A New Framework for Quantum Oblivious Transfer

Amit Agarwal* James Bartusek† Dakshita Khurana‡ Nishant Kumar §

Abstract

We present a new template for building oblivious transfer from quantum information that we call the "fixed basis" framework. Our framework departs from prior work (eg., Crepeau and Kilian, FOCS '88) by fixing the *correct* choice of measurement basis used by each player, except for some hidden *trap* qubits that are intentionally measured in a conjugate basis. We instantiate this template in the quantum random oracle model (QROM) to obtain simple protocols that implement, with security against malicious adversaries:

- *Non-interactive* random-input bit OT in a model where parties share EPR pairs a priori.
- Two-round random-input bit OT without setup, obtained by showing that the protocol above remains secure even if the (potentially malicious) OT receiver sets up the EPR pairs.
- Three-round chosen-input string OT from BB84 states without entanglement or setup. This improves upon natural variations of the CK88 template that require at least five rounds.

Along the way, we develop technical tools that may be of independent interest. We prove that natural functions like XOR enable *seedless* randomness extraction from certain quantum sources of entropy. We also use idealized (i.e. extractable and equivocal) bit commitments, which we obtain by proving security of simple and efficient constructions in the QROM.

*UIUC. Email: amita2@illinois.edu
†UC Berkeley. Email: bartusek.james@gmail.com
‡UIUC. Email: dakshita@illinois.edu
§UIUC.

In loving memory of Nishant (December 2, 1994 - April 10, 2022),
who led this research and was deeply passionate about cryptography.

Contents

1 Introduction

Stephen Wiesner's celebrated paper [Wie83] that kickstarted the field of quantum cryptography suggested a way to use quantum information in order to achieve *a means for transmitting two messages either but not both of which may be received*. Later, it was shown that this powerful primitive – named oblivious transfer (OT) [Rab05, EGL85] – serves as the foundation for secure computation [GMW87, Kil88], which is a central goal of modern crytography.

Wiesner's original proposal only required uni-directional communication, from the sender to the receiver. However, it was not proven secure, and succesful attacks on the proposal (given the ability for the receiver to perform multi-qubit measurements) where even discussed in the paper. Later, [CK88] suggested a way to use both *interaction* and *bit commitments* (which for example can be instantiated using cryptographic hash functions) to obtain a secure protocol. In this work, we investigate how much interaction is really required to obtain oblivious transfer from quantum information (and hash functions). In particular, we ask

Can a sender non-interactively transmit two bits to a receiver
such that the receiver will be able to recover one but not both of the bits?

We obtain a positive answer to this question *if the sender and receiver share prior entanglement*, and we analyze the (malicious, simulation-based) security of our protocol in the quantum random oracle model (QROM).

Specifically, we consider the EPR setup model, where a sender and receiver each begin with halves of EPR pairs, which are maximally entangled two-qubit states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Such simple entangled states are likely to be a common shared setup in quantum networks (see e.g. [SQ20] and references therein), and have attracted much interest as a quantum analogue of the classical common reference string (CRS) model [Kob03, CVZ20, MY21a, DLS22]. They have already been shown to be useful for many two-party tasks such as quantum communication via teleportation [BBC$^+$93], entanglement-assisted quantum error correction [BDH06], and even cryptographic tasks like key distribution [Eke91] and non-interactive zero-knowledge [CVZ20, MY21a].

Non-interactive Bit OT in the EPR Setup Model. We show that once Alice and Bob share a certain (fixed) number of EPR pairs between them, they can realize a *one-shot*[1] bit OT protocol, *securely* implementing an ideal functionality that takes two *bits* m_0, m_1 from Alice and delivers m_b for a uniformly random $b \leftarrow \{0,1\}$ to Bob. We provide an unconditionally secure protocol in the QROM, and view this as a first step towards protocols that rely on concrete properties of hash functions together with entanglement setup.

Furthermore, our result helps understand the power of entanglement as a cryptographic resource. Indeed, non-interactive oblivious transfer is impossible to achieve classically, under any computational assumption, even in the common reference string and/or random oracle model. Thus, the only viable one-message solution is to assume the parties already start with so-called *OT correlations*, where the sender gets random bits x_0, x_1 from a trusted dealer, and the receier gets x_b for a random bit b. On the other hand, our result shows that OT can be acheived in a one-shot manner just given shared EPR pairs.

[1] We use the terms "one-shot", "one-message", and "non-interactive" interchangably in this work, all referring to a protocol between two parties Alice and Bob that consists only of a single message from Alice to Bob.

We note that an "OT correlations setup" is fundementally different than an EPR pair setup. First of all, OT correlations are *specific to OT*, while, as desribed above, shared EPR pairs are already known to be broadly useful, and have been widely studied independent of OT. Moreover, an OT correlations setup requires *private* (hidden) randomness, while generating EPR pairs is a deterministic process. In particular, any (even semi-honest) dealer that sets up OT correlations can learn the parties' private inputs by observing the resulting transcript of communication, while this is not necesarily true of an EPR setup by monogamy of entanglement. Furthermore, as we describe next, our OT protocol remains secure even if a *potentially malicious receiver* dishonestly sets up the entanglement.

Two-Message Bit OT without Setup. The notion of two-message oblivious transfer has been extensively studied in the classical setting [AIR01, NP01, PVW08, HK12, DGH+20] and is of particular theoretical and practical interest. We show that the above protocol remains secure even if the receiver were the one performing the EPR pair setup (as opposed to a trusted dealer / network administrator). That is, we consider a two-message protocol where the receiver first sets up EPR pairs and sends one half of every pair to the sender, following which the sender sends a message to the receiver as before. We show that this protocol also realizes the same bit OT functionality with random receiver choice bit.

This results in the first two-message maliciously-secure variant of OT, without setup, that does not (necessarily) make use of public-key cryptography. However, we remark that we still only obtain the random receiver input functionality in this setting, and leave a construction of two-message chosen-input string OT without public-key cryptography as an intriguing open problem.

Another Perspective: OT Correlations from Entanglement via 1-out-of-2 Deletion. It is well-known that shared halves of EPR pairs can be used to generate shared randomness by having each player measure their halves of EPR pairs in a common basis. But can they also be used to generate OT correlations, where one of the players (say Alice) outputs a random pair of bits, while the other (say Bob) learns only *one* of these (depending on a hidden choice bit), and cannot guess the other bit?[2]

At first, it may seem like the following basic property of EPR pairs gives a candidate solution that requires *no* communication: if Alice and Bob measure their halves in the same basis (say, both computational, hereafter referred to as the $+$ basis), then they will obtain the same random bit r, while if Alice and Bob measure their halves in conjugate bases (say, Alice in the $+$ basis and Bob in the Hadamard basis, hereafter referred to as the $\times$ basis), then they will obtain random and *independent* bits r_A, r_B. Indeed, if Alice and Bob share two EPR pairs, they could agree that Alice measures both of her halves in either the $+$ basis or the $\times$ basis depending on whether her choice bit is 0 or 1, while Bob always measures his first half in the $+$ basis and his second half in the $\times$ basis. Thus, Bob obtains (r_0, r_1), and, depending on her choice b, Alice obtains r_b, while *deleting* information about r_{1-b} by measuring the corresponding register in a conjugate basis.

Of course, there is nothing preventing Alice from simply measuring her first half in the $+$ basis and her second half in the $\times$ basis, obtaining both r_0, r_1 and rendering this initial candidate completely insecure. However, what if Alice could *prove* to Bob that she indeed measured both qubits in the same basis, *without* revealing to Bob which basis she chose? Then, Bob would be

[2]While this framing of the problem is different from the previous page, the two turn out to be equivalent thanks to OT reversal and reorientation methods [IKNP03].

convinced that one of his bits is independent of Alice's view, while the privacy of Alice's choice b would remain intact. We rely on the Random Oracle to implement a cut-and-choose based proof that helps us obtain secure bit OT.

We emphasize that this problem is also interesting in the plain model under computational assumptions. We leave this as an open problem for future work, and discuss it (together with other open problems arising from this work) in Section 1.1.

Other Technical Contributions. We make additional technical contributions along the way, that may be of independent interest.

- **Seedless Extraction from Quantum Sources of Entropy.** Randomness extraction has been a crucial component in all quantum OT protocols, and *seeded* randomness extraction from the quantum sources of entropy that arise in such protocols has been extensively studied (see e.g. [RK05, BF10]). In our non-interactive and two-message settings, it becomes necessary to extract entropy without relying on the existence of a random seed. As such, we prove the security of *seedless* randomness extractors in this context, which may be of independent interest. In particular, we show that either the XOR function or a random oracle (for better rate) can be used in place of the seeded universal hashing used in prior works. The XOR extractor has been used in subsequent work [BK22] as a crucial tool in building cryptosystems with certified deletion.

- **Extractable and Equivocal Commitments in the QROM.** We abstract out a notion of (non-interactive) extractable and equivocal bit commitments in the quantum random oracle model, that we make use of in our OT protocols. We provide a simple construction based on prior work [AHU19, Zha19, DFMS21].

- **Three-Message String OT without Entanglement or Setup.** We show that our fixed basis framework makes it possible to eliminate the need for both entanglement and setup with just three messages. The resulting protocol realizes string OT with no entanglement, and only requires one quantum message containing BB84 states followed by two classical messages. Furthermore, it allows both the sender and the receiver to *choose* their inputs to the OT (as opposed to sampling a random input to one of the parties).

  On the other hand, we find that using prior templates [CK88] necessitates a multi-stage protocol where players have to first exchange basis information in order to establish two channels, resulting in protocols that require at least an extra round of interaction.

- **Concrete Parameter Estimates.** We also estimate the number of EPR pairs/BB84 states required for each of our protocols, and derive concrete security losses incurred by our protocols. This is discussed in Section 2.6, where we also provide a table of our estimates. We expect that future work will be able to further study and optimize the concrete efficiency of quantum OT in the QROM, and our work provides a useful starting point.

1.1 Open problems and directions for future research.

Our new frameworks for oblivious transfer raise several fundamental questions of both theoretical and practical interest.

Strengthening Functionality. It would be interesting to obtain non-interactive or two-message variants of non-trivial quantum OT realizing stronger functionality than we obtain in this work[3]. Our work leaves open the following natural questions.

- Does there exist two-message non-trivial quantum *chosen-input* bit OT, that allows both parties to choose inputs?
- Does there exist one- or two-message non-trivial quantum chosen-sender-input *string* OT, with chosen sender strings and random receiver choice bit? Such a string OT may be sufficient to construct non-interactive secure computation (NISC) [IKO+11] with chosen sender input and random receiver input.
- Does there exist two-message non-trivial quantum OT without entanglement?
- Can our quantum OT protocols serve as building blocks for other non-interactive functionalities, eg., by relying on techniques in [GIK+15] for one-way secure computation, or [BV17] for obfuscation?

Strengthening Security. While analyses in this work are restricted to the QROM, our frameworks are of conceptual interest even beyond this specific model. In particular, one could ask the following question.

- Does there exist non-interactive OT with shared EPR pair setup from *any concrete computational hardness assumption*?

One possible direction towards acheiving this would be to instantiate our template with post-quantum extractable and equivocal commitments in the CRS model, and then attempt to instantiate the Fiat-Shamir paradigm in this setting based on a concrete hash function (e.g. [CGH04, KRR17, CCH+19] and numerous followups). Going further, one could even try to instantiate our templates from weak computational hardness including one-way functions (or even pseudorandom states). We imagine that such an OT would find useful applications even beyond MPC, given how two-message classical OT [AIR01, NP01] has been shown to imply a variety of useful protocols including two-message proof systems, non-malleable commitments, and beyond [OPP14, BGI+17, JKKR17, KS17, BGJ+17, KKS18, BGJ+18].

Finally, we note that any cryptographic protocol in a broader context typically requires the protocol to satisfy strong composability properties. It would be useful to develop a formal model for UC security with a (global) quantum random oracle, and prove UC security for our OT protocols in this model. Another question is whether one can achieve composably (UC) secure protocols with minimal interaction by building on our frameworks in the CRS model.

Practical Considerations. Our concrete quantum resource requirements and security bounds are computed assuming no transmission errors. On the other hand, actual quantum systems, even those that do not rely on entanglement, are often prone to errors. One approach to reconcile these differences is to employ techniques to first improve fidelity, eg. of our EPR pair setup via entanglement purification; and then execute our protocol on the resulting states. Another natural

[3]Here *non-trivial* quantum OT refers to OT that is based on assumptions (such as symmetric-key cryptography) or ideal models that are not known to imply classical OT.

approach (following eg., [BBCS92]) could involve directly building error-resilient versions of our protocols that tolerate low fidelity and/or coherence. Another question is whether our games can be improved to reduce resource consumption and security loss, both in the idealized/error-free and error-prone models.

1.2 Related Work

Wiesner [Wie83] suggested the first template for quantum OT, but his work did not contain a security proof (and even discussed some potential attacks). Crepeau and Kilian [CK88] made progress by demonstrating an approach for basing oblivious transfer on properties of quantum information *plus* a secure "bit commitment" scheme. This led to interest in building bit commitment from quantum information. Unfortunately, it was eventually shown by Mayers, Lo, and Chau [May97, LC97] that bit commitment (and thus oblivious transfer) is *impossible* to build by relying solely on the properties of quantum information.

This is indeed a strong negative result, and rules out the possibility of basing secure computation on quantum information alone. However, it was still apparent to researchers that quantum information must offer *some* advantage in building secure computation systems. One could interpret the Mayers, Lo, Chau impossibility result as indicating that in order to hone in and understand this advantage, it will be necessary to make additional physical, computational, or modeling assumptions beyond the correctness of quantum mechanics. Indeed, much research has been performed in order to tease out the answer to this question, with three lines of work being particularly prominent and relevant to this work[4].

- **Quantum OT from bit commitment.** Although unconditionally-secure bit commitment cannot be constructed using quantum information, [CK88]'s protocol is still meaningful and points to a fundamental difference between the quantum and classical setting, where bit commitment is not known to imply OT. A long line of work has been devoted to understanding the security of [CK88]'s proposal: e.g. [BBCS92, MS94, Yao95, DFL$^+$09, Unr10, BF10].

- **Quantum OT in the bounded storage model.** One can also impose physical assumptions in order to recover quantum OT with unconditional security. [DFSS08] introduced the *quantum bounded-storage model*, and [WST08] introduced the more general *quantum noisy-storage model*, and showed how to construct unconditionally-secure quantum OT in these idealized models. There has also been much followup work focused on implementation and efficiency [WCSL10, ENG$^+$14, IKS$^+$17, FGS$^+$18].

- **Quantum OT from "minicrypt" assumptions.** While [CK88]'s proposal for obtaining OT from bit commitment scheme suggests that public-key cryptography is not required for building OT in a quantum world, a recent line of work has been interested in identifying the *weakest* concrete assumptions required for quantum OT, with [BCKM21, GLSV21] showing that the existence of one-way functions suffices and [MY21b, AQY21] showing that the existence of pseudo-random quantum states suffices.

Our work initiates the explicit study of quantum oblivious transfer in the *quantum random oracle model*, a natural model in which to study *unconditionally-secure* quantum oblivious transfer.

[4] Another line of work studies (unconditional) oblivious transfer with *imperfect* security [CKS13, CGS16, KST20], which we view as largely orthogonal to our work.

Any protocol proven secure in the idealized random oracle model immediately gives rise to a natural "real-world" protocol where the oracle is replaced by a cryptographic hash function, such as SHA-256. As long as there continue to exist candidate hash functions with good security against quantum attackers, our protocols remain useful and relevant. On the other hand, the bounded storage model assumes an upper bound on the adversary's quantum storage while noisy storage model assumes that any qubit placed in quantum memory undergoes a certain amount of noise. The quantum communication complexity of these protocols increases with the bounds on storage/noise. It is clear that advances in quantum storage and computing technology will steadily degrade the security and increase the cost of such protocols, whereas protocols in the QROM do not suffer from these drawbacks.

2 Technical overview

Notation. We will consider the following types of OT protocols.

- $\mathcal{F}_{\mathsf{OT}[k]}$: the *chosen-input string* OT functionality takes as input a bit b from the receiver and two strings $m_0, m_1 \in \{0,1\}^k$ from the sender. It delivers m_b to the receiver.
- $\mathcal{F}_{\mathsf{R-ROT}[1]}$: the *random-receiver-input bit* OT functionality takes as input $\top$ from the receiver and two bits $m_0, m_1 \in \{0,1\}$ from the sender. It samples $b \leftarrow \{0,1\}$ and delivers (b, m_b) to the receiver.
- $\mathcal{F}_{\mathsf{S-ROT}[k]}$: the *random-sender-input string* OT functionality takes as input $\top$ from the sender and (b, m) from the receiver for $b \in \{0,1\}, m \in \{0,1\}^k$. It set $m_b = m$, samples $m_{1-b} \leftarrow \{0,1\}^k$ and delivers (m_0, m_1) to the sender.

2.1 Non-Interactive OT in the shared EPR pair model

As discussed in the introduction, there is a skeleton candidate OT protocol that requires no communication in the shared EPR model that we describe in Figure 1.

- **Setup**: 2 EPR pairs on registers $(\mathcal{A}_0, \mathcal{B}_0)$ and $(\mathcal{A}_1, \mathcal{B}_1)$, where Alice has registers $(\mathcal{A}_0, \mathcal{A}_1)$ and Bob has registers $(\mathcal{B}_0, \mathcal{B}_1)$.
- **Alice's output**: Input $b \in \{0,1\}$.
  1. If $b = 0$, measure both of $\mathcal{A}_0, \mathcal{A}_1$ in basis $+$ to obtain r'_0, r'_1. Output r'_0
  2. If $b = 1$, measure both of $\mathcal{A}_0, \mathcal{A}_1$ in basis $\times$ to obtain r'_0, r'_1. Output r'_1.
- **Bob's output**: Measure $\mathcal{B}_0$ in basis $+$ to obtain r_0 and $\mathcal{B}_1$ in basis $\times$ to obtain r_1. Output (r_0, r_1).

Figure 1: An (insecure) skeleton OT candidate.

The next step is for Alice to prove that she measured both her qubits in the same basis, without revealing what basis she chose. While it is unclear how Alice could directly prove this, we could hope to rely on the cut-and-choose paradigm to check that she measured "most" out of a *set* of pairs of qubits in the same basis. Indeed, a cut-and-choose strategy implementing a type of "measurement check" protocol has appeared in the original quantum OT proposal of [CK88] and many followups. Inspired by these works, we develop such a strategy for our protocol as follows.

Non-interactive Measurement Check. To achieve security, we first modify the protocol so that Alice and Bob use $2n$ EPR pairs, where Alice has one half of every pair and Bob has the other half.

Alice samples a set of n bases $\theta_1, \ldots, \theta_n \leftarrow \{+, \times\}^n$. For each $i \in [n]$, she must measure the i^{th} pair of qubits (each qubit corresponding to a half of an EPR pair) in basis θ_i, obtaining measurement outcomes $(r_{i,0}, r_{i,1})$. Then, she must commit to her bases and outcomes $\mathsf{com}(\theta_1, r_{1,0}, r_{1,1}), \ldots, \mathsf{com}(\theta_n, r_{n,0}, r_{n,1})$. Once committed, she must *open* commitments corresponding to a randomly chosen (by Bob) $T \subset [n]$ of size k, revealing $\{\theta_i, r_{i,0}, r_{i,1}\}_{i \in T}$. Given these openings, for every $i \in T$, Bob will measure his halves of EPR pairs in bases (θ_i, θ_i) to obtain $(r'_{i,0}, r'_{i,1})$. Bob aborts if his outcomes $(r'_{i,0}, r'_{i,1})$ do not match Alice's claimed outcomes $(r_{i,0}, r_{i,1})$ for any $i \in T$. If outcomes on all $i \in T$ match, we will say that Bob accepts the measurement check.

Now, suppose Alice passes Bob's check with noticeable probability. Because she did not know the check subset T at the time of committing to her measurement outcomes, we can conjecture that for "most" $i \in [n] \setminus T$, Alice also correctly committed to results of measuring her qubits in bases (θ_i, θ_i). Moreover we can conjecture that the act of committing and passing Bob's check removed from Alice's view information about at least one out of $(r_{i,0}, r_{i,1})$ for most $i \in [n] \setminus T$. We build on techniques for analyzing quantum "cut-and-choose" protocols [DFL+09, BF10] to prove that this is the case.

In fact, we obtain a *non-interactive* instantiation of such a measurement-check by leveraging the random oracle to perform the Fiat-Shamir transform. That is, Alice applies a hash function, modeled as a random oracle, to her set of commitments in order to derive the "check set" T of size k. Then, she can compute openings to the commitments in the set T, and finally send all of her n commitments together with k openings in a single message to Bob. Finally, the unopened positions will be used to derive two strings (t_0, t_1) of $n - k$ bits each, with the guarantee that – as long as Alice passes Bob's check – there exists b such that Alice only has partial information about the string t_{1-b}. We point out that to realize OT, it is not enough for Alice to only have partial information about t_{1-b}, we must in fact ensure that she obtains *no information* about t_{1-b}. We achieve this by developing techniques for *seedless randomness extraction* in this setting, which we discuss later in this overview. The resulting protocol is described in Fig. 2.[5]

To prove security, we build on several recently developed quantum random oracle techniques [Zha19, DFMS19, DFMS21] as well as techniques for analyzing "quantum cut-and-choose" protocols [DFL+09, BF10]. In particular, we require the random oracle based commitments to be *extractable*, and then argue that Bob's state on registers $\{\mathcal{B}_{i,0}, \mathcal{B}_{i,1}\}_{i \in \overline{T}}$ is in some sense close to the state $|\psi\rangle$ described by the information $\{\theta_i, r_{i,0}, r_{i,1}\}_{i \in \overline{T}}$ in Alice's unopened commitments. To do so, we use the Fiat-Shamir result of [DFMS19, DFMS21] and the quantum sampling formalism of [BF10] to bound the trace distance between Bob's state and a state that is in a "small" superposition of vectors close to $|\psi\rangle$.

[5] Our actual protocol involves an additional step that allows Alice to program any input m_b of her choice, but we suppress this detail in this overview.

- **Setup**: Random oracle RO and $2n$ EPR pairs on registers $\{\mathcal{A}_{i,b}, \mathcal{B}_{i,b}\}_{i\in[n],b\in\{0,1\}}$, where Alice has register $\mathcal{A} \coloneqq \{\mathcal{A}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ and Bob has register $\mathcal{B} \coloneqq \{\mathcal{B}_{i,b}\}_{i\in[n],b\in\{0,1\}}$.
- **Alice's message**: Input $b \in \{0,1\}$.
  1. Sample $\theta_1, \ldots, \theta_n \leftarrow \{+,\times\}^n$ and measure each $\mathcal{A}_{i,0}, \mathcal{A}_{i,1}$ in basis θ_i to obtain $r_{i,0}, r_{i,1}$.
  2. Compute commitments $\mathsf{com}_1, \ldots, \mathsf{com}_n$ to $(\theta_1, r_{1,0}, r_{1,1}), \ldots, (\theta_n, r_{n,0}, r_{n,1})$.
  3. Compute $T = \mathsf{RO}(\mathsf{com}_1, \ldots, \mathsf{com}_n)$, where T is parsed as a subset of $[n]$ of size k.
  4. Compute openings $\{u_i\}_{i\in T}$ for $\{\mathsf{com}_i\}_{i\in T}$.
  5. Let $\overline{T} = [n] \setminus T$, and for all $i \in \overline{T}$, set $d_i = b \oplus \theta_i$ (interpreting $+$ as 0 and $\times$ as 1).
  6. Send $\{\mathsf{com}_i\}_{i\in[n]}, T, \{r_{i,0}, r_{i,1}, \theta_i, u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$ to Bob.
- **Alice's output**: $m_b \coloneqq \mathsf{Extract}(t_b \coloneqq \{r_{i,\theta_i}\}_{i\in\overline{T}})$.
- **Bob's computation**:
  1. Abort if $T \neq \mathsf{RO}(\mathsf{com}_1, \ldots, \mathsf{com}_n)$ or if verifying any commitment in the set T fails.
  2. For each $i \in T$, measure registers $\mathcal{B}_{i,0}, \mathcal{B}_{i,1}$ in basis θ_i to obtain $r'_{i,0}, r'_{i,1}$, and abort if $r_{i,0} \neq r'_{i,0}$ or $r_{i,1} \neq r'_{i,1}$.
  3. For each $i \in \overline{T}$, measure register $\mathcal{B}_{i,0}$ in the $+$ basis and register $\mathcal{B}_{i,1}$ in the $\times$ basis to obtain $r'_{i,0}, r'_{i,1}$.
- **Bob's output**: $m_0 \coloneqq \mathsf{Extract}(t_0 \coloneqq \{r_{i,d_i}\}_{i\in\overline{T}}), m_1 \coloneqq \mathsf{Extract}(t_1 \coloneqq \{r_{i,d_i\oplus 1}\}_{i\in\overline{T}})$.

Figure 2: Non-interactive OT in the shared EPR pair model. $\mathsf{Extract}$ is an (unspecified) seedless hash function used for randomness extraction.

New Techniques for Randomness Extraction. We also note that the arguments above have not yet established a fully secure OT correlation. In particular, Alice might have *some* information about t_{1-b}, whereas OT security would require one of Bob's strings to be completely uniform and independent of Alice's view.

This situation also arises in prior work on quantum OT, and is usually solved via *seeded randomness extraction*. Using this approach, a seed s would be sampled by Bob, and the final OT strings would be defined as $m_0 = \mathsf{Extract}(s, t_0)$ and $m_1 = \mathsf{Extract}(s, t_1)$, where $\mathsf{Extract}$ is a universal hash function. Indeed, quantum privacy amplication [RK05] states that even given s, $\mathsf{Extract}(s, t_{1-b})$ is uniformly random from Alice's perspective as long as t_{1-b} has sufficient (quantum) min-entropy conditioned on Alice's state.

Unfortunately, this approach would require Bob to transmit the seed s to Alice in order for Alice to obtain her output $m_b = \mathsf{Extract}(s, t_b)$, making the protocol no longer non-interactive. Instead, we develop techniques for *seedless* randomness extraction that work in our setting, allowing us to make the full description of the hash function used to derive the final OT strings *public* at the

beginning of the protocol.

We provide two instantiations of seedless randomness extraction that work in a setting where the entropy source comes from measuring a state supported on a small superposition of basis vectors in the conjugate basis. More concretely, given a state on two registers $\mathcal{A}, \mathcal{B}$, where the state on $\mathcal{B}$ is supported on standard basis vectors with small Hamming weight, consider measuring $\mathcal{B}$ in the Hadamard basis to produce x. For what unseeded hash functions Extract does $\mathsf{Extract}(x)$ look uniformly random, even given the state on register $\mathcal{A}$?

- **XOR extractor.** First, we observe that one can obtain a *single* bit of uniform randomness by XORing all of the bits of x together, as long as the superposition on register $\mathcal{B}$ only contains vectors with relative Hamming weight $< 1/2$. This can be used to obtain a *bit* OT protocol, where the OT messages m_0, m_1 consist of a single bit. In fact, by adjusting the parameters of the quantum cut-and-choose, the XOR extractor could be used bit-by-bit to extract any number of λ bits. However, this setting of parameters would require a number of EPR pairs that grows with λ^3, resulting in a very inefficient protocol.

- **RO extractor.** To obtain a more efficient method of extracting λ bits, we turn to the random oracle model, which has proven to be a useful seedless extractor in the classical setting. Since an adversarial Alice in our protocol has some control over the state on registers $\mathcal{A}, \mathcal{B}$, arguing that $\mathsf{RO}(x)$ looks uniformly random from her perspective requires some notion of *adaptive* re-programming in the QROM. While some adaptive re-programming theorems have been shown before (e.g. [Unr15, GHHM21]), they have all *only considered x sampled from a classical probability distribution*. This is for good reason, since counterexamples in the quantum setting exist, even when x has high min-entropy given the state on register $\mathcal{A}$.[6] In this work, we show that in the special case of x being sampled via measurement in a conjugate basis, one *can* argue that $\mathsf{RO}(x)$ can be replaced with a uniformly random r, without detection by the adversary. Our proof relies on the superposition oracle of [Zha19] and builds on proof techniques in [GHHM21]. We leverage our RO extractor to obtain non-interactive λ-bit string OT with a number of EPR pairs that only grows *linearly* in λ.

Differences from the CK88 template. As mentioned earlier, the original quantum OT proposal [CK88] and its followups also incorporate a commit-challenge-response measurement-check protocol to enforce honest behavior. However, we point out one key difference in our approach that enables us to completely get rid of interaction. In CK88, each party measures their set of qubits[7] using a *uniformly random* set of basis choices. Then, in order to set up the two channels required for OT, they need to exchange their basis choices with each other (after the measurement check commitments have been prepared and sent). This requires multiple rounds of interaction. In our setting, it is crucial that one of the parties measures (or prepares) qubits in a *fixed* set of bases known to the other party, removing the need for a two-way exchange of basis information. In the case of Fig. 2, this party is Bob. Hereafter, we refer to the CK88 template as the *random basis framework*, and our template as the *fixed basis framework*.

[6] For example, consider an adversary that, via a single superposition query to the random oracle, sets register $\mathcal{B}$ to be a superposition over all x such that the first bit of $\mathsf{RO}(x)$ is 0. Then, measuring $\mathcal{B}$ in the computational basis will result in an x with high min-entropy, but where $\mathsf{RO}(x)$ is distinguishable from a uniformly random r.

[7] More accurately, since the protocol only uses BB84 states, one party prepares and the other party measures.

Non-interactive OT reversal. So far, our techniques have shown that, given shared EPR pairs, Alice can send a single classical message to Bob that results in the following correlations: Alice outputs a bit b and string m_b, while Bob outputs strings m_0, m_1, thus implementing the $\mathcal{F}_{\mathsf{S-ROT}}$ functionality treating Bob as the "sender".

However, an arguably more natural functionality would treat Alice as the sender, with some chosen inputs m_0, m_1, and Bob as the receiver, who can recover b, m_b from Alice's message. In fact, for the case that m_0, m_1 are single bits, a "reversed" version of the protocol can already be used to acheive this due to the non-interactive OT reversal of [IKNP03]. Let (b, r_b) and (r_0, r_1) be Alice and Bob's output from our protocol, where Alice has chosen b uniformly at random. Then Alice can define $\ell_0 = m_0 \oplus r_b, \ell_1 = m_1 \oplus r_b \oplus b$ and send (ℓ_0, ℓ_1) along with her message to Bob. Bob can then use r_0 to recover m_c from ℓ_c for his "choice bit" $c = r_0 \oplus r_1$. Moreover, since in our protocol the bits r_0, r_1 can be sampled uniformly at random by the functionality, this implies that c is a uniformly random choice bit, unknown to Alice, but unable to be tampered with by Bob. This results in a protocol that satisfies the $\mathcal{F}_{\mathsf{R-ROT}[1]}$ functionality, and we have referred to it as our one-shot bit OT protocol in the introduction.

2.2 Two-message OT without trusted setup

Next, say that we don't want to assume a *trusted* EPR pair setup. In particular, what if we allow Bob to set up the EPR pairs? In this case, a malicious Bob may send any state of his choice to Alice. However, observe that in Fig. 2, Alice's bit b is masked by her random choices of θ_i. These choices remain hidden from Bob due to the hiding of the commitment scheme, plus the fact that they are only used to measure Alice's registers. Regardless of the state that a malicious Bob may send, he will not be able to detect which basis Alice measures her registers in, and thus will not learn any information about b. As a result, we obtain a *two-message* quantum OT protocol in the QROM. As we show in Section 6.2 , this protocol satisfies the $\mathcal{F}_{\mathsf{S-ROT}}$ OT ideal functionality that allows Alice to choose her inputs (b, m), and sends Bob random outputs (m_0, m_1) subject to $m_b = m$.

Moreover, adding another reorientation message at the end from Bob to Alice – where Bob uses m_0, m_1 as keys to encode his chosen inputs – results in a three-round chosen input string OT protocol realizing the $\mathcal{F}_{\mathsf{OT}[k]}$ functionality. However, as we will see in the next section, with three messages, we can *remove the need for entanglement* while still realizing $\mathcal{F}_{\mathsf{OT}[k]}$.

Finally, in the case that m_0, m_1 are bits, we can apply the same non-interactive [IKNP03] reversal described above to the two-round protocol, resulting in a two-round secure realization of the $\mathcal{F}_{\mathsf{R-ROT}[1]}$ ideal functionality. This results in our two-round bit OT protocol as referenced in the introduction.

2.3 Three-message chosen-input OT

We now develop a three-message protocol that realizes the chosen-input string OT functionality $\mathcal{F}_{\mathsf{OT}}$, which takes two strings m_0, m_1 from the sender and a bit b from the receiver, and delivers m_b to the receiver. This protocol will not require entanglement, but still uses the *fixed basis framework*, just like the one discussed in Section 2.1.

Recall that in the EPR-based protocol, Bob would obtain (r_0, r_1) by measuring his halves of two EPR pairs in basis $(+, \times)$, while Alice would obtain (r_0, r_1') or (r_0', r_1) respectively by measuring her halves in basis $(+, +)$ or $(\times, \times)$, where (r_0', r_1') are uniform and independent of (r_0, r_1).

Our first observation is that a similar effect is achieved by having Bob send BB84 states polarized in *a fixed basis* instead of sending EPR pairs. That is, Bob samples uniform (r_0, r_1) and sends to Alice the states $|r_0\rangle_+, |r_1\rangle_\times$. Alice would obtain (r_0, r'_1) or (r'_0, r_1) respectively by measuring these states in basis $(+,+)$ or $(\times,\times)$ respectively, where (r'_0, r'_1) are uniform and independent of (r_0, r_1). The skeleton protocol is sketched in Figure 3.

- **Bob's message and output**:
  1. Sample $(r_0, r_1) \leftarrow \{0,1\}$ and send $|r_0\rangle_+, |r_1\rangle_\times$ in registers $\mathcal{A}_0, \mathcal{A}_1$ to Alice.
  2. Bob's output is (r_0, r_1).
- **Alice's output**: Input $b \in \{0,1\}$.
  1. If $b = 0$, measure both of $\mathcal{A}_0, \mathcal{A}_1$ in basis $+$ to obtain r'_0, r'_1. Output r'_0
  2. If $b = 1$, measure both of $\mathcal{A}_0, \mathcal{A}_1$ in basis $\times$ to obtain r'_0, r'_1. Output r'_1.

Figure 3: Another (insecure) skeleton OT candidate.

As before, though, there is nothing preventing Alice from retrieving both (r_0, r_1) by measuring the states she obtains in basis $(+,\times)$. Thus, as before, we need a *measurement check* to ensure that Alice measures "most" out of a *set* of pairs of qubits in the same basis. But implementing such a check with BB84 states turns out to be more involved than in the EPR pair protocol.

Non-interactive measurement check without entanglement. Towards building a measurement check, we first modify the skeleton protocol so that Bob sends $2n$ BB84 qubits $\{|r_{i,0}\rangle_+, |r_{i,1}\rangle_\times\}_{i\in[n]}$ on registers $\{\mathcal{A}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ to Alice (instead of just two qubits).

Now Alice is required to sample a set of n bases $\theta_1, \ldots, \theta_n \leftarrow \{+,\times\}^n$. For each $i \in [n]$, she must measure the i^{th} pair of qubits in basis θ_i, obtaining measurement outcomes $(r'_{i,0}, r'_{i,1})$. Then, she will commit to her bases and outcomes $\mathsf{com}(\theta_1, r'_{1,0}, r'_{1,1}), \ldots, \mathsf{com}(\theta_n, r'_{n,0}, r'_{n,1})$. Once committed, she will *open* commitments corresponding to a randomly chosen (by Bob) $T \subset [n]$ of size k, revealing $\{\theta_i, r'_{i,0}, r'_{i,1}\}_{i\in T}$.

But Bob cannot check these openings the same way as in the EPR-based protocol. Recall that in the EPR protocol, for every $i \in T$, Bob would measure his halves of EPR pairs in bases (θ_i, θ_i) to obtain $(r_{i,0}, r_{i,1})$, and compare the results against Alice's response. On the other hand, once Bob has sent registers $\{\mathcal{A}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ containing $\{|r_{i,0}\rangle_+, |r_{i,1}\rangle_\times\}_{i\in[n]}$ to Alice, there is no way for him to recover the result of measuring any pair of registers $(\mathcal{A}_{i,0}, \mathcal{A}_{i,1})$ in basis (θ_i, θ_i).

To fix this, we modify the protocol to allow for a (randomly chosen and hidden) set U of "trap" positions. For all $i \in U$, Bob outputs registers $(\mathcal{A}_{i,0}, \mathcal{A}_{i,1})$ containing $|r_{i,0}\rangle_{\vartheta_i}, |r_{i,1}\rangle_{\vartheta_i}$, that is, both qubits are polarized in the same basis $\vartheta_i \leftarrow \{+,\times\}$. All other qubits are sampled the same way as before, i.e. as $|r_{i,0}\rangle_+, |r_{i,1}\rangle_\times$. Alice commits to her measurement outcomes $\{\theta_i, r'_{i,0}, r'_{i,1}\}_{i\in[n]}$, and then reveals commitment openings $\{\theta_i, r'_{i,0}, r'_{i,1}\}_{i\in T}$ for a randomly chosen subset of size T, as before. But Bob can now check Alice on all positions i in the intersection $T \cap U$ where $\vartheta_i = \theta_i$. Specifically, Bob aborts if for any $i \in T \cap U$, $\vartheta_i = \theta_i$ but $(r'_{i,0}, r'_{i,1}) \neq (r_{i,0}, r_{i,1})$. Otherwise, Alice

and Bob will use the set $[n] \setminus T \setminus U$ to generate their OT outputs. The resulting protocol is sketched in Figure 4. Crucially, we make use of a third round in order to allow Bob to transmit his choice of U to Alice, so that they can both agree on the set $[n] \setminus T \setminus U$.

Again, we must argue that any Alice that passes Bob's check with noticeable probability loses information about one out of $r_{i,0}$ and $r_{i,1}$ for "most" $i \in [n] \setminus T \setminus U$. Because she did not know the check subset T or Bob's trap subset U at the time of committing to her measurement outcomes, we can again conjecture that for "most" $i \in [n] \setminus T$, Alice also correctly committed to results of measuring her qubits in bases (θ_i, θ_i). Moreover we can conjecture that the act of committing and passing Bob's check removed from Alice's view information about at least one out of $(r_{i,0}, r_{i,1})$ for most $i \in [n] \setminus T$. This requires carefully formulating and analyzing a quantum sampling strategy that is somewhat more involved than the one in Section 2.1. Furthermore, as in Section 2.1, we make the measurement check non-interactive by relying on the Fiat-Shamir transform. A formal analysis of this protocol can be found in Section 7.

2.4 The random basis framework

Next, we shift our attention to analyzing the original template for commitment-based quantum OT, due to [CK88], and studied in many followups including [BBCS92, MS94, Yao95, DFL+09, BF10, Unr10, GLSV21, BCKM21]. In this template, one party (say, Bob) prepares random BB84 states and sends them to Alice, who is then supposed to immediately measure each received state in a random basis. That is, each party samples their own uniformly random sequence of bases $\theta_A = \theta_{A,1}, \ldots, \theta_{A,n}, \theta_B = \theta_{B,1}, \ldots, \theta_{B,n}$ during the protocol, and thus we refer to this template as the "random basis framework". After this initial prepare-and-measure step, Alice then convinces Bob via a cut-and-choose measurement check that she indeed measured her states, thus simulating a type of erasure channel. The rest of the protocol can be viewed as a conversion from the resulting erasure channel to OT.

First, we observe that, given a non-interactive commitment for use in the measurement check, this protocol can naturally be written as a five-message OT between a receiver Alice and a sender Bob as follows.

1. Bob samples and sends random BB84 states to Alice, where θ_B are the bases and r_B are the bits encoded.

2. Alice measures the received states in bases θ_A, commits to θ_A and the measurement results, and sends the commitments to Bob.

3. Bob samples a random subset T of the commitments to ask Alice to open, and sends T and θ_B to Alice.

4. Alice computes openings to the commitments in T, and then encodes her choice bit b as follows: set $S_b = \{i \in \overline{T} : \theta_{A,i} = \theta_{B,i}\}$ and set $S_{1-b} = \{i \in \overline{T} : \theta_{A,i} \neq \theta_{B,i}\}$. She sends her openings and (S_0, S_1) to Bob.

5. Bob checks that the commitment openings verify and that Alice was honestly measuring her qubits in T. If so, Bob encrypts m_0 using $\{r_{B,i}\}_{i \in S_0}$, encrypts m_1 using $\{r_{B,i}\}_{i \in S_1}$, and sends the two encryptions to Alice.

- **Inputs:** Bob has inputs m_0, m_1 each in $\{0,1\}^\lambda$, Alice has input $b \in \{0,1\}$.
- **Bob's Message**:
  1. Sample a "large enough" subset $U \subset [n]$, and for every $i \in U$, sample $\vartheta_i \leftarrow \{+, \times\}$.
  2. For every $i \in [n]$, sample $(r_{i,0}, r_{i,1}) \leftarrow \{0,1\}$.
  3. For $i \in U$, set registers $(\mathcal{A}_{i,0}, \mathcal{A}_{i,1})$ to $(|r_{i,0}\rangle_{\vartheta_i}, |r_{i,1}\rangle_{\vartheta_i})$.
  4. For $i \in [n] \setminus U$, set registers $(\mathcal{A}_{i,0}, \mathcal{A}_{i,1})$ to $(|r_{i,0}\rangle_{+}, |r_{i,0}\rangle_{\times})$.
  5. Send $\{\mathcal{A}_{i,0}, \mathcal{A}_{i,1}\}_{i\in[n]}$ to Alice.
- **Alice's message**:
  1. Sample $\theta_1, \ldots, \theta_n \leftarrow \{+, \times\}^n$ and measure each $\mathcal{A}_{i,0}, \mathcal{A}_{i,1}$ in basis θ_i to obtain $r'_{i,0}, r'_{i,1}$.
  2. Compute commitments $\mathsf{com}_1, \ldots, \mathsf{com}_n$ to $(\theta_1, r'_{1,0}, r'_{1,1}), \ldots, (\theta_n, r'_{n,0}, r'_{n,1})$.
  3. Compute $T = \mathsf{RO}(\mathsf{com}_1, \ldots, \mathsf{com}_n)$, where T is parsed as a subset of $[n]$ of size k.
  4. Compute openings $\{u_i\}_{i\in T}$ for $\{\mathsf{com}_i\}_{i\in T}$.
  5. Let $\overline{T} = [n] \setminus T$, and for all $i \in \overline{T}$, set $d_i = b \oplus \theta_i$ (interpreting $+$ as 0 and $\times$ as 1).
  6. Send $\{\mathsf{com}_i\}_{i\in[n]}, T, \{r'_{i,0}, r'_{i,1}, \theta_i, u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$ to Bob.
- **Bob's Message**:
  1. Abort if $T \neq \mathsf{RO}(\mathsf{com}_1, \ldots, \mathsf{com}_n)$ or if verifying any commitment in the set T fails.
  2. If for any $i \in T \cap U$, $r_{i,0} \neq r'_{i,0}$ or $r_{i,1} \neq r'_{i,1}$, abort.
  3. Set $x_0 = m_0 \oplus \mathsf{Extract}(t_0 \coloneqq \{r_{i,d_i}\}_{i\in[n]\setminus T\setminus U})$ and $x_1 = m_1 \oplus \mathsf{Extract}(t_1 \coloneqq \{r_{i,d_i\oplus 1}\}_{i\in[n]\setminus T\setminus U})$.
  4. Send (x_0, x_1, U) to Alice.
- **Alice's output**: $m_b \coloneqq x_b \oplus \mathsf{Extract}(t_b \coloneqq \{r'_{i,\theta_i}\}_{i\in\overline{T}})$.

Figure 4: Three-message chosen-input OT without entanglement. Extract is an (unspecified) function used for randomness extraction. Since Bob is sending the final message, we may use a seeded function here.

Now, a natural question is whether we can reduce interaction in the QROM via a non-interactive measurment check, as accomplished above in the fixed basis framework. Unfortunately, the structure of the random basis framework appears to prevent this optimiziation. Indeed, Alice cannot encode her choice bit until *after* she receives θ_B from Bob, which he cannot send until after he receives Alice's commitments.

However, while these reasons prevent us from obtaining a one or two message protocol as in the fixed basis framework, we do show a different optimiziation that allows us to obtain a four-

message chosen-input OT and a three-message random-input OT utilizing this framework, which we discuss next.

Reverse Crepeau-Kilian OT. Suppose instead that *Alice* sends random BB84 states $\{|r_{A,i}\rangle_{\theta_{A,i}}\}_{i\in[n]}$, after which Bob measures these states in random bases θ_B to obtain $\{r_{B,i}\}_{i\in[n]}$. Now, instead of waiting to obtain the "correct" bases θ_A, Bob simply sends θ_B to Alice. When $\theta_{A,i}$ and $\theta_{B,i}$ match, $r_{A,i} = r_{B,i}$, and when $\theta_{A,i}$ and $\theta_{B,i}$ do not match, then $r_{A,i}$ and $r_{B,i}$ should be uncorrelated: again establishing an erasure channel on which Bob can send Alice messages. However, unlike CK88, the player that is performing measurements in random bases *need not wait to learn the right bases*, and instead simply announces his own bases to set up a reverse erasure channel.

However, this protocol leads to new avenues of attack for a malicious Alice. In particular, Alice may send halves of EPR pairs in the first round, and, given θ_B, perform measurements to determine all the $r_{B,i}$ values. Such an attack can be prevented by means of a "reverse" measurement check: namely, Alice *commits to all $r_{A,i}$ and $\theta_{A,i}$ values* in the first message (she commits to the descriptions of her states), and, given a random check set T chosen by Bob, reveals all committed values $\{r_{A,i}, \theta_{A,i}\}_{i\in T}$. Given Alice's openings, for every $i \in [T]$ such that $\theta_{A,i} = \theta_{B,i}$ Bob checks that $r_{A,i} = r_{B,i}$. The resulting four-round chosen-input OT protocol is summarized in Figure 5. We also note that, using our seedless extaction techniques described above, this template can be used to obtain *three-message* protocols for $\mathcal{F}_{\mathsf{S-ROT}}$ and $\mathcal{F}_{\mathsf{R-ROT}}$.

Finally, we note that it is unclear how to apply Fiat-Shamir to this reversed protocol in order to reduce interaction even further. Indeed, in this case it seems the Fiat-Shamir hash function would also have to take as input Alice's *quantum states*, since otherwise she could determine these states after observing the result of the hash.

The ideal commitment model. We observe that the protocols that we obtain in the random basis framework (if we used seeded extraction or the XOR extractor) actually do not use the random oracle beyond its usage in building the commitment scheme. Thus, these protocols could be seen as being constructed in an "ideal commitment model", which is motivated by prior work [DFL+09, GLSV21, BCKM21] that established commitments as the only necessary cryptographic building block for quantum OT. It may be interesting to explore these protocols combined with other (say, plain model or CRS model) instantiations of the required commitments.

2.5 Extractable and Equivocal Commitments

To achieve simulation-based security, our constructions rely on commitments that satisfy *extractability and equivocality*. We model these as classical non-interactive bit commitments that, informally, satisfy the following properties.

- Equivocality: This property ensures that the commitment scheme admits an efficient simulator, let's say $\mathcal{S}_{\mathsf{Equ}}$, that can sample commitment strings that are indistinguishable from commitment strings generated honestly and later, during the opening phase, provide valid openings for either 0 or 1.
- Extractability: This property ensures that the commitment scheme admits an efficient extractor, let's say $\mathcal{S}_{\mathsf{Ext}}$, that, given access to the committer who outputs a commitment string, can output the committed bit.

- **Inputs:** Bob has inputs $m_0, m_1 \in \{0,1\}^\lambda$, Alice has input $b \in \{0,1\}$.
- **Alice's first message:**
  1. For every $i \in [n]$, sample $r_{A,i} \leftarrow \{0,1\}$ and $\theta_{A,i} \leftarrow \{+,\times\}$, and prepare the state $|r_{A,i}\rangle_{\theta_{A,i}}$ on register $\mathcal{A}_i$.
  2. Compute commitments $\mathsf{com}_1, \ldots, \mathsf{com}_n$ to $(\theta_{A,i}, r_{A,i}), \ldots, (\theta_{A,n}, r_{A,n})$.
  3. Send $\{\mathcal{A}_i\}_{i\in[n]}$ and $\{\mathsf{com}_i\}_{i\in[n]}$ to Bob.
- **Bob's first message:**
  1. Sample $\theta_B = \theta_{B,1}, \ldots, \theta_{B,n} \leftarrow \{+,\times\}^n$ and measure each $\mathcal{A}_i$ in basis $\theta_{B,i}$ to obtain $r_{B,i}$.
  2. Sample a "large enough" subset $T \subset [n]$.
  3. Send T and θ_B to Alice.
- **Alice's second message:**
  1. Compute openings $\{u_i\}_{i\in T}$ for $\{\mathsf{com}_i\}_{i\in T}$.
  2. Set $S_b = \{i \in \overline{T} : \theta_{A,i} = \theta_{B,i}\}$ and $S_{1-b} = \{i \in \overline{T} : \theta_{A,i} \neq \theta_{B,i}\}$.
  3. Send $\{u_i\}_{i\in T}, S_0, S_1$ to Bob.
- **Bob's second message:**
  1. Check that the openings to the commitments in T verify, and that for each $i \in T$ such that $\theta_{A,i} = \theta_{B,i}$, it holds that $r_{A,i} = r_{B,i}$.
  2. Set $x_0 = m_0 \oplus \mathsf{Extract}(\{r_{B,i}\}_{i\in S_0})$ and $x_1 = m_1 \oplus \mathsf{Extract}(\{r_{B,i}\}_{i\in S_1})$.
  3. Send (x_0, x_1) to Alice.
- **Alice's output:** $m_b := x_b \oplus \mathsf{Extract}(\{r_{A,i}\}_{i\in S_b})$.

Figure 5: Four-message chosen-input OT from commitments. Extract is an (unspecified) function used for randomness extraction. Since Bob is sending the final message, we may use a seeded function here.

The need for these two additional properties is not new to our work. Indeed, [DFL+09] showed that bit commitment schemes satisfying extraction and equivocation suffice to instantiate the original [CK88, BBCS92] QOT template. [DFL+09] called their commitments dual-mode commitments, and provided a construction based on the quantum hardness of the learning with errors (QLWE) assumption. In two recent works [BCKM21, GLSV21], constructions of such commitment schemes were achieved by relying on just post-quantum one-way functions (in addition to quantum communication).

We show that the most common construction of random-oracle based commitments – where

a commitment to bit b is $H(b||r)$ for uniform r – satisfies both extractability and equivocality in the QROM. Our proof of extractability applies the techniques of [Zha19, DFMS21] for on-the-fly simulation with extraction, and our proof of equivocality relies on a one-way-to-hiding lemma from [AHU19].

2.6 Concrete parameters

Beyond proving the our protocols have negligible security error, we also compute both concrete bounds for the number of quantum resources required by our protocols (as a function of the security parameter), and derive exact security losses incurred by our protocols. This involves careful analyses of the cut-and-choose strategies underlying the measurement-check parts of our protocols. Such strategies were generically analyzed in [BF10], and we strengthen their classical analyses to obtain improved parameters for our quantum sampling games.

We summarize our parameters in Table 1 below, where we discuss the number of EPR pairs/BB84 states required by each of our fixed-basis protocols in the first two columns, and in our optimization of random-basis protocols in the last two columns. We also compute concrete bounds that we obtain when relying on the XOR extractor (to obtain bit OT) versus when relying on the random oracle or seeded extractors (to obtain string OT).

	Fixed Basis Framework		Random Basis Framework	
	1 round $\mathcal{F}_{\mathsf{S-ROT}}$ (EPR pairs)	3 round $\mathcal{F}_{\mathsf{OT}}$ (BB84 states)	3 round $\mathcal{F}_{\mathsf{S-ROT}}$ (BB84 states)	4 round $\mathcal{F}_{\mathsf{OT}}$ (BB84 states)
Bit OT (XOR extractor)	300λ	3200λ	1600λ	1600λ
String OT (RO/seeded extractor)	6420λ (RO)	$84\,200\lambda$ (seeded)	$23\,000\lambda$ (RO)	$10\,300\lambda$ (seeded)

Table 1: A summary of quantum resources required for our protocols. λ denotes the security parameter. All of our protocols have security losses bounded by $\frac{O(q^{3/2}\lambda)}{2^\lambda}$, where q is the number of queries made by the adversary to the random oracle. We refer the reader to the following sections for additional details and concrete bounds: (Section 6.1, Section 6.2) for the fixed basis EPR pair protocols, (Section 7 and Appendix C) for the fixed basis BB84 state protocols, and Appendix B for the random basis protocols.

3 Preliminaries

We use $[n]$ to denote the set $\{1, 2, \ldots n\}$ and $[a, b]$ (where $a < b$) to denote the set $\{a, a+1, \ldots b\}$. We use $\mathcal{HW}(x)$ to denote the Hamming weight of a binary string $x \in \{0,1\}^*$, and $\omega(x)$ to denote its *relative* Hamming weight $\mathcal{HW}(x)/|x|$. For two strings $x, y \in \{0,1\}^*$, we use $\Delta(x, y) = \omega(x \oplus y)$ to denote the relative Hamming distance of x, y. For finite sets X, Y, let $F_{X\to Y}$ be the set of functions with domain X and codomain Y. For a set $T \subseteq [n]$, $\{i\}_{i\in T}$ is used to represent a set indexed by T. Let $h_b(x)$ denote the binary entropy function, $h_b(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. We make use of the well-known fact that the number of strings of length n with relative Hamming weight at most δ is $\leq 2^{h_b(\delta)n}$.

3.1 Quantum preliminaries

A register $\mathcal{X}$ is a named Hilbert space $\mathbb{C}^{2^n}$. A pure quantum state on register $\mathcal{X}$ is a unit vector $|\psi\rangle_{\mathcal{X}} \in \mathbb{C}^{2^n}$, and we say that $|\psi\rangle_{\mathcal{X}}$ consists of n qubits. A mixed state on register $\mathcal{X}$ is described by a density matrix $\rho_{\mathcal{X}} \in \mathbb{C}^{2^n \times 2^n}$, which is a positive semi-definite Hermitian operator with trace 1.

A quantum operation F is a completely-positive trace-preserving (CPTP) map from a register $\mathcal{X}$ to a register $\mathcal{Y}$, which in general may have different dimensions. That is, on input a density matrix $\rho_{\mathcal{X}}$, the operation F produces $F(\rho_{\mathcal{X}}) = \tau_{\mathcal{Y}}$ a mixed state on register $\mathcal{Y}$. A *unitary* $U : \mathcal{X} \to \mathcal{X}$ is a special case of a quantum operation that satisfies $U^\dagger U = UU^\dagger = \mathbb{I}_{\mathcal{X}}$, where $\mathbb{I}_{\mathcal{X}}$ is the identity matrix on register $\mathcal{X}$. A *projector* Π is a Hermitian operator such that $\Pi^2 = \Pi$, and a *projective measurement* is a collection of projectors $\{\Pi_i\}_i$ such that $\sum_i \Pi_i = \mathbb{I}$.

Let Tr denote the trace operator. For registers $\mathcal{X}, \mathcal{Y}$, the *partial trace* $\mathsf{Tr}_{\mathcal{Y}}$ is the unique operation from $\mathcal{X}, \mathcal{Y}$ to $\mathcal{X}$ such that for all $\rho_{\mathcal{X}}, \tau_{\mathcal{Y}}$, $\mathsf{Tr}_{\mathcal{Y}}(\rho, \tau) = \mathsf{Tr}(\tau)\rho$. The *trace distance* between states ρ, τ, denoted $\mathsf{TD}(\rho, \tau)$ is defined as

$$\mathsf{TD}(\rho, \tau) \coloneqq \frac{1}{2}\|\rho - \tau\|_1 \coloneqq \frac{1}{2}\mathsf{Tr}\left(\sqrt{(\rho - \tau)^\dagger(\rho - \tau)}\right).$$

We will often use the fact that the trace distance between two states ρ and τ is an upper bound on the probability that any algorithm can distinguish ρ and τ.

Lemma 3.1 (Gentle measurement [Win99])**.** *Let $\rho_{\mathcal{X}}$ be a quantum state and let $(\Pi, \mathbb{I} - \Pi)$ be a projective measurement on $\mathcal{X}$ such that $\mathrm{Tr}(\Pi\rho) \geq 1 - \delta$. Let*

$$\rho' = \frac{\Pi\rho\Pi}{\mathrm{Tr}(\Pi\rho)}$$

be the state after applying $(\Pi, \mathbb{I} - \Pi)$ to ρ and post-selecting on obtaining the first outcome. Then, $\mathsf{TD}(\rho, \rho') \leq 2\sqrt{\delta}$.

Finally, we will make use of the convention that $+$ denotes the computational basis $\{|0\rangle, |1\rangle\}$ and $\times$ denotes the Hadamard basis $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. For a bit $r \in \{0, 1\}$, we write $|r\rangle_+$ to denote r encoded in the computational basis, and $|r\rangle_\times$ to denote r encoded in the Hadamard basis.

3.2 Quantum machines and protocols

Quantum interactive machines. A quantum interactive machine (QIM) is a family of machines $\{M_\lambda\}_{\lambda\in\mathbb{N}}$, where each M_λ consists of a sequence of quantum operations $M_{\lambda,1}, \ldots, M_{\lambda,\ell(\lambda)}$, where $\ell(\lambda)$ is the number of rounds in which M_λ operates. Usually, we drop the indexing by λ and refer to the machine $M = M_1, \ldots, M_\ell$. Each machine M_i may have a designated input and output register used to communicate with its environment.

Quantum oracle machines. Let X, Y be finite sets and let $O : X \to Y$ be an arbitrary function. We say that A^O is a q-query *quantum oracle machine* (QOM) if it can be written as $A_{q+1}U_O A_q U_O \ldots U_O A_2 U_O A_1$, where $A_1, \ldots, A_{q+1}$ are arbitrary quantum operations, and $U[O]$ is the unitary defined by

$$U[O] : |x\rangle_{\mathcal{X}} |y\rangle_{\mathcal{Y}} \to |x\rangle_{\mathcal{X}} |y \oplus O(x)\rangle_{\mathcal{Y}},$$

operating on a designated oracle input register $\mathcal{X}$ and oracle output register $\mathcal{Y}$. We say that A is a *quantum interactive oracle machine* (QIOM) if $A = A_1^O, \ldots, A_\ell^O$ is such that each A_i^O is a quantum oracle machine.

Sometimes, it will be convenient to consider *controlled* queries to an oracle O, which would be implemented by a unitary

$$U_c[O] : |b\rangle_{\mathcal{B}} |x\rangle_{\mathcal{X}} |y\rangle_{\mathcal{Y}} \to |b\rangle_{\mathcal{B}} |x\rangle_{\mathcal{X}} |y \oplus b \cdot O(x)\rangle_{\mathcal{Y}} .$$

However, it is easy to see that such a controlled query can be implemented with two standard queries, by introducing an extra register $\mathcal{Z}$, as follows:

$$\begin{aligned} |b\rangle_{\mathcal{B}} |x\rangle_{\mathcal{X}} |y\rangle_{\mathcal{Y}} |0\rangle_{\mathcal{Z}} &\xrightarrow{U[O_0]_{\mathcal{X},\mathcal{Z}}} |b\rangle_{\mathcal{B}} |x\rangle_{\mathcal{X}} |y\rangle_{\mathcal{Y}} |O(x)\rangle_{\mathcal{Z}} \to |b\rangle_{\mathcal{B}} |x\rangle_{\mathcal{X}} |y \oplus b \cdot O(x)\rangle_{\mathcal{Y}} |O(x)\rangle_{\mathcal{Z}} \\ &\xrightarrow{U[O_0]_{\mathcal{X},\mathcal{Z}}} |b\rangle_{\mathcal{B}} |x\rangle_{\mathcal{X}} |y \oplus b \cdot O(x)\rangle_{\mathcal{Y}} |0\rangle_{\mathcal{Z}} . \end{aligned}$$

It will also be convenient to consider algorithms A^{O_0,O_1} with access to *multiple* oracles $O_0 : X_0 \to Y_0, O_1 : X_1 \to Y_1$, written as $A_{q+1}U_{O_1}A_qU_{O_0}\ldots U_{O_1}A_2U_{O_0}A_1$. Defining $O(b,x) = O_b(x)$ for $(b,x) \in (0,X_0) \cup (1,X_1)$, it is easy to see that any A^{O_0,O_1} can be written as an oracle algorithm B^O. On the other hand, given a q-query oracle algorithm A^O where $O : X \to Y$, and a partition of X into $(0,X') \cup (1,X')$, we can write A as a $4q$-query algorithm B^{O_0,O_1}, where $O_b : X' \to Y$ is such that $O_b(x') = O(b,x')$. This follows by answering each query to O using one controlled query to O_0 and one controlled query to O_1. This can be extended to splitting up an oracle O into k oracles, with a multiplicative factor of $2k$ in the number of queries made by the adversary. Thus, throughout this work, we often consider machines that have access to multiple (potentially independently sampled) oracles, while noting that this model is equivalent to considering machines with access to a single oracle, up to a difference in the number of oracle queries. In particular, any adversarial algorithm that has superposition access to a single oracle O with an input space that can be partitioned into k parts may be written as an adversarial algorithm wth access to k appropriately defined separate oracles $O_1, \ldots, O_k$.

Functionalities and protocols in the quantum random oracle model. Let $\mathcal{F}$ denote a *functionality*, which is a classical interactive machine specifying the instructions to realize a cryptographic task. A two-party protocol[8] Π for $\mathcal{F}$ consists of two QIMs (A,B).[9] A protocol Π in the *quantum random oracle model* (QROM) consists of two *QIOMs* (A^H, B^H) that have quantum oracle access to a uniformly random function H sampled from $F_{X\to Y}$ for some finite sets X and Y.

An adversary intending to attack the protocol along with a distinguisher can be described by a family $\{\mathsf{Adv}_\lambda, \mathsf{D}_\lambda, x_\lambda\}_{\lambda\in\mathbb{N}}$, where Adv_λ is a QIOM that corrupts party $M \in \{A,B\}$, D_λ is a QOM, and x_λ is the input of the honest party $P \in \{A,B\}$. Define the one-bit random variable $\Pi[\mathsf{Adv}_\lambda, \mathsf{D}_\lambda, x_\lambda]$ as follows.

- H is sampled uniformly at random.
- Adv_λ^H interacts with $P^H(x_\lambda)$ during the execution of Π, and Adv_λ outputs a quantum state ρ, while P^H outputs a classical string y.

[8] One can also consider multi-party protocols, but we restrict to the two-party setting in this work.

[9] Technically, A and B are infinite families of interactive machines, parameterized by the security parameter λ.

- $\mathsf{D}_\lambda^H(\rho, y)$ outputs a bit b.

An *ideal-world* protocol $\widetilde{\Pi}_{\mathcal{F}}$ for functionality $\mathcal{F}$ consists of two "dummy" parties $\widetilde{A}, \widetilde{B}$ that have access to an additional "trusted" party that implements $\mathcal{F}$. That is, $\widetilde{A}, \widetilde{B}$ each interact directly with $\mathcal{F}$, which eventually returns outputs to $\widetilde{A}, \widetilde{B}$. We consider the execution of ideal-world protocols in the presence of a simulator followed by a distinguisher, described by a family $\{\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, x_\lambda\}_{\lambda\in\mathbb{N}}$. Define the random variable $\widetilde{\Pi}_{\mathcal{F}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, x_\lambda]$ over one bit output a follows.

- Sim_λ interacts with $\widetilde{P}(x_\lambda)$ during the execution of $\widetilde{\Pi}_{\mathcal{F}}$, and Sim_λ outputs a quantum state ρ, while $\widetilde{P}$ outputs a classical string y.
- $\mathsf{D}_\lambda^{\mathsf{Sim}_\lambda}(\rho, y)$ outputs a bit b.

In the above, Sim_λ may be *stateful*, meaning that the part of Sim_λ that interacts with $\widetilde{P}(x)$ may pass an arbitrary state to the part of Sim_λ that answers $\mathsf{D}'_\lambda s$ oracle queries.

Furthermore, we will only consider the notion of security with abort where every ideal functionality is slightly modified to (1) know the identities of corrupted parties and (2) be slightly reactive: after all parties have provided input, the functionality computes outputs and delivers the outputs to the corrupt parties only. Then the functionality awaits either a "deliver" or "abort" command from the corrupted parties. Upon receiving "deliver", the functionality delivers the outputs to all the honest parties. Upon receiving "abort", the functionality delivers an abort output ($\perp$) to all the honest parties.

Definition 3.2 (Securely Realizing Functionalities with Abort)**.** *A protocol Π μ-securely realizes a functionality $\mathcal{F}$ with abort in the quantum random oracle model if there exists a polynomial s such that for any function q and any $\{\mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$, there exists a simulator $\{\mathsf{Sim}_\lambda\}_{\lambda\in\mathbb{N}}$ such that the run-time of Sim_λ is at most the run-time of Adv_λ plus $s(\lambda, q(\lambda))$, and for all $\{\mathsf{D}_\lambda, x_\lambda\}_{\lambda\in\mathbb{N}}$ with the property that the combined number of oracle queries made by Adv_λ and D_λ is at most $q(\lambda)$, it holds that*

$$\left|\Pr[\Pi[\mathsf{Adv}_\lambda, \mathsf{D}_\lambda, x_\lambda] = 1] - \Pr\left[\widetilde{\Pi}_{\mathcal{F}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, x_\lambda] = 1\right]\right| = \mu(\lambda, q(\lambda)).$$

Furthermore, we say that a protocol Π securely realizes *a functionality $\mathcal{F}$ if it μ-securely realizes $\mathcal{F}$ where μ is such that for any $q(\lambda) = \mathrm{poly}(\lambda)$, $\mu(\lambda, q(\lambda)) = \mathrm{negl}(\lambda)$.*

3.3 Oblivious transfer functionalities

We will consider various oblivious transfer functionalities in this work. Some of these will be used as stepping stones towards other constructions.

- $\mathcal{F}_{\mathsf{OT}[k]}$: the *chosen-input string* OT functionality takes as input a bit b from the receiver and two strings $m_0, m_1 \in \{0,1\}^k$ from the sender. It delivers m_b to the receiver.
- $\mathcal{F}_{\mathsf{R-ROT}[1]}$: the *random-receiver-input bit* OT functionality takes as input $\top$ from the receiver and two bits $m_0, m_1 \in \{0,1\}$ from the sender. It samples $b \leftarrow \{0,1\}$ and delivers (b, m_b) to the receiver.

- $\mathcal{F}_{\mathsf{S-ROT}[k]}$: the *random-sender-input (string)* OT functionality takes as input $\top$ from the sender and (b, m) from the receiver for $b \in \{0,1\}, m \in \{0,1\}^k$. It set $m_b = m$, samples $m_{1-b} \leftarrow \{0,1\}^k$ and delivers (m_0, m_1) to the sender.

We will often refer to the following bit OT reversal theorem.

Imported Theorem 3.3 ([IKNP03]). *Any protocol that securely realizes the functionality $\mathcal{F}_{\mathsf{S-ROT}[1]}$ can be converted into a protocol that securely realizes the functionality $\mathcal{F}_{\mathsf{R-ROT}[1]}$, without adding any messages.*

For concreteness, we specify how the OT reversal works. Suppose that Alice and Bob have access to an ideal OT functionality $\mathcal{F}_{\mathsf{S-ROT}[1]}$ where Alice is the receiver and Bob is the sender. Their goal is to realize $\mathcal{F}_{\mathsf{R-ROT}[1]}$ with roles reversed, i.e. with Alice as sender and Bob as receiver. This is achieved as follows.

- Alice has input $m_0, m_1 \in \{0,1\}$, and samples $c \leftarrow \{0,1\}, r \leftarrow \{0,1\}$.
- Alice and Bob run the protocol for $\mathcal{F}_{\mathsf{S-ROT}[1]}$ where Alice inputs (c, r) as receiver to $\mathcal{F}_{\mathsf{S-ROT}[1]}$, and Alice sends
$$\ell_0 \coloneqq m_0 \oplus r, \ell_1 \coloneqq m_1 \oplus r \oplus c$$
along with her OT message to Bob.
- Bob obtains output (r_0, r_1) from the protocol for $\mathcal{F}_{\mathsf{S-ROT}[1]}$. Then, he sets
$$b \coloneqq r_0 \oplus r_1, m_b \coloneqq \ell_b \oplus r_0,$$
and outputs (b, m_b).

3.4 Quantum oracle results

We state here some results on quantum oracle machine from prior literature, which we use in our proofs.

Imported Theorem 3.4 (One-way to hiding [AHU19]). *Let X, Y be finite non-empty sets and let $(S, O_1, O_2, |\psi\rangle)$ be sampled from an arbitrary distribution such that $S \subseteq X$, $O_1, O_2 : X \to Y$ are such that $\forall x \notin S, O_1(x) = O_2(x)$, and $|\psi\rangle$ is a quantum state on an arbitrary number of qubits. Let $A^O(|\psi\rangle)$ be a quantum oracle algorithm that makes at most q queries. Let $B^O(|\psi\rangle)$ be an oracle algorithm that does the following: pick $i \leftarrow [q]$, run $A^O(|\psi\rangle)$ until (just before) the i^{th} query, measure the query input register in the computational basis, and output the measurement outcome x. Let*

- $P_{left} = \Pr\big[A^{O_1}(|\psi\rangle) = 1\big]$,
- $P_{right} = \Pr\big[A^{O_2}(|\psi\rangle) = 1\big]$,
- *and* $P_{guess} = \Pr\big[x \in S : x \leftarrow B^{O_1}(|\psi\rangle)\big]$.

Then it holds that
$$|P_{left} - P_{right}| \leq 2q\sqrt{P_{guess}}.$$

The above theorem is actually a generalization of the theorem stated in [AHU19], in which the input $|\psi\rangle$ is assumed to be a *classical* bit string z. However, the proof given in [AHU19] readily extends to considering quantum input. The proof is split up into [AHU19, Lemma 8] and [AHU19, Lemma 9]. In Lemma 8, (S, O_1, O_2, z) are fixed, and z is used to define A's initial state $|\Psi_0\rangle$. Here, we can just define A's initial state as $|\psi\rangle$. In Lemma 9, an expectation is taken over (S, O_1, O_2, z), and the same expectation can be taken over $(S, O_1, O_2, |\psi\rangle)$.

Imported Theorem 3.5 (Measure-and-reprogram [DFMS19, DFM20]). [10] *Let X, Y be finite non-empty sets, and let $q \in \mathbb{N}$. Let* Adv *be a quantum oracle machine with initial state ρ that makes at most q queries to a uniformly random function $H : X \to Y$ and that outputs an $x \in X$ along with an arbitrary quantum state σ on register $\mathcal{A}$. There exists a quantum interactive machine* Sim[Adv] *such that for any projection*

$$\Pi[y] := \sum_x |x\rangle\langle x| \otimes \Pi_{\mathcal{A}}^{x,y},$$

where each $\Pi^{x,y}$ is an arbitrary projection on register $\mathcal{A}$ that is parameterized by strings $x \in X$ and $y \in Y$, it holds that

$$\begin{aligned}
&\mathop{\mathbb{E}}_H \left[\mathrm{Tr}\left(\Pi[H(x)]\left(|x\rangle\langle x| \otimes \sigma\right)\right) : (x, \sigma) \leftarrow \mathsf{Adv}^H(\rho) \right] \\
&\leq (2q+1)^2 \, \mathbb{E}\left[\mathrm{Tr}\left(\Pi[y]\left(|x\rangle\langle x| \otimes \sigma\right)\right) : \begin{array}{r} (x, \mathsf{st}) \leftarrow \mathsf{Sim}[\mathsf{Adv}](\rho) \\ y \leftarrow Y \\ \sigma \leftarrow \mathsf{Sim}[\mathsf{Adv}](y, \mathsf{st}) \end{array} \right].
\end{aligned}$$

Moreover, Sim[Adv] *runs* Adv *except for the following differences: i) it introduces an intermediate measurement of one of the registers maintained by* Adv *to obtain x, and ii) it simulates responses to* Adv*'s oracle queries to H.*

Finally, we will often make use of an "on-the-fly" method for simulating a quantum random oracle, due to [Zha19]. This method of simulation is *efficient* and does not depend on an a priori upper bound on the number of queries q to be made by the adversary. In fact, as shown by [DFMS21], this simulation method may be augmented with an extraction interface that essentially allows to recovers a pre-image x given an image $y = H(x)$.

Below, we define *independent queries* to an interface to be two consecutive queries that can in principle be performed in either order. More formally, two consecutive queries are independent if they can applied to disjoint registers, meaning that one query may be applied to input and output registers $\mathcal{X}$ and $\mathcal{Y}$, while the other may be applied to disjoint input and output registers $\mathcal{X}'$ and $\mathcal{Y}'$.

Furthermore, we say that two quantum operations E and F *α-almost-commute* if for any input state ρ, $\mathsf{TD}(E(F(\rho)), F(E(\rho)) \leq \alpha$. We say that two quantum operations E and F *commute* if for any input state ρ, $\mathsf{TD}(E(F(\rho)), F(E(\rho)) = 0$.

Imported Theorem 3.6 (On-the-fly simulation with extraction [Zha19, DFMS21]). *Let X be a finite non-empty set and $Y = \{0,1\}^n$. There exists a simulator* $\mathsf{Sim}_{\mathsf{RO}}$ *that consists of an initialization step and an interface* $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ *that maintains an internal state.* $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$*, given registers $\mathcal{X}$ and $\mathcal{Y}$, applies a*

[10] This theorem was stated more generally in [DFMS19, DFM20] to consider the drop in expectation for each specific $x^* \in X$.

quantum operation to these registers and its internal state.[11] *The following properties hold for any oracle algorithm A.*

1. ***Indistinguishable simulation.***

$$\Pr_H[1 \leftarrow A^H] = \Pr\left[1 \leftarrow A^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}\right].$$

2. ***Efficiency.*** *Suppose that A makes q queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$. Then the total runtime of $\mathsf{Sim}_{\mathsf{RO}}$ is $O(q^2)$.*

There also exists an interface $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$ that upon input a classical value $y \in \{0,1\}^n$, outputs a classical value $\hat{x} \in X \cup \{\emptyset\}$. The following properties hold for any oracle algorithm A.

1. ***Correctness of extraction.*** *Suppose that A makes q queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ and no queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$, and outputs $\mathbf{x} \in X^\ell$ and $\mathbf{y} \in Y^\ell$. Then,*

$$\Pr\left[\exists\, i \,:\, (\mathbf{y}_i = \hat{\mathbf{y}}_i) \wedge (\mathbf{x}_i \neq \hat{\mathbf{x}}_i) \,\middle|\, \begin{array}{r} \mathbf{x},\mathbf{y} \leftarrow A^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}} \\ \hat{\mathbf{y}} \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(\mathbf{x}) \\ \hat{\mathbf{x}} \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}(\mathbf{y}) \end{array}\right] \leq \frac{296(q+\ell+1)^3+2}{2^n}.$$

2. ***Almost commutativity of $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ and $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$.*** *Any two independent queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$ and $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ $\frac{8\sqrt{2}}{2^{n/2}}$-almost-commute.*

3. ***Efficiency.*** *Suppose that A makes q_{RO} queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ and q_{E} queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$. Then the total runtime of $\mathsf{Sim}_{\mathsf{RO}}$ is $O(q_{\mathsf{RO}}q_{\mathsf{E}} + q_{\mathsf{RO}}^2)$.*

3.5 Quantum entropy and leftover hashing

Quantum conditional min-entropy. Let $\rho_{\mathcal{X}\mathcal{Y}}$ denote a bipartite quantum state over registers $\mathcal{X},\mathcal{Y}$. Following [Ren08, KRS09], the conditional min-entropy of $\rho_{\mathcal{X}\mathcal{Y}}$ given $\mathcal{Y}$ is then defined to be

$$\mathbf{H}_\infty(\rho_{\mathcal{X}\mathcal{Y}} \mid \mathcal{Y}) := \sup_\tau \max\{h \in \mathbb{R} : 2^{-h} \cdot \mathbb{I}_{\mathcal{X}} \otimes \tau_{\mathcal{Y}} - \rho_{\mathcal{X}\mathcal{Y}} \geq 0\}.$$

In this work, we will exclusively consider the case where the $\rho_{\mathcal{X}\mathcal{Y}}$ is a joint distribution of the form (R,τ) where R is a classical random variable. In other words, $\rho_{\mathcal{X}\mathcal{Y}}$ can be written as

$$\sum_x \Pr[X = x] \left|x\right\rangle \left\langle x\right| \otimes \tau_x.$$

We refer to such $\rho_{\mathcal{X}\mathcal{Y}}$ as a classical-quantum state. In this case, quantum conditional min-entropy exactly corresponds to the maximum probability of guessing x given the state on register $\mathcal{Y}$.

Imported Theorem 3.7 ([KRS09]). *Let $\rho_{\mathcal{X},\mathcal{Y}}$ be a classical-quantum state, and let $p_{\mathsf{guess}}(\rho_{\mathcal{X},\mathcal{Y}}|\mathcal{Y})$ be the maximum probability that any quantum operation can output the x on register $\mathcal{X}$, given the state on register $\mathcal{Y}$. Then*

$$p_{\mathsf{guess}}(\rho_{\mathcal{X},\mathcal{Y}}|\mathcal{Y}) = 2^{-\mathbf{H}_\infty(\rho_{\mathcal{X},\mathcal{Y}}|\mathcal{Y})}.$$

[11] We can also consider applying $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ to a classical input x and producing classical output y, which corresponds to applying the quantum operation on $\left|x\right\rangle_{\mathcal{X}} \left|0\right\rangle_{\mathcal{Y}}$ and measuring the register $\mathcal{Y}$ to produce the output.

Leftover hash lemma with quantum side information. We now state a generalization of the leftover hash lemma to the setting of quantum side information.

Imported Theorem 3.8 ([RK05]). *Let $\mathcal{H}$ be a family of universal hash functions from X to $\{0,1\}^\ell$, i.e. for any $x \neq x'$, $\Pr_{h\leftarrow\mathcal{H}}[h(x) = h(x')] = 2^{-\ell}$. Let $\rho_{\mathcal{X}\mathcal{Y}}$ be any classical-quantum state. Let $\mathcal{R}$ be a register that holds $h \leftarrow \mathcal{H}$, let $\mathcal{K}$ be a register that holds $h(x)$, where x is on register $\mathcal{X}$, and define $\rho_{\mathcal{X}\mathcal{Y}\mathcal{R}\mathcal{K}}$ to be the entire system. Then, it holds that*

$$\left\| \rho_{\mathcal{Y}\mathcal{R}\mathcal{K}} - \rho_{\mathcal{Y}\mathcal{R}} \otimes \frac{1}{2^\ell} \sum_u |u\rangle\langle u| \right\|_1 \leq \frac{1}{2^{1+\frac{1}{2}(\mathbf{H}_\infty(\rho_{\mathcal{X}\mathcal{Y}}|\mathcal{Y})-\ell)}}.$$

Small superposition of terms. We will also make use of the following lemma from [BF10].

Imported Theorem 3.9. *([BF10]) Let $\mathcal{X}, \mathcal{Y}$ be registers of arbitrary size, and let $\{|i\rangle\}_{i\in I}$ and $\{|w\rangle\}_{w\in W}$ be orthonormal bases of $\mathcal{X}$. Let $|\psi\rangle_{\mathcal{X}\mathcal{Y}}$ and $\rho_{\mathcal{X}\mathcal{Y}}$ be of the form*

$$|\psi\rangle = \sum_{i\in J} \alpha_i |i\rangle_{\mathcal{X}} |\psi_i\rangle_{\mathcal{Y}} \text{ and } \rho = \sum_{i\in J} |\alpha_i|^2 |i\rangle\langle i|_{\mathcal{X}} \otimes |\psi_i\rangle\langle\psi_i|_{\mathcal{Y}}$$

for some subset $J \subseteq I$. Furthermore, let $\widehat{\rho}_{\mathcal{X}\mathcal{Y}}$ and $\widehat{\rho}^{\mathsf{mix}}_{\mathcal{X}\mathcal{Y}}$ be the classical-quantum states obtained by measuring register $\mathcal{X}$ of $|\psi\rangle$ and ρ, respectively, in basis $\{|w\rangle\}_{w\in W}$ to observe outcome w. Then,

$$\mathbf{H}_\infty(\widehat{\rho}_{\mathcal{X},\mathcal{Y}}|\mathcal{Y}) \geq \mathbf{H}_\infty(\widehat{\rho}^{\mathsf{mix}}_{\mathcal{X},\mathcal{Y}}|\mathcal{Y}) - \log|J|.$$

3.6 Sampling in a quantum population

In this section, we describe a generic framework presented in [BF10] for analyzing cut-and-choose strategies applied to quantum states.

Classical sampling stratiegies. Let A be a set, and let $\mathbf{q} = (q_1, \ldots, q_n) \in A^n$ be a string of length n. We consider the problem of estimating the relative Hamming weight of a substring $\omega(\mathbf{q}_{\bar{t}})$ by only looking at the substring $\mathbf{q}_t$ of $\mathbf{q}$, for a subset $t \subset [n]$. We consider sampling strategies $\Psi = (P_T, P_S, f)$, where P_T is an (independently sampled) distribution over subsets $t \subseteq [n]$, P_S is a distribution over seeds $s \in S$, and $f : \{(t, \mathbf{v}) : t \subset [n], \mathbf{v} \in A^t\} \times S \to \mathbb{R}$ is a function that takes the subset t, the substring $\mathbf{v}$, and a seed s, and outputs an estimate for the relative Hamming weight of the remaining string. For a fixed subset t, seed s, and a parameter δ, define $B^\delta_{t,s}(\Psi) \subseteq A^n$ as

$$B^\delta_{t,s} := \{\mathbf{b} \in A^n : |\omega(\mathbf{b}_{\bar{t}}) - f(t, \mathbf{b}_t, s)| < \delta\}.$$

Then we define the *classical error probability* of strategy Ψ as follows.

Definition 3.10 (Classical error probability). *The classical error probability of a sampling strategy $\Psi = (P_T, P_S, f)$ is defined as the following value, paraterized by $0 < \delta < 1$:*

$$\epsilon^\delta_{\mathsf{classical}}(\Psi) := \max_{\mathbf{q}\in A^n} \Pr_{t\leftarrow P_T, s\leftarrow P_S} \left[\mathbf{q} \notin B^\delta_{t,s}(\Psi)\right].$$

Quantum sampling strategies. Now, let $A = A_1, \ldots, A_n$ be an n-partite quantum system on registers $\mathcal{A} = \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n$, where each system has dimension d. Let $\{|a\rangle\}_a$ be a fixed orthonormal basis for each $\mathcal{A}_i$. $\mathcal{A}$ may be entangled with another system $\mathcal{E}$, and we write the purified state on $\mathcal{A}$ and $\mathcal{E}$ as $|\psi\rangle_{\mathcal{AE}}$. We consider the problem of testing whether the state on $\mathcal{A}$ is close to the all-zero reference state $|0\rangle_{\mathcal{A}_1} \ldots |0\rangle_{\mathcal{A}_n}$. There is a natural way to apply any sampling strategy $\Psi = (P_T, P_S, f)$ to this setting: sample t, s according to P_T, P_S, measure subsystems $\mathcal{A}_i$ for $i \in [t]$ in basis $\{|a\rangle\}_a$ to observe $\mathbf{q}_t \in A^{|t|}$, and compute an estimate $f(t, \mathbf{q}_t, s)$.

In order to analyze the effect of this strategy, we first consider the mixed state on registers $\mathcal{T}$ (holding the subset t), $\mathcal{S}$ (holding the seed s), and $\mathcal{A}, \mathcal{E}$ that results from sampling t and s according to $P_{TS} = P_T P_S$

$$\rho_{\mathcal{TSAE}} = \sum_{t,s} P_{TS}(t,s) \, |t,s\rangle \langle t,s| \otimes |\psi\rangle \langle \psi| \, .$$

Next, we compare this state to an *ideal* state, parameterized by $0 < \delta < 1$, of the form

$$\widetilde{\rho}_{\mathcal{TSAE}} = \sum_{t,s} P_{TS}(t,s) \, |t,s\rangle \langle t,s| \otimes \left|\widetilde{\psi}^{ts}\right\rangle \left\langle \widetilde{\psi}^{ts}\right| \text{ with } \left|\psi^{ts}\right\rangle \in \mathsf{span}\left(B^{\delta}_{t,s}\right) \otimes \mathcal{E},$$

where

$$\mathsf{span}\left(B^{\delta}_{t,s}\right) \coloneqq \mathsf{span}\left(\{|\mathbf{b}\rangle : \mathbf{b} \in B^{\delta}_{t,s}\}\right) = \mathsf{span}\left(\{|\mathbf{b}\rangle : |\omega(\mathbf{b}_{\bar{t}}) - f(t, \mathbf{b}_t, s)| < \delta\}\right).$$

That is, $\widetilde{\rho}_{\mathcal{TSAE}}$ is a state such that it holds *with certainty* that the state on registers $\mathcal{A}_{\bar{t}}\mathcal{E}$, after having measured $\mathcal{A}_t$ and oberserving $\mathbf{q}_t$, is in a superposition of states with relative Hamming weight δ-close to $f(t, \mathbf{q}_t, s)$. This leads us to the definition of the *quantum error probability* of strategy Ψ.

Definition 3.11 (Quantum error probability)**.** *The quantum error probability of a sampling strategy $\Psi = (P_T, P_S, f)$ is defined as the following value, parameterized by $0 < \delta < 1$:*

$$\epsilon^{\delta}_{\mathsf{quantum}}(\Psi) \coloneqq \max_{\mathcal{E}} \max_{|\psi\rangle_{\mathcal{AE}}} \min_{\widetilde{\rho}_{\mathcal{TSAE}}} \mathsf{TD}\left(\rho_{\mathcal{TSAE}}, \widetilde{\rho}_{\mathcal{TSAE}}\right),$$

where the first max is over all finite-dimensional registers $\mathcal{E}$, the second max is over all state $|\psi\rangle_{\mathcal{AE}}$ and the min is over all ideal state $\widetilde{\rho}_{\mathcal{TSAE}}$ of the form described above.

Finally, we relate the classical and quantum error probabilities.

Imported Theorem 3.12 ([BF10])**.** *For any sampling strategy Ψ and $\delta > 0$,*

$$\epsilon^{\delta}_{\mathsf{quantum}}(\Psi) \leq \sqrt{\epsilon^{\delta}_{\mathsf{classical}}(\Psi)}.$$

4 Seedless extraction from quantum sources

In this section, we consider the problem of seedless randomness extraction from a quantum source of entropy. The source of entropy we are interested in comes from applying a Hadamard basis measurement to a state that is in a "small" superposition of computational basis vectors. More concretely, consider an arbitrarily entangled system on registers $\mathcal{A}, \mathcal{X}$, where $\mathcal{X}$ is in a small superposition of computational basis vectors. Then, we want to specify an extractor E such that, if

x is obtained by measuring register $\mathcal{X}$ in the Hadamard basis, then $E(x)$ looks uniformly random, even given the "side information" on register $\mathcal{A}$. Note that *seeded* randomness extraction in this setting has been well-studied (e.g. [RK05, DFL+09, BF10]).

Proofs of the following two theorems are given in Appendix A.

4.1 The XOR extractor

First, we observe that if E just XORs all the bits of x together, then the resulting bit $E(x)$ is *perfectly* uniform, as long as the original state on $\mathcal{X}$ is only supported on vectors with relative Hamming weight $< 1/2$.

Theorem 4.1. *Let $\mathcal{X}$ be an n-qubit register, and consider any state $|\gamma\rangle_{\mathcal{A},\mathcal{X}}$ that can be written as*

$$|\gamma\rangle = \sum_{u:\mathcal{HW}(u)<n/2} |\psi_u\rangle_{\mathcal{A}} \otimes |u\rangle_{\mathcal{X}} .$$

Let $\rho_{\mathcal{A},\mathcal{P}}$ be the mixed state that results from measuring $\mathcal{X}$ in the Hadamard basis to produce x, and writing $\bigoplus_{i\in[n]} x_i$ into the single qubit register $\mathcal{P}$. Then it holds that

$$\rho_{\mathcal{A},\mathcal{P}} = \mathrm{Tr}_{\mathcal{X}}(|\gamma\rangle\langle\gamma|) \otimes \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right).$$

4.2 The RO extractor

Next, our goal is to extract multiple bits of randomness from x. To do this, we model E as a *random oracle*. We derive a bound on the advantage any adversary has in distinguishing $E(x)$ from a uniformly random string, based on the number of qubits k in the register $\mathcal{X}$, the number of vectors C in the superposition on register $\mathcal{X}$, and the number of queries q made to the random oracle. In fact, to be as general as possible, we consider a random oracle with input length n, and allow $n-k$ of the bits of the input to the random oracle to be (adaptively) determined by the adversary, while the remaining k bits are sampled by measuring a k-qubit register $\mathcal{X}$.

Theorem 4.2. *Let $H : \{0,1\}^n \to \{0,1\}^m$ be a uniformly random function, and let q, C, k be integers. Consider a two-stage oracle algorithm (A_1^H, A_2^H) that combined makes at most q queries to H. Suppose that A_1^H outputs classical strings $(T, \{x_i\}_{i\in T})$, and let $|\gamma\rangle_{\mathcal{A},\mathcal{X}}$ be its left-over quantum state,[12] where $T \subset [n]$ is a set of size $n-k$, each $x_i \in \{0,1\}$, $\mathcal{A}$ is a register of arbitary size, and $\mathcal{X}$ is a register of k qubits. Suppose further that with probability 1 over the sampling of H and the execution of A_1, there exists a set $L \subset \{0,1\}^k$ of size at most C such that $|\gamma\rangle$ may be written as follows:*

$$|\gamma\rangle = \sum_{u\in L} |\psi_u\rangle_{\mathcal{A}} \otimes |u\rangle_{\mathcal{X}} .$$

Now consider the following two games.

- REAL*:*

[12] That is, consider sampling H, running a purified A_1^H, measuring at the end to obtain $(T, \{x_i\}_{i\in T})$, and then defining $|\gamma\rangle$ to be the left-over state on $\mathcal{A}$'s remaining registers.

– *A_1^H outputs $T, \{x_i\}_{i\in T}, |\gamma\rangle_{\mathcal{A},\mathcal{X}}$.*
– *$\mathcal{X}$ is measured in the Hadamard basis to produce a k-bit string which is parsed as $\{x_i\}_{i\in\overline{T}}$, and a left-over state $|\gamma'\rangle_{\mathcal{A}}$ on register $\mathcal{A}$. Define $x = (x_1, \ldots, x_n)$.*
– *A_2^H is given $T, \{x_i\}_{i\in T}, |\gamma'\rangle_{\mathcal{A}}, H(x)$, and outputs a bit.*

- IDEAL*:*
  – *A_1^H outputs $T, \{x_i\}_{i\in T}, |\gamma\rangle_{\mathcal{A},\mathcal{X}}$.*
  – *$r \leftarrow \{0,1\}^m$.*
  – *A_2^H is given $T, \{x_i\}_{i\in T}, \mathrm{Tr}_{\mathcal{X}}(|\gamma\rangle\langle\gamma|), r$, and outputs a bit.*

Then,

$$|\Pr[\mathsf{REAL}=1] - \Pr[\mathsf{IDEAL}=1]| \leq \frac{2\sqrt{q}C + 2q\sqrt{C}}{2^{k/2}} < \frac{4qC}{2^{k/2}}.$$

5 Non-interactive extractable and equivocal commitments

A non-interactive commitment scheme with partial opening in the quantum random oracle model consists of classical oracle algorithms $(\mathsf{Com}, \mathsf{Open}, \mathsf{Rec})$ with the following syntax.

- $\mathsf{Com}^H(1^\lambda, \{m_i\}_{i\in[n]})$: On input the security parameter λ and n messages $\{m_i \in \{0,1\}^k\}_{i\in[n]}$, output n commitments $\{\mathsf{com}_i\}_{i\in[n]}$ and a state st.
- $\mathsf{Open}^H(\mathsf{st}, T)$: On input a state st and a set $T \subseteq [n]$, output messages $\{m_i\}_{i\in T}$ and openings $\{u_i\}_{i\in T}$.
- $\mathsf{Rec}^H(\{\mathsf{com}_i\}_{i\in[n]}, T, \{m_i, u_i\}_{i\in T})$: on input n commitments $\{\mathsf{com}_i\}_{i\in[n]}$, a set T, and a set of message opening pairs $\{m_i, u_i\}_{i\in T}$, output either $\{m_i\}_{i\in T}$ or $\perp$.

The commitment scheme is parameterized by $n = n(\lambda)$ which is the number of messages to be committed in parallel, and $k = k(\lambda)$ which is the number of bits per message.

5.1 Definitions

Definition 5.1 (Correctness)**.** *A non-interactive commitment scheme with partial opening in the QROM is* correct *if for any $\{m_i\}_{i\in[n]}$ and $T \subseteq [n]$,*

$$\Pr\left[\mathsf{Rec}^H(\{\mathsf{com}_i\}_{i\in[n]}, T, \{m_i, u_i\}_{i\in T}) = \{m_i\}_{i\in T} : \begin{array}{r}(\mathsf{st}, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Com}^H(1^\lambda, \{m_i\}_{i\in[n]}) \\ \{m_i, u_i\}_{i\in T} \leftarrow \mathsf{Open}^H(\mathsf{st}, T)\end{array}\right] = 1.$$

Definition 5.2 (μ-Hiding)**.** *A non-interactive commitment scheme with partial opening in the QROM is μ-hiding if for any adversary Adv that makes at most $q(\lambda)$ queries to the random oracle, and any two sets of messages $\{m_{i,0}\}_{i\in[n]}$ and $\{m_{i,1}\}_{i\in[n]}$, it holds that*

$$\Big|\Pr\left[\mathsf{Adv}^H(\{\mathsf{com}_i\}_{i\in[n]}) = 1 : \{\mathsf{com}_i\}_{i\in[n]} \leftarrow \mathsf{Com}^H(1^\lambda, \{m_{i,0}\}_{i\in[n]})\right] -$$

$$\Pr\left[\mathsf{Adv}^H(\{\mathsf{com}_i\}_{i\in[n]}) = 1 : \{\mathsf{com}_i\}_{i\in[n]} \leftarrow \mathsf{Com}^H(1^\lambda, \{m_{i,1}\}_{i\in[n]})\right]\Big| = \mu(\lambda, q(\lambda)).$$

Furthermore, we say that a commitment is hiding *if it is μ-hiding, where μ is such that for any $q(\lambda) = \mathrm{poly}(\lambda)$, $\mu(\lambda, q(\lambda)) = \mathrm{negl}(\lambda)$.*

Definition 5.3 (μ-Extractability)**.** *A non-interactive commitment scheme with partial opening in the QROM is* μ-extractable *if there exists a polynomial s and a simulator* SimExt *consisting of an interface* SimExt.RO *and an algorithm* SimExt.Ext *that may share a common state, such that for any family of quantum oracle algorithms $\{\mathsf{Adv}_\lambda = (\mathsf{Adv}_{\mathsf{Commit},\lambda}, \mathsf{Adv}_{\mathsf{Open},\lambda}, \mathsf{D}_\lambda)\}_{\lambda\in\mathbb{N}}$ that makes at most $q(\lambda)$ queries to the random oracle, it holds that*

$$\left|\Pr_H\left[\mathsf{D}_\lambda^H(\boldsymbol{\rho}_2,\mathsf{out})=1:\begin{array}{r}(\boldsymbol{\rho}_1,\{\mathsf{com}_i\}_{i\in[n]})\leftarrow\mathsf{Adv}^H_{\mathsf{Commit},\lambda}\\(\boldsymbol{\rho}_2,T,\{m_i,u_i\}_{i\in T})\leftarrow\mathsf{Adv}^H_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)\\\mathsf{out}\leftarrow\mathsf{Rec}^H(\{\mathsf{com}_i\}_{i\in[n]},T,\{m_i,u_i\}_{i\in T})\end{array}\right]\right.$$
$$\left.-\Pr\left[\mathsf{D}_\lambda^{\mathsf{SimExt.RO}}(\boldsymbol{\rho}_2,\mathsf{out})=1:\begin{array}{r}(\boldsymbol{\rho}_1,\{\mathsf{com}_i\}_{i\in[n]})\leftarrow\mathsf{Adv}^{\mathsf{SimExt.RO}}_{\mathsf{Commit},\lambda}\\\{m_i^*\}_{i\in[n]}\leftarrow\mathsf{SimExt.Ext}(\{\mathsf{com}_i\}_{i\in[n]})\\(\boldsymbol{\rho}_2,T,\{m_i,u_i\}_{i\in T})\leftarrow\mathsf{Adv}^{\mathsf{SimExt.RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)\\\mathsf{out}\leftarrow\mathsf{Rec}^{\mathsf{SimExt.RO}}(\{\mathsf{com}_i\}_{i\in[n]},T,\{m_i,u_i\}_{i\in T})\\\mathsf{out}:=\mathsf{FAIL}\text{ if }\mathsf{out}\notin\{\{m_i^*\}_{i\in T},\bot\}\end{array}\right]\right|=\mu(\lambda,q(\lambda)),$$

where the state of SimExt *was kept implicit, and the total run-time of* SimExt *on security parameter 1^λ is at most $s(\lambda, q(\lambda))$. The interface* SimExt.RO *is invoked on each query to H made by* Adv *and* Rec*, while the algorithm* SimExt.Ext *is invoked on the classical commitments output by* Adv*.*

Furthermore, we say that a commitment is extractable *if it is μ-extractable, where μ is such that for any $q(\lambda) = \mathrm{poly}(\lambda)$, $\mu(\lambda, q(\lambda)) = \mathrm{negl}(\lambda)$.*

Finally, we say that the commitment scheme satisfies extraction with a ν-commuting simulator *if a call to* SimExt.RO *$\nu(\lambda)$-almost-commutes with the operation* SimExt.Ext *when the input and output registers of* SimExt.RO *and* SimExt.Ext *are disjoint.*[13]

Definition 5.4 (μ-Equivocality)**.** *A non-interactive commitment scheme with partial opening in the QROM is* μ-equivocal *if there exists a polynomial s and a simulator* SimEqu *that consists of an interface* SimEqu.RO *and two algorithms* SimEqu.Com, SimEqu.Open *that may all share a common state, such that for any family of quantum oracle algorithms $\{\mathsf{Adv}_\lambda = (\mathsf{Adv}_{\mathsf{RCommit},\lambda}, \mathsf{Adv}_{\mathsf{ROpen},\lambda}, \mathsf{D}_\lambda)\}_{\lambda\in\mathbb{N}}$ that makes at most $q(\lambda)$ queries to the random oracle, it holds that*

$$\left|\Pr_H\left[\mathsf{D}_\lambda^H(\boldsymbol{\rho}_2,\{\mathsf{com}_i,m_i,u_i\}_{i\in[n]})=1:\begin{array}{r}(\boldsymbol{\rho}_1,\{m_i\}_{i\in[n]})\leftarrow\mathsf{Adv}^H_{\mathsf{RCommit},\lambda}\\(\mathsf{st},\{\mathsf{com}_i\}_{i\in[n]})\leftarrow\mathsf{Com}^H(1^\lambda,\{m_i\}_{i\in[n]})\\\boldsymbol{\rho}_2\leftarrow\mathsf{Adv}^H_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1,\{\mathsf{com}_i\}_{i\in[n]})\\\{m_i,u_i\}_{i\in[n]}\leftarrow\mathsf{Open}^H(\mathsf{st},[n])\end{array}\right]\right.$$
$$\left.-\Pr\left[\mathsf{D}_\lambda^{\mathsf{SimEqu.RO}}(\boldsymbol{\rho}_2,\{\mathsf{com}_i,m_i,u_i\}_{i\in[n]})=1:\begin{array}{r}(\boldsymbol{\rho}_1,\{m_i\}_{i\in[n]})\leftarrow\mathsf{Adv}^{\mathsf{SimEqu.RO}}_{\mathsf{RCommit},\lambda}\\\{\mathsf{com}_i\}_{i\in[n]}\leftarrow\mathsf{SimEqu.Com}\\\boldsymbol{\rho}_2\leftarrow\mathsf{Adv}^{\mathsf{SimEqu.RO}}_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1,\{\mathsf{com}_i\}_{i\in[n]})\\\{u_i\}_{i\in[n]}\leftarrow\mathsf{SimEqu.Open}(\{m_i\}_{i\in[n]})\end{array}\right]\right|=\mu(\lambda,q(\lambda)),$$

where the state of SimEqu *was kept implicit, and the total run-time of* SimEqu *on security parameter 1^λ is at most $s(\lambda, q(\lambda))$. The interface* SimEqu.RO *is invoked on each query to H made by* Adv*, the algorithm*

[13] Note that SimExt.RO and SimExt.Ext can share a common state, so do not necesarily commute even when their inputs and output registers are disjoint.

SimEqu.Com *is invoked to produce commitments, and the algorithm* SimEqu.Open *is invoked on a set of messages to produce openings.*

Furthermore, we say that a commitment is equivocal *if it is μ-equivocal, where μ is such that for any $q(\lambda) = \text{poly}(\lambda)$, $\mu(\lambda, q(\lambda)) = \text{negl}(\lambda)$.*

It is easy to see that a μ-equivocal commitment satisfies 2μ-hiding, since one can first move from committing to $\{m_{i,0}\}_{i\in[n]}$ to a hybrid where the equivocality simulator is run, and then move to committing to $\{m_{i,1}\}_{i\in[n]}$.

We also note that all our definitions consider *classical commitments*, where the commitment string itself is purely classical. Furthermore, we assume that any potentially quantum state sent by a malicious committer is immediately measured by an honest receiver to produce a classical string – it is this classical string that serves as the commitment. This is similar to prior works that consider commitments in the QROM (eg., [DFMS21]), and we refer the reader to [BB21] for additional discussions about enforcing classical (parts of) commitments via measurement.

5.2 Construction

Protocol 6

Parameters: security parameter λ, number of commitments $n = n(\lambda)$
Random oracle: $H : \{0,1\}^{\lambda+1} \to \{0,1\}^{\lambda+1}$.

- $\mathsf{Com}^H(1^\lambda, \{b_i\}_{i\in[n]})$: For all $i \in [n]$, sample $r_i \leftarrow \{0,1\}^\lambda$ and set $\mathsf{com}_i = H(b_i||r_i)$. Set $\mathsf{st} = \{b_i, r_i\}_{i\in[n]}$ and output $(\mathsf{st}, \{\mathsf{com}_i\}_{i\in[n]})$.
- $\mathsf{Open}^H(\mathsf{st}, T)$: Parse st as $\{b_i, r_i\}_{i\in[n]}$ and output $\{b_i, r_i\}_{i\in T}$.
- $\mathsf{Rec}^H(\{\mathsf{com}_i\}_{i\in[n]}, T, \{b_i, r_i\}_{i\in T})$: Output $\perp$ if there exists $i \in T$ s.t. $H(b_i||r_i) \neq \mathsf{com}_i$. Otherwise output $\{b_i\}_{i\in T}$.

Figure 6: Extractable and equivocal commitment scheme

We construct extractable and equivocal bit commitments in the QROM in Fig. 6. Without loss of generality, a committer can commit to strings of length > 1 by committing to each bit in the string one by one, and sending all commitments in parallel.

5.3 Extractability

In this section, we prove the following theorem by relying on Imported Theorem 3.6. We remark that our proof of extraction uses ideas already present in [DFMS21] to establish that our construction satisfies Definition 5.3.

Theorem 5.5. *Protocol 6 is a μ-extractable non-interactive commitment scheme with partial opening in the QROM, with message length 1 (i.e. $k = 1$), satisfying Definition 5.3, where $\mu(\lambda, q, n) = \frac{8qn}{2^{\lambda/2}} +$*

$\frac{148(q+n+1)^3+1}{2^\lambda}$[14], *and where the runtime of the simulator is bounded by* $s(\lambda, q) = O(q^2 + q \cdot n(\lambda))$. *In addition, the protocol satisfies extraction with* ν*-commuting simulator, where* $\nu(\lambda) = \frac{8}{2^{\lambda/2}}$.

Proof. Let $(\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}, \mathsf{Sim}_{\mathsf{RO}}.\mathsf{E})$ be the on-the-fly random oracle simulator with extraction from Imported Theorem 3.6. The extractable commitment simulator $\mathsf{SimExt} = (\mathsf{SimExt.RO}, \mathsf{SimExt.Ext})$ is defined as follows.

- $\mathsf{SimExt.RO} = \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$
- $\mathsf{SimExt.Ext}$ runs $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$ to obtain either a $\lambda+1$ bit string x^*, or $\emptyset$. In the case of x^*, output the first bit of x^*. In the case of $\emptyset$, output 0.

We now prove that for any family of quantum oracle algorithms $\{\mathsf{Adv}_\lambda = (\mathsf{Adv}_{\mathsf{Commit},\lambda}, \mathsf{Adv}_{\mathsf{Open},\lambda}, \mathsf{D}_\lambda)\}_{\lambda\in\mathbb{N}}$, the two experiments in Definition 5.3 are $\mu(\lambda, q)$ close, where $\mu(\lambda, q) = \frac{148(q+n+1)^3+1}{2^\lambda} + \frac{8qn}{2^{\lambda/2}}$. We consider the following sequence of hybrids (where parts in blue indicate difference from the previous hybrid):

- Hyb_0: This corresponds to the "real" experiment in Definition 5.3.
  1. Sample oracle $H \leftarrow F_{\{0,1\}^{\lambda+1}\to\{0,1\}^{\lambda+1}}$.
  2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^H_{\mathsf{Commit},\lambda}$
  3. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^H_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$
  4. $\mathsf{out} \leftarrow \mathsf{Rec}^H(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$
  5. Output $b \leftarrow \mathsf{D}^H_\lambda(\boldsymbol{\rho}_2, \mathsf{out})$
- Hyb_1: This is the same as previous hybrid, except that all oracle calls to H are answered by $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$.
  1. Initialize the extractable random oracle simulator, $\mathsf{Sim}_{\mathsf{RO}}$.
  2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Commit},\lambda}$
  3. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$
  4. $\mathsf{out} \leftarrow \mathsf{Rec}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$
  5. Output $b \leftarrow \mathsf{D}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_\lambda(\boldsymbol{\rho}_2, \mathsf{out})$
- Hyb_2: This is the same as the previous hybrid except for an additional query to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ that is performed at the end of the experiment, along with an event BAD that we define. Notice also that we have opened up the description of the algorithm Rec below. The hybrid outputs the following distribution.
  1. Initialize the extractable random oracle simulator, $\mathsf{Sim}_{\mathsf{RO}}$.
  2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Commit},\lambda}$
  3. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$

[14] When $n = c\lambda$ for some arbitrary fixed constant c, then we can define $\mu_c(\lambda, q) = \frac{2q(c\lambda)^{1/2}}{2^{\lambda/2}}$. In all our OT protocols, we will set n in this manner and will assume that μ is a function of λ, q.

4. $\mathsf{out} \leftarrow \mathsf{Rec}^{\mathsf{Sim_{RO}.RO}}(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$
   - If there exists $i \in T$ s.t. $\mathsf{Sim_{RO}.RO}(b_i||r_i) \neq \mathsf{com}_i$, set $\mathsf{out} := \bot$, otherwise set $\mathsf{out} := \{b_i\}_{i\in T}$.
5. Obtain bit $b \leftarrow \mathsf{D}_\lambda^{\mathsf{Sim_{RO}.RO}}(\boldsymbol{\rho}_2, \mathsf{out})$.
6. For all $i \in [n]$, set $y_i \leftarrow \mathsf{Sim_{RO}.RO}(b_i||r_i)$.
7. If $\mathsf{out} \neq \bot$ and there exists $i \in T$ such that $y_i \neq \mathsf{com}_i$, output BAD, otherwise output b.

- Hyb_3 : This is the same as the previous hybrid except that there is a query to $\mathsf{Sim_{RO}.E}$, and an extra condition in the BAD event. The hybrid outputs the following distribution:

1. Initialize the extractable random oracle simulator, $\mathsf{Sim_{RO}}$.
2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{\mathsf{Sim_{RO}.RO}}_{\mathsf{Commit},\lambda}$
3. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^{\mathsf{Sim_{RO}.RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$
4. $\mathsf{out} \leftarrow \mathsf{Rec}^{\mathsf{Sim_{RO}.RO}}(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$
   - If there exists $i \in T$ s.t. $\mathsf{Sim_{RO}.RO}(b_i||r_i) \neq \mathsf{com}_i$, set $\mathsf{out} := \bot$, otherwise set $\mathsf{out} := \{b_i\}_{i\in T}$.
5. Obtain bit $b \leftarrow \mathsf{D}_\lambda^{\mathsf{Sim_{RO}.RO}}(\boldsymbol{\rho}_2, \mathsf{out})$
6. For all $i \in [n]$, set $y_i \leftarrow \mathsf{Sim_{RO}.RO}(b_i||r_i)$.
7. For all $i \in [n]$, set $x_i^* \leftarrow \mathsf{Sim_{RO}.E}(\mathsf{com}_i)$.
8. If there exists $i \in T$ such that $(x_i^* \neq (b_i||r_i)) \wedge (y_i = \mathsf{com}_i)$, output BAD, or if $\mathsf{out} \neq \bot$ and there exists $i \in T$ such that $y_i \neq \mathsf{com}_i$, output BAD, otherwise output b.

- Hyb_4: This hybrid is identical to the previous one except that $\mathsf{Sim_{RO}.E}$ is called earlier on in the hybrid. The hybrid outputs the following distribution:

1. Initialize the extractable random oracle simulator, $\mathsf{Sim_{RO}}$.
2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{\mathsf{Sim_{RO}.RO}}_{\mathsf{Commit},\lambda}$
3. For all $i \in [n]$, set $x_i^* \leftarrow \mathsf{Sim_{RO}.E}(\mathsf{com}_i)$.
4. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^{\mathsf{Sim_{RO}.RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$
5. $\mathsf{out} \leftarrow \mathsf{Rec}^{\mathsf{Sim_{RO}.RO}}(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$
   - If there exists $i \in T$ s.t. $\mathsf{Sim_{RO}.RO}(b_i||r_i) \neq \mathsf{com}_i$, set $\mathsf{out} := \bot$, otherwise set $\mathsf{out} := \{b_i\}_{i\in T}$.
6. $b \leftarrow \mathsf{D}_\lambda^{\mathsf{Sim_{RO}.RO}}(\boldsymbol{\rho}_2, \mathsf{out})$
7. For all $i \in [n]$, set $y_i \leftarrow \mathsf{Sim_{RO}.RO}(b_i||r_i)$.
8. If there exists $i \in T$ such that $(x_i^* \neq (b_i||r_i)) \wedge (y_i = \mathsf{com}_i)$, output BAD, or if $\mathsf{out} \neq \bot$ and there exists $i \in T$ such that $y_i \neq \mathsf{com}_i$, output BAD, otherwise output b.

- Hyb_5: This hybrid is identical to the previous hybrid except for altering the variable out to sometimes take the value FAIL. The hybrid outputs the following distribution:

1. Initialize the extractable random oracle simulator, $\mathsf{Sim_{RO}}$.

2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Commit},\lambda}$
3. For all $i \in [n]$, set $x_i^* \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}(\mathsf{com}_i)$. For all $i \in [n]$, if $x_i^* = \emptyset$, set $b_i^* := 0$, and otherwise set b_i^* equal to the first bit of x_i^*.
4. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$
5. Obtain $\mathsf{out} \leftarrow \mathsf{Rec}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$ as follows:
   - If there exists $i \in T$ s.t. $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(b_i||r_i) \neq \mathsf{com}_i$, set $\mathsf{out} := \bot$, otherwise set $\mathsf{out} := \{b_i\}_{i\in T}$.
6. If $\mathsf{out} \notin \{\{b_i^*\}_{i\in T}, \bot\}$, set $\mathsf{out} = \mathsf{FAIL}$.
7. $b \leftarrow \mathsf{D}_\lambda^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}(\boldsymbol{\rho}_2, \mathsf{out})$
8. For all $i \in [n]$, set $y_i \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(b_i||r_i)$.
9. If there exists $i \in T$ such that $(x_i^* \neq (b_i||r_i)) \wedge (y_i = \mathsf{com}_i)$, output BAD, or if $\mathsf{out} \neq \bot$ and there exists $i \in T$ such that $y_i \neq \mathsf{com}_i$, output BAD, otherwise output b.

- Hyb_6: This hybrid is identical to the previous hybrid except for removing the final query to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ and the event BAD.

1. Initialize the extractable random oracle simulator, $\mathsf{Sim}_{\mathsf{RO}}$.
2. $(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Commit},\lambda}$
3. For all $i \in [n]$, set $x_i^* \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}(\mathsf{com}_i)$. For all $i \in [n]$, if $x_i^* = \emptyset$, set $b_i^* := 0$, and otherwise set b_i^* equal to the first bit of x_i^*.
4. $(\boldsymbol{\rho}_2, \{b_i, r_i\}_{i\in T}) \leftarrow \mathsf{Adv}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}_{\mathsf{Open},\lambda}(\boldsymbol{\rho}_1)$
5. Obtain $\mathsf{out} \leftarrow \mathsf{Rec}^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}(\{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in T})$ as follows:
   - If there exists $i \in T$ s.t. $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(b_i||r_i) \neq \mathsf{com}_i$, set $\mathsf{out} := \bot$, otherwise set $\mathsf{out} := \{b_i\}_{i\in T}$.
6. If $\mathsf{out} \notin \{\{b_i^*\}_{i\in T}, \bot\}$, set $\mathsf{out} = \mathsf{FAIL}$.
7. $b \leftarrow \mathsf{D}_\lambda^{\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}}(\boldsymbol{\rho}_2, \mathsf{out})$
8. ~~For all $i \in [n]$, set $y_i \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(b_i||r_i)$.~~
9. ~~If there exists $i \in T$ such that $(x_i^* \neq (b_i||r_i)) \wedge (y_i = \mathsf{com}_i)$, output BAD, or if out $\neq \bot$ and there exists $i \in T$ such that $y_i \neq \mathsf{com}_i$, output BAD, otherwise output b.~~

We note that Hyb_6 is the simulated distribution. We prove indistinguishability between the hybrids below.

Claim 5.6. $\Pr[\mathsf{Hyb}_0 = 1] = \Pr[\mathsf{Hyb}_1 = 1]$

Proof. This follows from the indistinguishable simulation property of Imported Theorem 3.6. □

Claim 5.7. $\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1]$

Proof. First, adding the extra query to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ does not affect the output of the experiment since it is performed after b is computed. Next, the event BAD only occurs if some classical query $(b_i||r_i)$ to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ returns different classical values at different points in the experiment. However, this can never occur due to the indistinguishable simulation property of Imported Theorem 3.6, and because two classical queries to an oracle H always return the same value.

□

Claim 5.8. $|\Pr[\mathsf{Hyb}_2 = 1] - \Pr[\mathsf{Hyb}_3 = 1]| \leq \frac{148(q+n+1)^3+1}{2^\lambda}$

Proof. First, adding the query to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$ does not affect the output of the experiment since it is performed after the information needed to determine the output is already computed.

Thus, to prove this claim, it suffices to show that

$$\Pr_{\mathsf{Hyb}_2}[\exists\, i \in T \,:\, (x_i^* \neq (b_i||r_i)) \wedge (y_i = \mathsf{com}_i)] \leq \frac{296(q+n+1)^3+2}{2^{\lambda+1}}.$$

Consider adversary B that runs steps 2 through 5 in Hyb_2, and outputs $\{\mathsf{com}_i\}_{i\in T}, \{b_i||r_i\}_{i\in T}$. Note that B does not make any queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$. Now consider the experiment where B is run as above, followed by running $y_i \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(b_i||r_i)$ for all $i \in T$ and then $x_i^* \leftarrow \mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}(\mathsf{com}_i)$ for all $i \in T$, and outputting 1 if $\exists\, i \in T \,:\, (x_i^* \neq (b_i||r_i)) \wedge (\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(b_i||r_i) = \mathsf{com}_i)$. Applying the correctness of extraction property of Imported Theorem 3.6, and bounding $|T|$ by n, we get the required claim. □

Claim 5.9. $|\Pr[\mathsf{Hyb}_3 = 1] - \Pr[\mathsf{Hyb}_4 = 1]| \leq \frac{8qn}{2^{\lambda/2}}$

Proof. This follows from the almost commutativity of $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$ and $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ property of Imported Theorem 3.6. Indeed, since $\{\mathsf{com}_i\}_{i\in[n]}$ are classical strings output by the experiment after step 2, all subsequent queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ are independent of $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}(\mathsf{com}_i)$ for any i, in the sense that they may operate on disjoint input and output registers. Thus, the statistical distance between the two experiments is at most $\frac{8qn}{2^{\lambda/2}}$, since there are most q queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$, and n queries to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$.

□

Claim 5.10. $\Pr[\mathsf{Hyb}_4 = 1] = \Pr[\mathsf{Hyb}_5 = 1]$

Proof. The only change in Hyb_5 is that the variable out is modified and set to FAIL when $\mathsf{out} \notin \{\{b_i^*\}_{i\in T}, \perp\}$. We show that whenever out is set of FAIL, the event BAD occurs, which means that the output of the experiment is anyway BAD.

Indeed, in the case of FAIL, we know that out is not equal to $\perp$ or $\{b_i^*\}_{i\in T}$. Since $\mathsf{out} \neq \perp$, this means that either BAD occurs, or $y_i = \mathsf{com}_i$ for all $i \in T$. Since $\mathsf{out} \neq \{b_i^*\}_{i\in T}$, there must there exist $i \in T$ such that $x_i^* \neq (b_i||r_i)$. But then if $y_i = \mathsf{com}_i$ for all $i \in T$, the event BAD also occurs.

□

Claim 5.11. $\Pr[\mathsf{Hyb}_6 = 1] \geq \Pr[\mathsf{Hyb}_5 = 1]$

Proof. This follows by observing that the distribution Hyb_6 is identical to Hyb_5 except that it never outputs BAD, and therefore the probability that it outputs 1 cannot possibly reduce. □

Combining all claims, we have that

$$\Pr[\mathsf{Hyb}_0 = 1] \leq \Pr[\mathsf{Hyb}_6 = 1] + \left(\frac{148(q+n+1)^3+1}{2^\lambda} + \frac{8qn}{2^{\lambda/2}}\right), \tag{1}$$

and by a similar argument

$$\Pr[\mathsf{Hyb}_0 = 0] \leq \Pr[\mathsf{Hyb}_6 = 0] + \left(\frac{148(q+n+1)^3+1}{2^\lambda} + \frac{8qn}{2^{\lambda/2}}\right).$$

Because the output of Hyb_0 and Hyb_6 is a single bit, the equation above implies that

$$\Pr[\mathsf{Hyb}_6 = 1] \leq \Pr[\mathsf{Hyb}_0 = 1] + \left(\frac{148(q+n+1)^3+1}{2^\lambda} + \frac{8qn}{2^{\lambda/2}}\right) \tag{2}$$

Combining equations (1) and (2), we have

$$\left|\Pr[\mathsf{Hyb}_6 = 1] - \Pr[\mathsf{Hyb}_0 = 1]\right| \leq \left(\frac{148(q+n+1)^3+1}{2^\lambda} + \frac{8qn}{2^{\lambda/2}}\right), \tag{3}$$

In addition, by Property 3 in Imported Theorem 3.6, the runtime of Sim is bounded by a polynomial $s(\lambda, q) = O(q^2 + q \cdot n)$. Finally, by the almost commutativity of $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ and $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{E}$ property of Imported Theorem 3.6, it follows that the simulator Sim is ν-commuting, with $\nu(\lambda) = \frac{8}{2^{\lambda/2}}$. □

5.4 Equivocality

Theorem 5.12. *Protocol 6 is a μ-equivocal bit commitment scheme with partial opening in the QROM satisfying Definition 5.4, where $\mu(\lambda, q, n) = \frac{2qn^{1/2}}{2^{\lambda/2}}$ [15] and where the runtime of the simulator is bounded by $s(\lambda, q) = O(q^2 + \mathrm{poly}(\lambda))$.*

Proof. We construct a simulator $\mathsf{SimEqu} = (\mathsf{SimEqu.RO}, \mathsf{SimEqu.Com}, \mathsf{SimEqu.Open})$ as follows:

1. Initialize the efficient on-the-fly random oracle simulator, $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$, from Imported Theorem 3.6. For all $i \in [n]$, sample $r_i \leftarrow \{0,1\}^\lambda, R_0^i, R_1^i \leftarrow \{0,1\}^{\lambda+1}$.

2. Let SimEqu.RO answer oracle queries of $\mathsf{Adv}_{\mathsf{RCommit},\lambda}$ and $\mathsf{Adv}_{\mathsf{ROpen},\lambda}$ using the oracle $H^\perp$ which is defined as follows:

$$H^\perp(x) = \begin{cases} R_0^i & \text{if } x = 0||r_i \text{ for some } i \in [n] \\ R_1^i & \text{if } x = 1||r_i \text{ for some } i \in [n] \\ \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(x) & \text{otherwise} \end{cases}$$

   In an abuse of notation, we have defined $H^\perp$ using the quantum operation $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$. $H^\perp$ will actually be implemented by issuing a *controlled* query to $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ (see discussion on controlled queries in Section 3.2), controlled on the x in input register $\mathcal{X}$ not being in the set $\{b||r_i\}_{b\in\{0,1\},i\in[n]}$, and then, for each $i \in [n]$ and $b \in \{0,1\}$, implementing a controlled query to a unitary that maps $|x, y\rangle \to |x, y \oplus R_b^i\rangle$, controlled on the input $\mathcal{X}$ register being $(b||r_i)$.

3. SimEqu.Com: To output commitments, for all $i \in [n]$, sample $c_i \leftarrow \{0,1\}^{\lambda+1}$, set $\mathsf{com}_i = c_i$ and output $\{\mathsf{com}_i\}_{i\in[n]}$.

4. SimEqu.Open: When given input $\{b_i\}_{i\in[n]}$, output $\{b_i, r_i\}_{i\in[n]}$.

[15] When $n = c\lambda$ for some arbitrary fixed constant c, then we can define $\mu_c(\lambda, q) = \frac{2q(c\lambda)^{1/2}}{2^{\lambda/2}}$. In all our OT protocols, we will set n in this manner and will assume that μ is a function of λ, q.

5. Let $\mathsf{SimEqu.RO}$ answer oracle queries of D_λ using the oracle $H_R^\perp$ which is defined as follows:

$$H_R^\perp(x) = \begin{cases} c_i & \text{if } x = b_i||r_i \text{ for some } i \in [n] \\ \mathsf{Sim_{RO}.RO}(x) & \text{otherwise} \end{cases}$$

Note that $H_R^\perp$ can be implemented in a similar way as described above.

Consider then the following sequence of hybrids to prove that Protocol 6 is an equivocal bit commitment scheme in QROM satisfying Definition 5.4 (parts in blue are different from previous hybrid):

- Hyb_0: This hybrid outputs the following distribution, which matches the real output distribution in Definition 5.4.
  - Sample oracle $H \leftarrow F_{\{0,1\}^{\lambda+1} \to \{0,1\}^{\lambda+1}}$.
  - $(\boldsymbol{\rho}_1, \{b_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^H_{\mathsf{RCommit},\lambda}$
  - $(\mathsf{st}, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Com}^H(1^\lambda, \{b_i\}_{i\in[n]})$
  - $\boldsymbol{\rho}_2 \leftarrow \mathsf{Adv}^H_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]})$
  - $\{b_i, r_i\}_{i\in[n]} \leftarrow \mathsf{Open}^H(\mathsf{st}, [n])$
  - Output $\mathsf{D}^H_\lambda(\boldsymbol{\rho}_2, \{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in[n]})$.
- Hyb_1: This is the same as the previous hybrid except that the randomness used in Com is sampled at the beginning of the experiments and is used to define a different oracle $H^\perp$. $H^\perp$ is then used to answer queries of $\mathsf{Adv}_{\mathsf{RCommit},\lambda}, \mathsf{Adv}_{\mathsf{ROpen},\lambda}$. Concretely, this hybrid outputs the following distribution.
  - Sample oracle $H \leftarrow F_{\{0,1\}^{\lambda+1} \to \{0,1\}^{\lambda+1}}$.
  - For all $i \in [n]$, sample $r_i \leftarrow \{0,1\}^\lambda, R_0^i, R_1^i \leftarrow \{0,1\}^{\lambda+1}$ and define oracle $H^\perp$ as:

$$H^\perp(x) = \begin{cases} R_0^i & \text{if } x = 0||r_i \text{ for some } i \in [n] \\ R_1^i & \text{if } x = 1||r_i \text{ for some } i \in [n] \\ H(x) & \text{otherwise} \end{cases}$$

  - $(\boldsymbol{\rho}_1, \{b_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{H^\perp}_{\mathsf{RCommit},\lambda}$
  - $(\mathsf{st}, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Com}^H(1^\lambda, \{b_i\}_{i\in[n]})$
  - $\boldsymbol{\rho}_2 \leftarrow \mathsf{Adv}^{H^\perp}_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]})$
  - Output $\mathsf{D}^H_\lambda(\boldsymbol{\rho}_2, \{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in[n]})$.
- Hyb_2: This is the same as previous hybrid, except that the commitments are sampled as fresh uniformly random string, and another oracle $H_R^\perp$ is defined that is used to answer oracle queries of D_λ. Concretely, this hybrid outputs the following distribution.
  - Sample oracle $H \leftarrow F_{\{0,1\}^{\lambda+1} \to \{0,1\}^{\lambda+1}}$.

– For all $i \in [n]$, sample $r_i \leftarrow \{0,1\}^\lambda, R_0^i, R_1^i \leftarrow \{0,1\}^{\lambda+1}$ and define oracle $H^\perp$ as:

$$H^\perp(x) = \begin{cases} R_0^i & \text{if } x = 0||r_i \text{ for some } i \in [n] \\ R_1^i & \text{if } x = 1||r_i \text{ for some } i \in [n] \\ H(x) & \text{otherwise} \end{cases}$$

– $(\boldsymbol{\rho}_1, \{b_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{H^\perp}_{\mathsf{RCommit},\lambda}$

– For all $i \in [n]$, sample $c_i \leftarrow \{0,1\}^{\lambda+1}$ and set $\mathsf{com}_i = c_i$.

– $\boldsymbol{\rho}_2 \leftarrow \mathsf{Adv}^{H^\perp}_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]})$

– Define oracle $H^\perp_R$ as follows:

$$H^\perp_R(x) = \begin{cases} c_i & \text{if } x = b_i||r_i \text{ for some } i \in [n] \\ H(x) & \text{otherwise} \end{cases}$$

– Output $\mathsf{D}_\lambda^{H^\perp_R}(\boldsymbol{\rho}_2, \{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in[n]})$.

- Hyb_3: This is the same as previous hybrid, except that the oracle H is replaced by the efficient on-the-fly simulator $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$. This hybrid distribution is also the simulated output distribution in Definition 5.4. Concretely, this hybrid outputs the following distribution.

  – Initialize on-the-fly simulator $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$.

  – For all $i \in [n]$, sample $r_i \leftarrow \{0,1\}^\lambda, R_0^i, R_1^i \leftarrow \{0,1\}^{\lambda+1}$ and define oracle $H^\perp$ as:

$$H^\perp(x) = \begin{cases} R_0^i & \text{if } x = 0||r_i \text{ for some } i \in [n] \\ R_1^i & \text{if } x = 1||r_i \text{ for some } i \in [n] \\ \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(x) & \text{otherwise} \end{cases}$$

  – $(\boldsymbol{\rho}_1, \{b_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^{H^\perp}_{\mathsf{RCommit},\lambda}$

  – For all $i \in [n]$, sample $c_i \leftarrow \{0,1\}^{\lambda+1}$, and set $\mathsf{com}_i = c_i$.

  – $\boldsymbol{\rho}_2 \leftarrow \mathsf{Adv}^{H^\perp}_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]})$

  – Define oracle $H^\perp_R$ as follows:

$$H^\perp_R(x) = \begin{cases} c_i & \text{if } x = b_i||r_i \text{ for some } i \in [n] \\ \mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}(x) & \text{otherwise} \end{cases}$$

  – Output $\mathsf{D}_\lambda^{H^\perp_R}(\boldsymbol{\rho}_2, \{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in[n]})$.

Consider the following indistinguishability claims between the hybrids:

Claim 5.13. $|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]| \leq \frac{2qn^{1/2}}{2^{\lambda/2}}$

Proof. The two hybrids differ in the way oracle queries of Adv_λ are answered. In Hyb_1, queries of $\mathsf{Adv}_{\mathsf{RCommit},\lambda}$ and $\mathsf{Adv}_{\mathsf{ROpen},\lambda}$ are answered using oracle $H^\perp$ instead of H as in Hyb_0. Assume then for sake of contradiction that there exists some $\mathsf{Adv} = \{\boldsymbol{\rho}_\lambda, \mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$ for which $|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_0 = 1]| > \frac{2q^{3/2}n^{1/2}}{2^{\lambda/2}}$. Fix such Adv.

We derive a contradiction by relying on the One-Way to Hiding lemma (Imported Theorem 3.4). We first define oracle algorithms $\mathsf{A}, \mathsf{B}, \mathsf{C}$. Our goal after defining these algorithms will be to show C succeeds in a particular event with more probability than is allowed by the statement of the lemma, which gives us a contradiction.

$\underline{\mathsf{A}^O(H, \{r_i\}_{i\in[n]})}$

- $(\boldsymbol{\rho}_1, \{b_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}^O_{\mathsf{RCommit},\lambda}$
- $(\mathsf{st}, \{\mathsf{com}_i\}_{i\in[n]}) \leftarrow \mathsf{Com}^H(1^\lambda, \{b_i\}_{i\in[n]}; \{r_i\}_{i\in[n]})$
- $\boldsymbol{\rho}_2 \leftarrow \mathsf{Adv}^O_{\mathsf{ROpen},\lambda}(\boldsymbol{\rho}_1, \{\mathsf{com}_i\}_{i\in[n]})$
- $\{b_i, r_i\}_{i\in[n]} \leftarrow \mathsf{Open}^H(\mathsf{st}, [n])$
- Output $\mathsf{D}^H_\lambda(\boldsymbol{\rho}_2, \{\mathsf{com}_i\}_{i\in[n]}, \{b_i, r_i\}_{i\in[n]})$.

$\underline{\mathsf{B}^O(H, \{r_i\}_{i\in[n]})}$ Fix $q := q(\lambda)$ non-uniformly as (an upper bound on) the number of oracle queries of Adv_λ, and thus also A^O. Pick $i \leftarrow [q]$, run A^O until just before the i^{th} query, measure the query register and output the measurement outcome x.

$\underline{\mathsf{C}^O(H, \{r_i\}_{i\in[n]})}$ Run $x \leftarrow \mathsf{B}^O(H, \{r_i\}_{i\in[n]})$, parse x as $b||r$, where $|b| = 1, |r| = \lambda$, and output r.

We begin by proving the following claim about B.

SubClaim 5.14. *Given oracle H and $(\mathbf{r}, \mathbf{R}_0, \mathbf{R}_1) = \{r_i, R^i_0, R^i_1\}_{i\in[n]}$, define oracle $H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}$ as*

$$H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}(x) = \begin{cases} R^i_0 & \text{if } x = 0||r_i \text{ for some } i \in [n] \\ R^i_1 & \text{if } x = 1||r_i \text{ for some } i \in [n] \\ H(x) & \text{otherwise} \end{cases}$$

Then,

$$\Pr\left[x \in S_{\mathbf{r}} \;\middle|\; \begin{array}{r} H \leftarrow F_{\{0,1\}^{\lambda+1}\to\{0,1\}^{\lambda+1}} \\ \forall i \in [n], r_i \leftarrow \{0,1\}^\lambda, R^i_0, R^i_1 \leftarrow \{0,1\}^{\lambda+1} \\ x \leftarrow \mathsf{B}^{H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}(H, \{r_i\}_{i\in[n]}) \\ S_{\mathbf{r}} = \{(b||r_i)\}_{b\in\{0,1\},i\in[n]} \end{array}\right] > \frac{n}{2^\lambda}$$

Proof. Note that over the randomness of sampling $H, \mathbf{r}, \mathbf{R}_0, \mathbf{R}_1$, $\mathsf{A}^{H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}(H, \{r_i\}_{i\in[n]})$ is the experiment in Hyb_1, while $\mathsf{A}^H(H, \{r_i\}_{i\in[n]})$ is the experiment in Hyb_0.

For any oracle H, and any $\mathbf{r} := \{r_i\}_{i\in[n]}, \mathbf{R}_0 := \{R^i_0\}_{i\in[n]}, \mathbf{R}_1 := \{R^i_1\}_{i\in[n]}$,

$$P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{left}} := \Pr\left[\mathsf{A}^{H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}(H, \{r_i\}_{i\in[n]}) = 1\right], \quad P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{right}} := \Pr\left[\mathsf{A}^H(H, \{r_i\}_{i\in[n]}) = 1\right]$$

This implies that

$$\mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}\left[P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{left}}\right] = \Pr[\mathsf{Hyb}_1 = 1], \quad \mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}\left[P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{right}}\right] = \Pr[\mathsf{Hyb}_0 = 1]$$

Therefore,

$$\begin{aligned}\mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}\left|P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{left}} - P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{right}}\right| &\geq \left|\mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}\left[P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{left}}\right] - \mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}\left[P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{right}}\right]\right| \\ &= \left|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_0 = 1]\right| > \frac{2qn^{1/2}}{2^{\lambda/2}} \end{aligned} \tag{4}$$

where the first inequality follows by Jensen's inequality and linearity of expectation. Also, letting $S_{\mathbf{r}} = \{(b||r_i)\}_{b\in\{0,1\},i\in[n]}$, define

$$P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{guess}} := \Pr\left[x \in S_{\mathbf{r}} \mid x \leftarrow \mathsf{B}^{H^{\perp}_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}(H, \{r_i\}_{i\in[n]})\right].$$

Invoking the one-way to hiding lemma (Imported Theorem 3.4), with O_1, O_2 set as $H^{\perp}_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}, H$, and noting the oracle algorithm B in the lemma is exactly the same as B in our claim, and that set $S_{\mathbf{r}}$ is the set of points such that $\forall x \notin S_{\mathbf{r}}, H(x) = H^{\perp}_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}(x)$, we get

$$\begin{aligned}&\forall H, \mathbf{r}, \mathbf{R}_0, \mathbf{R}_1,\ P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{guess}} \geq \frac{\left|P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{left}} - P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{right}}\right|^2}{4q^2} \\ &\implies \mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}[P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{guess}}] \geq \mathop{\mathbb{E}}_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}\left[\frac{\left|P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{left}} - P^{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}_{\text{right}}\right|^2}{4q^2}\right] > \frac{n}{2^{\lambda}} \quad \text{(using Eq. (4))}\end{aligned}$$

Therefore,

$$\Pr_{H,\mathbf{r},\mathbf{R}_0,\mathbf{R}_1,\mathsf{B}}[x \in S_{\mathbf{r}} \mid x \leftarrow \mathsf{B}^{H^{\perp}_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}(H, \{r_i\}_{i\in[n]})] > \frac{n}{2^{\lambda}}$$

as desired. □

SubClaim 5.15. *Given oracle H and $(\mathbf{r}, \mathbf{R}_0, \mathbf{R}_1) = \{r_i, R^i_0, R^i_1\}_{i\in[n]}$, define oracle $H^{\perp}_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}$ as*

$$H^{\perp}_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}(x) = \begin{cases} R^i_0 & \text{if } x = 0||r_i \text{ for some } i \in [n] \\ R^i_1 & \text{if } x = 1||r_i \text{ for some } i \in [n] \\ H(x) & \text{otherwise} \end{cases}$$

Then,

$$\Pr\left[y \in \{r_i\}_{i\in[n]} \;\middle|\; \begin{array}{r} H \leftarrow F_{\{0,1\}^{\lambda+1}\to\{0,1\}^{\lambda+1}} \\ \forall i \in [n], r_i \leftarrow \{0,1\}^{\lambda}, R^i_0, R^i_1 \leftarrow \{0,1\}^{\lambda+1} \\ y \leftarrow \mathsf{C}^{H^{\perp}_{r,R_0,R_1}}(H, \{r_i\}_{i\in[n]}) \end{array}\right] > \frac{n}{2^{\lambda}}$$

Proof. This follows from Subclaim 5.14, and noting that for any $x \in S_{\mathbf{r}}$, x is of the form $b||r$, where $|b| = 1, |r| = \lambda$ and $r \in \{r_i\}_{i\in[n]}$.

□

To complete the proof of Claim 5.13, we note that by SubClaim 5.15, it holds that

$$\Pr[y \in \{r_i\}_{i\in[n]}] > \frac{n}{2^\lambda}$$

where y and $\{r_i\}_{i\in[n]}$ are sampled according to the process below:

- Sample oracle $H \leftarrow F_{\{0,1\}^{\lambda+1}\to\{0,1\}^{\lambda+1}}$.
- For all $i \in [n]$, sample $r_i \leftarrow \{0,1\}^\lambda, R_0^i, R_1^i \leftarrow \{0,1\}^{\lambda+1}$
- Sample $\iota \leftarrow [q]$ and execute the steps below until the adversary makes the ι^{th} query.
  - $(\boldsymbol{\rho}_1, \{b_i\}_{i\in[n]}) \leftarrow \mathsf{Adv}_{\mathsf{RCommit},\lambda}^{H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}$
  - $\boldsymbol{\rho}_2 \leftarrow \mathsf{Adv}_{\mathsf{ROpen},\lambda}^{H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}}(\boldsymbol{\rho}_1, \{H(b_i||r_i)\}_{i\in[n]})$
- Measure the adversary's query register to obtain x, parse x as $b||y$ where $|b| = 1, |y| = \lambda$.

Note that the view of $\mathsf{Adv}_{\mathsf{RCommit},\lambda}$ and $\mathsf{Adv}_{\mathsf{ROpen},\lambda}$ consists of $(H^\perp_{\mathbf{r},\mathbf{R}_0,\mathbf{R}_1}, \{H(b_i||r_i)\}_{i\in[n]}) \equiv (O, \{c_i\}_{i\in[n]})$ for a oracle O and strings $\{c_i\}_{i\in[n]}$ that are sampled uniformly and *independently* of each other and independently of $\{r_i\}_{i\in[n]}$. This means that the adversary is required to guess one out of n uniform λ-bit strings $\{r_i\}_{i\in[n]}$ given uniform and independent auxiliary information. Since this is impossible except with probability at most $\frac{n}{2^\lambda}$, we obtain a contradiction, proving our claim. □

Claim 5.16. $\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1]$

Proof. Note that the distribution of $\{\mathsf{com}_i\}_{i\in[n]}$ in either hybrid is a set of uniformly independently sampled random strings, sampled independently of the oracle that is accessed by $\mathsf{Adv}_{\mathsf{ROpen},\lambda}$. Therefore, the distribution of the output of $\mathsf{Adv}_{\mathsf{ROpen},\lambda}$ in either hybrid is identical. Conditioned on this, note that the following two distributions representing the inputs/oracle D_λ has access to, are identical:

- In Hyb_1, $(H, \{\mathsf{com}_i, b_i, r_i\}_{i\in[n]}) = (H, \{H(b_i||r_i), b_i, r_i\}_{i\in[n]})$.
- In Hyb_2, $(H^\perp_R, \{\mathsf{com}_i, b_i, r_i\}_{i\in[n]}) = (H^\perp_R, \{c_i, b_i, r_i\}_{i\in[n]})$, where for all $i \in [n], H^\perp_R(b_i||r_i) = c_i$.

Since the distributions are identical, the claim then follows. □

Claim 5.17. $\Pr[\mathsf{Hyb}_2 = 1] = \Pr[\mathsf{Hyb}_3 = 1]$

Proof. Indistinguishability follows immediately from the indistinguishable simulation property of Imported Theorem 3.6. □

Combining all claims, we get $|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_3 = 1]| \le \frac{2qn^{1/2}}{2^{\lambda/2}}$. In addition, note that the runtime of $\mathsf{Sim}_{\mathsf{Equ}}$ is bounded by $s(\lambda, q) = O(q^2 + \mathrm{poly}(\lambda))$, where the $O(q^2)$ terms comes from using $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ (Imported Theorem 3.6). □

6 The fixed basis framework: OT from entanglement

We first obtain non-interactive OT in the shared EPR model, and then show that the protocol remains secure even when one player does the EPR pair setup.

6.1 Non-interactive OT in the shared EPR pair model

Theorem 6.1. *Instantiate Protocol 7 with any non-interactive commitment scheme that is* correct *(Definition 5.1),* hiding *(Definition 5.2), and* extractable *(Definition 5.3). Then the following hold.*

- *When instantiated with the XOR extractor, there exist constants A, B such that Protocol 7 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{S-ROT}[1]}$.*
- *When instantiated with the ROM extractor, there exist constants A, B such that Protocol 7 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$.*

Furthermore, letting λ be the security parameter, q be an upper bound on the total number of random oracle queries made by the adversary, and using the commitment scheme from Section 5.2 with security parameter $\lambda_{\mathsf{com}} = 4\lambda$, the following hold.

- *When instantiatied with the XOR extractor and constants $A = 50$, $B = 100$, Protocol 7 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where*

$$\mu_{\mathsf{R}^*} = \left(\frac{8q^{3/2}}{2^{\lambda}} + \frac{3600\lambda q}{2^{2\lambda}} + \frac{148(450\lambda + q + 1)^3 + 1}{2^{4\lambda}}\right), \mu_{\mathsf{S}^*} = \left(\frac{85\lambda^{1/2}q}{2^{2\lambda}}\right).$$

  This requires a total of $2(A + B)\lambda = 300\lambda$ EPR pairs.

- *When instantiated with the ROM extractor and constants $A = 1050$, $B = 2160$, Protocol 7 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where*

$$\mu_{\mathsf{R}^*} = \left(\frac{8q^{3/2} + 4\lambda}{2^{\lambda}} + \frac{77040\lambda q}{2^{2\lambda}} + \frac{148(9630\lambda + q + 1)^3 + 1}{2^{4\lambda}}\right), \mu_{\mathsf{S}^*} = \left(\frac{197\lambda^{1/2}q}{2^{2\lambda}}\right).$$

  This requires a total of $2(A + B)\lambda = 6420\lambda$ EPR pairs.

Then, applying non-interactive bit OT reversal (Imported Theorem 3.3) to the protocol that realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$ immediately gives the following corollary.

Corollary 6.2. *Given a setup of 300λ shared EPR pairs, there exists a one-message protocol in the QROM that $O\left(\frac{q^{3/2}}{2^{\lambda}}\right)$-securely realizes $\mathcal{F}_{\mathsf{R-ROT}[1]}$.*

In this section, we provide the proof of Theorem 6.1.

Proof. We will prove the part of the theorem statement that considers instantiating Protocol 7 with the specific commitment from Section 5.2, and note that the more general part of the theorem statement follows along the same arguments.

Let H_C be the random oracle used by the commitment scheme. We treat H_C and H_{FS} (and H_{Ext} in the case of the ROM extractor) as separate oracles that the honest parties and adversaries query, which is without loss of generality (see Section 3.2).

Sender security. First, we show security against a malicious receiver R^*. Let $(\mathsf{SimExt.RO}, \mathsf{SimExt.Ext})$ be the simulator for the commitment scheme (Definition 5.3) against a malicious committer. We describe a simulator for our OT protocol against a malicious receiver below.

$\mathsf{Sim}[\mathsf{R}^*]$:

- Prepare $2n$ EPR pairs on registers $\mathcal{R}$ and $\mathcal{S}$.
- Initialize R^* with the state on register $\mathcal{R}$. Answer H_{FS} (and H_{Ext}) queries using the efficient on-the-fly random oracle simulator (Imported Theorem 3.6), and answer H_C queries using $\mathsf{SimExt.RO}$.
- Obtain $(x_0, x_1), \{c_i\}_{i\in[n]}, T, \{(r_{i,0}, r_{i,1}, \theta_i), u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$ from R^* and run
$$\{(r^*_{i,0}, r^*_{i,1}, \theta^*_i)\}_{i\in[n]} \leftarrow \mathsf{SimExt.Ext}(\{c_i\}_{i\in[n]}).$$
- Run the "check receiver message" part of the honest sender strategy, except that $\{r^*_{i,0}, r^*_{i,1}\}_{i\in T}$ are used in place of $\{r_{i,0}, r_{i,1}\}_{i\in T}$ for the third check. If any check fails, send abort to the ideal functionality, output R^*'s state, and continue to answering the distinguisher's queries.
- Let $b := \mathsf{maj}\{\theta^*_i \oplus d_i\}_{i\in\overline{T}}$. For all $i \in \overline{T}$, measure the register $\mathcal{S}_{i,b\oplus d_i}$ in basis $+$ if $b \oplus d_i = 0$ or basis $\times$ if $b \oplus d_i = 1$ to obtain r'_i. Let $m_b := x_b \oplus E(\{r'_i\}_{i\in\overline{T}})$.
- Send (b, m_b) to the ideal functionality, output R^*'s state, and continue to answering the distinguisher's queries.
- Answer the distinguisher's H_{FS} (and H_{Ext}) queries with the efficient on-the-fly random oracle simulator and H_C queries with $\mathsf{SimExt.RO}$.

Now, given a distinguisher D such that R^* and D make a total of at most q queries combined to H_{FS} and H_C (and H_{Ext}), consider the following sequence of hybrids.

- Hyb_0: The result of the real interaction between R^* and S. Using the notation of Definition 3.2, this is a distribution over $\{0,1\}$ described by $\Pi[\mathsf{R}^*, \mathsf{D}, \top]$.
- Hyb_1: This is identical to Hyb_0, except that all H_C queries of R^* and D are answered via the $\mathsf{Sim.RO}$ interface, and $\{(r^*_{i,0}, r^*_{i,1}, \theta^*_i)\} \leftarrow \mathsf{Sim.Ext}(\{c_i\}_{i\in[n]})$ is run after R^* outputs its message. The values $\{r^*_{i,0}, r^*_{i,1}\}_{i\in T}$ are used in place of $\{r_{i,0}, r_{i,1}\}_{i\in T}$ for the third sender check.
- Hyb_2: The result of $\mathsf{Sim}[\mathsf{R}^*]$ interacting in $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[1]}}$ (or $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}$). Using the notation of Definition 3.2, this is a distribution over $\{0,1\}$ described by $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[1]}}[\mathsf{Sim}[\mathsf{R}^*], \mathsf{D}, \top]$ (or $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}[\mathsf{Sim}[\mathsf{R}^*], \mathsf{D}, \top]$).

The proof of security against a malicious R^* follows by combining the two claims below, Claim 6.3 and Claim 6.4.

Claim 6.3.
$$|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]| \leq \frac{24(A+B)\lambda q}{2^{2\lambda}} + \frac{148(q+3(A+B)\lambda+1)^3+1}{2^{4\lambda}}.$$

Proof. This follows by a direct reduction to extractability of the commitment scheme (Definition 5.3). Indeed, let $\mathsf{Adv}_{\mathsf{Commit}}$ be the machine that runs Hyb_0 until R^* outputs its message, which includes $\{c_i\}_{i\in[n]}$. Let $\mathsf{Adv}_{\mathsf{Open}}$ be the machine that takes as input the rest of the state of Hyb_0, which includes T and the openings $\{(r_{i,0}, r_{i,1}, \theta_i), u_i\}_{i\in[T]}$, and outputs T and these openings. Let D be the machine that runs the rest of Hyb_0 and outputs a bit.

Then, the bound follows from plugging in $\lambda_{\mathsf{com}} = 4\lambda$ and $n = 3(A+B)\lambda$ (the number of bits committed) to the bound from Theorem 5.5.

□

Claim 6.4. *For any $q \geq 4$, when E is the XOR extractor and $A = 50$, $B = 100$, or when E is the ROM extractor and $A = 1050, B = 2160$,*

$$|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{8q^{3/2}}{2^\lambda}.$$

Proof. First, note that the only difference between these hybrids is that in Hyb_2, the m_{1-b} received by D as part of the sender's output is sampled uniformly at random (by the ideal functionality), where b is defined as $\mathsf{maj}\{\theta_i^* \oplus d_i\}_{i\in\overline{T}}$. Now, we introduce some notation.

- Let $\mathbf{c} \coloneqq (c_1, \ldots, c_n)$ be the classical commitments.
- Write the classical extracted values $\{(r_{i,0}^*, r_{i,1}^*, \theta_i^*)\}_{i\in[n]}$ as

$$\mathbf{R}^* \coloneqq \begin{bmatrix} r_{1,0}^* & \cdots & r_{n,0}^* \\ r_{1,1}^* & \cdots & r_{n,1}^* \end{bmatrix}, \boldsymbol{\theta}^* \coloneqq \begin{bmatrix} \theta_1^* & \cdots & \theta_n^* \end{bmatrix}.$$

- Given any $\mathbf{R}, \boldsymbol{\theta} \in \{0,1\}^{2\times n}$, define $|\mathbf{R}_{\boldsymbol{\theta}}\rangle$ as a state on n two-qubit registers, where register i contains the vector $|\mathbf{R}_{i,0}, \mathbf{R}_{i,1}\rangle$ prepared in the $(\boldsymbol{\theta}_i, \boldsymbol{\theta}_i)$-basis.
- Given $\mathbf{R}, \mathbf{R}^* \in \{0,1\}^{2\times n}$ and a subset $T \subset [n]$, define $\mathbf{R}_T$ to be the columns of $\mathbf{R}$ indexed by T, and define $\Delta(\mathbf{R}_T, \mathbf{R}_T^*)$ as the fraction of columns $i \in T$ such that $(\mathbf{R}_{i,0}, \mathbf{R}_{i,1}) \neq (\mathbf{R}_{i,0}^*, \mathbf{R}_{i,1}^*)$.
- For $T \subset [n]$, let $\overline{T} \coloneqq [n] \setminus T$.
- Given $\mathbf{R}^*, \boldsymbol{\theta}^* \in \{0,1\}^{2\times n}$, $T \subseteq [n]$, and $\delta \in (0,1)$, define

$$\Pi^{\mathbf{R}^*,\boldsymbol{\theta}^*,T,\delta} \coloneqq \sum_{\mathbf{R}:\mathbf{R}_T=\mathbf{R}_T^*, \Delta\left(\mathbf{R}_{\overline{T}}, \mathbf{R}_{\overline{T}}^*\right)\geq\delta} |\mathbf{R}_{\boldsymbol{\theta}^*}\rangle\langle\mathbf{R}_{\boldsymbol{\theta}^*}|.$$

  Intuitively, this is a projection onto "bad" states as defined by $\mathbf{R}^*, \boldsymbol{\theta}^*, T, \delta$, i.e., states that agree with $\mathbf{R}^*$ on all registers T but are at least δ-"far" from $\mathbf{R}^*$ on registers $\overline{T}$.

Now, consider the following projection, which has hard-coded the description of H_{FS}:

$$\Pi_{\mathsf{bad}}^{\delta} \coloneqq \sum_{\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*} |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes |\mathbf{R}^*, \boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*, \boldsymbol{\theta}^*|_{\mathcal{Z}} \otimes \Pi_{\mathcal{S}}^{\mathbf{R}^*,\boldsymbol{\theta}^*,H_{FS}(\mathbf{c}),\delta},$$

where $\mathcal{C}$ is the register holding the classical commitments, $\mathcal{Z}$ is the register holding the output of $\mathsf{SimExt.Ext}$, and $\mathcal{S}$ is the register holding the sender's halves of EPR pairs.

SubClaim 6.5. *Let*

$$\tau := \sum_{\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*} p^{(\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)}\, \tau^{(\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)},$$

where

$$\tau^{(\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)} = |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes |\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*|_{\mathcal{Z}} \otimes \rho_{\mathcal{S},\mathcal{X}}^{(\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)}$$

is the entire state of the system, including the sender's halves of EPR pairs and the receiver's entire state in Hyb_1 *(equivalently also* Hyb_2*) at the point in the experiment that is right after* R^* *outputs its message and* $\mathsf{SimExt.Ext}$ *is run. Here, each* $p^{(\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)}$ *is the probability that the registers* $\mathcal{C},\mathcal{Z}$ *holds the classical string* $\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*$*,* $\mathcal{S}$ *is the register holding the sender's halves of EPR pairs, and* $\mathcal{X}$ *is a register holding the remaining state of the system, which includes the rest of the receiver's classical message and its private state. Then,*

- *If* $A = 50, B = 100$*, then* $\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{0.25}\tau\right) \leq \frac{64q^3}{2^{2\lambda}}$.
- *If* $A = 1050, B = 2160$*, then* $\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{0.054}\tau\right) \leq \frac{64q^3}{2^{2\lambda}}$.

Proof. Define $\mathsf{Adv}_{\mathsf{R}^*}^{H_{FS}}$ to be the oracle machine that runs Hyb_1 until R^* outputs $\mathbf{c}$ (and the rest of its message), then runs $\mathsf{SimExt.Ext}$ to obtain $|\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*|$, and then outputs the remaining state $\rho_{\mathcal{S},\mathcal{X}}$. Consider running the measure-and-reprogram simulator $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ from Imported Theorem 3.5, which simulates H_{FS} queries, measures and outputs $\mathbf{c}$, then receives a uniformly random subset $T \subset [n]$ of size k, and then continues to run $\mathsf{Adv}_{\mathsf{R}^*}$ until it outputs $|\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*| \otimes \rho_{\mathcal{S},\mathcal{X}}$. Letting

$$\Pi_{\mathsf{bad}}^{\delta}[T] := \sum_{\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*} |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes |\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*|_{\mathcal{Z}} \otimes \Pi_{\mathcal{S}}^{\mathbf{R}^*,\boldsymbol{\theta}^*,T,\delta},$$

for $T \subset [n]$, Imported Theorem 3.5 implies that

$$\begin{aligned}
&\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{\delta}\tau\right) \\
&\quad \leq (2q+1)^2\, \mathbb{E}\left[\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{\delta}[T]\sigma\right) : \begin{array}{r}(\mathbf{c},\mathsf{st}) \leftarrow \mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}] \\ T \leftarrow S_{n,k} \\ (\mathbf{R}^*,\boldsymbol{\theta}^*,\rho_{\mathcal{S},\mathcal{X}}) \leftarrow \mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}](T,\mathsf{st})\end{array}\right],
\end{aligned}$$

where

$$\sigma = |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes |\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*|_{\mathcal{Z}} \otimes \rho_{\mathcal{S},\mathcal{X}},$$

and $S_{n,k}$ is the set of all subsets of $[n]$ of size k.

Now, recall that the last thing that $\mathsf{Adv}_{\mathsf{R}^*}$ does in Hyb_1 is run $\mathsf{SimExt.Ext}$ on $\mathbf{c}$ to obtain $(\mathbf{R}^*,\boldsymbol{\theta}^*)$. Consider instead running $\mathsf{SimExt.Ext}$ on $\mathbf{c}$ immediately after $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ outputs $\mathbf{c}$. Note that $\mathsf{SimExt.Ext}$ only operates on the register holding $\mathbf{c}$ and its own private state used for simulating H_C, so since com has a $\frac{8}{2^{\lambda_{\mathsf{com}}/2}}$-commuting simulator (Definition 5.3), we have that,

$$
\begin{aligned}
&\mathrm{Tr}\left(\Pi^{\delta}_{\mathsf{bad}}\tau\right)\\
&\leq (2q+1)^2\left(\mathbb{E}\left[\mathrm{Tr}\left(\Pi^{\delta}_{\mathsf{bad}}[T]\sigma\right):\begin{array}{r}(\mathbf{c},\mathsf{st})\leftarrow\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]\\(\mathbf{R}^*,\boldsymbol{\theta}^*)\leftarrow\mathsf{SimExt.Ext}(\mathbf{c})\\T\leftarrow S_{n,k}\\\rho_{\mathcal{S},\mathcal{X}}\leftarrow\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}](T,\mathsf{st})\end{array}\right]+\frac{8q}{2^{2\lambda}}\right)\\
&:= (2q+1)^2\epsilon+\frac{8q(2q+1)^2}{2^{2\lambda}},
\end{aligned}
$$

where

$$\sigma = |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{B}}\otimes|\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*|_{\mathcal{Z}}\otimes\rho_{\mathcal{S},\mathcal{X}},$$

and where we denote the expectation inside the parantheses by ϵ, and we plugged in $\lambda_{\mathsf{com}} = 4\lambda$.

Towards bounding ϵ, we now consider the following quantum sampling game.

- Fix a state on register $\mathcal{S}$ (and potentially other registers of arbitrary size), where $\mathcal{S}$ is split into n registers $\mathcal{S}_1,\ldots,\mathcal{S}_n$ of dimension 4, and fix $\mathbf{R}^*,\boldsymbol{\theta}^*\in\{0,1\}^{2\times n}$.
- Sample $T\subset[n]$ as a uniformly random subset of size k.
- For each $i\in T$, measure registers $\mathcal{S}_i$ in the $(\boldsymbol{\theta}^*_i,\boldsymbol{\theta}^*_i)$-basis to obtain a matrix $\mathbf{R}_T\in\{0,1\}^{2\times|T|}$, and output $\Delta(\mathbf{R}_T,\mathbf{R}^*_T)$.

Next, we argue that ϵ is bounded by the quantum error probability $\epsilon^{\delta}_{\mathsf{quantum}}$ (Definition 3.11) of the above game. This corresponds to the trace distance between the initial state on register $\mathcal{S}$ and an "ideal" state (as defined in Definition 3.11). This ideal state is supported on vectors $|\mathbf{R}_{\boldsymbol{\theta}^*}\rangle$ such that $\Delta(\mathbf{R}_{\overline{T}},\mathbf{R}^*_{\overline{T}})<\Delta(\mathbf{R}_T,\mathbf{R}^*_T)+\delta$. In particular, for any $|\mathbf{R}_{\boldsymbol{\theta}^*}\rangle$ with $\Delta(\mathbf{R}_T,\mathbf{R}^*_T)=0$ in the support of the ideal state, it holds that $\Delta(\mathbf{R}_{\overline{T}},\mathbf{R}^*_{\overline{T}})<\delta$. Thus, this ideal state is orthogonal to the subspace $\Pi^{\mathbf{R}^*,\boldsymbol{\theta}^*,T,\delta}_{\mathcal{S}}$, and so it follows that ϵ is bounded by $\epsilon^{\delta}_{\mathsf{quantum}}$.

Thus, by Imported Theorem 3.12, ϵ is then bounded by $\sqrt{\epsilon^{\delta}_{\mathsf{classical}}}$, where $\epsilon^{\delta}_{\mathsf{classical}}$ is the *classical* error probability (Definition 3.10) of the following sampling game.

- Let $\mathbf{R}\in\{0,1\}^{2\times n}$ be an arbitrary matrix.
- Sample a uniformly random subset $T\subset[n]$ of size k.
- Let δ^* be the fraction of columns $(\mathbf{R}_{i,0},\mathbf{R}_{i,1})$ for $i\in T$ that are non-zero, and output δ^*.

The classical error of the above game is the probability that $\geq\delta^*+\delta$ of the columns $(\mathbf{R}_{i,0},\mathbf{R}_{i,1})$ for $i\in\overline{T}$ are non-zero. Using the analysis in Appendix D.2, we can bound this probability by $2\exp\left(-2(1-k/n)^2\delta^2k\right)$.

- For $\delta=0.25$, this probability is bounded by

$$2\exp\left(-2(0.25)^2(1-A/(A+B))^2A\right)<2^{-4\lambda-1},$$

for $A=50, B=100$. Thus, we can bound $\epsilon^{\delta}_{\mathsf{classical}}$ by $2/2^{4\lambda}$ and thus ϵ by $\sqrt{2}/2^{2\lambda}$.

- For $\delta = 0.054$, this probability is bounded by

$$2\exp\left(-2(0.054)^2(1-A/(A+B))^2 A\right) < 2^{-4\lambda-1},$$

for $A = 1050, B = 2160$. Thus, we can bound $\epsilon_{\mathsf{classical}}$ by $2/2^{4\lambda}$ and thus ϵ by $\sqrt{2}/2^{2\lambda}$.

Summarizing, we have that in either case,

$$\mathrm{Tr}\left(\Pi^{\delta}_{\mathsf{bad}}\tau\right) \leq \frac{\sqrt{2}(2q+1)^2 + 8q(2q+1)^2}{2^{2\lambda}} \leq \frac{64q^3}{2^{2\lambda}},$$

for $q \geq 4$.

□

Thus, by gentle measurement (Lemma 3.1), the τ defined in SubClaim 6.5 is within $\frac{8q^{3/2}}{2^{\lambda}}$ trace distance of a state τ_{good} in the image of $\mathbb{I} - \Pi^{0.25}_{\mathsf{bad}}$ if $A = 50, B = 100$ and in the image of $\mathbb{I} - \Pi^{0.054}_{\mathsf{bad}}$ if $A = 1050, B = 2160$.

For readability, we note that

$$\mathbb{I} - \Pi^{\delta}_{\mathsf{bad}} = \sum_{\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*} |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes |\mathbf{R}^*,\boldsymbol{\theta}^*\rangle\langle\mathbf{R}^*,\boldsymbol{\theta}^*|_{\mathcal{Z}} \otimes \left(\mathbb{I} - \Pi^{\mathbf{R}^*,\boldsymbol{\theta}^*,H_{FS}(\mathbf{c}),\delta}\right)_{\mathcal{S}},$$

where for any T,

$$\mathbb{I} - \Pi^{\mathbf{R}^*,\boldsymbol{\theta}^*,T,\delta} = \sum_{\mathbf{R}:(\mathbf{R}_T \neq \mathbf{R}^*_T)\vee(\Delta(\mathbf{R}_{\overline{T}},\mathbf{R}^*_{\overline{T}})<\delta)} |\mathbf{R}_{\boldsymbol{\theta}^*}\rangle\langle\mathbf{R}_{\boldsymbol{\theta}^*}|.$$

We require the following two sub-claims to complete the proof of Claim 6.4.

SubClaim 6.6. *If E is the XOR extractor, then conditioned on τ being in the image of $\mathbb{I} - \Pi^{0.25}_{\mathsf{bad}}$, it holds that*

$$\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1].$$

Proof. First note that if the T sent by R^* to the sender is not equal to $H_{FS}(\mathbf{c})$, then the sender will abort, and the hybrids are perfectly indistinguishable. So it suffices to analyze the state τ conditioned on the register that contains T being equal to $H_{FS}(\mathbf{c})$.

Now, if τ is in $\mathbb{I} - \Pi^{0.25}_{\mathsf{bad}}$, it must be the case that the register $\mathcal{S}$ is in the image of $\mathbb{I} - \Pi^{\mathbf{R}^*,\boldsymbol{\theta}^*,T,0.25}$, where $\mathbf{R}^*, \boldsymbol{\theta}^*$ were output by $\mathsf{SimExt.Ext}$. Recall that the sender aborts if the positions measured in T are not equal to $\mathbf{R}^*_T$, and in this case the hybrids would be perfectly indistinguishable. Thus, we can condition on the sender not aborting, which, by the definition of $\mathbb{I} - \Pi^{\mathbf{R}^*,\boldsymbol{\theta}^*,T,0.25}$ implies that register $\mathcal{S}_{\overline{T}}$ is supported on vectors $\left|(\mathbf{R}_{\overline{T}})_{\boldsymbol{\theta}^*}\right\rangle$ such that $\Delta(\mathbf{R}_{\overline{T}}, \mathbf{R}^*_{\overline{T}}) < 0.25$.

Now, to obtain m_{1-b}, the sender measures register $\mathcal{S}_{i,d_i\oplus b\oplus 1}$ in basis $d_i \oplus b \oplus 1$ for each $i \in \overline{T}$ to obtain a string $r' \in \{0,1\}^{n-k}$. Then, m_{1-b} is set to $E(r')$. Since b is defined as $\mathsf{maj}\{\boldsymbol{\theta}^*_i \oplus d_i\}_{i\in\overline{T}}$ in Hyb_2, at least $(n-k)/2$ of the bits r'_i are obtained by measuring in $1 \oplus \boldsymbol{\theta}^*_i$. Let $M \subset \overline{T}$ be this set of size at least $(n-k)/2$, and define $\mathbf{r}^* \in \{0,1\}^n$ such that $\mathbf{r}^*_i = \mathbf{R}^*_{i,d_i\oplus b\oplus 1}$. We know from above that the register $\mathcal{S}_M$ is supported on vectors $|(\mathbf{r}_M)_{\boldsymbol{\theta}^*}\rangle$ for $\mathbf{r}_M$ such that $\Delta(\mathbf{r}_M, \mathbf{r}^*_M) < 0.5$. Thus, recalling that each of these states is measured in the basis $1 \oplus \boldsymbol{\theta}^*_i$, we can appeal to Theorem 4.1 (with an appropriate change of basis) to show that m_{1-b} is perfectly uniformly random from R^*'s perspective, completing the proof.

□

SubClaim 6.7. *If E is the ROM extractor and $B \geq 326, q \geq 4$, then conditioned on τ being in the image of $\mathbb{I} - \Pi_{\mathsf{bad}}^{0.054}$, it holds that*

$$|\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{4q}{2^\lambda}.$$

Proof. This follows the same argument as the above sub-claim, until we see that there are $(n-k)/2$ qubits of $\mathcal{S}$ that are measured in basis $1 \oplus \boldsymbol{\theta}^*_M$, and that the state on these qubits is supported on vectors $|(\mathbf{r}_M)_{\boldsymbol{\theta}^*}\rangle$ for $\mathbf{r}_M$ such that $\Delta(\mathbf{r}_M, \mathbf{r}^*_M) < 0.108$. We can then apply Theorem 4.2 with random oracle input size $n-k$, register $\mathcal{X}$ size $(n-k)/2$, and $|L| \leq 2^{h_b(0.108)(n-k)/2}$. Note that, when applying this theorem, we are fixing any outcome of the $(n-k)/2$ bits of the random oracle input that are measured in $\boldsymbol{\theta}^*$, and setting register $\mathcal{X}$ to contain the $(n-k)/2$ registers that are measured in basis $1 \oplus \boldsymbol{\theta}^*$. This gives a bound of

$$\frac{4q 2^{h_b(0.108)(n-k)/2}}{2^{(n-k)/4}} = \frac{4q}{2^{(n-k)(\frac{1}{4} - \frac{1}{2}h_b(0.108))}} = \frac{4q}{2^{B\lambda(\frac{1}{4} - \frac{1}{2}h_b(0.108))}} \leq \frac{4q}{2^\lambda},$$

for $B \geq 326$.

□

This completes the proof of Claim 6.4. □

Receiver security. Next, we show security against a malicious sender S^*. During the proof, we will use an efficient quantum random oracle "wrapper" algorithm $W[(x,z)]$ that provides an interface between any quantum random oracle simulator, such as the on-the-fly simulator (Imported Theorem 3.6), and the machine querying the random oracle. The wrapper will implement a controlled query to the actual random oracle simulator, controlled on the input $\mathcal{X}$ register not being equal to x. Then, it will implement a controlled query to a unitary that maps $|x,y\rangle \to |x, y \oplus z\rangle$, controlled on the input $\mathcal{X}$ register being equal to x. The effect of this wrapper is that the oracle presented to the machine is the oracle H simulated by the simulator, but with $H(x)$ reprogrammed to z.

$\mathsf{Sim}[\mathsf{S}^*]$:

- Query the ideal functionality with $\perp$ and obtain m_0, m_1.
- Sample T as a uniformly random subset of $[n]$ of size k, sample $d_i \leftarrow \{0,1\}$ for each $i \in \overline{T}$, and sample $\theta_i \leftarrow \{+, \times\}$ for each $i \in T$.
- For each $i \in [n]$, sample $r_{i,0}, r_{i,1} \leftarrow \{0,1\}$ and prepare BB84 states $|\psi_{i,0}\rangle, |\psi_{i,1}\rangle$ as follows.
  - If $i \in T$, set $|\psi_{i,0}\rangle = |r_{i,0}\rangle_{\theta_i}, |\psi_{i,1}\rangle = |r_{i,1}\rangle_{\theta_i}$.
  - If $i \in \overline{T}$, set $|\psi_{i,0}\rangle = |r_{i,0}\rangle_{+}, |\psi_{i,1}\rangle = |r_{i,1}\rangle_{\times}$.
- For each $i \in T$, let $e_i := (r_{i,0}, r_{i,1}, \theta_i)$ and for each $i \in \overline{T}$, let $e_i := (0,0,0)$. Compute $(\mathsf{st}, \{c_i\}_{i\in[n]}) \leftarrow \mathsf{Com}(\{e_i\}_{i\in[n]})$ and $\{u_i\}_{i\in T} \leftarrow \mathsf{Open}(\mathsf{st}, T)$.
- Set $x_0 := E(\{r_{i,d_i}\}_{i\in\overline{T}}) \oplus m_0$ and $x_1 := E(\{r_{i,d_i\oplus 1}\}_{i\in\overline{T}}) \oplus m_1$ (where if E is the ROM extractor, this is accomplished via classical queries to an on-the-fly random oracle simulator for H_{Ext}).

- Run S^* on input $(x_0, x_1), \{c_i\}_{i\in[n]}, T, \{r_{i,0}, r_{i,1}, \theta_i, u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$, $\{|\psi_{i,b}\rangle\}_{i\in[n],b\in\{0,1\}}$. Answer H_C queries using the on-the-fly random oracle simulator, answer H_{FS} queries using the on-the-fly random oracle simulator wrapped with $W[\{c_i\}_{i\in[n]}, T]$, and if E is the ROM extractor, answer H_{Ext} queries using the on-the-fly random oracle simulator. Output S^*'s final state and continue to answering the distinguisher's random oracle queries.

Now, given a receiver input $b \in \{0,1\}$, and distinguisher D such that S^* and D make a total of at most q queries combined to H_{FS} and H_C (and H_{Ext}), consider the following sequence of hybrids.

- Hyb_0: The result of the real interaction between $\mathsf{R}(b)$ and S^*. Using the notation of Definition 3.2, this is a distribution over $\{0,1\}$ desrcibed by $\Pi[\mathsf{S}^*, \mathsf{D}, b]$.
- Hyb_1: This is the same as the previous hybrid except that T is sampled uniformly at random as in the simulator, and H_{FS} queries are answered with the wrapper $W[(\{c_i\}_{i\in[n]}, T)]$.
- Hyb_2: This is the same as the previous hybrid except that the messages $\{(r_{i,0}, r_{i,1}, \theta_i)\}_{i\in\overline{T}}$ are replaced with $(0,0,0)$ inside the commitent.
- Hyb_3: The result of $\mathsf{Sim}[\mathsf{S}^*]$ interacting in $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[1]}}$ (or $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}$). Using the notation of Definition 3.2, this is a distribution over $\{0,1\}$ described by $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[1]}}[\mathsf{Sim}[\mathsf{S}^*], \mathsf{D}, b]$ (or $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}[\mathsf{Sim}[\mathsf{S}^*], \mathsf{D}, b]$).

The proof of security against a malicious S^* follows by combining the following three claims.

Claim 6.8.

$$\Pr[\mathsf{Hyb}_0 = 1] = \Pr[\mathsf{Hyb}_1 = 1].$$

Proof. These hybrids are identically distributed, since H_{FS} is a random oracle and T is uniformly random in Hyb_1. □

Claim 6.9.

$$|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{4q\sqrt{3(A+B)\lambda}}{2^{2\lambda}}.$$

Proof. This follows directly from the hiding of the commitment scheme (Definition 5.2), which is implied by its equivocality (see Section 5.1). To derive the bound, we plug in $\lambda_{\mathsf{com}} = 4\lambda$ and $n = 3(A+B)\lambda$ to the bound from Theorem 5.12. □

Claim 6.10.

$$\Pr[\mathsf{Hyb}_2 = 1] = \Pr[\mathsf{Hyb}_3 = 1].$$

Proof. First, note that one difference in how the hybrids are specified is that in Hyb_2, the receiver samples x_{1-b} uniformly at random, while in Hyb_3, x_{1-b} is set to $E(\{r_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}})\oplus m_{1-b}$. However, since m_{1-b} is sampled uniformly at random by the functionality, this is an equivalent distribution.

Thus, the only difference between these these hybrids is the basis in which the states on registers $\{\mathcal{S}_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}}$ are prepared (which are the registers $\{\mathcal{S}_{i,\theta_i\oplus 1}\}_{i\in\overline{T}}$ in Hyb_2). Indeed, note that in Hyb_2, the state on register $\mathcal{S}_{i,d_i\oplus b_i\oplus 1}$ is prepared by having the receiver measure their corresponding half of an EPR pair (register $\mathcal{R}_{i,d_i\oplus b_i\oplus 1}$) in basis $\theta_i = d_i \oplus b$, while in Hyb_3, this state is prepared by sampling a uniformly random bit and encoding it in the basis $d_i \oplus b_i \oplus 1$. However, these

sampling procedures both produce a maximally mixed state on register $\mathcal{S}_{i,d_i\oplus b\oplus 1}$, and thus these hybrids are equivalent.

□

This completes the proof of the theorem. □

6.2 Two-round OT without setup

In this section, we analyze a variant of the EPR-based protocol (Fig. 7) where we allow the sender to generate the EPR setup. That is, an honest sender will prepare $2n$ EPR pairs between registers $\mathcal{R}$ and $\mathcal{S}$, and send $\mathcal{R}$ to the reciever, while a malicious sender may prepare and send an arbitary state.

Thus, the resulting protocol is a two-round protocol without setup. We show that it securely realizes the $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$ OT ideal functionality, where the receiver can send chosen inputs (b, m) to the functionality and the functionality outputs to the sender random (m_0, m_1) such that $m_b = m$.

Theorem 6.11. *Consider instantiating the two-round variant of Protocol 7 with any non-interactive commitment scheme that is* correct *(Definition 5.1),* equivocal *(Definition 5.4), and* extractable *(Definition 5.3). Then the following hold.*

- *When instantiated with the XOR extractor, there exist constants A, B such that the two-round variant of Protocol 7 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{S-ROT}[1]}$.*
- *When instantiated with the ROM extractor, there exist constants A, B such that the two-round variant of Protocol 7 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$.*

Letting λ be the security parameter, q be an upper bound on the total number of random oracle queries made by the adversary, and using the commitment scheme from Section 5.2 with security parameter $\lambda_{\mathsf{com}} = 4\lambda$, the following hold.

- *When instantiatied with the XOR extractor and constants $A = 50$, $B = 100$, the two-round variant of Protocol 7 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$ with $\mu_{\mathcal{R}^*}$-security against a malicious receiver and $\mu_{\mathcal{S}^*}$-security against a malicious sender, where*

$$\mu_{\mathcal{R}^*} = \left(\frac{8q^{3/2}}{2^{\lambda}} + \frac{3600\lambda q}{2^{2\lambda}} + \frac{148(450\lambda + q + 1)^3 + 1}{2^{4\lambda}}\right), \mu_{\mathcal{S}^*} = \left(\frac{85\lambda^{1/2}q}{2^{2\lambda}}\right).$$

  This requires a total of $2(A + B)\lambda = 300\lambda$ EPR pairs.

- *When instantiated with the ROM extractor and constants $A = 1050$, $B = 2160$, the two-round variant of Protocol 7 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$ with $\mu_{\mathcal{R}^*}$-security against a malicious receiver and $\mu_{\mathcal{S}^*}$-security against a malicious sender, where*

$$\mu_{\mathcal{R}^*} = \left(\frac{8q^{3/2} + 4\lambda}{2^{\lambda}} + \frac{77040\lambda q}{2^{2\lambda}} + \frac{148(9630\lambda + q + 1)^3 + 1}{2^{4\lambda}}\right), \mu_{\mathcal{S}^*} = \left(\frac{197\lambda^{1/2}q}{2^{2\lambda}}\right).$$

  This requires a total of $2(A + B)\lambda = 6420\lambda$ EPR pairs.

Then, applying non-interactive bit OT reversal (Imported Theorem 3.3) to the protocol that realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$ immediately gives the following corollary.

Corollary 6.12. *Given a setup of 300λ shared EPR pairs, there exists a one-message protocol in the QROM that $O\left(\frac{q^{3/2}}{2^\lambda}\right)$-securely realizes $\mathcal{F}_{\mathsf{R-ROT}[1]}$.*

Proof. Security against a malicious receiver remains the same as Theorem 6.1, so we only show security against a malicious sender. Let S^* be a malicious sender. Let $(\mathsf{SimEqu.RO}, \mathsf{SimEqu.Com}, \mathsf{SimEqu.Open})$ be the equivocal simulator for the commitment scheme (Definition 5.4).

$\mathsf{Sim}[\mathsf{S}^*]$:

- Run S^*. Answer H_{FS} (and H_{Ext}) queries using the efficient on-the-fly random oracle simulator, and answer H_C queries using $\mathsf{SimEqu.RO}$. Eventually, S^* outputs a state on register $\mathcal{R} = (\mathcal{R}_{1,0}, \mathcal{R}_{1,1}, \ldots, \mathcal{R}_{n,0}, \mathcal{R}_{n,1})$.
- Query the ideal functionality with $\perp$ and obtain m_0, m_1.
- Run the following strategy on behalf of the receiver.
  - Compute $\{c_i\}_{i\in[n]} \leftarrow \mathsf{SimEqu.Com}$.
  - Compute $T = H_{FS}(c_1\| \ldots \|c_n)$ and parse T as a subset of $[n]$ of size k.
  - For each $i \in T$, sample $\theta \leftarrow \{+, \times\}$ and measure registers $\mathcal{R}_{i,0}$ and $\mathcal{R}_{i,1}$ in basis θ_i to obtain $r_{i,0}, r_{i,1}$.
  - Compute $\{u_i\}_{i\in T} \leftarrow \mathsf{SimEqu.Open}(\{r_{i,0}, r_{i,1}, \theta_i\}_{i\in T})$.
  - For each $i \in \overline{T}$, measure register $\mathcal{R}_{i,0}$ in basis $+$ and register $\mathcal{R}_{i,1}$ in basis $\times$ to obtain $r_{i,0}, r_{i,1}$.
  - For each $i \in \overline{T}$, sample $d_i \leftarrow \{0, 1\}$. Compute $x_0 \coloneqq E(\{r_{i,d_i}\}_{i\in\overline{T}}) \oplus m_0, x_1 \coloneqq E(\{r_{i,d_i\oplus 1}\}_{i\in\overline{T}}) \oplus m_1$.
- Send $(x_0, x_1), \{c_i\}_{i\in[n]}, T, \{(r_{i,0}, r_{i,1}, \theta_i), u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$ to S^*, and run S^* until it outputs a final state, answering H_{FS} (and H_{Ext}) queries using the efficient on-the-fly random oracle simulator and H_C queries using $\mathsf{SimEqu.RO}$. Output S^*'s final state.
- Answer the distinguisher's H_{FS} (and H_{Ext}) queries using the efficient on-the-fly random oracle simulator and H_C queries using $\mathsf{SimEqu.RO}$.

Now, given a distinguisher D such that S^* and D make a total of at most q queries combined to H_{FS} and H_C, and a receiver input (b, m_b), consider the following sequence of hybrids.

- Hyb_0: The result of the real interaction between S^* and R. Using the notation of Definition 3.2, this is a distribution over bits described by $\Pi[\mathsf{S}^*, \mathsf{D}, (b, m_b)]$.
- Hyb_1: Answer all H_C queries of S^* and D with $\mathsf{SimEqu.RO}$. Run the honest receiver strategy, except $\{c_i\}_{i\in[n]} \leftarrow \mathsf{SimEqu.Com}$, and $\{u_i\} \leftarrow \mathsf{SimEqu.Open}(\{(r_{i,0}, r_{i,1}, \theta_i)\}_{i\in T})$.
- Hyb_2: The result of $\mathsf{Sim}[\mathsf{S}^*]$ interacting in $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[1]}}$ (or $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}$). Using the notation of Definition 3.2, this is a distribution over bits described by $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[1]}}[\mathsf{Sim}[\mathsf{S}^*], \mathsf{D}, (b, m_b)]$ (or $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}[\mathsf{Sim}[\mathsf{S}^*], \mathsf{D}, (b, m_b)]$).

Claim 6.13.

$$|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]| \leq \frac{2q\sqrt{3(A+B)\lambda}}{2^{2\lambda}}.$$

Proof. This follows by a direct reduction to equivocality of the commitment scheme (Definition 5.4). Indeed, let $\mathsf{Adv}_{\mathsf{RCommit}}$ be the machine that runs Hyb_0 until S^* outputs its message on register $\mathcal{R}$ and R runs the **Measurement** portion of its honest strategy to produce $\{r_{i,0}, r_{i,1}, \theta_i\}_{i\in[n]}$. Let $\mathsf{Adv}_{\mathsf{ROpen}}$ be the machine computes $T = H_{FS}(c_1\| \ldots \|c_n)$. Let D be the machine that runs the rest of Hyb_0, from the **Reorientation** portion of its honest receiver's strategy to the final bit output by the distinguisher.

Then, plugging in $\lambda_{\mathsf{com}} = 4\lambda$ and $n = 3(A+B)\lambda$ to Theorem 5.12 gives the bound in the claim. □

Claim 6.14.

$$\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1].$$

Proof. First, note that one difference in how the hybrids are specified is that in Hyb_1, the receiver samples x_{1-b} uniformly at random, while in Hyb_2, x_{1-b} is set to $E(\{r_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}})\oplus m_{1-b}$. However, since m_{1-b} is sampled uniformly at random by the functionality, this is an equivalent distribution.

Then, the only difference between these these hybrids is the basis in which the states on registers $\{\mathcal{R}_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}}$ are measured (which are the registers $\{\mathcal{R}_{i,\theta_i\oplus 1}\}_{i\in\overline{T}}$ in Hyb_1). Indeed, since the resulting bits $r_{i,d_i\oplus b\oplus 1}$ are unused by the receiver in Hyb_1, and masked by m_{1-b} in Hyb_2, they are independent of the sender's view. Thus, measuring them in different bases has no effect on the sender's view, and so the hybrids are identical. □

This completes the proof of the claim, as desired. □

Protocol 7

Ingredients and parameters.

- Security parameter λ, and constants A, B. Let $n = (A+B)\lambda$ and $k = A\lambda$.
- A non-interactive extractable commitment scheme $(\mathsf{Com}, \mathsf{Open}, \mathsf{Rec})$, where commitments to 3 bits have size $\ell := \ell(\lambda)$.
- A random oracle $H_{FS} : \{0,1\}^{n\ell} \to \{0,1\}^{\lceil \log \binom{n}{k} \rceil}$.
- An extractor E with domain $\{0,1\}^{n-k}$ which is either
  - The XOR function, so $E(r_1, \ldots, r_{n-k}) = \bigoplus_{i \in [n-k]} r_i$.
  - A random oracle $H_{Ext} : \{0,1\}^{n-k} \to \{0,1\}^{\lambda}$.

Setup.

- $2n$ EPR pairs on registers $\{\mathcal{R}_{i,b}, \mathcal{S}_{i,b}\}_{i \in [n], b \in \{0,1\}}$, where the receiver has register $\mathcal{R} := \{\mathcal{R}_{i,b}\}_{i \in [n], b \in \{0,1\}}$ and the sender has register $\mathcal{S} := \{\mathcal{S}_{i,b}\}_{i \in [n], b \in \{0,1\}}$.

Protocol.

- **Receiver message.** R, on input $b \in \{0,1\}, m \in \{0,1\}^{\lambda}$, does the following.
  - **Measurement.** Sample $\theta_1 \theta_2 \ldots \theta_n \leftarrow \{+, \times\}^n$ and for $i \in [n]$, measure registers $\mathcal{R}_{i,0}, \mathcal{R}_{i,1}$ in basis θ_i to obtain $r_{i,0}, r_{i,1}$.
  - **Measurement check.**
    - Compute $\left(\mathsf{st}, \{c_i\}_{i \in [n]}\right) \leftarrow \mathsf{Com}\left(\{(r_{i,0}, r_{i,1}, \theta_i)\}_{i \in [n]}\right)$.
    - Compute $T = H_{FS}(c_1 \| \ldots \| c_n)$, parse T as a subset of $[n]$ of size k.
    - Compute $\{(r_{i,0}, r_{i,1}, \theta_i), u_i\}_{i \in [T]} \leftarrow \mathsf{Open}(\mathsf{st}, T)$.
  - **Reorientation.** Let $\overline{T} = [n] \setminus T$, and for all $i \in \overline{T}$, set $d_i = b \oplus \theta_i$ (interpreting $+$ as 0, $\times$ as 1).
  - **Sampling.** Set $x_b = E\left(\{r_{i,\theta_i}\}_{i \in \overline{T}}\right) \oplus m$, and sample $x_{1-b} \leftarrow \{0,1\}^{\lambda}$.
  - **Message.** Send to S

$$(x_0, x_1), \{c_i\}_{i \in [n]}, T, \{r_{i,0}, r_{i,1}, \theta_i, u_i\}_{i \in [T]}, \{d_i\}_{i \in \overline{T}}.$$

- **Sender computation.** S does the following.
  - **Check Receiver Message.** Abort if any of the following fails.
    - Check that $T = H_{FS}(c_1 \| \ldots \| c_n)$.
    - Check that $\mathsf{Rec}(\{c_i\}_{i \in T}, \{(r_{i,0}, r_{i,1}, \theta_i), u_i\}_{i \in T}) \neq \perp$.
    - For every $i \in T$, measure the registers $\mathcal{S}_{i,0}, \mathcal{S}_{i,1}$ in basis θ_i to obtain $r'_{i,0}, r'_{i,1}$, and check that $r_{i,0} = r'_{i,0}$ and $r_{i,1} = r'_{i,1}$.
  - **Output.** For all $i \in \overline{T}$, measure the register $\mathcal{S}_{i,0}$ in basis $+$ and the register $\mathcal{S}_{i,1}$ in basis $\times$ to obtain $r'_{i,0}, r'_{i,1}$. Output

$$m_0 := x_0 \oplus E\left(\{r'_{i,d_i}\}_{i \in \overline{T}}\right), m_1 := x_1 \oplus E\left(\{r'_{i,d_i \oplus 1}\}_{i \in \overline{T}}\right).$$

Figure 7: Non-interactive random-sender-input OT in the shared EPR pair model.

7 The fixed basis framework: OT without entanglement or setup

In Fig. 8, we formalize our 3 round chosen-input OT protocol that does not rely on entanglement or setup.

Theorem 7.1. *Instantiate Protocol 8 with any non-interactive commitment scheme that is* extractable *(Definition 5.3) and* equivocal *(Definition 5.4). Then there exist constants A, B such that Protocol 8 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{OT}[\lambda]}$.*

Furthermore, letting λ be the security parameter, q be an upper bound on the total number of random oracle queries made by the adversary, and using the commitment scheme from Section 5.2 with security parameter $\lambda_{\mathsf{com}} = 4\lambda$, for constants $A = 11\ 700, B = 30\ 400$, Protocol 8 securely realizes $\mathcal{F}_{\mathsf{OT}[\lambda]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where

$$\mu_{\mathsf{R}^*} = \frac{3\sqrt{10}q^{3/2}}{2^{\lambda}} + \frac{1}{2^{5\lambda}} + \frac{148(q+126300\lambda+1)^3+1}{2^{4\lambda}} + \frac{1010400q\lambda}{2^{2\lambda}}, \quad \mu_{\mathsf{S}^*} = \left(\frac{712q\lambda^{1/2}}{2^{2\lambda}}\right).$$

This requires a total of $2(A+B)\lambda = 84\ 200\lambda$ BB84 states.

Proof. We begin by proving security against malicious senders below.

Receiver security

We now describe a simulator Sim that simulates the view of an arbitrary malicious sender S^*. Sim will answer random oracle queries to H using SimEqu.RO, the random oracle simulator for the commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$. Additionally, the queries to H_{FS} will be simulated using an efficient on-the-fly random oracle simulator $\mathsf{Sim}_{\mathsf{RO}}$.RO as mentioned in Imported Theorem 3.6.

The Simulator. $\mathsf{Sim}[\mathsf{S}^*]$ does the following.

1. Receive $\{|\psi\rangle\}_{i\in[n]}$ from S^*.
2. Perform the following steps.
   - **Measurement Check Message.**
     - Compute $\left(\{c_i\}_{i\in[n]}\right) \leftarrow \mathsf{SimEqu.Com}$.
     - Compute $T = H_{FS}(c_1||\ldots||c_n)$ and parse T as a subset of $[n]$ of size k.
     - Perform (delayed) measurements on $\{|\psi\rangle\}_{i\in[n]}$ as follows:
       - Sample $\widehat{\theta} \leftarrow \{0,1\}^n$.
       - For all $i \in T$, measure the i^{th} pair of qubits in basis $\widehat{\theta}_i$ to obtain $\widehat{r}_i^{\,0}, \widehat{r}_i^{\,1}$.
       - For all $i \in \overline{T}$, measure the first qubit of $|\psi\rangle_i$ in the computational basis and the second qubit in the Hadamard basis to obtain $\widehat{r}_i^{\,0}, \widehat{r}_i^{\,1}$ respectively.
     - Compute $\{u_i\}_{i\in[n]} \leftarrow \mathsf{SimEqu.Open}(\{(\widehat{r}_i^{\,0}, \widehat{r}_i^{\,1}, \widehat{\theta}_i)\}_{i\in[n]})$.
   - **Reorientation.** Let $\overline{T} = [n] \setminus T$, and for all $i \in \overline{T}$, set $d_i = \widehat{\theta}_i$.
   - **Message.** Send to S
   $$\{c_i\}_{i\in[n]}, T, \{\widehat{r}_i^{\,0}, \widehat{r}_i^{\,1}, \widehat{\theta}_i, u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}.$$

Protocol 8

Ingredients / parameters / notation.

- Security parameter λ and constants A, B. Let $k = A\lambda, n = (A+B)\lambda$.
- For classical bits (x, θ), let $|x\rangle_\theta$ denote $|x\rangle$ if $\theta = 0$, and $(|0\rangle + (-1)^x |1\rangle)/\sqrt{2}$ if $\theta = 1$.
- A non-interactive extractable and equivocal commitment $(\mathsf{Com}, \mathsf{Open}, \mathsf{Rec})$, where commitments to 3 bits have size $\ell := \ell(\lambda)$.
- A random oracle $H_{FS} : \{0,1\}^{n\ell} \to \{0,1\}^{\lceil \log \binom{n}{k} \rceil}$, and a universal hash function family $h : \{0,1\}^{p(\lambda)} \times \{0,1\}^{\leq B\lambda} \to \{0,1\}^\lambda$.

Sender Input: Messages $m_0, m_1 \in \{0,1\}^\lambda$. **Receiver Input:** Choice bit b.

1. **Sender Message.** S samples strings $r^0 \leftarrow \{0,1\}^n, r^1 \leftarrow \{0,1\}^n$, a random subset $U \subset [n]$ of size k, and for $i \in U$, it samples $b_i \leftarrow \{0,1\}$ uniformly at random. It computes state $|\psi\rangle = |\psi\rangle_1 \dots |\psi\rangle_n$ as follows, and sends it to R: for $i \in U$, $|\psi\rangle_i = (|r_i^0\rangle_{b_i}, |r_i^1\rangle_{b_i})$ and for $i \in [n] \setminus U$, $|\psi\rangle_i = (|r_i^0\rangle_0, |r_i^1\rangle_1)$.
2. **Receiver Message.** R does the following.
   - Choose $\widehat{\theta} \leftarrow \{0,1\}^n$ and measure the i^{th} pair of qubits in basis $\widehat{\theta}_i$ to obtain $\widehat{r}_i^0, \widehat{r}_i^1$.
   - **Measurement Check Message.**
     - Compute $\left(\mathsf{st}, \{c_i\}_{i\in[n]}\right) \leftarrow \mathsf{Com}\left(\{(\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i)\}_{i\in[n]}\right)$.
     - Compute $T = H_{FS}(c_1 || \dots || c_n)$ and parse T as a subset of $[n]$ of size k.
     - Compute $\{(\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i), u_i\}_{i\in T} \leftarrow \mathsf{Open}(\mathsf{st}, T)$.
   - **Reorientation.** Let $\overline{T} := [n] \setminus T$, and for all $i \in \overline{T}$, set $d_i = b \oplus \widehat{\theta}_i$.
   - **Message.** Send to S the values $\{c_i\}_{i\in[n]}, T, \{\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i, u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$.
3. **Sender Message.** S does the following.
   - **Check Receiver Message.** S aborts if any of these checks fail:
     - Check that $T = H_{FS}(c_1 || \dots || c_n)$.
     - Check that $\mathsf{Rec}(\{c_i\}_{i\in T}, T, \{(\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i), u_i\}_{i\in T}) \neq \perp$.
     - For every $i \in T \cap U$ such that $\widehat{\theta}_i = b_i$, check that $\widehat{r}_i^0 = r_i^0$ and $\widehat{r}_i^1 = r_i^1$.
   - **Message.** Sample $s \leftarrow \{0,1\}^{p(\lambda)}$, let R_β denote the concatenation of $\{r_i^{d_i \oplus \beta}\}_{i\in\overline{T}\setminus U}$ and send to R the values $(s, U, ct_0 = m_0 \oplus h(s, R_0), ct_1 = m_1 \oplus h(s, R_1))$.
4. **Receiver Output.** Output $m_b = ct_b \oplus h(s, R)$ where R is the concatenation $\{\widehat{r}_i^{\widehat{\theta}_i}\}_{i\in\overline{T}\setminus U}$.

Figure 8: Three-round chosen-input OT without entanglement

3. Upon receiving (s, U, ct_0, ct_1) from S^*,

   - Set R_0 to be the concatenation $\{\widehat{r_i}^{\widehat{\theta}_i}\}_{i\in\overline{T}\setminus U}$ and R_1 to be the concatenation of $\{\widehat{r_i}^{\widehat{\theta}_i\oplus 1}\}_{i\in\overline{T}\setminus U}$.
   - Compute $\widehat{m_0} := ct_0 \oplus h(s, R_0)$, $\widehat{m_1} := ct_1 \oplus h(s, R_1)$, and send $\widehat{m_0}, \widehat{m_1}$ to the ideal functionality.

Analysis. Fix any adversary $\{\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, b_\lambda\}_{\lambda\in\mathbb{N}}$, where S^*_λ is a QIOM that corrupts the sender, D_λ is a QOM, and b_λ is the input of the honest receiver. For any receiver input $b_\lambda \in \{0,1\}$ consider the random variables $\Pi[\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, b_\lambda]$ and $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{OT}[\lambda]}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, b_\lambda]$ according to Definition 3.2 for the protocol in Figure 8. Let $q(\cdot)$ denote an upper bound on the combined number of queries of S^*_λ and D_λ. We will show that :

$$\left|\Pr[\Pi[\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, b_\lambda] = 1] - \Pr\left[\widetilde{\Pi}_{\mathcal{F}_{\mathsf{OT}[\lambda]}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, b_\lambda] = 1\right]\right| = \mu(\lambda, q(\lambda)).$$

This is done via a sequence of hybrids, as follows:

- Hyb_0 : The output of this hybrid is the *real* distribution $\Pi[\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, b_\lambda]$.
- Hyb_1: The output of this hybrid is the same as the previous hybrid except that the challenger uses switches H_{FS} with an efficient on-the-fly random oracle simulator $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ as mentioned in Imported Theorem 3.6.
- Hyb_2 : The output of this hybrid is the same as the previous hybrid except that instead of running $(\mathsf{Com}, \mathsf{Open})$, the challenger uses $(\mathsf{SimEqu.RO}, \mathsf{SimEqu.Com}, \mathsf{SimEqu.Open})$ to prepare their commitments. It answers any random oracle queries to H_C by calling $\mathsf{SimEqu.RO}$ instead.
- Hyb_3 : The output of this hybrid is the same as the previous hybrid except that the measurement of $\{|\psi\rangle_i\}_{i\in[n]}$ on behalf of R is done after computing set T and before invoking $\mathsf{SimEqu.Open}$ on the measured values.
- Hyb_4 : The output of this hybrid is the same as the previous hybrid except the following modification on behalf of R, for all $i \in \overline{T}$:
  - Sample $\widehat{\theta}_i \leftarrow \{0,1\}$
  - Measure the first qubit of $|\psi\rangle_i$ in the computational basis and the second qubit in the Hadamard basis. Let the outcomes be $\widehat{r}_i^0, \widehat{r}_i^1$ respectively.
- Hyb_5 : The output of this hybrid is the same as the previous hybrid except the following modification.
  - For $i \in \overline{T}$, set reorientation bit $d_i := \widehat{\theta}_i$.
  - After receiving the last sender message.
    * Set R_0 to be the concatenation $\{\widehat{r_i}^{\widehat{\theta}_i}\}_{i\in\overline{T}\setminus U}$ and R_1 to be the concatenation of $\{\widehat{r_i}^{\widehat{\theta}_i\oplus 1}\}_{i\in\overline{T}\setminus U}$.
    * Compute $\widehat{m_0} := ct_0 \oplus h(s, R_0)$, $\widehat{m_1} := ct_1 \oplus h(s, R_1)$, and send $\widehat{m_0}, \widehat{m_1}$ to the ideal functionality.

The output of this last hybrid is identical to the *ideal* distribution $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{OT}[\lambda]}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, b_\lambda]$.

We show that $|\Pr[\mathsf{Hyb}_5 = 1] - \Pr[\mathsf{Hyb}_0 = 1]| \leq \mu(\lambda, q(\lambda))$, where $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ is a $\mu(\lambda, q(\lambda))$-equivocal bit commitment scheme, where $\mu(\lambda, q, n_{\mathsf{com}}) = \frac{2qn_{\mathsf{com}}^{1/2}}{2^{\lambda_{\mathsf{com}}/2}}$ for the specific commitment scheme that we construct in Section 5.2, where n_{com} is the number of bit commitments and λ_{com} is the security parameter for the commitment scheme. Later, we will set $n_{\mathsf{com}} = c_1\lambda$ and $\lambda_{\mathsf{com}} = c_2\lambda$ for some fixed constants c_1, c_2. Thus μ will indeed be a function of λ and q. We now procced with the proof by arguing indistinguishability of each pair of consecutive hybrids in the sequence above.

Claim 7.2. $\Pr[\mathsf{Hyb}_0 = 1] = \Pr[\mathsf{Hyb}_1 = 1]$.

Proof. This follows from the indistinguishable simulation property of $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ as mention in the Imported Theorem 3.6. □

Claim 7.3. $|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \mu(\lambda, q(\lambda))$.

Proof. Suppose there exists an adversary Adv_λ corrupting S, a distinguisher D_λ, and a bit b such that,

$$\left|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]\right| > \mu(\lambda, q(\lambda))$$

We will build a reduction adversary $\{\mathsf{Adv}^*_\lambda = (\mathsf{Adv}_{\mathsf{RCommit},\lambda}, \mathsf{Adv}_{\mathsf{ROpen},\lambda}, \mathsf{D}^*_\lambda)\}_{\lambda\in\mathbb{N}}$ that makes at most $q(\lambda)$ queries to the random oracle, and contradicts the μ-equivocality of the commitment $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ as defined in Definition 5.4. In the following reduction, all random oracle queries to H_C will be answered by the equivocal commitment challenger whereas calls to H_{FS} will be simulated by Adv^*_λ by internally running $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$.

$\mathsf{Adv}_{\mathsf{RCommit},\lambda}$:

- Initalize the OT protocol with between honest receiver R and Adv corrupting S.
- Output intermediate state $\rho^*_{\lambda,1}$ representing the joint state of S and R along with the measurement information $\{(\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i)\}_{i\in[n]}$ computed by R.

The measurement information $\{(\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i)\}_{i\in[n]}$ is sent as messages to the reduction challenger which then returns a set of commitments $\{\mathsf{com}_i\}_{i\in[n]}$.

$\mathsf{Adv}_{\mathsf{ROpen},\lambda}(\rho^*_{\lambda,1}, \{\mathsf{com}_i\}_{i\in[n]})$: Use $\rho^*_{\lambda,1}$ to initialize the joint state of S and R, and output the new joint state $\rho^*_{\lambda,2}$ after R has computed T.

The challenger returns $\{u_i\}_{i\in[n]}$ which is then fed to the following distinguisher (along with the information $\{\mathsf{com}_i, (\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i)\}_{i\in[n]}$ from the aforementioned execution).

$\mathsf{D}^*_\lambda(\rho^*_{\lambda,2}, \{\mathsf{com}_i, (\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i), u_i\}_{i\in[n]})$:

- Use $\rho^*_{\lambda,2}$ to initialize the joint state of S and R. Run it until completion using $\{(\widehat{r}_i^0, \widehat{r}_i^1, \widehat{\theta}_i), u_i\}_{i\in T}$ as openings of R in the measurement check proof

- Let τ_λ^* be the final state of Adv and y^* be the output of R. Run $\mathsf{D}_\lambda(\tau_\lambda^*, y^*)$ and output the bit b returned by the distinguisher.

By construction, when the challenger executes $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C})$, the reduction will generate a distribution identical to Hyb_1. Similarly, when the challenger executes $(\mathsf{SimEqu.Com}, \mathsf{SimEqu.Open})$, the reduction will generate a distribution identical to Hyb_2. Therefore, the reduction $\{\mathsf{Adv}_\lambda^* = (\mathsf{Adv}_{\mathsf{RCommit},\lambda}, \mathsf{Adv}_{\mathsf{ROpen},\lambda}, \mathsf{D}_\lambda^*)\}_{\lambda\in\mathbb{N}}$ directly contradicts the μ-equivocality of the underlying commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ as in Definition 5.4. □

Claim 7.4. $\Pr[\mathsf{Hyb}_2 = 1] = \Pr[\mathsf{Hyb}_3 = 1]$

Proof. The only difference in Hyb_3 from Hyb_2 is that we commute the measurement of $\{|\psi\rangle\}_{i\in[n]}$ past the invocation of SimEqu.Com and the computation of T. Since these two operators are applied to disjoint subsystems, this can be done without affecting the hybrid distribution. □

Claim 7.5. $\Pr[\mathsf{Hyb}_3 = 1] = \Pr[\mathsf{Hyb}_4 = 1]$

Proof. The only difference in Hyb_4 from Hyb_3 is the following. For all $i \in \overline{T}$: If $\widehat{\theta}_i = 0$, we measure the second qubit of $|\psi_i\rangle$ in the Hadamard basis (instead of the computational basis as defined in the previous hybrid). If $\widehat{\theta}_i = 1$, we measure the first qubit of $|\psi_i\rangle$ in computational basis (instead of the Hadamard basis as defined in the previous hybrid). But this doesn't affect the hybrid distribution because the values on these registers are not used anywhere in the hybrid and are eventually traced out. □

Claim 7.6. $\Pr[\mathsf{Hyb}_4 = 1] = \Pr[\mathsf{Hyb}_5 = 1]$

Proof. The only difference between these experiments is the way in which we define the output of honest receiver. Assuming the correctness of $\mathcal{F}_{\mathsf{OT}[\lambda]}$, the two hybrids are identical. In Hyb_4, the receiver's output is computed by the challenger as $\widehat{m_b} = ct_b \oplus h(s, ||_{i\in\overline{T}\setminus U} \widehat{r_i}^{\widehat{\theta}_i})$ (where $||_{i\in G} x_i$ denotes the concatenation of x_i for $i \in G$, in increasing order of i). In Hyb_5, the receiver's output is derived via the OT ideal functionality which receives sender's input strings $\widehat{m_0} := ct_0 \oplus h(s, ||_{i\in\overline{T}\setminus U} \widehat{r_i}^{\widehat{\theta}_i})$ and $\widehat{m_1} := ct_1 \oplus h(s, ||_{i\in\overline{T}\setminus U} \widehat{r_i}^{\widehat{\theta}_i\oplus 1})$ from the challenger and receiver choice bit b. The OT ideal functionality sends $\widehat{m_b} = ct_b \oplus h(s, ||_{i\in\overline{T}\setminus U} \widehat{r_i}^{\widehat{\theta}_i\oplus b})$ to the ideal receiver which it then outputs. Therefore for any fixing of the adversary's state and receiver choice bit, the two hybrids result in identical $\widehat{m_b}$. □

Combining all the claims, we get that $|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_5 = 1]| \leq \mu(\lambda, q(\lambda))$. Using Theorem 5.12 where we derived $\mu(\lambda, q, n_{\mathsf{com}}) = \frac{2qn_{\mathsf{com}}^{1/2}}{2^{\lambda_{\mathsf{com}}/2}}$ and plugging $\lambda_{\mathsf{com}} = 4\lambda$, $n_{\mathsf{com}} = 3n$ (as we are committing to 3 bits at a time) where $n = 42\ 100\lambda$ (this setting of n is the same as that needed in the sender security part of the proof), we get $\frac{712q\sqrt{\lambda}}{2^{2\lambda}}$ security against a malicious sender. □

Sender security

Let $\mathsf{SimExt} = (\mathsf{SimExt.RO}, \mathsf{SimExt.Ext})$ be the simulator for the extractable commitment scheme from Section 5. Let $+$ refer to the computational basis and $\times$ to the hadamard basis. Below we describe the simulator $\mathsf{Sim}[\mathsf{R}^*]$ against a malicious receiver R^* for Protocol 8.

$\mathsf{Sim}[\mathsf{R}^*]$:

- Initialize the on-the-fly random oracle simulator $\mathsf{Sim}_{\mathsf{RO}}$ from Imported Theorem 3.6. Run R^* answering its oracle queries to H_{FS} using $\mathsf{Sim}_{\mathsf{RO}}$ and queries to H_C using $\mathsf{SimExt.RO}$.
- Sample $2n$ EPR pairs on registers $\{(\mathcal{S}_{i,b}, \mathcal{R}_{i,b})\}_{i\in[n],b\in\{0,1\}}$ (where each $\mathcal{S}_{i,b}, \mathcal{R}_{i,b}$ is a 2-dimensional register). Send registers $\{\mathcal{R}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ to R^*.
- When R^* outputs $\{c_i\}_{i\in[n]}, T, \{(\widehat{r}_i^{\,0}, \widehat{r}_i^{\,1}, \widehat{\theta}_i), u_i\}_{i\in T}, \{d_i\}_{i\in\overline{T}}$, run $\{(\widetilde{r}_i^{\,0}, \widetilde{r}_i^{\,1}, \widetilde{\theta}_i)\}_{i\in[n]} \leftarrow \mathsf{SimExt.Ext}(\{c_i\}_{i\in[n]})$.
- Run the "check receiver message" part of the honest sender strategy, except do the following in place of the third check. If any of the checks fail, send abort to the ideal functionality, output R^*'s state and continue answering distinguisher's queries.
  - Sample subset $U \subset [n]$ of size k and for each $i \in [n]$, sample bit $b_i \in \{0,1\}$.
  - For each $i \in [n]$, do the following:
    - If $i \in U$, measure both registers $\mathcal{S}_{i,0}$ and $\mathcal{S}_{i,1}$ in basis $+$ when $b_i = 0$, and both in basis $\times$ when $b_i = 1$. Denote measurement outcomes from $\mathcal{S}_{i,0}$ and $\mathcal{S}_{i,1}$ by r_i^0 and r_i^1 respectively.
    - If $i \notin U$, then measure $\mathcal{S}_{i,0}$ in basis $+$ and $\mathcal{S}_{i,1}$ in basis $\times$ and denote outcomes by outcomes r_i^0, r_i^1 respectively.
  - For each $i \in T \cap U$ such that $\widetilde{\theta}_i = b_i$, check that $\widetilde{r}_i^{\,0} = r_i^0$ and $\widetilde{r}_i^{\,1} = r_i^1$.
- Set $b := \mathsf{maj}\{\widetilde{\theta}_i \oplus d_i\}_{i\in\overline{T}\setminus U}$ and send b to $\mathcal{F}_{\mathsf{OT}[\lambda]}$ to obtain m_b.
- Compute the last message using the honest sender strategy except for using $m_{1-b} := 0^\lambda$.
- Send R^* this last message, output the final state of R^* and terminate.
- Answer any queries of distinguisher to H_{FS} and H_C using $\mathsf{Sim}_{\mathsf{RO}}$ and $\mathsf{SimExt.RO}$ respectively.

Fix any distinguisher D and let q denote the total queries that R^*, D make to H_{FS} and H_C. Consider the following sequence of hybrids:

- Hyb_0: This is the real world interaction between R^* and S. Using the notation of Definition 3.2, this is a distribution over $\{0,1\}$ denoted by $\Pi[\mathsf{R}^*, \mathsf{D}, (m_0, m_1)]$.
- Hyb_1: This is the same as the previous hybrid, except the following are run instead to generate the first sender message: (1) Sample $2n$ EPR pairs on registers $\{(\mathcal{S}_{i,b}, \mathcal{R}_{i,b})\}_{i\in[n],b\in\{0,1\}}$. (2) Run the following algorithm:

  Algorithm Measure-EPR:
  - Sample subset $U \subset [n]$ of size k and for each $i \in [n]$, sample bit $b_i \in \{0,1\}$.
  - For each $i \in [n]$, do the following:
    - If $i \in U$, measure registers $\mathcal{S}_{i,0}$ and $\mathcal{S}_{i,1}$ in basis $+$ when $b_i = 0$, and in basis $\times$ when $b_i = 1$, to get outcomes r_i^0 and r_i^1 respectively.
    - If $i \notin U$, then measure $\mathcal{S}_{i,0}$ in basis $+$ and $\mathcal{S}_{i,1}$ in basis $\times$ to get outcomes r_i^0, r_i^1 respectively.

Thereafter, registers $\{\mathcal{R}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ are sent over to R^* and the rest of the experiment works as the previous hybrid.

- Hyb_2: This is the same previous hybrid, except that the sender does not perform any measurements before sending registers $\{\mathcal{R}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ to R^*, and delays running the algorithm Measure-EPR to just before executing the third check in "check receiver message" part of the honest sender strategy.

- Hyb_3: This is the same as the previous hybrid, except for the following changes: queries of R^* to H_C are now answered using $\mathsf{SimExt.RO}$. Once R^* outputs its second message, run $\{(\widetilde{r}_i^0,\widetilde{r}_i^1,\widetilde{\theta}_i)\}_{i\in[n]} \leftarrow \mathsf{SimExt.Ext}(\{c_i\}_{i\in[n]})$. Thereafter, $\{(\widetilde{r}_i^0,\widetilde{r}_i^1,\widetilde{\theta}_i)\}_{i\in T}$ are used for the third check in the "check receiver part" of the honest sender strategy (instead of using $\{(\widehat{r}_i^0,\widehat{r}_i^1,\widehat{\theta}_i)\}_{i\in T}$).

- Hyb_4: This is the result of the interaction between $\mathsf{Sim}[\mathsf{R}^*]$, $\mathcal{F}_{\mathsf{OT}[\lambda]}$ and honest sender S. Using the notation of Definition 3.2, this is denoted by $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{OT}[\lambda]}}[\mathsf{Sim}[\mathsf{R}^*],\mathsf{D},(m_0,m_1)]$.

We prove the indistinguishability between the hybrids using the following claims:

Claim 7.7. $\Pr[\mathsf{Hyb}_0=1]=\Pr[\mathsf{Hyb}_1=1]$

Proof. The only difference between the two hybrids is in how S samples the state on the registers that it sends to R^*. Denote the registers that S sends to R^* in either hybrid by $\{\mathcal{R}_{i,b}\}_{i\in[n],b\in\{0,1\}}$. In Hyb_0, each pair $(\mathcal{R}_{i,0},\mathcal{R}_{i,1})$ contains state $(|r_i^0\rangle_{b_i},|r_i^1\rangle_{b_i})$, for $i\in U$ and b_i chosen uniformly from $\{+,\times\}$, and $(|r_i^0\rangle_0,|r_i^1\rangle_1)$ for $i\notin U$, and for independently uniformly sampled bits r_i^0,r_i^1. In Hyb_1, the challenger prepares $2n$ EPR pairs on registers $\{(\mathcal{S}_{i,b},\mathcal{R}_{i,b})\}_{i\in[n],b\in\{0,1\}}$, then for every $i\in U$ measures the pair $\mathcal{S}_{i,0},\mathcal{S}_{i,1}$ in basis b_i that is uniformly sampled from $\{+,\times\}$, and for $i\notin U$ measures $\mathcal{S}_{i,0},\mathcal{S}_{i,1}$ in basis $0,1$ respectively. By elementary properties of EPR pairs, each register $\mathcal{R}_{i,b}$ is in a state $|r\rangle$ for a uniformly independently sampled bit r and in a basis that is chosen from the same distribution in both experiments. □

Claim 7.8. $\Pr[\mathsf{Hyb}_1=1]=\Pr[\mathsf{Hyb}_2=1]$

Proof. In Hyb_1, S measures the registers $\{\mathcal{S}_{i,b}\}_{i\in[n],b\in\{0,1\}}$ first, after which R^* operates on registers $\{\mathcal{R}_{i,b}\}_{i\in[n],b\in\{0,1\}}$. In Hyb_2, S performs the same measurements, but after receiving the second round message from R^*. Indistinguishability follows because measurements on disjoint subsystems commute. □

Claim 7.9.

$$|\Pr[\mathsf{Hyb}_2=1]-\Pr[\mathsf{Hyb}_3=1]|\leq\frac{148(q+3n+1)^3+1}{2^{4\lambda}}+\frac{24qn}{2^{2\lambda}}.$$

Proof. This follows by a direct reduction to extractability of the commitment scheme (Definition 5.3). Indeed, let $\mathsf{Adv}_{\mathsf{Commit}}$ be the machine that runs Hyb_0 until R^* outputs its message, which includes $\{c_i\}_{i\in[n]}$. Let $\mathsf{Adv}_{\mathsf{Open}}$ be the machine that takes as input the rest of the state of Hyb_0, which includes T and the openings $\{(\widehat{r}_i^0,\widehat{r}_i^1,\widehat{\theta}_i),u_i\}_{i\in T}$, and outputs T and these openings. Let D be the machine that runs the rest of Hyb_0 and outputs a bit.

Then, plugging in $\lambda_{\mathsf{com}} = 4\lambda$, Definition 5.3 when applied to $(\mathsf{Adv}_{\mathsf{Commit}}, \mathsf{Adv}_{\mathsf{Open}}, \mathsf{D})$ implies that the hybrids cannot be distinguished except with probability

$$\frac{148(q+3n+1)^3+1}{2^{4\lambda}} + \frac{24qn}{2^{2\lambda}},$$

since we are committing to a total of $3n$ bits. □

Claim 7.10. *For $A = 11\,700, B = 30\,400$, and $q \geq 5$,*

$$|\Pr[\mathsf{Hyb}_3 = 1] - \Pr[\mathsf{Hyb}_4 = 1]| \leq \frac{3\sqrt{10}q^{3/2}}{2^{\lambda}} + \frac{1}{2^{5\lambda}}$$

Proof. The only difference between Hyb_3 and Hyb_4 is that $m_{1-b} = 0^{\lambda}$, where $b = \mathsf{maj}\{\widetilde{\theta}_i \oplus d_i\}_{i\in\overline{T}}$. In what follows, we show that m_{1-b} is masked with a string that is (statistically close to) uniformly random from even given the view of R^* in either hybrid, which implies the given claim.

Notation: We setup some notation before proceeding.

- Let $\mathbf{c} \coloneqq (c_1, \ldots, c_n)$ be the classical commitments and $\mathbf{b} \coloneqq (b_1, \ldots b_n)$ be the bits sampled by the sender while executing its checks.
- Write the classical extracted values $\{(\widetilde{r}_i^{\,0}, \widetilde{r}_i^{\,1}, \widetilde{\theta}_i)\}_{i\in[n]}$ as matrices

$$\widetilde{\mathbf{R}} \coloneqq \begin{bmatrix} \widetilde{r}_1^{\,0} & \ldots & \widetilde{r}_n^{\,0} \\ \widetilde{r}_1^{\,1} & \ldots & \widetilde{r}_n^{\,1} \end{bmatrix}, \widetilde{\boldsymbol{\theta}} \coloneqq \begin{bmatrix} \widetilde{\theta}_1 & \ldots & \widetilde{\theta}_n \end{bmatrix}.$$

- Given any $\mathbf{R} \in \{0,1\}^{2\times n}$, $\boldsymbol{\theta} \in \{0,1\}^n$, define $|\mathbf{R}_{\boldsymbol{\theta}}\rangle$ as a state on n 4-dimensional registers, where register i contains the state $|\mathbf{R}_{i,0}, \mathbf{R}_{i,1}\rangle$ prepared in the $(\boldsymbol{\theta}_i, \boldsymbol{\theta}_i)$-basis.
- Given $\mathbf{R}, \widetilde{\mathbf{R}} \in \{0,1\}^{2\times n}$ and a subset $T \subseteq [n]$, define $\mathbf{R}_T$ be the columns of $\mathbf{R}$ indexed by T, and define $\Delta\left(\mathbf{R}_T, \widetilde{\mathbf{R}}_T\right)$ as the fraction of columns $i \in T$ such that $(\mathbf{R}_{i,0}, \mathbf{R}_{i,1}) \neq (\widetilde{\mathbf{R}}_{i,0}, \widetilde{\mathbf{R}}_{i,1})$.
- For $T \subset [n]$, let $\overline{T} \coloneqq [n] \setminus T$.
- Given $\widetilde{\mathbf{R}} \in \{0,1\}^{2\times n}, \widetilde{\boldsymbol{\theta}} \in \{0,1\}^n, T \subseteq [n], U \subseteq [n]$, $\mathbf{b} \in \{0,1\}^n$, and $\delta \in (0,1)$, define

$$\Pi^{\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},T,U,\mathbf{b},\delta} \coloneqq \sum_{\substack{\mathbf{R}\,:\,\mathbf{R}_{S'}=\widetilde{\mathbf{R}}_{S'},\Delta\left(\mathbf{R}_{\overline{T}\setminus U},\widetilde{\mathbf{R}}_{\overline{T}\setminus U}\right)\geq\delta \\ \text{where } S'=\{j\,|\,j\in T\cap U \wedge \mathbf{b}_j=\widetilde{\boldsymbol{\theta}}_j\}}} \left|\mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right\rangle \left\langle \mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right|.$$

Now, consider the following projection, which has hard-coded the description of H_{FS}:

$$\Pi^{\delta}_{\mathsf{bad}} \coloneqq \sum_{\substack{\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},\mathbf{b}, \\ U\subseteq[n],|U|=k}} |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes \left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \Pi_{\mathcal{S}}^{\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},H_{FS}(\mathbf{c}),U,\mathbf{b},\delta},$$

where $\mathcal{C}$ is the register holding the classical commitments, $\mathcal{Z}_1$ is the register holding the output of $\mathsf{SimExt.Ext}$, $\mathcal{Z}_2$ is the register holding the subset U and bits $\mathbf{b}$ sampled by sender, and $\mathcal{S}$ denotes all the registers holding the sender's halves of EPR pairs.

SubClaim 7.11. *Let*

$$\tau := \sum_{\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b}} p^{(\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b})} \tau^{(\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b})},$$

where

$$\tau^{(\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b})} = |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes \left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \rho_{\mathcal{S},\mathcal{X}}^{(\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b})}$$

is the entire state of Hyb_3 *(equivalently also* Hyb_4*) immediately after* R^* *outputs its message (which includes* $\mathbf{c}$*),* $\mathsf{SimExt.Ext}$ *is run to get* $\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}$*, and sender samples the set* $U \subseteq [n]$ *of size* d *and bits* $\mathbf{b} \in \{0,1\}^n$*. Here, each* $p^{(\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b})}$ *is the probability that the string* $\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b}$ *is contained in the registers* $\mathcal{C},\mathcal{Z}_1,\mathcal{Z}_2$*. Also,* $\mathcal{S}$ *is the register holding the sender's halves of EPR pairs and* $\mathcal{X}$ *is a register holding remaining state of the system, which includes the rest of the receiver's classical message and its private state. Then, for* $A = 11\,700, B = 30\,400$ *and for* $q \geq 5$*,*

$$\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{11/200}\tau\right) \leq \frac{45q^3}{2^{2\lambda}}$$

Proof. Define $\mathsf{Adv}_{\mathsf{R}^*}^{H_{FS}}$ to be the oracle machine that runs Hyb_3 until R^* outputs $\mathbf{c}$ (and the rest of its message), then runs $\mathsf{SimExt.Ext}$ to obtain $\left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1}$, followed by sampling the set $U \subseteq [n]$ of size d, and bits $\mathbf{b} \in \{0,1\}^n$ in the register $\mathcal{Z}_2$, and finally outputting the remaining state $\rho_{\mathcal{S},\mathcal{X}}$. Consider running the measure-and-reprogram simulator $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ from Imported Theorem 3.5, which simulates H_{FS} queries, measures and outputs $\mathbf{c}$, then receives a uniformly random subset $T \subset [n]$ of size k, and then continues to run $\mathsf{Adv}_{\mathsf{R}^*}$ until it outputs $\left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \rho_{\mathcal{S},\mathcal{X}}$. Letting

$$\Pi_{\mathsf{bad}}^{\delta}[T] := \sum_{\substack{\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},\mathbf{b} \\ U\subseteq[n],|U|=d}} |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes \left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \Pi_{\mathcal{S}}^{\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},T,U,\mathbf{b},\delta},$$

for $T \subset [n]$, Imported Theorem 3.5 implies that $\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{\delta}\tau\right) \leq (2q+1)^2\gamma$, where

$$\gamma = \mathbb{E}\left[\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{\delta}[T]\left(|\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes \left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \rho_{\mathcal{S},\mathcal{X}}\right)\right)\right]$$

with expectation defined over the following experiment:

- $(\mathbf{c},\mathsf{st}) \leftarrow \mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$,
- $T \leftarrow S_{n,k}$, the set of all subsets of $[n]$ of size k,
- $\left(\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b},\rho_{\mathcal{S},\mathcal{X}}\right) \leftarrow \mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}](T,\mathsf{st})$.

Now, recall that one of the last things that $\mathsf{Adv}_{\mathsf{R}^*}$ does in Hyb_3 is run $\mathsf{SimExt.Ext}$ on $\mathbf{c}$ to obtain $(\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}})$. Consider instead running $\mathsf{SimExt.Ext}$ on $\mathbf{c}$ immediately after $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ outputs $\mathbf{c}$. Note that $\mathsf{SimExt.Ext}$ only operates on the register holding $\mathbf{c}$ and its own private state used for simulating H_C, so since Com^{H_C} has a $\frac{8}{2^{\lambda_{\mathsf{com}}/2}}$-commuting simulator (Definition 5.3), we have that,

$$\mathrm{Tr}\left(\Pi^{\delta}_{\mathsf{bad}}\tau\right) \leq (2q+1)^2\left(\epsilon + \frac{8q}{2^{\lambda_{\mathsf{com}}/2}}\right) \tag{5}$$

where

$$\epsilon \coloneqq \mathbb{E}\left[\mathrm{Tr}\left(\Pi^{\delta}_{\mathsf{bad}}[T]\left(|\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes \left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \rho_{\mathcal{S},\mathcal{X}}\right)\right)\right] \tag{6}$$

over the randomness of the following experiment:

- $(\mathbf{c},\mathsf{st}) \leftarrow \mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$,
- $(\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}) \leftarrow \mathsf{SimExt.Ext}(\mathbf{c})$,
- $T \leftarrow S_{n,k}$,
- $\left(\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},U,\mathbf{b},\rho_{\mathcal{S},\mathcal{X}}\right) \leftarrow \mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}](T,\mathsf{st})$.

The sampling of $T, U \subseteq [n]$ each of size k uniformly and independently at random in the experiment above is equivalent to the following sampling strategy. First, sample the size of their intersection, i.e. sample and fix $s = |T \cap U|$, this fixes the size of $T \cup U$ to be $2k - s$, since $|T| = |U| = s$. Next sample and fix a set T' of size $2k - s$ (that will eventually represent the union $T \cup U$). Finally, sample a subset $S \subset T'$ of size s (which will eventually represent the intersection $T \cap U$), and then obtain T and U by paritioning $T' \setminus S$ into two random subsets each of size $k - s$, and then computing the union of each set with S. This is described formally below.

- Fix a state on register $\mathcal{S}$ (and potentially other registers of arbitrary size), where $\mathcal{S}$ is split into n registers $\mathcal{S}_1, \ldots, \mathcal{S}_n$ of dimension 4, and fix $\widetilde{\mathbf{R}} \in \{0,1\}^{2\times n}, \widetilde{\boldsymbol{\theta}} \in \{0,1\}^n$.
- Sample two independent and uniform subsets of $[n]$ each of size k. Let s denote the size of their intersection. Fix s, and discard the subsets themselves.
- Sample a random subset T' of $[n]$, of size $2k - s$.
- Sample subsets $T, U, S' \subseteq T'$ as follows:
  - Sample and fix a random subset set of size s of T', call this subset S.
  - Partition $T' \setminus S$ (note: this has size $2k - 2s$) into two equal sets W_1 and W_2 of size $k - s$. This can be done by first sampling a set W_1 of size $k - s$ uniformly at random from $T' \setminus S$ and setting $W_2 = (T' \setminus S) \setminus W_1$.
  - Let $T = W_1 \cup S$ and $U = W_2 \cup S$.
  - Sample bits $\mathbf{b} \in \{0,1\}^n$ and set $S' = \{j \mid j \in S \wedge \mathbf{b}_j = \widetilde{\boldsymbol{\theta}}_j\}$.
- For each $i \in S'$, measure the register $\mathcal{S}_i$ in basis $\widetilde{\boldsymbol{\theta}}_i$ to get $\mathbf{R}_{S'} \in \{0,1\}^{2\times|S'|}$. Output $\Delta(\mathbf{R}_{S'}, \widetilde{\mathbf{R}}_{S'})$.

The quantum error probability $\epsilon^{\delta}_{\mathsf{quantum}}$ (Definition 3.11) of the above game corresponds to the trace distance between the initial state on register $\mathcal{S}$ and an "ideal" state (as defined in Definition 3.11). This ideal state is supported on vectors $\left|\mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right\rangle$ such that $|\Delta(\mathbf{R}_{\overline{T'}}, \widetilde{\mathbf{R}}_{\overline{T'}}) - \Delta(\mathbf{R}_{S'}, \widetilde{\mathbf{R}}_{S'})| < \delta$. In particular, for any $\left|\mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right\rangle$ with $\Delta(\mathbf{R}_{S'}, \widetilde{\mathbf{R}}_{S'}) = 0$ in the support of the ideal state, it holds that $\Delta(\mathbf{R}_{\overline{T'}}, \widetilde{\mathbf{R}}_{\overline{T'}}) < \delta$, or $\Delta(\mathbf{R}_{\overline{T}\setminus U}, \widetilde{\mathbf{R}}_{\overline{T}\setminus U}) < \delta$ (since $\overline{T'} = \overline{T} \setminus U$ in the sampling game above). Thus, this ideal state is orthogonal to the subspace $\Pi_{\mathcal{S}}^{\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},T,U,\mathbf{b},\delta}$, and so it follows that ϵ is bounded by $\epsilon^{\delta}_{\mathsf{quantum}}$.

Thus, by Imported Theorem 3.12, ϵ is then bounded by $\sqrt{\epsilon^{\delta}_{\mathsf{classical}}}$, where $\epsilon^{\delta}_{\mathsf{classical}}$ is the *classical* error probability (Definition 3.10) in the corresponding classical sampling game, defined as follows:

- Let $\mathbf{R}, \widetilde{\mathbf{R}} \in \{0,1\}^{2\times n}$ s.t. $\mathbf{R}$ is the matrix on which we are running the sampling and $\widetilde{\mathbf{R}}$ is an arbitrary matrix.
- Sample two independent and uniform subsets of $[n]$ each of size k. Let s denote the size of their intersection. Fix s, and discard the subsets themselves. Sample a random subset T' of $[n]$, of size $2k - s$.
- Sample subset $S' \subseteq T'$ as follows:
  - Sample S as a random subset of T' of size s.
  - Sample bits $\mathbf{b} \in \{0,1\}^n$ and set $S' = \{j \,|\, j \in S \wedge \mathbf{b}_j = \widetilde{\boldsymbol{\theta}}_j\}$.
- Output $\Delta(\mathbf{R}_{S'}, \widetilde{\mathbf{R}}_{S'})$.

We provide an analysis of this classical sampling game in Appendix D.3. Using Lemma D.4 from the same appendix, we get that for $0 < \epsilon, \beta, \delta < 1$ and $0 < \gamma < \delta$,

$$\begin{aligned}\epsilon^{\delta}_{\mathsf{classical}} \leq\ & 2\exp\left(-2\left(\frac{(n-k)^2 - 3\epsilon k^2}{(n-k)^2 + (1-2\epsilon)k^2}\right)^2 \gamma^2(1-\epsilon)\frac{k^2}{n}\right) \\ & + 2\exp\left(-(\delta-\gamma)^2(1-\beta)(1-\epsilon)\frac{k^2}{n}\right) \\ & + \exp\left(-\frac{\beta^2(1-\epsilon)k^2}{2n}\right) + 2\exp\left(-\frac{2\epsilon^2 k^3}{n^2}\right)\end{aligned}$$

Setting $\delta = 11/200, \epsilon = 0.03917, \beta = 0.04213, \gamma = 0.02456, k = A\lambda, n = (A+B)\lambda, A = 11\ 700, B = 30\ 400$, we get each of the exp terms above is $\leq \frac{1}{2^{4\lambda}}$. Thus, $\epsilon^{\delta}_{\mathsf{classical}} \leq \frac{7}{2^{4\lambda}}$, giving us, $\epsilon \leq \epsilon^{\delta}_{\mathsf{quantum}} \leq \sqrt{\epsilon^{\delta}_{\mathsf{classical}}} \leq \frac{\sqrt{7}}{2^{2\lambda}}$.

This gives using Eq. (5) that:

$$\mathrm{Tr}\left(\Pi^{11/200}_{\mathsf{bad}}\tau\right) \leq (2q+1)^2\left[\frac{\sqrt{7}}{2^{2\lambda}} + \frac{8q}{2^{\lambda_{\mathsf{com}}/2}}\right]$$

For $\lambda_{\mathsf{com}} = 4\lambda$ and $q \geq 5$,

$$\mathrm{Tr}\left(\Pi^{11/200}_{\mathsf{bad}}\tau\right) \leq (2q+1)^2\left[\frac{\sqrt{7}}{2^{2\lambda}} + \frac{8q}{2^{2\lambda}}\right] \leq \frac{(2q+1)^2(8q+\sqrt{7})}{2^{2\lambda}} \leq \frac{5q^2\cdot 9q}{2^{2\lambda}} \leq \frac{45q^3}{2^{2\lambda}}$$

□

Thus, by gentle measurement (Lemma 3.1), the τ defined in SubClaim 7.11 is within trace distance $\frac{3\sqrt{10}q^{3/2}}{2^\lambda}$ of a state τ_{good} in the image of $\mathbb{I} - \Pi_{\mathsf{bad}}^{11/200}$.The following sub-claim completes the proof of Claim 7.10.

SubClaim 7.12. *If $h : \{0,1\}^m \times \{0,1\}^{\leq A\lambda} \to \{0,1\}^\lambda$ is a universal family of hash functions, then conditioned on τ (defined in SubClaim 6.5) being the image of $\mathbb{I} - \Pi_{\mathsf{bad}}^{11/200}$, and $A = 11\,700, B = 30\,400$, it holds that*

$$|\Pr[\mathsf{Hyb}_3 = 1] - \Pr[\mathsf{Hyb}_4 = 1]| \leq \frac{1}{2^{5\lambda}}$$

where h_b is the binary entropy function.

Proof. Note that

$$\mathbb{I} - \Pi_{\mathsf{bad}}^{\delta} = \sum_{\substack{\mathbf{c},\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}},\mathbf{b},\\ U\subseteq[n],|U|=d}} |\mathbf{c}\rangle\langle\mathbf{c}|_{\mathcal{C}} \otimes \left|\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right\rangle\left\langle\widetilde{\mathbf{R}},\widetilde{\boldsymbol{\theta}}\right|_{\mathcal{Z}_1} \otimes |U,\mathbf{b}\rangle\langle U,\mathbf{b}|_{\mathcal{Z}_2} \otimes \left(\sum_{\substack{\mathbf{R}:\mathbf{R}_{S'}\neq\widetilde{\mathbf{R}}_{S'} \text{ or } \Delta\left(\mathbf{R}_{\overline{T}\setminus U},\widetilde{\mathbf{R}}_{\overline{T}\setminus U}\right)<\delta\\ \text{where } T=H_{FS}(\mathbf{c}),\\ S'=\{j\,|\,j\in T\cap U\wedge \mathbf{b}_j=\widetilde{\boldsymbol{\theta}}_j\}}} \left|\mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right\rangle\left\langle\mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right|_{\mathcal{S}} \right) \tag{7}$$

Since τ is in the image of $\mathbb{I} - \Pi_{\mathsf{bad}}^{11/200}$, by definition the state on register $\mathcal{S}$ is in a superposition of states as in the summation above. However, note that if $T \neq H_{FS}(\mathbf{c})$ or if $\mathbf{R}_{S'} \neq \widetilde{\mathbf{R}}_{S'}$ (where $S' = \{j \,|\, j \in T\cap U \wedge \mathbf{b}_j = \widetilde{\boldsymbol{\theta}}_j\}$), then the sender side check will fail and the two hybrids are perfectly indistinguishable. So, it suffices to analyze states τ where the register containing T equals $H_{FS}(\mathbf{c})$ and where $\mathbf{R}_{S'} = \widetilde{\mathbf{R}}_{S'}$. Thus, conditioned on the sender not aborting, the above equation implies that the register $\mathcal{S}$ is in superposition of states $\left|\mathbf{R}_{\widetilde{\boldsymbol{\theta}}}\right\rangle$ s.t. $\mathbf{R}_{S'} = \widetilde{\mathbf{R}}_{S'}, \Delta(\mathbf{R}_{\overline{T}\setminus U}, \widetilde{\mathbf{R}}_{\overline{T}\setminus U}) < 11/200$, for S' as defined above.

Recall that τ is the state of Hyb_3 (equivalently also Hyb_4) immediately after R^* outputs its message (which includes $\mathbf{c}$), SimExt.Ext is run to get $\widetilde{\mathbf{R}}, \widetilde{\boldsymbol{\theta}}$, and sender samples the set $U \subseteq [n]$ of size d and bits $\mathbf{b} \in \{0,1\}^n$ next the sender measures register $\mathcal{S}$. Since measurements on different subsystems commute, we may assume that the sender measures the registers $\mathcal{S}_{T\cup U}$ first (recall that we are trying to argue that the remaining registers have entropy). Then, by the argument in the previous paragraph, this leaves the remaining registers $\mathcal{S}_{\overline{T}\setminus U}$ in a superposition of states $\left|\left(\mathbf{R}_{\overline{T}\setminus U}\right)_{\widetilde{\boldsymbol{\theta}}}\right\rangle$ for $\mathbf{R}_{\overline{T}\setminus U}$ s.t. $\Delta(\mathbf{R}_{\overline{T}\setminus U}, \widetilde{\mathbf{R}}_{\overline{T}\setminus U}) < \frac{11}{200}$.

Next, to obtain ct_c for $c \in \{0,1\}$, the sender measures registers $\mathcal{S}_{i,d_i\oplus c}$ in basis $d_i \oplus c$ to obtain a string $\mathbf{r}'_c \in \{0,1\}^{|\overline{T}\setminus U|}$. Then, ct_c is set as $m_c \oplus h(s, \mathbf{r}'_c)$, where s is uniformly sampled seed for a universal hash function h. Recall, in addition, in Hyb_4 the sender defines b as $\mathsf{maj}\{\widetilde{\boldsymbol{\theta}}_i \oplus d_i\}_{i\in\overline{T}\setminus U}$. We now prove a lower bound on the quantum min-entropy of $\mathbf{r}'_{b\oplus 1}$, which by the Leftover Hash lemma (Imported Theorem 3.8) would imply our claim.

Consider the subset $W \subseteq \{0,1\} \times \overline{T} \setminus U$ defined as $W = \{i, d_i \oplus b \oplus 1\}_{i\in\overline{T}\setminus U}$. Consider again by the commuting property of measurements on different systems that registers $\mathcal{S}_{\overline{T}\setminus(U\cup W)} =$

$\{\mathcal{S}_{i,d_i\oplus b}\}_{i\in\overline{T}\setminus U}$ are measured first, leaving the registers $\mathcal{S}_W = \{\mathcal{S}_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}\setminus U}$ in a superposition of states $\left|\mathbf{r}_{\widetilde{\boldsymbol{\theta}}_{W[1]}}\right\rangle$, where $\Delta\left(\mathbf{r},\widetilde{\mathbf{R}}_W\right) < 11/200$, and where $W[1]$ denotes the projection of W on the second set, i.e. $W[1] = \{d_i \oplus b \oplus 1\}_{i\in\overline{T}\setminus U}$. Hence, since $\mathbf{r}'_{b\oplus 1}$ is obtained by measuring registers $\mathcal{S}_W = \{\mathcal{S}_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}\setminus U}$ in basis $d_i\oplus b\oplus 1$, majority of the bits of $\mathbf{r}'_{b\oplus 1}$ are obtained by measuring $\mathcal{S}_W$ in basis $\widetilde{\boldsymbol{\theta}}_i \oplus 1$ (since b was defined as $\text{maj}\{\widetilde{\boldsymbol{\theta}}_i \oplus d_i\}_{i\in\overline{T}\setminus U}$, this means in the majority of the places in $\overline{T}\setminus U$, the following holds: $b = \widetilde{\boldsymbol{\theta}}_i \oplus d_i \iff d_i \oplus b \oplus 1 = \widetilde{\boldsymbol{\theta}}_i \oplus 1$).

Therefore, registers $\mathcal{S}_W$ are in a superposition of states $\left|\mathbf{r}_{\widetilde{\boldsymbol{\theta}}_{W[1]}}\right\rangle$, where $\Delta\left(\mathbf{r},\widetilde{\mathbf{R}}_W\right) < 11/200$. Recall that $\mathcal{S}_W = \{\mathcal{S}_{i,d_i\oplus b\oplus 1}\}_{i\in\overline{T}\setminus U}$, then the paragraph above implies that for a majority of $i \in \overline{T}\setminus U$, register $\mathcal{S}_{i,\widetilde{\boldsymbol{\theta}}_i\oplus 1}$ is measured in basis $\widetilde{\boldsymbol{\theta}}_i \oplus 1$. Using Imported Theorem 3.9, we get,

$$\begin{aligned}
\mathbf{H}_\infty(\mathbf{r}'_{b\oplus 1}\,|\,\mathcal{C},\mathcal{Z}_1,\mathcal{Z}_2,\mathcal{X}) &\geq \frac{|\overline{T}\setminus U|}{2} - h_b\left(\frac{11}{200}\right)|\overline{T}\setminus U| \\
&\geq \frac{n-2k}{2} - h_b\left(\frac{11}{200}\right)(n-k) \\
&\geq \frac{n-2k}{2} - 0.3073(n-k)
\end{aligned}$$

For $n = (A+B)\lambda, k = A\lambda, A = 11\,700, B = 30\,400$, we get,

$$\mathbf{H}_\infty(\mathbf{r}'_{b\oplus 1}\,|\,\mathcal{C},\mathcal{Z}_1,\mathcal{Z}_2,\mathcal{X}) \geq 9\lambda.$$

where h_b is the binary entropy function, and we bound the number of strings of length n with relative hamming weight at most δ by $h_b(\delta)n$. Hence, using the leftover hash lemma (Imported Theorem 3.8), $(s, h(s,\mathbf{r}'_{b\oplus 1}))$ is $\frac{1}{2^{5\lambda}}$. □

This completes the proof of the claim, as desired. □

References

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 269–295. Springer, Heidelberg, August 2019.

[AIR01] William Aiello, Yuval Ishai, and Omer Reingold. Priced oblivious transfer: How to sell digital goods. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 119–135. Springer, Heidelberg, May 2001.

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 788–817. Springer, Heidelberg, May 2020.

[AQY21] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. Cryptology ePrint Archive, Report 2021/1663, 2021. https://ia.cr/2021/1663.

[BB21] Nir Bitansky and Zvika Brakerski. Classical binding for quantum commitments. In Kobbi Nissim and Brent Waters, editors, *TCC*, 2021.

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[BBCS92] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 351–366. Springer, Heidelberg, August 1992.

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. Springer-Verlag, 2021.

[BDH06] Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement. *Science (New York, N.Y.)*, 314:436–9, 11 2006.

[BF10] Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 724–741. Springer, Heidelberg, August 2010.

[BGI+17] Saikrishna Badrinarayanan, Sanjam Garg, Yuval Ishai, Amit Sahai, and Akshay Wadia. Two-message witness indistinguishability and secure computation in the plain model from new assumptions. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part III*, volume 10626 of *LNCS*, pages 275–303. Springer, Heidelberg, December 2017.

[BGJ+17] Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Dakshita Khurana, and Amit Sahai. Round optimal concurrent MPC via strong simulation. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 743–775. Springer, Heidelberg, November 2017.

[BGJ+18] Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai. Promise zero knowledge and its applications to round optimal MPC. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 459–487. Springer, Heidelberg, August 2018.

[BK22] James Bartusek and Dakshita Khurana. Cryptography with certified deletion. Cryptology ePrint Archive, Paper 2022/1178, 2022. https://eprint.iacr.org/2022/1178.

[BV17] Nir Bitansky and Vinod Vaikuntanathan. A note on perfect correctness by derandomization. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 592–606. Springer, Heidelberg, April / May 2017.

[CCH+19] Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, and Daniel Wichs. Fiat-Shamir: from practice to theory. In Moses Charikar and Edith Cohen, editors, *51st ACM STOC*, pages 1082–1090. ACM Press, June 2019.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, jul 2004.

[CGS16] André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chic. J. Theor. Comput. Sci.*, 2016, 2016.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th FOCS*, pages 42–52. IEEE Computer Society Press, October 1988.

[CKS13] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. *Quantum Info. Comput.*, 13(1–2):158–177, jan 2013.

[CVZ20] Andrea Coladangelo, Thomas Vidick, and Tina Zhang. Non-interactive zero-knowledge arguments for qma, with preprocessing. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 799–828, Cham, 2020. Springer International Publishing.

[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*, pages 408–427. Springer, Heidelberg, August 2009.

[DFM20] Jelle Don, Serge Fehr, and Christian Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 602–631. Springer, Heidelberg, August 2020.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.

[DFMS21] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. Cryptology ePrint Archive, Report 2021/280, 2021.

[DFSS08] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. *SIAM J. Comput.*, 37:1865–1890, 01 2008.

[DGH+20] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, Daniel Masny, and Daniel Wichs. Two-round oblivious transfer from CDH or LPN. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 768–797. Springer, Heidelberg, May 2020.

[DLS22] Frédéric Dupuis, Philippe Lamontagne, and Louis Salvail. Fiat-shamir for proofs lacks a proof even in the presence of shared entanglement, 2022.

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, jun 1985.

[Eke91] Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67 6:661–663, 1991.

[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, 2014.

[FGS+18] F. Furrer, T. Gehring, C. Schaffner, C. Pacher, R. Schnabel, and S. Wehner. Continuous-variable protocol for oblivious transfer in the noisy-storage model. *Nature Communications*, 9(1), 2018.

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the qrom. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 637–667, Cham, 2021. Springer International Publishing.

[GIK+15] Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2015.

[GLSV21] Alex Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. Springer-Verlag, 2021.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987.

[HK12] Shai Halevi and Yael Kalai. Smooth projective hashing and two-message oblivious transfer. *Journal of Cryptology*, 25:158–193, 01 2012.

[Hol19] Alexander S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. De Gruyter, 2019.

[IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 145–161. Springer, Heidelberg, August 2003.

[IKO+11] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 667–684. Springer, Heidelberg, August 2011.

[IKS+17] T. Ito, H. Koizumi, N. Suzuki, I. Kakesu, K. Iwakawa, A. Uchida, T. Koshiba, J. Muramatsu, K. Yoshimura, M. Inubushi, and P. Davis. Physical implementation of oblivious transfer using optical correlated randomness. *Scientific Reports*, 7(1), 2017.

[JKKR17] Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Ron Rothblum. Distinguisher-dependent simulation in two rounds and its applications. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 158–189. Springer, Heidelberg, August 2017.

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

[KKS18] Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai. Statistical witness indistinguishability (and more) in two messages. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 34–65. Springer, Heidelberg, April / May 2018.

[Kob03] Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In Toshihide Ibaraki, Naoki Katoh, and Hirotaka Ono, editors, *Algorithms and Computation*, pages 178–188, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[KRR17] Yael Tauman Kalai, Guy N. Rothblum, and Ron D. Rothblum. From obfuscation to the security of Fiat-Shamir for proofs. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 224–251. Springer, Heidelberg, August 2017.

[KRS09] Robert Konig, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *IEEE Transactions on Information theory*, 55(9):4337–4347, 2009.

[KS17] Dakshita Khurana and Amit Sahai. How to achieve non-malleability in one or two rounds. In Chris Umans, editor, *58th FOCS*, pages 564–575. IEEE Computer Society Press, October 2017.

[KST20] Srijita Kundu, Jamie Sikora, and Ernest Y-Z Tan. A device-independent protocol for xor oblivious transfer. *arXiv: Quantum Physics*, 2020.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[MS94] Dominic Mayers and Louis Salvail. Quantum oblivious transfer is secure against all individual measurements. In *Proceedings Workshop on Physics and Computation. PhysComp'94*, pages 69–77. IEEE, 1994.

[MY21a] Tomoyuki Morimae and Takashi Yamakawa. Classically verifiable nizk for qma with preprocessing, 2021.

[MY21b] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. Cryptology ePrint Archive, Report 2021/1691, 2021. https://ia.cr/2021/1691.

[NP01] Moni Naor and Benny Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '01, page 448–457, USA, 2001. Society for Industrial and Applied Mathematics.

[OPP14] Rafail Ostrovsky, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky. Maliciously circuit-private FHE. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 536–553. Springer, Heidelberg, August 2014.

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 554–571. Springer, Heidelberg, August 2008.

[Rab05] Michael O. Rabin. How to exchange secrets with oblivious transfer. *IACR Cryptol. ePrint Arch.*, 2005:187, 2005.

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

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 407–425. Springer, Heidelberg, February 2005.

[SQ20] Shouqian Shi and Chen Qian. Concurrent entanglement routing for quantum networks: Model and designs. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, page 62–75, New York, NY, USA, 2020. Association for Computing Machinery.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 486–505. Springer, Heidelberg, May / June 2010.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 755–784. Springer, Heidelberg, April 2015.

[WCSL10] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo. Implementation of two-party protocols in the noisy-storage model. *Physical Review A - Atomic, Molecular, and Optical Physics*, 81(5), 2010.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15:78–88, 1983.

[Win99] Andreas J. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7):2481–2485, 1999.

[WST08] Stephanie Wehner, Christian Schaffner, and Barbara Terhal. Cryptography from noisy storage. *Physical review letters*, 100:220502, 06 2008.

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *27th ACM STOC*, pages 67–75. ACM Press, May / June 1995.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, August 2019.

A Security of the seedless extractors

In this section, we show the security of the XOR and ROM extractors.

A.1 XOR extractor

Theorem A.1. *Let $\mathcal{X}$ be an n-qubit register, and consider any state $|\gamma\rangle_{\mathcal{A},\mathcal{X}}$ that can be written as*

$$|\gamma\rangle = \sum_{u:\mathcal{HW}(u)<n/2} |\psi_u\rangle_{\mathcal{A}} \otimes |u\rangle_{\mathcal{X}} .$$

Let $\rho_{\mathcal{A},\mathcal{P}}$ be the mixed state that results from measuring $\mathcal{X}$ in the Hadamard basis to produce x, and writing $\bigoplus_{i\in[n]} x_i$ into the single qubit register $\mathcal{P}$. Then it holds that

$$\rho_{\mathcal{A},\mathcal{P}} = \mathrm{Tr}_{\mathcal{X}}(|\gamma\rangle\langle\gamma|) \otimes \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right).$$

Proof. First, write the state on $(\mathcal{A},\mathcal{X},\mathcal{P})$ that results from applying Hadamard to $\mathcal{X}$ and writing the parity, denoted by $p(x) \coloneqq \bigoplus_{i\in[n]} x_i$, to $\mathcal{P}$:

$$\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} \left(\sum_{u:\mathcal{HW}(u)<n/2} (-1)^{u\cdot x} |\psi_u\rangle \right) |x\rangle |p(x)\rangle .$$

Then we have that

$$\begin{aligned}
\rho_{\mathcal{A},\mathcal{P}} &= \frac{1}{2^n}\sum_{x:p(x)=0}\left(\sum_{u_1,u_2}(-1)^{(u_1\oplus u_2)\cdot x}\left|\psi_{u_1}\right\rangle\left\langle\psi_{u_2}\right|\right)\otimes|0\rangle\langle 0| \\
&\quad+\frac{1}{2^n}\sum_{x:p(x)=1}\left(\sum_{u_1,u_2}(-1)^{(u_1\oplus u_2)\cdot x}\left|\psi_{u_1}\right\rangle\left\langle\psi_{u_2}\right|\right)\otimes|1\rangle\langle 1| \\
&= \frac{1}{2^n}\sum_{u_1,u_2}\left|\psi_{u_1}\right\rangle\left\langle\psi_{u_2}\right|\otimes\left(\sum_{x:p(x)=0}(-1)^{(u_1\oplus u_2)\cdot x}|0\rangle\langle 0|+\sum_{x:p(x)=1}(-1)^{(u_1\oplus u_2)\cdot x}|1\rangle\langle 1|\right) \\
&= \frac{1}{2^n}\sum_{u_1,u_2}2^{n/2}\delta_{u_1=u_2}\left|\psi_{u_1}\right\rangle\left\langle\psi_{u_2}\right|\otimes(|0\rangle\langle 0|+|1\rangle\langle 1|) \\
&= \frac{1}{2}\sum_{u:\mathcal{HW}<n/2}|\psi_u\rangle\langle\psi_u|\otimes(|0\rangle\langle 0|+|1\rangle\langle 1|) \\
&= \mathrm{Tr}_{\mathcal{X}}(|\gamma\rangle\langle\gamma|)\otimes\left(\frac{1}{2}|0\rangle\langle 0|+\frac{1}{2}|1\rangle\langle 1|\right),
\end{aligned}$$

where the 3rd equality is due to the following claim, plus the observation that $u_1 \oplus u_2 \neq 1^n$ for any u_1, u_2 such that $\mathcal{HW}(u_1), \mathcal{HW}(u_2) < n/2$.

Claim A.2. *For any $u \in \{0,1\}^n$ such that $u \notin \{0^n, 1^n\}$, it holds that*

$$\sum_{x:p(x)=0}(-1)^{u\cdot x} = \sum_{x:p(x)=1}(-1)^{u\cdot x} = 0.$$

Proof. For any such $u \notin \{0^n, 1^n\}$, define $S_0 = \{i : u_i = 0\}$ and $S_1 = \{i : u_i = 1\}$. Then, for any $y_0 \in \{0,1\}^{|S_0|}$ and $y_1 \in \{0,1\}^{|S_1|}$, define $x_{y_0,y_1} \in \{0,1\}^n$ to be the n-bit string that is equal to y_0 when restricted to indices in S_0 and equal to y_1 when restricted to indices in S_1. Then,

$$\begin{aligned}
\sum_{x:p(x)=0}(-1)^{u\cdot x} &= \sum_{y_1\in\{0,1\}^{|S_1|}}\ \sum_{y_0\in\{0,1\}^{|S_0|}:p(x_{y_0,y_1})=0}(-1)^{u\cdot x_{y_0,y_1}} \\
&= \sum_{y_1\in\{0,1\}^{|S_1|}}2^{|S_0|-1}(-1)^{1^{|S_1|}\cdot y_1} = 2^{|S_0|-1}\sum_{y_1\in\{0,1\}^{|S_1|}}(-1)^{p(y_1)} = 0,
\end{aligned}$$

and the same sequence of equalities can be seen to hold for $x : p(x) = 1$. □

□

A.2 RO extractor

Theorem A.3. *Let $H : \{0,1\}^n \to \{0,1\}^m$ be a uniformly random function, and let q, C, k be integers. Consider a two-stage oracle algorithm (A_1^H, A_2^H) that combined makes at most q queries to H. Suppose that A_1^H outputs classical strings $(T, \{x_i\}_{i\in T})$, and let $|\gamma\rangle_{\mathcal{A},\mathcal{X}}$ be its left-over quantum state,[16] where $T \subset [n]$*

[16] That is, consider sampling H, running a purified A_1^H, measuring at the end to obtain $(T, \{x_i\}_{i\in T})$, and then defining $|\gamma\rangle$ to be the left-over state on $\mathcal{A}$'s remaining registers.

is a set of size $n-k$, each $x_i \in \{0,1\}$, $\mathcal{A}$ is a register of arbitary size, and $\mathcal{X}$ is a register of k qubits. Suppose further that with probability 1 over the sampling of H and the execution of A_1, there exists a set $L \subset \{0,1\}^k$ of size at most C such that $|\gamma\rangle$ may be written as follows:

$$|\gamma\rangle = \sum_{u \in L} |\psi_u\rangle_{\mathcal{A}} \otimes |u\rangle_{\mathcal{X}} .$$

Now consider the following two games.

- REAL*:*
  - *A_1^H outputs $T, \{x_i\}_{i\in T}, |\gamma\rangle_{\mathcal{A},\mathcal{X}}$.*
  - *$\mathcal{X}$ is measured in the Hadamard basis to produce a k-bit string which is parsed as $\{x_i\}_{i\in\overline{T}}$, and a left-over state $|\gamma'\rangle_{\mathcal{A}}$ on register $\mathcal{A}$. Define $x = (x_1, \ldots, x_n)$.*
  - *A_2^H is given $T, \{x_i\}_{i\in T}, |\gamma'\rangle_{\mathcal{A}}, H(x)$, and outputs a bit.*
- IDEAL*:*
  - *A_1^H outputs $T, \{x_i\}_{i\in T}, |\gamma\rangle_{\mathcal{A},\mathcal{X}}$.*
  - *$r \leftarrow \{0,1\}^m$.*
  - *A_2^H is given $T, \{x_i\}_{i\in T}, \mathrm{Tr}_{\mathcal{X}}(|\gamma\rangle\langle\gamma|), r$, and outputs a bit.*

Then,

$$|\Pr[\mathsf{REAL}=1] - \Pr[\mathsf{IDEAL}=1]| \leq \frac{2\sqrt{q}C + 2q\sqrt{C}}{2^{k/2}} < \frac{4qC}{2^{k/2}}.$$

Proof. The proof follows via two steps. First, we define a HYBRID distribution where we re-program the random oracle at input x to a uniformly random string r, and argue that the adversary cannot notice, even given x. Intuitively, this is establishing that $H(x)$ must have been quite close to uniformly random from the adversary's perspective at the point that x is measured (on average over x). This requires a new "adaptive re-programming" lemma for the QROM, where the point x that is adaptively re-programmed may be sampled from a *quantum* source of entropy. As mentioned in the introduction, all previous adaptive re-programming lemmas have only handled classical entropy sources. Second, we "undo" the re-programming of $H(x)$, but still output (uniformly random) r as the extracted string. Indistinguishability of these two games, on the other hand, can be established via a one-way-to-hiding lemma, since in the final game, the adversary is given no information at all about the measured string x. In particular, it suffices to use the fact that x has high quantum min-entropy conditioned on the adversary's state to argue that the adversary cannot guess x and thus cannot notice whether or not $H(x)$ was re-programmed.

Now we formalize this strategy. Consider the following hybrid game.

- HYBRID:
  - A_1^H outputs $T, \{x_i\}_{i\in T}, |\gamma\rangle_{\mathcal{A},\mathcal{X}}$.
  - $\mathcal{X}$ is measured in the Hadamard basis to produce a k-bit string which is parsed as $\{x_i\}_{i\in\overline{T}}$, and a left-over state $|\gamma'\rangle_{\mathcal{A}}$ on register $\mathcal{A}$. Define $x = (x_1, \ldots, x_n)$. Sample $r \leftarrow \{0,1\}^m$, and re-program $H(x)$ to r.

– A_2^H is given $T, \{x_i\}_{i\in T}, |\gamma'\rangle_{\mathcal{A}}, r$, and outputs a bit.

The theorem follows by combining the two following claims.

Claim A.4.

$$|\Pr[\mathsf{REAL}=1] - \Pr[\mathsf{HYBRID}=1]| \leq \frac{2\sqrt{q}C}{2^{k/2}}.$$

Proof. Consider purifying the random oracle H on register $\mathcal{R}$, and let $|\widehat{\gamma}\rangle_{\mathcal{R},\mathcal{A},\mathcal{X}}$ be the left-over state of A_1 and the random oracle in REAL or HYBRID after A_1 outputs $(T, \{x_i\}_{i\in T})$. By Imported Theorem A.6, the state $|\widehat{\gamma}\rangle_{\mathcal{R},\mathcal{A},\mathcal{X}}$ satisfies the premise of Lemma A.7 below, where $\mathcal{F}$ is the set of 2^k sub-registers of $\mathcal{R}$ corresponding to each $x' \in \{0,1\}^n$ such that $x'_i = x_i$ for all $i \in T$.

Now, consider a reduction that receives the state ρ^{REAL} or ρ^{REPROG} from Lemma A.7, measures $\mathcal{F}_x$ in the computational basis to obtain $H(x)$, and then continues to run A_2 on input $H(x)$ (along with A_1's state on $\mathcal{A}$ and T, $\{x_i\}_{i\in T}$). In the case of ρ^{REAL}, this exactly matches the REAL game and in the case of ρ^{REPROG}, this exactly matches the HYBRID game, using the fact that $|\phi_0\rangle$ (as defined in Imported Theorem A.6) is the uniform superposition state.

□

Claim A.5.

$$|\Pr[\mathsf{HYBRID}=1] - \Pr[\mathsf{IDEAL}=1]| \leq \frac{2q\sqrt{C}}{2^{k/2}}.$$

Proof. This follows from an invocation of Imported Theorem 3.4. Consider the distribution over $(S, O_1, O_2, |\psi\rangle)$ that results from the following.

- Sample O_1 as a random oracle H,
- run A_1^H to obtain $T, \{x_i\}_{i\in T}, |\gamma\rangle_{\mathcal{A},\mathcal{X}}$,
- measure to obtain $\{x_i\}_{i\in\overline{T}}$ as in the HYBRID game, define $x = (x_1, \ldots, x_n)$, and define $S = \{x\}$,
- sample $r \leftarrow \{0,1\}^m$, and let O_2 be the same as O_1, except that $O_2(x) = r$,
- let $|\psi\rangle$ be the resulting state on register $\mathcal{A}$ along with the classical information $(T, \{x_i\}_{i\in T}, r)$.

Then, $\Pr[\mathsf{IDEAL}=1] = P_{\text{left}}$ and $\Pr[\mathsf{HYBRID}=1] = P_{\text{right}}$, so it suffices to bound P_{guess}. By Imported Theorem 3.7, P_{guess} is upper bounded by $1/2^\ell$, where ℓ is the quantum conditional min-entropy of $\{x_i\}_{i\in\overline{T}}$ given register $\mathcal{A}$. By Imported Theorem 3.9, and the fact that measuring an unentangled k-bit standard basis vector in the Hadamard basis gives k bits of quantum conditional min-entropy, P_{guess} is upper bounded by $\frac{C}{2^k}$. Thus, Imported Theorem 3.4 gives the final bound of $\frac{2q\sqrt{C}}{2^{k/2}}$.

□

□

A.3 The superposition oracle

Following [Zha19, GHHM21], we will use the fact that a quantum accesible random oracle $H : \{0,1\}^n \to \{0,1\}^m$ can be implemented as follows.

- Let $\mathcal{F}$ be a $(m \cdot 2^n)$-qubit register split into 2^n subregisters $\{\mathcal{F}_x\}_{x\in\{0,1\}^n}$ of size m. Let $|\phi_0\rangle$ be the uniform superposition state. Prepare an initial state

$$|\Psi\rangle_{\mathcal{F}} = \bigotimes_{x\in\{0,1\}^n} |\phi_0\rangle_{\mathcal{F}_x}.$$

- A query on registers $\mathcal{X}, \mathcal{Y}$ is answered with a unitary $O_{\mathcal{X},\mathcal{Y},\mathcal{F}}$ such that

$$O_{\mathcal{X},\mathcal{Y},\mathcal{F}} |x\rangle \langle x|_{\mathcal{X}} = |x\rangle \langle x|_{\mathcal{X}} \otimes (\mathsf{CNOT}^{\otimes m})_{\mathcal{F}_x:\mathcal{Y}}.$$

- Register $\mathcal{F}$ is measured to obtain a random function H.

Imported Theorem A.6 ([AMRS20, GHHM21]). *Let $|\psi_q\rangle_{\mathcal{A},\mathcal{F}}$ be the joint adversary-oracle state state after an adversary has made q queries to the superposition oracle on register $\mathcal{F}$. Then this state can be written as*

$$|\psi_q\rangle_{\mathcal{A},\mathcal{F}} = \sum_{S\subset\{0,1\}^n, |S|\leq q} |\psi_{q,S}\rangle_{\mathcal{A},\mathcal{F}_S} \otimes \left(|\phi_0\rangle^{\otimes(2^n-|S|)}\right)_{\mathcal{F}_{\overline{S}}},$$

where $|\psi_{q,S}\rangle$ are such that $\langle\phi_0|_{\mathcal{F}_x} |\psi_{q,S}\rangle_{\mathcal{A},\mathcal{F}_S} = 0$ for all $x \in S$.

A.4 Re-programming

In this section, we prove the following lemma.

Lemma A.7. *Let $|\phi_0\rangle$ be an m-qubit unit vector, and let $\mathcal{F}$ be a $(m \cdot 2^k)$-qubit register split into 2^k subregisters $\{\mathcal{F}_x\}_{x\in\{0,1\}^k}$ of m qubits. Let $\mathcal{A}$ be an arbitrary register and $\mathcal{X}$ be an k-qubit register. Consider any state $|\gamma\rangle_{\mathcal{F},\mathcal{A},\mathcal{X}}$, set $L \subseteq \{0,1\}^k$, and integer $q \in \mathbb{N}$, such that $|\gamma\rangle$ can be written as*

$$|\gamma\rangle = \sum_{u\in L} \left|\widehat{\psi}_u\right\rangle_{\mathcal{F},\mathcal{A}} \otimes |u\rangle_{\mathcal{X}},$$

where each

$$\frac{\left|\widehat{\psi}_u\right\rangle}{\| \left|\widehat{\psi}_u\right\rangle \|} = \sum_{S\subset\{0,1\}^n : |S|\leq q} |\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S} \otimes \left(|\phi_0\rangle^{(2^k-|S|)}\right)_{\mathcal{F}_{\overline{S}}},$$

and each $|\psi_{u,S}\rangle$ is orthogonal to $|\phi_0\rangle_{\mathcal{F}_x}$ for all $x \in S$. Let

- *$\rho^{\mathsf{REAL}}_{\mathcal{F},\mathcal{A},\mathcal{X}}$ be the mixed state that results from measuring $\mathcal{X}$ in the Hadamard basis to produce $x \in \{0,1\}^k$ and a left-over state $|\gamma_x\rangle_{\mathcal{F},\mathcal{A}}$, and outputting $|\gamma_x\rangle \langle\gamma_x| \otimes |x\rangle \langle x|$, and*
- *$\rho^{\mathsf{REPROG}}_{\mathcal{F},\mathcal{A},\mathcal{X}}$ be the mixed state that results from measuring $\mathcal{X}$ in the Hadamard basis to produce $x \in \{0,1\}^k$ and a left-over state $|\gamma_x\rangle_{\mathcal{F},\mathcal{A}}$, and outputting $\mathrm{Tr}_{\mathcal{F}_x}(|\gamma_x\rangle \langle\gamma_x|) \otimes |\phi_0\rangle \langle\phi_0|_{\mathcal{F}_x} \otimes |x\rangle \langle x|$.*

Then,

$$\mathsf{TD}\left(\rho^{\mathsf{REAL}}, \rho^{\mathsf{REPROG}}\right) \leq \frac{2\sqrt{q}|L|}{2^{k/2}}.$$

Proof. For each $u \in L$, let $a_u := \| \left|\widehat{\psi_u}\right\rangle \|$, and $|\psi_u\rangle := \left|\widehat{\psi_u}\right\rangle / a_u$. Consider applying the Hadamard transform to register $\mathcal{X}$ of $|\gamma\rangle$, producing

$$\sum_{x\in\{0,1\}^k, u\in L} \frac{(-1)^{u\cdot x} a_u}{2^{k/2}} |\psi_u\rangle_{\mathcal{F},\mathcal{A}} \otimes |x\rangle_{\mathcal{X}} := \sum_{x\in\{0,1\}^k} |\gamma_x\rangle_{\mathcal{F},\mathcal{A}} \otimes |x\rangle_{\mathcal{X}}$$

and then measuring in the computational basis to produce x and left-over state $|\gamma_x\rangle\langle\gamma_x|_{\mathcal{F},\mathcal{A}}$.

The lemma asks to bound the following quantity.

$$\begin{aligned}
&\frac{1}{2}\left\| \sum_{x\in\{0,1\}^k} |\gamma_x\rangle\langle\gamma_x|_{\mathcal{F},\mathcal{A}} \otimes |x\rangle\langle x| - \sum_{x\in\{0,1\}^k} \mathrm{Tr}_{\mathcal{F}_x}\left(|\gamma_x\rangle\langle\gamma_x|_{\mathcal{F},\mathcal{A}}\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} \otimes |x\rangle\langle x| \right\|_1 \\
&= \frac{1}{2}\left\| \frac{1}{2^k} \sum_{x\in\{0,1\}^k} \sum_{u_1,u_2\in L} (-1)^{(u_1\oplus u_2)\cdot x} a_{u_1} a_{u_2} |\psi_{u_1}\rangle\langle\psi_{u_2}| \otimes |x\rangle\langle x| \right. \\
&\quad \left. - \frac{1}{2^k} \sum_{x\in\{0,1\}^k} \mathrm{Tr}_{\mathcal{F}_x}\left(\sum_{u_1,u_2\in L} (-1)^{(u_1\oplus u_2)\cdot x} a_{u_1} a_{u_2} |\psi_{u_1}\rangle\langle\psi_{u_2}| \right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} \otimes |x\rangle\langle x| \right\|_1 \\
&\leq \frac{1}{2^{k+1}} \sum_{u_1,u_2\in L} a_{u_1} a_{u_2} \left\| \sum_{x\in\{0,1\}^k} \left(|\psi_{u_1}\rangle\langle\psi_{u_2}| \otimes |x\rangle\langle x|\right) - \left(\mathrm{Tr}_{\mathcal{F}_x}\left(|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} \otimes |x\rangle\langle x|\right) \right\|_1 \\
&\leq \frac{1}{2^{k+1}} \sum_{u_1,u_2\in L} a_{u_1} a_{u_2} \sum_{x\in\{0,1\}^n} \left\| |\psi_{u_1}\rangle\langle\psi_{u_2}| - \mathrm{Tr}_{\mathcal{F}_x}\left(|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} \right\|_1,
\end{aligned}$$

where the inequalities follow from the triangle inequality. Now, following the proof of [GHHM21, Theorem 6], for any u_1, u_2, and x, we can write

$$\begin{aligned}
|\psi_{u_1}\rangle\langle\psi_{u_2}| = &\langle\phi_0|_{\mathcal{F}_x}|\psi_{u_1}\rangle\langle\psi_{u_2}|\phi_0\rangle_{\mathcal{F}_x} \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} + |\psi_{u_1}\rangle\langle\psi_{u_2}|\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right) \\
&+ \left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)|\psi_{u_1}\rangle\langle\psi_{u_2}|\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{Tr}_{\mathcal{F}_x}\left(|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} = &\langle\phi_0|_{\mathcal{F}_x}|\psi_{u_1}\rangle\langle\psi_{u_2}|\phi_0\rangle_{\mathcal{F}_x} \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} \\
&+ \mathrm{Tr}_{\mathcal{F}_x}\left(\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}
\end{aligned}$$

so

$$\begin{aligned}
&\left\| |\psi_{u_1}\rangle\langle\psi_{u_2}| - \mathrm{Tr}_{\mathcal{F}_x}\left(|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x} \right\|_1 \leq \| |\psi_{u_1}\rangle\langle\psi_{u_2}|\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)\|_1 \\
&+ \|\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)|\psi_{u_1}\rangle\langle\psi_{u_2}|\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\|_1 + \|\,\mathrm{Tr}_{\mathcal{F}_x}\left(\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\|_1.
\end{aligned}$$

Now, for each x, u, define $\alpha_{x,u} = \| \langle\phi_0|_{\mathcal{F}_x}|\psi_u\rangle \|$. The first term above simplifies as

$$\| |\psi_{u_1}\rangle\langle\psi_{u_2}|\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)\|_1 = \| \langle\psi_{u_2}|\left(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right)\| = \sqrt{1 - \langle\psi_{u_2}|\phi_0\rangle\langle\phi_0|\psi_{u_2}\rangle} = \sqrt{1 - \alpha_{x,u_2,}^2}.$$

The second term above simplifies as

$$\|(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x})|\psi_{u_1}\rangle\langle\psi_{u_2}|\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\|_1 \leq \|(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x})|\psi_{u_1}\rangle\langle\psi_{u_2}|\|_1$$
$$= \|(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x})|\psi_{u_1}\rangle\| = \sqrt{1 - \langle\psi_{u_1}|\phi_0\rangle\langle\phi_0|\psi_{u_1}\rangle} = \sqrt{1 - \alpha_{x,u_1}^2},$$

where the inequality is Holder's inequality. The third term simplifies as

$$\left\|\mathrm{Tr}_{\mathcal{F}_x}\left((\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x})|\psi_{u_1}\rangle\langle\psi_{u_2}|\right) \otimes |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x}\right\|_1 = \left\|\mathrm{Tr}_{\mathcal{F}_x}\left((\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x})|\psi_{u_1}\rangle\langle\psi_{u_2}|\right)\right\|_1$$
$$\leq \left\|(\mathbb{I} - |\phi_0\rangle\langle\phi_0|_{\mathcal{F}_x})|\psi_{u_1}\rangle\langle\psi_{u_2}|\right\|_1 = \sqrt{1 - \alpha_{x,u_1}^2},$$

where the inequality is the following fact from [Hol19]: for any bounded operator T on $\mathcal{A} \otimes \mathcal{B}$, $\|\mathrm{Tr}_{\mathcal{B}}(T)\|_1 \leq \|T\|_1$.

Thus, the distinguishing advantage can be bounded by

$$\frac{1}{2^{k+1}} \sum_{u_1,u_2 \in L} a_{u_1} a_{u_2} \sum_{x \in \{0,1\}^k} 2\sqrt{1 - \alpha_{x,u_1}^2} + \sqrt{1 - \alpha_{x,u_2}^2}$$
$$\leq \frac{1}{2^k} \sum_{u_1,u_2 \in L} a_{u_1} a_{u_2} \left(\sum_{x \in \{0,1\}^k} \sqrt{1 - \alpha_{x,u_1}^2} + \sum_{x \in \{0,1\}^k} \sqrt{1 - \alpha_{x,u_2}^2} \right)$$
$$\leq \frac{1}{2^k} \sum_{u_1,u_2 \in L} a_{u_1} a_{u_2} \left(\sqrt{2^k \left(2^k - \sum_{x \in \{0,1\}^k} \alpha_{x,u_1}^2\right)} + \sqrt{2^k \left(2^k - \sum_{x \in \{0,1\}^k} \alpha_{x,u_2}^2\right)} \right),$$

where the second inequality follows from Cauchy-Schwartz.

Now, for any u,

$$\sum_{x \in \{0,1\}^k} \alpha_{x,u}^2 = \sum_{x \in \{0,1\}^k} \|\langle\phi_0|_{\mathcal{F}_x}|\psi_u\rangle\|^2\|$$
$$= \sum_{x \in \{0,1\}^k} \left\| \sum_{S \subset \{0,1\}^k : |S| \leq q} \langle\phi_0|_{\mathcal{F}_x}|\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S} \otimes \left(|\phi_0\rangle^{(2^k - |S|)}\right)_{\mathcal{F}_{\overline{S}}} \right\|^2$$
$$= \sum_{x \in \{0,1\}^k} \left\| \sum_{S \not\ni x} |\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S} \otimes \left(|\phi_0\rangle^{(2^k - |S|)}\right)_{\mathcal{F}_{\overline{S}}} \right\|^2,$$

where the last equality follows since $|\phi_0\rangle_{\mathcal{F}_x}$ is orthogonal to $|\psi_{u,S}\rangle$ for all $x \in S$, and $|\phi_0\rangle$ is normalized. Now, since each of the summands in the inner summation are pairwise orthogonal (so that we can move the summation outside of the norm), we can write

$$\sum_{x\in\{0,1\}^k}\left\|\sum_{S\not\ni x}|\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S}\otimes\left(|\phi_0\rangle^{(2^k-|S|)}\right)_{\mathcal{F}_{\overline{S}}}\right\|^2=\sum_S\sum_{x\notin S}\left\||\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S}\otimes\left(|\phi_0\rangle^{(2^k-|S|)}\right)_{\mathcal{F}_{\overline{S}}}\right\|^2$$
$$\geq(2^k-q)\sum_S\left\||\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S}\otimes\left(|\phi_0\rangle^{(2^k-|S|)}\right)_{\mathcal{F}_{\overline{S}}}\right\|^2=(2^k-q)\left\|\sum_S|\psi_{u,S}\rangle_{\mathcal{A},\mathcal{F}_S}\otimes\left(|\phi_0\rangle^{(2^k-|S|)}\right)_{\mathcal{F}_{\overline{S}}}\right\|^2$$
$$=(2^k-q)\||\psi_u\rangle\|^2=2^k-q.$$

Thus, the distinguishing advantage can be bounded by

$$\frac{2}{2^k}\sqrt{2^k\cdot q}\sum_{u_1,u_2\in L}a_{u_1}a_{u_2}\leq\frac{2\sqrt{q}|L|}{2^{k/2}},$$

since, by Cauchy-Schwartz and the fact that $\sum_{u\in L}a_u^2=1$, we can bound $\sum_{u\in L}a_u\leq\sqrt{|L|}$. □

B The random basis framework

In this section, we obtain three round OT realizing $\mathcal{F}_{\mathsf{S-ROT}}$, and we provide a modification that yields four round chosen input $\mathcal{F}_{\mathsf{OT}[\lambda]}$. The constructions make use of standard BB84 states, therefore we refer to this as the random basis framework.

Theorem B.1 (Three round random-sender-input OT.)**.** *Instantiate Protocol 9 with any non-interactive commitment scheme that is* extractable *(Definition 5.3) and* equivocal *(Definition 5.4). Then the following hold.*

- *When instantiated with the XOR extractor, there exist constants A, B such that Protocol 9 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{S-ROT}[1]}$.*
- *When instantiated with the ROM extractor, there exist constants A, B such that Protocol 9 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$.*

Furthermore, letting λ be the security parameter, q be an upper bound on the total number of random oracle queries made by the adversary, and using the commitment scheme from Section 5.2 with security parameter $\lambda_{\mathsf{com}}=2\lambda$, the following hold.

- *When instantiatied with the XOR extractor and constants $A=1100$, $B=500$, Protocol 9 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where*

$$\mu_{\mathsf{R}^*}=\frac{\sqrt{5}+1}{2^\lambda}+\frac{148(q+3200\lambda+1)^3+1}{2^{2\lambda}}+\frac{25600q\lambda}{2^\lambda},\quad\mu_{\mathsf{S}^*}=\frac{114q\sqrt{\lambda}}{2^\lambda}.$$

This requires a total of $(A+B)\lambda=1600\lambda$ BB84 states.

- *When instantiated with the ROM extractor and constants $A = 11\,000, B = 12\,000$, Protocol 9 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where*

$$\mu_{\mathsf{R}^*} = \frac{\sqrt{5}}{2^\lambda} + \frac{4q}{2^{18\lambda}} + \frac{148(q + 46000\lambda + 1)^3 + 1}{2^{2\lambda}} + \frac{368000q\lambda}{2^\lambda}, \quad \mu_{\mathsf{S}^*} = \frac{430q\sqrt{\lambda}}{2^\lambda}.$$

  This requires a total of $(A + B)\lambda = 23\,000\lambda$ BB84 states.

Theorem B.2 (Four Round chosen input string OT.)**.** *Instantiate Protocol 10 with any non-interactive commitment scheme that is* extractable *(Definition 5.3) and* equivocal *(Definition 5.4). Then there exist constants A, B such that Protocol 10 securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{OT}[\lambda]}$.*

Furthermore, letting λ be the security parameter, q be an upper bound on the total number of random oracle queries made by the adversary, and using the commitment scheme from Section 5.2 with security parameter $\lambda_{\mathsf{com}} = 2\lambda$, for constants $A = 5300, B = 5000$, Protocol 10 securely realizes $\mathcal{F}_{\mathsf{OT}[\lambda]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where

$$\mu_{\mathsf{R}^*} = \frac{\sqrt{5}}{2^\lambda} + \frac{1}{2^{9\lambda}} + \frac{148(q + 2n + 1)^3 + 1}{2^{2\lambda}} + \frac{16qn}{2^\lambda}, \quad \mu_{\mathsf{S}^*} = \frac{288q\sqrt{\lambda}}{2^\lambda}.$$

This requires a total of $(A + B)\lambda = 10\,300\lambda$ BB84 states.

B.1 Three-round random-input OT

In this section, we prove Theorem B.1.

Sender Security Let $\mathsf{SimExt} = (\mathsf{SimExt.RO}, \mathsf{SimExt.Ext})$ be the simulator for the extractable commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ (according to Definition 5.3). Let $\epsilon = 0.053$ (for XOR extractor) or 0.010748 (for ROM extractor) be a constant. We describe the simulator $\mathsf{Sim}[\mathsf{R}^*]$ against a malicious receiver R^*.

$\underline{\mathsf{Sim}[\mathsf{R}^*]}$:

- Initialize R^* and answer its oracle queries to H_C using $\mathsf{SimExt.RO}$ and in case of ROM extractor queries to H_{Ext} using the efficient on-the-fly random oracle simulator (Imported Theorem 3.6). Wait to receive n qubits and commitments $\{c_i\}_{i\in[n]}$ from R^*.
- $\{(x_i^*, \theta_i^*)\}_{i\in[n]} \leftarrow \mathsf{SimExt.Ext}(\{c_i\}_{i\in[n]})$.
- Choose $\widehat{\theta} \leftarrow \{0,1\}^n$ and measure all the received qubits in bases $\widehat{\theta}$ to get measurement outcomes $\widehat{x}$. Also, sample a random subset $T \leftarrow [n]$ s.t. $|T| = k$ and send $T, \{\widehat{\theta}_i\}_{i\in\overline{T}}$ to R^*, where $\overline{T} := [n] \setminus T$.
- Wait to receive sets I_0, I_1, where $I_0 \subseteq \overline{T}$, $I_1 = \overline{T} \setminus I_0$ and openings $\{(x_i, \theta_i), u_i\}_{i\in T}$.
- Check if $\mathsf{Rec}(\{c_i\}_{i\in T}, \{(x_i, \theta_i), u_i\}_{i\in T}) = \perp$ or if there exists $i \in T$ s.t. $\widehat{\theta}_i = \theta_i^*$ but $\widehat{x}_i \neq x_i^*$. If any of the checks fail, send abort to the ideal functionality, output R^*'s state and continue answering distinguisher's queries.

Protocol 9

Ingredients, parameters and notation.

- Security parameter λ and constants A, B. Let $n = (A+B)\lambda$ and $k = A\lambda$.
- For classical bits (x, θ), let $|x\rangle_\theta$ denote $|x\rangle$ if $\theta = 0$, and $(|0\rangle + (-1)^x |1\rangle)/\sqrt{2}$ if $\theta = 1$.
- A non-interactive extractable and equivocal commitment scheme $(\mathsf{Com}, \mathsf{Open}, \mathsf{Rec})$, where commitments to 2 bits have size $\ell := \ell(\lambda)$.
- An extractor E with domain $\{0,1\}^{n-k}$ which is either
  - The XOR function, so $E(r_1, \ldots, r_{n-k}) = \bigoplus_{i \in [n-k]} r_i$.
  - A random oracle $H_{Ext} : \{0,1\}^{n-k} \to \{0,1\}^\lambda$.

Receiver input: $b \in \{0,1\}, m \in \{0,1\}^z$, where z is the output length of the extractor.

1. **Receiver message.** R performs the following steps.
   (a) Choose $x \leftarrow \{0,1\}^n, \theta \leftarrow \{0,1\}^n$ and prepare the states $\{|x_i\rangle_{\theta_i}\}_{i\in[n]}$.
   (b) Compute $\left(\mathsf{st}, \{c_i\}_{i\in[n]}\right) \leftarrow \mathsf{Com}\left(\{(x_i, \theta_i)\}_{i\in[n]}\right)$, and send $\{|x_i\rangle_{\theta_i}, c_i\}_{i\in[n]}$ to S.
2. **Sender message.** S performs the following steps.
   (a) Choose $\widehat{\theta} \leftarrow \{0,1\}^n$. For all $i \in [n]$, measure $|x_i\rangle_{\theta_i}$ in basis $\widehat{\theta}_i$ to get outcome $\widehat{x}_i$.
   (b) Sample a random subset T of $[n]$ of size k. Send $T, \{\widehat{\theta}_i\}_{i\in\overline{T}}$ to R, where $\overline{T} := [n] \setminus T$.
3. **Receiver message.** R performs the following steps.
   (a) Divide $\overline{T}$ into 2 disjoint subsets S_0, S_1 as follows. Set $I_b = S_0$ and $I_{1-b} = S_1$, where $S_0 = \{i \mid i \in \overline{T} \wedge \theta_i = \widehat{\theta}_i\}, S_1 = \{i \mid i \in \overline{T} \wedge \theta_i \neq \widehat{\theta}_i\}$.
   (b) Compute $\{(x_i, \theta_i), u_i\}_{i\in T} \leftarrow \mathsf{Open}(\mathsf{st}, T)$.
   (c) Compute X as the concatenation of $\{x_i\}_{i\in I_b}$, set $r_b := E(X) \oplus m$, and sample $r_{1-b} \leftarrow \{0,1\}^z$, where z is the output length of extractor.
   (d) Send $I_0, I_1, \{(x_i, \theta_i), u_i\}_{i\in T}, (r_0, r_1)$ to S.
4. **Output computation** S does the following:
   (a) Abort if $\mathsf{Rec}(\{c_i\}_{i\in T}, \{(x_i, \theta_i), u_i\}_{i\in T}) = \perp$ or if $\exists i \in T$ s.t. $\theta_i = \widehat{\theta}_i$ but $x_i \neq \widehat{x}_i$.
   (b) Compute $\widehat{X}_0, \widehat{X}_1$ as the concatenation of $\{\widehat{x}_i\}_{i\in I_0}, \{\widehat{x}_i\}_{i\in I_1}$ respectively. Output $m_0 := E(\widehat{X}_0) \oplus r_0$ and $m_1 := E(\widehat{X}_1) \oplus r_1$.

Figure 9: Three-round OT protocol realizing $\mathcal{F}_{\mathsf{S-ROT}[1]}$.

Protocol 10

Ingredients, parameters and notation.

- Security parameter λ and constants A, B. Let $n = (A+B)\lambda$ and $k = A\lambda$.
- For classical bits (x, θ), let $|x\rangle_\theta$ denote $|x\rangle$ if $\theta = 0$, and $(|0\rangle + (-1)^x |1\rangle)/\sqrt{2}$ if $\theta = 1$.
- A non-interactive extractable and equivocal commitment scheme $(\mathsf{Com}, \mathsf{Open}, \mathsf{Rec})$, where commitments to 2 bits have size $\ell := \ell(\lambda)$.
- A universal hash function $h : \{0,1\}^{p(\lambda)} \times \{0,1\}^{\leq B\lambda} \to \{0,1\}^\lambda$.

Sender input: $m_0, m_1 \in \{0,1\}^\lambda$, **Receiver input**: $b \in \{0,1\}$.

1. **Receiver message.** R performs the following steps.
   (a) Choose $x \leftarrow \{0,1\}^n$, $\theta \leftarrow \{0,1\}^n$ and prepare the states $\{|x_i\rangle_{\theta_i}\}_{i\in[n]}$.
   (b) Compute $(\mathsf{st}, \{c_i\}_{i\in[n]}) \leftarrow \mathsf{Com}\left(\{(x_i, \theta_i)\}_{i\in[n]}\right)$.
   (c) Send $\{|x_i\rangle_{\theta_i}, c_i\}_{i\in[n]}$ to S.
2. **Sender message.** S performs the following steps.
   (a) Choose $\widehat{\theta} \leftarrow \{0,1\}^n$. For all $i \in [n]$, measure $|x_i\rangle_{\theta_i}$ in basis $\widehat{\theta}_i$ to get outcome $\widehat{x}_i$.
   (b) Sample a random subset T of $[n]$ of size k. Send $T, \{\widehat{\theta}_i\}_{i\in\overline{T}}$ to R, where $\overline{T} := [n] \setminus T$.
3. **Receiver message.** R performs the following steps.
   (a) Divide $\overline{T}$ into 2 disjoint subsets S_0, S_1 as follows. Set $I_b = S_0$ and $I_{1-b} = S_1$, where $S_0 = \{i \mid i \in \overline{T} \wedge \theta_i = \widehat{\theta}_i\}, S_1 = \{i \mid i \in \overline{T} \wedge \theta_i \neq \widehat{\theta}_i\}$.
   (b) Compute $\{(x_i, \theta_i), u_i\}_{i\in T} \leftarrow \mathsf{Open}(\mathsf{st}, T)$.
   (c) ~~Compute X as the concatenation of $\{x_i\}_{i\in I_b}$, set $r_b := E(X) \oplus m$, and sample $r_{1-b} \leftarrow \{0,1\}^z$, where z is the output length of extractor.~~
   (d) Send $I_0, I_1, \{(x_i, \theta_i), u_i\}_{i\in T}$, ~~$(r_0, r_1)$~~ to S.
4. **Sender message.** S and R do the following:
   - S does the following:
     - Abort if $\mathsf{Rec}(\{c_i\}_{i\in T}, \{(x_i, \theta_i), u_i\}_{i\in T}) = \perp$ or if $\exists i \in T$ s.t. $\theta_i = \widehat{\theta}_i$ but $x_i \neq \widehat{x}_i$.
     - Compute $\widehat{X}_0, \widehat{X}_1$ as the concatenation of $\{\widehat{x}_i\}_{i\in I_0}, \{\widehat{x}_i\}_{i\in I_1}$ respectively.
     - Sample $s \leftarrow \{0,1\}^{p(\lambda)}$, send $(s, ct_0 = m_0 \oplus h(s, \widehat{X}_0), ct_1 = m_1 \oplus h(s, \widehat{X}_1))$ to R.
   - R computes X as the concatenation of $\{x_i\}_{i\in I_b}$ and outputs $ct_b \oplus h(s, X)$.

Figure 10: Four-round OT protocol realizing $\mathcal{F}_{\mathsf{OT}[\lambda]}$. Parts in blue are different than the 3-round OT protocol realizing $\mathcal{F}_{\mathsf{S-ROT}[1]}$ in Protocol 9.

- Compute the set $Q = \{i \mid i \in I_0 \wedge \theta_i^* \neq \widehat{\theta}_i\}$. If $|Q| \geq \frac{(1-\epsilon)(n-k)}{4}$, then set $b = 1$, else set $b = 0$. Compute $m_b = \{\widehat{x}_i\}_{i \in I_b}$, send (b, m_b) to the ideal functionality and output R^*'s state.
- Continue answering distinguisher's queries to H_C (and H_{Ext}) using $\mathsf{SimExt.RO}$ (and the efficient on-the-fly random oracle simulator).

Consider a distinguisher $(\mathsf{D}, \boldsymbol{\sigma})$ such that R^*, D make a total of q queries combined to H_C (and H_{Ext}). Consider the following sequence of hybrids:

- Hyb_0: This is the real world interaction between R^*, S. Using the notation of Definition 3.2, this is a distribution over $\{0,1\}$ denoted by $\Pi[\mathsf{R}^*, \mathsf{D}, \top]$.
- Hyb_1: This is identical to the previous hybrid, except that queries to H_C are answered using $\mathsf{SimExt.RO}$, and $\{(x_i^*, \theta_i^*)\}_{i \in [n]} \leftarrow \mathsf{SimExt.Ext}(\{c_i\}_{i \in [n]})$ is run after R^* outputs its first message. After R^* sends its openings in the third round, the sender performs the following checks: check if $\mathsf{Rec}(\{c_i\}_{i \in T}, \{(x_i, \theta_i), u_i\}_{i \in T}) = \perp$ or if there exists $i \in T$ s.t. $\theta_i^* = \widehat{\theta}_i$ but $x_i^* \neq \widehat{x}_i$ (note that it uses x_i^*, θ_i^* for its second check, rather than x_i, θ_i as in the honest sender strategy). It then continues with the rest of the protocol as in the honest sender strategy.
- Hyb_2: This is the result of $\mathsf{Sim}[\mathsf{R}^*]$ interacting in $\widetilde{\Pi}_{\mathsf{S-ROT}[1]}[\mathsf{Sim}[\mathsf{R}^*], \mathsf{D}, \top]$ (or $\widetilde{\Pi}_{\mathsf{S-ROT}[\lambda]}[\mathsf{Sim}[\mathsf{R}^*], \mathsf{D}, \top]$).

Claim B.3. $|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]| \leq \frac{148(q+2n+1)^3+1}{2^{2\lambda}} + \frac{16qn}{2^\lambda}$.

Proof. This follows by a direct reduction to extractability of the commitment scheme (Definition 5.3). Indeed, let $\mathsf{Adv}_{\mathsf{Commit}}$ be the machine that runs Hyb_0 until R^* outputs its message, which includes $\{c_i\}_{i \in [n]}$. Let $\mathsf{Adv}_{\mathsf{Open}}$ be the machine that takes as input the rest of the state of Hyb_0, and runs it till the third round to get set T and openings $\{(x_i, \theta_i), u_i\}_{i \in T}$, and outputs T and these openings. Let D be the machine that runs the rest of Hyb_0 and outputs a bit.

Then, plugging in $\lambda_{\mathsf{com}} = 2\lambda$, Definition 5.3 when applied to $(\mathsf{Adv}_{\mathsf{Commit}}, \mathsf{Adv}_{\mathsf{Open}}, \mathsf{D})$ implies that the hybrids cannot be distinguished except with probability

$$\frac{148(q+2n+1)^3+1}{2^{2\lambda}} + \frac{16qn}{2^\lambda},$$

since we are committing to a total of $2n$ bits. □

Claim B.4. *When instantiated with the XOR extractor and constants $A = 1100, B = 500$, we have,*

$$|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{\sqrt{5}+1}{2^\lambda}.$$

And when instantiated with the ROM extractor and constants $A = 11\,000, B = 12\,000$, we have,

$$|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{\sqrt{5}}{2^\lambda} + \frac{4q}{2^{18\lambda}}.$$

Proof. In Hyb_1, while both R_0, R_1 were set according to the honest sender strategy, in Hyb_2, for b as defined by the simulator, R_{1-b} (output by the honest sender) is set as a uniformly random string. In the following, we show that in either hybrid R_{1-b} is statistically close to a uniformly random string given R^*'s view which would imply this claim. We setup some notation before proceeding:

- Let $\mathcal{X} = \{\mathcal{X}_i\}_{i\in[n]}$ denote the n registers, each holding a single qubit, sent by R^* in its first round.
- For a vector $\mathbf{x} = (x_1, \ldots x_n)$, and a set $S \subseteq [n]$, let $\mathbf{x}_S$ denotes the values of $\mathbf{x}$ indexed by S.
- For vectors $\mathbf{x}, \boldsymbol{\theta} \in \{0,1\}^n$, let $|\mathbf{x}_{\boldsymbol{\theta}}\rangle$ denote the state on n single-qubit registers, where register i contains the state $|\mathbf{x}_i\rangle$ prepared in the $\boldsymbol{\theta}_i$ basis.
- For a set $T \subseteq [n]$, let $\overline{T} \coloneqq [n] \setminus T$.
- Using notation as defined in Section 3, for a subset $S \subseteq [n]$ and two vectors $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$, $\Delta(\mathbf{x}_S, \mathbf{y}_S)$ denotes the fraction of values $\mathbf{x}_i, i \in S$ s.t. $\mathbf{x}_i \neq \mathbf{y}_i$.

Consider the following quantum sampling game (defined as in Section 3.6):

- Fix some state on register $\mathcal{X}$ and some strings $\mathbf{x}^*, \boldsymbol{\theta}^* \in \{0,1\}^n$.
- Sample $T \subseteq [n]$ as a uniform random subset of size k.
- Sample $\widehat{\boldsymbol{\theta}} \leftarrow \{0,1\}^n$, and let $S = \{i \,|\, i \in T \wedge \widehat{\boldsymbol{\theta}}_i = \boldsymbol{\theta}^*_i\}$. For each $i \in S$, measure register $\mathcal{X}_i$ in basis $\boldsymbol{\theta}^*_i$ to get outcome x_i.
- Let $\mathbf{x}_S$ be the concatenation of $\{x_i\}_{i\in S}$. Output $\Delta(\mathbf{x}_S, \mathbf{x}^*_S)$.

This quantum sampling game corresponds to the execution in either hybrid, where register $\mathcal{X}$ is the register sent by R^* in its first message, $(\mathbf{x}^*, \boldsymbol{\theta}^*)$ represent the values extracted by running $\mathsf{SimExt.Ext}$, and $\widehat{\boldsymbol{\theta}}$ respresents the bases sampled by the sender. By Definition 3.11, the quantum error probability $\epsilon^{\delta}_{\mathsf{quantum}}$ of the above game corresponds to the trace distance between the initial state on the register $\mathcal{X}$ and an "ideal" state, where it holds with certainty that register $\mathcal{X}$ is in a superposition of states $|\mathbf{x}_{\boldsymbol{\theta}^*}\rangle$ for $\mathbf{x}$ s.t. $|\Delta(\mathbf{x}_{\overline{T}}, \mathbf{x}^*_{\overline{T}}) - \Delta(\mathbf{x}_S, \mathbf{x}^*_S)| < \delta$. In the following we find a bound $\epsilon^{\delta}_{\mathsf{quantum}}$ and show that given the state on register $\mathcal{X}$ is in the ideal state described above, the two hybrids are statistically indistinguishable.

SubClaim B.5. *$\epsilon^{\delta}_{\mathsf{quantum}} \leq \frac{\sqrt{5}}{2^\lambda}$ when instantiated with the XOR extractor (with $\delta = 0.1183$) or with the ROM extractor (with $\delta = 0.0267$).*

Proof. Using Imported Theorem 3.12, $\epsilon^{\delta}_{\mathsf{quantum}}$ can be bound by the square root of the classical error probability, $\epsilon^{\delta}_{\mathsf{classical}}$, of the corresponding classical sampling game, described as follows:

- Given a string $\mathbf{q} \in \{0,1\}^n$, sample $T \subseteq [n]$ as a uniform random subset of size k.
- Sample a subset $S \subseteq T$ as follows: sample bits $\mathbf{b} \leftarrow \{0,1\}^n$. Let set $S = \{i \,|\, i \in T \wedge \mathbf{b}_i = 1\}$.
- Output $\omega(\mathbf{q}_S)$.

Since setting S as above is equivalent to choosing a random subset of T (chosen uniformly among all possible subsets of T), using the analysis in Appendix D.2, we get, for $0 < \beta < 1$ and $0 < \eta < \delta$,

$$\epsilon^{\delta}_{\mathsf{classical}} \leq 2\exp\left(-2\left(1-\frac{k}{n}\right)^2\eta^2 k\right) + 2\exp\left(-(\delta-\eta)^2(1-\beta)k\right) + \exp\left(-\frac{\beta^2 k}{2}\right).$$

For the case of XOR extractor, for $\delta = 0.1183, \beta = 0.051, \eta = 0.081$, we have each of the expressions inside the exp terms above bounded by $\frac{1}{2^{2\lambda}}$, giving us $\epsilon^{\delta}_{\mathsf{classical}} \leq \frac{5}{2^{2\lambda}}$, which means $\epsilon^{\delta}_{\mathsf{quantum}} \leq \frac{\sqrt{5}}{2^{\lambda}}$.

And for the case of ROM extractor, for $\delta = 0.0267, \beta = 0.01588, \eta = 0.01538$, we achieve the same bounds and get $\epsilon^{\delta}_{\mathsf{quantum}} \leq \frac{\sqrt{5}}{2^{\lambda}}$. □

SubClaim B.6. *Given the state on register $\mathcal{X}$ is in a superposition of states $|\mathbf{x}_{\boldsymbol{\theta}^*}\rangle$ s.t. $|\Delta(\mathbf{x}_{\overline{T}}, \mathbf{x}^*_{\overline{T}}) - \Delta(\mathbf{x}_S, \mathbf{x}^*_S)| < \delta$, where $S = \{i \,|\, i \in T \ \wedge \ \widehat{\theta}_i = \theta^*_i\}$, the following holds:*

- *When instantiated with the XOR extractor and $\delta = 0.1183, A = 1100, B = 500$,*

$$|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{1}{2^{\lambda}}$$

- *When instantiated with ROM extractor and $\delta = 0.0267, A = 11\,000, B = 12\,000$,*

$$|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{4q}{2^{18\lambda}}$$

Proof. Note that the checks performed by the sender once R^* sends the openings in the third round correspond to checking if $\Delta(\mathbf{x}_S, \mathbf{x}^*_S) = 0$. If this check fails, the sender aborts and the hybrids are perfectly indistinguishable. So it suffices to analyze the states on $\mathcal{X}$ that are in a superposition of states $|\mathbf{x}_{\boldsymbol{\theta}^*}\rangle$ s.t. $\Delta(\mathbf{x}_S, \mathbf{x}^*_S) = 0$ and $\Delta(\mathbf{x}_{\overline{T}}, \mathbf{x}^*_{\overline{T}}) < \delta$.

Recall that in either hybrid, for $i \in \overline{T}$, the sender chooses bit $\widehat{\theta}_i \leftarrow \{0, 1\}$ and measures register $\mathcal{X}_i$ in basis $\widehat{\theta}_i$. Using Hoeffding's inequality (stated in Appendix D), the number of positions $i \in \overline{T}$ s.t. $\widehat{\theta}_i \neq \theta^*_i$ is at least $\frac{(1-\epsilon)(n-k)}{2}$ except with probability $\exp\left(-\frac{\epsilon^2(n-k)}{2}\right)$. Hence, given any partition (I_0, I_1) of $\overline{T}$ that R^* provides in the third round, it holds that there exists a bit b and partition I_{1-b} s.t. there are at least $\frac{(1-\epsilon)(n-k)}{4}$ positions i with $\widehat{\theta}_i \neq \theta^*_i$ except with probability $\exp\left(-\frac{\epsilon^2(n-k)}{2}\right)$. Call this subset of positions in I_{1-b} as M. Also, note that in Hyb_3, the bit b used by $\mathsf{Sim}[\mathsf{R}^*]$ is the same bit used above.

- *XOR extractor*: For the case of XOR extractor, for $\epsilon = 0.053, n - k = B\lambda, B = 500$, this probability above $\exp\left(-\frac{\epsilon^2(n-k)}{2}\right) < \frac{1}{2^{\lambda}}$.

  Combining the two parts above, we have that register $\mathcal{X}_M = \{\mathcal{X}_i\}_{i \in M}$ is in a superposition of states $\left|\mathbf{x}_{\boldsymbol{\theta}^*_M}\right\rangle$ s.t. $\Delta(\mathbf{x}, \mathbf{x}^*_M) < \frac{\delta(n-k)}{(1-\epsilon)(n-k)/4} = \frac{4\delta}{1-\epsilon} \approx 0.49968 < \frac{1}{2}$ (for $\delta = 0.1183, \epsilon = 0.053$). Using Theorem 4.1, it then follows that m_{1-b} is uniformly random string, hence proving the given claim.

- *ROM extractor*: For the case of ROM extractor, for $\epsilon = 0.01013, n - k = B\lambda, B = 13\,500$, this probability above $\exp\left(-\frac{\epsilon^2(n-k)}{2}\right) < \frac{1}{2^{\lambda}}$.

  In a similar way as above, we have that register $\mathcal{X}_M = \{\mathcal{X}_i\}_{i \in M}$ is in a superposition of states $\left|\mathbf{x}_{\boldsymbol{\theta}^*_M}\right\rangle$ s.t. $\Delta(\mathbf{x}, \mathbf{x}^*_M) < \frac{\delta(n-k)}{(1-\epsilon)(n-k)/4} = \frac{4\delta}{1-\epsilon} < 0.10796$ (for $\delta = 0.0267, \epsilon = 0.010748$). We now apply Theorem 4.2 with random oracle input size $n - k$, register $\mathcal{X}$ of size $|M|$, and $|L| \leq 2^{h_b(0.10796)(1-\epsilon)(n-k)/4}$. Note that, when applying this theorem, we are fixing the outcome of the $n - k - |M|$ bits of the random oracle input that are measured in basis θ^*_i, and

setting $\mathcal{X}$ to contain the $|M|$ registers are measured in basis $\widehat{\theta}_i = \theta_i^* \oplus 1$. This gives a bound of

$$\frac{4 \cdot q \cdot 2^{h_b(0.10796)(1-\epsilon)(n-k)/4}}{2^{(1-\epsilon)(n-k)/8}} = \frac{4q}{2^{\left(\frac{1}{2}-h_b(0.10796)\right)(1-\epsilon)(n-k)/4}}$$
$$= \frac{4q}{2^{\left(\frac{1}{2}-h_b(0.10796)\right)(1-\epsilon)B\lambda/4}} \leq \frac{4q}{2^{18\lambda}}$$

for $B = 12\,000, \epsilon = 0.010748$.

□

□

Receiver Security. Let $\mathsf{SimEqu} = (\mathsf{SimEqu.RO}, \mathsf{SimEqu.Com}, \mathsf{SimEqu.Open})$ be the simulator for the equivocal commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ (according to Definition 5.3). We describe the simulator $\mathsf{Sim}[\mathsf{S}^*]$ against a malicious receiver S^*. Sim will answer random oracle queries to H_C using $\mathsf{SimEqu.RO}$. Additionally, if randomness extractor E in the protocol is H_{Ext}, then its simulation is accomplished via queries to an on-the-fly random oracle simulator $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ as mentioned in Imported Theorem 3.6.

The Simulator.

1. Prepare n EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[n]}$
2. Compute the commitments strings $\{c_i\}_{i\in[n]}$ by calling $\mathsf{SimEqu.Com}$ for the underlying commitment scheme.
3. Send $\{\mathcal{S}_i\}_{i\in[n]}$ and $\{c_i\}_{i\in[n]}$ to S^*.
4. Receive $T, \{\widehat{\theta}_i\}_{i\in\overline{T}}$ from S^*.
5. For all $i \in T$, sample $\theta_i \leftarrow \{+, \times\}$ and measure $\mathcal{R}_i$ in the basis θ_i to obtain outcome x_i. For all $i \in \overline{T}$, measure $\mathcal{R}_i$ in the basis $\widehat{\theta}_i$ to obtain outcome $\widetilde{x}_i$.
6. Call $\mathsf{SimEqu.Open}(\{x_i, \theta_i\}_{i\in[T]})$ of the underlying commitment scheme to obtain openings $\{(x_i, \theta_i), u_i\}_{i\in[T]}$.
7. Generate a partition I_0, I_1 of $\overline{T}$ as follows: for every $i \in \overline{T}$, flip a random bit b_i and place $i \in I_{b_i}$.
8. Receives m_0, m_1 from $\mathcal{F}_{\mathsf{S-ROT}}$ functionality.
9. Set $r_0 = E(\{\widetilde{x}_i\}_{i\in I_0}) \oplus m_0$, $r_1 = E(\{\widetilde{x}_i\}_{i\in I_1}) \oplus m_1$.
10. Send $I_0, I_1, \{(x_i, \theta_i), u_i\}_{i\in T}, (r_0, r_1)$ to S^*.

Analysis. Fix any adversary $\{\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)\}_{\lambda\in\mathbb{N}}$, where S^*_λ is a QIOM that corrupts the sender, D_λ is a QOM, and (b_λ, m_λ) is the input of the honest receiver. For any receiver input $b_\lambda \in \{0,1\}, m_\lambda \in \{0,1\}^v$, where v is the output lenght of extractor, consider the random variables $\Pi[\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)]$ and $\widetilde{\Pi}_{\mathcal{F}^{\mathsf{OT}}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)]$ according to Definition 3.2 for the protocol in Figure 9. Let $q(\cdot)$ denote an upper bound on the number of queries of S^*_λ and D_λ. We will show that :

$$\left|\Pr[\Pi[\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)] = 1] - \Pr\left[\widetilde{\Pi}_{\mathcal{F}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)] = 1\right]\right| = \mu(\lambda, q(\lambda))$$

where the term on the right corresponds to the security error in the equivocal commitment.

This is done via a sequence of hybrids, as follows [17]:

- Hyb_0 : The output of this hybrid is the *real* distribution $\Pi[\mathsf{S}^*_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)]$.
- Hyb_1 : This is the same as the previous hybrid except that instead of running the Com and Open algorithm, as in Figure 9, the challenger now answers random oracle queries to H_C using $\mathsf{SimEqu.RO}$, the random oracle simulator for the commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$. Additionally, it performs the following modified steps on behalf of R:
  - Prepare the commitments by calling $\mathsf{SimEqu.Com}$ for the underlying commitment protocol.
  - Prepare the opening by calling $\mathsf{SimEqu.Open}(\{x_i, \theta_i\}_{i\in[n]})$, where $\{x_i, \theta_i\}_{i\in[n]}$ are as defined in the previous hybrid.
- Hyb_2 : This is the same as the previous hybrid except the following change: in protocol round 1, the challenger calls Algorithm EPR-to-BB84(i) for every $i \in [n]$ to obtain $|x_i\rangle_{\theta_i}$.

  Algorithm EPR-to-BB84 (i)**:**

  1. Sample EPR pair on registers $\mathcal{S}_i, \mathcal{R}_i$.
  2. Randomly sample a basis $\theta_i \leftarrow \{+, \times\}$
  3. Measure $\mathcal{R}_i$ in the basis θ_i and let the outcome be x_i
  4. Use $\mathcal{S}_i$ as a BB84 state $|x_i\rangle_{\theta_i}$
- Hyb_3: This is the same as the previous hybrid, except that in protocol round 1, the challenger sends halves of n EPR pairs $\{\mathcal{S}_i\}_{i\in[n]}$, prepared by executing Step 1 of the algorithm EPR-to-BB84, to S^* while retaining $\{\mathcal{R}\}_{i\in[n]}$ with itself. After round 2, the challenger runs Steps 2 and 3 of the Algorithm EPR-to-BB84 for every $i \in [n]$ to obtain $\{x_i, \theta_i\}_{i\in[n]}$. The resulting values $\{x_i, \theta_i\}_{i\in T}$ are used as inputs to $\mathsf{SimEqu.Open}$ to prepare openings in round 3. Step 4 of the Algorithm EPR-to-BB84(i) is not relevant in this hybrid.
- Hyb_4: This is the same as the previous hybrid, except the following changes. After round 2, the challenger runs the Steps 2-3 of algorithm EPR-to-BB84 for every $i \in [T]$, leaving $\{\mathcal{R}_i\}_{i\in\overline{T}}$

[17] If randomness extractor E in the protocol is H_{Ext}, then there will be an additonal hybrid between Hyb_0 and Hyb_1 where we switch from using H_{Ext} to simulating it using an efficient on-the-fly random oracle simulator $\mathsf{Sim}_{\mathsf{RO}}.\mathsf{RO}$ as mentioned in Imported Theorem 3.6. This hybrid's (perfect) indistinguishability will follow directly from the indistinguishable simulation property as mentioned in Imported Theorem 3.6.

unmeasured. It generates a partition I_0, I_1 of $\overline{T}$ as follows: for every $i \in \overline{T}$, flip a random bit b_i and place $i \in I_{b_i}$.

For all $i \in \overline{T}$, the challenger measures $\{\mathcal{R}_i\}_{i\in\overline{T}}$ in the basis $\{\widehat{\theta}_i\}_{i\in\overline{T}}$ where $\{\widehat{\theta}_i\}_{i\in\overline{T}}$ was obtained from S^* in round 2. Denote measurement outcomes by $\{\widetilde{x}_i\}_{i\in\overline{T}}$. Using the resulting outcomes, the challenger sets $r_b := E(\{\widetilde{x}_i\}_{i\in I_b}) \oplus m$.

- Hyb_5 : This is the same as the previous hybrid, except that in Round 3, the challenger sets $r_0 = E(\{\widetilde{x}_i\}_{i\in I_0}) \oplus m_0$, $r_1 = E(\{\widetilde{x}_i\}_{i\in I_1}) \oplus m_1$ where m_0, m_1 are received from $\mathcal{F}_{\mathsf{S-ROT}}$

  The output of this experiment is identical to the *ideal* distribution $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}}}[\mathsf{Sim}_\lambda, \mathsf{D}_\lambda, (b_\lambda, m_\lambda)]$.

We show that $|\Pr[\mathsf{Hyb}_5 = 1] - \Pr[\mathsf{Hyb}_0 = 1]| \leq \mu(\lambda, q(\lambda))$, where $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ is a $\mu(\lambda, q(\lambda))$-equivocal bit commitment scheme, where $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ is a $\mu(\lambda, q(\lambda))$-equivocal bit commitment scheme, where $\mu(\lambda, q, n_{\mathsf{com}}) = \frac{2qn_{\mathsf{com}}^{1/2}}{2^{\lambda_{\mathsf{com}}/2}}$ for the specific commitment scheme that we construct in Section 5.2, where n_{com} is the number of bit commitments and λ_{com} is the security parameter for the commitment scheme. Later, we will set $n_{\mathsf{com}} = c_1\lambda$ and $\lambda_{\mathsf{com}} = c_2\lambda$ for some fixed constants c_1, c_2. Thus μ will indeed be a function of λ and q. We now procced with the proof by arguing the computational indistinguishability of each pair of consecutive hybrids in the above sequence.

Claim B.7. $|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]| \leq \mu(\lambda, q(\lambda))$.

Proof. Suppose there exists an adversary Adv_λ corrupting S, a distinguisher D_λ, quantuam states $\rho_\lambda, \sigma_\lambda$ and a bit b such that,

$$\left|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]\right| > \mu(\lambda, q(\lambda))$$

We will construct a reduction $\{\mathsf{Adv}^*_\lambda = (\mathsf{Adv}_{\mathsf{RCommit},\lambda}, \mathsf{Adv}_{\mathsf{ROpen},\lambda}, \mathsf{D}^*_\lambda)\}_{\lambda\in\mathbb{N}}$ that makes at most $q(\lambda)$ queries to the random oracle, and contradicts the μ-equivocality of the underlying commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ as defined in Definition 5.4. In the following reduction, all random oracle queries to H_C will be answered by the equivocal commitment challenger.

$\mathsf{Adv}_{\mathsf{RCommit},\lambda}(\rho_\lambda)$:

- Initalize the OT protocol with between honest receiver R and $\mathsf{Adv}(\rho_\lambda)$ corrupting S.
- After R samples $\{(x_i, \theta_i)\}_{i\in[n]}$, output the intermediate state $\rho^*_{\lambda,1}$ representing the joint state of S and R along with $\{(x_i, \theta_i)\}_{i\in[n]}$.

The commitment challenger obtains $\{(x_i, \theta_i)\}_{i\in[n]}$ and returns a set of commitments $\{\mathsf{com}_i\}_{i\in[n]}$.

$\mathsf{Adv}_{\mathsf{ROpen},\lambda}(\rho^*_{\lambda,1}, \{\mathsf{com}_i\}_{i\in[n]})$: Use $\rho^*_{\lambda,1}$ to initialize the joint state of S and R, and $\{\mathsf{com}_i\}_{i\in[n]}$ as commitments of R in the protocol. Output the new joint state $\rho^*_{\lambda,2}$ after R has computed I_0 and I_1.

The challenger returns $\{u_i\}_{i\in[n]}$ which is then fed to the following distinguisher (along with the information $\{\mathsf{com}_i, (x_i, \theta_i)\}_{i\in[n]}$ from the aforementioned execution).

$\mathsf{D}^*_\lambda(\rho^*_{\lambda,2}, \{\mathsf{com}_i, (x_i, \theta_i), u_i\}_{i\in[n]})$:

- Use $\rho^*_{\lambda,2}$ to initialize the joint state of S and R. Run it until completion using $\{(x_i, u_i)\}_{i\in T}$ as openings of R.
- Let τ^*_λ be the final state of Adv and y^* be the output of R. Run $\mathsf{D}_\lambda(\sigma_\lambda, \tau^*_\lambda, y^*)$ and output the bit b returned by it.

By construction, when the challenger executes $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C})$, the reduction will generate a distribution identical to Hyb_0. Similarly, when the challenger executes $(\mathsf{SimEqu.Com}, \mathsf{SimEqu.Open})$ algorithms, the reduction will generate a distribution identical to Hyb_1. Therefore, the reduction directly contradicts the μ-equivocality of the underlying commitment scheme $(\mathsf{Com}^{H_C}, \mathsf{Open}^{H_C}, \mathsf{Rec}^{H_C})$ according to Definition 5.4, as desired.

□

Claim B.8. $\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1]$

Proof. The only difference between the two hybrids is a syntactic change in the way BB84 states are sampled in round 1. The distribution $(x_i, \theta_i, |x_i\rangle_{\theta_i})_{i\in[16\lambda]}$ resulting from these syntactically different sampling strategies is identical in both hybrids. □

Claim B.9. $\Pr[\mathsf{Hyb}_2 = 1] = \Pr[\mathsf{Hyb}_3 = 1]$

Proof. Hyb_3 constitutes a purification of the receiver's strategy in round 1 and since actions on disjoint subsystems commute, this does not affect the joint distribution of the sender's view and receiver output. □

Claim B.10. $\Pr[\mathsf{Hyb}_3 = 1] = \Pr[\mathsf{Hyb}_4 = 1]$

Proof. Hyb_4 constitutes a purification of the receiver's strategy in round 3 and since actions on disjoint subsystems commute, this does not affect the joint distribution of the sender's view and receiver output. □

Claim B.11. $\Pr[\mathsf{Hyb}_4 = 1] = \Pr[\mathsf{Hyb}_5 = 1]$

Proof. Assuming correctness of $\mathcal{F}_{\mathsf{S-ROT}}$, the two hybrids are identical.Suppose ideal world receiver's input is $(b = 0, m)$. In this case, $\mathcal{F}_{\mathsf{S-ROT}}$ sends $m_0 = m, m_1$ to the challenger where $m_1 \leftarrow \{0,1\}^v$. In Hyb_5, this would lead to $r_0 = E(\{\widetilde{x_i}\}_{i\in I_0}) \oplus m$ (which is same as Hyb_4) and $r_1 = E(\{\widetilde{x_i}\}_{i\in I_1}) \oplus m_1$ (which is uniformly random as in Hyb_4). Moreover, the output on sender side in Hyb_5 is $(E(\{\widetilde{x_i}\}_{i\in I_0}) \oplus r_0, E(\{\widetilde{x_i}\}_{i\in I_1}) \oplus r_1)$ = (m, m_1) as desired. The case when ideal world receiver bit b is 1 can be proved in a similar way. Therefore for any fixing of the adversary's state and receiver's input, the two hybrids result in identical distributions. □

Combining all the claims, we get that $|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_5 = 1]| \leq \mu(\lambda, q(\lambda))$. In Theorem 5.12, we derived $\mu(\lambda, q, n_{\mathsf{com}}) = \frac{2qn_{\mathsf{com}}^{1/2}}{2^{\lambda_{\mathsf{com}}/2}}$. We will now state the parameters for n_{com} and λ_{com}.

- *XOR extractor*: Plugging $\lambda_{\mathsf{com}} = 2\lambda$, $n_{\mathsf{com}} = 2n$ (as we are committing to 2 bits at a time) where $n = 1600\lambda$ (this setting of n is the same as that needed in the sender security part of the proof), we get $\frac{114q\sqrt{\lambda}}{2^\lambda}$ security against a malicious sender.
- *ROM extractor*: Plugging $\lambda_{\mathsf{com}} = 2\lambda$, $n_{\mathsf{com}} = 2n$ (as we are committing to 2 bits at a time) where $n = 23\,000\lambda$ (this setting of n is the same as that needed in the sender security part of the proof), we get $\frac{430q\sqrt{\lambda}}{2^\lambda}$ security against a malicious sender.

B.2 Four-round chosen-input OT

In this section, we prove Theorem B.2.

Sender Security The proof of this follows along a similar line as the proof of security against a malicious receiver for the 3-round protocol described before. We only describe the changes to the corresponding proof from before over here.

The only change to the simulator (compared to $\mathsf{Sim}[\mathsf{R}^*]$ for the 3-round protocol described earlier) is that after computing b at the end of third round, it sends b to $\mathcal{F}_{\mathsf{OT}[\lambda]}$ to receive back m_b, sets $m_{1-b} := 0^\lambda$, and thereafter completes the protocol as in the honest sender strategy. Once it outputs R^*'s state, it continues answering distinguisher's queries using $\mathsf{SimExt.RO}$.

The hybrids $(\mathsf{Hyb}_0, \mathsf{Hyb}_1, \mathsf{Hyb}_2)$ also remain same as in the proof before, and the indistinguishability between $\mathsf{Hyb}_0, \mathsf{Hyb}_1$ proceeds as before. The indistiguishability between $\mathsf{Hyb}_1, \mathsf{Hyb}_2$ follows using a slightly modified analysis of SubClaim B.5 and SubClaim B.6. Specifically, for the proof of SubClaim B.5, we use $\delta = 0.04, \beta = 0.023, \eta = 0.0236, A = 5300, B = 5000$, and obtain the same result of $\epsilon^{\delta}_{\mathsf{quantum}} \leq \frac{\sqrt{5}}{2^\lambda}$.

For the proof of SubClaim B.5, we use a different analysis as follows: set $\epsilon = 0.017$. By assumption of the subclaim and using a similar analysis as the proof of SubClaim B.5, the state on $\mathcal{X}$ is in a superposition of states $|\mathbf{x}_{\boldsymbol{\theta}^*}\rangle$ s.t. $\Delta(\mathbf{x}_S, \mathbf{x}^*_S) = 0$ and $\Delta(\mathbf{x}_{\overline{T}}, \mathbf{x}^*_{\overline{T}}) < \delta$. Using Hoeffding's inequality, the number of positions $i \in \overline{T}$ s.t. $\widehat{\theta}_i \neq \theta^*_i$ is at least $\frac{(1-\epsilon)(n-k)}{2}$ except with probability $\exp\left(-\frac{\epsilon^2(n-k)}{2}\right)$. For $\epsilon = 0.053, n-k = B\lambda, B = 5000$, this probability is $< \frac{1}{2^\lambda}$. Next, as before, given any partition (I_0, I_1) of $\overline{T}$ that R^* sends in the third round, it holds that there exists a bit b and partition I_{1-b} s.t. there are at least $\frac{(1-\epsilon)(n-k)}{4}$ positions i with $\widehat{\theta}_i \neq \theta^*_i$.

Hence, $\mathcal{X}_{I_{1-b}}$ is in a superposition of states $\left|\mathbf{x}_{\left(\boldsymbol{\theta}^*_{I_{1-b}}\right)}\right\rangle$ s.t. $\Delta(\mathbf{x}, \mathbf{x}^*_{I_{1-b}}) < \delta$ and at least $\frac{(1-\epsilon)(n-k)}{4}$ positions of it are measured in basis $\widehat{\theta}_i \neq \theta^*_i$. Let $\widehat{X}_{1-b}$ be the string obtained by concatenating the measurement outcomes of I_{1-b}. Also, let $\mathcal{C}$ denote the register for the complete system (including the private state of R^*), but excluding register $\mathcal{X}$. Using Imported Theorem 3.9, we get,

$$\begin{aligned}\mathbf{H}_\infty(\widehat{X}_{1-b} \,|\, \mathcal{X}_{I_b}, \mathcal{C}) &\geq \frac{(1-\epsilon)(n-k)}{4} - h_b(\delta)|I_{1-b}| \\ &\geq \frac{(1-\epsilon)(n-k)}{4} - h_b(\delta)(n-k)\end{aligned}$$

For $\epsilon = 0.017, \delta = 0.04, n-k = B\lambda, B = 5000$, we get, $\mathbf{H}_\infty(\widehat{X}_{1-b} \,|\, \mathcal{X}_{I_b}, \mathcal{C}) \geq 17\lambda$, and also, that $\mathbf{H}_\infty(\widehat{X}_{1-b} \,|\, \widehat{X}_{I_b}, \mathcal{C}) \geq 17\lambda$. Using Imported Theorem 3.8, we then get that $(s, h(s, \widehat{X}_{I_{1-b}}))$ is $\frac{1}{2^{9\lambda}}$ statistically close to uniformly random string. Hence, $|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{\sqrt{5}}{2^\lambda} + \frac{1}{2^{9\lambda}}$.

Receiver Security The proof of this is similar to the proof of receiver security for the 3 round random basis protocol described before. We only describe the changes here. The only change to the simulator is the following: Instead of executing Steps 8-10, it computes $\widetilde{X_0}, \widetilde{X_1}$ as the concatenation of $\{\widetilde{x_i}\}_{i \in I_0}, \{\widetilde{x_i}\}_{i \in I_1}$ respectively. It sends $I_0, I_1, \{(x_i, \theta_i), u_i\}_{i \in T}$ to S. On receiving s, ct_0, ct_1 from S in Round 4, it extracts $m_0 := ct_0 \oplus h(s, \widetilde{X_0})$, $m_1 := ct_1 \oplus h(s, \widetilde{X_1})$, and sends m_0, m_1 to $\mathcal{F}_{\mathsf{OT}}$.

The hybrids $\mathsf{Hyb}_0, \mathsf{Hyb}_1, \mathsf{Hyb}_2, \mathsf{Hyb}_3$ remain same as before. In Hyb_4, instead of setting r_b, the challenger just outputs $m_b := ct_b \oplus h(s, \{\widetilde{x_i}\}_{i \in I_b})$ after Round 4. In Hyb_5, instead of setting r_0, r_1,

the challenger extracts $m_0 := ct_0 \oplus h(s, \{x_i\}_{i \in I_0})$, $m_1 := ct_1 \oplus h(s, \{x_i\}_{i \in I_1})$ after Round 4, and sends m_0, m_1 to $\mathcal{F}_{\mathsf{OT}}$. The proof of indistinguishability between each pair of hybrids is similar to the prior proof.

The only security loss in the proof is between Hyb_0 and Hyb_1 (when we invoke the equivocality of the underlying commitment scheme). Using Theorem 5.12 where we derived $\mu(\lambda, q, n_{\mathsf{com}}) = \frac{2qn_{\mathsf{com}}^{1/2}}{2^{\lambda_{\mathsf{com}}/2}}$ and plugging $\lambda_{\mathsf{com}} = 2\lambda$, $n_{\mathsf{com}} = 2n$ (as we are committing to 2 bits at a time) where $n = 10\ 300\lambda$ (this setting of n is the same as that needed in the sender security part of the proof), we get $\frac{288q\sqrt{\lambda}}{2^\lambda}$ security against a malicious sender.

C Three round chosen input bit OT via the XOR extractor

In this section, we derive parameters required when using a seedless XOR extractor in place of a universal hash function, in Protocol 8.

Theorem C.1 (Three round chosen input bit OT.)**.** *Consider Protocol 8 and modify it to use the XOR extractor in place of the universal hash function. In addition, instantiate the protocol with any non-interactive commitment scheme that is* extractable *(Definition 5.3) and* equivocal *(Definition 5.4). Then there exist constants A, B such that Protocol 8 (modified to use XOR extractor) securely realizes (Definition 3.2) $\mathcal{F}_{\mathsf{OT}[1]}$.*

Furthermore, letting λ be the security parameter, q be an upper bound on the total number of random oracle queries made by the adversary, and using the commitment scheme from Section 5.2 with security parameter $\lambda_{\mathsf{com}} = 4\lambda$, for constants $A = 800, B = 800$, Protocol 8 (modified to use XOR extractor) securely realizes $\mathcal{F}_{\mathsf{OT}[1]}$ with μ_{R^*}-security against a malicious receiver and μ_{S^*}-security against a malicious sender, where

$$\mu_{\mathsf{R}^*} = \frac{3\sqrt{10}q^{3/2}}{2^\lambda} + \frac{148(q + 4800\lambda + 1)^3 + 1}{2^{4\lambda}} + \frac{38400q\lambda}{2^{2\lambda}}, \quad \mu_{\mathsf{S}^*} = \frac{80\sqrt{3}q\lambda}{2^{2\lambda}}.$$

This requires a total of $2(A + B)\lambda = 3200\lambda$ BB84 states.

Proof. The proof of this proceeds along the same line as that of Protocol 8. We only describe the changes here.

Sender security We define the same hybrids as used in the proof of sender security of Protocol 8, and the proof of the indistinguishability between $\mathsf{Hyb}_0, \mathsf{Hyb}_1, \mathsf{Hyb}_2, \mathsf{Hyb}_3$ proceeds along the same way. For the proof of indistinguishability between Hyb_3 and Hyb_4 as well, the proof proceeds similarly except that the proof of some subclaims change. Specifically, SubClaim 7.11 now proves that for $A = 800, B = 800, q \geq 5$, $\mathrm{Tr}\left(\Pi_{\mathsf{bad}}^{0.245}\tau\right) \leq \frac{45q^3}{2^{2\lambda}}$. In particular, in the proof of SubClaim 7.11 we get $\epsilon^{\delta}_{\mathsf{classical}} \leq \frac{7}{2^\lambda}$ assuming $\delta = 0.245, \epsilon = 0.08326, \beta = 0.123, \gamma = 0.152, k = A\lambda, n = (A + B)\lambda, A = 800, B = 800$.

As in that proof then, by gentle measurement (Lemma 3.1), the τ defined in SubClaim 7.11 is within trace distance $\frac{3\sqrt{10}q^{3/2}}{2^\lambda}$ of a state τ_{good} in the image of $\mathbb{I} - \Pi_{\mathsf{bad}}^{0.245}$. And now conditioned on τ being in the image of $\mathbb{I} - \Pi_{\mathsf{bad}}^{0.245}$, and $A = 800, B = 800$, we show that $\Pr[\mathsf{Hyb}_3 = 1] = \Pr[\mathsf{Hyb}_4 = 1]$.

To prove this, as in the proof of SubClaim 7.12, we have registers $\mathcal{S}_W$ are in a superposition of states $\left|\mathbf{r}_{\widetilde{\boldsymbol{\theta}}_{W[1]}}\right\rangle$, where $\Delta\left(\mathbf{r}, \widetilde{\mathbf{R}}_W\right) < 0.245$. Recalling that $\mathcal{S}_W = \{\mathcal{S}_{i, d_i \oplus b \oplus 1}\}_{i \in \overline{T} \setminus U}$, we have, for a

majority of $i \in \overline{T} \setminus U$, register $\mathcal{S}_{i,\widetilde{\boldsymbol{\theta}}_i \oplus 1}$ is measured in basis $\widetilde{\boldsymbol{\theta}}_i \oplus 1$. Call these set of registers that are measured in basis $\widetilde{\boldsymbol{\theta}}_i \oplus 1$ as M. We then have that registers $\mathcal{S}_M$ are in superposition of states $\left|\mathbf{r}_{\widetilde{\boldsymbol{\theta}}_M}\right\rangle$, where $\Delta\left(\mathbf{r}, \widetilde{\mathbf{R}}_M\right) \leq \frac{0.245 \cdot |\overline{T} \setminus U|}{|M|} \leq \frac{0.245 \cdot |\overline{T} \setminus U|}{|\overline{T} \setminus U|/2} = 2 \cdot 0.245 = 0.49 < \frac{1}{2}$.

Hence, using Theorem 4.1 it then follows that the measured bit is a uniformly random bit.

Receiver Security This proceeds in the same way as the proof of receiver security. The only difference is the security loss incurred during in the indistinguishability between Hyb_1 and Hyb_2. As before, $|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{2qn_{\mathsf{com}}^{1/2}}{2^{\lambda_{\mathsf{com}}/2}}$. Plugging $\lambda_{\mathsf{com}} = 4\lambda$, $n_{\mathsf{com}} = 3n$ (as we are committing to 3 bits at a time) where $n = 1600\lambda$ (this setting of n is the same as that needed in the sender security part of the proof), we get $\frac{80\sqrt{3}q\lambda}{2^{2\lambda}}$ security against a malicious sender. □

D Classical sampling strategies

We analyze some common sampling strategies to find their classical error probability, $\epsilon^{\delta}_{\mathsf{classical}}$ in this section. Before doing so, we recall Hoeffding's inequality, which we make extensive use of below.

Hoeffding's inequality Let $X_1, \ldots X_n$ be independent bounded random variables with $X_i \in [a, b]$ for all i, where $-\infty < a \leq b < \infty$. Let $X = \sum_{i \in [n]} X_i$. Then, for $\epsilon > 0$,

$$\Pr[X \geq \mathbb{E}[X] + \epsilon] \leq \exp\left(-\frac{2\epsilon^2}{n(b-a)^2}\right), \Pr[X \leq \mathbb{E}[X] - \epsilon] \leq \exp\left(-\frac{2\epsilon^2}{n(b-a)^2}\right)$$

D.1 Random subset without replacement

This corresponds to sampling $T \subseteq [n]$ of size k uniformly at random without replacement and outputting $\omega(\mathbf{q}_T)$. Then, for $0 < \delta < 1$, $\epsilon^{\delta}_{\mathsf{classical}} \leq 2\exp\left(-2\left(1 - \frac{k}{n}\right)^2 \delta^2 k\right)$ [BF10, Appendix B.1].

D.2 Random subset without replacement, using only part of the sample

This corresponds to sampling a set $T \subseteq [n]$ of size k without replacement, then sampling $S \subseteq T$ uniformly at random among all possible subsets of T and outputting $\omega(\mathbf{q}_S)$. We provide a tighter analysis of this compared to [BF10, Appendix B.4].

Lemma D.1. *For $0 < \delta, \beta < 1$ and $0 < \eta < \delta$,*

$$\epsilon^{\delta}_{\mathsf{classical}} \leq 2\exp\left(-2\left(1 - \frac{k}{n}\right)^2 \eta^2 k\right) + 2\exp\left(-(\delta - \eta)^2(1 - \beta)k\right) + \exp\left(-\frac{\beta^2 k}{2}\right).$$

Proof.

$$\epsilon^{\delta}_{\mathsf{classical}} = \max_{\mathbf{q}} \Pr_{T,S}[|\omega(\mathbf{q}_{\overline{T}}) - \omega(\mathbf{q}_S)| \geq \delta]$$

We have using the sampling strategy above, for $0 < \eta < 1$,

$$\max_{\mathbf{q}} \Pr_T[|\omega(\mathbf{q}_{\overline{T}}) - \omega(\mathbf{q}_T)| \geq \eta] \leq 2\exp\left(-2\left(1-\frac{k}{n}\right)^2 \eta^2 k\right) \tag{8}$$

In the following, given a string $\mathbf{q}$, we find a bound on $\Pr_S[|\omega(\mathbf{q}_T) - \omega(\mathbf{q}_S)| \geq \gamma]$. Relating this to the above, we will get the final bound. Conditioning on the size of S being s, the sampling of S corresponds to sampling a uniform subset of size s. We have the following subclaim:

SubClaim D.2.

$$\Pr_S\left[|\omega(\mathbf{q}_T) - \omega(\mathbf{q}_S)| \geq \gamma \,\middle|\, |S| = s\right] \leq 2\exp\left(-2\gamma^2 s\right)$$

Proof. We find a bound using Hoeffding's inequality applied to sampling S with replacement (sampling S without replacement will only be tighter). For each $i \in [s]$, let $Y_i = 1$ if the i^{th} drawn element of S is 1. Let $Y = \sum_{i\in[s]} Y_i, \overline{Y} = Y/s$. Then, using Hoeffding's inequality, since Y_i are independent bounded random variables, for $\gamma' > 0$, $\Pr[|Y - \mathbb{E}[Y]| \geq \gamma'] \leq 2\exp\left(-\frac{2\gamma'^2}{s}\right)$ or $\Pr\left[|\overline{Y} - \mathbb{E}[\overline{Y}]| \geq \gamma\right] \leq 2\exp\left(-2\gamma^2 s\right)$ for $\gamma = \gamma'/s$. Since, $\mathbb{E}[\overline{Y}] = \omega(\mathbf{q}_T)$, we have for $0 < \gamma < 1$, $\Pr\left[|\omega(\mathbf{q}_S) - \omega(\mathbf{q}_T)| \geq \gamma \,|\, |S| = s\right] \leq 2\exp\left(-2\gamma^2 s\right)$. □

Using the distribution of $|S|$, we have,

SubClaim D.3. *For* $0 < \gamma, \beta < 1$, $\Pr_S\left[|\omega(\mathbf{q}_T) - \omega(\mathbf{q}_S)| \geq \gamma\right] \leq 2\exp\left(-2\gamma^2(1-\beta)\frac{k}{2}\right) + \exp\left(-\frac{\beta^2 k}{2}\right)$.

Proof. To find the distribution of $|S|$, note that sampling S corresponds to choosing each element of T at random with probability $1/2$. For $i \in [k]$, let $X_i = 1$ if i^{th} element is chosen to be part of the set, and let $X = \sum_{i\in[k]} X_i$. Then, $\Pr[X_i = 1] = 1/2$ and each X_i is an independent bounded random variable. Using Hoeffding's inequality, for $\beta' > 0$, $\Pr[X \leq \mathbb{E}[X] - \beta'] \leq \exp\left(-\frac{2\beta'^2}{k}\right)$. Setting $\beta' = \mathbb{E}[X]\beta$, we get, $\Pr[X \leq (1-\beta)\,\mathbb{E}[X]] \leq \exp\left(-\frac{2\beta^2(\mathbb{E}[X])^2}{k}\right)$. Since $\beta' > 0$, we have $\beta > 0$. In particular, for $0 < \beta < 1$, we have, $\Pr_S[|S| \leq (1-\beta)\frac{k}{2}] \leq \exp\left(-\frac{\beta^2 k}{2}\right)$.

Therefore,

$$\begin{aligned}
\Pr\left[|\omega(\mathbf{q}_S) - \omega(\mathbf{q}_T)| \geq \gamma\right] &= \sum_{s\leq(1-\beta)k/2} \Pr\left[|\omega(\mathbf{q}_S) - \omega(\mathbf{q}_T)| \geq \gamma \,\middle|\, |S| = s\right] \Pr[|S| = s] \\
&\quad + \sum_{s>(1-\beta)k/2} \Pr\left[|\omega(\mathbf{q}_S) - \omega(\mathbf{q}_T)| \geq \gamma \,\middle|\, |S| = s\right] \Pr[|S| = s] \\
&\leq \exp\left(-\frac{\beta^2 k}{2}\right) + \sum_{s>(1-\beta)k/2} 2\exp\left(-2\gamma^2 s\right) \\
&\leq \exp\left(-\frac{\beta^2 k}{2}\right) + 2\exp\left(-2\gamma^2(1-\beta)\frac{k}{2}\right)
\end{aligned}$$

□

Combining the above with Eq. (8), we get, for any string $\mathbf{q} \in \{0,1\}^n$,

$$\Pr\left[|\omega(\mathbf{q}_{\overline{T}}) - \omega(\mathbf{q}_S)| \geq \eta + \gamma\right] \leq 2\exp\left(-2\left(1-\frac{k}{n}\right)^2 \eta^2 k\right) + 2\exp\left(-2\gamma^2(1-\beta)\frac{k}{2}\right) + \exp\left(-\frac{\beta^2 k}{2}\right).$$

For $\delta = \eta + \gamma$, we get, for $0 < \delta < 1, 0 < \eta < \delta$ and $0 < \beta < 1$,

$$\Pr\left[|\omega(\mathbf{q}_{\overline{T}}) - \omega(\mathbf{q}_S)| \geq \delta\right] \leq 2\exp\left(-2\left(1-\frac{k}{n}\right)^2 \eta^2 k\right) + 2\exp\left(-(\delta-\eta)^2(1-\beta)k\right) + \exp\left(-\frac{\beta^2 k}{2}\right).$$

□

D.3 Intersection of two uniform subsets and then using part of the sample

This corresponds to sampling two independent uniform subsets $T, U \subseteq [n]$, each of size k, setting $S = T \cap U$, and then taking a random subset of S (among all possible subsets of S). This is the strategy followed in our 3 round chosen input OT protocol (Section 7). In terms of the sampling strategy definition in Section 3.6, the above strategy can be thought of as the following sampling strategy Ψ:

- $P_{T'}$: Sample two independent and uniform subsets of $[n]$ each of size k. Let s denote their intersection size. Fix s, and discard the subsets themselves. Sample a random subset T' of $[n]$, of size $2k - s$, and output T'.
- $P_{S'}$: Given T', reverse calculate s as $2k - |T'|$. Sample a uniformly random subset S of T', of size s. Sample a uniformly random subset S' of S (among all possible subsets of S). Output S'.
- $f(T', \mathbf{q}_{T'}, S')$: Output $\omega(\mathbf{q}_{S'})$.

We prove then the following:

Lemma D.4. *For $0 < \epsilon, \beta, \delta < 1$ and $0 < \gamma < \delta$,*

$$\epsilon^{\delta}_{\mathsf{classical}}(\Psi) \leq 2\exp\left(-2\left(\frac{(n-k)^2 - 3\epsilon k^2}{(n-k)^2 + (1-2\epsilon)k^2}\right)^2 \gamma^2(1-\epsilon)\frac{k^2}{n}\right) + 2\exp\left(-(\delta-\gamma)^2(1-\beta)(1-\epsilon)\frac{k^2}{n}\right) + \exp\left(-\frac{\beta^2(1-\epsilon)k^2}{2n}\right) + 2\exp\left(-\frac{2\epsilon^2 k^3}{n^2}\right)$$

Proof.

$$\begin{aligned}\epsilon^{\delta}_{\mathsf{classical}}(\Psi) &= \max_{\mathbf{q}} \Pr_{T' \leftarrow P_{T'}, S' \leftarrow P_{S'}} \left[\mathbf{q} \notin B^{\delta}_{T',S'}\right] \\ &= \max_{\mathbf{q}} \Pr_{T' \leftarrow P_{T'}, S' \leftarrow P_{S'}} \left[|\omega(\mathbf{q}_{\overline{T'}}) - \omega(\mathbf{q}_{S'})| \geq \delta\right]\end{aligned}$$

To relate $\omega(\mathbf{q}_{\overline{T'}})$ with $\omega(\mathbf{q}_{S'})$, consider the following equivalent sampling strategy Ψ':

- Sample two independent and uniform subsets of $[n]$ each of size k. Let s denote their intersection size. Fix s, and discard the subsets themselves. Sample a random subset R of $[n]$, of size $n - 2(k - s)$.
- Sample a uniformly random subset S of R, of size s. Sample a uniformly random subset - S', of S (among all possible subsets of S). Output $\omega(\mathbf{q}_{S'})$.

In intuitive terms, compared to the original sampling strategy where $T, U \subseteq [n]$ of size k each were sampled, in sampling strategy Ψ, set T' corresponds to sampling $T \cup U$ first, and then sampling $S = T \cap U$. And in the above sampling strategy, Ψ', sampling R corresponds to sampling $\overline{T \cup U} \cup (T \cap U)$, or in terms of sampling strategy Ψ it corresponds to sampling $\overline{T'} \cup S$. Therefore, $\omega(\mathbf{q}_{\overline{T'}})$ in sampling strategy Ψ is equivalent to $\omega(\mathbf{q}_{R \setminus S})$ in Ψ'. Therefore,

$$\begin{aligned}\epsilon^{\delta}_{\mathsf{classical}}(\Psi) &= \max_{\mathbf{q}} \Pr_{T' \leftarrow P_{T'}, S' \leftarrow P_{S'}} \left[|\omega(\mathbf{q}_{\overline{T'}}) - \omega(\mathbf{q}_{S'})| \geq \delta\right] \\ &= \max_{\mathbf{q}} \Pr_{s,R,S,S'} \left[|\omega(\mathbf{q}_{R \setminus S}) - \omega(\mathbf{q}_{S'})| \geq \delta\right] \qquad (9)\end{aligned}$$

But note that given s, sampling S and S' from R corresponds exactly the sampling analyzed in Appendix D.2. Therefore, using the same result, we get, for $0 < \delta, \beta < 1$ and $0 < \gamma < \delta$,

$$\begin{aligned}\max_{\mathbf{q}} \Pr_{S,S'} \left[|\omega(\mathbf{q}_{R \setminus S}) - \omega(\mathbf{q}_{S'})| \geq \delta \,\middle|\, |S| = s\right] \leq 2 \exp\left(-2\left(1 - \frac{s}{n - 2(k-s)}\right)^2 \gamma^2 s\right) \\ + 2\exp\left(-(\delta - \gamma)^2 (1 - \beta) s\right) + \exp\left(-\frac{\beta^2 s}{2}\right).\end{aligned}$$

We now factor in the distribution of s, which we analyze using Hoeffding's inequality applied to sampling with replacement. Consider the following experiment - sample subset $T \subseteq [n]$ size k uniformly at random. Now sample k elements from $[n]$ with replacement and call that set U. Set $s = |T \cap U|$. Let for all $i \in [k]$, $X_i = 1$ iff the i^{th} drawn element for U is drawn from T. Then, $\Pr[X_i = 1] = k/n$. Let $X = \sum_{i \in [k]} X_i$ represent $s = T \cap U$. $\mathbb{E}[X] = k^2/n$. Since X_i are independently drawn binary random variables, applying Hoeffding's inequality, for $\epsilon' > 0$,

$$\begin{aligned}\Pr\left[|X - \mathbb{E}[X]| \geq \epsilon'\right] &\leq 2\exp\left(\frac{-2\epsilon'^2}{k}\right) \\ \implies \Pr\left[\left|s - \frac{k^2}{n}\right| \geq \epsilon'\right] &\leq 2\exp\left(\frac{-2\epsilon'^2}{k}\right) \\ \implies \Pr\left[\left|s - \frac{k^2}{n}\right| \geq \frac{\epsilon k^2}{n}\right] &\leq 2\exp\left(\frac{-2\epsilon^2 k^3}{n^2}\right)\end{aligned}$$

where we substituted $\epsilon' = \frac{\epsilon k^2}{n}$. Therefore, $s \in \left(\frac{(1-\epsilon)k^2}{n}, \frac{(1+\epsilon)k^2}{n}\right)$ except with probability $2\exp\left(\frac{-2\epsilon^2 k^3}{n^2}\right)$ for $0 < \epsilon < 1$. We have then for $0 < \epsilon, \beta, \delta < 1$ and $0 < \gamma < \delta$,

$$
\begin{aligned}
&\Pr_{s,R,S,S'}\left[|\omega(\mathbf{q}_{R\setminus S}) - \omega(\mathbf{q}_{S'})| \geq \delta\right] \\
&= \sum_{s_0:\,|s_0 - k^2/n| \geq \frac{\epsilon k^2}{n}} \Pr_{R,S,S'}\left[|\omega(\mathbf{q}_{R\setminus S}) - \omega(\mathbf{q}_{S'})| \geq \delta \,|\, s = s_0\right] \Pr_s\left[s = s_0\right] \\
&+ \sum_{s_0:\,|s_0 - k^2/n| < \frac{\epsilon k^2}{n}} \Pr_{R,S,S'}\left[|\omega(\mathbf{q}_{R\setminus S}) - \omega(\mathbf{q}_{S'})| \geq \delta \,|\, s = s_0\right] \Pr_s\left[s = s_0\right] \\
&\leq \sum_{s_0:\,|s_0 - k^2/n| \geq \frac{\epsilon k^2}{n}} \Pr_s\left[s = s_0\right] + \sum_{s_0:\,|s_0 - k^2/n| < \epsilon} 2\exp\left(-2\left(1 - \frac{s}{n - 2(k-s)}\right)^2 \gamma^2 s\right) \\
&\qquad\qquad + 2\exp\left(-(\delta-\gamma)^2(1-\beta)s\right) + \exp\left(-\frac{\beta^2 s}{2}\right) \\
&\leq 2\exp\left(-2\left(\frac{(n-k)^2 - 3\epsilon k^2}{(n-k)^2 + (1-2\epsilon)k^2}\right)^2 \gamma^2 (1-\epsilon)\frac{k^2}{n}\right) \\
&+ 2\exp\left(-(\delta-\gamma)^2(1-\beta)(1-\epsilon)\frac{k^2}{n}\right) + \exp\left(-\frac{\beta^2(1-\epsilon)k^2}{2n}\right) + 2\exp\left(-\frac{2\epsilon^2 k^3}{n^2}\right)
\end{aligned}
$$

where we substituted the upper bound and lower bound of s to get the last inequality. Since this is true for any string $\mathbf{q}$, it is also true for $\max_{\mathbf{q}}$ and hence using Eq. (9), we get $\epsilon^{\delta}_{\mathsf{classical}}$ is bounded by the quantity above. □