A New Framework for Quantum Oblivious Transfer

Amit Agarwal[⋆], James Bartusek[⋆⋆], Dakshita Khurana[⋆⋆⋆], and 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.

1 Introduction

Stephen Wiesner's celebrated paper [61] 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) [54, 29] – serves as the foundation for secure computation [32, 43], 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

[⋆] UIUC. Email: amita2@illinois.edu

[⋆⋆] UC Berkeley. Email: bartusek.james@gmail.com

[⋆⋆⋆] UIUC. Email: dakshita@illinois.edu

[†] UIUC.

measurements) where even discussed in the paper. Later, [20] 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?

In a setting where the sender and receiver share prior EPR pairs, we obtain a positive answer to this question (for random receiver bit). We prove (malicious, simulation-based) security of our protocol in the quantum random oracle model.

Specifically, we consider a setup where the sender and receiver each begin with halves of EPR pairs, which are maximally entangled two-qubit states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. These are the simplest type of entangled quantum states, and are likely to be a common shared setup in quantum networks (see e.g. [56] and references therein). They have also attracted much interest as a quantum analogue of the classical common reference string (CRS) model [44, 19, 49, 26]. They have already been shown to be useful for many two-party tasks such as quantum communication via teleportation [10], entanglement-assisted quantum error correction [14], and even cryptographic tasks like key distribution [27] and non-interactive zero-knowledge [19, 49].

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 receiver gets x_b for a random bit b. On the other hand, our result shows that OT can be achieved in a one-shot manner just given shared EPR pairs.

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

[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.

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 [2, 51, 53, 35, 25] 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 Bob) outputs a random pair of bits, while the other (say Alice) 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

[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 [36].

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 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 *maliciously* 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 other open problems) 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. [55, 13]). 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 [9] 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 QROM, that we make use of in our OT protocols. We provide a simple construction based on prior work [3, 63, 24].
- **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 [20] 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 the full version [1], 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) [37] 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 [31] for one-way secure computation, or [12] 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 achieving 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. [16, 41, 15] 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 [2, 51] has been shown to imply a variety of useful protocols including two-message proof systems, non-malleable commitments, and beyond [52, 5, 39, 42, 7, 40, 6].

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.

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

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 approach (following eg., [11]) 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 [61] 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 [20] 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 [47, 46] 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[4].

- **Quantum OT from bit commitment.** Although unconditionally-secure bit commitment cannot be constructed using quantum information, [20]'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 [20]'s proposal: e.g. [11, 48, 62, 21, 57, 13].
- **Quantum OT in the bounded storage model.** One can also impose physical assumptions in order to recover quantum OT with unconditional security. [22] introduced the *quantum bounded-storage model*, and [60] 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 [59, 28, 38, 30].

[4] Another line of work studies (unconditional) oblivious transfer with *imperfect* security [18, 17, 45], which we view as largely orthogonal to our work.

- **Quantum OT from "minicrypt" assumptions.** While [20]'s proposal for obtaining OT from bit commitments 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 [8, 34] showing that the existence of one-way functions suffices and [50, 4] 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. 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.

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

- **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).

Fig. 1: An (insecure) skeleton OT candidate.

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 [20] 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 [21, 13] 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] Security against (malicious) Bob is relatively straightforward in this setting, and essentially reduces to proving that Alice's input bit b remains hidden; this follows due to the hiding of the commitment.

- **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. Commit $\mathsf{com}_1, \ldots, \mathsf{com}_n$ 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 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**: $m_0 \coloneqq \mathsf{Extract}(t_0 \coloneqq \{r_{i,d_i}\}_{i\in\overline{T}}), m_1 \coloneqq \mathsf{Extract}(t_1 \coloneqq \{r_{i,d_i\oplus 1}\}_{i\in\overline{T}})$.

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

To formally prove security against malicious Alice, we build on several recently developed quantum random oracle techniques [63, 23, 24] as well as techniques for analyzing "quantum cut-and-choose" protocols [21, 13]. In particular, we require the random oracle based commitments to be *extractable*, and then take inspiration from [13] to argue that Bob's state on registers $\{\mathcal{B}_{i,0}, \mathcal{B}_{i,1}\}_{i\in\overline{T}}$

[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.

is in some sense close to a state described by the information $\{\theta_i, r_{i,0}, r_{i,1}\}_{i \in \overline{T}}$ in Alice's unopened commitments. In more detail, we define a projector Π on registers $\{\mathcal{B}_{i,0}, \mathcal{B}_{i,1}\}_{i \in \overline{T}}$ spanned by all states in the $\{\theta_i\}_{i \in \overline{T}}$ basis that are "close" in Hamming distance to the collection of bits $\{r_{i,0}, r_{i,1}\}_{i \in \overline{T}}$. Since these bits are unopened, defining this projector requires us to run the extractor of the commitment scheme to obtain $\{r_{i,0}, r_{i,1}\}_{i \in \overline{T}}$. We show that, conditioned on Bob not aborting, his left-over state on registers $\{\mathcal{B}_{i,0}, \mathcal{B}_{i,1}\}_{i \in \overline{T}}$ must be negligibly close to the image of Π.

To do so, at a high level, we apply the measure-and-reprogram technique from [23, 24], which roughly shows that in this setting, it suffices to consider an *interactive* version of the protocol, where all the commitments are output by Alice *before* T is chosen uniformly at random. At this point, it becomes possible to argue by standard Hoeffding inequalities that Bob's registers must be close to the image of Π (conditioned on Bob not aborting).

Finally, recall that Bob is measuring each $\mathcal{B}_{i,0}$ in the standard basis and each $\mathcal{B}_{i,1}$ in the Hadamard basis (whereas before measurement, as we just determined, most pairs $\mathcal{B}_{i,0}, \mathcal{B}_{i,1}$ were in the image of Π, i.e., "close" to basis states in the same basis). Thus, intuitively, honest Bob's measurements must produce at least some entropy (from Alice's perspective) when performed on any state in Π. Converting this entropy into uniform randomness, as is required by the definition of OT security, turns out to be non-trivial even given prior work on randomness extraction. In the next section, we discuss hurdles and new methods for *extracting uniform randomness* from this entropy.

New Techniques for Randomness Extraction. Note that the arguments above have not yet established a fully secure OT correlation. In particular, Alice may 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 [55] 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 for Alice to obtain her output $m_b = \mathsf{Extract}(s, t_b)$, making the protocol no longer non-interactive.[6] Instead, we develop techniques for *seedless* extraction that work in our setting, allowing us to make the full description of the hash function used to derive the final 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

[6] One idea would be to sample the seed s as part of the output of the random oracle. However, this does not ensure that s is uniformly random. For example Alice could bias certain bits of s by choosing her commitments in a certain way.

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 $\mathsf{Extract}$ 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 *bit* OT, 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 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. [58, 33]), 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 $\mathcal{A}$.[7] 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 [63] and builds on proof techniques in [33]. 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 [20] 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, parties measure their set of qubits[8] 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,

[7] 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.

[8] Technically, one party prepares and the other measures BB84 states.

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*.

Non-interactive OT reversal. So far, our techniques have shown that, given shared EPR pairs, Alice can send a single message to Bob that results in the following correlations: Alice outputs a bit b and string m_b, while Bob outputs m_0, m_1, thus implementing the $\mathcal{F}_{\mathsf{S-ROT}}$ functionality with 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 [36]. 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 the full version [1], 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 (m_0, m_1) s.t. $m_b = m$.

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 [36] 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.

Fig. 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 $(\mathcal{A}_{i,0}, \mathcal{A}_{i,1})$ 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.

2.4 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.

The need for these two additional properties is not new to our work. Indeed, [21] showed that bit commitment schemes satisfying extraction and equivocation suffice to instantiate the original [20, 11] QOT template. [21] called their

- **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 $x_0 = m_0 \oplus \mathsf{Extract}(t_0 := \{r_{i,d_i}\}_{i \in [n] \setminus T \setminus U})$ and $x_1 = m_1 \oplus \mathsf{Extract}(t_1 := \{r_{i,d_i \oplus 1}\}_{i \in [n] \setminus T \setminus U})$.
  4. Send (x_0, x_1, U) to Alice.
- **Alice's output**: $m_b := x_b \oplus \mathsf{Extract}(t_b := \{r'_{i,\theta_i}\}_{i \in \overline{T}})$.

Fig. 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.

commitments dual-mode commitments, and provided a construction based on the quantum hardness of the learning with errors (QLWE) assumption. In two recent works [8, 34], constructions of such commitment schemes were achieved by relying on just post-quantum one-way functions (and 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 [63, 24] for on-the-fly simulation with extraction, and our proof of equivocality relies on a one-way-to-hiding lemma from [3].

3 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. [55, 21, 13]).

3.1 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 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

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

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

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

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 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 $x : p(x) = 1$. □

This completes the proof of the theorem. □

3.2 The Random Oracle 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 3. *Let $H : \{0,1\}^n \rightarrow \{0,1\}^m$ 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,*[9] *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*:*
  - 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,

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

The proof of this theorem appears in the full version [1].

4 The fixed basis framework: OT from entanglement

We define (non-interactive) commitments in the quantum random oracle model, and use them to build protocols for OT from shared EPR pairs.

[9] 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.

Commitments in the Random Oracle Model. 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 $\{m_i\}_{i\in T}$ or $\perp$.

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

In the full version [1], we define correctness, hiding, extractability and equivocality for these commitments. We prove that a natural construction which essentially commits to a bit b as $H(b||r)$ for $r \leftarrow \{0,1\}^{\lambda_{\mathsf{com}}}$, satisfies extractability and equivocality in the QROM. The extractability definition guarantees the existence of a simulator $\mathsf{SimExt} = (\mathsf{SimExt.RO}, \mathsf{SimExt.Ext})$ where $\mathsf{SimExt.RO}$ responds to the adversary's random oracle queries and $\mathsf{SimExt.Sim}$ extracts from the commitment strings output by the adversary.

Theorem 4. *Instantiate Protocol 5 with the* correct, hiding, *and* extractable *non-interactive commitment scheme above. Then the following hold.*

- *When instantiated with the XOR extractor, there exist constants A, B such that Protocol 5 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$.*
- *When instantiated with the ROM extractor, there exist constants A, B such that Protocol 5 securely realizes $\mathcal{F}_{\mathsf{S-ROT}[\lambda]}$.*

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 above with security parameter $\lambda_{\mathsf{com}} = 4\lambda$, the following hold.

- *When instantiatied with the XOR extractor and constants $A = 50$, $B = 100$, Protocol 5 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 5 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.

Protocol 5

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 $H_{FS} : \{0,1\}^{n\ell} \rightarrow \{0,1\}^{\lceil \log \binom{n}{k} \rceil}$.
- 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 $H_{Ext} : \{0,1\}^{n-k} \rightarrow \{0,1\}^{\lambda}$.

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 $\mathsf{Rec}(\{c_i\}_{i \in T}, \{(r_{i,0}, r_{i,1}, \theta_i), u_i\}_{i \in T}) \neq \bot$.
        - $*$ 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

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

Fig. 5: Non-interactive random-sender-input OT in the shared EPR pair model.

Then, applying non-interactive bit OT reversal [36] to the protocol that realizes $\mathcal{F}_{\mathsf{S-ROT}[1]}$ immediately gives the following corollary.

Corollary 1. *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 (of Theorem 4) 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 random oracle randomness extractor) as separate oracles that the honest parties and adversaries query, which is without loss of generality. We prove security below.

Sender security. First, we show security against a malicious receiver R^*. We will use *on-the-fly* simulation, introduced in [63] as a method of guaranteeing *efficient* simulation of the oracle independent of the number of queries. We will also use the extractor $\mathsf{SimExt} = (\mathsf{SimExt.RO}, \mathsf{SimExt.Sim})$ guaranteed by the commitment scheme. We describe the 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 any H_{FS} (and H_{Ext}) queries using an efficient on-the-fly random oracle simulator. 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" bullet 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 oracle 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 at most q queries combined to H_{FS} and H_C (and H_{Ext}), we consider the following hybrids. The distributions $\Pi[\mathsf{R}^*, \mathsf{D}, \top]$ and $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}}}[\mathsf{Sim}[\mathsf{R}^*], \mathsf{D}, \top]$ are formally defined in the full version [1] to be the real and simulated executions of the protocol, respectively.

- Hyb_0: The result of the real interaction between R^* and S. 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 $\mathsf{SimExt.RO}$ 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 $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}$). 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 5 and Claim 6.

Claim 5.

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

Proof. This follows by a direct reduction to extractability of the commitment scheme, since the only difference is whether or not we simulate the adversary's access to H_C and use the extracted values $\{r^*_{i,0}, r^*_{i,1}\}_{i\in T}$ in place of the opened values $\{r_{i,0}, r_{i,1}\}_{i\in T}$. □

Claim 6. *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 $\mathbf{c} := (c_1, \ldots, c_n)$ be the classical commitments.
- Write the classical extracted values $\{(r^*_{i,0}, r^*_{i,1}, \theta^*_i)\}_{i\in[n]}$ as matrices

$$\mathbf{R}^* := \begin{bmatrix} r^*_{1,0} & \cdots & r^*_{n,0} \\ r^*_{1,1} & \cdots & r^*_{n,1} \end{bmatrix}, \boldsymbol{\theta}^* := \begin{bmatrix} \theta^*_1 & \cdots & \theta^*_n \end{bmatrix}.$$

- 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 $\overline{T} := [n] \setminus T$.
- Given $\mathbf{R}^*, \boldsymbol{\theta}^* \in \{0,1\}^{2\times n}$, $T \subseteq [n]$, and $\delta \in (0,1)$, define

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

  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 $\overline{T}$.

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

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

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. Intuitively, this is a projection onto "bad" states defined by the values $\mathbf{R}^*, \boldsymbol{\theta}^*$, and where the check set T is computed by $H_{FS}(\mathbf{c})$.

We will now prove the following sub-claim, which essentially states that the global state of the system after the malicious receiver outputs their message only has negligible overlap with the "bad" subspace defined above.

SubClaim 7. *Let* $\tau := \sum_{H,\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*} p^{(H,\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)}\ \tau^{(H,\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)}$*, where*

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

be 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 right after* R^* *outputs its message and* $\mathsf{SimExt.Ext}$ *is run. Here, each* $p^{(H,\mathbf{c},\mathbf{R}^*,\boldsymbol{\theta}^*)}$ *is the probability that the random oracle* H_{FS} *is initialized to the function* H *and the registers* $\mathcal{C}, \mathcal{Z}$ *hold the classical strings* $\mathbf{c}, \mathbf{R}^*, \boldsymbol{\theta}^*$*. We also define* $\mathcal{S}$ *to be the register holding the sender's halves of EPR pairs, and* $\mathcal{X}$ *to be the 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* $\mathrm{Tr}\big(\mathit{\Pi}_{\mathsf{bad}}^{0.25}\tau\big) \leq \frac{64q^3}{2^{2\lambda}}$.
- *If* $A = 1050, B = 2160$*, then* $\mathrm{Tr}\big(\mathit{\Pi}_{\mathsf{bad}}^{0.054}\tau\big) \leq \frac{64q^3}{2^{2\lambda}}$.

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 $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ [23, 24] (described formally in the full version [1]) 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

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

for $T \subset [n]$, the measure-and-reprogram theorem [23, 24] (also full version [1]) gives

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

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. Crucially, because $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ is defined to just run $\mathsf{Adv}_{\mathsf{R}^*}$ and answer their oracle queries to H_{FS}, it does not touch the sender's registers $\mathcal{S}$ after initializing them with halves of EPR pairs.

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 $\mathbf{c}$. In the full version [1], we show that com has a $\frac{8}{2^{\lambda_{\mathsf{com}}/2}}$-commuting simulator, which means that each time we commute the $\mathsf{SimExt.Ext}$ query past a $\mathsf{SimExt.RO}$ query, the overall state of the system changes by at most $\frac{8}{2^{\lambda_{\mathsf{com}}/2}}$ in trace distance. Thus, plugging in $\lambda_{\mathsf{com}} = 4\lambda$,

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

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.

Now, since the $\mathcal{S}$ register is not touched by $\mathsf{Sim}[\mathsf{Adv}_{\mathsf{R}^*}]$ at any point after $(\mathbf{R}^*, \boldsymbol{\theta}^*)$ are output, we can imagine measuring the $\mathcal{S}$ registers in the $\boldsymbol{\theta}^*$-basis even before T is sampled. Thus, ϵ is at most the probabilty that the following procedure outputs 1, where $\mathbf{R}^*$ represents the matrix output by SimExt, and $\mathbf{R}$ represents the matrix obtained by measuring register $\mathcal{S}$ in the $\boldsymbol{\theta}^*$-basis.

- Let $\mathbf{R}, \mathbf{R}^* \in \{0,1\}^{2\times n}$ be two matrices.
- Sample a uniformly random subset $T \subset [n]$ of size k.
- Output 1 if and only if $(\mathbf{R}_{i,0}, \mathbf{R}_{i,1}) = (\mathbf{R}^*_{i,0}, \mathbf{R}^*_{i,1})$ for all $i \in T$, and $(\mathbf{R}_{i,0}, \mathbf{R}_{i,1}) \neq (\mathbf{R}^*_{i,0}, \mathbf{R}^*_{i,1})$ for at least δ fraction of $i \in \overline{T}$.

In the full version [1], we bound this probability by $2\exp\left(-2(1-k/n)^2\delta^2 k\right)$, using standard Hoeffding inequalities.

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

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

  for $A = 50, B = 100$.
- For $\delta = 0.054$, this probability is bounded by

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

  for $A = 1050, B = 2160$.

Summarizing, we have that in either case,

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

for $q \geq 4$.

□

By the calculations above, and by Gentle Measurement (full version [1]), the τ defined in SubClaim 7 is within $\frac{8q^{3/2}}{2^{\lambda}}$ trace distance of a state τ_{good} in the image of $\mathbb{I} - \mathit{\Pi}_{\mathsf{bad}}^{0.25}$ if $A = 50, B = 100$ and in the image of $\mathbb{I} - \mathit{\Pi}_{\mathsf{bad}}^{0.054}$ if $A = 1050, B = 2160$.

For readability, we note that

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

where for any T,

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

Finally, we show the following two sub-claims to complete the proof of Claim 6.

SubClaim 8. *If E is the XOR extractor, then conditioned on τ being in the image of $\mathbb{I} - \mathit{\Pi}_{\mathsf{bad}}^{0.25}$, it holds that*

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

Proof. It suffices to analyze the state τ conditioned on the register that contains T being equal to $H_{FS}(\mathbf{c})$ (otherwise the honest sender/simulator will abort).

If τ is in $\mathbb{I} - \mathit{\Pi}_{\mathsf{bad}}^{0.25}$, it must be the case that the register $\mathcal{S}$ is in the image of $\mathbb{I} - \mathit{\Pi}^{\mathbf{R}^*, \boldsymbol{\theta}^*, T, 0.25}$, 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 $\mathbf{R}^*_T$. Thus, we can condition on the sender not aborting, which, by the definition of $\mathbb{I} - \mathit{\Pi}^{\mathbf{R}^*, \boldsymbol{\theta}^*, T, 0.25}$ implies that register $\mathcal{S}_{\overline{T}}$ is supported on vectors $\left|(\mathbf{R}_{\overline{T}})_{\boldsymbol{\theta}^*}\right\rangle$ such that $\mathit{\Delta}(\mathbf{R}_{\overline{T}}, \mathbf{R}^*_{\overline{T}}) < 0.25$.

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 $\mathit{\Delta}(\mathbf{r}_M, \mathbf{r}^*_M) < 0.5$. Thus, recalling that each of these states is measured in the basis $1 \oplus \boldsymbol{\theta}^*_i$, we can appeal to Theorem 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 9. *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 3 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 $\frac{4q2^{h_b(0.108)(n-k)/2}}{2^{(n-k)/4}} = \frac{4q}{2^{(n-k)(\frac{1}{4}-\frac{1}{2}h_b(0.108))}} = \frac{4q}{2^{B\lambda(\frac{1}{4}-\frac{1}{2}h_b(0.108))}} \leq \frac{4q}{2^{\lambda}}$ for $B \geq 326$. □

This completes the proof of Claim 6. □

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, 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 $|x,y\rangle \rightarrow |x, y \oplus z\rangle$, 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 $e_i \coloneqq (r_{i,0}, r_{i,1}, \theta_i)$ and for each $i \in \overline{T}$, let $e_i \coloneqq (0,0,0)$. 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 $x_0 \coloneqq E(\{r_{i,d_i}\}_{i\in\overline{T}}) \oplus m_0$ and $x_1 \coloneqq E(\{r_{i,d_i\oplus 1}\}_{i\in\overline{T}}) \oplus m_1$ (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^*. 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 $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}$). 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 $\widetilde{\Pi}_{\mathcal{F}_{\mathsf{S-ROT}[\lambda]}}[\mathsf{Sim}[\mathsf{S}^*], \mathsf{D}, b]$).

Security against a malicious S^* follows by observing that Hyb_0 and Hyb_1 are identically distributed, since H_{FS} is a random oracle and T is uniformly random in Hyb_1, and the following claims.

Claim 10. $|\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| \leq \frac{4q\sqrt{3(A+B)\lambda}}{2^{2\lambda}}$.

This follows from hiding of the commitments (appropriately parameterized).

Claim 11. $\Pr[\mathsf{Hyb}_2 = 1] = \Pr[\mathsf{Hyb}_3 = 1]$.

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. In the full version [1], we also analyze a two-round variant without setup where the receiver sets up entanglement. In addition, we formally describe our 3 round chosen-input OT without entanglement or setup, as well as optimizations of the CK template to minimize round complexity.

Acknowledgments

A. Agarwal, D. Khurana and N. Kumar were supported in part by by NSF CNS-2238718, DARPA SIEVE and a gift from Visa Research. This material is based upon work supported by the Defense Advanced Research Projects Agency through Award HR00112020024.

References

1. Agarwal, A., Bartusek, J., Khurana, D., Kumar, N.: A new framework for quantum oblivious transfer. Cryptology ePrint Archive, Paper 2022/1191 (2022), https://eprint.iacr.org/2022/1191
2. Aiello, W., Ishai, Y., Reingold, O.: Priced oblivious transfer: How to sell digital goods. In: Pfitzmann, B. (ed.) Advances in Cryptology – EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045, pp. 119–135. Springer, Heidelberg, Germany, Innsbruck, Austria (May 6–10, 2001). https://doi.org/10.1007/3-540-44987-6_8
3. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 269–295. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019). https://doi.org/10.1007/978-3-030-26951-7_10
4. Ananth, P., Qian, L., Yuen, H.: Cryptography from pseudorandom quantum states. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13507, pp. 208–236. Springer (2022). https://doi.org/10.1007/978-3-031-15802-5_8
5. Badrinarayanan, S., Garg, S., Ishai, Y., Sahai, A., Wadia, A.: Two-message witness indistinguishability and secure computation in the plain model from new assumptions. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017, Part III. Lecture Notes in Computer Science, vol. 10626, pp. 275–303. Springer, Heidelberg, Germany, Hong Kong, China (Dec 3–7, 2017). https://doi.org/10.1007/978-3-319-70700-6_10
6. Badrinarayanan, S., Goyal, V., Jain, A., Kalai, Y.T., Khurana, D., Sahai, A.: Promise zero knowledge and its applications to round optimal MPC. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018, Part II. Lecture Notes in Computer Science, vol. 10992, pp. 459–487. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2018). https://doi.org/10.1007/978-3-319-96881-0_16
7. Badrinarayanan, S., Goyal, V., Jain, A., Khurana, D., Sahai, A.: Round optimal concurrent MPC via strong simulation. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017: 15th Theory of Cryptography Conference, Part I. Lecture Notes in Computer Science, vol. 10677, pp. 743–775. Springer, Heidelberg, Germany, Baltimore, MD, USA (Nov 12–15, 2017). https://doi.org/10.1007/978-3-319-70500-2_25
8. Bartusek, J., Coladangelo, A., Khurana, D., Ma, F.: One-way functions imply secure computation in a quantum world. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture

Notes in Computer Science, vol. 12825, pp. 467–496. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_17

9. Bartusek, J., Khurana, D.: Cryptography with certified deletion. Cryptology ePrint Archive, Paper 2022/1178 (2022), https://eprint.iacr.org/2022/1178
10. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (Mar 1993). https://doi.org/10.1103/PhysRevLett.70.1895
11. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) Advances in Cryptology – CRYPTO'91. Lecture Notes in Computer Science, vol. 576, pp. 351–366. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 11–15, 1992). https://doi.org/10.1007/3-540-46766-1_29
12. Bitansky, N., Vaikuntanathan, V.: A note on perfect correctness by derandomization. In: Coron, J.S., Nielsen, J.B. (eds.) Advances in Cryptology – EUROCRYPT 2017, Part II. Lecture Notes in Computer Science, vol. 10211, pp. 592–606. Springer, Heidelberg, Germany, Paris, France (Apr 30 – May 4, 2017). https://doi.org/10.1007/978-3-319-56614-6_20
13. Bouman, N.J., Fehr, S.: Sampling in a quantum population, and applications. In: Rabin, T. (ed.) Advances in Cryptology – CRYPTO 2010. Lecture Notes in Computer Science, vol. 6223, pp. 724–741. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 15–19, 2010). https://doi.org/10.1007/978-3-642-14623-7_39
14. Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science (New York, N.Y.) **314**, 436–9 (11 2006). https://doi.org/10.1126/science.1131563
15. Canetti, R., Chen, Y., Holmgren, J., Lombardi, A., Rothblum, G.N., Rothblum, R.D., Wichs, D.: Fiat-Shamir: from practice to theory. In: Charikar, M., Cohen, E. (eds.) 51st Annual ACM Symposium on Theory of Computing. pp. 1082–1090. ACM Press, Phoenix, AZ, USA (Jun 23–26, 2019). https://doi.org/10.1145/3313276.3316380
16. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM **51**(4), 557–594 (jul 2004). https://doi.org/10.1145/1008731.1008734
17. Chailloux, A., Gutoski, G., Sikora, J.: Optimal bounds for semi-honest quantum oblivious transfer. Chic. J. Theor. Comput. Sci. **2016** (2016). https://doi.org/https://doi.org/10.48550/arXiv.1310.3262
18. Chailloux, A., Kerenidis, I., Sikora, J.: Lower bounds for quantum oblivious transfer. Quantum Info. Comput. **13**(1–2), 158–177 (jan 2013). https://doi.org/https://doi.org/10.48550/arXiv.1007.1875
19. Coladangelo, A., Vidick, T., Zhang, T.: Non-interactive zero-knowledge arguments for qma, with preprocessing. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 799–828. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-56877-1_28
20. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions (extended abstract). In: 29th Annual Symposium on Foundations of Computer Science. pp. 42–52. IEEE Computer Society Press, White Plains, NY, USA (Oct 24–26, 1988). https://doi.org/10.1109/SFCS.1988.21920
21. Damgård, I., Fehr, S., Lunemann, C., Salvail, L., Schaffner, C.: Improving the security of quantum protocols via commit-and-open. In: Halevi, S. (ed.) Advances in Cryptology – CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677,

pp. 408–427. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 16–20, 2009). https://doi.org/10.1007/978-3-642-03356-8_24

22. Damgård, I., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded quantum-storage model. SIAM J. Comput. **37**, 1865–1890 (01 2008). https://doi.org/10.1137/060651343
23. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the Fiat-Shamir transformation in the quantum random-oracle model. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 356–383. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019). https://doi.org/10.1007/978-3-030-26951-7_13
24. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Online-extractability in the quantum random-oracle model. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13277, pp. 677–706. Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_24
25. Döttling, N., Garg, S., Hajiabadi, M., Masny, D., Wichs, D.: Two-round oblivious transfer from CDH or LPN. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 768–797. Springer, Heidelberg, Germany, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45724-2_26
26. Dupuis, F., Lamontagne, P., Salvail, L.: Fiat-shamir for proofs lacks a proof even in the presence of shared entanglement (2022). https://doi.org/10.48550/ARXIV.2204.02265
27. Ekert: Quantum cryptography based on bell's theorem. Physical review letters **67 6**, 661–663 (1991). https://doi.org/https://doi.org/10.1103/PhysRevLett.67.661
28. Erven, C., Ng, N., Gigov, N., Laflamme, R., Wehner, S., Weihs, G.: An experimental implementation of oblivious transfer in the noisy storage model. Nature Communications **5** (2014). https://doi.org/10.1038/ncomms4418
29. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Commun. ACM **28**(6), 637–647 (jun 1985). https://doi.org/10.1145/3812.3818
30. Furrer, F., Gehring, T., Schaffner, C., Pacher, C., Schnabel, R., Wehner, S.: Continuous-variable protocol for oblivious transfer in the noisy-storage model. Nature Communications **9**(1) (2018). https://doi.org/10.1038/s41467-018-03729-4
31. Garg, S., Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Cryptography with one-way communication. In: Gennaro, R., Robshaw, M.J.B. (eds.) Advances in Cryptology – CRYPTO 2015, Part II. Lecture Notes in Computer Science, vol. 9216, pp. 191–208. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 16–20, 2015). https://doi.org/10.1007/978-3-662-48000-7_10
32. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or A completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th Annual ACM Symposium on Theory of Computing. pp. 218–229. ACM Press, New York City, NY, USA (May 25–27, 1987). https://doi.org/10.1145/28395.28420
33. Grilo, A.B., Hövelmanns, K., Hülsing, A., Majenz, C.: Tight adaptive reprogramming in the qrom. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2021. pp. 637–667. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-92062-3_22

34. Grilo, A.B., Lin, H., Song, F., Vaikuntanathan, V.: Oblivious transfer is in miniqcrypt. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12697, pp. 531–561. Springer (2021). https://doi.org/10.1007/978-3-030-77886-6_18
35. Halevi, S., Kalai, Y.: Smooth projective hashing and two-message oblivious transfer. Journal of Cryptology **25**, 158–193 (01 2012). https://doi.org/10.1007/s00145-010-9092-8
36. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) Advances in Cryptology – CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729, pp. 145–161. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2003). https://doi.org/10.1007/978-3-540-45146-4_9
37. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Prabhakaran, M., Sahai, A., Wullschleger, J.: Constant-rate oblivious transfer from noisy channels. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011. Lecture Notes in Computer Science, vol. 6841, pp. 667–684. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 14–18, 2011). https://doi.org/10.1007/978-3-642-22792-9_38
38. Ito, T., Koizumi, H., Suzuki, N., Kakesu, I., Iwakawa, K., Uchida, A., Koshiba, T., Muramatsu, J., Yoshimura, K., Inubushi, M., Davis, P.: Physical implementation of oblivious transfer using optical correlated randomness. Scientific Reports **7**(1) (2017). https://doi.org/10.1038/s41598-017-08229-x
39. Jain, A., Kalai, Y.T., Khurana, D., Rothblum, R.: Distinguisher-dependent simulation in two rounds and its applications. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017, Part II. Lecture Notes in Computer Science, vol. 10402, pp. 158–189. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2017). https://doi.org/10.1007/978-3-319-63715-0_6
40. Kalai, Y.T., Khurana, D., Sahai, A.: Statistical witness indistinguishability (and more) in two messages. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018, Part III. Lecture Notes in Computer Science, vol. 10822, pp. 34–65. Springer, Heidelberg, Germany, Tel Aviv, Israel (Apr 29 – May 3, 2018). https://doi.org/10.1007/978-3-319-78372-7_2
41. Kalai, Y.T., Rothblum, G.N., Rothblum, R.D.: From obfuscation to the security of Fiat-Shamir for proofs. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017, Part II. Lecture Notes in Computer Science, vol. 10402, pp. 224–251. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2017). https://doi.org/10.1007/978-3-319-63715-0_8
42. Khurana, D., Sahai, A.: How to achieve non-malleability in one or two rounds. In: Umans, C. (ed.) 58th Annual Symposium on Foundations of Computer Science. pp. 564–575. IEEE Computer Society Press, Berkeley, CA, USA (Oct 15–17, 2017). https://doi.org/10.1109/FOCS.2017.58
43. Kilian, J.: Founding cryptography on oblivious transfer. In: 20th Annual ACM Symposium on Theory of Computing. pp. 20–31. ACM Press, Chicago, IL, USA (May 2–4, 1988). https://doi.org/10.1145/62212.62215
44. Kobayashi, H.: Non-interactive quantum perfect and statistical zero-knowledge. In: Ibaraki, T., Katoh, N., Ono, H. (eds.) Algorithms and Computation. pp. 178–188. Springer Berlin Heidelberg, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-24587-2_20

45. Kundu, S., Sikora, J., Tan, E.Y.Z.: A device-independent protocol for xor oblivious transfer. arXiv: Quantum Physics (2020). https://doi.org/10.22331/q-2022-05-30-725
46. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Physical Review Letters **78**(17), 3410 (1997). https://doi.org/https://doi.org/10.1103/PhysRevLett.78.3410
47. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Physical review letters **78**(17), 3414 (1997). https://doi.org/10.1103/PhysRevLett.78.3414
48. Mayers, D., Salvail, L.: Quantum oblivious transfer is secure against all individual measurements. In: Proceedings Workshop on Physics and Computation. PhysComp'94. pp. 69–77. IEEE (1994). https://doi.org/10.1109/PHYCMP.1994.363696
49. Morimae, T., Yamakawa, T.: Classically verifiable NIZK for QMA with preprocessing. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 13794, pp. 599–627. Springer (2022). https://doi.org/10.1007/978-3-031-22972-5_21
50. Morimae, T., Yamakawa, T.: Quantum commitments and signatures without one-way functions. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13507, pp. 269–295. Springer (2022). https://doi.org/10.1007/978-3-031-15802-5_10
51. Naor, M., Pinkas, B.: Efficient oblivious transfer protocols. In: Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms. p. 448–457. SODA '01, Society for Industrial and Applied Mathematics, USA (2001). https://doi.org/https://dl.acm.org/doi/10.5555/365411.365502
52. Ostrovsky, R., Paskin-Cherniavsky, A., Paskin-Cherniavsky, B.: Maliciously circuit-private FHE. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014, Part I. Lecture Notes in Computer Science, vol. 8616, pp. 536–553. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2014). https://doi.org/10.1007/978-3-662-44371-2_30
53. Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) Advances in Cryptology – CRYPTO 2008. Lecture Notes in Computer Science, vol. 5157, pp. 554–571. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2008). https://doi.org/10.1007/978-3-540-85174-5_31
54. Rabin, M.O.: How to exchange secrets with oblivious transfer. IACR Cryptol. ePrint Arch. **2005**, 187 (2005), https://eprint.iacr.org/2005/187
55. Renner, R., König, R.: Universally composable privacy amplification against quantum adversaries. In: Kilian, J. (ed.) TCC 2005: 2nd Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 3378, pp. 407–425. Springer, Heidelberg, Germany, Cambridge, MA, USA (Feb 10–12, 2005). https://doi.org/10.1007/978-3-540-30576-7_22
56. Shi, S., Qian, C.: 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. p. 62–75. SIGCOMM '20, Association

for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3387514.3405853

57. Unruh, D.: Universally composable quantum multi-party computation. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 486–505. Springer, Heidelberg, Germany, French Riviera (May 30 – Jun 3, 2010). https://doi.org/10.1007/978-3-642-13190-5_25
58. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015, Part II. Lecture Notes in Computer Science, vol. 9057, pp. 755–784. Springer, Heidelberg, Germany, Sofia, Bulgaria (Apr 26–30, 2015). https://doi.org/10.1007/978-3-662-46803-6_25
59. Wehner, S., Curty, M., Schaffner, C., Lo, H.K.: Implementation of two-party protocols in the noisy-storage model. Physical Review A - Atomic, Molecular, and Optical Physics **81**(5) (2010). https://doi.org/10.1103/PhysRevA.81.052336
60. Wehner, S., Schaffner, C., Terhal, B.: Cryptography from noisy storage. Physical review letters **100**, 220502 (06 2008). https://doi.org/10.1103/PhysRevLett.100.220502
61. Wiesner, S.: Conjugate coding. SIGACT News **15**, 78–88 (1983). https://doi.org/https://doi.org/10.1145/1008908.1008920
62. Yao, A.C.C.: Security of quantum protocols against coherent measurements. In: 27th Annual ACM Symposium on Theory of Computing. pp. 67–75. ACM Press, Las Vegas, NV, USA (May 29 – Jun 1, 1995). https://doi.org/10.1145/225058.225085
63. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 239–268. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019). https://doi.org/10.1007/978-3-030-26951-7_9