Oblivious Transfer Is in MiniQCrypt

Alex B. Grilo[1(✉)], Huijia Lin[2(✉)], Fang Song[3(✉)], and Vinod Vaikuntanathan[4(✉)]

[1] CNRS, LIP6, Sorbonne Université, Paris, France
Alex.Bredariol-Grilo@lip6.fr
[2] University of Washington, Seattle, WA, USA
rachel@cs.washington.edu
[3] Portland State University, Portland, OR, USA
fsong@pdx.edu
[4] MIT, Cambridge, MA, USA
vinodv@csail.mit.edu

Abstract. MiniQCrypt is a world where quantum-secure one-way functions exist, and quantum communication is possible. We construct an oblivious transfer (OT) protocol in MiniQCrypt that achieves simulation-security in the plain model against malicious quantum polynomial-time adversaries, building on the foundational work of Crépeau and Kilian (FOCS 1988) and Bennett, Brassard, Crépeau and Skubiszewska (CRYPTO 1991). Combining the OT protocol with prior works, we obtain secure two-party and multi-party computation protocols also in MiniQCrypt. This is in contrast to the classical world, where it is widely believed that one-way functions alone do not give us OT.

In the common random string model, we achieve a *constant-round* universally composable (UC) OT protocol.

1 Introduction

Quantum computing and modern cryptography have enjoyed a highly productive relationship for many decades ever since the conception of both fields. On the one hand, (large-scale) quantum computers can be used to break many widely used cryptosystems based on the hardness of factoring and discrete logarithms, thanks to Shor's algorithm [60]. On the other hand, quantum information and computation have helped us realize cryptographic tasks that are otherwise impossible, for example quantum money [65] and generating certifiable randomness [13,17,63].

Yet another crown jewel in quantum cryptography is the discovery, by Bennett and Brassard [8], of a key exchange protocol whose security is unconditional. That is, they achieve information-theoretic security for a cryptographic task that classically necessarily has to rely on unproven computational assumptions. In a nutshell, they accomplish this using the uncloneability of quantum states, a bedrock principle of quantum mechanics. What's even more remarkable is the

A full version of this paper appears on ePrint Archive Report 2020/1500 [35].

A. Canteaut and F.-X. Standaert (Eds.): EUROCRYPT 2021, LNCS 12697, pp. 531–561, 2021.
https://doi.org/10.1007/978-3-030-77886-6_18

fact that their protocol makes minimalistic use of quantum resources, and consequently, has been implemented in practice over very large distances [23,45]. This should be seen in contrast to large scale quantum *computation* whose possibility is still being actively debated.

Bennett and Brassard's groundbreaking work raised a *tantalizing* possibility for the field of cryptography:

Could every *cryptographic primitive*
be realized unconditionally using quantum information?

A natural next target is oblivious transfer (OT), a versatile cryptographic primitive which, curiously, had its origins in Wiesner's work in the 1970s on quantum information [65] before being rediscovered in cryptography by Rabin [56] in the 1980s. Oblivious transfer (more specifically, 1-out-of-2 OT) is a two-party functionality where a receiver Bob wishes to obtain one out of two bits that the sender Alice owns. The OT protocol must ensure that Alice does not learn which of the two bits Bob received, and that Bob learns only one of Alice's bits and no information about the other. Oblivious transfer lies at the foundation of secure computation, allowing us to construct protocols for the secure multiparty computation (MPC) of any polynomial-time computable function [33,42,43].

Crépeau and Killian [19] and Bennett, Brassard, Crépeau and Skubiszewska [9] constructed an OT protocol given an *ideal* bit commitment protocol and quantum communication. In fact, the only quantum communication in their protocol consisted of Alice sending several so-called "BB84 states" to Bob. Unfortunately, *unconditionally secure* commitment [49,53] and *unconditionally secure* OT [16,48] were soon shown to be impossible even with quantum resources.

However, given that bit commitment can be constructed from one-way functions (OWF) [37,54], the hope remains that OT, and therefore a large swathe of cryptography, can be based on only *OWF* together with (practically feasible) quantum communication. Drawing our inspiration from Impagliazzo's five worlds in cryptography [39], we call such a world, where post-quantum secure one-way functions (pqOWF) exist and quantum computation and communication are possible, Mini**Q**Crypt. The question that motivates this paper is:

Do OT and MPC exist in MiniQCrypt?

Without the quantum power, this is widely believed to be impossible. That is, given only OWFs, there are no *black-box* constructions of OT or even key exchange protocols [40,57]. The fact that [8] overcome this barrier and construct a key exchange protocol with quantum communication (even without the help of OWFs) reinvigorates our hope to do the same for OT.

Aren't We Done Already? At this point, the reader may wonder why we do not have an affirmative answer to this question already, by combining the OT protocol of [9,19] based on bit commitments, with a construction of bit commitments from pqOWF [37,54]. Although this possibility was mentioned already in [9], where they note that "...computational complexity based quantum cryptography is interesting since it allows to build oblivious transfer around one-way functions.", attaining this goal remains elusive as we explain below.

First, proving the security of the [9,19] OT protocol (regardless of the assumptions) turns out to be a marathon. After early proofs against limited adversaries [52,66], it is relatively recently that we have a clear picture with formal proofs against arbitrary quantum polynomial-time adversaries [12,20,21,61]. Based on these results, we can summarize the state of the art as follows.

- *Using Ideal Commitments:* If we assume an *ideal* commitment protocol, formalized as universally composable (UC) commitment, then the quantum OT protocol can be proven secure in strong simulation-based models, in particular the quantum UC model that admits sequential composition or even concurrent composition in a network setting [12,20,30,61]. However, UC commitments, in contrast to vanilla computationally-hiding and statistically-binding commitments, are powerful objects that do not live in Minicrypt. In particular, UC commitments give us key exchange protocols and are therefore black-box separated from Minicrypt.[1]
- *Using Vanilla Commitments:* If in the [9,19] quantum OT protocol we use a *vanilla* statistically-binding and computationally hiding commitment scheme, which exists assuming a pqOWF, the existing proofs, for example [12], fall short in two respects.
  First, for a malicious receiver, the proof of [12] constructs only an *in*efficient simulator. Roughly speaking, this is because the OT receiver in [9,19] acts as a committer, and vanilla commitments are not extractable. Hence, we need an inefficient simulator to extract the committed value by brute force. Inefficient simulation makes it hard, if not impossible, to use the OT protocol to build other protocols (even if we are willing to let the resulting protocol have inefficient simulation). Our work will focus on achieving the standard ideal/real notion of security [32] with efficient simulators.
  Secondly, it is unclear how to construct a simulator (even ignoring efficiency) for a malicious sender. Roughly speaking, the issue is that simulation seems to require that the commitment scheme used in [9,19] be secure against selective opening attacks, which vanilla commitments do not guarantee [6].
- *Using Extractable Commitments:* It turns out that the first difficulty above can be addressed if we assume a commitment protocol that allows *efficient extraction* of the committed value – called extractable commitments. Constructing extractable commitments is surprisingly challenging in the quantum world because of the hardness of rewinding. Moreover, to plug into the quantum OT protocol, we need a strong version of extractable commitments from which the committed values can be extracted efficiently *without destroying or*

[1] The key exchange protocol between Alice and Bob works as follows. Bob, playing the simulator for a malicious sender in the UC commitment protocol, chooses a common reference string (CRS) with a trapdoor TD and sends the CRS to Alice. Alice, playing the sender in the commitment scheme, chooses a random K and runs the committer algorithm. Bob runs the straight-line simulator-extractor (guaranteed by UC simulation) using the TD to get K, thus ensuring that Alice and Bob have a common key. An eavesdropper Eve should not learn K since the above simulated execution is indistinguishable from an honest execution, where K is hidden.

even disturbing the quantum states of the malicious committer,[2] a property that is at odds with quantum unclonability and rules out several extraction techniques used for achieving arguments of knowledge such as in [62]. In particular, we are not aware of a construction of such extractable commitments without resorting to strong assumptions such as (unleveled) quantum FHE and LWE [2,10], which takes us out of minicrypt. Another standard way to construct extractable commitments is using public-key encryption in the CRS model, which unfortunately again takes us out of minicrypt.

To summarize, we would like to stress that before our work, the claims that quantum OT protocols can be constructed from pqOWFs [9,28] were rooted in misconceptions.

Why MiniQCrypt. Minicrypt is one of five Impagliazzo's worlds [39] where OWFs exist, but public-key encryption schemes do not. In Cryptomania, on the other hand, public-key encryption schemes do exist.

Minicrypt is robust *and* efficient. It is robust because there is an abundance of candidates for OWFs that draw from a variety of sources of hardness, and most do not fall to quantum attacks. Two examples are (OWFs that can be constructed from) the advanced encryption standard (AES) and the secure hash standard (SHA). They are "structureless" and hence typically do not have any subexponential attacks either. In contrast, cryptomania seems fragile and, to some skeptics, even endangered due to the abundance of subexponential and quantum attacks, except for a handful of candidates. It is efficient because the operations are combinatorial in nature and amenable to very fast implementations; and the key lengths are relatively small owing to OWFs against which the best known attacks are essentially brute-force key search. We refer the reader to a survey by Barak [3] for a deeper perspective.

Consequently, much research in (applied) cryptography has been devoted to minimizing the use of public-key primitives in advanced cryptographic protocols [5,41]. However, complete elimination seems hard. In the classical world, in the absence of quantum communication, we can construct pseudorandom generators and digital signatures in Minicrypt, but not key exchange, public-key encryption, oblivious transfer or secure computation protocols. With quantum *communication* becoming a reality not just academically [23,38,55] but also commercially [45], we have the ability to reap the benefits of robustness and efficiency that Minicrypt affords us, *and* construct powerful primitives such as oblivious transfer and secure computation that were so far out of reach.

Our Results. In this paper, we finally show that the longstanding (but previously unproved) claim is true.

Theorem 1.1 (Informal). *Oblivious transfer protocols in the plain model that are simulation-secure against malicious quantum polynomial-time adversaries*

[2] This is because when using extractable commitment in a bigger protocol, the proof needs to extract the committed value and continue the execution with the adversary.

exist assuming that post-quantum one-way functions exist and that quantum communication is possible.

Our main technical contribution consists of showing a construction of an extractable commitment scheme based solely on pqOWFs and using quantum communication. Our construction involves three ingredients. The first is vanilla post-quantum commitment schemes which exist assuming that pqOWFs exist [54]. The second is post-quantum zero-knowledge protocols which also exist assuming that pqOWFs exist [64]. The third and final ingredient is a special multiparty computation protocol called conditional disclosure of secrets (CDS) constructing which in turns requires OT. This might seem circular as this whole effort was to construct an OT protocol to begin with! Our key observation is that the CDS protocol is only required to have a mild type of security, namely *unbounded simulation*, which *can* be achieved with a slight variant of the [9,19] protocol. Numerous difficulties arise in our construction, and in particular proving consistency of a protocol execution involving quantum communication appears difficult: how do we even write down an statement (e.g., NP or QMA) that encodes consistency? Overcoming these difficulties constitutes the bulk of our technical work. We provide a more detailed discussion on the technical contribution of our work in Sect. 1.1.

We remark that understanding our protocol requires only limited knowledge of quantum computation. Thanks to the composition theorems for (stand-alone) simulation-secure quantum protocols [36], much of our protocol can be viewed as a *classical* protocol in the (unbounded simulation) OT-hybrid model. The only quantumness resides in the instantiation of the OT hybrid with [9,19].

We notice that just as in [8,9,19], the honest execution of our protocols does not need strong quantum computational power, since one only needs to create, send and measure "BB84" states, which can be performed with current quantum technology.[3] Most notably, creating the states does not involve creating or maintaining long-range correlations between qubits.

In turn, plugging our OT protocol into the protocols of [24,27,42,61] (and using the sequential composition theorem [36]) gives us secure two-party computation and multi-party computation (with a dishonest majority) protocols, even for quantum channels.

Theorem 1.2 (Informal). *Assuming that post-quantum one-way functions exist and quantum communication is possible, for every classical two-party and multi-party functionality $\mathcal{F}$, there is a quantum protocol in the plain model that is simulation-secure against malicious quantum polynomial-time adversaries. Under the same assumptions, there is a quantum two-party and multi-party protocol for any quantum circuit Q.*

Finally, we note that our OT protocol runs in $\mathsf{poly}(\lambda)$ number of rounds, where λ is a security parameter, and that is only because of the zero-knowledge

[3] A BB84 state is a single-qubit state that is chosen uniformly at random from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Alternatively, it can be prepared by computing $H^h X^x |0\rangle$ where X is the bit-flip gate, H is the Hadamard gate, and $h, x \in \{0, 1\}$ are random bits.

proof. Watrous' ZK proof system [64] involves repeating a classical ZK proof (such as that graph coloring ZK proof [34] or the Hamiltonicity proof [11]) *sequentially*. A recent work of Bitansky and Shmueli [10] for the first time constructs a *constant-round* quantum ZK protocol (using only classical resources) but they rely on a strong assumption, namely (unleveled) quantum FHE and quantum hardness of LWE, which does not live in minicrypt. Nevertheless, in the common random string (CRS) model, we can instantiate the zero-knowledge protocol using a WI protocol and a Pseudo-Random Generator (PRG) with additive λ bit stretch as follows: To prove a statement x, the prover proves using the WI protocol that either x is in the language or the common random string is in the image of the PRG. To simulate a proof, the simulator samples the CRS as a random image of the PRG, and proves using the WI protocol that it belongs to the image in a straight-line. Moreover, this modification allows us to achieve *straight-line simulators*, leading to *universally-composable* (UC) security [15]. Therefore, this modification would give us the following statement.

Theorem 1.3 (Informal). *Constant-round oblivious transfer protocols in the common random string (CRS) model that are UC-simulation-secure against malicious quantum poly-time adversaries exist assuming that post-quantum one-way functions exist and that quantum communication is possible.*

Plugging the above UC-simulation-secure OT into the protocol of [42] gives constant-round multi-party computation protocols for classical computation in the common random string model that are UC-simulation-secure against malicious quantum poly-time adversaries.

Going Below MiniQCrypt? We notice that all of the primitives that we implement in our work *cannot* be implemented unconditionally, even in the quantum setting [16,48,49,53]. Basing their construction on pqOWFs seems to be the next best thing, but it does leave with the intriguing question if they could be based on weaker assumptions. More concretely, assume a world with quantum communication as we do in this paper. Does the existence of quantum OT protocols imply the existence of pqOWFs? Or, does a weaker *quantum* notion of one-way functions suffice? We leave the exploration of other possible cryptographic worlds below MiniQCrypt to future work.

Other Related Work. Inspired by the quantum OT protocol [9,19], a family of primitives, named *k-bit cut-and-choose*, has been shown to be sufficient to realize OT statistically by quantum protocols [25,29] which is provably impossible by classical protocols alone [51]. These offer further examples demonstrating the power of quantum cryptographic protocols.

There has also been extensive effort on designing quantum protocols OT and the closely related primitive of *one-time-memories* under *physical* rather than *computational* assumptions, such as the bounded-storage model, noisy-storage model, and isolated-qubit model, which restrict the quantum memory or admissible operations of the adversary [21,22,44,46,47,58]. They provide important alternatives, but the composability of these protocols are not well understood.

Meanwhile, there is strengthening on the impossibility for quantum protocols to realize secure computation statistically from scratch [14,59].

We note that there exist classical protocols for two-party and multi-party computation that are quantum-secure assuming strong assumptions such as post-quantum dense encryption and superpolynomial quantum hardness of the learning-with-errors problem [1,36,50]. And prior to the result in [24], there is a long line of work on secure multi-party *quantum* computation (Cf. [7,18,26,27]).

We remark that the idea to use OT and ZK for obtaining extractable commitment was also used (at least implicitly) in [10,36,50].

Finally, we notice that [4] have independently and concurrently proposed a quantum protocol for extractable and equivocal commitments, which can be used in the protocol of [9,19] to achieve OT (and secure multi-party computation) in MiniQCrypt. In comparison, their extractable and equivocal commitment scheme is statistically hiding, which leads to one-sided statistical security in their OT protocols. Furthermore, their commitment and OT protocols make black-box use of the underlying one-way function. Our protocols do not have these properties. On the other hand, our commitment scheme is statistically binding, and we give constant-round UC-secure protocols in the *reusable* CRS model. We also believe that our notion of verifiable CDS is of independent interest.

1.1 Technical Overview

We give an overview of our construction of post-quantum OT protocol in the plain model from post-quantum one-way functions. In this overview, we assume some familiarity with post-quantum MPC in the stand-alone, sequential composition, and UC models, and basic functionalities such as $\mathcal{F}_{\mathtt{ot}}$ and $\mathcal{F}_{\mathtt{com}}$. We will also consider *parallel versions* of them, denoted as $\mathcal{F}_{\mathtt{p\text{-}ot}}$ and $\mathcal{F}_{\mathtt{so\text{-}com}}$. The parallel OT functionality $\mathcal{F}_{\mathtt{p\text{-}ot}}$ enables the sender to send some polynomial number of pairs of strings $\{s_0^i, s_1^i\}_i$ and the receiver to choose one per pair to obtain $s_{c_i}^i$ in parallel. The commitment with selective opening functionality $\mathcal{F}_{\mathtt{so\text{-}com}}$ enables a sender to commit to a string m while hiding it, and a receiver to request opening of a subset of bits at locations $T \subseteq [|m|]$ and obtain $m_T = (m_i)_{i \in T}$. We refer the reader to Sect. 2 for formal definitions of these functionalities.

BBCS OT in the $\mathcal{F}_{\mathtt{so\text{-}com}}$-Hybrid Model. We start by describing the quantum OT protocol of [9] in the $\mathcal{F}_{\mathtt{so\text{-}com}}$ hybrid model.

BBCS OT protocol: The sender $\mathsf{ot.S}$ has strings $s_0, s_1 \in \{0,1\}^\ell$, the receiver $\mathsf{ot.R}$ has a choice bit $c \in \{0,1\}$.

1. **Preamble.** $\mathsf{ot.S}$ sends $n \gg \ell$ BB94 qubits $|x^A\rangle_{\theta^A}$ prepared using random bits $x^A \in_R \{0,1\}^n$ and random basis $\theta^A \in_R \{+,\times\}^n$.
   $\mathsf{ot.R}$ measures these qubits in randomly chosen bases $\theta^B \in_R \{+,\times\}^n$ and commits to the measured bits together with the choice of the bases, that is $\{\theta_i^B, x_i^B\}_i$, using $\mathcal{F}_{\mathtt{so\text{-}com}}$.
2. **Cut and Choose.** $\mathsf{ot.S}$ requests to open a random subset T of locations, of size say $n/2$, and gets $\{\theta_i^B, x_i^B\}_{i \in T}$ from $\mathcal{F}_{\mathtt{so\text{-}com}}$.
   Importantly, it aborts if for any i $\theta_i^B = \theta_i^A$ but $x_i^B \neq x_i^A$. Roughly speaking, this is because it's an indication that the receiver has not reported honest measurement outcomes.

3. **Partition Index Set.** ot.S reveals $\theta^A_{\bar{T}}$ for the unchecked locations $\bar{T}$. ot.R partitions $\bar{T}$ into a subset of locations where it measured in the same bases as the sender $I_c := \{i \in \bar{T} : \theta^A_i = \theta^B_i\}$ and the rest $I_{1-c} := \bar{T} - I_c$, and sends (I_0, I_1) to the sender.
4. **Secret Transferring**. ot.S hides the two strings s_i for $i = 0, 1$ using randomness extracted from $x^A_{I_i}$ via a universal hash function f and sends $m_i := s_i \oplus f(x^A_{I_i})$, from which ot.R recovers $s := m_c \oplus f(x^B_{I_c})$.

Correctness follows from that for every $i \in I_c$, $\theta^A_i = \theta^B_i$ and $x^A_{I_c} = x^B_{I_c}$, hence the receiver decodes s_c correctly.

The security of the BBCS OT protocol relies crucially on two important properties of the $\mathcal{F}_{\texttt{so-com}}$ commitments, namely extractability and equivocability, which any protocol implementing the $\mathcal{F}_{\texttt{so-com}}$ functionality must satisfy.

Equivocability: To show the receiver's privacy, we need to efficiently simulate the execution with a malicious sender ot.S* without knowing the choice bit c and extract both sender's strings s_0, s_1. To do so, the simulator ot.SimS would like to measure at these unchecked locations $\bar{T}$ using exactly the same bases $\theta^A_{\bar{T}}$ as ot.S* sends in Step 3. In an honest execution, this is impossible as the receiver must commit to its bases θ^B and pass the checking step. However, in simulation, this can be done by invoking the equivocability of $\mathcal{F}_{\texttt{so-com}}$. In particular, ot.SimS can *simulate* the receiver's commitments in the preamble phase without committing to any value. When it is challenged to open locations at T, it measures qubits at T in random bases, and *equivocates* commitments at T to the measured outcomes and bases. Only after ot.S* reveals its bases $\theta^A_{\bar{T}}$ for the unchecked locations, does ot.SimS measure qubits at $\bar{T}$ in exactly these bases. This ensures that it learns both $x^A_{I_0}$ and $x^A_{I_1}$ and hence can recover both s_0 and s_1.

Extractability: To show the sender's privacy, we need to efficiently extract the choice bit c from a malicious receiver ot.R* and simulate the sender's messages using only s_c. To do so, the simulator ot.SimR needs to extract efficiently from the $\mathcal{F}_{\texttt{so-com}}$ commitments all the bases θ^B, so that, later given I_0, I_1 it can figure out which subset I_c contains more locations i where the bases match $\theta^B_i = \theta^A_i$, and use the index of that set as the extracted choice bit. Observe that it is important that extraction does not "disturb" the quantum state of ot.R* at all, so that ot.SimR can continue simulation with ot.R*. This is easily achieved using $\mathcal{F}_{\texttt{so-com}}$ as extraction is done in a straight-line fashion, but challenging to achieve in the plain model as rewinding a quantum adversary is tricky. Indeed, the argument of knowledge protocol of [62] can extract a witness but disturbs the state of the quantum adversary due to measurement. Such strong extractable commitment is only known in the plain model under stronger assumptions [2,10,36] or assuming public key encryption in the CRS model.

It turns out that equivocability *can* be achieved using zero-knowledge protocols, which gives a post-quantum OT protocol with an inefficient simulator ot.SimR against malicious receivers (and efficient ot.SimS). Our main technical contribution lies in achieving efficient extractability while assuming only post-quantum one-way functions. In particular, we will use the OT with unbounded simulation as a tool for this. We proceed to describing these steps in more detail.

Achieving Equivocability Using Zero-Knowledge. The idea is to let the committer commit $c = \mathtt{com}(\mu; \rho)$ to a string $\mu \in \{0,1\}^n$ using any statistically binding computationally hiding commitment scheme $\mathtt{com}$ whose decommitment can be verified classically, for instance, Naor's commitment scheme [54] from post-quantum one-way functions. For now in this overview, think of $\mathtt{com}$ as non-interactive. (Jumping ahead, later we will also instantiate this commitment with a multi-round extractable commitment scheme that we construct.)

Any computationally hiding commitment can be simulated by simply committing to zero, $\widetilde{c} = \mathtt{com}(0; \rho)$. The question is how to equivocate $\widetilde{c}$ to any string μ' later in the decommitment phase. With a post-quantum ZK protocol, instead of asking the committer to reveal its randomness ρ which would statistically bind $\widetilde{c}$ to the zero string, we can ask the committer to send μ' and give a zero-knowledge proof that $\widetilde{c}$ indeed commits to μ'. As such, the simulator can cheat and successfully open to any value μ' by simulating the zero-knowledge argument to the receiver.

Equivocable Commitment: The sender $\mathsf{com.S}$ has a string $\mu \in \{0,1\}^n$, the receiver $\mathsf{com.R}$ has a subset $T \subseteq [n]$.

1. **Commit Phase.** $\mathsf{com.S}$ commits to μ using a statistically binding commitment scheme $\mathtt{com}$ using randomness ρ. Let c be the produced commitment.
   NOTE: *Simulation against malicious receivers commits to* 0^n. *Simulation against malicious senders is inefficient to extract* μ *by brute force.*
2. **Decommit Phase.** Upon $\mathsf{com.R}$ requesting to open a subset T of locations, $\mathsf{com.S}$ sends μ' and gives a single zero knowledge argument that c commits to μ such that $\mu' = \mu_T$.
   NOTE: *To equivocate to* $\mu' \neq \mu_T$, *the simulator sends* μ' *and simulates the zero-knowledge argument (of the false statement).*

The above commitment protocol implements $\mathcal{F}_{\mathtt{so\text{-}com}}$ with efficient simulation against malicious receivers, but inefficient simulation against malicious senders. Plugging it into BBCS OT protocol, we obtain the following corollary:

Corollary 1.1 (Informal). *Assume post-quantum one-way functions. In the plain model, there is:*

- *a protocol that securely implements the OT functionality* $\mathcal{F}_{ot}$, *and*
- *a protocol that securely implements the parallel OT functionality* $\mathcal{F}_{p\text{-}ot}$,

in the sequential composition setting, and with efficient simulation against malicious senders but inefficient simulation against malicious receivers.

The second bullet requires some additional steps, as parallel composition does not automatically apply in the stand-alone (as opposed to UC) setting (e.g., the ZK protocol of [64] is not simulatable in parallel due to rewinding). Instead, we first observe that the BBCS OT UC-implements $\mathcal{F}_{\mathtt{ot}}$ in the $\mathcal{F}_{\mathtt{so\text{-}com}}$ hybrid model, and hence parallel invocation of BBCS OT UC-implements $\mathcal{F}_{\mathtt{p\text{-}ot}}$ in the $\mathcal{F}_{\mathtt{so\text{-}com}}$ hybrid model. Note that parallel invocation of BBCS OT invokes $\mathcal{F}_{\mathtt{so\text{-}com}}$ in parallel, which in fact can be merged into a single invocation to $\mathcal{F}_{\mathtt{so\text{-}com}}$. Therefore, plugging in the above commitment protocol gives an OT protocol that

implements $\mathcal{F}_{\texttt{p-ot}}$. In particular, digging deeper into the protocol, this ensures that we are invoking a *single* ZK protocol for all the parallel copies of the parallel OT, binding the executions together.

Achieving Extractability Using OT with Unbounded Simulation. Interestingly, we show that OT with (even 2-sided) unbounded simulation plus zero-knowledge is sufficient for constructing extractable commitments, which when combined with zero-knowlege again as above gives an implementation of $\mathcal{F}_{\texttt{so-com}}$ in the sequential composition setting in the plain model.

The initial idea is to convert the power of simulation into the power of extraction via two-party computation, and sketched below.

Initial Idea for Extractable Commitment: The sender $\mathsf{com.S}$ has $\mu \in \{0,1\}^n$.

1. **Trapdoor setup:** The receiver $\mathsf{com.R}$ sends a commitment c of a statistically binding commitment scheme $\texttt{com}$, and gives a zero-knowledge proof that c commits to 0.
2. **Conditional Disclosure of Secret (CDS):** $\mathsf{com.S}$ and $\mathsf{com.R}$ run a two-party computation protocol implementing the CDS functionality $\mathcal{F}_{\mathsf{cds}}$ for the language $\mathcal{L}_{\texttt{com}} = \{(c', b') : \exists r' \text{ s.t. } c' = \texttt{com}(b'; r')\}$, where the CDS functionality $\mathcal{F}_{\mathsf{cds}}$ for $\mathcal{L}_{\texttt{com}}$ is defined as below:

   $\mathcal{F}_{\mathsf{cds}}$: Sender input (x, μ), Receiver input w

   $$\text{Sender has no output, Receiver outputs } x \text{ and } \mu' = \begin{cases} \mu & \text{if } \mathcal{R}_{\mathcal{L}_{\texttt{com}}}(x, w) = 1 \\ \perp & \text{otherwise} \end{cases}$$

   $\mathsf{com.S}$ acts as the CDS sender using input $(x = (c, 1), \mu)$ while $\mathsf{com.R}$ acts as the CDS receiver using witness $w = 0$.

It may seem paradoxical that we try to implement commitments using the much more powerful tool of two-party computation. The *key observation* is that the hiding and extractability of the above commitment protocol only relies on the *input-indistinguishability property* of the CDS protocol, which is *implied by unbounded simulation.*

- *Hiding:* A commitment to μ can be simulated by simply commiting to 0^n honestly, that is, using $(x = (c, 1), 0^n)$ as the input to the CDS. The simulation is indistinguishable as the soundness of ZK argument guarantees that c must be a commitment to 0 and hence the CDS statement $(c, 1)$ is false and should always produce $\mu' = \perp$. Therefore, the unbounded-simulation security of the CDS protocol implies that it is indistinguishable to switch the sender's input from μ to 0^n.
- *Extraction:* To efficiently extract from a malicious sender $\mathsf{com.S}^*$, the idea (which however suffers from a problem described below) is to let the simulator-extractor $\mathsf{com.SimS}$ set up a trapdoor by committing to 1 (instead of 0) and simulate the ZK argument; it can then use the decommitment (call it r) to 1 as a valid witness to obtain the committed value from the output of the CDS protocol. Here, the unbounded-simulation security of CDS again implies that

interaction with an honest receiver who uses $w = 0$ is indistinguishable from that with $\mathsf{com.SimS}$ who uses $w = r$ as $\mathsf{com.S}^*$ receives no output via CDS.

The advantage of CDS with unbounded simulation is that it can be implemented using OT with unbounded simulation: Following the work of [42,43,61], post-quantum MPC protocols exist in the $\mathcal{F}_{\mathtt{ot}}$-hybrid model, and instantiating them with the unbounded-simulation OT yields unbounded simulation MPC and therefore CDS.

NP-Verifiability and the Lack of It. Unfortunately, the above attempt has several problems: how do we show that the commitment is binding? how to decommit? and how to guarantee that the extracted value agrees with the value that can be decommitted to? We can achieve binding by having the sender additionally commit to μ using a statistically binding commitment scheme $\mathtt{com}$, and send the corresponding decommitment in the decommitment phase. However, to guarantee that the extractor would extract the same string μ from CDS, we need a way to verify that the same μ is indeed used by the CDS sender. Towards this, we formalize a verifiability property of a CDS protocol:

A CDS protocol is verifiable if

- The honest CDS sender $\mathsf{cds.S}$ additionally outputs (x, μ) and a "proof" π (on a special output tape) at the end of the execution.
- There is an efficient *classical* verification algorithm $\mathsf{Ver}(\tau, x, \mu, \pi)$ that verifies the proof, w.r.t. the transcript τ of the *classical* messages exchanged in the CDS protocol.
- *Binding:* No malicious sender $\mathsf{cds.S}^*$ after interacting with an honest receiver $\overline{\mathsf{cds.R}(w)}$ can output (x, μ, π), such that the following holds simultaneously: (a) $\mathsf{Ver}(\tau, x, \mu, \pi) = 1$, (b) $\mathsf{cds.R}$ did not abort, and (c) $\mathsf{cds.R}$ outputs μ' inconsistent with the inputs (x, μ) and w, that is, $\mu' \neq \begin{cases} \mu & \text{if } \mathcal{R}_{\mathcal{L}}(x, w) = 1 \\ \perp & \text{otherwise} \end{cases}$

We observe first that classical protocols with perfect correctness have verifiability for free: The proof π is simply the sender's random coins r, and the verification checks if the honest sender algorithm with input (x, μ) and random coins r produces the same messages as in the transcript τ. If so, perfect correctness guarantees that the output of the receiver must be consistent with x, μ. However, verifiability cannot be taken for granted in the $\mathcal{F}_{\mathtt{ot}}$ hybrid model or in the quantum setting. In the $\mathcal{F}_{\mathtt{ot}}$ hybrid model, it is difficult to write down an NP-statement that captures consistency as the OT input is *not* contained in the protocol transcript and is unconstrained by it. In the quantum setting, protocols use quantum communication, and consistency cannot be expressed as an NP-statement. Take the BBCS protocol as an example, the OT receiver receives from the sender ℓ qubits and measures them locally; there is no way to "verify" this step in NP.

Implementing Verifiable CDS. To overcome the above challenge, we implement a verifiable CDS protocol in the $\mathcal{F}_{\mathtt{p\text{-}ot}}$ hybrid model assuming only post-quantum one-way functions. We develop this protocol in a few steps below.

Let's start by understanding why the standard two-party comptuation protocol is not verifiable. The protocol proceeds as follows: First, the sender $\mathsf{cds.S}$ locally garbles a circuit computing the following function into $\widehat{G}$ with labels $\{\ell_b^j\}_{j\in[m],b\in\{0,1\}}$ where $m = |w|$:

$$G_{x,\mu}(w) = \mu' = \begin{cases} \mu & \text{if } \mathcal{R}_{\mathcal{L}}(x,w) = 1 \\ \perp & \text{otherwise} \end{cases} \tag{1}$$

Second, $\mathsf{cds.S}$ sends the pairs of labels $\{\ell_0^j, \ell_1^j\}_j$ via $\mathcal{F}_{\mathtt{p\text{-}ot}}$. The receiver $\mathsf{cds.R}$ on the other hand chooses $\{w_j\}_j$ to obtain $\{\widetilde{\ell}_{w_j}^j\}_j$, and evaluates $\widehat{G}$ with these labels to obtain μ'. This protocol is not NP-verifiable because consistency between the labels of the garbled circuit and the sender's inputs to $\mathcal{F}_{\mathtt{p\text{-}ot}}$ cannot be expressed as a NP statement.

To fix the problem, we devise a way for the receiver to verify the OT sender's strings. Let $\mathsf{cds.S}$ additionally commit to all the labels $\{c_b^j = \mathtt{com}(\ell_b^j; r_b^j)\}_{j,b}$ and the message $c = \mathtt{com}(\mu; r)$ and prove in ZK that $\widehat{G}$ is consistent with the labels and message committed in the commitments, as well as the statement x. Moreover, the sender sends both the labels and decommitments $\{(\ell_0^j, r_0^j), (\ell_1^j, r_1^j)\}_j$ via $\mathcal{F}_{\mathtt{p\text{-}ot}}$. The receiver after receiving $\{\widetilde{\ell}_{w_j}^j, \widetilde{r}_{w_j}^j\}_j$ can now verify their correctness by verifying the decommitment w.r.t. $c_{w_j}^j$, and aborts if verification fails. This gives the following new protocol:

A Verifiable but Insecure CDS Protocol: The sender $\mathsf{cds.S}$ has (x, μ) and the receiver $\mathsf{cds.R}$ has w.

1. **Sender's Local Preparation:** $\mathsf{cds.S}$ generate a garbled circuits $\widehat{G}$ for the circuit computing $G_{x,\mu}$ (Equation (1)), with labels $\{\ell_b^{i,j}\}_{j,b}$. Moreover, it generates commitments $c = \mathtt{com}(\mu, r)$ and $c_b^j = \mathtt{com}(\ell_b^j; r_b^j)$ for every j, b.
2. **OT:** $\mathsf{cds.S}$ and $\mathsf{cds.R}$ invoke $\mathcal{F}_{\mathtt{p\text{-}ot}}$. For every j, the sender sends $(\ell_0^j, r_0^j), (\ell_1^j, r_1^j)$, and the receiver chooses w_j and obtains $(\widetilde{\ell}_{w_j}^j, \widetilde{r}_{w_j}^j)$.
3. **Send Garbled Circuit and Commitments:** $\mathsf{cds.S}$ sends $\widehat{G}$, c, and $\{c_b^j\}_{j,b}$ and proves via a ZK protocol that they are all generated consistently w.r.t. each other and x.
4. **Receiver's Checks:** $\mathsf{cds.R}$ aborts if ZK is not accepting, or if for some j, $c_{w_j}^j \neq \mathtt{com}(\widetilde{\ell}_{w_j}^j, \widetilde{r}_{w_j}^j)$. Otherwise, it evaluates $\widehat{G}$ with the labels and obtain $\mu' = G_{x,\mu}(w)$.

We argue that this protocol is NP-verifiable. The sender's proof is simply the decommitment r of c, and $\mathsf{Ver}(\tau, (x, \mu), r) = 1$ iff r is a valid decommitment to μ of the commitment c contained in the transcript τ. To show the binding property, consider an interaction between a cheating sender $\mathsf{cds.S}^*$ and $\mathsf{cds.R}(w)$. Suppose $\mathsf{cds.R}$ does not abort, it means that 1) the ZK argument is accepting and hence $\widehat{G}$ must be consistent with $x, \{c_b^j\}, c$, and 2) the receiver obtains the labels committed in $c_{w_j}^j$'s. Therefore, evaluating the garbled circuit with these labels must produce $\mu' = G_{x,\mu}(w)$ for the μ committed to in c.

Unfortunately, the checks that the receiver performs render the protocol insecure. A malicious sender $\mathsf{com.S}^*$ can launch the so-called selective abort attack

to learn information of w. For instance, to test if $w_1 = 0$ or not, it replaces ℓ_0^1 with zeros. If $w_1 = 0$ the honest receiver would abort; otherwise, it proceeds normally.

The Final Protocol. To circumvent the selective abort attack, we need a way to check the validity of sender's strings that is independent of w. Our idea is to use a variant of cut-and-choose. Let $\mathsf{cds.S}$ create 2λ copies of garbled circuits and commitments to their labels, $\{\widehat{G}^i\}_{i\in[2\lambda]}$ and $\{c_b^{i,j} = \mathtt{com}(\ell_b^{i,j}; r_b^{i,j})\}_{i,j,b}$ and prove via a ZK protocol that they are all correctly generated w.r.t. the same c and x. Again, $\mathsf{cds.S}$ sends the labels and decommitment via $\mathcal{F}_{\mathtt{p\text{-}ot}}$, but $\mathsf{cds.R}$ does not choose w universally in all copies. Instead, it secretly samples a random subset $\Lambda \in [2\lambda]$ by including each i with probability $1/2$; for copy $i \in \Lambda$, it chooses random string $s^i \leftarrow \{0,1\}^m$ and obtains $\{\widetilde{\ell}_{s_j^i}^{i,j}, \widetilde{r}_{s_j^i}^{i,j}\}_j$, whereas for copy $i \notin \Lambda$, it choose w and obtains $\{\widetilde{\ell}_{w_j}^{i,j}, \widetilde{r}_{w_j}^{i,j}\}_j$. Now, in the checking step, $\mathsf{cds.R}$ only verifies the validity of $\{\widetilde{\ell}_{s_j^i}^{i,j}, \widetilde{r}_{s_j^i}^{i,j}\}_{i\in\Lambda,j}$ received in copies in Λ. Since the check is now completely independent of w, it circumvents the selective abort attack.

Furthermore, NP-verifiability still holds. The key point is that if the decommitments $\mathsf{cds.R}$ receives in copies in Λ are all valid, with overwhelming probability, the number of *bad copies* where the OT sender's strings are not completely valid is bounded by $\lambda/4$. Hence, there must exist a copy $i \notin \Lambda$ where $\mathsf{cds.R}$ receives the right labels $\ell_{w_j}^{i,j}$ committed to in $c_{w_j}^{i,j}$. $\mathsf{cds.R}$ can then evaluate $\widehat{G}^i$ to obtain μ'. By the same argument as above, μ' must be consistent with the (x, μ) and w, for μ committed in c, and NP-verifiability follows. The final protocol is described in Fig. 3.

Organization of the Paper. We review the quantum stand-alone security model introduced by [36] in Sect. 2. In section Sect. 3, we construct a quantum parallel-OT protocol with one-sided, unbounded simulation. In more detail, we review in Sect. 3.1 the quantum OT protocol from [9] based on ideal commitments with selective opening security. Then in Sect. 3.2, we show how to boost it to construct a *parallel* OT protocol from the same assumptions. And finally, we provide a classical implementation of the commitment scheme with selective opening security in Sect. 3.3 which gives us ideal/real security except with unbounded receiver simulation. This result will be fed into our main technical contribution in Sect. 4 where we show how to construct extractable commitments from unbounded-simulation parallel-OT. In Sect. 4.2, we show how to construct (the intermediate primitive of) CDS from parallel-OT and one-way functions, and then in Sect. 4.3 we construct extractable commitments from CDS. Finally, in Sect. 5 we lift our results to achieve quantum protocols for multi-party (quantum) computation from one-way functions.

2 Quantum Stand-Alone Security Model

We adopt the quantum stand-alone security model from the work of Hallgren, Smith and Song [36], tailored to the two-party setting.

Let $\mathcal{F}$ denote a *functionality*, which is a classical interactive machine specifying the instructions to realize a cryptographic task. A two-party protocol Π consists of a pair of quantum interactive machines (A, B). We call a protocol *efficient* if A and B are both quantum poly-time machines. If we want to emphasize that a protocol is classical, i.e., all computation and all messages exchanged are classical, we then use lower-case letters (e.g., π). Finally, an adversary $\mathcal{A}$ is another quantum interactive machine that intends to attack a protocol.

When a protocol $\Pi = (A, B)$ is executed under the presence of an adversary $\mathcal{A}$, the state registers are initialized by a security parameter 1^λ and a joint quantum state σ_λ. Adversary $\mathcal{A}$ gets activated first, and may either **deliver** a message, i.e., instructing some party to read the proper segment of the network register, or **corrupt** a party. We assume all registers are authenticated so that $\mathcal{A}$ cannot modify them, but otherwise $\mathcal{A}$ can schedule the messages to be delivered in any arbitrary way. If $\mathcal{A}$ corrupts a party, the party passes all of its internal state to $\mathcal{A}$ and follows the instructions of $\mathcal{A}$. Any other party, once receiving a message from $\mathcal{A}$, gets activated and runs its machine. At the end of one round, some message is generated on the network register. Adversary $\mathcal{A}$ is activated again and controls message delivery. At some round, the party generates some output and terminates.

We view Π and $\mathcal{A}$ as a whole and model the composed system as another QIM, call it $M_{\Pi,\mathcal{A}}$. Then executing Π in the presence of $\mathcal{A}$ is just running $M_{\Pi,\mathcal{A}}$ on some input state, which may be entangled with a reference system available to a distighuisher.

Protocol emulation and secure realization of a functionality. A secure protocol is supposed to "emulate" an idealized protocol. Consider two protocols Π and Γ, and let $M_{\Pi,\mathcal{A}}$ be the composed machine of Π and an adversary $\mathcal{A}$, and $M_{\Gamma,\mathcal{S}}$ be that of Γ and another adversary $\mathcal{S}$. Informally, Π emulates Γ if the two machines $M_{\Pi,\mathcal{A}}$ and $M_{\Gamma,\mathcal{S}}$ are indistinguishable.

It is of particular interest to emulate an *ideal-world* protocol $\widetilde{\Pi}_{\mathcal{F}}$ for a functionality $\mathcal{F}$ which captures the security properties we desire. In this protocol, two (dummy) parties $\widetilde{A}$ and $\widetilde{B}$ have access to an additional "trusted" party that implements $\mathcal{F}$. We abuse notation and call the trusted party $\mathcal{F}$ too. Basically $\widetilde{A}$ and $\widetilde{B}$ invoke $\mathcal{F}$ with their inputs, and then $\mathcal{F}$ runs on the inputs and sends the respective outputs back to $\widetilde{A}$ and $\widetilde{B}$. An execution of $\widetilde{\Pi}$ with an adversary $\mathcal{S}$ is as before, except that $\mathcal{F}$ cannot be corrupted. We denote the composed machine of $\mathcal{F}$ and $\widetilde{\Pi}_{\mathcal{F}}$ as $M_{\mathcal{F},\mathcal{S}}$.

Definition 2.1 (Computationally Quantum-Stand-Alone Emulation). *Let Π and Γ be two poly-time protocols. We say Π* computationally quantum-stand-alone *(`C-QSA`) emulates Γ, if for any poly-time QIM $\mathcal{A}$ there exists a poly-time QIM $\mathcal{S}$ such that $M_{\Pi,\mathcal{A}} \approx_{qc} M_{\Gamma,\mathcal{S}}$.*

Definition 2.2 (`C-QSA` Realization of a Functionality). *Let $\mathcal{F}$ be a poly-time two-party functionality and Π be a poly-time two-party protocol. We say Π* computationally quantum-stand-alone *realizes $\mathcal{F}$, if Π `C-QSA` emulates $\widetilde{\Pi}_{\mathcal{F}}$.*

Namely, for any poly-time $\mathcal{A}$, there is a poly-time $\mathcal{S}$ such that $M_{\Pi,\mathcal{A}} \approx_{qc} M_{\mathcal{F},\mathcal{S}}$.

Definition 2.3 (Statistically Quantum-Stand-Alone Emulation). *Let Π and Γ be two poly-time protocols. We say Π* statistically quantum-stand-alone *(*`S-QSA`*) emulates Γ, if for any QIM $\mathcal{A}$ there exists an QIM $\mathcal{S}$ that runs in poly-time of that of $\mathcal{A}$, such that $M_{\Pi,\mathcal{A}} \approx_{\diamond} M_{\Gamma,\mathcal{S}}$.*

We assume *static* corruption only in this work, where the identities of corrupted parties are determined before protocol starts. The definitions above consider computationally bounded (poly-time) adversaries, including simulators. Occasionally, we will work with *inefficient* simulators, which we formulate as unbounded simulation of corrupted party P.

Definition 2.4 (Unbounded Simulation of Corrupted P). *Let Π and Γ be two poly-time protocols. For any poly-time QIM $\mathcal{A}$ corrupting party P, we say that Π* `C-QSA`*-emulates Γ against corrupted P with unbounded simulation, if there exists a QIM $\mathcal{S}$ possibly unbounded such that $M_{\Pi,\mathcal{A}} \approx_{qc} M_{\Gamma,\mathcal{S}}$.*

2.1 Modular Composition Theorem

It's shown that protocols satisfying the definitions of stand-alone emulation admit a modular composition [36]. Specifically, let Π be a protocol that uses another protocol Γ as a subroutine, and let Γ' be a protocol that QSA emulates Γ. We define the *composed* protocol, denoted $\Pi^{\Gamma/\Gamma'}$, to be the protocol in which each invocation of Γ is replaced by an invocation of Γ'. We allow multiple calls to a subroutine and also using multiple subroutines in a protocol Π. **However, quite importantly, we require that at any point, only one subroutine call be in progress**. This is more restrictive than the "network" setting, where many instances and subroutines may be executed *concurrently*.

In a *hybrid* model, parties can make calls to an ideal-world protocol $\widetilde{\Pi}_{\mathcal{G}}$ of some functionality $\mathcal{G}$[4]. We call such a protocol a $\mathcal{G}$*-hybrid* protocol, and denote it $\Pi^{\mathcal{G}}$. The execution of a hybrid-protocol in the presence of an adversary $\mathcal{A}$ proceeds in the usual way. Assume that we have a protocol Γ that realizes $\mathcal{G}$ and we have designed a $\mathcal{G}$-hybrid protocol $\Pi^{\mathcal{G}}$ realizing another functionality $\mathcal{F}$. Then the composition theorem allows us to treat sub-protocols as equivalent to their ideal versions.

If the secure emulation involves unbounded simulation against a party, the proof in [36] can be extended to show that the composed protocol also emulates with unbounded simulation against the corresponding corrupted party.

Theorem 2.1 (Modular Composition). *All of the following holds.*

- *Let Π, Γ and Γ' be two-party protocols such that Γ'* `C-QSA`*-emulates Γ, then $\Pi^{\Gamma/\Gamma'}$* `C-QSA` *emulates Π. If Γ'* `C-QSA` *emulates Γ against corrupted P with unbounded simulation, then $\Pi^{\Gamma/\Gamma'}$* `C-QSA` *emulates against corrupted P with unbounded simulation.*

[4] In contrast, we call it the *plain model* if no such trusted set-ups are available.

– *Let $\mathcal{F}$ and $\mathcal{G}$ be poly-time functionalities. Let $\Pi^{\mathcal{G}}$ be a $\mathcal{G}$-hybrid protocol that* C-QSA *realizes $\mathcal{F}$, and Γ be a protocol that* C-QSA *realizes $\mathcal{G}$, then $\Pi^{\mathcal{G}/\Gamma}$* C-QSA *realizes $\mathcal{F}$. If Γ* C-QSA *realizes $\mathcal{G}$ against corrupted P with unbounded simulation then $\Pi^{\mathcal{G}/\Gamma}$* C-QSA *realizes $\mathcal{F}$ against corrupted P with unbounded simulation.*

3 Parallel OT with Unbounded Simulation from OWF

The goal of this section is to prove the following theorem.

Theorem 3.1. *Assuming the existence of pqOWF, there exists a protocol $\Pi_{p\text{-}ot}$ that* C-QSA*-emulates $\mathcal{F}_{p\text{-}ot}$ with unbounded simulation against a malicious receiver.*

We prove this theorem as follows. In Sect. 3.1, we review the protocol of [9] that implies stand-alone-secure OT in $\mathcal{F}_{\text{so-com}}$-hybrid model. Then, in Sect. 3.2, we show how to build $\mathcal{F}_{\text{p-ot}}$ from $\mathcal{F}_{\text{so-com}}$. Finally in Sect. 3.3, we construct $\mathcal{F}_{\text{so-com}}$ with unbounded simulation against malicious sender.

3.1 Stand-Alone-Secure OT in $\mathcal{F}_{\text{so-com}}$-hybrid Model

In this section we present the quantum OT protocol assuming a selective opening-secure commitment scheme, that is, in the $\mathcal{F}_{\text{so-com}}$ hybrid model. We would like to stress that the results in this section are not novel; they consist of a straightforward adaptation of previous results [9,20,61] to our setting/language, and our goal in this presentation is to to provide a self-contained proof of its security. We describe the protocol Π_{QOT} in Sect. 1.1 and we have the following.

Theorem 3.2. *Π_{QOT}* C-QSA*-realizes $\mathcal{F}_{ot}$ in the $\mathcal{F}_{so\text{-}com}$ hybrid model.*

3.2 Parallel Repetition for Protocols with Straight-Line Simulation

We show now that if π implements $\mathcal{F}$ in the $\mathcal{G}$-hybrid model with an (efficient/unbounded) *straight-line* simulator, then a parallel repetition of π, denoted $\pi^{||}$ implements $\mathcal{F}^{||}$ in the $\mathcal{G}^{||}$-hybrid model with an (efficient/unbounded) simulator. As a corollary, we get that a parallel repetition of the $\mathcal{F}_{ot}$ protocol from the previous section is a secure implementation of parallel OT in the $\mathcal{F}_{\text{so-com}}$ hybrid model.

Theorem 3.3 (Parallel Repetition). *Let $\mathcal{F}$ and $\mathcal{G}$ be two-party functionalities and let π be a secure implementation of $\mathcal{F}$ in the $\mathcal{G}$-hybrid model with a* straight-line *simulator. Then, $\pi^{||}$ is a secure implementation of $\mathcal{F}^{||}$ in the $\mathcal{G}^{||}$-hybrid model with straight-line simulation as well.*

Corollary 3.1. *The parallel repetition of any protocol that* C-QSA*-realizes $\mathcal{F}_{ot}$ in the $\mathcal{F}_{so\text{-}com}$-hybrid model with a straight-line simulator achieves $\mathcal{F}_{p\text{-}ot}$ in the $\mathcal{F}_{so\text{-}com}$-hybrid model.*

3.3 Implementing $\mathcal{F}_{\texttt{so-com}}$ with Unbounded Simulation

In this section we provide an implementation of $\mathcal{F}_{\texttt{so-com}}$ from Naor's commitment scheme and ZK protocols. Our protocol $\Pi_{\texttt{so-com}}$ is described in Fig. 1 and we prove the following result.

Theorem 3.4. *Assuming the existence of pqOWF, $\Pi_{\texttt{so-com}}$ C-QSA-realizes $\mathcal{F}_{\texttt{so-com}}$. with unbounded simulation against malicious committer.*

We prove Theorem 3.4 by showing security against malicious committer with unbounded simulator in Lemma 3.1 and security against malicious receiver in Lemma 3.2.

Parties: The committer C and the receiver R.
Inputs: C gets k ℓ-bit strings $m_1,...m_k$ and R gets a subset $I \subseteq [k]$ of messages to be decommited

Commitment Phase

1. R sends ρ for Naor's commitment scheme
2. For $i \in [k]$, C generates the commitments $c_i = \texttt{com}_\rho(m_i, r_i)$, where r_i is some private randomness.
3. C sends $c_1, ..., c_k$ to R

Decommitment Phase

1. R sends I to C
2. C sends $(m_i)_{i\in I}$ to R and they run a ZK protocol to prove that there exists $\left((\widetilde{m}_i)_{i\notin I}, (r_i)_{i\in[k]}\right)$ such that $c_i = \texttt{com}_\rho(\widetilde{m}_i, r_i)$

Fig. 1. Protocol for selective-opening commitment scheme $\Pi_{\texttt{so-com}}$.

Lemma 3.1. *Assuming the existence of pqOWF, $\Pi_{\texttt{so-com}}$ C-QSA-emulates $\mathcal{F}_{\texttt{so-com}}$ against corrupted committer $\mathcal{A}$ with unbounded simulation.*

Proof. The unbounded simulator $\mathcal{S}$ works as follows:

1. In the commitment phase, $\mathcal{S}$ runs the honest protocol with $\mathcal{A}$ and when receives the commitments $\widehat{c}_1, ..., \widehat{c}_k$ from $\mathcal{A}$ and $\mathcal{S}$ finds the messages $\widehat{m}_1, ..., \widehat{m}_k$ by brute force. If there is a $\widehat{c}_i$ that does not decommit to any message or decommits to more than one message $\mathcal{S}$ aborts. Finally, $\mathcal{S}$ inputs $\widehat{m}_1, ..., \widehat{m}_k$ to $\mathcal{F}_{\texttt{so-com}}$
2. In the Decommitment phase, $\mathcal{S}$ receives I from $\mathcal{F}_{\texttt{so-com}}$, forwards it to $\mathcal{A}$. $\mathcal{S}$ receives $(\widetilde{m}_i)_{i\in I}$ from $\mathcal{A}$ runs the honest verifier in the ZK protocol with $\mathcal{A}$, and rejects iff the ZK rejects or if for any $i \in I$, $\widehat{m}_i \neq \widetilde{m}_i$.

The proof follows the statistically-binding property of Naor's commitment scheme, so we can ignore commitments that open to more than one message, and by the ZK soundness property, which ensures that, up to negligible probability, if the commitments are not well-formed or if the sender tries to open then to a different value, both the simulator and the original receiver abort.

Due to space restrictions, we leave the details to the full version of our paper.

We now show security against malicious receiver.

Lemma 3.2. *Assuming the existence of pqOWF,* $\Pi_{\texttt{so-com}}$ $\texttt{C-QSA}$*-realizes* $\mathcal{F}_{\texttt{so-com}}$ *against corrupted receiver* $\mathcal{A}$*.*

Proof. The simulator $\mathcal{S}$ works as follows:

1. In the commitment phase, $\mathcal{S}$ sends $c_i = \texttt{com}_\rho(0, r_i)$ to $\mathcal{A}$
2. In the decommitment phase, $\mathcal{S}$ receives I from $\mathcal{A}$, uses it as input of $\mathcal{F}_{\texttt{so-com}}$. $\mathcal{S}$ receives back the messages $(m_i)_{i\in I}$, sends them to $\mathcal{A}$ and runs the ZK simulator of the proof that $(c_i)_{i\in I}$ open to $(m_i)_{i\in I}$ and that $(c_i)_{i\notin I}$ are valid commitments.

The fact that $M_{\Pi_{\texttt{so-com}},\mathcal{A}} \approx_{qc} M_{\mathcal{F}_{\texttt{so-com}},\mathcal{S}}$ follows from the computational zero-knowledge of the protocol and the computatinally-hiding property of Naor's commitment scheme.

4 Extractable Commitment from Unbounded Simulation OT

In this section, we construct an extractable commitment scheme using the unbounded simulation OT from Sect. 3. We do this in two steps. First, we define a new primitive, namely *verifiable* conditional disclosure of secrets (vCDS) in Sect. 4.1, and we construct a (unbounded simulation) vCDS protocol in Sect. 4.2 from the unbounded simulation OT. We then show how to use vCDS to construct an extractable commitment protocol that implements $\mathcal{F}_{\texttt{so-com}}$ with efficient simulators in Sect. 4.3.

4.1 Verifiable Conditional Disclosure of Secrets (vCDS)

We define the primitive of (verifiable) conditional disclosure of secrets. Conditional disclosure of secrets [31] (CDS) for an NP-language $\mathcal{L}$ is a two-party protocol where a sender (denoted $\mathsf{cds.S}$) and a receiver (denoted $\mathsf{cds.R}$) have a common input x, the sender has a message μ, and the receiver (purportedly) has a witness w for the NP-relation $R_{\mathcal{L}}$. At the end of the protocol, $\mathsf{cds.R}$ gets μ if $R_{\mathcal{L}}(x, w) = 1$ and $\perp$ otherwise, and the sender gets nothing. In a sense, this can be viewed as a *conditional* version of oblivious transfer, or as an interactive version of witness encryption.

The CDS functionality is defined in Fig. 2. We will construct a protocol $\Pi = \langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ that securely realizes the CDS functionality in the quantum

The Conditional Disclosure of Secret (CDS) Functionality $\mathcal{F}_{CDS}$ for an NP language $\mathcal{L}$.

Security Parameter: λ.
Parties: Sender S and Receiver R, adversary $\mathcal{A}$.

Sender Query: $\mathcal{F}_{CDS}$ receives $(\text{Send}, sid, (x, \mu))$ from S, where $x \in \mathcal{L} \cap \{0,1\}^{n_1(\lambda)}$ and $m \in \{0,1\}^{n_2(\lambda)}$ for polynomials n_1 and n_2, records $(sid, (x, \mu))$ and sends (Input, sid, x) to R and $\mathcal{A}$.
$\mathcal{F}_{CDS}$ ignores further send messages from S with sid.

Receiver Query: $\mathcal{F}_{CDS}$ receives $(\text{Witness}, sid, w)$ from party R, where $w \in \{0,1\}^{m(\lambda)}$ for a polynomial m. $\mathcal{F}_{CDS}$ ignores the message if no $(sid, \star)$ was recorded. Otherwise $\mathcal{F}_{CDS}$ sends $(\text{Open}, sid, x, \mu')$ to R where

$$\mu' = \begin{cases} \mu \text{ if } \mathcal{R}_{\mathcal{L}}(x, w) = 1 \\ \perp \text{ if } \mathcal{R}_{\mathcal{L}}(x, w) = 0 \end{cases}$$

$\mathcal{F}_{CDS}$ sends (Open, sid, x) to $\mathcal{A}$ and ignores further messages from R with sid.

Fig. 2. The Conditional Disclosure of Secrets (CDS) functionality

stand-alone model. We will consider protocols with either efficient or unbounded simulators.

Verifiability. We will, in addition, also require the CDS protocol to be *verifiable*. Downstream, when constructing our extractable commitment protocol in Sect. 4.3, we want to be able to prove consistency of the transcript of a CDS sub-protocol. It is not a-priori clear how to do this since the CDS protocol we construct will either live in the OT-hybrid model, in which case the OT input is *not* contained in the protocol transcript and is unconstrained by it; or it uses quantum communication, in which case, again consistency cannot be expressed as an NP-statement.

Definition 4.1 (Verifiability). *Let $\mathcal{L}$ be an* NP *language, and $\Pi = \langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ be a CDS protocol between a sender* $\mathsf{cds.S}$ *and a receiver* $\mathsf{cds.R}$. *Π is* verifiable *(w.r.t.* $\mathsf{cds.S}$*) if there is a polynomial time classical algorithm* Ver*, such that, the following properties are true:*

Correctness: *For every (x, μ) and every w, $\mathsf{cds.S}(x, \mu)$ after interacting with $\mathsf{cds.R}(w)$, outputs on a special output tape a proof π, such that, $\mathsf{Ver}(\tau, x, \mu, \pi) = 1$ where τ is the transcript of classical messages exchanged in the interaction.*

Binding: *For every $\lambda \in \mathbb{N}$, every (potentially unbounded) adversary $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$, every sequence of witnesses $\{w_\lambda\}_\lambda$, the probability that $\mathcal{A}_\lambda$ wins in the following experiment is negligible.*

- *$\mathcal{A}_\lambda$ after interacting with $\mathsf{cds.R}(1^\lambda, w)$, outputs (x, μ, π). Let τ be the transcript of classical messages exchanged in the interaction.*

– $\mathcal{A}_\lambda$ *wins if (a)* $\mathsf{Ver}(\tau, x, \mu, \pi) = 1$*, (b)* $\mathsf{cds.R}$ *did not abort, and (c)* $\mathsf{cds.R}$ *outputs* μ' *inconsistent with inputs* (x, μ) *and* w*, that is,*

$$\mu' \neq \begin{cases} \mu & \text{if } \mathcal{R}_{\mathcal{L}}(x, w) = 1 \\ \bot & \text{otherwise} \end{cases}$$

Definition 4.2 (Verifiable CDS). *Let* $\mathcal{L}$ *be an* NP *language, and* $\Pi = \langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ *be a protocol between a sender* $\mathsf{cds.S}$ *and a receiver* $\mathsf{cds.R}$*.* Π *is a* verifiable CDS *protocol if (a) it* $\mathtt{C\text{-}QSA}$*-emulates* $\mathcal{F}_{\mathsf{cds}}$ *with an efficient simulator; and (b) it is verifiable according to Definition 4.1.*

4.2 CDS Protocol from Unbounded Simulation OT

Theorem 4.1. *Assume the existence of pqOWF. For every* NP *language* $\mathcal{L}$*, there is a verifiable CDS protocol* $\Pi = \langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ *that* $\mathtt{C\text{-}QSA}$*-emulates* $\mathcal{F}_{\mathsf{cds}}$ *for* $\mathcal{L}$ *in the* $\mathcal{F}_{\mathtt{p\text{-}ot}}$ *hybrid model.*

Corollary 4.1. *Assume the existence of pqOWF, and a protocol that* $\mathtt{C\text{-}QSA}$*-emulates* $\mathcal{F}_{\mathtt{p\text{-}ot}}$ *with unbounded simulation. Then, for every* NP *language* $\mathcal{L}$*, there is a verifiable CDS protocol* $\Pi = \langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ *that* $\mathtt{C\text{-}QSA}$*-emulates* $\mathcal{F}_{\mathsf{cds}}$ *for* $\mathcal{L}$ *with unbounded simulation.*

Proof of Theorem 4.1. The verifiable CDS protocol is described in Fig. 3. The protocol uses Naor's classical statistically binding commitment protocol, Yao's garbled circuits, and post-quantum zero knowledge proofs, all of which can be implemented from pqOWF. For a more detailed description of these ingredients, see the full version of our paper.

In Lemma 4.1, we show that the protocol has an efficient simulator for a corrupted receiver, and in Lemma 4.2, an efficient simulator for a corrupted sender (both in the OT hybrid model). Lemma 4.3 shows that the protocol is verifiable. □

Lemma 4.1. *There is an efficient simulator against a malicious receiver.*

Proof. The simulator $\mathcal{S}$ interacts with $\mathsf{cds.R}^*$, receives a string ρ from $\mathsf{cds.R}^*$ in Step 1, and intercepts the OT queries $(\sigma^1, \ldots, \sigma^{2\lambda})$ in Step 4.

– **Case** 1. $R_{\mathcal{L}}(x, \sigma^i) = 1$ **for some** i**.** Send $(\text{Witness}, sid, \sigma^i)$ to the CDS functionality and receive μ. Simulate the rest of the protocol honestly using the CDS sender input (x, μ).
– **Case** 2. $R_{\mathcal{L}}(x, \sigma^i) = 0$ **for all** i**.** Simulate the rest of the protocol honestly using the CDS sender input $(x, 0)$.

We now show, through a sequence of hybrids, that this simulator produces a view that is computationally indistinguishable from that in the real execution of $\mathsf{cds.S}(x, \mu)$ with $\mathsf{cds.R}^*$.

Parties: The sender cds.S and the receiver cds.R. Inputs: cds.S has input (x, μ) and cds.R has input $w \in \{0,1\}^m$.

1. **Preamble**: cds.R sends a random string ρ as the first message of Naor's commitment scheme to cds.S and cds.S sends x to cds.R
2. **Compute Garbled Circuits:** cds.S generates 2λ garbled circuits, for the circuit computing $G_{x,\mu}(w) = \mu' = \begin{cases} \mu & \text{if } \mathcal{R}_{\mathcal{L}}(x,w) = 1 \\ \perp & \text{otherwise} \end{cases}$.
   That is, for every $i \in [2\lambda]$, $(\widehat{G}^i, \{\ell_b^{i,j}\}_{j\in[m],b\in\{0,1\}}) = \mathsf{Garb}(G_{x,\mu}; \gamma_i)$, where $\widehat{G}^i$ are the garbled circuits, and ℓ's are its associated labels.
3. **Cut-and-Choose:** cds.R samples a random subset $\Lambda \subseteq [2\lambda]$, by including each $i \in [2\lambda]$ with probability 1/2. For every $i \in [2\lambda]$, set
   $\sigma^i = \begin{cases} s^i \leftarrow \{0,1\}^m & i \in \Lambda \\ w & i \notin \Lambda \end{cases}$
4. **OT:** For every $i \in [2\lambda], j \in [m], b \in \{0,1\}$, cds.S samples $r_b^{i,j}$, the random coins for committing to the labels $\ell_b^{i,j}$ via Naor's commitment scheme.
   cds.S and cds.R invokes $\mathcal{F}_{\text{p-ot}}$ for $2\lambda \times m$ parallel OT, where the (i,j)'th OT for $i \in [2\lambda], j \in [m]$ has sender's input strings $(\ell_0^{i,j}, r_0^{i,j})$ and $(\ell_1^{i,j}, r_1^{i,j})$, and receiver's choice bit $\sigma^{i,j}$ (which is the j-th bit of σ^i) and cds.R receives $(\widetilde{\ell}^{i,j}, \widetilde{r}^{i,j})$.
   We refer to the OTs with index $(i, \star)$ as the i'th batch. as they transfer labels of the i'th garbled circuit $\widehat{G}_i$.
5. **Send Garbled Circuits and Commitments to the Labels and μ:** cds.S samples r^* and computes $c^* = \mathtt{com}_\rho(\mu; r^*)$ and $c_b^{i,j} = \mathtt{com}_\rho(\ell_b^{i,j}; r_b^{i,j})$.
   Send $\{\widehat{G}^i\}_{i\in[2\lambda]}$ and $(c^*, \{c_b^{i,j}\}_{i\in[2\lambda],j\in[m],b\in\{0,1\}})$ to the receiver cds.R.
6. **Proof of Consistency:** cds.S proves via ZK protocol that (a) c^* is a valid commitment to μ, (b) every $\widehat{G}^i$ is a valid garbling of $G_{x,\mu}$ with labels $\{\ell_b^{i,j}\}_{j\in[m],b\in\{0,1\}}$, and (c) $c_b^{i,j}$ is a valid commitment to $\ell_b^{i,j}$.
7. **Checks:** cds.R performs the following checks:
   - If the ZK proof in the previous step is not accepting, cds.R aborts.
   - **Λ-checks.** If there is $i \in \Lambda$ and $j \in [m]$, such that, $c_{\sigma^{i,j}}^{i,j} \neq \mathtt{com}_\rho(\widetilde{\ell}^{i,j}, \widetilde{r}^{i,j})$, cds.R aborts and outputs $\perp$.
   - **$\overline{\Lambda}$-check.** If for every $i \notin \Lambda$, there exists $j \in [m]$, such that, $c_{\sigma^{i,j}}^{i,j} \neq \mathtt{com}_\rho(\widetilde{\ell}^{i,j}, \widetilde{r}^{i,j})$, cds.R aborts and outputs $\perp$.
8. **Output:** If cds.R does not abort, there must exist $i \notin \Lambda$ such that, for all $j \in [m]$, $c_{\sigma^{i,j}}^{i,j} = \mathtt{com}_\rho(\widetilde{\ell}^{i,j}, \widetilde{r}^{i,j})$. Evaluate the i'th garbled circuit $\widehat{G}^i$ to get $\mu' = \mathsf{GEval}(\widehat{G}^i, \{\widetilde{\ell}^{i,j}\}_{j\in[m]})$, and output x', μ'.

Fig. 3. The verifiable CDS Scheme in $\mathcal{F}_{\text{p-ot}}$-hybrid model. The steps in color involve communication while the others only involve local computation.

Hybrid 0. This corresponds to the real execution of the protocol where the sender has input (x, m). The view of $\mathsf{cds.R}^*$ consists of

$$\left[\rho, \{\widehat{G}^i, \widetilde{\ell}^{i,j}, \widetilde{r}^{i,j}, c_b^{i,j}\}_{i\in[2\lambda],j\in[m],b\in\{0,1\}}, c^*, \tau_{\mathsf{ZK}}\right]$$

where ρ is the message sent by $\mathsf{cds.R}^*$ in Step 1, the strings $\widetilde{\ell}^{i,j}$ and $\widetilde{r}^{i,j}$ are received by $\mathsf{cds.R}^*$ from the OT functionality in Step 4, the garbled circuits $\widehat{G}^i$ and the commitments $c_b^{i,j}$ and c^* in Step 5, and τ_{ZK} is the transcript of the ZK protocol between $\mathsf{cds.S}$ and $\mathsf{cds.R}^*$ in Step 6. (See the protocol in Fig. 3).

Hybrid 1. This is identical to hybrid 0 except that we run the simulator to intercept the OT queries $(\sigma^1, \ldots, \sigma^{2\lambda})$ of $\mathsf{cds.R}^*$. The rest of the execution remains the same. Of course, the transcript produced is identical to that in hybrid 0.

Hybrid 2. In this hybrid, we replace the transcript τ_{ZK} of the zero-knowledge protocol with a simulated transcript. This is indistinguishable from hybrid 1 by (post-quantum) computational zero-knowledge. Note that generating this hybrid does not require us to use the randomness underlying the commitments $c_{1-\sigma^{i,j}}^{i,j}$ and c^*. (The randomness underlying $c_{\sigma^{i,j}}^{i,j}$ *are* revealed as part of the OT responses to $\mathsf{cds.R}^*$.)

Hybrid 3. In this hybrid, we replace half the commitments, namely $c_{1-\sigma^{i,j}}^{i,j}$, as well as c^* with commitments of 0. This is indistinguishable from hybrid 2 by (post-quantum) computational hiding of Naor commitments.

Hybrid 4. In this hybrid, we proceed as follows. If the simulator is in case 1, that is $R_{\mathcal{L}}(x, \sigma^i) = 1$ for some i, proceed as in hybrid 3 with no change. On the other hand, if the simulator is in case 2, that is $R_{\mathcal{L}}(x, \sigma^i) = 0$ for all i, replace the garbled circuits with simulated garbled circuits that always output $\perp$ and let the commitments $c_{\sigma^{i,j}}^{i,j}$ be commitments of the simulated labels. This is indistinguishable from hybrid 3 where the garbled circuits are an honest garbling of $G_{x,\mu}$ because of the fact that all the garbled evaluations output $\perp$ in hybrid 3, and because of the post-quantum security of the garbling scheme.

Hybrids 5–7 undo the effects of hybrids 2–4 in reverse.

Hybrid 5. In this hybrid, we replace the simulated garbled circuit with the real garbled circuit for the circuit $G_{x,0}$. This is indistinguishable from hybrid 4 because of the fact that all the garbled evaluations output $\perp$ in this hybrid, and because of the post-quantum security of the garbling scheme.

Hybrid 6. In this hybrid, we let all commitments be to the correct labels and messages. This is indistinguishable from hybrid 5 by (post-quantum) computational hiding of Naor commitments.

Hybrid 7. In this hybrid, we replace the simulated ZK transcript with the real ZK protocol transcript. This is indistinguishable from hybrid 7 by (post-quantum) computational zero-knowledge.

This final hybrid matches exactly the simulator. This finishes the proof.

Lemma 4.2. *There is an inefficient statistical simulator against a malicious sender.*

Proof. The simulator $\mathcal{S}$ interacts with $\mathsf{cds.S}^*$ as follows:

1. Send a string ρ to $\mathsf{cds.S}^*$ in Step 1, as in the protocol;
2. *Intercept* the OT messages $(\ell_0^{i,j}, r_0^{i,j})$ and $(\ell_1^{i,j}, r_1^{i,j})$ from $\mathsf{cds.S}^*$ in Step 4.
3. Run the rest of the protocol as an honest receiver $\mathsf{cds.R}$ would.
4. If the ZK proof rejects or if any Λ-check fails, $\mathcal{S}$ aborts and outputs $\perp$. (Note the simulator does not perform the $\overline{\Lambda}$-check).
5. Otherwise, extract μ from c^* using unbounded time, and send (x, μ) to the ideal functionality and halt.

The transcript generated by $\mathcal{S}$ is identical to the one generated in the real world where $\mathsf{cds.R}$ on input w interacts with $\mathsf{cds.S}^*$. It remains to analyze the output distribution of $\mathsf{cds.R}$ in the simulation vis-a-vis the real world.

1. Since the Λ-checks performed on the commitments of garbled instances in Λ by the simulator and the ones performed by the honest receiver in the real protocol are exactly the same, we have that the probability that the probability of abort is the same (for this step) in both scenarios.
2. The probability that the honest receiver in the real protocol aborts on the $\overline{\Lambda}$-check, conditioned on the fact that the Λ-checks passed, is negligible.

Thus, we have that the output distributions of the receiver are negligibly close between the simulation and the real world, finishing up the proof.

Lemma 4.3. *The protocol is verifiable.*

Proof. We first construct a verification algorithm Ver.

- The classical transcript τ consists of $\rho, x, \{\widehat{G}^i\}_{i\in[2\lambda]}, c^*, \{c_b^{i,j}\}_{i\in[2\lambda],j\in[m],b\in\{0,1\}}$.
- At the end of the protocol, $\mathsf{cds.S}$ outputs (x, μ, r^*) on its special output tape.
- The verification algorithm $\mathsf{Ver}(\tau, x, \mu', r') = 1$ iff $c^* = \mathtt{com}_\rho(\mu'; r')$.

We first claim that for honest $\mathsf{cds.S}$ and $\mathsf{cds.R}$ with $(x, w) \in \mathcal{R}_\mathcal{L}$, we have that $\mathsf{Ver}(\tau, x, \mu, r) = 1$. Since all parties in the protocol are honest the input x in τ is the same as the one output by $\mathsf{cds.S}$ and we have that c^* is the commitment to the honest message using the correct randomness, so Ver outputs 1.

To show binding, assume that the verification passes and the receiver does not abort. Then, we know that there is at least one $i \notin \Lambda$ such that the i-th garbled circuit+input pair is correct and the circuit is the garbling of $G_{x,\mu}$. The verifier will evaluate the circuit on input w and obtain either $\perp$ when $R_\mathcal{L}(x, w) = 0$ or μ when $R_\mathcal{L}(x, w) = 1$, exactly as required.

4.3 Extractable Commitment from CDS

Theorem 4.2. *Assume the existence of pqOWF. There is a commitment protocol $\langle C, R\rangle$ that* $\mathtt{C\text{-}QSA}$*-emulates $\mathcal{F}_{\mathtt{so\text{-}com}}$ with efficient simulators.*

Parties: The committer C and the receiver R.
Inputs: C gets a message vector $\vec{\mu} = (\mu_1, \ldots, \mu_{\ell(n)})$ and R gets 1^n.

Commitment Phase

1. **Preamble.** C sends a random string ρ to R, and R sends a random string ρ^* to C, as the first message of the Naor commitment scheme.
2. **Set up a Trapdoor Statement.**
   - R sends a Naor commitment $c = \mathtt{com}_\rho(0; r)$.
   - R proves to C using a ZK protocol that c is a commitment to 0, that is, $((c, \rho, 0), r) \in \mathcal{R}_{\mathcal{L}_{\mathtt{com}}}$. If the ZK verifier rejects, C aborts.
3. **CDS.** C and R run the CDS protocol $\langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ for the language $\mathcal{L}_{\mathtt{com}}$ where C acts as $\mathsf{cds.S}$ with input $x = (c, \rho, 1)$ and message $\vec{\mu}$, and R acts as $\mathsf{cds.R}$ with input 0.
   C aborts if $\mathsf{cds.S}$ aborts, else C obtains the protocol transcript τ and $\mathsf{cds.S}$'s proof π. R aborts if $\mathsf{cds.R}$ aborts, or if $\mathsf{cds.R}$ outputs $(x', \vec{\mu}')$ but $x' \neq (\rho, c, 1)$.
4. **Commit and Prove Consistency.**
   - C sends a Naor commitment $c^* = \mathtt{com}_{\rho^*}(\vec{\mu}; r^*)$.
   - C proves to R using a ZK protocol there exists a $\vec{\mu}$ such that $(x = (\rho, c, 1), \vec{\mu})$ is the input that C used in the CDS protocol and $\vec{\mu}$ is committed in c^*, that is:

$$\mathsf{Ver}(\tau, x, \vec{\mu}, \pi) = 1 \text{ and } c^* = \mathtt{com}_{\rho^*}(\vec{\mu}, r^*)$$

5. R accepts this commitment if the ZK proof is accepting.

Decommitment Phase

1. R sends $I \subseteq [\ell]$.
2. C sends $\vec{\mu}|_I$ and proves via a ZK protocol that $c^*|_I$ commits to $\vec{\mu}|_I$.
3. R accepts this decommitment if the ZK proof is accepting.

Fig. 4. Extractable Selective-Opening-Secure commitment scheme

Proof. The construction of our extractable commitment scheme is given in Fig. 4. The protocol uses Naor's classical statistically binding commitment protocol and a verifiable CDS protocol $\Pi = \langle \mathsf{cds.S}, \mathsf{cds.R} \rangle$ that $\mathtt{C\text{-}QSA}$-emulates $\mathcal{F}_{\mathsf{cds}}$ (with unbounded simulation) for $\mathcal{L}_{\mathtt{com}}$, the language consisting of all Naor's commtiments (ρ, c) to a bit b: $\mathcal{R}_{\mathcal{L}_{\mathtt{com}}}((\rho, c, b), r) = 1$ iff $c = \mathtt{com}_\rho(b; r)$.

We defer a detailed description of these tools to the full version of our paper.

In Lemma 4.4 (resp. Lemma 4.5), we show that the protocol has an efficient simulator for a corrupted sender (resp. receiver).

Lemma 4.4. *There is an efficient simulator against a malicious sender.*

Proof. The simulator $\mathcal{S}$ against a malicious committer C^* works as follows.

1. In step 1, proceed as an honest receiver would.

2. In step 2, send a Naor commitment $c = \mathtt{com}_\rho(1; r)$ (instead of 0) and simulate the ZK proof.
3. In step 3, run the honest CDS protocol with r as witness, gets $\boldsymbol{\mu}$ and sends it to the ideal functionality $\mathcal{F}_{\mathtt{so\text{-}com}}$.
4. Run the rest of the protocol as an honest receiver would.

We now show, through a sequence of hybrids, that this simulator produces a joint distribution of a view of C^* together with an output of R that is computationally indistinguishable from that in the real execution of C^* with R. In order to show this we consider the following sequence of hybrids.

Hybrid 0. This corresponds to the protocol $\Pi^{\mathsf{ECom}}_{\mathtt{H}_0}$, where $\mathcal{S}_0$ sits between C^* and the honest receiver in the real protocol and just forwards their messages. It follows trivially that $M_{\Pi_{\mathsf{ECom}}, C^*} \approx_{qc} M_{\Pi^{\mathsf{ECom}}_{\mathtt{H}_0}, \mathcal{S}_0}$.

Hybrid 1. $\mathcal{S}_1$ interacts with C^* following the protocol $\Pi^{\mathsf{ECom}}_{\mathtt{H}_1}$, which is the same as $\Pi^{\mathsf{ECom}}_{\mathtt{H}_0}$ except that $\mathcal{S}_1$ uses the ZK simulator instead of the proof that $((c, \rho, 0), r) \in \mathcal{R}_{\mathcal{L}_{\mathsf{com}}}$. From the computational zero-knowledge property of the protocol, we have that $M_{\Pi^{\mathsf{ECom}}_{\mathtt{H}_0}, \mathcal{S}_0} \approx_{qc} M_{\Pi^{\mathsf{ECom}}_{\mathtt{H}_1}, \mathcal{S}_1}$.

Hybrid 2. $\mathcal{S}_2$ interacts with C^* following the protocol $\Pi^{\mathsf{ECom}}_{\mathtt{H}_2}$, which is the same as $\Pi^{\mathsf{ECom}}_{\mathtt{H}_1}$ except that $\mathcal{S}_2$ sends $c' = \mathtt{com}_\rho(1; r)$ instead of the (honest) commitment of 0. When $\mathcal{S}_2$ simulates $\mathcal{F}_{\mathtt{zk}}$, she still sends a message that c' is a valid input. It follows from computationally hiding property of Naor's commitment scheme that $M_{\Pi^{\mathsf{ECom}}_{\mathtt{H}_1}, \mathcal{S}_1} \approx_{qc} M_{\Pi^{\mathsf{ECom}}_{\mathtt{H}_2}, \mathcal{S}_2}$.

Hybrid 3. $\mathcal{S}_3$ interacts with C^* following the protocol $\Pi^{\mathsf{ECom}}_{\mathtt{H}_3}$, which is the same as $\Pi^{\mathsf{ECom}}_{\mathtt{H}_2}$ except that $\mathcal{S}_3$ now uses the private randomness r as a witness that c' is a commitment of 1.

Since our protocol realizes $\mathcal{F}_{CDS}$, $\mathsf{cds.S}^*$ (controlled by C^*) does not behave differently depending on the input of $\mathsf{cds.R}$, so the probability of abort in step 3 does not change. Notice also that $\mathsf{Ver}(\tau, x, \boldsymbol{\mu}, \pi)$ is independent of $\mathsf{cds.R}$'s message, so the acceptance probability of the ZK proof does not change either.

Then, if the ZK proof leads to acceptance, by the soundness of the protocol, we know that $\mathsf{Ver}(\tau, x, \boldsymbol{\mu}, \pi) = 1$ and by the binding of the commitment c^*, such a $\boldsymbol{\mu}$ is uniquely determined.

Finally, by the verifiability of the CDS protocol, we know that the receiver either aborts or outputs the specified $\boldsymbol{\mu}$. Thus, the outputs of the receiver R in the simulated execution and the real execution must be the same in this case.

Lemma 4.5. *There is an efficient simulator against a malicious receiver.*

Proof. The simulator $\mathcal{S}$ against a malicious receiver R^* proceeds as follows.

- In steps 1 and 2, proceed as an honest sender would.
- In step 3, run the CDS protocol using a message vector $\boldsymbol{\mu} = \mathbf{0}$ of all zeroes.
- In step 4, commit to the all-0 vector and produce a simulated ZK proof.
- During decommitment, send $I \subseteq [\ell]$ to the ideal functionality and receive $\boldsymbol{\mu}|_I$. Send $\boldsymbol{\mu}|_I$ to R^*, and simulate the ZK proof.

We now show, through a sequence of hybrids, that this simulator is computationally indistinguishable from the real execution of $C(\boldsymbol{\mu})$ with R^*.

Hybrid 0. This corresponds to the protocol $\Pi^{\mathsf{ECom}}_{\mathsf{H}_0}$, where $\mathcal{S}_0$ sits between the honest commiter C and R^*, and it just forwards their messages. It follows trivially that $M_{\Pi_{\mathsf{ECom}},C^*} \approx_{qc} M_{\Pi^{\mathsf{ECom}}_{\mathsf{H}_0},\mathcal{S}_0}$.

Hybrid 1. $\mathcal{S}_1$ interacts with R^* following the protocol $\Pi^{\mathsf{ECom}}_{\mathsf{H}_1}$, which is the same as $\Pi^{\mathsf{ECom}}_{\mathsf{H}_0}$ except that $\mathcal{S}_1$ uses the ZK simulator in Step 4 and the decommitment phase. From the computational zero-knowledge property, we have that $M_{\Pi^{\mathsf{ECom}}_{\mathsf{H}_0},\mathcal{S}_0} \approx_{qc} M_{\Pi^{\mathsf{ECom}}_{\mathsf{H}_1},\mathcal{S}_1}$.

Hybrid 2. $\mathcal{S}_2$ interacts with R^* following the protocol $\Pi^{\mathsf{ECom}}_{\mathsf{H}_2}$, which is the same as $\Pi^{\mathsf{ECom}}_{\mathsf{H}_1}$ except that $\mathcal{S}_2$ sets c^* to be a commitment to 0. It follows from the computationally-hiding property of the commitment scheme that $M_{\Pi^{\mathsf{ECom}}_{\mathsf{H}_1},\mathcal{S}_1} \approx_{qc} M_{\Pi^{\mathsf{ECom}}_{\mathsf{H}_2},\mathcal{S}_2}$.

Hybrid 3. $\mathcal{S}_3$ interacts with R^* following the protocol $\Pi^{\mathsf{ECom}}_{\mathsf{H}_3}$, which is the same as $\Pi^{\mathsf{ECom}}_{\mathsf{H}_2}$ except that $\mathcal{S}_3$ uses $\boldsymbol{\mu} = 0^\ell$ as the $\mathsf{cds.S}$ message.

From the soundness of the ZK proof in Step 2, we have that c is not a commitment of 1. In this case, by the security of CDS, R^* does not receive $\boldsymbol{\mu}$, so the change of the message cannot be distinguished.

Notice that Hybrid 3 matches the description of the simulator $\mathcal{S}$, and therefore $M_{\Pi^{\mathsf{ECom}}_{\mathsf{H}_2},\mathcal{S}_2} \approx_{qc} M_{\mathcal{F}_{\mathtt{so\text{-}com}},\mathcal{S}}$.

5 Multiparty (Quantum) Computation in MiniQCrypt

Our quantum protocol realizing $\mathcal{F}_{\mathtt{so\text{-}com}}$ from quantum-secure OWF allows us to combine existing results and realize secure computation of any two-party or multi-party classical functionality as well as quantum circuit in MiniQCrypt.

Theorem 5.1. *Assuming that post-quantum secure one-way functions exist, for every classical two-party and multi-party functionality $\mathcal{F}$, there is a quantum protocol* C-QSA*-emulates $\mathcal{F}$.*

Proof. By Theorem 3.2, we readily realize $\mathcal{F}_{\mathtt{ot}}$ in MiniQCrypt. In the $\mathcal{F}_{\mathtt{ot}}$-hybrid model, any classical functionality $\mathcal{F}$ can be realized statistically by a classical protocol in the universal-composable model [42]. The security can be lifted to the quantum universal-composable model as shown by Unruh [61]. As a result, we also get a classical protocol in the $\mathcal{F}_{\mathtt{ot}}$-hybrid model that S-QSA emulates $\mathcal{F}$. Plugging in the quantum protocol for $\mathcal{F}_{\mathtt{ot}}$, we obtain a quantum protocol that C-QSA-emulates $\mathcal{F}$ assuming existence of quantum-secure one-way functions.

Now that we have a protocol that realizes any classical functionality in MiniQCrypt, we can instantiate $\mathcal{F}_{mpc}$ used in the work of [24] to achieve a protocol for secure multi-party quantum computation where parties can jointly evaluate an arbitrary quantum circuit on their private quantum input states. Specifically

consider a quantum circuit Q with k input registers. Let $\mathcal{F}_Q$ be the ideal protocol where a trusted party receives private inputs from k parties, evaluate Q, and then send the outputs to respective parties. We obtain the following.

Theorem 5.2. *Assuming that post-quantum secure one-way functions exist, for any quantum circuit Q, there is a quantum protocol that* `C-QSA`*-emulates the $\mathcal{F}_Q$.*

Acknowledgements. We thank the Simons Institute for the Theory of Computing for providing a meeting place where the seeds of this work were planted. VV thanks Ran Canetti for patiently answering his questions regarding universally composable commitments.

Most of this work was done when AG was affiliated to CWI and QuSoft. HL was supported by NSF grants CNS-1528178, CNS-1929901, CNS-1936825 (CAREER), CNS-2026774, a Hellman Fellowship, a JP Morgan AI Research Award, the Defense Advanced Research Projects Agency (DARPA) and Army Research Office (ARO) under Contract No. W911NF-15-C-0236, and a subcontract No. 2017-002 through Galois. FS was supported by NSF grants CCF-2041841, CCF-2042414, and CCF-2054758 (CAREER). VV was supported by DARPA under Agreement No. HR00112020023, a grant from the MIT-IBM Watson AI, a grant from Analog Devices, a Microsoft Trustworthy AI grant, and a DARPA Young Faculty Award. The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense, DARPA, the National Science Foundation, or the U.S. Government.

References

1. Agarwal, A., Bartusek, J., Goyal, V., Khurana, D., Malavolta, G.: Post-quantum multi-party computation in constant rounds (2020). arXiv:2005.12904. https://arxiv.org/abs/2005.12904
2. Ananth, P., La Placa, R.L.: Secure quantum extraction protocols. CoRR, abs/1911.07672 (2019)
3. Barak, B.: The complexity of public-key cryptography. Cryptology ePrint Archive, Report 2017/365, 2017. https://eprint.iacr.org/2017/365
4. Bartusek, J., Coladangelo, A., Khurana, D., Ma, F.: One-way functions imply secure computation in a quantum world (2020)
5. Beaver, D.: Correlated pseudorandomness and the complexity of private computations. In: Miller, G.L. (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, pp. 479–488. ACM (1996)
6. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_1
7. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: 47th Annual IEEE Symposium on Foundations of Computer Science, pp. 249–260. IEEE (2006)
8. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: EEE International Conference on Computers, Systems and Signal Processing, vol. 175, p. 8 (1984)

9. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.-H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_29 As references [10, 11] and [51, 52] are same, we have deleted the duplicate reference and renumbered accordingly. Please check and confirm
10. Bitansky, N., Shmueli, O.: Post-quantum zero knowledge in constant rounds. In: Makarychev, K., Makarychev, Y., Tulsiani, M., Kamath, G., Chuzhoy, J. (eds.) STOC 2020, pp. 269–279. ACM (2020)
11. Blum, M.: How to prove a theorem so no one else can claim it. In: Proceedings of the International Congress of Mathematicians (1986)
12. Bouman, N.J., Fehr, S.: Sampling in a quantum population, and applications. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 724–741. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_39
13. Brakerski, Z., Christiano, P., Mahadev, U., Vazirani, U.V., Vidick, T.: A cryptographic test of quantumness and certifiable randomness from a single quantum device. In: FOCS 2018, pp. 320–331 (2018)
14. Buhrman, H., Christandl, M., Schaffner, C.: Complete insecurity of quantum protocols for classical two-party computation. Phys. Rev. Lett. **109**(16), 160501 (2012)
15. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: FOCS, pp. 136–145. IEEE (2001)
16. Chailloux, A., Gutoski, G., Sikora, J.: Optimal bounds for semi-honest quantum oblivious transfer. Chic. J. Theor. Comput. Sci. **2016**, 1–17 (2016)
17. Colbeck, R.: Quantum and relativistic protocols for secure multi-party computation. Ph.D. Thesis, Trinity College, University of Cambridge (2009)
18. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, pp. 643–652 (2002)
19. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions. In: 29th Annual Symposium on Foundations of Computer Science, pp. 42–52 (1988)
20. Damgård, I., Fehr, S., Lunemann, C., Salvail, L., Schaffner, C.: Improving the security of quantum protocols via commit-and-open. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 408–427. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_24
21. Damgård, I.B., Fehr, S., Renner, R., Salvail, L., Schaffner, C.: A tight high-order entropic quantum uncertainty relation with applications. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 360–378. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_20
22. Damgård, I.B., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded-quantum-storage model. SIAM J. Comput. **37**(6), 1865–1890 (2008)
23. Dixon, A.R., Yuan, Z.L., Dynes, J.F., Sharpe, A.W., Shields, A.J.: Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. Opt. Express **16**(23), 18790 (2008)
24. Dulek, Y., Grilo, A.B., Jeffery, S., Majenz, C., Schaffner, C.: Secure multi-party quantum computation with a dishonest majority. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part III. LNCS, vol. 12107, pp. 729–758. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_25
25. Dupuis, F., Fehr, S., Lamontagne, P., Salvail, L.: Adaptive versus non-adaptive strategies in the quantum setting with applications. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part III. LNCS, vol. 9816, pp. 33–59. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53015-3_2

26. Dupuis, F., Nielsen, J.B., Salvail, L.: Secure two-party quantum evaluation of unitaries against specious adversaries. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 685–706. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_37
27. Dupuis, F., Nielsen, J.B., Salvail, L.: Actively secure two-party evaluation of any quantum operation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 794–811. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_46
28. Fang, J., Unruh, D., Weng, J., Yan, J., Zhou, D.: How to base security on the perfect/statistical binding property of quantum bit commitment? IACR Cryptol. ePrint Arch. **2020**, 621 (2020)
29. Fehr, S., Katz, J., Song, F., Zhou, H.-S., Zikas, V.: Feasibility and completeness of cryptographic tasks in the quantum world. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 281–296. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36594-2_16
30. Fehr, S., Schaffner, C.: Composing quantum protocols in a classical environment. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 350–367. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00457-5_21
31. Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. In: Vitter, J.S. (ed.) STOC 1998, pp. 151–160. ACM (1998)
32. Goldreich, O.: Foundations of Cryptography: Volume 2 Basic Applications, 1st edn. Cambridge University Press, Cambridge (2009)
33. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th ACM STOC, pp. 218–229. ACM Press (May 1987)
34. Goldreich, O., Micali, S., Wigderson, A.: How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design (extended abstract). In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 171–185. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_11
35. Grilo, A.B., Lin, H., Song, F., Vaikuntanathan, V.: Oblivious transfer is in miniqcrypt. Cryptology ePrint Archive, Report 2020/1500 (2020). https://eprint.iacr.org/2020/1500
36. Hallgren, S., Smith, A., Song, F.: Classical cryptographic protocols in a quantum world. Int. J. Quant. Inf. **13**(04), 1550028 (2015). Preliminary version in Crypto 2011
37. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM J. Comput. **28**(4), 1364–1396 (1999)
38. Hiskett, P.A., et al.: Long-distance quantum key distribution in optical fibre. New J. Phys. **8**(9), 193 (2006)
39. Impagliazzo, R.: A personal view of average-case complexity. In: Structure in Complexity Theory Conference, Annual, p. 134, Los Alamitos, CA, USA. IEEE Computer Society (Jun 1995)
40. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Johnson, D.S. (ed.) STOC 1989, pp. 44–61. ACM (1989)
41. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 145–161. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_9
42. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding cryptography on oblivious transfer – efficiently. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 572–591. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_32

43. Kilian, J.: Founding cryptography on oblivious transfer. In: 20th ACM STOC, pp. 20–31. ACM Press (May 1988)
44. Konig, R., Wehner, S., Wullschleger, J.: Unconditional security from noisy quantum storage. IEEE Trans. Inf. Theor. **58**(3), 1962–1984 (2012)
45. Liao, S.-K., et al.: Satellite-relayed intercontinental quantum network. Phys. Rev. Lett. **120**(3), 030501 (2018)
46. Liu, Y.K.: Building one-time memories from isolated qubits. In: 5th Conference on Innovations in Theoretical Computer Science, pp. 269–286 (2014)
47. Liu, Y.-K.: Single-shot security for one-time memories in the isolated qubits model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 19–36. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44381-1_2
48. Lo, H.-K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
49. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**(17), 3410–3413 (1997)
50. Lunemann, C., Nielsen, J.B.: Fully simulatable quantum-secure coin-flipping and applications. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 21–40. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21969-6_2
51. Maji, H.K., Prabhakaran, M., Rosulek, M.: A zero-one law for cryptographic complexity with respect to computational UC security. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 595–612. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_32
52. Mayers, D., Salvail L.: Quantum oblivious transfer is secure against all individual measurements. In: Proceedings Workshop on Physics and Computation. PhysComp 1994, pp. 69–77 (1994)
53. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414 (1997)
54. Naor, M.: Bit commitment using pseudo-randomness. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 128–136. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_13
55. Pugh, C.J., et al.: Airborne demonstration of a quantum key distribution receiver payload. Quant. Sci. Technol. **2**(2), 024009 (2017)
56. Rabin, M.: How to exchange secrets by oblivious transfer. Technical Memo TR-81, Aiken Computation Laboratory, Harvard University (1981)
57. Rudich, S.: The use of interaction in public cryptosystems. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 242–251. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_19
58. Salvail, L.: Quantum bit commitment from a physical assumption. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 338–353. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0055740
59. Salvail, L., Schaffner, C., Sotáková, M.: Quantifying the leakage of quantum protocols for classical two-party cryptography. Int. J. Quant. Inf. **13**(04), 1450041 (2015)
60. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: FOCS 1994, pp. 124–134. IEEE Computer Society (1994)
61. Unruh, D.: Universally composable quantum multi-party computation. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 486–505. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_25

62. Unruh, D.: Quantum proofs of knowledge. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 135–152. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_10
63. Vazirani, U., Vidick, T.: Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In: STOC 2012, pp. 61–76. Association for Computing Machinery (2012)
64. Watrous, J.: Zero-knowledge against quantum attacks. SIAM J. Comput. **39**(1), 25–58 (2009). Preliminary version in STOC 2006
65. Wiesner, S.: Conjugate coding. SIGACT News **15**(1), 78–88 (1983)
66. Yao, A.C.C.: Security of quantum protocols against coherent measurements. In: 27th ACM STOC, pp. 67–75. ACM Press (May/June 1995)