Secure Computation with Shared EPR Pairs (Or: How to Teleport in Zero-Knowledge)

James Bartusek* , Dakshita Khurana**, and Akshayaram Srinivasan***

Abstract. Can a sender non-interactively transmit one of two strings to a receiver without knowing which string was received? Does there exist minimally-interactive secure multiparty computation that only makes (black-box) use of symmetric-key primitives? We provide affirmative answers to these questions in a model where parties have access to shared EPR pairs, thus demonstrating the cryptographic power of this resource.

- First, we construct a one-shot (i.e., single message) string oblivious transfer (OT) protocol with random receiver bit in the shared EPR pairs model, assuming the (sub-exponential) hardness of LWE.

  Building on this, we show that *secure teleportation through quantum channels* is possible. Specifically, given the description of any quantum operation Q, a sender with (quantum) input ρ can send a single classical message that securely transmits $Q(\rho)$ to a receiver. That is, we realize an ideal quantum channel that takes input ρ from the sender and provably delivers $Q(\rho)$ to the receiver without revealing any other information.

  This immediately gives a number of applications in the shared EPR pairs model: (1) non-interactive secure computation of unidirectional *classical* randomized functionalities, (2) NIZK for QMA from standard (sub-exponential) hardness assumptions, and (3) a non-interactive *zero-knowledge* state synthesis protocol.
- Next, we construct a two-round (round-optimal) secure multiparty computation protocol for classical functionalities in the shared EPR pairs model that is *unconditionally-secure* in the (quantum-accessible) random oracle model.

Classically, both of these results cannot be obtained without some form of correlated randomness shared between the parties, and the only known approach is to have a trusted dealer set up random (string) OT correlations. In the quantum world, we show that shared EPR pairs (which are simple and can be deterministically generated) are sufficient. At the heart of our work are novel techniques for making use of entangling operations to generate string OT correlations, and for instantiating the Fiat-Shamir transform using correlation-intractability in the quantum setting.

* UC Berkeley. Email: bartusek.james@gmail.com
** UIUC. Email: dakshita@illinois.edu
*** Tata Institute of Fundamental Research. Email: akshayaram.srinivasan@tifr.res.in

1 Introduction

Understanding the nature of shared entanglement is one of the most prominent goals of quantum information science, and its study has repeatedly unearthed surprisingly strong properties. A remarkable example of this is the quantum teleportation protocol of [15], which demonstrated that shared EPR pairs [32], the most basic entangled resource, are "complete" for quantum communication using classical channels. That is, if Alice and Bob share EPR pairs a priori, then Alice can communicate an arbitrary state ρ to Bob by sending just a single classical message. In particular, this result positions shared EPR pairs at the center of proposals for building a quantum internet.

1.1 Our contributions

In this work, we investigate the *cryptographic* power of shared EPR pairs.

Secure Teleportation through a Quantum Channel. First, we revisit the setting of quantum teleportation, which shows that shared EPR pairs and one-way classical communication give rise to a quantum channel implementing the identity map $\rho \to \rho$. We ask: what if Alice would instead like to send her state ρ to Bob through some arbitrary quantum map $\rho \to Q(\rho)$?[1]

Note that this is trivial given quantum teleportation if we allow either Alice or Bob to compute the map $\rho \to Q(\rho)$ for themselves. However, we are interested in guaranteeing that the effect of the protocol would be (computationally) "no different" than the effect of Alice inputting ρ to an "ideal" channel Q, and Bob receiving $Q(\rho)$ on the other side, *even if* Alice or Bob attempt to save extra information from or deviate from the protocol. In particular, we require each of the following three properties to hold against arbitrarily malicious adversaries: (1) Alice would not learn any side information created during the computation of $Q(\rho)$, (2) Bob would learn nothing about ρ beyond $Q(\rho)$, and (3) Bob would be convinced that the state he received was actually computed as the output of the map Q (on some input ρ). We show that this is possible under the sub-exponential hardness of learning with errors (LWE), a standard post-quantum security assumption.

Informal Theorem 1. *For any efficient quantum map Q, there exists a protocol for "secure teleportation through Q" in the shared EPR pairs model assuming the sub-exponential hardness of LWE. That is, there exists a one-shot[2] protocol in the shared EPR pairs model that computes the ideal functionality $\rho \to Q(\rho)$.*

[1] We will also allow for preserving entanglement that ρ may have with its environment, so technically we consider Q to map a state on Alice's input register $\mathcal{A}$ to a state on Bob's output register $\mathcal{B}$.

[2] We use one-shot, one-message, and non-interactive interchangeably to refer to a protocol that consists of a single message from a sender to a receiver.

Building Block: One-shot String OT. The main building block for this protocol, and the key technical contribution of this paper, is a one-shot protocol for (random receiver bit) *string oblivious transfer* (OT) in the shared EPR pairs model, which realizes an ideal funtionality that takes two strings m_0, m_1 from a sender Alice, and delivers (b, m_b) to Bob for a uniformly random bit b.[3]

Informal Theorem 2. *Assuming the sub-exponential hardness of LWE, there exists a simulation-secure one-shot protocol for (random receiver bit) string OT in the shared EPR pairs model.*

Given such an OT protocol, we rely on two key previous results to obtain our final implication to secure teleportation through quantum channels: (1) [34] showed how to construct a one-message protocol for secure computation of any unidirectional *classical* randomized functionality f that maps $x \to f(x; r)$ given a one-message protocol for string OT, and (2) [8] (building on the work of [19]) showed (implicitly) how to construct a one-message protocol for secure computation of any unidirectional *quantum* functionality given a one-message protocol for unidirectional classical functionalities.

Correlation Interactability. There have been many recent works that show how to instantiate random oracles with a concrete hash function family and base the security of (classical) primitives such as NIZKs and SNARGs on standard cryptographic assumptions [21, 54, 18, 45, 46, 40, 25, 49, 24, 41, 48, 23]. These works proceed by constructing a special hash function family that satisfies the cryptographic notion of *correlation-intractability* [22]. Ours is the first to apply correlation-intractability to a setting that involves *quantum communication*, addressing technical barriers along the way. In fact, we obtain our one-message string OT protocol (refer to Informal Theorem 2) by utilizing correletion-intractability, which we discuss further in Section 2.

The Multiparty Setting. Next, we consider the *multiparty* setting, where all pairs of parties have access to shared EPR pairs. If each party has their own private input x_i, and their goal is to compute $C(x_1, \ldots, x_n)$ for some (classical) circuit C, they will have to use at least two rounds of interaction as single round protocols are susceptible to resetting attacks [39].

Classically, two rounds are known to suffice for secure multiparty computation, under the (minimal) assumption that two-round (chosen-input) oblivious transfer [36, 13] protocols exist.[4] In the classical setting, OT is a "public-key-style" primitive that provably cannot be built from "minicrypt-style" primitives, including hash functions modeled as a random oracle [42]. On the other hand, a line of work beginning with [28] and culminating with [9, 38] established that

[3] Note that it is impossible to obtain a one-shot protocol for fixed receiver bit OT, since Bob does not send any message.

[4] In chosen-input OT, the receiver specifies their input bit b, and they receive the message m_b. We contrast this with the notion of OT discussed above, where the receiver's bit b is chosen uniformly at random.

with quantum communication, it is possible to obtain oblivious transfer, and thus multiparty computation, from one-way functions or potentially even weaker assumptions [47, 7, 53]. However, these protocols require many rounds, and the possibility of achieving *round-optimal* (two-round) secure computation without public-key primitives was left open.

In this work, we show that round-optimal secure computation that makes black-box use of symmetric-key primitives (specifically, a random oracle) can be obtained in the shared EPR pairs model.

Informal Theorem 3. *There exists a two-round secure multiparty computation protocol in the shared EPR pairs model with either of the following properties.*

- *Unconditional security in the quantum-accesible random oracle model (QROM).*
- *Computational security assuming (the black-box use of) non-interactive extractable commitments and hash functions that are correlation-intractable for efficient functions.*

Discussion: Towards Weaker Correlated Randomness. In the classical world, it can be shown that without any form of correlated randomness shared between the parties, it is impossible to obtain either one-shot OT or two-round MPC (even with public-key primitives). Furthermore, we show in the full version [11] that one-shot (random receiver bit) string OT is impossible in the classical common reference string model, even when parties can compute and communicate quantumly. On the other hand, we remark that both our results can be obtained (even in the classical world) with an "OT correlations" setup, which assumes that a trusted dealer has sampled random strings x_0, x_1 and bit b and delivered x_0, x_1 to the sender and b, x_b to the receiver. For the case of string OT, this consequence is immediate and for the case of two-round MPC, this result follows from the work of Garg et al. [35].

Our results state that in the quantum world, shared EPR pairs are sufficient to obtain (i) one-shot (random receiver bit) string OT and (ii) two-round MPC from symmetric-key primitives. As noted in [2], shared EPR pairs are a fundamentally different resource than OT correlations. Indeed, OT correlations are *specific* to OT, while, as indicated above, shared EPR pairs are 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 fully deterministic quantum process.[5] Our work can thus be viewed as a step towards realizing secure computation protocols using weaker

[5] 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 pair setup, by monogamy of entanglement. We also remark that obtaining OT correlations from *any* deterministically generated shared quantum state is non-trivial. In particular, if the parties shared a (deterministically generated) superposition over classical OT correlations, the receiver could simply decide not to measure the register holding their choice bit, and obtain a superposition over the sender's strings, which violates the security of OT.

forms of correlated randomness. Finally, we remark that, unlike the case of one-shot OT, it may be possible to achieve two-round MPC from symmetric-key primitives in the classical common reference string model (i.e., without shared EPR pairs), and we leave this as an intriguing open question for future study.

1.2 Applications

We now discuss several applications of our one-shot string OT construction and secure teleportation through quantum channel protocol.

Non-Interactive Computation of Unidirectional Functionalities. The study of non-interactive protocols for unidirectional classical functionalities was initiated by [34]. Such functionalities are defined by a classical circuit f, take an input x from the sender, (potentially) sample some random coins r, and deliver $f(x;r)$ to the receiver. They showed the possibility (or impossibility) of achieving them in a model where the sender and the receiver have access to an *one-way communication channel*. In particular, they showed that ideal string OT channel suffices to build non-interactive secure computation of unidirectional classical functionalities. On the other hand, the work of Agrawal et al. [4] showed that bit OT channels provably do *not* suffice for non-interactive secure computation.[6]

Using our one-shot string OT construction, we can instantiate the results of Garg et al. [34] and obtain non-interactive secure computation of unidirectional functionalities in the shared EPR pairs model, assuming sub-exponential LWE.

The works of [34, 5] also discuss several applications of non-interactive secure computation of unidirectional classical functionalities, and we mention one intriguing application here. The modern internet relies on a public-key infrastructure, where certificate authorities validate public keys by signing them under their own signing key.[7] A single message protocol for unidirectional classical functionalities would enable key authorities to *non-interactively* generate and send freshly sampled and signed public key secret key pairs to clients, *without* learning the client's secret key. Moreover, the client would not learn the secret signing key of the authority who sent their fresh pair. Thus, we show that there is a truly non-interactive solution to this widespread key certification functionality in a world where nodes are connected by shared EPR pairs.[8]

NIZKs for QMA. Our secure telportation through quantum channels immediately gives a non-interactive zero-knowlede (NIZK) for QMA in the shared EPR pairs model, by letting the channel Q compute a QMA verification circuit and

[6] A followup work of [5] showed that, assuming *ideal obfuscation*, there exists a protocol over a bit OT channel with $1/\mathrm{poly}(\lambda)$ security.

[7] Note that despite the existence of quantum key distribution [14], public-key infrastructure would still likely be required for the quantum internet, since QKD requires authenticated classical channels.

[8] We do stress that our model assumes the EPR pairs are generated honestly, for example by an honest network administrator. Otherwise, such secure one-message protocols would be impossible to achieve.

output the resulting bit to the receiver. The only previous NIZK for QMA in the shared EPR pairs model is due to [52], who argued security in the quantum random oracle model.[9] Thus, we obtain the first such protocol from a standard (sub-exponential) hardness assumption.

Non-Interactive Zero-Knowledge State Synthesis. Many recent works consider the problem of quantum *state synthesis* [1, 55, 43], which studies the efficiency of preparing a complex quantum state with the help of an oracle or untrusted powerful prover. That is, given the implicit description of a quantum circuit Q, can a verifier prepare $|\psi\rangle = Q|0^n\rangle$ with the help of a prover, and be convinced that they end up with the correct state?

In fact, [55] asked whether there is any meaningful notion of *zero-knowledge* state synthesis. In this work, we propose one way to define zero-knowledge state synthesis. Roughly, we consider any *family* of circuits $\{Q_w\}_w$ parameterized by a potentially secret witness w, and require that a prover help the verifier prepare $|\psi_w\rangle = Q_w|0^n\rangle$ without leaking the witness w. We formalize our definition in the full version [11] and show that our secure teleportation protocol immediately gives a *one-message* solution to this task in the shared EPR pairs model. We stress that there may be other meaningful ways to define zero-knowledge state synthesis, and we leave a more thorough exploration of definitions and applications of zero-knowledge state synthesis to future work.

Non-Interactive Quantum Cryptography. Finally, we observe that the full power of non-interactive secure computation of unidirectional quantum functionalities gives rise to quantum analogues of the classical applications mentioned above. For example, a certificate authority could non-interactively prepare and send signed key pairs for encryption schemes with *uncloneable* or *revocable* decryption keys [37, 26, 3, 10, 6], where decryption keys are quantum states that can either provably not be distributed or verifiably be destroyed. The novel guarantee is that even the certificiate authority itself will not learn the (description of) the decrpytion key.[10] As another example, a bank could non-interactively distribute signed *quantum money* states (technically, the serial number would be signed), without ever learning the classical description of the state. In particular, while valid money states could be provably generated and distributed non-interactively, no one (not even the bank) would ever learn a classical description that would enable cloning.

1.3 Related Works

This work continues a long line of research that studies the power of shared entanglement as a resource. We show that shared EPR pairs, which already

[9] We also remark that [12] achieve NIZK for QMA in the (incomparable) common reference string model, but they argue security using classical oracles, or alternatively assuming indistinguishability obfuscation and the non-black-box use of a hash function modeled as a random oracle.

[10] In this setting, *publicly-verifiable* revocation [10] seems crucial to ensure that no one need know the classical description of the secret key.

have a long history of study in communication [16, 15], cryptography [33, 51, 31, 2], and error-correction [20], can be leveraged to obtain perhaps surprisingly powerful secure computation tasks.

We also compare our results with the prior work of [2], which also studies oblivious transfer in the shared EPR pairs model. They achieve a one-message protocol for *bit* OT, where the sender's inputs are one bit each, and explicitly leave open the problem of building *string* OT, which we address in this work. We note that bit OT is not known to be complete for one-message secure computation [34, 4]. Moreover, security of the protocols in [2] are all argued in the quantum random oracle model, while we argue security *without* random oracles, and based on concrete properies of hash functions instead.

Concurrent Work. Finally, we mention a concurrent and independent work [27] that was posted recently to the arXiv. Their results and techniques are orthogonal to ours: in particular, they obtain two-message OT in the CRS model assuming NIZK (and an assumption on hash functions), whereas we obtain one-message OT from sub-exponential LWE, as well as unconditional two-round MPC in the QROM, both in the shared EPR pairs model. We do not believe that (a simple modification of) either work's results or techniques immediately subsumes or improves results in the other. We also remark that both our work and [27] leave open the intriguing question of obtaining minimally-interactive (two-round) MPC in the CRS model without the use of public-key primitives.

Acknowledgments

D. Khurana was supported in part by NSF CAREER CNS-2238718 and NSF CNS-2247727, DARPA SIEVE. This material is based upon work supported by the Defense Advanced Research Projects Agency through Award HR00112020024. A. Srinivasan is supported in part by a SERB startup grant and Google India Research Award.

2 Technical Overview

2.1 One-shot string OT

In this subsection, we focus on our key technical contribution, which is a construction of one-shot string OT in the shared EPR pairs model. Throughout this section, we define *one-shot string OT* as a one-message protocol that takes two strings m_0, m_1 from the sender, and delivers m_b to the receiver for a random bit $b \leftarrow \{0,1\}$. For more discussion on our applications, we refer the reader to the full version [11].

A string OT skeleton. As mentioned earlier, [2] constructed a one-shot *bit* OT protocol in the shared EPR pairs model (where the sender's inputs are one bit each). However, their techniques don't appear to extend easily to the setting of

one-shot *string* OT, for arbitrary length strings. In fact, [34, 4] showed that in the non-interactive setting, it is impossible to obtain string OT from bit OT. We additionally observe that prior quantum OT templates [28, 2] only obtain "bitwise" correlations by sending unentangled BB84 states or by immediately measuring each EPR pair independently.

To get around this barrier, our idea is to directly obtain string correlations from shared entanglement. This can be done by first *entangling* the separate EPR pairs in a special way before performing measurements.

Setup: An EPR pair on registers $(\mathcal{S}^{\mathsf{ctl}}, \mathcal{R}^{\mathsf{ctl}})$ and λ EPR pairs on registers $(\mathcal{S}^{\mathsf{msg}}, \mathcal{R}^{\mathsf{msg}})$.

Sender's message:

- Sample $x \leftarrow \{0,1\}^\lambda$ and for each $i \in [\lambda]$ such that $x_i = 1$, apply a CNOT gate from $\mathcal{S}^{\mathsf{ctl}}$ to $\mathcal{S}^{\mathsf{msg}}_i$.
- Measure $\mathcal{S}^{\mathsf{msg}}$ in the standard basis to obtain $v \in \{0,1\}^\lambda$, and measure $\mathcal{S}^{\mathsf{ctl}}$ in the Hadamard basis to delete the control bit.
- Given input (m_0, m_1), send $\widetilde{m}_0 = m_0 \oplus v, \widetilde{m}_1 = m_1 \oplus v \oplus x$.

Receiver's computation:

- Measure $\mathcal{R}^{\mathsf{ctl}}, \mathcal{R}^{\mathsf{msg}}$ in the standard basis to obtain b, v', and output $(b, m_b = \widetilde{m}_b \oplus v')$.

Fig. 1. An (insecure) skeleton for one-shot string OT

Our approach is illustrated in Fig. 1. Note that after the sender applies the random CNOT gates and measures $\mathcal{S}^{\mathsf{msg}}$ to obtain v, the remaining state of the system is

$$\frac{1}{\sqrt{2}} |0\rangle_{\mathcal{S}^{\mathsf{ctl}}} |0\rangle_{\mathcal{R}^{\mathsf{ctl}}} |v\rangle_{\mathcal{R}^{\mathsf{msg}}} + \frac{1}{\sqrt{2}} |1\rangle_{\mathcal{S}^{\mathsf{ctl}}} |1\rangle_{\mathcal{R}^{\mathsf{ctl}}} |v \oplus x\rangle_{\mathcal{R}^{\mathsf{msg}}} .$$

Thus, tracing out $\mathcal{S}^{\mathsf{ctl}}$, we see that the receiver has a uniform mixture over $|0, v\rangle$ and $|1, v \oplus x\rangle$, where $v, v \oplus x$ are uniformly random strings from their perspective, exactly as desired. Unfortunately, since the sender's control register is entangled with the receiver's, the sender could know exactly which bit b the receiver obtains by measuring $\mathcal{S}^{\mathsf{ctl}}$ in the standard basis. Thus, we instead ask that the sender "delete" their control bit by measuring it in the *Hadamard* basis. Of course, a malicious (or even specious) sender may not follow these instructions, rendering this protocol insecure. However, this protocol serves as the foundation for our eventual secure realization of one-shot string OT.

Measurement check. Next, we add a mechansim for "forcing" the sender to delete their control bit. We build on the commitment-based cut-and-choose approach [28, 17, 2] as follows. Suppose the sender really did behave honestly, and measured $\mathcal{S}^{\mathsf{ctl}}$ in the Hadamard basis to obtain a bit h. Then, the state on the receiver's side will be

$$|\psi_{v,x,h}\rangle := \frac{1}{\sqrt{2}}\left(|0, v\rangle + (-1)^h |1, v \oplus x\rangle\right).$$

So if the receiver was given (v, x, h), they could measure $(\mathcal{R}^{\mathsf{ctl}}, \mathcal{R}^{\mathsf{msg}})$ in the

$$\{|\psi_{v,x,h}\rangle\langle\psi_{v,x,h}|, \mathbb{I} - |\psi_{v,x,h}\rangle\langle\psi_{v,x,h}|\}$$

basis and accept if the first outcome is observed. Of course, sending (v, x, h) to the receiver would render the protocol insecure because the receiver could now obtain both v and $v \oplus x$. Instead, we apply a variant of the Fiat-Shamir-based non-interactive measurement check subprotocol of [2], using a non-interactive commitment scheme Com and a hash function H:

- Repeat the skeleton protocol ℓ times in parallel, and have the sender commit to all descriptions $\mathsf{cm}_1 = \mathsf{Com}(v_1, x_1, h_1), \ldots, \mathsf{cm}_\ell = \mathsf{Com}(v_\ell, x_\ell, h_\ell)$.
- Hash $T = H(\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell)$ to obtain a subset $T \subset [\ell]$ of commitments.
- The sender sends $(\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell)$ along with openings to $\{\mathsf{cm}_i\}_{i \in T}$.
- For each $i \in T$, the receiver measures registers $\mathcal{R}_i^{\mathsf{ctl}}, \mathcal{R}_i^{\mathsf{msg}}$ in basis

  $$\{|\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|, \mathbb{I} - |\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|\}$$

  and aborts if any of these measurements reject. Otherwise, the parties continue the protocol using indices $i \in \overline{T}$.

Now, assuming H behaves as a random oracle, we should be able to claim that conditioned on the receiver not aborting, their states on registers $\{\mathcal{R}_i^{\mathsf{ctl}}, \mathcal{R}_i^{\mathsf{msg}}\}_{i \in \overline{T}}$ should be "close" to the honest states $\{|\psi_{v_i,x_i,h_i}\rangle\}_{i \in \overline{T}}$. We can make this precise by arguing that after an appropriate change of basis, the states $\{\mathcal{R}_i^{\mathsf{ctl}}\}_{i \in \overline{T}}$ are in a superposition of Hadamard basis states that are close in Hamming distance to the honest state $H^{\otimes|\overline{T}|}|h_{\overline{T}}\rangle$, where $h_{\overline{T}}$ are the bits $\{h_i\}_{i \in \overline{T}}$. If this is the case, then by the "XOR extractor" lemma of [2], measuring these bits in the standard basis and XORing the results together would produce a bit b that is truly uniformly random and independent of the sender's view. Thus, we should be able to extract a perfectly random receiver's bit by *combining* correlations obtained from multiple instances $i \in \overline{T}$ of the skeleton protocol.

Defining two sender strings. Unfortunately, if we XOR together the correlations from all $i \in \overline{T}$, it is no longer clear how to define the two sender strings. Indeed, the receiver will obtain one out of two of each pair $\{(v_i, v_i \oplus x_i)\}_{i \in \overline{T}}$, which means one out of $2^{|T|}$ possible sets of strings! However, note that if the sender had used the same offset x for each repetition, then if the receiver XORs together one out of two of each $\{(v_i, v_i \oplus x)\}_{i \in \overline{T}}$, they obtain either $\bigoplus_{i \in \overline{T}} v_i$ or $x \oplus \bigoplus_{i \in \overline{T}} v_i$

depending on the parity of their choice bits. Of course, since we are opening the commitments on indices $i \in T$, the receiver would learn x, rendering this approach insecure.

Our solution is to make use of this "common offset" approach in a less direct manner. In addition to the ℓ repetitions of the skeleton protocol described above, the sender will sample an independent collection of strings $t_1, \ldots, t_\ell, \Delta$ and include commitments

$$\widehat{\mathsf{cm}}_{1,0} = \mathsf{Com}(t_1), \widehat{\mathsf{cm}}_{1,1} = \mathsf{Com}(t_1 \oplus \Delta), \ldots, \widehat{\mathsf{cm}}_{\ell,0} = \mathsf{Com}(t_\ell), \widehat{\mathsf{cm}}_{\ell,1} = \mathsf{Com}(t_\ell \oplus \Delta)$$

in their message. Then, the sender will use the random strings $(v_1, v_1 \oplus x_1), \ldots, (v_\ell, v_\ell \oplus x_\ell)$ to mask the *openings* for the commitments $(\widehat{\mathsf{cm}}_{1,0}, \widehat{\mathsf{cm}}_{1,1}), \ldots, (\widehat{\mathsf{cm}}_{\ell,0}, \widehat{\mathsf{cm}}_{\ell,1})$. The effect of this is that the receiver will be able to open one out of two of each pair of commitments $\{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}\}_{i \in \overline{T}}$, obtaining either $\bigoplus_{i \in \overline{T}} t_i$ or $\Delta \oplus \bigoplus_{i \in \overline{T}} t_i$.

Finally, to maintain security, we require that the sender computes a non-interactive zero-knowledge (NIZK) argument that they sampled $\{\widehat{\mathsf{cm}}_{i,b}\}_{i \in [\ell], b \in \{0,1\}}$ as commitments to pairs of strings that all share the same offset Δ.

Using correlation-intractability. This nearly completes the description of our protocol. Turning to the security proof, our goal is to reduce to a standard cryptographic assumption. Fortunately, the flavors of commitments and zero-knowledge we require are known from LWE. However, we also need some security from the Fiat-Shamir hash function H. In [2] this hash was modeled as a random oracle, and it was left open whether one could obtain security in the plain model.

Classically, a recent exciting line of work has shown how to securely instantiate the Fiat-Shamir transform from standard cryptographic assumptions in many settings [21, 54, 18, 45, 46, 40, 25, 49, 24, 41, 48, 23]. These works rely on the notion of *correlation-intractability* (CI), which is a property of the hash function H requiring that for some relation R over inputs and outputs, the adversary can't find any input x such that $(x, H(x)) \in R$. In particular, it is known how to obtain CI for efficiently computable *functions* from LWE [21, 54]. Moreover, [40] showed to extend this result to CI for efficiently verifiable product relations R, where the range of H is the t-wise cartesian product of a set Y, and each input x is associated with sets $S_{x,1}, \ldots, S_{x,t} \subset Y$ such that $(x, (y_1, \ldots, y_t)) \in R$ iff each $y_i \in S_{x,i}$. The property of efficient verifiability states that there is an efficient (classical) algorithm that, given (x, i, y_i), determines whether $y_i \in S_{x,i}$.

Recall that in our protocol, we apply H to a set of ℓ commitments in order to obtain the description of a subset $T \subset [\ell]$ of commitments to open. Intuitively, we want it to be difficult for the sender to find a set of commitments $(\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell)$ to strings $(v_1, x_1, h_1), \ldots, (v_\ell, x_\ell, h_\ell)$ such that $T = H(\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell)$ is a "bad" set, meaning that the receiver's registers $\{(\mathcal{R}_i^{\mathsf{ctl}}, \mathcal{R}_i^{\mathsf{msg}})\}_{i \in T}$ are "close" to the states $\{|\psi_{v_i, x_i, h_i}\rangle\}_{i \in T}$ (so the receiver won't abort) but the registers $\{(\mathcal{R}_i^{\mathsf{ctl}}, \mathcal{R}_i^{\mathsf{msg}})\}_{i \in \overline{T}}$ are "far" from the states $\{|\psi_{v_i, x_i, h_i}\rangle\}_{i \in \overline{T}}$. Thus, given an input $(\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell)$, it appears that determining whether or not a potential output T is "bad" requires (at least) applying some *quantum measurement* to the receiver's registers. Unfortunately, all prior work has used CI in a purely classical setting, and extending

the notion of efficiently verifiable relation to handle *quantum* verification algorithms appears to be beyond the reach of current techniques (though this may be an interesting direction for future research).

Instead, we take a different approach. Suppose that the sender's choices of $x_1, \ldots, x_\ell$ were fixed before the protocol begins. Then, we could pre-measure the receiver's registers even before initializing the malicious sender to obtain $(v_1, h_1), \ldots, (v_\ell, h_\ell)$. That is, we could first apply CNOTs from $\mathcal{R}_i^{\mathsf{ctl}}$ to each of the qubits in $\mathcal{R}_i^{\mathsf{msg}}$ controlled on x_i, and then measure $\mathcal{R}_i^{\mathsf{ctl}}$ in the Hadamard basis to obtain h_i and measure $\mathcal{R}_i^{\mathsf{msg}}$ in the standard basis to obtain v_i. Then given just this classical data, we can distinguish between honest commitments cm_i to (v_i, x_i, h_i) and dishonest commitments cm_i to some other string (as long as the commitment is efficiently extractable). If we split ℓ into t disjoint groups and parse T as t different subsets of $[\ell/t]$, then we can formulate a classically efficiently verifiable product relation R where $((\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell), T) \in R$ iff all $\{\mathsf{cm}_i\}_{i \in T}$ are honest and "many" $\{\mathsf{cm}_i\}_{i \in \overline{T}}$ are dishonest.

Now, while we cannot guarantee that a malicious sender will sample any fixed $(x_1, \ldots, x_\ell)$, we can *guess* beforehand which $x_1, \ldots, x_\ell$ they will use, and simply give up on reducing to CI if the guess is wrong. Using complexity leveraging (and setting the security parameter of the CI hash function large enough), we can hope that this is enough to still break *sub-exponentially-secure* CI. It turns out that this strategy can only be made to work if our guessing loss depends only on the security parameter λ, and *not* on the number of repetitions ℓ (which must depend on the level of security required from the CI hash). Thus, we make one final tweak to the protocol. The sender will be required to sample $x_1, \ldots, x_\ell$ as the output of a pseudorandom generator with seed s of length $\{0,1\}^\lambda$, and prove using the NIZK that they have done so honestly. Then, in the reduction to CI, it suffices to guess a λ-bit string s rather than a $\lambda\ell$-bit string $(x_1, \ldots, x_\ell)$. This allows us to eventually reduce security to the sub-exponential hardness of LWE.

Unconditional Protocols in the QROM. We remark that it appears plausible to obtain more efficient and unconditionally secure variants of our non-interactive protocols in the (quantum) random oracle model. In particular, following [2], we expect that the measure-and-reprogram technique [30] in the quantum random oracle model can be used in place of correlation intractability, which would remove the need for sampling $x_1, \ldots, x_\ell$ as the output of a PRG, and remove complexity leveraging in the approach outlined above. It also may be possible to rely on *black-box* commit-and-prove sigma protocols (e.g., variants of the protocol in [50]) to prove that commitments to pairs of strings share a common offset, thereby making our protocol black-box and unconditionally secure in the QROM. We leave a formalization and detailed analysis of this approach, and more generally an exploration of one-message protocols in the QROM, to future work.

2.2 Two-round MPC

In this section, we give a brief overview of our approach to building two-round MPC in the shared EPR model, which is presented in the full version [11]. Our starting point is a three-round chosen-input string OT protocol from [2], which can be viewed as a two-round protocol in the shared EPR model. In order to use this protocol to build two-round MPC, we take the following steps.

1. Show that the protocol is "black-box friendly". That is, we split the protocol into an *input-independent* phase that uses both quantum measurements and cryptographic operations, and an *input-dependent* phase that is fully classical and information-theoretic.
2. Appeal to existing compilers (e.g. [29, 44]) to obtain a "black-box friendly" MPC protocol in the shared EPR pair model. Again, we have (1) an input-independent phase at the beginning where every party performs a measurement on their halves of EPR pairs, broadcasts a message, and performs some crytographic checks, and (2) an input-dependent multi-round phase that is entirely classical and information-theoretic.
3. Use the [36] round-compressing compiler and two-round OT in the shared EPR pair model to compress this black-box-friendly protocol into a two-round MPC in the shared EPR pair model. Crucially, the compiler only has to operate on the second (multi-round input-dependent) phase, and thus we obtain a final protocol that makes black-box use of cryptography.

We stress that to make the above compiler work, we need to start with an OT protocol in which all *cryptographic operations* and *quantum computations* are performed *indepedently* of the parties' inputs and *before* the second message. That is, it does not follow from any two-round quantum OT protocol.

If we start with the protocol from [2] that was proven secure in the quantum random oracle model, then we obtain a final MPC protocol in the quantum random oracle model. In addition, we prove that a slight variant of the [2] protocol is secure *without* random oracles, assuming non-interactive extractable commitments and correlation-intractability for efficient functions. Interestingly, while we use a similar approach as described above, we do not have to resort to sub-exponential assumptions here. Roughly, this is because the [2] protocol is built from "bitwise" rather than "stringwise" correlations, and it suffices for the reduction to correctly guess a random subset of the adversary's bitwise measurements.

3 Preliminaries

Let λ denote the security parameter. We write $\mathsf{negl}(\cdot)$ to denote any *negligible* function, which is a function f such that for every constant $c \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that for all $n > N$, $f(n) < n^{-c}$. We write $\mathsf{non\text{-}negl}(\cdot)$ to denote any function f that is not negligible. That is, there exists a constant c such that for infinitely many n, $f(n) \geq n^{-c}$.

3.1 Quantum information

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

A *quantum operation* (also referred to as quantum map or quantum channel) Q is a completely-positive trace-preserving (CPTP) map from a register $\mathcal{X}$ to a register $\mathcal{Y}$, which in general may have different dimensions. That is, on input a density matrix $\rho^{\mathcal{X}}$, the operation Q produces $\tau^{\mathcal{Y}} \leftarrow Q(\rho^{\mathcal{X}})$ a mixed state on register $\mathcal{Y}$. We will sometimes write a quantum operation Q applied to a state on register $\mathcal{X}$ and resulting in a state on register $\mathcal{Y}$ as $\mathcal{Y} \leftarrow Q(\mathcal{X})$. Note that we have left the actual mixed states on these registers implicit in this notation, and just work with the names of the registers themselves.

A *unitary* $U : \mathcal{X} \to \mathcal{X}$ is a special case of a quantum operation that satisfies $U^\dagger U = UU^\dagger = \mathbb{I}^{\mathcal{X}}$, where $\mathbb{I}^{\mathcal{X}}$ is the identity matrix on register $\mathcal{X}$. A *projector* Π is a Hermitian operator such that $\Pi^2 = \Pi$, and a *projective measurement* is a collection of projectors $\{\Pi_i\}_i$ such that $\sum_i \Pi_i = \mathbb{I}$.

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

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

The trace distance between two states ρ and τ is an upper bound on the probability that any (unbounded) algorithm can distinguish ρ and τ. When clear from context, we will write $\mathsf{TD}(\mathcal{X}, \mathcal{Y})$ to refer to the trace distance between a state on register $\mathcal{X}$ and a state on register $\mathcal{Y}$.

Lemma 1 (Gentle measurement [56]). *Let $\rho^{\mathcal{X}}$ be a quantum state and let $(\Pi, \mathbb{I} - \Pi)$ be a projective measurement on $\mathcal{X}$ such that $\mathrm{Tr}(\Pi\rho) \geq 1 - \delta$. Let*

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

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

A non-uniform quantum polynomial-time (QPT) machine $\{\mathsf{Adv}_\lambda, |\psi\rangle_\lambda\}_{\lambda \in \mathbb{N}}$ is a family of polynomial-size quantum machines Adv_λ, where each is initialized with a polynomial-size advice state $|\psi_\lambda\rangle$. Each Adv_λ is in general described by a CPTP map. Similar to above, when we write $\mathcal{Y} \leftarrow \mathsf{Adv}(\mathcal{X})$, we mean that the machine Adv takes as input a state on register $\mathcal{X}$ and produces as output a state on register $\mathcal{Y}$, and we leave the actual descripions of these states implicit. Finally, a quantum *interactive* machine is simply a sequence of quantum operations, with designated input, output, and work registers.

Finally we will often use $\approx_c$ as a shorthard to denote *computational* indistinguishability between two families of distributions (over quantum states), and $\approx_s$ as a shorthard to denote *statistical* indistinguishability (or negligible closeness in trace distance) between two families of distributions.

3.2 Correlation intractability

Definition 1 (Correlation intractable hash function). *Let $\{\mathcal{X}_\lambda, \mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ be families of finite sets. An efficiently computable keyed hash function family $\{H_\lambda : \{0,1\}^{k(\lambda)} \times \mathcal{X}_\lambda \to \mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ with keys of length $k(\lambda)$ is* $\epsilon(\lambda)$-correlation intractable *for a relation ensemble $\{R_\lambda \subseteq \mathcal{X}_\lambda \times \mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ if for any QPT adversary $\{\mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$,*

$$\Pr\left[(x, H_\lambda(\mathsf{hk}, x)) \in R_\lambda : \begin{array}{c}\mathsf{hk} \leftarrow \{0,1\}^{k(\lambda)} \\ x \leftarrow \mathsf{Adv}_\lambda(\mathsf{hk})\end{array}\right] \leq \epsilon(\lambda).$$

We say that $\{H_\lambda\}_{\lambda\in\mathbb{N}}$ is sub-exponentially *correlation intractable for $\{R_\lambda\}_{\lambda\in\mathbb{N}}$ if it is $2^{-\lambda^\delta}$-correlation intractable for some constant $\delta > 0$.*

Definition 2 (Sparse, efficiently verifiable, approximate product relations [40]). *A relation $R \subseteq \mathcal{X} \times \mathcal{Y}^t$ is an efficiently verifiable α-approximate product relation with sparsity ρ if the following hold.*

- ***Approximate product.*** *For every x, the set $R_x \coloneqq \{y : (x, y) \in R\}$ consists of $y = (y_1, \ldots, y_t) \in \mathcal{Y}^t$ such that*

$$|\{i \in [t] : y_i \in S_i\}| \geq \alpha t$$

  for some sets $S_{1,x}, \ldots, S_{t,x} \subseteq \mathcal{Y}$ that may depend on x.
- ***Efficiently verifiable.*** *There is a polynomial-size circuit C such that for every x, the sets $S_{1,x}, \ldots, S_{t,x}$ are such that for any $i, y_i \in S_{i,x}$ if and only if $C(x, y_i, i) = 1$.*
- ***Sparse.*** *For every x, the sets $S_{1,x}, \ldots, S_{t,x}$ are such that for all i, $|S_{i,x}| \leq \rho|\mathcal{Y}|$.*

Imported Theorem 4 ([40])**.** *Assuming the existence of an efficiently computable keyed hash function family that is $\epsilon(\lambda)$-correlation intractable for any efficient function, there exists an efficiently computable keyed hash function family $\{H_\lambda : \{0,1\}^{k(\lambda)} \times \mathcal{X}_\lambda \to \mathcal{Y}_\lambda^{t(\lambda)}\}_{\lambda\in\mathbb{N}}$ that is $\epsilon(\lambda)$-correlation intractable for any efficiently verifiable α-approximate product relation ensemble $\{R_\lambda \subseteq \mathcal{X}_\lambda \times \mathcal{Y}_\lambda^{t(\lambda)}\}_{\lambda\in\mathbb{N}}$ with sparsity ρ, as long as $\rho < \alpha$ and $t(\lambda) \geq \lambda/(\alpha - \rho)^3$.*

Imported Theorem 5 ([21, 54])**.** *Assuming the $\epsilon(\lambda)$-hardness of LWE, there exists an efficiently computable keyed hash function family that is $\epsilon(\lambda)$-correlation intractable for any efficient function.*

Definition 3 (Programmability). *A hash function family* $\{H_\lambda : \{0,1\}^{k(\lambda)} \times \mathcal{X}_\lambda \to \mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ *is* programmable *if for any* $\lambda, x \in \mathcal{X}_\lambda$, *and* $y \in \mathcal{Y}_\lambda$,

$$\Pr_{\mathsf{hk}\leftarrow\{0,1\}^{k(\lambda)}}[H_\lambda(\mathsf{hk}, x) = y] = \frac{1}{2^{m(\lambda)}},$$

and there exists a PPT sampling algorithm $\mathsf{Samp}(1^\lambda, x, y)$ *that samples from the conditional distribution*

$$\mathsf{hk} : H_\lambda(\mathsf{hk}, x) = y.$$

Remark 1. [21] show a simple transformation that generically adds the above notion of programmability to natural correlation intractable hash functions.

In the full version [11], we present additional preliminaries covering commitments, zero-knowledge, and quantum leftover hashing.

3.3 Secure computation

An ideal functionality $\mathcal{F}$ is an interactive (classical or quantum) machine specifying some distributed computation. In this work, we will specifically focus on *two-party* functionalities between party A and party B. In some cases, party B will have a random input, or no input. The ideal functionalities we will consider in this work are specified in Fig. 2.

Security with abort. In what follows, we will by default consider the notion of security with abort, where the ideal functionality $\mathcal{F}$ is always modified to (1) know the identity of the corrupt party (if one exists) and (2) be slightly reactive: after the parties have provided input, the functionality computes outputs and sends output to the corrupt party only (if it expects output). Then the functionality awaits either a "deliver" or "abort" command from the corrupted party. Upon receiving "deliver", the functionality delivers the honest party output. Upon receiving "abort", the functionality instead delivers an abort message $\perp$ to the honest party. In the case where the corrupt party does not expect output, the functionality $\mathcal{F}$ still awaits a "deliver" or "abort" from the corrupt party before delivering output (or $\perp$) to the honest party.

The real-ideal paradigm. A two-party protocol $\Pi_\mathcal{F}$ for computing the functionality $\mathcal{F}$ consists of two families of quantum interactive machines $\{\mathsf{A}_\lambda\}_{\lambda\in\mathbb{N}}, \{\mathsf{B}_\lambda\}_{\lambda\in\mathbb{N}}$. An adversary intending to attack the protocol by corrupting one of the parties can be described by a family of quantum interactive machines $\{\mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$ and a family of initial quantum states $\{|\psi_\lambda\rangle^{\mathcal{X},\mathcal{A},\mathcal{D}}\}_{\lambda\in\mathbb{N}}$ on registers $(\mathcal{X}, \mathcal{A}, \mathcal{D})$, where $\mathcal{X}$ is the honest party's input register, $\mathcal{A}$ is the adversary's input register, and $\mathcal{D}$ is given directly to the distinguisher. That is, the honest party takes as input the state on register $\mathcal{X}$, Adv_λ takes as input the state on register $\mathcal{A}$, and they interact in the protocol $\Pi_\mathcal{F}$. Then, the honest party outputs a state on register $\mathcal{X}'$, Adv_λ outputs a state on register $\mathcal{A}'$, and we define the random variable $\Pi_\mathcal{F}[\mathsf{Adv}_\lambda, |\psi_\lambda\rangle]$

Ideal functionalities

Setup: Parties A and B, security parameter λ.

$\underline{\mathcal{F}_{\mathsf{OT}}}$

- $\mathcal{F}_{\mathsf{OT}}$ receives input $m_0, m_1 \in \{0,1\}^\lambda$ from A and $b \in \{0,1\}$ from B.
- $\mathcal{F}_{\mathsf{OT}}$ delivers m_b to B.

$\underline{\mathcal{F}_{\mathsf{ROT}}}$

- $\mathcal{F}_{\mathsf{ROT}}$ receives input $m_0, m_1 \in \{0,1\}^\lambda$ from A.
- $\mathcal{F}_{\mathsf{ROT}}$ samples a bit $b \leftarrow \{0,1\}$ and delivers (b, m_b) to B.

$\underline{\mathcal{F}_{\mathsf{CL}}[C]}$

- C is a classical circuit with two inputs, one of length $n_1 = n_1(\lambda)$ and one of length $n_2 = n_2(\lambda)$.
- $\mathcal{F}_{\mathsf{CL}}[C]$ receives input $x \in \{0,1\}^{n_1}$ from A.
- $\mathcal{F}_{\mathsf{CL}}[C]$ samples a string $r \leftarrow \{0,1\}^{n_2}$ and delivers $C(x,r)$ to B.

$\underline{\mathcal{F}_{\mathsf{QU}}[Q]}$

- Q is a quantum operation that takes as input a state on register $\mathcal{X}$ of $n = n(\lambda)$ qubits and outputs a state on register $\mathcal{Y}$.
- $\mathcal{F}_{\mathsf{QU}}[Q]$ receives as input a state on register $\mathcal{X}$ from A.
- $\mathcal{F}_{\mathsf{QU}}[Q]$ computes $Q(\mathcal{X}) = \mathcal{Y}$ and delivers $\mathcal{Y}$ to B.

Fig. 2. Ideal functionalities considered in this work.

to consist of the resulting state on registers $(\mathcal{X}', \mathcal{A}', \mathcal{D})$, which will be given to a distinguisher. In the case where the honest party has no input, we don't include a register $\mathcal{X}$, and just consider families $\{|\psi_\lambda\rangle^{\mathcal{A},\mathcal{D}}\}_{\lambda\in\mathbb{N}}$ on registers $\mathcal{A}$ and $\mathcal{D}$. In the case where the honest party has a classical input, we assume that $\mathcal{X}$ is in a standard basis state. In other words, we consider families $\{(x_\lambda, |\psi_\lambda\rangle^{\mathcal{A},\mathcal{D}})\}_{\lambda\in\mathbb{N}}$, where each x_λ is a classical string.

An *ideal-world* protocol $\widetilde{\Pi}_{\mathcal{F}}$ for functionality $\mathcal{F}$ consists of "dummy" parties $\widetilde{A}$ and $\widetilde{B}$ that have access to an additional "trusted" party that implements $\mathcal{F}$. That is, $\widetilde{A}$ and $\widetilde{B}$ only interact directly with $\mathcal{F}$, providing inputs and receiving outputs, and do not interact with each other. We consider the execution of ideal-world protocols in the presence of a simulator, described by a family of quantum interactive machines $\{\mathsf{Sim}_\lambda\}_{\lambda\in\mathbb{N}}$ that controls either party $\widetilde{A}$ or $\widetilde{B}$. The execution of the protocol in the presence of the simulator also begins with a family of states $\{|\psi_\lambda\rangle^{\mathcal{X},\mathcal{A},\mathcal{D}}\}_{\lambda\in\mathbb{N}}$ on registers $(\mathcal{X}, \mathcal{A}, \mathcal{D})$ as described above, and we define the analogous random variable $\widetilde{\Pi}_{\mathcal{F}}[\mathsf{Sim}_\lambda, |\psi_\lambda\rangle]$.

Secure realization. We define what it means for a protocol to securely realize an ideal functionality.

Definition 4 (Secure realization). *A protocol $\Pi_{\mathcal{F}}$* securely realizes *the functionality $\mathcal{F}$ if for any QPT adversary $\{\mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$ corrupting party $M \in \{A, B\}$, there exists a QPT simulator $\{\mathsf{Sim}_\lambda\}_{\lambda\in\mathbb{N}}$ corrupting party M such that for any QPT distinguisher $\{\mathsf{D}_\lambda\}_{\lambda\in\mathbb{N}}$ and polynomial-size family of states $\{|\psi_\lambda\rangle^{\mathcal{X},\mathcal{A},\mathcal{D}}\}_{\lambda\in\mathbb{N}}$,*

$$\left|\Pr[1 \leftarrow \mathsf{D}_\lambda(\Pi_{\mathcal{F}}[\mathsf{Adv}_\lambda, |\psi_\lambda\rangle])] - \Pr\left[1 \leftarrow \mathsf{D}_\lambda(\widetilde{\Pi}_{\mathcal{F}}[\mathsf{Sim}_\lambda, |\psi_\lambda\rangle])\right]\right| = \mathrm{negl}(\lambda).$$

3.4 The XOR extractor

Imported Theorem 6 ([2])**.** *Let $\mathcal{X}$ be an n-qubit register, and consider any quantum state $|\gamma\rangle^{\mathcal{A},\mathcal{X}}$ that can be written as*

$$|\gamma\rangle^{\mathcal{A},\mathcal{X}} = \sum_{u:\mathsf{hw}(u)<n/2} |\psi_u\rangle^{\mathcal{A}} |u\rangle^{\mathcal{X}},$$

where $\mathsf{hw}(\cdot)$ denotes the Hamming weight. Let $\rho^{\mathcal{A},\mathcal{P}}$ be the mixed state that results from measuring $\mathcal{X}$ in the Hadamard basis to produce a string $x \in \{0,1\}^n$, and writing $\bigoplus_{i\in[n]} x_i$ into a single qubit register $\mathcal{P}$. Then it holds that

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

4 One-Shot String Oblivious Transfer

4.1 Construction

In this section, we give our construction of one-shot (random receiver bit) string oblivious transfer in the shared EPR pairs model.

Ingredients

- Non-interactive extractable commitment $(\mathsf{Com}, \mathsf{ExtGen}, \mathsf{Ext})$ in the common random string model. This is known from LWE.
- A programmable hash function family $\{H_\lambda\}_{\lambda\in\mathbb{N}}$ that is sub-exponentially correlation intractable for efficiently verifiable approximate product relations with constant sparsity (Section 3.2). This is known from the sub-exponential hardness of LWE (Imported Theorems 4 and 5).
- Non-interactive zero-knowledge argument $(\mathsf{NIZK.Prove}, \mathsf{NIZK.Ver}, \mathsf{NIZK.Sim})$ in the common random string model. This is known from LWE.
- Pseudorandom generator PRG.

Parameters

- Security parameter λ.
- Correlation intractable hash security parameter $\lambda_{\mathsf{CI}} := \lambda^{1/\delta}$, where $\delta > 0$ is the constant such that $\{H_{\lambda_{\mathsf{CI}}}\}_{\lambda_{\mathsf{CI}} \in \mathbb{N}}$ is $2^{-\lambda_{\mathsf{CI}}^{\delta}}$-correlation intractable.
- Size of commitment key $h = h(\lambda)$.
- Size of NIZK crs $n = n(\lambda)$.
- Size of hash key $k = k(\lambda_{\mathsf{CI}})$.
- Approximation parameter $\alpha = 1/120$.
- Number of repetitions in each group $c = 480$.
- Sparsity $\rho = \frac{\binom{(1-\alpha)c}{(1/2)c}}{2^c} < \alpha$.
- Product parameter $t = t(\lambda_{\mathsf{CI}}) = 180^3 \lambda_{\mathsf{CI}} \geq \lambda_{\mathsf{CI}}/(\alpha - \rho)^3$.
- Total number of repetitions $\ell = \ell(\lambda) = c \cdot t = \mathrm{poly}(\lambda)$.
- PRG range $\{0,1\}^{2\lambda\ell}$.
- CI hash range $\mathcal{Y}^t$, where $\mathcal{Y}$ is the set of subsets of $[c]$ of size $c/2$. We will also parse $T \in \mathcal{Y}^t$ as a subset of $[\ell]$ of size $\ell/2$.

We remark that we have not tried to fully optimize the constants in the parameters above.

Setup

- ℓ collections of EPR pairs indexed by $i \in [\ell]$. Each collection consists of one "control" pair $\{\mathcal{S}_i^{\mathsf{ctl}}, \mathcal{R}_i^{\mathsf{ctl}}\}$ and 2λ "message" pairs on registers $\{\mathcal{S}_{i,j}^{\mathsf{msg}}, \mathcal{R}_{i,j}^{\mathsf{msg}}\}_{j \in [2\lambda]}$. For each $i \in [\ell]$, we define $\mathcal{S}_i := (\mathcal{S}_i^{\mathsf{ctl}}, \mathcal{S}_{i,1}^{\mathsf{msg}}, \ldots, \mathcal{S}_{i,2\lambda}^{\mathsf{msg}})$ and $\mathcal{R}_i := (\mathcal{R}_i^{\mathsf{ctl}}, \mathcal{R}_{i,1}^{\mathsf{msg}}, \ldots, \mathcal{R}_{i,2\lambda}^{\mathsf{msg}})$.
- Commitment key $\mathsf{ck} \leftarrow \{0,1\}^h$.
- NIZK common random string $\mathsf{crs} \leftarrow \{0,1\}^n$.
- Correlation intractable hash key $\mathsf{hk} \leftarrow \{0,1\}^k$.

Note that a shared uniformly random string can be obtained by measuring shared EPR pairs in the same basis, and thus this entire Setup can be obtained with just shared EPR pairs.

Finally, given a commitment key ck for Com and a set $\overline{T} \subset [\ell]$, we define the NP language $\mathcal{L}_{\mathsf{ck},\overline{T}}$ of instance-witness pairs as follows.

$$\left(\left(\{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}\}_{i \in \overline{T}}, \{\mathsf{cm}_i\}_{i \in [\ell]}\right), \left(\{t_i\}_{i \in \overline{T}}, \Delta, s\right)\right) \in \mathcal{L}_{\mathsf{ck},\overline{T}}$$

if and only if[11]

$$\begin{aligned} &\forall i \in \overline{T}, \widehat{\mathsf{cm}}_{i,0} \in \mathsf{Com}(\mathsf{ck}, t_i) \wedge \widehat{\mathsf{cm}}_{i,1} \in \mathsf{Com}(\mathsf{ck}, t_i \oplus \Delta), \text{ and} \\ &\forall i \in [\ell], \mathsf{cm}_i \in \mathsf{Com}(\mathsf{ck}, (\cdot, x_i, \cdot)), \text{where } (x_1, \ldots, x_\ell) := \mathsf{PRG}(s). \end{aligned}$$

Now, our protocol is described in Fig. 3.

[11] Technically, the random coins used to compute the commitments must also be included in the witness.

One-shot protocol for $\mathcal{F}_{\mathsf{ROT}}$

Sender message. Input strings $m_0, m_1 \in \{0,1\}^\lambda$.

1. Sample a PRG seed $s \leftarrow \{0,1\}^\lambda$ and set $(x_1, \ldots, x_\ell) \coloneqq \mathsf{PRG}(s)$, where each $x_i \in \{0,1\}^{2\lambda}$.
2. For each $i \in [\ell]$:
   - For each $j \in [2\lambda]$ such that $x_{i,j} = 1$, apply a CNOT gate from register $\mathcal{S}_i^{\mathsf{ctl}}$ to register $\mathcal{S}_{i,j}^{\mathsf{msg}}$.
   - Measure $\{\mathcal{S}_{i,j}^{\mathsf{msg}}\}_{j\in[2\lambda]}$ in the standard basis to obtain $v_i \in \{0,1\}^{2\lambda}$ and measure $\mathcal{S}_i^{\mathsf{ctl}}$ in the Hadamard basis to obtain $h_i \in \{0,1\}$.
   - Compute $\mathsf{cm}_i \coloneqq \mathsf{Com}(\mathsf{ck}, (v_i, x_i, h_i); r_i)$, where $r_i \leftarrow \{0,1\}^\lambda$ are the random coins used for commitment.
3. Compute $T = H_\lambda(\mathsf{hk}, (\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell)) \subset [\ell]$ and let $\overline{T} \coloneqq [\ell] \setminus T$.
4. Sample $\Delta \leftarrow \{0,1\}^\lambda$ and for each $i \in \overline{T}$:
   - Sample $t_i \leftarrow \{0,1\}^\lambda$ and compute $\widehat{\mathsf{cm}}_{i,0} \coloneqq \mathsf{Com}(\mathsf{ck}, t_i; r_{i,0})$ and $\widehat{\mathsf{cm}}_{i,1} \coloneqq \mathsf{Com}(\mathsf{ck}, t_i \oplus \Delta; r_{i,1})$ where $r_{i,0}, r_{i,1} \leftarrow \{0,1\}^\lambda$ are the random coins used for commitment.
   - Define $z_{i,0} = (t_i, r_{i,0}) \oplus v_i, \quad z_{i,1} = (t_i \oplus \Delta, r_{i,1}) \oplus v_i \oplus x_i$.
5. Define
$$\widetilde{m}_0 \coloneqq m_0 \oplus \bigoplus_{i\in\overline{T}} t_i, \quad \widetilde{m}_1 \coloneqq m_1 \oplus \Delta \oplus \bigoplus_{i\in\overline{T}} t_i.$$
6. Compute $\pi \leftarrow \mathsf{NIZK.Prove}\left(\mathsf{crs}, \left(\{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}\}_{i\in\overline{T}}, \{\mathsf{cm}_i\}_{i\in[\ell]}\right), \left(\{t_i\}_{i\in\overline{T}}, \Delta, s\right)\right)$ for the language $\mathcal{L}_{\mathsf{ck},\overline{T}}$.
7. Send $\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$ to the receiver.

Receiver computation. In what follows, abort and output $\perp$ if any check fails.

1. Compute $T = H_\lambda(\mathsf{hk}, (\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell))$ and check that for all $i \in T$, $\mathsf{cm}_i = \mathsf{Com}(\mathsf{ck}, (v_i, x_i, h_i); r_i)$.
2. For each $i \in T$, define $|\psi_{v_i,x_i,h_i}\rangle \coloneqq \frac{1}{\sqrt{2}}\left(|0, v_i\rangle + (-1)^{h_i}|1, v_i \oplus x_i\rangle\right)$, and measure register $\mathcal{R}_i$ in the basis $\{|\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|, \mathbb{I} - |\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|\}$. Check that for all $i \in T$, the first outcome is observed.
3. Check that $\mathsf{NIZK.Ver}\left(\mathsf{crs}, \left(\{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}\}_{i\in\overline{T}}, \{\mathsf{cm}_i\}_{i\in[\ell]}\right), \pi\right) = \top$.
4. For each $i \in \overline{T}$, measure register $\mathcal{R}_i$ in the standard basis to obtain $b_i \in \{0,1\}$ and $v_i' \in \{0,1\}^{2\lambda}$, compute $(t_i', r_i') = z_{i,b_i} \oplus v_i'$, and check that for each $i \in \overline{T}$, $\widehat{\mathsf{cm}}_{i,b_i} = \mathsf{Com}(\mathsf{ck}, t_i'; r_i')$.
5. Output
$$b \coloneqq \bigoplus_{i\in\overline{T}} b_i, \quad m_b \coloneqq \widetilde{m}_b \oplus \bigoplus_{i\in\overline{T}} t_i'.$$

Fig. 3. A protocol for one-shot random string OT in the shared EPR pair model.

4.2 Security

Theorem 7. *The protocol in Fig. 3 securely realizes (Definition 4) the functionality $\mathcal{F}_{\mathsf{ROT}}$. Thus, assuming the sub-exponential hardness of LWE, there exists a one-message protocol for $\mathcal{F}_{\mathsf{ROT}}$ in the shared EPR pair model.*

The proof of this theorem follows from receiver security, which is shown in Lemma 2 and sender security, which is more straightforward and is deferred to the full version [11].

Lemma 2. *The protocol in Fig. 3 is secure against a malicious sender.*

Proof. Let $\{\mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$ be a QPT adversary corrupting the sender, which takes as input register $\mathcal{A}$ of $\{|\psi_\lambda\rangle^{\mathcal{A},\mathcal{D}}\}_{\lambda\in\mathbb{N}}$. Note that we don't consider a register $\mathcal{X}$ holding the honest party's input, since an honest receiver has no input. We will define a sequence of hybrids, beginning with the real distribution $\mathit{\Pi}_{\mathcal{F}_{\mathsf{ROT}}}[\mathsf{Adv}_\lambda, |\psi_\lambda\rangle]$ and ending with the distribution $\widetilde{\mathit{\Pi}}_{\mathcal{F}_{\mathsf{ROT}}}[\mathsf{Sim}_\lambda, |\psi_\lambda\rangle]$ defined by a simulator $\{\mathsf{Sim}_\lambda\}_{\lambda\in\mathbb{N}}$. Each hybrid is a distribution described by applying an operation to the input register $\mathcal{A}$, and a QPT distinguisher will obtain the output of this distribution along with the register $\mathcal{D}$. We drop the dependence of the hybrids on λ for convenience.

$\underline{\mathcal{H}_0(\mathcal{A})}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $\mathsf{ck} \leftarrow \{0,1\}^h$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

  and a state on register $\mathcal{A}'$.
- Run the Receiver's honest computation on the sender's message to obtain an output (b, m_b) or $\perp$. Output either $(\mathcal{A}', (b, m_b))$ or $(\mathcal{A}', \perp)$.

$\underline{\mathcal{H}_1(\mathcal{A})}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

  and a state on register $\mathcal{A}'$.
- Run the Receiver's honest computation on the sender's message to obtain an output (b, m_b) or $\perp$. Output either $(\mathcal{A}', (b, m_b))$ or $(\mathcal{A}', \perp)$.

$\underline{\mathcal{H}_2(\mathcal{A})}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.

– Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

and a state on register $\mathcal{A}'$.
– Run Steps 1-3 of the Receiver's honest computation on the sender's message.
– We will now *coherently* apply the check described in Step 4 to the registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$. First we introduce some notation. For commitment key ck, commitment $\widehat{\mathsf{cm}}$, and two strings $z_0, z_1 \in \{0,1\}^{2\lambda}$, let $\Pi[\mathsf{ck}, \widehat{\mathsf{cm}}, z_0, z_1]$ be a projection onto strings $(b, v') \in \{0,1\}^{1+2\lambda}$ such that $\widehat{\mathsf{cm}} = \mathsf{Com}(\mathsf{ck}, t; r)$, where $(t, r) := z_b \oplus v'$.
Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and aborts if the projection fails.
– If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, for each $i \in \overline{T}$, measure register $\mathcal{R}_i$ in the standard basis to obtain $b_i \in \{0,1\}$ and $v'_i \in \{0,1\}^{2\lambda}$, and compute $(t'_i, r'_i) = z_{i,b_i} \oplus v'_i$. Then, define

$$b := \bigoplus_{i\in\overline{T}} b_i, \quad m_b := \widetilde{m}_b \oplus \bigoplus_{i\in\overline{T}} t'_i,$$

and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_3(\mathcal{A})}$

– Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
– Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

and a state on register $\mathcal{A}'$.
– Run Steps 1-3 of the Receiver's honest computation on the sender's message.
– Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and abort if the projection fails.
– For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.
– If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, for each $i \in \overline{T}$, measure register $\mathcal{R}_i$ in the standard basis to obtain $b_i \in \{0,1\}$ and $v'_i \in \{0,1\}^{2\lambda}$, and compute $(t'_i, r'_i) = z_{i,b_i} \oplus v'_i$. Then, define

$$b := \bigoplus_{i\in\overline{T}} b_i, \quad m_b := \widetilde{m}_b \oplus \bigoplus_{i\in\overline{T}} t'_i,$$

and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_4(\mathcal{A})}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

  and a state on register $\mathcal{A}'$.
- Run Steps 1-3 of the Receiver's honest computation on the sender's message.
- Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

  and abort if the projection fails.
- For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.
- If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, for each $i \in \overline{T}$, measure register $\mathcal{R}_i^{\mathsf{ctl}}$ in the standard basis to obtain $b_i \in \{0,1\}$. Then, define

$$b := \bigoplus_{i\in\overline{T}} b_i, \quad m_0 := \bigoplus_{i\in\overline{T}} t_{i,0}, \quad m_1 := \widetilde{m}_1 \oplus \Delta \oplus \bigoplus_{i\in\overline{T}} t_{i,0},$$

  and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_5(\mathcal{A})}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

  and a state on register $\mathcal{A}'$.
- Run Steps 1-3 of the Receiver's honest computation on the sender's message.
- We will insert a measurement on the registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$. Before specifying this measurement, we introduce some notation.
  - For $\{(v_i, x_i, h_i)\}_{i\in\overline{T}}$ and a string $e \in \{0,1\}^{|\overline{T}|}$, define

$$\Pi[e, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}]^{\{\mathcal{R}_i\}_{i\in\overline{T}}} := \bigotimes_{i:e_i=0} |\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|^{\mathcal{R}_i} \otimes \bigotimes_{i:e_i=1} \mathbb{I} - |\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|^{\mathcal{R}_i}.$$

  - For $\{(v_i, x_i, h_i)\}_{i\in\overline{T}}$ and a constant $\gamma \in [0,1]$, define

$$\Pi[\gamma, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}]^{\{\mathcal{R}_i\}_{i\in\overline{T}}} := \sum_{e\in\{0,1\}^{|S|}:\mathsf{hw}(e)<\gamma|\overline{T}|} \Pi[e, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}]^{\{\mathcal{R}_i\}_{i\in\overline{T}}}.$$

Compute $(v_i, x_i, h_i) \leftarrow \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$ for each $i \in \overline{T}$. Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\Pi\left[1/30, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right],$$

and abort if this projection fails.

- Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and abort if the projection fails.

- For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.
- If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, for each $i \in \overline{T}$, measure register $\mathcal{R}_i^{\mathsf{ctl}}$ in the standard basis to obtain $b_i \in \{0,1\}$. Then, define

$$b := \bigoplus_{i\in\overline{T}} b_i, \quad m_0 := \bigoplus_{i\in\overline{T}} t_{i,0}, \quad m_1 := \widetilde{m}_1 \oplus \Delta \oplus \bigoplus_{i\in\overline{T}} t_{i,0},$$

and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_6(\mathcal{A})}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

and a state on register $\mathcal{A}'$.

- Run Steps 1-3 of the Receiver's honest computation on the sender's message.
- Compute $(v_i, x_i, h_i) \leftarrow \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$ for each $i \in \overline{T}$. Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\Pi\left[1/30, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right],$$

and abort if this projection fails.

- Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and abort if the projection fails.

- Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\Pi\left[1/2, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right],$$

and abort if this projection fails.

- For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.

– If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, for each $i \in \overline{T}$, measure register $\mathcal{R}_i^{\mathsf{ctl}}$ in the standard basis to obtain $b_i \in \{0,1\}$. Then, define

$$b := \bigoplus_{i \in \overline{T}} b_i, \quad m_0 := \bigoplus_{i \in \overline{T}} t_{i,0}, \quad m_1 := \widetilde{m}_1 \oplus \Delta \oplus \bigoplus_{i \in \overline{T}} t_{i,0},$$

and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_7(\mathcal{A})}$

– Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
– Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

and a state on register $\mathcal{A}'$.
– Run Steps 1-3 of the Receiver's honest computation on the sender's message.
– Compute $(v_i, x_i, h_i) \leftarrow \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$ for each $i \in \overline{T}$. Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\Pi\left[1/30, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right],$$

and abort if this projection fails.
– Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and abort if the projection fails.
– Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\Pi\left[1/2, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right],$$

and abort if this projection fails.
– For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.
– If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, sample $b \leftarrow \{0,1\}$. Then, define

$$m_0 := \bigoplus_{i \in \overline{T}} t_{i,0}, \quad m_1 := \widetilde{m}_1 \oplus \Delta \oplus \bigoplus_{i \in \overline{T}} t_{i,0},$$

and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_8(\mathcal{A})}$

– Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
– Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

and a state on register $\mathcal{A}'$.

– Run Steps 1-3 of the Receiver's honest computation on the sender's message.
– Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and abort if the projection fails.
– For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.
– If there was an abort, output $(\mathcal{A}', \bot)$. Otherwise, sample $b \leftarrow \{0,1\}$. Then, define

$$m_0 := \bigoplus_{i\in\overline{T}} t_{i,0}, \quad m_1 := \widetilde{m}_1 \oplus \Delta \oplus \bigoplus_{i\in\overline{T}} t_{i,0},$$

and output $(\mathcal{A}', (b, m_b))$.

$\underline{\mathcal{H}_9(\mathcal{A}) \ / \ \mathsf{Sim}(\mathcal{A})}$

– Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$, and sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
– Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$ until it outputs a message

$$\left(\{\mathsf{cm}_i\}_{i\in[\ell]}, \{v_i, x_i, h_i, r_i\}_{i\in T}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}, z_{i,0}, z_{i,1}\}_{i\in\overline{T}}, \pi, \widetilde{m}_0, \widetilde{m}_1\right)$$

and a state on register $\mathcal{A}'$.
– Run Steps 1-3 of the Receiver's honest computation on the sender's message.
– Attempt to project registers $\{\mathcal{R}_i\}_{i\in\overline{T}}$ onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i},$$

and abort if the projection fails.
– For each $i \in \overline{T}, b \in \{0,1\}$, compute $t_{i,b} \leftarrow \mathsf{Ext}(\mathsf{ek}, \widehat{\mathsf{cm}}_{i,b})$. Abort if any $t_{i,b} = \bot$ or if there does not exist Δ such that $t_{i,1} = \Delta \oplus t_{i,0}$ for all $i \in \overline{T}$.
– If there was an abort, send $\bot$ to the ideal functionality, and output $\mathcal{A}'$. Otherwise, define

$$m_0 := \bigoplus_{i\in\overline{T}} t_{i,0}, \quad m_1 := \widetilde{m}_1 \oplus \Delta \oplus \bigoplus_{i\in\overline{T}} t_{i,0},$$

send (m_0, m_1) to the ideal functionality, and output $\mathcal{A}'$.

Observe that $\mathcal{H}_9(\mathcal{A})$ describes the behavior of a simulator Sim that operates on input register $\mathcal{A}$, and interacts with the ideal functionality $\mathcal{F}_{\mathsf{ROT}}$. Thus, The following sequence of claims completes the proof.

Claim 8. $\mathcal{H}_0 \approx_c \mathcal{H}_1$.

Proof. This follows directly from the extractability of the commitment. □

Claim 9. $\mathcal{H}_1 \equiv \mathcal{H}_2$.

Proof. The only difference is that we have applied the Step 4 check coherently before measuring in the standard basis. Since these measurements commute, these hybrids describe the same distribution. □

Claim 10. $\mathcal{H}_2 \approx_s \mathcal{H}_3$.

Proof. The newly introcued abort condition will only be triggered with negligible probability due to the soundness of the NIZK and the extractability of the commitment. □

Claim 11. $\mathcal{H}_3 \approx_s \mathcal{H}_4$.

Proof. We are now defining m_0, m_1 based on the strings extracted by Ext rather than the strings measured by the Receiver. Since the strings measured by the Receiver must be valid commitment openings, this only introduces a negligible difference due to the extractability of the commitment. □

Claim 12. $\mathcal{H}_4 \approx_s \mathcal{H}_5$.

Proof. By Gentle Measurement (Lemma 1), it suffices to argue that the projection introduced in $\mathcal{H}_5$ will succeed with probability $1 - \mathrm{negl}(\lambda)$. So towards contradiction, assume that the projection fails with non-negligible probability. We will eventually use this assumption to break the correlation intractability of H. First, consider the following experiment.

$\underline{\mathsf{Exp}_1}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$. Sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$, and receive a message that includes $\{\mathsf{cm}_i\}_{i\in[\ell]}, \{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}\}_{i\in\overline{T}}, \pi$.
- Compute $T = H_\lambda(\mathsf{hk}, (\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell))$, check that for all $i \in T$, $\mathsf{cm}_i = \mathsf{Com}(\mathsf{ck}, (v_i, x_i, h_i); r_i)$, and that $\mathsf{NIZK.Ver}\left(\mathsf{crs}, \left(\{\widehat{\mathsf{cm}}_{i,0}, \widehat{\mathsf{cm}}_{i,1}\}_{i\in\overline{T}}, \{\mathsf{cm}_i\}_{i\in[\ell]}\right), \pi\right) = \top$, and abort if not.
- For each $i \in [\ell]$, compute $(v_i, x_i, h_i) \leftarrow \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$, and abort if any are $\perp$.
- For each $i \in [\ell]$, measure registers $\mathcal{R}_i$ in the basis $\{|\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|, \mathbb{I} - |\psi_{v_i,x_i,h_i}\rangle\langle\psi_{v_i,x_i,h_i}|\}$ and define the bit $e_i = 0$ if the first outome is observed and $e_i = 1$ if the second outcome is observed.
- Output 1 if (i) there exists an $s \in \{0,1\}^\lambda$ such that $(x_1, \ldots, x_\ell) = \mathsf{PRG}(s)$,[12] (ii) $e_i = 0$ for all $i \in T$, and (iii) $e_i = 1$ for at least $1/30$ fraction of $i : i \in \overline{T}$.

[12] Note that this step is not efficient to implement, but this will not be important for our arguments.

We claim that $\Pr[\mathsf{Exp}_1 \to 1] = \mathsf{non\text{-}negl}(\lambda)$. This nearly follows from the assumption that the measurement introduced in $\mathcal{H}_5$ rejects with non-negligible probability, except for the following two differences. One difference from $\mathcal{H}_3$ is that in Exp_1, we are using $\{(v_i, x_i, h_i)\}_{i\in T}$ extracted from $\{\mathsf{cm}_i\}_{i\in T}$ to measure registers $\{\mathcal{R}_i\}_{i\in T}$, rather than the strings sent by the adversary. However, this introduces a negligible difference due to the extractability of the commitment scheme. The other difference is that we require $(x_1, \ldots, x_\ell)$, which are extracted from $\{\mathsf{cm}_i\}_{i\in[\ell]}$, to be in the image of $\mathsf{PRG}(\cdot)$. However, by extractability of the commitment scheme and soundness of the NIZK, the probability that the procedure does not abort and this fails to occur is negligible. Next, consider the following experiment.

$\underline{\mathsf{Exp}_2}$

- Prepare ℓ collections of EPR pairs on registers $\{\mathcal{S}_i, \mathcal{R}_i\}_{i\in[\ell]}$. Sample $(\mathsf{ck}, \mathsf{ek}) \leftarrow \mathsf{ExtGen}(1^\lambda)$, $\mathsf{crs} \leftarrow \{0,1\}^n$, and $\mathsf{hk} \leftarrow \{0,1\}^k$.
- Sample $s^* \leftarrow \{0,1\}^\lambda$ and set $(x_1^*, \ldots, x_\ell^*) = \mathsf{PRG}(s^*)$. For each $i \in [\ell]$ and $j \in [2\lambda]$ such that $x_{i,j} = 1$, apply a CNOT gate from register $\mathcal{R}_i^{\mathsf{ctl}}$ to $\mathcal{R}_{i,j}^{\mathsf{msg}}$, then measure $\mathcal{R}_i^{\mathsf{ctl}}$ in the Hadamard basis to obtain h_i^* and measure $\mathcal{R}_{i,1}^{\mathsf{msg}}, \ldots, \mathcal{R}_{i,2\lambda}^{\mathsf{msg}}$ in the standard basis to obtain v_i^*.
- Run Adv_λ on input $\mathcal{A}, \{\mathcal{S}_i\}_{i\in[\ell]}, \mathsf{ck}, \mathsf{crs}, \mathsf{hk}$, and receive a message that includes $\{\mathsf{cm}_i\}_{i\in[\ell]}$.
- Compute $T = H_\lambda(\mathsf{hk}, (\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell))$ and $(v_i, x_i, h_i) \leftarrow \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$ for each $i \in [\ell]$.
- Output 1 if (i) $(x_1, \ldots, x_\ell) = (x_1^*, \ldots, x_\ell^*)$, (ii) $(v_i, h_i) = (v_i^*, h_i^*)$ for all $i \in T$, and (iii) $(v_i, h_i) \neq (v_i^*, h_i^*)$ for at least $1/30$ fraction of $i : i \in \overline{T}$.

It follows that $\Pr[\mathsf{Exp}_2 \to 1] = \mathsf{non\text{-}negl}(\lambda)/2^\lambda > 1/2^{\lambda^\delta_{\mathsf{CI}}}$, since the guess of s^* is uniformly random and independent of the adversary's view. Finally, we will show that Exp_2 can be used to break the correlation intractability of H, but first we introduce some notation.

- For each $(\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]})$, define the relation $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]$ as follows. Recalling that $\ell = c \cdot t$, we will associate each $i \in [\ell]$ with a pair (ι, κ) for $\iota \in [t], \kappa \in [c]$. Also, for each set of strings $\{\mathsf{cm}_i\}_{i\in[\ell]}$, we fix $(v_i, x_i, h_i) := \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$ for each $i \in [\ell]$. Then the domain will consist of strings $\{\mathsf{cm}_i\}_{i\in[\ell]}$ such that (i) $(x_1, \ldots, x_\ell) = \mathsf{PRG}(s^*)$, (ii) $|i : (v_i, h_i) = (v_i^*, h_i^*)| \leq (1 - 1/60)\ell$, and (iii) for each $\iota \in [t]$, $|\kappa : (v_{(\iota,\kappa)}, h_{(\iota,\kappa)}) = (v_{(\iota,\kappa)}^*, h_{(\iota,\kappa)}^*)| \geq (1/2)c$.
- For each $\{\mathsf{cm}_i\}_{i\in[\ell]}$ in the domain of $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]$, define the sets $\{S_{\iota,\{\mathsf{cm}_i\}_{i\in[\ell]}}\}_{\iota\in[t]}$ as follows. If $(1/2)c \leq |\kappa : (v_{(\iota,\kappa)}, h_{(\iota,\kappa)}) = (v_{(\iota,\kappa)}^*, h_{(\iota,\kappa)}^*)| \leq (1 - 1/120)c$, let $S_{\iota,\{\mathsf{cm}_i\}_{i\in[\ell]}}$ consist of subsets $C \subset [c]$ of size $c/2$ such that for all $\kappa \in C$, $(v_{(\iota,\kappa)}, h_{(\iota,\kappa)}) = (v_{(\iota,\kappa)}^*, h_{(\iota,\kappa)}^*)$. Otherwise, let $S_{\iota,\{\mathsf{cm}_i\}_{i\in[\ell]}} = \emptyset$.
- Define the set $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]_{\{\mathsf{cm}_i\}_{i\in[\ell]}}$ to consist of all $y = (C_1, \ldots, C_t)$ such that $C_\iota \in S_{\iota,\{\mathsf{cm}\}_{i\in[\ell]}}$ for all ι such that $S_{\iota,\{\mathsf{cm}\}_{i\in[\ell]}} \neq \emptyset$. We claim that there are always at least $1/120$ fraction of $\iota \in [t]$ such that $S_{\iota,\{\mathsf{cm}_i\}_{i\in[\ell]}} \neq \emptyset$. To see this, note that $S_{\iota,\{\mathsf{cm}_i\}_{i\in[\ell]}} \neq \emptyset$ iff $|\kappa : (v_{(\iota,\kappa)}, h_{(\iota,\kappa)}) \neq (v_{(\iota,\kappa)}^*, h_{(\iota,\kappa)}^*)| >$

$(1/120)c$. However, if less $1/120$ fraction of ι satisfies this condition, then the fraction of $i \in [\ell]$ such that $(v_i, h_i) \neq (v_i^*, h_i^*)$ is at most $(1/120) + (1/120)(1 - 1/120) < 1/60$, which would contradict the fact that $\{\mathsf{cm}_i\}_{i\in[\ell]}$ is in the domain of $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]_{\{\mathsf{cm}_i\}_{i\in[\ell]}}$.

Thus, $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]$ is an α-approximate efficiently verifiable product relation for $\alpha = 1/120$ with sparsity $\rho = \binom{(1-\alpha)c}{(1/2)c}/2^c < \alpha$.

Now, whenever $\mathsf{Exp}_2 = 1$, it must be the case that $\{\mathsf{cm}_i\}_{i\in[\ell]}$ is in the domain of $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]$, and $T \in R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]_{\{\mathsf{cm}_i\}_{i\in[\ell]}}$. Thus, we can break correlation intractability as follows. Begin running Exp_2, but don't sample hk. Once ek, s^* are sampled and $\{v_i^*, h_i^*\}_{i\in[\ell]}$ are measured, declare the relation $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]$. Then, receive hk from the correlation intractability challenger, continue running Exp_2 until $\{\mathsf{cm}_i\}_{i\in[\ell]}$ is obtained, and output this to the challenger. The above analysis shows that this breaks correlation intractability for the relation $R[\mathsf{ek}, s^*, \{v_i^*, h_i^*\}_{i\in[\ell]}]$.

□

Claim 13. $\mathcal{H}_5 \approx_s \mathcal{H}_6$.

Proof. By Gentle Measurement (Lemma 1), it suffices to show that the projection introduced in $\mathcal{H}_6$ will succeed with probability $1 - \mathrm{negl}(\lambda)$. To do so, we will rule out one bad case. For each $i \in \overline{T}$, define the bit $f_i = 0$ if and only if $\widehat{\mathsf{cm}}_{i,0} = \mathsf{Com}(\mathsf{ck}, t_{i,0}; r_{i,0})$ and $\widehat{\mathsf{cm}}_{i,1} = \mathsf{Com}(\mathsf{ck}, t_{i,1}; r_{i,1})$, where $(t_{i,0}, r_{i,0}) = z_{i,0} \oplus v_i$, $(t_{i,1}, r_{i,1}) = z_{i,1} \oplus v_i \oplus x_i$, and $(v_i, x_i, h_i) \coloneqq \mathsf{Ext}(\mathsf{ek}, \mathsf{cm}_i)$. Now we claim that if the fraction of $i \in \overline{T}$ such that $f_i = 1$ is $\geq 1/2 - 1/30$, then the attempted projection onto

$$\bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}]^{\mathcal{R}_i}$$

performed during Step 4 of the receiver's computation would have failed with probabilty $1 - \mathrm{negl}(\lambda)$. To see this, consider any state $|\psi\rangle^{\{\mathcal{R}_i\}_{i\in[\ell]},\mathcal{X}}$ in the image of $\Pi\left[1/30, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right]$, where $\mathcal{X}$ is an arbitrary auxiliary register. Then, defining $\gamma = 1/30$, we write $|\psi\rangle$ as

$$|\psi\rangle \coloneqq \sum_{e\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e)<\gamma|\overline{T}|} \left(\bigotimes_{i:e_i=0} |\psi_{v_i,x_i,h_i}\rangle^{\mathcal{R}_i}\right) \otimes |\psi_e\rangle^{\{\mathcal{R}_i\}_{i:e_i=1},\mathcal{X}},$$

where $|\psi_e\rangle$ is some unit vector that is orthogonal to $|\psi_{v_i,x_i,h_i}\rangle$ for all i such that $e_i = 1$. Then,

$$\begin{aligned}
&\left\| \bigotimes_{i\in\overline{T}} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}] \, |\psi\rangle \right\|^2 \\
&\leq \left\| \sum_{e\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e)<\gamma|\overline{T}|} \bigotimes_{i:e_i=0} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_i, z_{i,0}, z_{i,1}] \, |\psi_{v_i,x_i,h_i}\rangle^{\mathcal{R}_i} \right\|^2 \\
&\leq \binom{|\overline{T}|}{\gamma|\overline{T}|} \sum_{e\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e)<\gamma|\overline{T}|} \left\| \bigotimes_{i:e_i=0} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_i, z_{i,0}, z_{i,1}] \, |\psi_{v_i,x_i,h_i}\rangle^{\mathcal{R}_i} \right\|^2 \\
&\leq \binom{|\overline{T}|}{\gamma|\overline{T}|}^2 \cdot 2^{-(1/2-2\gamma)|\overline{T}|} \leq (3/\gamma)^{2\gamma|\overline{T}|} \cdot 2^{-(1/2-2\gamma)|\overline{T}|} \\
&= 2^{|\overline{T}|(2\gamma\log(3/\gamma)-(1/2-2\gamma))} = \mathrm{negl}(\lambda)
\end{aligned}$$

where the second inequality is Cauchy-Schwartz, the third inequality follow from the fact that there are at least $1/2 - 2\gamma$ fraction of indices where $f_i = 1$ and $e_i = 0$, and the final equality follows because $\gamma = 1/30$ is such that $2\gamma\log(3/\gamma) - (1/2 - 2\gamma) = O(1)$ and $|\overline{T}| = \ell/2 = \Omega(\lambda)$, so the exponent is $\Omega(\lambda)$.

Thus it suffices to consider the case where the fraction of $i \in \overline{T}$ such that $f_i = 1$ is $< 1/2 - 1/30$. So consider any state $|\psi\rangle^{\{\mathcal{R}_i\}_{i\in[\ell]},\mathcal{X}}$ in the image of $\Pi\left[1/30, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right]$, which we can write as

$$|\psi\rangle \coloneqq \sum_{e\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e)<|\overline{T}|/30} \left(\bigotimes_{i:e_i=0} |\psi_{v_i,x_i,h_i}\rangle^{\mathcal{R}_i} \right) \otimes |\psi_e\rangle^{\{\mathcal{R}_i\}_{i:e_i=1},\mathcal{X}}.$$

Then,

$$\begin{aligned}
&\Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}] \, |\psi\rangle \\
&= \sum_{e\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e)<|\overline{T}|/30} \left(\bigotimes_{i:e_i=0\wedge f_i=0} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}] \, |\psi_{v_i,x_i,h_i}\rangle \right) \\
&\qquad\qquad \otimes \left(\bigotimes_{i:e_i=1\vee f_i=1} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}] \right) |\psi_e\rangle \\
&= \sum_{e\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e)<|\overline{T}|/30} \left(\bigotimes_{i:e_i=0\wedge f_i=0} |\psi_{v_i,x_i,h_i}\rangle \right) \otimes \left(\bigotimes_{i:e_i=1\vee f_i=1} \Pi[\mathsf{ck}, \widehat{\mathsf{cm}}_{i,0}, z_{i,0}, z_{i,1}] \right) |\psi_e\rangle \\
&= \sum_{e'\in\{0,1\}^{|\overline{T}|}:\mathsf{hw}(e')<|\overline{T}|/2} \left(\bigotimes_{i:e'_i=0} |\psi_{v_i,x_i,h_i}\rangle \right) \otimes |\psi_{e'}\rangle \\
&\in \mathsf{Im}\left(\Pi\left[1/2, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right]\right),
\end{aligned}$$

where the $|\psi_{e'}\rangle$ are some set of unit vectors.

□

Claim 14. $\mathcal{H}_6 \equiv \mathcal{H}_7$.

Proof. It suffices to show that in $\mathcal{H}_6$, the bit $b = \bigoplus_{i\in\overline{T}} b_i$ sampled by measuring registers $\{\mathcal{R}_i^{\mathsf{ctl}}\}_{i\in\overline{T}}$ of $|\psi\rangle^{\{\mathcal{R}_i\}_{i\in[\ell]},\mathcal{X}}$ in the standard basis is uniformly random, even conditioned on the auxiliary register $\mathcal{X}$ (which includes the view of the adversarial sender). This follows from Imported Theorem 6 by applying a change of basis. In more detail, define the unitary U_{v_i,x_i,h_i} to be applied to $\mathcal{R}_i$ as follows: For each $j \in [2\lambda]$ such that $x_{i,j} = 1$ apply a CNOT gate from $\mathcal{R}_{i,j}^{\mathsf{ctl}}$ to $\mathcal{R}_{i,j}^{\mathsf{msg}}$, then apply a classically controlled phase flip Z^{h_i} to $\mathcal{R}_i^{\mathsf{ctl}}$, and finally apply a Hadamard gate to $\mathcal{R}_i^{\mathsf{ctl}}$. In particular,

$$U_{v_i,x_i,h_i} |\psi_{v_i,x_i,h_i}\rangle = |0\rangle |v_i\rangle .$$

Thus, for any $|\psi\rangle \in \mathsf{Im}(\Pi\left[1/2, \{(v_i, x_i, h_i)\}_{i\in\overline{T}}\right])$, it holds that registers $\{\mathcal{R}_i^{\mathsf{ctl}}\}_{i\in\overline{T}}$ of $(\bigotimes_{i\in\overline{T}} U_{v_i,x_i,h_i}) |\psi\rangle$ are in a superposition of standard basis states with Hamming weight $< |\overline{T}|/2$. Since applying $U_{v_i,x_i,h_i}^\dagger$ to a standard basis measurement of $\mathcal{R}_i^{\mathsf{ctl}}$ yields a Hadamard basis measurement of $\mathcal{R}_i^{\mathsf{ctl}}$, Imported Theorem 6 directly implies that the bit $b = \bigoplus_{i\in\overline{T}} b_i$ is uniformly random, even conditioned on the auxiliary register $\mathcal{X}$.

□

Claim 15. $\mathcal{H}_7 \approx_s \mathcal{H}_8$.

Proof. We are removing the two measurements introduced in hybrids $\mathcal{H}_5$ and $\mathcal{H}_6$, and indistinguishability follows from the same arguments used in the corresponding claims Claim 12 and Claim 13. □

Claim 16. $\mathcal{H}_8 \equiv \mathcal{H}_9$.

Proof. This is just a syntactic switch, routing information through the ideal functionality $\mathcal{F}_{\mathsf{ROT}}$. □

□

References

1. Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes, 2016.
2. Amit Agarwal, James Bartusek, Dakshita Khurana, and Nishant Kumar. A new framework for quantum oblivious transfer. In *Eurocrypt 2023 (to appear)*, 2023.
3. Shweta Agarwal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Public key encryption with secure key leasing. In *Eurocrypt 2023 (to appear)*, 2023.

4. Shweta Agrawal, Yuval Ishai, Eyal Kushilevitz, Varun Narayanan, Manoj Prabhakaran, Vinod M. Prabhakaran, and Alon Rosen. Cryptography from one-way communication: On completeness of finite channels. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part III*, volume 12493 of *Lecture Notes in Computer Science*, pages 653–685. Springer, 2020.
5. Shweta Agrawal, Yuval Ishai, Eyal Kushilevitz, Varun Narayanan, Manoj Prabhakaran, Vinod M. Prabhakaran, and Alon Rosen. Secure computation from one-way noisy communication, or: Anti-correlation via anti-concentration. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II*, volume 12826 of *Lecture Notes in Computer Science*, pages 124–154. Springer, 2021.
6. Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. Cryptology ePrint Archive, Paper 2023/325, 2023. https://eprint.iacr.org/2023/325.
7. Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 208–236. Springer, 2022.
8. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. On the round complexity of secure quantum computation. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 406–435, Cham, 2021. Springer International Publishing.
9. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 467–496, Cham, 2021. Springer International Publishing.
10. James Bartusek, Sanjam Garg, Vipul Goyal, Dakshita Khurana, Giulio Malavolta, Justin Raizes, and Bhaskar Roberts. Obfuscation and outsourced computation with certified deletion. Cryptology ePrint Archive, Paper 2023/265, 2023. https://eprint.iacr.org/2023/265.
11. James Bartusek, Dakshita Khurana, and Akshayaram Srinivasan. Secure computation with shared epr pairs (or: How to teleport in zero-knowledge). Cryptology ePrint Archive, Paper 2023/564, 2023. https://eprint.iacr.org/2023/564.
12. James Bartusek and Giulio Malavolta. Indistinguishability obfuscation of null quantum circuits and applications. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 15:1–15:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.
13. Fabrice Benhamouda and Huijia Lin. k-round multiparty computation from k-round oblivious transfer via garbled interactive circuits. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 500–532. Springer, Heidelberg, April / May 2018.
14. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

15. Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.
16. Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.
17. Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 724–741. Springer, Heidelberg, August 2010.
18. Zvika Brakerski, Venkata Koppula, and Tamer Mour. NIZK from LPN and trapdoor hash via correlation intractability for approximable relations. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO*, volume 12172 of *Lecture Notes in Computer Science*, pages 738–767. Springer, 2020.
19. Zvika Brakerski and Henry Yuen. Quantum garbled circuits. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, page 804–817, New York, NY, USA, 2022. Association for Computing Machinery.
20. Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement. *Science (New York, N.Y.)*, 314:436–9, 11 2006.
21. Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, and Daniel Wichs. Fiat-shamir: From practice to theory. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 1082–1090, New York, NY, USA, 2019. Association for Computing Machinery.
22. Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, 2004.
23. Arka Rai Choudhuri, Sanjam Garg, Abhishek Jain, Zhengzhong Jin, and Jiaheng Zhang. Correlation intractability and SNARGs from sub-exponential DDH. 2022. https://eprint.iacr.org/2022/1486.
24. Arka Rai Choudhuri, Abhishek Jain, and Zhengzhong Jin. Non-interactive batch arguments for NP from standard assumptions. *IACR Cryptol. ePrint Arch.*, 2021:807, 2021.
25. Arka Rai Choudhuri, Abhishek Jain, and Zhengzhong Jin. Snargs for P from LWE. *IACR Cryptol. ePrint Arch.*, page 808, 2021.
26. Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 556–584, Cham, 2021. Springer International Publishing.
27. Léo Colisson, Garazi Muguruza, and Florian Speelman. Oblivious transfer from zero-knowledge proofs, or how to achieve round-optimal quantum oblivious transfer and zero-knowledge proofs on quantum states, 2023.
28. Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th FOCS*, pages 42–52. IEEE Computer Society Press, October 1988.
29. Claude Crépeau, Jeroen van de Graaf, and Alain Tapp. Committed oblivious transfer and private multi-party computation. In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 110–123. Springer, Heidelberg, August 1995.
30. Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.

31. Frédéric Dupuis, Philippe Lamontagne, and Louis Salvail. Fiat-shamir for proofs lacks a proof even in the presence of shared entanglement, 2022.
32. A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.
33. Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.
34. Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2015.
35. Sanjam Garg, Yuval Ishai, and Akshayaram Srinivasan. Two-round MPC: Information-theoretic and black-box. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part I*, volume 11239 of *LNCS*, pages 123–151. Springer, Heidelberg, November 2018.
36. Sanjam Garg and Akshayaram Srinivasan. Two-round multiparty secure computation from minimal assumptions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 468–499. Springer, Heidelberg, April / May 2018.
37. Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Paper 2020/877, 2020. https://eprint.iacr.org/2020/877.
38. Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 531–561, Cham, 2021. Springer International Publishing.
39. Shai Halevi, Yehuda Lindell, and Benny Pinkas. Secure computation on the web: Computing without simultaneous interaction. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 132–150. Springer, Heidelberg, August 2011.
40. Justin Holmgren, Alex Lombardi, and Ron D. Rothblum. Fiat–shamir via list-recoverable codes (or: Parallel repetition of gmw is not zero-knowledge). In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, page 750–760, New York, NY, USA, 2021. Association for Computing Machinery.
41. James Hulett, Ruta Jawale, Dakshita Khurana, and Akshayaram Srinivasan. Snargs for P from sub-exponential DDH and QR. In Orr Dunkelman and Stefan Dziembowski, editors, *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 II*, volume 13276 of *Lecture Notes in Computer Science*, pages 520–549. Springer, 2022.
42. Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 8–26. Springer, Heidelberg, August 1990.
43. Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. Quantum search-to-decision reductions and the state synthesis problem. In *Proceedings of the 37th Computational Complexity Conference*, CCC '22, Dagstuhl, DEU, 2022. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
44. Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, Heidelberg, August 2008.

45. Abhishek Jain and Zhengzhong Jin. Non-interactive zero knowledge from sub-exponential DDH. In Anne Canteaut and François-Xavier Standaert, editors, *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 I*, volume 12696 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2021.
46. Ruta Jawale, Yael Tauman Kalai, Dakshita Khurana, and Rachel Zhang. Snargs for bounded depth computations and PPAD hardness from sub-exponential LWE. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 708–721. ACM, 2021.
47. Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Heidelberg, August 2018.
48. Yael Kalai, Alex Lombardi, and Vinod Vaikuntanathan. SNARGs and PPAD hardness from the Decisional Diffie-Hellman Assumption. In *Eurocrypt 2023 (to appear)*, 2023.
49. Yael Tauman Kalai, Vinod Vaikuntanathan, and Rachel Yun Zhang. Somewhere statistical soundness, post-quantum security, and snargs. Cryptology ePrint Archive, Report 2021/788, 2021. https://ia.cr/2021/788.
50. Dakshita Khurana, Rafail Ostrovsky, and Akshayaram Srinivasan. Round optimal black-box "commit-and-prove". In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part I*, volume 11239 of *LNCS*, pages 286–313. Springer, Heidelberg, November 2018.
51. Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In Toshihide Ibaraki, Naoki Katoh, and Hirotaka Ono, editors, *Algorithms and Computation*, pages 178–188, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
52. Tomoyuki Morimae and Takashi Yamakawa. Classically verifiable nizk for qma with preprocessing. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 599–627, Cham, 2022. Springer Nature Switzerland.
53. Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. *CoRR*, abs/2210.03394, 2022.
54. Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from (plain) learning with errors. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 89–114. Springer, Heidelberg, August 2019.
55. Gregory Rosenthal and Henry S. Yuen. Interactive proofs for synthesizing quantum states and unitaries. In *ITCS*, 2022.
56. Andreas J. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7):2481–2485, 1999.