewinding Lemma

Lemma 2.9 (Rewinding lemma with small perturbations [Wat06]). *Let Q be an (n,k)-quantum circuit that outputs a classical bit b and m qubits. For any input state $|\psi\rangle \in \mathcal{B}_1(\mathbb{C}^n)$, let $p(\psi)$ be the probability of measuring the classical bit $b = 0$ such that the state after measuring the action of the the circuit Q is $|\phi_0(\psi)\rangle \in \mathcal{B}_1(\mathbb{C}^m)$. Let $p_0 \in (0,1)$, $\epsilon \in (0,1/2)$ and $q \in (0,1)$, where q is the probability that the quantum circuit acts like a unitary, be such that:*

1. *$|p(\psi) - q| < \epsilon$, $\forall\, |\psi\rangle \in \mathcal{B}_1(\mathbb{C}^n)$,*
2. *$p_0 < p(\psi)$, $\forall\, |\psi\rangle \in \mathcal{B}_1(\mathbb{C}^n)$,*
3. *$p_0(1-p_0) \leq q(1-q)$.*

Then, there exists a general quantum circuit $\mathcal{R}$ of size $\mathcal{O}\left(\frac{\log(1/\epsilon)|Q|}{p_0(1-p_0)}\right)$, such that, for every input state $|\psi\rangle$, the output $R(|\psi\rangle)$ satisfies:

$$\|R(|\psi\rangle) - |\phi_0(\psi)\rangle\|_1 \leq 4\sqrt{\epsilon}\frac{\log(1/\epsilon)}{p_0(1-p_0)}.$$

2.5 Error resilience

Handling error correction in our protocol involves more subtleties compared to, for example, QKD, since in our case Alice and Bob are not trusted. In quantum communication protocols, there are two primary sources of errors: noise and loss. In the case of loss, since the proposed protocol incorporates bit commitments for each BB84 state, the loss of a state will result in the absence of a commitment for that instance of the protocol. Discarding non-committed instances has no impact on the security analysis of the protocol.

The potential presence of malicious parties prevents them from cooperating to estimate the noise. Therefore, an error correction subroutine must be included in the protocol to handle errors without any collaboration between parties [DFSS06,ENG+14,LPAK23]. An $(\mathcal{M}, K, t)$-error correction code can correct errors in a code C composed of K elements from a metric space $\mathcal{M}$, such that for every element $w \in \mathcal{M}$, there exists at most one codeword $c \in C$ within a ball of radius t around w.

We propose the use of a non-interactive (classical) error correction code, which is syndrome-based, such as Low-Density Parity-Check (LDPC) codes [Gal60]. The syndrome of an element w is its projection onto the orthogonal subspace of the code, capturing all the necessary information for decoding.

Finally, we consider the possibility of multiphoton events. While an ideal BB84 source generates single photons, experimental sources could accidentally generate more than one copy of a BB84 instance. We take into account this leakage of information for the privacy amplification of our proposed protocol. We present this as a general variable ϑ that accounts for the information leakage.

3 Equivocal Commitment

In this section, we present a compiler that yields an equivocal η-relaxed statistically binding bit commitment from a statistically binding computationally hiding bit commitment. As previously discussed in the Introduction, our compiler is directly based on [BCKM21], but we reduce the number of repetitions in order to improve efficiency at the cost of requiring relaxed binding properties. The protocol is described in Algorithm 1 and we prove the relaxed binding property in Section 3.1 and equivocality in Section 3.2.

3.1 Relaxed statistical binding

Given a statistical binding and computationally hiding commitment, we can build a commitment named *EqCommitment* that is η-relaxed statistically binding (Definition 2.4) and computationally hiding (Definition 2.1).

Theorem 3.1. *If Com is a statistically binding commitment scheme, then, for any function $\eta(n)$, EqCommitment is $(\eta, 2^{-n\eta})$-relaxed statistically binding.*

Proof. Let us consider n sequential repetitions of the EqCommitment protocol. Let us denote $c^{\gamma}_{\delta,i}$ as the commitment c^{γ}_{δ} of the i-th run of the protocol. Notice that all $c^{\gamma}_{\delta,i}$ are statistically binding, so with overwhelming probability, we can define the values $u^{\gamma}_{\delta,i}$ such that the opening of $c^{\gamma}_{\delta,i}$ to a value that is different than $u^{\gamma}_{\delta,i}$ fails.

Let us define the set of $B_0 = \{i : \exists\gamma \quad u^{\gamma}_{0,i} \neq u^{\gamma}_{1,i}\}$. Let us also define the event E where the check on Step 4 passes on all runs of the protocol. Notice that for each $j \notin B_0$, the j-th run of the commitment is statistically binding, and the goal is now to connect $|B_0|$ and $\mathbb{P}[E]$. It can be shown that:

$$\mathbb{P}[E] \leq \frac{1}{2^{|B_0|}}, \tag{3.1}$$

which is equivalent to the fact that if $\mathbb{P}[E] \geq 2^{-n\eta}$, then $|B_0| \leq n\eta$, which shows that EqCommitment is $(\eta, 2^{-n\eta})$-relaxed statistically binding. The proof of Equation (3.1) holds since for each $i \in B_0$, there exists one γ^*_i such that $u^{\gamma^*_i}_{0,i} \neq u^{\gamma^*_i}_{1,i}$, and in order for E be true, the challenged γ_i for that run is different than γ^*_i,

Algorithm 1 EqCommitment: Equivocal commitment

Input of $\mathcal{C}$: bit $b \in \{0,1\}$, seeds $\boldsymbol{p}_0^0, \boldsymbol{p}_1^0, \boldsymbol{p}_0^1, \boldsymbol{p}_1^1 \in \{0,1\}^{\lambda_{PQS}}$.
Assumptions: Bit commitment Com_r that is statistically binding and computationally hiding and which uses r as the randomness for the commitment

Commit phase:

1: $\mathcal{C}$ chooses two random bits $u^0, u^1 \in \{0,1\}$.
2: $\mathcal{C}$ and $\mathcal{R}$ commit to four values, by using the input seeds in the following way:
   - $c_0^0 = Com_{\boldsymbol{p}_0^0}\langle \mathcal{C}(u^0), \mathcal{R}\rangle$
   - $c_1^0 = Com_{\boldsymbol{p}_1^0}\langle \mathcal{C}(u^0), \mathcal{R}\rangle$
   - $c_0^1 = Com_{\boldsymbol{p}_0^1}\langle \mathcal{C}(u^1), \mathcal{R}\rangle$
   - $c_1^1 = Com_{\boldsymbol{p}_1^1}\langle \mathcal{C}(u^1), \mathcal{R}\rangle$
3: $\mathcal{R}$ sends a bit $\gamma \in \{0,1\}$ to $\mathcal{C}$
4: $\mathcal{R}$ and $\mathcal{C}$ decommit $u_0^\gamma = Decom_{\boldsymbol{p}_0^\gamma}(c_0^\gamma)$ and $u_1^\gamma = Decom_{\boldsymbol{p}_1^\gamma}(c_1^\gamma)$
5: $\mathcal{R}$ aborts if $u_0^\gamma \neq u_1^\gamma$.
6: $\mathcal{C}$ computes $e = b \oplus u^{\bar{\gamma}}$ and sends it to $\mathcal{R}$.

Decommit phase:

7: $\mathcal{C}$ chooses a random bit $\delta \in \{0,1\}$ and sends both, δ and b to $\mathcal{R}$.
8: $\mathcal{C}$ and $\mathcal{R}$ decommit $c_\delta^{\bar{\gamma}}$:

$$u_\delta^{\bar{\gamma}} = Decom_{\boldsymbol{p}_\delta^{\bar{\gamma}}}(c_\delta^{\bar{\gamma}})$$

9: $\mathcal{R}$ aborts if $u_\delta^{\bar{\gamma}} \neq b \oplus e$.

which happens with probability $\frac{1}{2}$. Since all challenges are picked independently, the probability is:

$$\mathbb{P}[\forall i \in B_0 : \gamma_i \neq \gamma_i^*] = \prod_{i \in B_0} \mathbb{P}[\gamma_i \neq \gamma_i^*] \leq \frac{1}{2^{|B_0|}},$$

where the inequality accounts for the trivial case where $\nexists \gamma_i$ such that $u_{0,i}^{\gamma_i} \neq u_{1,i}^{\gamma_i}$, resulting in $\mathbb{P}[E] = 0$.

3.2 Equivocality

Our proof of equivocality is the same as [BCKM21], and we provide it here for completeness. We apply Watrous' rewinding on the equivocal simulator in Algorithm 2 to pass the verification test while not having consistent commitments.

Theorem 3.2. *If Com is a computationally hiding commitment, then EqCommitment is an equivocal bit commitment*

Proof. In order to apply the rewinding lemma, we can consider a communication scheme as follows.

- $\mathcal{C}$: the committer $\mathcal{C}$ commits and communicates with the malicious receiver $\mathcal{R}^*$ through the polynomial-size register M.

Algorithm 2 Equivocal simulator $\mathcal{Q}_{Eq}$

1: $\mathcal{Q}_{\mathcal{R}^*}$ samples a random bit $\tilde{\gamma} \in \{0,1\}$ and stores it in P.
2: $\mathcal{C}$ samples two random bits $\tilde{u}, \tilde{y} \in \{0,1\}$
3: Commitment subprotocol for the simulated committer $\tilde{\mathcal{C}}$
- If $\tilde{\gamma} = 0$, $\tilde{\mathcal{C}}$ commits to:
  1. $\tilde{c}_0^0 = Com_{\boldsymbol{p}_0^0}\langle\tilde{\mathcal{C}}(\tilde{y}), \mathcal{R}^*\rangle$
  2. $\tilde{c}_1^0 = Com_{\boldsymbol{p}_1^0}\langle\tilde{\mathcal{C}}(\tilde{y}), \mathcal{R}^*\rangle$
  3. $\tilde{c}_0^1 = Com_{\boldsymbol{p}_0^1}\langle\tilde{\mathcal{C}}(\tilde{u}), \mathcal{R}^*\rangle$
  4. $\tilde{c}_1^1 = Com_{\boldsymbol{p}_1^1}\langle\tilde{\mathcal{C}}(1-\tilde{u}), \mathcal{R}^*\rangle$
- If $\tilde{\gamma} = 1$, $\tilde{\mathcal{C}}$ commits to:
  1. $\tilde{c}_0^0 = Com_{\boldsymbol{p}_0^0}\langle\tilde{\mathcal{C}}(\tilde{u}), \mathcal{R}^*\rangle$
  2. $\tilde{c}_1^0 = Com_{\boldsymbol{p}_1^0}\langle\tilde{\mathcal{C}}(1-\tilde{u}), \mathcal{R}^*\rangle$
  3. $\tilde{c}_0^1 = Com_{\boldsymbol{p}_0^1}\langle\tilde{\mathcal{C}}(\tilde{y}), \mathcal{R}^*\rangle$
  4. $\tilde{c}_1^1 = Com_{\boldsymbol{p}_1^1}\langle\tilde{\mathcal{C}}(\tilde{y}), \mathcal{R}^*\rangle$
- Run commitment phase between $\mathcal{C}$ and $\mathcal{R}^*$.
- Measure γ in the register A. If $\tilde{\gamma} = \gamma$, the simulator was successful, output 0. Otherwise, output 1.

4: Let $u = b \oplus e$
5: $\mathcal{Q}_{\mathcal{R}^*}$ and $\mathcal{R}^*$ decommits to:
- If $\tilde{\gamma} = 0$, decommits to the $(u \oplus \tilde{u} + 2)^{th}$ committed bit.
- If $\tilde{\gamma} = 1$, decommits to the $(u \oplus \tilde{u})^{th}$ committed bit.

- $\mathcal{R}^*$: the malicious receiver has three different registers: W, V and A. The first one, W, represents the quantum input. The registers V and A are the work space of $\mathcal{R}^*$ and both are initialized in the zero state. While V is a polynomial-size register, A is a one qubit register. $\mathcal{R}^*$ measures this second register A for sampling $\gamma \in \{0,1\}$. After the honesty check, $\mathcal{R}^*$ outputs the registers (W,V,A,M).
- $\mathcal{Q}_{\mathcal{R}^*}$: the quantum simulator works with registers P and Z in addition to (W,V,A,M). P is a one qubit register for the guess $\tilde{\gamma}$, and Z is the auxiliary register in which Algorithm 2 is implemented.

The condition to apply Watrous' lemma is that the probability for the simulator to guess the output has to be nearly independent of the probability distribution of the malicious receiver $\mathcal{R}^*$'s choice. This is guaranteed by the computationally hiding property of the underlying bit commitment. Then, $|p(\psi) - 1/2| = negl(\lambda)$, for every input state $|\psi\rangle$ of $\mathcal{R}^*$ in $\mathcal{Q}_{Eq}$. Due to Lemma 2.9, there is a poly-size circuit $\mathcal{R}$ that outputs a state inverse-exponentially close to the final state conditioned to $\tilde{\gamma} = \gamma$ of the Algorithm 2.

Once the simulator $\mathcal{Q}_{R^*,com}$ has measured the qubit register P and obtained γ, it proceeds to do the honesty check, as described in Algorithm 2 and outputs the registers (W,V,A,M) after tracing out the remaining registers.

If a quantum poly-time distinguisher $\mathcal{D}^* = \{\mathcal{D}^*_\lambda, \sigma_\lambda\}$ could distinguish $Real_b$ and $Ideal_b$, it would mean that $\mathcal{D}^*$ is able to discriminate the commitments of the simulator $\mathcal{Q}_{R^*}$ and the honest committer $\mathcal{C}$. This would imply that the dis-

tinguisher is able to open the committed values which contradicts the definition of computational hiding of the base commitment scheme. □

4 Equivocal and relaxed extractable commitment

We construct an equivocal and χ-relaxed extractable commitment (Definition 2.5), named *ERE-Commitment*, based on an equivocal and η-relaxed statistically binding commitment.

We present our protocol in Algorithm 3. We first notice that if the committer and receiver are honest, then the protocol succeeds.

Lemma 4.1. *Given an implementation of ERE-Commmitment for which the noise error in the BB84 transmission is $\delta \leq \alpha$ between an honest committer and an honest receiver, the committer does not abort.*

Proof. As discussed in Section 2.5, an $(\mathcal{M}, 4\lambda_{EX}, 4\alpha\lambda_{EX})$-error correction code can unambiguously correct up to a proportion of α errors. Therefore, for any $\delta \leq \alpha$, there is at most one codeword inside the radius of the error correction code, not aborting in Step 11.3 of Algorithm 3 □

We now prove the equivocality and the relaxed extractability of our protocol.

4.1 Equivocality

The proof of equivocality is very similar to Theorem 3.2. Nevertheless, we also provide in Corollary 4.3 the condition for the Naor's commitment subprotocol of the ERE-Commitment to be computationally hiding, giving in Lemma 5.4 an analytical expression that quantifies it.

Theorem 4.2. *If Com is computationally hiding, then ERE-Commitment is an equivocal bit commitment.*

Proof. The main difference with respect to the proof for EqCommitment is that the equivocal simulator has to answer correctly the commitment of w equivocal boxes in parallel with single challenge bit γ_r. Given a computationally hiding bit commitment, $|p(\psi) - 1/2| = negl(\lambda)$ also for this case. Hence, all the properties of the Algorithm 2 and the application of Watrous' rewinding lemma are equivalent for this scheme. Therefore, from computational hiding, $Real_b$ and $Ideal_b$ of Def. 2.2 are indistinguishable.

□

Corollary 4.3. *If $Com_{\boldsymbol{p}_i^j}$ is implemented using Naor's bit commitment with input seeds $\boldsymbol{p}_i^j \in \{0,1\}^{\lambda_{PQS}}$, where $(\boldsymbol{p}_1^j, ..., \boldsymbol{p}_{2w}^j) = PRG(\boldsymbol{s}^j)$ for $\boldsymbol{s}^j \in \{0,1\}^{\lambda_{PQS}}$, then ERE-Commitment is an equivocal bit commitment.*

Proof. We have to prove that the Naor's bit commitment scheme [Nao91] is computationally hiding giving the pseudorandom seeds $\boldsymbol{p}_i^j \in \{0,1\}^{\lambda_{PQS}}$. Naor's bit commitment is an interactive bit commitment in which the receiver sends $k \xleftarrow{\$} \{0,1\}^{\lambda^3}$ to the committer, which commits to the bit b by sending $(b \cdot k) \oplus W(r)$, where $r \xleftarrow{\$} \{0,1\}^{\lambda}$ and $W : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda^3}$ is a pseudo-random generator. Thus, the computational hiding property is guaranteed by the pseudorandomness property of W. In this case, the seed $\boldsymbol{p}_i^j$ of the Naor's base commitment is not randomly sampled by the committer, but obtained as the output of a PRG which input is $(\boldsymbol{s}^j)_{j\in[2k]}$. $(\boldsymbol{s}^j)_{j\in[2k]}$ are generated by hashing the strings $(\tilde{\boldsymbol{x}}^j)_{j\in[2k]}$. Therefore, computational hiding would be fulfilled if the strings $(\boldsymbol{s}^j)_{j\in[2k]}$ are random strings. By applying the leftover hash lemma (Lemma 2.7), the obtained seeds are arbitrarily close to a random string, as proven in Theorem A.1 of Appendix A. □

4.2 Relaxed-extractability

Before proving relaxed-extractability, we first show that our commitment scheme is relaxed-binding.

Theorem 4.4. *If Com is a statistically binding commitment scheme, then for any function $\eta(k)$ ERE-Commitment is η-relaxed statistically binding.*

Proof. The proof is similar to the one of Theorem 3.1. In ERE-Commitment, the seeds of the base commitments Com_r are used as described in Algorithm 3. Therefore, when the honesty check is done, the sampled population is not the number of sequential repetitions of the EqCommitment wk but the number of different families k since the EqCommitment instances which make use of seeds derived from the same family $\boldsymbol{p}^j$ are opened together. □

To prove extractability, we will use the equivocality properties of EqCommitment. To prove that the simulator $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ defined in Algorithm 4 that represents the *Ideal* interaction from Definition 2.5 is indistinguishable from the *Real* one, we use the following sequence of hybrid arguments:

- **Hybrid 0**. Corresponds to the real protocol described in Algorithm 3.
- **Hybrid 1**. Similar to Hyb_0 except in Step 3, in which we execute the equivocal simulator $\mathcal{Q}_{\mathcal{R}^*,com}$ for $i \in [4\lambda_{EX}]$, and in Step 5, to open the challenged commitments $i \in [E]$, we execute $\mathcal{Q}_{\mathcal{R}^*,dec}$.
- **Hybrid 2**. Similar to Hyb_1, except that $|\boldsymbol{x}\rangle_{\boldsymbol{\theta}}$ is not measured during Step 2 of 3, but rather during Step 3 of Algorithm 4, i.e., only the positions $i \in E$ are measured and only after obtaining the sequence of indices.
- **Hybrid 3**. Identical to Hyb_2 but instead of performing the honesty check given by Step 11 of Algorithm 3, it does it as Step 8 of Algorithm 4.
- **Hybrid 4**. Identical to Hyb_3 but the simulator extracts the non-challenged commitments as described in Step 9 of 4.

Algorithm 3 ERE-Commitment: Equivocal and relaxed extractable commitment

Committer $\mathcal{C}$ Input: A sequence of bits $(b_i)_{i\in[wk]}$.

Assumptions: The parties use a $PRG : \{0,1\}^{\lambda_{PQS}} \to \{0,1\}^{2w\cdot\lambda_{PQS}}$, 2-universal hash functions $h_j(\cdot,\cdot) : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^{\lambda_{PQS}}$, an EqCommitment that is equivocal and a statistically binding and computationally hiding commitment Com_r which uses r as the randomness of the commitment.

1: $\mathcal{C}$ samples $\boldsymbol{x} \leftarrow \{0,1\}^{4\lambda_{EX}}$ and $\boldsymbol{\theta} \leftarrow \{+,\times\}^{4\lambda_{EX}}$ and sends $|\boldsymbol{x}\rangle_{\boldsymbol{\theta}}$ to $\mathcal{R}$.

2: $\mathcal{R}$ chooses his measurement bases $\hat{\boldsymbol{\theta}} \leftarrow \{+,\times\}^{4\lambda_{EX}}$ and measures $\hat{\boldsymbol{x}} \leftarrow \{0,1\}^{4\lambda_{EX}}$.

3: $\mathcal{R}$ sequentially commits to $\left((\hat{x}_i,\hat{\theta}_i)\right)_{i\in[4\lambda_{EX}]}$ using EqCommitment.

4: $\mathcal{C}$ challenges a random subset $E \subset [4\lambda_{EX}]$, such that $|E| = 2\lambda_{EX}$.

5: $\mathcal{C}$ and $\mathcal{R}$ execute EqDecommitment sequentially for every $i \in E$. Then, $\mathcal{C}$ obtains $\left((\hat{x}_i,\hat{\theta}_i)\right)_{i\in E}$. $\mathcal{C}$ aborts if the commitment fails to open.

6: $\mathcal{C}$ checks that $x_i = \hat{x}_i$ whenever $\theta_i = \hat{\theta}_i$, up to a fraction α due to the experimental error. If the test does not pass, $\mathcal{C}$ aborts.

7: $\mathcal{C}$ divides $\bar{E}$ into $2k$ consecutive disjoint subsets $M_j \subseteq \bar{E}$ of size m, with m given by the size of the preimage of a 2-universal hash function $\{h_j(\cdot,\cdot) : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^{\lambda_{PQS}}\}_{j\in[2k]}$, where $k = \lfloor \lambda_{EX}/m \rfloor$.

8: For every $j \in [2k]$, $\mathcal{C}$ samples $\boldsymbol{r}^j \in \{0,1\}^n$ and compute $\boldsymbol{s}^j = h_j(\boldsymbol{r}^j, \tilde{\mathbf{x}}^j)$ where $\tilde{\mathbf{x}}^j = \{x_i : i \in M_j\}$.

9: Given $PRG : \{0,1\}^{\lambda_{PQS}} \to \{0,1\}^{2w\cdot\lambda_{PQS}}$, $\mathcal{C}$ generates $\boldsymbol{p}^j = PRG(\boldsymbol{s}^j) = (\boldsymbol{p}_1^j, ..., \boldsymbol{p}_{2w}^j)$ for every $j \in [2k]$, where $\boldsymbol{p}_i^j \in \{0,1\}^{\lambda_{PQS}}$.

10: $\mathcal{C}$ sends $(M_j)_{j\in[2k]}$, $\boldsymbol{\theta}$ and $(\boldsymbol{r}^j)_{j\in[2k]}$ to $\mathcal{R}$. $\mathcal{C}$ sends the syndromes $(Synd_j)_{j\in[2k]}$ to correct a proportion α of errors.

11: $\mathcal{C}$ and $\mathcal{R}$ sequentially execute k sessions of w parallel EqCommitment. For each $r \in [k]$:

11.1: $\mathcal{C}$ commits in parallel to w pairs of random bits with $\left(\boldsymbol{p}_{i_{q,0}}^{j^{r,0}}, \boldsymbol{p}_{i_{q,1}}^{j^{r,0}}, \boldsymbol{p}_{i_{q,0}}^{j^{r,1}}, \boldsymbol{p}_{i_{q,1}}^{j^{r,1}}\right)_{q\in[w]} = \left(\boldsymbol{p}_{2q-1}^{2r-1}, \boldsymbol{p}_{2q}^{2r-1}, \boldsymbol{p}_{2q-1}^{2r}, \boldsymbol{p}_{2q}^{2r}\right)_{q\in[w]}$ as seeds.

11.2: For the honesty check of the EqCommitment, $\mathcal{R}$ samples $\gamma_r \xleftarrow{\$} \{0,1\}$ and sends it to $\mathcal{C}$.

11.3: $\mathcal{C}$ sends $\tilde{\mathbf{x}}^{j^{r,\gamma_r}}$ and $p^{j^{r,\gamma_r}}$ to $\mathcal{R}$. $\mathcal{R}$ checks if,

- $\tilde{x}_i = \tilde{\hat{x}}_i$ whenever $\tilde{\theta}_i = \hat{\theta}_i$, where $\tilde{\hat{x}}_i$ are $\mathcal{R}'s$ measures corrected with the syndromes $(Synd_j)_{j\in[2k]}$ and, if not, aborts.
- $PRG(h_{j^{r,\gamma_r}}(\tilde{\mathbf{x}}^{j^{r,\gamma_r}})) = \boldsymbol{p}^{j^{r,\gamma_r}}$ and, if not, aborts.
- $Decom_{\boldsymbol{p}_{i_{q,0}}^{j^{r,\gamma_r}}}(c_{i_{q,0}}^{j^{r,\gamma_r}}) = Decom_{\boldsymbol{p}_{i_{q,1}}^{j^{r,\gamma_r}}}(c_{i_{q,1}}^{j^{r,\gamma_r}})$ for every $q \in [w]$ and, if not, aborts.

11.4: $\mathcal{C}$ commits to each $(b_i)_{i\in[w]}$ as described in EqCommitment.

12: When necessary, $\mathcal{C}$ and $\mathcal{R}$ open to any of the committed bits $(b_i)_{i\in[wk]}$ by executing EqDecommitment. In order to do so, $\mathcal{C}$ sends the seeds $\boldsymbol{p}_{i_{q,\delta}}^{j^{r,\bar{\gamma}}}$ to $\mathcal{R}$.

– **Hybrid 5**. The *Ideal* distribution, i.e., the extractable simulator described in Algorithm 4. The difference with respect to Hyb_4 is that the simulator opens the non-extracted commitments to the value opened by the malicious committer, as described on Step 10.

Lemma 4.5. *There exists a negligible function $\nu(\lambda)$, such that:*

$$|I\!P[\mathcal{D}^*(\sigma, Hyb_1) = 1] - I\!P[\mathcal{D}^*(\sigma, Hyb_0) = 1]| = \nu(\lambda).$$

Proof. Suppose that there exists a non-negligible function for which $\mathcal{D}^*$ can distinguish between Hyb_0 and Hyb_1. This is equivalent to:

$$\left|\mathbb{P}[\mathcal{D}^*(\sigma, \mathrm{Hyb}_{0,i-1}) = 1] - \mathbb{P}[\mathcal{D}^*(\sigma, \mathrm{Hyb}_{0,i}) = 1]\right| \geq \frac{1}{poly(\lambda)4\lambda},$$

where $\mathrm{Hyb}_{0,j}$ is the sub-hybrid that is identical to Hyb_0 until the committed bit $j \in [4\lambda_{EX}]$ and then identical to Hyb_1. Therefore, $\mathcal{D}^*$ would be able to distinguish between the outputs ρ^{CO}_{final} of an honest and an equivocated commitment, contradicting Definition 2.2. □

Lemma 4.6. $|I\!P[\mathcal{D}^*(\sigma, Hyb_2) = 1] \equiv I\!P[\mathcal{D}^*(\sigma, Hyb_1) = 1]|$.

Proof. Since the states corresponding to the subset $E \subset 4\lambda_{EX}$ are also measured with randomly sampled bases $(\hat{\theta}_i)_{i\in E}$, the two experiments have exactly the same output distribution. □

Lemma 4.7. *There exists a negligible function $\nu(\lambda)$, such that,*

$$|I\!P[\mathcal{D}^*(\sigma, Hyb_3) = 1] - I\!P[\mathcal{D}^*(\sigma, Hyb_2) = 1]| = \nu(\lambda).$$

Proof. A quantum poly-time distinguisher $\mathcal{D}^*$ would be able to discriminate between both distributions if Hyb_2 and Hyb_3 had different probabilities for output $\perp$ during the honesty check. Since the honesty check is performed in the same way in both Hybrids, taking into account in the error correction, they are indistinguishable. □

Algorithm 4 Extractable simulator

1: $\mathcal{C}^*(\rho)$ outputs $\boldsymbol{\Psi}$
2: For $i \in [4\lambda_{EX}]$, execute sequentially the quantum equivocal simulator $\mathcal{Q}_{\mathcal{R}^*}$ to generate a tuple of $((c_\delta^{\tilde{j}})_{\delta=0,1}^{i})_{i\in[4\lambda_{EX}]}$ dummy commitments. After each commitment session, $(\rho_i^{\mathcal{S}}, \rho_{com,i}^{y}) \leftarrow\!\!\shortmid\; \mathcal{Q}_{\mathcal{R}^*,com}(\rho)$, where $\rho_i^{\mathcal{S}}$ is stored by $\mathcal{Q}_{\mathcal{C}^*}(\rho)$, and $\boldsymbol{\rho}_{com,i}^{y}$ is used by the malicious committer $\mathcal{C}^*$ as an input in the next session.
3: Once $\mathcal{C}^*$ has announced the challenged subset $E \subset [4\lambda_{EX}]$, $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ samples $\hat{\boldsymbol{\theta}} \leftarrow \{+,\times\}^{2\lambda_{EX}}$. $\mathcal{Q}_{\mathcal{C}^*}$ measures the i^{th} qubit of $\boldsymbol{\Psi}$, Ψ_i, for every $i \in E$ in the previous sampled bases, obtaining $(\hat{x}_i)_{i\in[E]}$.
4: By applying the equivocal simulator $\mathcal{Q}_{Eq}$, $\mathcal{Q}_{\mathcal{C}^*}$ opens the challenged bits $z_i \in E$ to the correct values $(\hat{x}_i, \hat{\theta}_i)_{i\in[E]}$. To do so, it executes for each $i \in [E]$: $\rho_{final}^{x} \leftarrow\!\!\shortmid\; \langle \mathcal{Q}_{\mathcal{R}^*,dec}(\hat{x}_i, \hat{\theta}_i, z_i, \rho_{com}^{x}), \mathcal{C}_{dec}^*(\rho_{com}^{y})\rangle$, where ρ_{com}^{x} is the current state of $\mathcal{C}^*$, updated after each session.
5: If $\mathcal{C}^*$ aborts at any point, $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ outputs $\perp$, otherwise continues.
6: $\mathcal{C}^*$ and $\mathcal{R}$ discard the tested positions and both reorder their respective tuples $((x_i,\theta_i))_{i\in\bar{E}}$ and $((\hat{x}_i,\hat{\theta}_i))_{i\in\bar{E}}$. $\mathcal{C}^*$ sends $\boldsymbol{\theta}$, computes the $(\boldsymbol{p}^j)_{j\in[2k]}$ as described in Algorithm 3 and sends $(\boldsymbol{r}^j)_{j\in[2k]}$.
7: $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ measures each qubit $\psi_i \in \bar{E}$ in the bases θ_i to obtain $\hat{x}_i = x_i$. $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ performs the error correction on $\hat{\boldsymbol{x}}$ by using the syndrome *Synd*. Then, $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ computes the seeds $\left(\left(\hat{\boldsymbol{p}}_{i_{q,0}}^{j^{r,0}}, \hat{\boldsymbol{p}}_{i_{q,1}}^{j^{r,0}}, \hat{\boldsymbol{p}}_{i_{q,0}}^{j^{r,1}}, \hat{\boldsymbol{p}}_{i_{q,1}}^{j^{r,1}}\right)_{q\in[w]}\right)_{r\in[k]}$.
8: $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ executes the honesty check as described in Step 11 of Algorithm 3.
9: $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ extracts the non challenged commitments:
  9.1: $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ checks if $Decom_{\hat{\boldsymbol{p}}_{i_{q,0}}^{j^{r,\gamma}}}(c_{i_{q,0}}^{j^{r,\gamma}}) = Decom_{\hat{\boldsymbol{p}}_{i_{q,1}}^{j^{r,\gamma}}}(c_{i_{q,1}}^{j^{r,\gamma}})$ where $\hat{\boldsymbol{p}}_{i_{q,\delta}}^{j^{r,\gamma}}$ are the ones obtained in Step 7.
  9.2: For the positions where this is the case, $b_{r,q}^* = Decom_{\hat{\boldsymbol{p}}_{i_{q,0}}^{j^{r,\gamma}}}(c_{i_{q,0}}^{j^{r,\gamma}} \oplus e_{r,q})$, otherwise $b_{r,q}^* = ?$.
  9.3: If the proportion of $b_i^* = ?$ is larger than $\chi = \eta + \zeta$, with $\eta = \zeta = \log^2(k)$, $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ outputs aborts, where $i = (r-1) * w + q$ are the reordered indexes.
  9.4: Otherwise, $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ outputs $(\boldsymbol{\rho}_{com}^{\mathcal{C}}, \boldsymbol{\rho}_{com}^{\mathcal{R}}, \boldsymbol{b}^*)$, where $\boldsymbol{b}^* \in \{0,1\}^{wk}$ is the string of bits in which $\boldsymbol{b}_i^* = b_i^*$ for the positions in which the output was not $?$ and an equivocated dummy commitment for the remaining positions by executing the quantum equivocal simulator $\mathcal{Q}_{Eq}$. $\boldsymbol{\rho}_{com}^{\mathcal{C}}$ is the resulting state of $\mathcal{C}^*$ and $\boldsymbol{\rho}_{com}^{\mathcal{R}} = (\boldsymbol{\theta}, \hat{\boldsymbol{\theta}}, \hat{\boldsymbol{x}})$.
10: $\mathcal{Q}_{\mathcal{C}^*}(\rho)$ opens the equivocated commitments corresponding to $?$ to the value opened by $\mathcal{C}^*$ in these positions by applying the equivocal simulator $\mathcal{Q}_{Eq}$.

Lemma 4.8. *There exists a negligible function $\nu(\lambda)$ such that:*

$$|I\!P[\mathcal{D}^*(\sigma, Hyb_4) = 1] - I\!P[\mathcal{D}^*(\sigma, Hyb_3) = 1]| = \nu(\lambda).$$

Proof. The only difference between Hyb_3 and Hyb_4 comes from the fact that the *Ideal* distribution, given by Hyb_4, outputs FAIL whenever $b_i^* \notin \{\perp, b_i, ?\}$ and the number of $?$ outputs is larger than the proportion $\chi \leq \eta + \zeta$, where ζ is the proportion of commitments seeded in a dishonest way.

In order to bound the probability of having more than a proportion ζ of dishonestly seeded commitments, let us consider again k sequential repetitions of w parallel EqCommitment protocols, as described in Algorithm 3. For the r-th instance, the q-th EqCommiment $\left(c^{j^{r,0}}_{i_{q,0}}, c^{j^{r,0}}_{i_{q,1}}, c^{j^{r,1}}_{i_{q,0}}, c^{j^{r,1}}_{i_{q,1}}\right)$ of the w parallel commitments, uses as seeds $\left(\boldsymbol{p}^{j^{r,0}}_{i_{q,0}}, \boldsymbol{p}^{j^{r,0}}_{i_{q,1}}, \boldsymbol{p}^{j^{r,1}}_{i_{q,0}}, \boldsymbol{p}^{j^{r,1}}_{i_{q,1}}\right)$.

Each $r \in [k]$ sequential honesty check is composed of a sequence of w EqCommitment that use the seeds $\boldsymbol{p}^{j^{r,0}} \leftarrow \tilde{\boldsymbol{x}}^{j^{r,0}}$ and $\boldsymbol{p}^{j^{r,1}} \leftarrow \tilde{\boldsymbol{x}}^{j^{r,1}}$. Let us define B_1 as the set of r indexes with at least one dishonestly seeded commitment $B_1 = \{r : \exists \gamma, \delta, q \quad \boldsymbol{p}^{j^{r,\gamma}}_{i_{q,\delta}}$ is not the seed of the commitment$\}$. Let us also define the event E_1 where the check on Step 11 of Algorithm 3 passes on all k sets. The goal is now to connect $|B_1|$ and $\mathbb{P}[E_1]$. It can be shown that:

$$\mathbb{P}[E_1] \leq \frac{1}{2^{|B_1|}}, \tag{4.1}$$

which is equivalent to the fact that, if $\mathbb{P}[E_1] \geq 2^{-\zeta k}$, then $|B_1| \leq \zeta k$. The proof of Equation (4.1) holds since, for each $r \in B_1$, there exists one set of indexes $\{\gamma^*, \delta^*, q^*\}$ such that $\boldsymbol{p}^{j^{r,\gamma^*}}_{i_{q^*,\delta^*}}$ is not the seed of the commitment, and in order for E_1 to be true, the challenged family of commitments seeded by $\boldsymbol{p}^{j^{r,\gamma}}$ for the r-th set of w EqCommitment instances is different from $\boldsymbol{p}^{j^{r,\gamma^*}}$, which happens with probability $\frac{1}{2}$. Since all challenges are picked independently, the probability that

$$\mathbb{P}[\forall r \in B_1 : \gamma \neq \gamma^*] = \prod_{r \in B_1} \mathbb{P}[\gamma \neq \gamma^*] \leq \frac{1}{2^{|B_1|}}.$$

Hyb_3 and Hyb_4 would be distinguishable if the malicious committer $\mathcal{C}^*$ has committed to b_i with an equivocated commitment more than a proportion $\eta = \omega(\log^2(k)/k)$, or if the malicious committer $\mathcal{C}^*$ uses as seeds $\boldsymbol{p}^j \neq PRG(h(\tilde{\mathbf{x}}^j))$ in more than a proportion $\zeta = \omega(\log^2(k)/k)$ of the keys and Hyb_3 has not output $\perp$ in the honesty check phase. This happens with probability:

$$\begin{aligned}\mathbb{P}[\text{FAIL}|\text{Ideal}] =& \mathbb{P}[\text{proportion of non extractable commitments} \geq \eta + \zeta] \\ &\leq \mathbb{P}[\text{ proportion of non extractable commitments} \geq \zeta].\end{aligned}$$

Then, $\mathbb{P}[\text{FAIL}|\text{Ideal}] < negl(\lambda)$ given Theorem 4.4. □

Lemma 4.9. $|I\!P[\mathcal{D}^*(\sigma, Hyb_5) = 1] \equiv I\!P[\mathcal{D}^*(\sigma, Hyb_4) = 1]|$.

Proof. Similar to the proof of Lemma 4.5. In the opening phase, since the opened value is the same as the one opened by the malicious committer $\mathcal{C}^*$, both distributions are indistinguishable. □

Thus, ERE-Commitment is equivocal and $\omega(\log^2(k)/k)$-relaxed-extractable in the sense of Definitions 2.2 and 2.5.

Algorithm 5 Oblivious transfer protocol

Alice A **Input:** Messages $m_0, m_1 \in \{0,1\}^\lambda$.
Bob B **Input:** Bit $b \in \{0,1\}$.
Assumptions: The parties use an ERE-Commitment that is χ-relaxed extractable and equivocal, $PRG : \{0,1\}^{\lambda_{PQS}} \to \{0,1\}^w$ and 2-universal hash functions $h_j(\cdot,\cdot) : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^{\lambda_{PQS}}$.

1: A chooses $\boldsymbol{x} \leftarrow \{0,1\}^{2\lambda_{OT}}$ and $\boldsymbol{\theta} \leftarrow \{+,\times\}^{2\lambda_{OT}}$ and sends $|x\rangle_\theta$ to B.
2: B samples his measurement bases $\hat{\boldsymbol{\theta}} \leftarrow \{+,\times\}^{2\lambda_{OT}}$ and measures $\hat{\boldsymbol{x}} \leftarrow \{0,1\}^{2\lambda_{OT}}$. A and B execute ERE-Commitment to commit to $\left((\hat{x}_i, \hat{\theta}_i)\right)_{i\in[2\lambda_{OT}]}$.
3: A challenges a random subset $T \subset [2\lambda_{OT}]$, such that $|T| = \lambda_{OT}$.
4: A and B execute ERE-Decommitment for every $i \in T$. Then, A obtains $\left((\hat{x}_i, \hat{\theta}_i)\right)_{i\in T}$.
5: A checks that $x_i = \hat{x}_i$ whenever $\theta_i = \hat{\theta}_i$, up to an experimental error α. If the test does not pass, A aborts.
6: A and B discard the tested positions and both reorder their respective sequences $((x_i, \theta_i))_{i\in\bar{T}}$ and $\left((\hat{x}_i, \hat{\theta}_i)\right)_{i\in\bar{T}}$. A sends $\boldsymbol{\theta}$ to B.
7: B partitions the set $\bar{T}$ into two different subsets: the subset in which both have measured in the same bases $I_b = \{i : \theta_i = \hat{\theta}_i\}$ and the subset in which they have not measured in the same bases $I_{\bar{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$. B sends (I_0, I_1) to A.
8: A sends the syndromes $Synd_0$ and $Synd_1$ for correcting a proportion α of errors of the bit strings $\boldsymbol{x}_0$ and $\boldsymbol{x}_1$ to B, where $\boldsymbol{x}_0 = \{x_i : i \in I_0\}$ and $\boldsymbol{x}_1 = \{x_i : i \in I_1\}$.
9: A samples seeds $s_0, s_1 \leftarrow \{0,1\}^{k(\lambda_{PQS})}$ and sends $(s_0, PRG(h(s_0, \boldsymbol{x}_0)) \oplus m_0, s_1, PRG(h(s_1, \boldsymbol{x}_1)) \oplus m_1)$.
10: B performs error correction on $\boldsymbol{x}_b$ using the syndrome $Synd_b$ and decrypts m_b by using $\hat{\boldsymbol{x}}_b$, with $\hat{\boldsymbol{x}}_b = \{\hat{x}_i : i \in I_b\}$.

5 OT from equivocal and relaxed-extractable bit commitment

In this section, we build an oblivious transfer functionality assuming an equivocal and χ-relaxed extractable bit commitment, with $\chi = \omega(\log^2(k)/k)$. The structure is similar to [DFL+09,BCKM21], but applying it to our setting. Lastly, we show how to optimize the number of runs of OT in Corollary 5.7.

The oblivious transfer functionality $\mathcal{F}_{OT}(\cdot,\cdot)$ is a quantum two-parties interactive functionality in which Alice, A, inputs two messages $m_0, m_1 \in \{0,1\}^\lambda$, and Bob, B, inputs a choice bit $b \in \{0,1\}$. The output after the interaction is (m_0, m_1) on Alice's side and (b, m_b) on Bob's side. More concretely, the OT functionality $\mathcal{F}_{\mathbf{OT}}$ works as follows:

- $\mathcal{F}_{\mathbf{OT}}((m_0, m_1), \cdot)$ takes an input b (or $\perp$), returns m_b to B and END (or $\perp$) to A.
- $\mathcal{F}_{\mathbf{OT}}(\cdot, b)$ takes an input (m_0, m_1) (or $\perp$), returns END to A and m_b (or $\perp$) to B.

Definition 5.1 (Secure OT functionality). *A protocol $\langle A(m_0, m_1), B(b)\rangle$ that implements the ideal OT functionality $\mathcal{F}_{OT}(\cdot,\cdot)$ is said to be simulation-based secure if it satisfies:*

- ***Security against a malicious Alice.*** *Given the interaction between a quantum poly-time non-uniform malicious Alice, A^*, and an honest Bob, their final state will be $\rho_{OUT,A^*}\langle A^*(m_0,m_1), B(b)\rangle$ and $OUT_B\langle A^*(m_0,m_1), B(b)\rangle$. There exists a simulator Sim_{A^*} that interacts with the ideal functionality $\mathcal{F}_{OT}(\cdot, b)$ in the following way. For every non-uniform advice $\rho, \sigma \in \mathcal{B}_1(\mathcal{H})$, where ρ and σ may be entangled, $Sim_{A^*}(\rho)$ sends either (m_0, m_1) or $\perp$ to $\mathcal{F}_{OT}(\cdot, b)$ and outputs the final state ρ_{SIM,OUT,A^*}. The output of the ideal functionality to the Bob is given by OUT_B. Then, for any quantum poly-time non-uniform distinguisher $\mathcal{D}^*$:*

$$\begin{aligned}&|I\!P[\mathcal{D}^*(\sigma, (\rho_{SIM,OUT,A^*}, OUT_B)) = 1]\\ &-I\!P[\mathcal{D}^*(\sigma, (\rho_{OUT,A^*}\langle A^*(m_0,m_1), B(b)\rangle, OUT_B\langle A^*(m_0,m_1), B(b)\rangle)) = 1]|\\ &= negl(\lambda)\end{aligned} \tag{5.1}$$

- ***Security against a malicious Bob.*** *Given the interaction between an honest Alice and a quantum poly-time non-uniform malicious Bob, B^*, their final state will be $OUT_A\langle A(m_0,m_1), B^*(b)\rangle$ and $\rho_{OUT,B^*}\langle A(m_0,m_1), B^*(b)\rangle$. There exists a simulator Sim_{B^*} that interacts with the ideal functionality $\mathcal{F}_{OT}((m_0,m_1),\cdot)$ in the following way. For every non-uniform advice $\rho, \sigma \in \mathcal{B}_1(\mathcal{H})$, where ρ and σ may be entangled, $Sim_{B^*}(\rho)$ sends either $b \in \{0,1\}$ or $\perp$ to $\mathcal{F}_{OT}((m_0,m_1),\cdot)$ and outputs the final state ρ_{SIM,OUT,B^*}. The output of the ideal functionality to Bob is given by OUT_A. Then, for any quantum poly-time non-uniform distinguisher $\mathcal{D}^*$:*

$$\begin{aligned}&|I\!P[\mathcal{D}^*(\sigma, (OUT_A, \rho_{SIM,OUT,B^*}) = 1]\\ &-I\!P[\mathcal{D}^*(\sigma, (OUT_A\langle A(m_0,m_1), B^*(b)\rangle), \rho_{OUT,B^*}\langle A(m_0,m_1), B^*(b)\rangle) = 1]|\\ &= negl(\lambda).\end{aligned} \tag{5.2}$$

5.1 Security against a malicious Alice

We will now establish the security of Bob against a quantum poly-time non-uniform malicious Alice, given Definition 5.1. To prove that Eq. 5.1 holds in the proposed scheme, the following hybrid argument is required:

- **Hybrid 0**. The *Real* distribution given by Algorithm 5.
- **Hybrid 1**. Similar to Hyb_0 except in Step 2, where we execute the equivocal simulator $\mathcal{Q}_{\mathcal{R}^*,com}$ for $i \in [2\lambda_{OT}]$. The second difference with respect to Hyb_0 is that in Step 4, to open the challenged commitments $i \in [T]$, we execute $\mathcal{Q}_{\mathcal{R}^*,dec}$.

– **Hybrid 2**. The *Ideal* distribution given by Algorithm 6.

Algorithm 6 Simulator Sim_{A^*}

1: $A^*(\rho)$ outputs the message $\boldsymbol{\Psi}$.
2: Sim_{A^*} executes $2\lambda_{OT}$ sessions of ERE-Commitment to commit to dummy values by executing the equivocal simulator $\mathcal{Q}_{\mathcal{R}^*}$.
3: Sim_{A^*} obtains the challenged set $T \subset 2\lambda_{OT}$ output by A^*.
4: Sim_{A^*} samples $\hat{\boldsymbol{\theta}} \leftarrow \{+,\times\}^{\lambda_{OT}}$. Sim_{A^*} measures the i^{th} qubit of $\boldsymbol{\Psi}$, Ψ_i, for every $i \in T$ in the previous sampled bases, obtaining $\{\hat{x}\}_{i\in[T]}$. By applying Watrous' rewinding, Sim_{A^*} opens the challenged bits to the correct values $\{\hat{x}_i, \hat{\theta}_i\}_{i\in[T]}$.
5: Sim_{A^*} discards the tested positions. A sends $\boldsymbol{\theta}$ to B. Sim_{A^*} obtains θ and measures each of the qubits $\psi_i \in \bar{T}$ in the bases θ_i to obtain $\hat{x_i} = x_i$.
6: Sim_{A^*} partitions the set $\bar{T}$ into two different subsets, by randomly sampling a bit $d_i \in \{0,1\}$ for each $i \in \bar{T}$, to create the sequences $I_0 = \{i : d_i = 0\}$ and $I_1 = \{i : d_i = 1\}$. Sim_{A^*} sends (I_0, I_1) to A^*.
7: Sim_{A^*} obtains $(s_0, PRG(h(s_0, \boldsymbol{x}_0)) \oplus m_0, s_1, PRG(h(s_1, \boldsymbol{x}_1)) \oplus m_1)$, and computes m_0 and m_1. Both, $\boldsymbol{x}_0$ and $\boldsymbol{x}_1$ are the corrected measured strings $\hat{\boldsymbol{x}}_0$ and $\hat{\boldsymbol{x}}_1$ with the syndromes $Synd_0$ and $Synd_1$.
8: If A^* aborts at any point, Sim_{A^*} sends $\perp$ to $\mathcal{F}_{OT}(\cdot, b)$. Otherwise, it sends (m_0, m_1) to $\mathcal{F}_{OT}(\cdot, b)$. The output is the final state of A^*.

Lemma 5.2. *There exists a negligible function $\nu(\lambda)$, such that:*

$$\Big| I\!P[\mathcal{D}^*(\sigma, Hyb_1) = 1] - I\!P[\mathcal{D}^*(\sigma, (\rho_{OUT,A^*}\langle A^*(\rho), B(b)\rangle, OUT_B\langle A^*(\rho), B(b)\rangle)) = 1] \Big| = \nu(\lambda).$$

Proof. It follows from the equivocality property of ERE-Commitment. □

Lemma 5.3. $I\!P[\mathcal{D}^*(\sigma, Hyb_1) = 1] \equiv I\!P[\mathcal{D}^*(\sigma, (\rho_{SIM,OUT,A^*}, OUT_B)) = 1]$.

Proof. It follows from the fact that the delay in the measurement of ψ_i with $i \in T$ cannot be noticed by A^* since, in both cases, the measurement bases are sampled at random, similar to Lemma 4.6. Then, both extracted messages m_0 and m_1 are obtained by using the same error correction syndromes as in Hyb_1, leading to the same distribution. □

5.2 Security against a malicious Bob

In this section, we prove security against malicious Bob. We start by analyzing the number of qubits necessary in the protocol to achieve the desired level of security in Lemma 5.4. Then, we prove the security of the protocol in Theorem 5.5.

Lemma 5.4 (Distance bound for a malicious Bob in QOT). *Consider a QOT protocol between an honest Alice and a malicious Bob (Algorithm 5) with ERE-Commitment as the bit commitment subprotocol (Algorithm 3). Let* $b \in \{0,1\}$ *be a random bit and* $K_b = h(r, \boldsymbol{x}_{I_b}) \in \{0,1\}^\ell$ *and* $K_{\bar{b}} = h(r, \boldsymbol{x}_{I_{\bar{b}}}) \in \{0,1\}^\ell$*, the keys.* $h(r,x) : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^\ell$ *is a 2-universal hash function, and* I_0 *and* I_1 *are the two subsets in which* $\bar{T} \subset [2\lambda_{OT}]$ *the unchallenged commitments are divided. Then, given* K_b*, for any sampling errors* $\xi, \delta > 0$*, a bit-flip error* $\alpha \geq 0$ *and a proportion* $\vartheta \geq 0$ *of leaked bits:*

$$\begin{aligned} &\Delta(\rho_{K_{\bar{b}} K_b E}, \frac{1}{2^\ell}\mathbb{I} \otimes \rho_{K_b E}) \\ &\leq \frac{1}{2} \cdot 2^{-\frac{1}{2}[(\frac{1}{2}-\xi-2\vartheta)\frac{\lambda_{OT}}{2} - h_2(\delta+\alpha+\chi)\frac{\lambda_{OT}}{2}(1-2\vartheta)-\ell-q]} \\ &+ \sqrt{6}\exp(-\lambda_{OT}\delta^2/100) + 2\exp(-\xi^2\lambda_{OT}/2), \end{aligned} \tag{5.3}$$

where E *denotes Bob's quantum state,* k*, the number of different seed families as described in Algorithm 3 and* q*, the length of the syndrome needed for performing the error correction code.* $\mathbb{I} \in \mathcal{B}(\mathbb{C}^{2^\ell})$ *is the identity operator.*

Proof. The opening and checking process, which is based on sampling, follows a structure akin to the proof provided in [BF12]. Interested readers can refer to it for a detailed analysis of the proof. This proof is done in the EPR setting in which Alice distributes half of an EPR pair to Bob in order for her to perform the sampling. Since Bob's and Alice's actions are equivalent in both settings, it suffices to prove the bound in the EPR setting. As the measurement bases are chosen randomly by Alice and Bob, the sampling strategy will be performed on a random subset $S \subseteq T$ defined as $S = \{i \in T : \theta_i = \hat{\theta}_i\}$. Alice will accept the opening phase of the bit commitment if $w(\boldsymbol{x}|_S, \hat{\boldsymbol{x}}|_S) \leq \alpha$, where $w(\cdot) = d_H(\cdot)/n$, with $n \in \mathbb{N}$ being the length of the bit-string.

Once the testing phase is accepted, the joint state $|\psi_{A_{\bar{T}}E}\rangle$ will be a superposition of states with relative Hamming weight δ close to α within $A_{\bar{T}}$ due to the statistical error of the sampling. This error given by the sampling strategy will be bounded by Hoeffding's bound:

$$\epsilon^\delta \leq \sqrt{6}\exp(-\lambda_{OT}\delta^2/100).$$

This bound is obtained in Appendix B.4 of [BF12]. Assuming that Alice chooses her bases following a uniform random distribution and for $\boldsymbol{\theta}|_{\bar{T}}$ representing the subsets of bases that were not challenged, $d_H(\boldsymbol{\theta}|_{\bar{T}}, \hat{\boldsymbol{\theta}}|_{\bar{T}}) \geq (1/2-\gamma)|\bar{T}| = (1/2-\gamma)\lambda_{OT}$ with Hoeffding's bound:

$$\epsilon^\gamma \leq 2\exp(-2\gamma^2\lambda_{OT}).$$

After the commitment and check subprotocols, the next step in the QOT protocol is when Alice sends the bases $\boldsymbol{\theta}|_{\bar{T}}$ to Bob, and Bob partitions $\bar{T}$ into two sets, I_0 and I_1. There exists a bit $b \in \{0,1\}$ such that $d_H(\boldsymbol{\theta}|_{I\bar{b}}, \hat{\boldsymbol{\theta}}|_{I\bar{b}}) \geq$

$(1/2-\epsilon-2\vartheta)\lambda_{OT}/2$, regardless of how Bob splits the sets of indexes and taking the maximum advantage of the leaked bits, i.e., all the leaked bits are used in the set $I_{\bar{b}}$. Moreover, the real size of the non-sampled subset $I_{\bar{b}}$ for which the binary entropy in bounded is $(1-2\vartheta)$. By applying Equation (2.1) to our state $\rho_{X_{\bar{b}}A^bE}$, itself obtained from measuring the subsystem $A^{\bar{b}}$ on $|\psi_{A^{\bar{b}}A^bE}\rangle$, privacy amplification gives, for $\xi = 2\gamma$:

$$\begin{aligned} H_{\min}(X_{\bar{b}}|A^bE) \geq & d_H(\boldsymbol{\theta}|_{I\bar{b}}, \hat{\boldsymbol{\theta}}|_{I\bar{b}}) - h_2(\delta+\alpha+\eta+\zeta)|I_{\bar{b}}| \\ & \geq \left(\frac{1}{2}-\xi-2\vartheta\right)\frac{\lambda_{OT}}{2} - h_2\left(\delta+\alpha+\chi\right)\frac{\lambda_{OT}}{2}\left(1-2\vartheta\right). \end{aligned}$$

Given a χ-relaxed extractable ERE-Commitment, with $\chi = \eta+\zeta = \omega(\log^2(k)/k)$, ERE-Commitment is relaxed extractable. □

We now move on to prove the security of the protocol against a quantum-poly time malicious Bob and an honest Alice. The sequence of hybrid arguments for this case is:

- **Hybrid 0**. The *Real* distribution given by Algorithm 5.
- **Hybrid 1**. Similar to Hyb_0 except in Step 2, in which we execute the extractable simulator $\mathcal{Q}_{\mathcal{R}^*,com}$ of Algorithm 4.
- **Hybrid 2**. The *Ideal* distribution given by Algorithm 7.

Algorithm 7 Simulator Sim_{B^*}

1: Sim_{B^*} chooses $\boldsymbol{x} \leftarrow \{0,1\}^{2\lambda_{OT}}$ and $\boldsymbol{\theta} \leftarrow \{+,\times\}^{2\lambda_{OT}}$ and sends $|\boldsymbol{x}\rangle_{\boldsymbol{\theta}}$ to B^*.
2: B^* and Sim_{B^*} execute $2\lambda_{OT}$ sessions of ERE-Commitment. Then, Sim_{B^*} extracts the committed values $\left(\hat{\theta}_i, \hat{x}_i\right)_{i\in[2\lambda_{OT}]}$ by applying the extractable simulator given by Algorithm 4 and aborts if the number of extracted commitments equal to $?$ are larger than $\chi = \eta+\zeta$.
3: Sim_{B^*} challenges a random subset $T \subset 2\lambda_{OT}$, such that $|T| = \lambda_{OT}$.
4: Sim_{B^*} and B^* execute ERE-Decommitment for every $i \in T$. Then, Sim_{B^*} obtains the set $\left((\hat{x}_i, \hat{\theta}_i)\right)_{i\in T}$ and checks that $x_i = \hat{x}_i$ whenever $\theta_i = \hat{\theta}_i$, up to an experimental error α. If the test does not pass, Sim_{B^*} aborts.
5: Sim_{B^*} discards the tested positions and sends $\boldsymbol{\theta}$ to B^*.
6: Sim_{B^*} obtains I_0 and I_1. Let S be the sequence of indices in I_0 such that $\theta_i \neq \hat{\theta}_i$. If $|S| \geq (1/2-\xi)\,\lambda_{OT}/2$ set $b=1$, otherwise set $b=0$.
7: Sim_{B^*} obtains m_b from $\mathcal{F}_{OT}$ and sets $m_{\bar{b}} = 0$.
8: Sim_{B^*} samples seeds $s_0, s_1 \leftarrow \{0,1\}^{k(\lambda_{PQS})}$ and sends $(s_0, PRG(h(s_0,\boldsymbol{x}_0)) \oplus m_0, s_1, PRG(h(s_1,\boldsymbol{x}_1)) \oplus m_1)$, where $\boldsymbol{x}_0 = \{x_i : i \in I_0\}$ and $\boldsymbol{x}_1 = \{x_i : i \in I_1\}$. He also sends the syndromes $Synd_0$ and $Synd_1$ for correcting a proportion α of errors of the bit strings $\boldsymbol{x}_0$ and $\boldsymbol{x}_1$. Sim_{B^*} outputs the final state of R^*.

Theorem 5.5. *There exists a negligible function $\nu(\lambda)$, such that,*

$$\Big| I\!P[\mathcal{D}^*(\sigma, Hyb_1) = 1]$$
$$- I\!P[\mathcal{D}^*(\sigma, (OUT_A\langle A(m_0, m_1), B^*(b)\rangle), \rho_{OUT,B^*}\langle A(m_0, m_1), B^*(b)\rangle) = 1]\Big| = \nu(\lambda)$$

Proof. It follows from the $\omega(\log^2(k)/k)$-relaxed-extractability definition of the bit commitment. □

Lemma 5.6. $|I\!P[\mathcal{D}^*(\sigma, Hyb_1) = 1] - I\!P[\mathcal{D}^*(\sigma, (OUT_A, \rho_{SIM,OUT,B^*}) = 1]| = \nu(\lambda)$.

Proof. This can be proven by contradiction. Suppose that there exists a distinguisher such that:

$$|\mathbb{P}[\mathcal{D}^*(\sigma, \mathrm{Hyb}_1) = 1] - \mathbb{P}[\mathcal{D}^*(\sigma, (\mathrm{OUT}_A, \rho_{SIM,\mathrm{OUT},B^*}) = 1]| \geq \frac{1}{poly(\lambda)}.$$

This would mean that there is a non-uniform quantum poly-time distinguisher $\mathcal{D}^*$ that can distinguish between the messages $m_{\bar{b}}$ obtained in Hyb_1 and $m_{\bar{b}}$ obtained in Hyb_2. Since $m_{\bar{b}}$ is encoded as $PRG(h(s_{\bar{b}}, \hat{\boldsymbol{x}}_{\bar{b}})) \oplus m_{\bar{b}}$, this would be equivalent to distinguishing between the seeds $h(s_{\bar{b}}, \hat{\boldsymbol{x}}_{\bar{b}})$ of Hyb_1 and Hyb_2. This leads to a contradiction since $h(s_{\bar{b}}, \hat{\boldsymbol{x}}_{\bar{b}})$ is statistically close to a random string due to privacy amplification, as proven in Lemma 5.4. Moreover, in both distributions, the applied syndromes for the error correction of the strings $\hat{\boldsymbol{x}}_{\bar{b}}$ and $\hat{\boldsymbol{x}}_b$ are the same one, leading to the same corrected strings. □

Corollary 5.7. *Given one implementation of the QOT protocol described in Algorithm 5 with the quantum distributed key $\boldsymbol{x} \in \{0,1\}^{2\lambda_{OT}}$, a quantity n_{OT} of 1-out-of-2 oblivious transfers can be distilled, where $n_{OT} = \lfloor \lambda_{OT}/v \rfloor$ and where v is the size of the preimage of a hash function such that $h(r, x) : \{0,1\}^{m(\lambda_{PQS})} \times \{0,1\}^m \to \{0,1\}^{\lambda_{PQS}}$. The parameter v is determined in such a way that:*

$$\begin{aligned}
&\Delta(\rho_{K_{\bar{b}}K_bE}, \frac{1}{2^\ell}\mathbb{I} \otimes \rho_{K_bE}) \\
&\leq \frac{1}{2} \cdot 2^{-\frac{1}{2}[(\frac{1}{2}-\xi)\frac{v}{2} - \vartheta\lambda_{OT} - h_2(\delta+\alpha+\chi)(\frac{v}{2}-\vartheta\lambda_{OT}) - \ell - q]} \\
&+ \sqrt{6}\exp(-\lambda_{OT}\delta^2/100) + 2\exp(-\xi^2\lambda_{OT}/2),
\end{aligned}$$

with $\ell = \lambda_{PQS}$.

Proof. The proof is similar to the one in Lemma 5.4. The sampling requires a large number of $\hat{x}_i$ and $\hat{\theta}_i$. On step 7 of Algorithm 5, Bob can choose subsets of length v of $\hat{\theta}_i$ and $\hat{x}_i$ to generate n_{OT} seeds $s_i \in \{0,1\}^{\lambda_{PQS}}$. By selecting a large enough v, we avoid finite-set sampling errors, leading ξ and δ to be representative of the whole population as in Theorem 3.2, and thus:

$$H_{\min}(X_{\bar{b}}|A^bE) \geq (\frac{1}{2} - \xi)\frac{v}{2} - \vartheta\lambda_{OT} - h_2(\delta+\alpha+\chi)(\frac{v}{2} - \vartheta\lambda_{OT}). \tag{5.4}$$

In order to obtain n_{OT} 2-out-of-1 OTs, the first difference with respect to Algorithm 5 is that, in Step 7, Bob chooses the tuple of sets $(I_{b,j})_{j\in[n_{OT}]}$ and $(I_{\bar{b},j})_{j\in[n_{OT}]}$, such that $I_{b,j} = \{i : \theta_i = \hat{\theta}_i\}$, $I_{b,j} \cap I_{b,j'} = \varnothing$, $I_{\bar{b},j} = \{i : \theta_i \neq \hat{\theta}_i\}$ and $I_{\bar{b},j} \cap I_{\bar{b},j'} = \varnothing$. Then B sends $((I_0, I_1)_j)_{j\in[n_{OT}]}$ to A. The second difference is that, in Step 8, we define $\mathbf{x}_{0,j} = \{x_i : i \in I_{0,j}\}$ and $\mathbf{x}_{1,j} = \{x_i : i \in I_{1,j}\}$. Alice can then send $((m_0, m_1)_j)_{j\in[n_{OT}]}$ different encoded messages. For each encoded message, Alice chooses at random a pair $(I_0, I_1)_j$ over the entire tuple $((I_0, I_1))_j\}_{j\in[n_{OT}]}$ and shares it with Bob, who can decrypt m messages m_b by using the strings $(\hat{\mathbf{x}}_{b,j})_{j\in[n_{OT}]}$ with $\hat{\mathbf{x}}_{b,j} = \{\hat{x}_i : i \in I_{b,j}\}$. □

6 Acknowledgements

AY acknowledges Lucas Hanouz for the discussions related with error correction. We also want to acknowledge Matías Bolaños for highlighting the necessity of adding multiphoton events and suggesting some improvements in the protocol. Lastly, we want to acknowledge anonymous reviewers for their feedback. ED, ABG and AY are supported by the European Union's Horizon Europe Framework Programme under the Marie Sklodowska Curie Grant No. 101072637, Project Quantum-Safe Internet (QSI). ED and PL acknowledge PEPR integrated project QCommTestbed ANR-22-PETQ-0011 part of Plan France 2030, VY acknowledges the support of European Research Council Starting Grant QUSCO, 758911. ED and AI acknowledge the support of QuantERA QuantaGENOMICS under Grant Agreement No. 101017733. ABG is supported by ANR JCJC TCS-NISQ ANR-22-CE47-0004. This work was done in part while ABG was visiting the Simons Institute for the Theory of Computing.

References

AAB+23. Costantino Agnesi, Marco Avesani, Federico Berra, Luca Calderaro, Sebastiano Cocchi, Giulio Foletto, Davide Scalcon, Andrea Stanco, Giuseppe Vallone, and Paolo Villoresi. A versatile and low-error polarization encoder for quantum communications. In *Quantum 2.0*, pages QTu3A–25. Optica Publishing Group, 2023.

ABKK22. Amit Agarwal, James Bartusek, Dakshita Khurana, and Nishant Kumar. A new framework for quantum oblivious transfer, 2022.

AQY22. P. Ananth, L. Qian, and H. Yuen. Cryptography from pseudorandom quantum states. In Y. Dodis and T. Shrimpton, editors, *Advances in Cryptology–CRYPTO 2022*, Lecture Notes in Computer Science, pages 208–236, Cham, 2022. Springer Nature Switzerland.

BB84. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

BBCS92. Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Maria H. Skubiszewska. Practical quantum oblivious transfer. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366, Berlin, Heidelberg, 1992. Springer.

BCKM21. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 467–496. Springer, 2021.

BF12. Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications, 2012.

CCLY23. Nai-Hui Chia, Kai-Min Chung, Xiao Liang, and Takashi Yamakawa. Post-quantum simulatable extraction with minimal assumptions: Black-box and constant-round, 2023.

CK88. Claude Crépeau and Joe Kilian. Weakening security assumptions and oblivious transfer (abstract). In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7. Springer, 1988.

DFL+09. Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, page 408–427, Heidelberg, August 2009. Springer.

DFSS06. Ivan Damgaard, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model, 2006.

ENG+14. 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.

Gal60. R. G. Gallager. *Low Density Parity Check Codes.* Sc.d. thesis, Massachusetts Institute of Technology, Cambridge, MA, September 1960.

GBR+23. Fadri Grünenfelder, Alberto Boaron, Giovanni V Resta, Matthieu Perrenoud, Davide Rusca, Claudio Barreiro, Raphaël Houlmann, Rebecka Sax, Lorenzo Stasi, Sylvain El-Khoury, et al. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. *Nature Photonics*, 17(5):422–426, 2023.

GLSV21. Alex B Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 531–561. Springer, 2021.

IPS08. Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer–efficiently. In *Advances in Cryptology–CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings 28*, pages 572–591. Springer, 2008.

IR90. Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In Shafi Goldwasser, editor, *Advances in Cryptology — CRYPTO' 88*, pages 8–26, New York, NY, 1990. Springer New York.

Kil88. Joe Kilian. Founding cryptography on oblivious transfer. In *20th ACM STOC*, pages 20–31. ACM Press, May 1988.

LC97. Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 1997.

LPAK23. Cosmo Lupo, James T. Peat, Erika Andersson, and Pieter Kok. Error-tolerant oblivious transfer in the noisy-storage model. *Physical Review Research*, 5(3), September 2023.

May97. Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 1997.

MY22. Tomoyuki Morimae and Takashi Yamakawa. *Quantum Commitments and Signatures Without One-Way Functions*, page 269–295. Springer Nature Switzerland, 2022.

Nao91. Moni Naor. Bit commitment using pseudorandomness. *Journal of cryptology*, 4(2):151–158, 1991.

PSC+23. Yoann Pelet, Grégory Sauder, Mathis Cohen, Laurent Labonté, Olivier Alibart, Anthony Martin, and Sébastien Tanzilli. Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers. *Physical Review Applied*, 20(4):044006, 2023.

Ren08. Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

Wat06. John Watrous. Zero-knowledge against quantum attacks. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing*, pages 296–305, 2006.

ZMM+24. Mujtaba Zahidy, Mikkel T Mikkelsen, Ronny Müller, Beatrice Da Lio, Martin Krehbiel, Ying Wang, Nikolai Bart, Andreas D Wieck, Arne Ludwig, Michael Galili, et al. Quantum key distribution using deterministic single-photon sources over a field-installed fibre link. *npj Quantum Information*, 10(1):2, 2024.

A Distance bound for a malicious Alice

Since Naor's commitment is computationally hiding, and so is the extractable layer, the security against a malicious Alice will be bound by the preservation of the hiding property, as discussed in Corollary 4.3. This bound is given by the Δ-distance between the key generated by ERE-Commitment and a string of uniformly random bits of length λ_{PQS}.

Theorem A.1 (Distance bound in ERE-Commitment for a malicious receiver). *Consider ERE-Commitment (see Algorithm 3), between an honest sender and a malicious receiver with a computationally hiding and* $(\eta, 2^{-\eta n})$*-relaxed statistically binding EqCommitment as base commitment. Let* $K := g(r, \boldsymbol{x})$ *be the key in* $\{0,1\}^\ell$ *output by Alice, where* $h(r,x) : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^\ell$ *is a universal hash function, and* $\bar{T} \subset [4\lambda_{EX}]$*, the set of commitments that have not been challenged. Moreover,* $m \in \bar{T}$ *is a randomly chosen subset of non-challenged commitments that are input in the hash function. Then, for any sampling error* $\xi, \delta > 0$*, a bit-flip error* $\alpha \geq 0$ *and a proportion* $\vartheta \geq 0$ *of leaked bits:*

$$\begin{aligned} &\Delta(\rho_{KE}, \frac{1}{2^\ell}\mathbb{I} \otimes \rho_E) \leq \\ &\leq \frac{1}{2} \cdot 2^{-\frac{1}{2}[(\frac{1}{2}-\xi)m - 2\vartheta\lambda_{EX} - h_2(\delta+\alpha+\eta)(m-2\vartheta\lambda_{EX}) - \ell - q]} \\ &+ \sqrt{6}\exp(-2\lambda_{EX}\delta^2/100) + 2\exp(-4\xi^2\lambda_{EX}), \end{aligned} \tag{A.1}$$

where E *denotes Bob's quantum state,* q *the length of the syndrome needed for performing the error correction code and* $\mathbb{I} \in \mathcal{B}(\mathbb{C}^{2^\ell})$ *is the identity operator.*

Proof. Since the sampling strategy is the same as the one of the OT layer, the sampling errors will be the same. The main difference is that, for this layer, the set of not challenged commitments $\bar{T} \subset [2\lambda_{EX}]$ is not divided into two different subsets. Therefore, the malicious Bob has less prior information:

$$\begin{aligned} H_{\min}(X|E) &\geq d_H(\boldsymbol{\theta}|_{\bar{T}}, \hat{\boldsymbol{\theta}}|_{\bar{T}}) - h_2(\delta+\alpha+\eta)|\bar{T}| \\ &\geq \left(\frac{1}{2} - \xi - \vartheta\right) 2\lambda_{EX} - h_2\left(\delta+\alpha+\eta\right)) 2\lambda_{EX}(1-\vartheta). \end{aligned} \tag{A.2}$$

As the subset $m \in \bar{T}$ is randomly chosen from the set $\bar{T}$, the sampling error for the bases and the states will be the same ones as for the set $\bar{T}$ for a large enough m. Therefore, its min-entropy will be:

$$H_{\min}(X_m|E) \geq \left(\frac{1}{2} - \xi\right) m - 2\vartheta\lambda_{EX} - h_2\left(\delta+\alpha+\eta\right)\left(m - 2\vartheta\lambda_{EX}\right). \tag{A.3}$$

Given a η-relaxed statistical binding EqCommitment, the probability of being relaxed statistical binding is $1 - negl(k)$ when $\eta = \omega(\log^2(k)/k)$

□