On the computational hardness needed for quantum cryptography

Zvika Brakerski[*]   Ran Canetti[†]   Luowen Qian[†]

Abstract

In the classical model of computation, it is well established that *one-way functions* (OWF) are minimal for computational cryptography: They are essential for almost any cryptographic application that cannot be realized with respect to computationally unbounded adversaries. In the quantum setting, however, OWFs appear not to be essential (Kretschmer 2021; Ananth et al., Morimae and Yamakawa 2022), and the question of whether such a minimal primitive exists remains open.

We consider EFI pairs — efficiently samplable, statistically far but computationally indistinguishable pairs of (mixed) quantum states. Building on the work of Yan (2022), which shows equivalence between EFI pairs and statistical commitment schemes, we show that EFI pairs are necessary for a large class of quantum-cryptographic applications. Specifically, we construct EFI pairs from minimalistic versions of commitments schemes, oblivious transfer, and general secure multiparty computation, as well as from QCZK proofs from essentially any non-trivial language. We also construct quantum computational zero knowledge (QCZK) proofs for all of QIP from any EFI pair.

This suggests that, for much of quantum cryptography, EFI pairs play a similar role to that played by OWFs in the classical setting: they are simple to describe, essential, and also serve as a linchpin for demonstrating equivalence between primitives.

1   Introduction

One of the most fundamental achievements of cryptography has been the conceptualization and eventual formalization of the forms of computational hardness that are needed for obtaining prevalent cryptographic tasks. Notions such as one-way functions [DH76, Yao82] (capturing functions that can be computed efficiently but are hard to meaningfully invert) and pseudorandom generators [Sha83, Yao82, BM84] (capturing the ability to efficiently expand short random strings into longer strings that are hard to distinguish from fully random) became foundational pillars for the design and reduction-based analysis of cryptographic schemes that are only "computationally secure" (that is, secure only against computationally-bounded attacks). Furthermore, the celebrated equivalence between the two notions [BM84, GL89, HILL99] has cemented the combined concept as the "foundational computational hardness for cryptography": One that is essential for realizing almost any cryptographic task that requires computational hardness, and at the same time suffices for realizing a large class of cryptographic tasks.

However, in the quantum setting, where parties can generate, process, and communicate quantum information, the lay of the land of computational hardness turns out to be different. First, quintessential tasks such as key-exchange with only public communication, which classically can only be computationally secure, can be obtained without any need for computational hardness [BB84, REN08]. Furthermore, quantum protocols can use (quantum-hard) one way functions to obtain tasks that are provably unobtainable from one way functions alone in the classical setting, at least in a relativizing manner. These include non-interactive commitments with either statistical hiding or statistical binding property [MP12, YWLQ15, BB21], and oblivious transfer [IR89, CLS01, BCKM21, GLSV21].

Even further, it has been recently shown how to obtain commitments, oblivious transfer and general multiparty computation from a form of computational hardness that appears to be "purely quantum", in the sense that it does not appear to imply one way functions (or any equivalent formulation of computational hardness) — not even ones against *classical* attackers [AQY22, MY22]. Superficially, this new form of computational hardness, called *Pseudorandom States (PRS),* is a straightforward generalization of pseudorandom generators: it postulates the ability to efficiently generate quantum states that are hard to distinguish from a Haar-random state even when given multiple instances [JLS18, BS19, BS20]. However this apparent similarity is deceiving; indeed, there are no relativizing constructions of one way functions from PRS [Kre21]. Also, in spite of initial attempts [MY22], the celebrated classical equivalence between one-wayness and pseudorandomness does not appear to naturally generalize to the quantum setting, at least not with respect to PRS. Still, we do not know whether PRS are *essential* for realizing any of the above cryptographic primitives.

This leaves quantum cryptography devoid of a convenient form of "foundational computational hardness", namely a form of computational hardness that is both necessary for any meaningful computational security, and sufficient for realizing a large class of tasks.

Our contributions. We formulate a relatively *simple and natural* primitive and show that its existence is both necessary and sufficient for a significant class of cryptographic applications in a quantum-enabled computational model. While many of these implications are either known or easily derived from known results, we hope that the proposed framing, along with the new implications, will help in understanding the computational foundations of quantum cryptography.

The proposed primitive draws from a classical primitive considered by Goldreich [Gol90], as well as from the notion of canonical quantum commitments proposed by Yan [Yan22]. Goldreich's primitive is aimed at capturing non-trivial and "cryptographically useful" computational indistinguishability:

Definition 1.1 (EFID pairs [Gol90])**.** *An EFID pair is a pair of efficient (classical) sampling algorithms such that their output distributions are statistically far but computationally indistinguishable.*

Goldreich's work leverages the result of Impagliazzo, Levin, and Luby [ILL89] to show that EFID pairs exist if and only if (classical) pseudorandom generators exist. This, together with what we know about pseudorandom generators, means the existence of a classical protocol for almost any cryptographic task that requires computational hardness implies existence of EFID pairs, and furthermore that EFID pairs suffice for realizing a large class of tasks. We consider a natural quantum analogue of EFID pairs:

Definition 1.2 (EFI pairs, informal). *An EFI pair is a pair of efficient quantum algorithms whose output* states *are statistically far but computationally indistinguishable.*

Clearly, any quantum-hard EFID pair is also an EFI pair. On the other hand, it is unknown whether existence of EFI pairs implies the existence of (classical) pseudorandom generators or one-way functions. Indeed, the implication is false in the relativizing setting (see [Kre21], combined with [AQY22, Theorem 4.1]).

A first indication that EFI pairs are central to quantum cryptography is the observation that they are essentially equivalent to the statically binding variant of canonical form quantum commitments [Yan22][1]. Building on this initial connection, we demonstrate that the existence of EFI pairs is essential for the existence of *any* commitment scheme, oblivious transfer protocols, non-trivial multi-party computation protocols, and zero-knowledge proofs for non-trivial languages. Furthermore, for each one of these primitives, we use EFI pairs as a tool for demonstrating that existence of protocols for a minimal version of the primitive implies existence of protocols for a full-fledged version of that primitive. Informally:

- **Quantum commitment schemes.** A commitment scheme is a cryptographic protocol where a committer commits to a hidden bit so that it can be later revealed but not modified. As mentioned, EFI pairs can be readily used to build (cannonical form) statistically binding non-interactive quantum commitments, which subsequently imply statistically hiding commitments [Yan22].
  We construct EFI pairs from any plain "semi-honest" interactive commitment scheme, namely an interactive commitment scheme that is (computationally) binding and hiding as long as both parties are honest during the commitment phase. (For commitment schemes that are either statistically hiding or statistically binding, this implication is essentially shown in [Yan22]. We extend this results to any commitment.)
- **Quantum oblivious transfer.** An oblivious transfer scheme is a cryptographic protocol where a sender makes two bits available to a receiver in a way that enables the receiver to obtain exactly one of them, without the sender learning which bit it obtained. Fully secure (namely, simulation-secure against adversaries that deviate from the protocol) quantum oblivious transfer is known to be constructible from quantum statistically binding commitments [BCKM21, AQY22] (and so also from EFI pairs).
  We show how to construct EFI pairs from any *semi-honest OT* protocol, namely any OT protocol that is only guaranteed to be secure when both parties follow the protocol instructions without abort and up to purifications (namely, without tracing out any register used by each party).
- **Quantum secure multiparty computation protocols.** A multiparty secure computation protocol is a protocol where participating parties jointly compute the output of a function of their secret inputs without revealing anything but the function value. Known constructions of general MPC from any statistically binding quantum commitment [AQY22] imply that EFI pairs can also be used to perform secure evaluation of any functionality.
  We show how any protocol for securely evaluating any non-trivial classical finite functionality (namely a function with an insecure minor as in [BMM99]), even in the semi-honest model, implies the existence of EFI pairs.

---

[1]Indeed, Yan [Yan22] suggests studying the connections between statistically binding canonical-form commitment schemes and other cryptographic primitives. This work follows the same path, while distilling EFI as the notion of interest. See more details in Section 1.1.

- **Quantum computational zero-knowledge (QCZK) proofs.** Finally, a computational zero-knowledge proof is an interactive proof system where any malicious verifier cannot learn anything beyond the fact that the statement is true, in the sense that their view could be efficiently simulated given only the public instance.

  By observing that zero knowledge is a special case of secure two-party computation (2PC), we have that if EFI pairs exist then QCZK = QIP, and any language in QMA also admits QCZK proofs with negligible soundness and an efficient prover that uses only a single copy of the witness. Conversely, we build on results from [YWLQ15] to construct EFI pairs from any *honest verifier* QCZK proof (QCZK$_{\mathsf{HV}}$) for any language that is hard on average for BQP. (QCZK$_{\mathsf{HV}}$ is a relaxation of QCZK where zero knowledge property is guaranteed to hold only against purified verifiers with abort, rather than arbitrary polytime verifiers.)

Furthermore, all these equivalences relativize[2]. Thus, Kretschmer's oracle separation [Kre21] immediately generalizes to show that none of the objects constructible from EFI pairs (or pseudo-random states) imply the existence of one-way functions (post-quantum or not) in a relativizing way.

1.1 Our techniques

This section presents an overview of the proofs for our results.

EFI pairs and statistical commitments. In the classical setting, building a commitment scheme from EFID pairs would naturally go via Goldreich's transformation to a PRG, and then use, say, Naor's commitment [Nao91]. However, it is not clear how this transformation could be generalized to the quantum setting. In particular, Goldreich's proof crucially relies on the fact that for a BPP (randomized) algorithm, it is possible to separate the randomness from the rest of the computation — or even arbitrarily *program* the randomness. Such techniques cannot work for quantum algorithms, as also observed by the recent work of Aaronson, Ingram, and Kretschmer [AIK22] comparing the complexity classes BPP and BQP.

Still, as noticed several times in the literature, EFI pairs give quantum commitments in a rather direct way. To sketch this basic construction, we first recall the syntax of a canonical form quantum commitment scheme:[3]

- To commit to b, the committer efficiently generates a bipartite (i.e., two-register) state $|\psi_b\rangle_{\mathsf{CR}}$, and sends the commitment register C.
- To open, simply reveal the other register R and b, and the receiver can perform a rank-1 projection onto the corresponding state $|\psi_b\rangle_{\mathsf{CR}}$ (or equivalently, uncompute the state generation

---

[2]We use the term *relativizing* to denote that the construction works even in the presence of (quantum) oracles. In particular, this allows the construction to invoke the next message function of a protocol as a black box or even run its purification. An example of a relativizing implication is Watrous's construction of a QSZK protocol from any honest-verifier QSZK$_{\mathsf{HV}}$ protocol [Wat02].

We reserve the use of the term *black-box reductions* to denote reductions which are black box in a primitive, namely reductions that use oracle access to the ideal functionality describing the primitive, irrespective of any particular implementation (as e.g. in the work of Kilian [Kil91]).

[3]This (non-interactive) canonical form of quantum bit commitment schemes was first introduced by the work of Yan et al. [YWLQ15], but the idea dates back to the work of Chailloux, Kerenidis, and Rosgen [CKR11]. Subsequently, it has been shown that canonical form commitments are as useful as traditional bit commitments by Yan et al. [YWLQ15, FUYZ20, Yan22] Its connection to (classical) EFID pairs was observed by Yan in a 2022 revision of their work [Yan22].
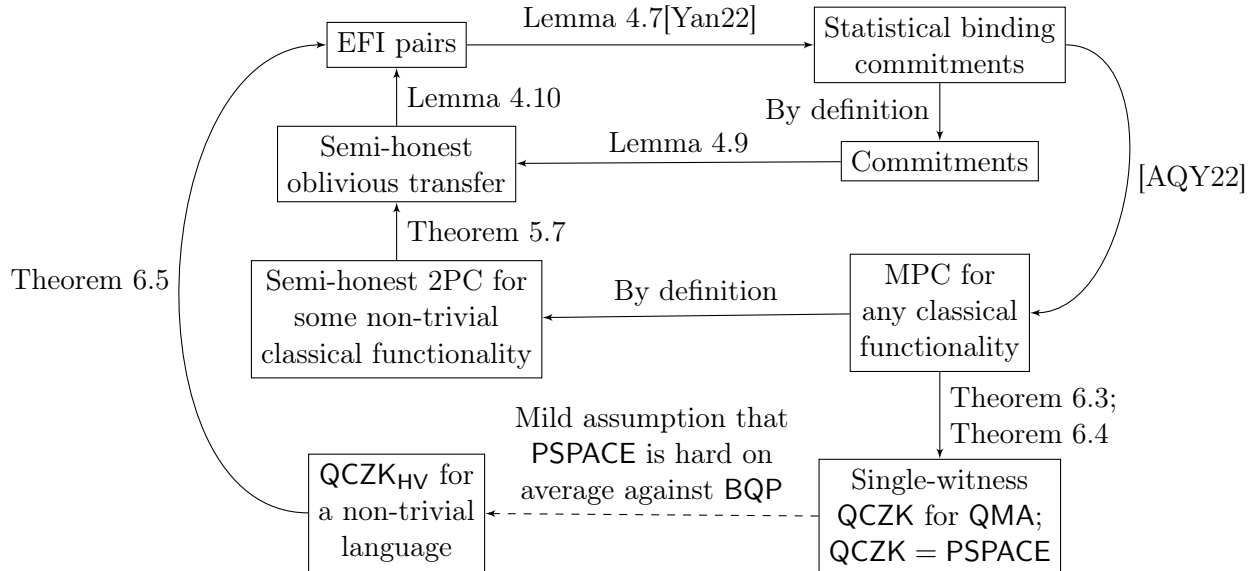
4

Figure 1: Our results for EFI pairs illustrated. We give a more detailed overview of these implications in Section 1.1.

> unitary for committing to b and check if we get back all zeroes) to check whether to accept the commitment.

It is possible to view the purified generation of the EFI pair as a canonical form commitment where the output corresponds to the commitment register C and the purification corresponds to the opening register R. When viewed this way, the statistical distance guarantee of the EFI pair translates to statistical binding property, whereas the computational indistinguishability of the EFI pair translates to the computational hiding property of the commitment. Thus an EFI pair is essentially a statistically binding canonical form commitment. This observation (which is implicit in [Yan22]) is indeed the starting point of our work.

Furthermore, the round collapsing theorem in [Yan22] shows that any quantum commitment can be compiled into the canonical form while preserving the hiding and binding properties. Since statistically binding commitments and statistically hiding commitments are equivalent [CLS01, Yan22], we can construct EFI pairs from either one.

Showing how to construct EFI pairs from commitment schemes that are neither statistically binding nor statistically hiding appears more challenging. One may hope to somehow construct a candidate EFI pair of states, and prove computational indistinguishability from computational security of the commitment, and statistical distance via an inefficient attack on the commitment scheme. However, it is not clear how to transform an inefficient attack against the binding property into a distinguishing attack as needed for EFI pairs. (Classically, this part can be done using one-way functions, but, as argued above, these techniques do not have natural quantum analogues.)

We get around this difficulty by going through oblivious transfer, where the security for both ends can be naturally viewed as distinguishing tasks, and is thus more amenable to constructing EFIs even without statistical security. In fact, we observe that semi-honest OT suffices. Let us elaborate.

5

EFI pairs from semi-honest OT. We first define a new notion of quantum oblivious transfer, which considers only "purification attacks". (This notion can be viewed as a quantum analogue of the classical "non-erasing, honest-but-curious" attacks.) Furthermore, the semi-honest adversaries must run the purified protocol till the end, i.e. are disallowed to abort. (Classically, this does not matter.)

We first describe constructing EFI from semi-honest OT, which is more straightforward. Consider the adversarial view in the following two executions:

- Here the sender is honest and the receiver is semi-honest. The sender chooses the bits uniformly at random and the semi-honest receiver chooses the choice bit uniformly at random. (By correctness, the receiver is always able to recover one bit specified by the choice bit with certainty. The task for the semi-honest receiver is to extract the sender's other bit from his purified view.)
- Here the receiver is honest and the sender is semi-honest. The receiver chooses the choice bit uniformly at random and the semi-honest sender prepares two equal superposition states $|+\rangle^{\otimes 2}$ for her input bits. (Here the task for the semi-honest sender is to extract receiver's choice bit from her purified view.)

It is easy to see that these views can be computed efficiently since the OT protocol is efficient; and by the semi-honest security of OT, both tasks should be impossible for efficient algorithms. At the same time, the impossibility of Chailloux, Gutoski, and Sikora [CGS16] states that for every OT protocol, one of these two tasks can be accomplished with success probability $\geq \frac{2}{3}$ inefficiently.

Now the construction of EFI pairs follows by simply reinterpreting these bit extraction tasks as a distinguishing task. In particular, for $b = 0, 1$, the b-th state is simply the concatenation of the two above views, conditioned on the correct answers being b in both executions. In other words, the b-th state consists of the semi-honest receiver's view of the first execution when the sender's other bit is b, followed by the semi-honest sender's view of the second execution when the receiver's choice bit is b.

Semi-honest OT from commitments. Many prior works have already studied constructing quantum oblivious transfer from commitments [CK88, BBCS91, Cré94, CLS01, FUYZ20, Yan22]. However, they all start with a commitment with some statistical security guarantee – either statistically binding or statistically hiding. On the other hand, we want to start from an arbitrary commitment scheme (which may be computationally binding and computationally hiding). While these constructions could probably still carry over, since here we are aiming for a much weaker security, we instead give a much simplified protocol with a self-contained description. Let us begin by considering the simplest (almost trivial) quantum oblivious transfer protocol inspired by Crépeau and Kilian [CK88], which is only secure if both parties are completely honest during the protocol:

1. The sender on input two message bits b_0, b_1, sends two qubits $|b_0\rangle \otimes H |b_1\rangle$, where the first qubit encodes the first message bit in the standard basis and the second qubit encodes the second message bit in the Hadamard basis.
2. The receiver measures both qubits in the standard basis to recover b_0 and a random bit b_1', or in the Hadamard basis to recover a random bit b_0' and b_1.

Security is straightforward: the sender gets no information at all, and the receiver destroys the information about the other bit by measuring it in an incompatible basis.

However, this is obviously not semi-honest secure as a purified receiver could simply uncompute a purified measurement to recover the other bit as well. Indeed, a better way to "erase" information in the semi-honest model is to simply send it to the other party: in this case, the receiver sends a copy of these two measured (classical) bits to the sender. Since the semi-honest receiver's purified view at the end has the sender's private registers traced out, doing this ensures that these measured bits do indeed collapse even for the purified view.

On the other hand, since these two bits contains information about the receiver's choice bit, we cannot simply send it in the clear as now the sender can break. One simple fix is to have the receiver instead commit to the two measured bits to the sender. This strategy is also often employed when designing maliciously secure OT from commitments [BBCS91, Cré94, CLS01].

It is easy to see that this committed-measurement OT remains secure against semi-honest sender by hiding of the commitment, and security against semi-honest receiver remains to be seen. If the commitment is statistically binding, then it can be seen that the collapse still occurs; but the computational binding case seems less clear. Fortunately, this can be overcome through Yan's computational collapse theorem [Yan22], which on a high level states that a canonical form computationally binding commitment scheme computationally "collapses" the commited qubit (given that the commit phase was performed semi-honestly), even if the commitment is never opened. (Their theorem is established via reducing a collapsing distinguishing adversary to an adversary that breaks computational binding of the canonical form commitment.) This completes the argument.

Multiparty secure computations for classical functionalities. Using a known sequence of transformations outlined in existing works [AQY22] (which builds on existing works including but not limited to [BBCS91, BCKM21, GLSV21]), it is already known how construct, given any statistically binding quantum commitment scheme (and hence also given any EFI pair), multi-party protocols that securely evaluate any classical function with any number of faults. Furthermore, these protocols provide statistical security guarantees against at least one of the parties. As an aside, via known results, these protocols can further be used to construct two-party secure computations for general quantum functions (or channels) where only one party obtains output [DNS12], and in addition, reactive (meaning stateful and interactive) classical functionalities [CGT95, IPS08].

For the converse direction, we can now use the powerful equivalence established for oblivious transfer above, and simply invoke the classical equivalence of Beimel, Malkin, and Micali [BMM99] to complete the proof. While the [BMM99] proof contains parts which do not naturally generalize to the quantum setting, the only thing we need from that proof is the reduction from semi-honest OT to semi-honest 2PC for any non-trivial classical functionality (i.e. if it contains an insecure minor), and this construction is black-box and hence extends to our setting. While the semi-honest models are slightly different, we verify that their semi-honest reduction also works for our model. Once we have semi-honest OT, we get EFI pairs by the equivalence above.

Zero knowledge proofs from EFI pairs. We now turn to establishing an equivalence between EFI pairs and non-trivial quantum computational zero knowledge (QCZK) proofs. We first consider the task of constructing QCZK protocols for QMA from EFI pairs. Here the commit-and-open QCZK protocol by Broadbent and Grilo [BG20] can be readily instantiated by any quantum commitment. However, this protocol uses sequential repetition, and as a consequence, requires multiple copies of the quantum witness to achieve negligible soundness. As also proposed by Broadbent et al. [BJSW20], this limitation can be avoided via performing 2PC for quantum (CPTP) functionali-

ties, which can be constructed from OT [DNS12] and thus EFI pairs.

We now move on to general QCZK proofs without any constraint on prover efficiency and show how to use EFI pairs to construct QCZK proofs for all of QIP. Before presenting our protocol, let us recall the celebrated construction of Ben-Or et al. [BGG$^+$88] that transforms any (without loss of generality, Arthur-Merlin or public-coin) IP protocol into a CZK protocol. In the transformed protocol, the parties first run the original public-coin protocol, where the prover only sends (statistically binding) commitments to its messages. Next, the parties engage in a zero-knowledge protocol where the instance consists of the transcript so far, and the language accepts a transcript if there exist valid openings to all the prover commitments that would have caused the original verifier to accept.

Since QIP = IP [Sha92, JJUW11], it is natural to consider extending the [BGG$^+$88] construction to our setting. However, direct extension hits a roadblock: the statement that needs to be proven in zero knowledge is now a *quantum statement* involving the commitment states when instantiated with quantum commitments. This is not a context that is traditionally considered by the zero knowledge literature. (Indeed, recall that even zero knowledge proofs for QMA still consider classical statements.) Even if we attempt to mimic a zero knowledge proof via statistical 2PC, we soon encounter another issue: how should the two parties agree on the quantum statement that is being proven? Sure, we could make the verifier send the quantum state in the statement to 2PC, but a malicious verifier could refuse to provide the correct state. This becomes an issue as the verifier might be able to manipulate the commitment message so that checking the validity of the commitments itself might reveal non-trivial information about the committed bit.

We thus take a different path: we have the prover and the verifier engage in a secure evaluation of the following reactive functionality (which also can be constructed from OT [CGT95, IPS08]). The verifier inputs its random challenges in the underlying interactive proof, and the functionality uses these challenges to play the verifier role in an interactive proof with the external prover. Finally the functionality outputs the acceptance bit to the external verifier. Both soundness and zero knowledge follow from the security of the MPC.

EFI pairs from non-trivial QCZK$_{HV}$. Finally, we show how to construct EFI pairs from any QCZK proof for any language that is hard on average against BQP. Note that the computational indistinguishability given by the QCZK security does not give EFI pairs immediately as it might be possible to generate the hoenst view efficiently.

One possible approach might be to try to extend the classical result of Ostrovsky and Widgerson [OW93] to our setting. However, they use the non-existence of one way functions to build universal extrapolators that efficiently turn simulators into cheating provers, and it is not clear how to use the non-existence of EFI pairs to construct quantum universal extrapolators.

We instead turn to the works of Ong and Vadhan [Vad06, OV08], showing an equivalence between instance-dependent commitments and CZK, that is a language admits an instance-dependent commitment (a commitment, parameterized by an instance x, whose computational hiding and statistical binding properties only hold if x is in or not in the language, respectively) if and only if it admits a CZK proof. We note that if a hard-on-average language admits an instance-dependent commitment, then this commitment is essentially a full-fledged commitment, thus implying the existence of EFI pairs. Therefore, it remains to extend the equivalence to the quantum setting, i.e. we wish to establish that any language admits a QCZK proof if and only if it admits instance-dependent quantum commitments.

The bad news is that going from CZK to instance-dependent commitments again involve going through instance-dependent one-way (universal hash) functions. However, we note that the mixed states considered by Watrous [Wat02] for handling QSZK readily gives an instance-dependent mixed state for QCZK protocols: a weak variant of EFI states that is only required to satisfy either statistical farness or computational indistinguishability if x is in or not in the language, respectively. It can be seen that the transformations described before also readily extends to the instance-dependent setting, and thus this gives an instance-dependent commitment. Indeed, this transformation from QCZK to instance-dependent quantum commitments has been observed by the work of Yan et al. [YWLQ15]. We then conclude that if L is hard on average for BQP, then this instance-dependent mixed state averaged over the hard distribution immediately gives an EFI pair.

Upon the completion of this work, we discovered a result by Chailloux, Kerenidis, and Rosgen [CKR11] that is similar to this part with very similar proof techniques. However, their separation is between QIP = PSPACE and QMA, which is technically incomparable with our separation between QCZK and BQP. Furthermore, they consider worst case hardness instead of average case hardness here, and thus only getting quantum auxiliary-input EFI. In our case, this difference is rather minor and the results can translate back and forth (see Theorem 6.8); and in their case, it is not clear how to get standard EFI pairs from any notion of average case hardness of QIP against QMA.[4]

1.2 Discussions and open questions

We now give a few open questions in this direction, organized into three categories. To keep the discussion succinct, we point the readers to the references for details of the terminologies.

EFI and quantum complexity. One way functions (and equivalently pseudorandom generators and classical EFID pairs) have been one of the central objects in complexity theory [AB09]. Since EFI pairs are both essential and sufficient for much of quantum cryptography, and furthermore are very simple to describe, it is natural to ask whether EFI pairs could also be a useful object to study from the complexity point of view. Note that the computational hardness underlying EFI pairs, which is the quantum state distinguishability problem, seems especially relevant to the study of the complexity of quantum states and transformations [Aar16].

One very important question, we think, is whether there is any barrier for proving the existence of EFI pairs. In the classical setting, existence of one-way functions implies P $\neq$ NP, but is there any barrier for establishing the existence of quantum EFI pairs? EFI pairs would immediately imply a quantum circuit lower bound for an explicit two-outcome measurement, but is there any reason to believe that such a lower bound would be hard to establish?

For a more concrete example, is P vs PSPACE a (classical) barrier for the existence of EFI pairs? In other words, does the existence of EFI pairs separate BQP from PSPACE? We know that the existence of pseudorandom states do separate BQP from PP = PostBQP [Kre21], but nothing is known for EFI pairs. One way to achieve this could be to demonstrate a way to synthesize the Helstrom measurement given a PSPACE oracle, which is closely related to the unitary synthesis

---

[4]For readers that are familiar with [CKR11], even if we assume QIP is hard on average against QMA for BQP samplable distributions, this still does not suffice for getting EFI pairs without quantum auxiliary input. The reason is that the quantum auxiliary input needs to specify the state that witnesses the diamond norm of the two channels, and it is not clear how this state could be prepared efficiently.

problem [AK07]: in particular, if the unitary synthesis problem could be done by a PSPACE oracle, then the existence of EFI pairs would separate PSPACE from BQP.

Hardness amplification for EFI. Another intriguing challenge is hardness amplification for EFI. Is it possible to construct full-fledged EFI pairs from weaker veriants where either the computational distance is non-negligible, or the statistical distance is bounded away from 1, or both? What is the minimal initial gap between the statistical and computational distances that still allows amplification?

Candidate EFI? Given the oracle separation, are there any concrete candidate assumptions that imply quantum EFI, with formal evidence that it does not imply one-way functions?

Two natural candidates come from pseudorandom state candidates. One possible approach is to assume that "sufficiently large" quantum random circuits are pseudorandom unitaries. These random quantum circuits are already being investigated with motivations like quantum supremacy [AA13, AC17] and the theory of black holes [BS18, BCH$^+$21, HFK$^+$22]. One could hope that pursuing this direction could ultimately lead to useful quantum cryptography that could be implemented on near-term quantum devices. The other possible approach is to consider the pseudorandom states proposed by Bouland, Fefferman, and Vazirani [BFV20] from the physical description of wormholes. Intuitively, such a construction could be secure based on the physical belief that a wormhole is highly "scrambling". In that paper, they also prove that their construction is a secure pseudorandom state generator if the evolution unitary is a black-box Haar random unitary.

Another candidate is proposed by Kawachi, Koshiba, Nishimura, and Yamakami [KKNY12]. On a high level, they consider computational indistinguishability between two types of random coset states, and show that it is at least as hard as the graph automorphism problem.

EFI and quantum cryptography. The importance of one way functions in classical cryptography cannot be overstated: virtually any non-trivial computational cryptography (those that cannot be realized with respect to computationally unbounded adversaries) implies the existence of one way functions classically. Yet it still remains to be seen how much of quantum cryptography is related to EFI. For instance:

Quantum pseudorandomness. The celebrated result of Goldreich [Gol90] shows existence of classical EFI pairs imply pseudorandom generators and subsequently pseudorandom functions. While we know how to construct various quantum cryptography from quantum EFI pairs, the way we do it completely avoids the need to construct quantum pseudorandomness. Nevertheless, given the many applications of both classical and quantum pseudorandomness, an important question is whether it is possible to construct quantum pseudorandomness (pseudorandom states, unitaries, or any other meaningful pseudorandom objects) from EFI pairs.

Quantum unforgeability. Cryptographic primitives such as digital signatures, message authentication codes, or quantum money appear to inherently require some flavor of one-wayness, in that a break involves solving a computationally hard search problem where solutions exist and are efficiently verifiable given some additional secret information. (In the public key setting, where some classical verification key is made public, solutions are verifiable publicly.) Another related object already proposed previously is one-way state generators [MY22]. As discussed, this form of computational hardness appears very different than indistinguishability. Still, can

we show that existence of any one of these primitives implies existence of EFI pairs? Can we construct any of these primitives from EFI pairs?

Quantum zero knowledge arguments. It is possible to extend our proof (Theorem 6.3) to show that if EFI pairs exist then we can give a QSZK argument for any QMA language with an efficient prover having a single copy of the witness. On the other hand, we are unable to show that if L admits an argument then the instance-dependent commitment constructed in Theorem 6.7 is computationally binding for NO instances. On a high level, the difficulty is that known techniques in the statistical binding setting do not translate to the computational setting, since we do not have a hardness amplification procedure for computationally binding commitments: it is not clear whether parallel repetition of commitments decreases the computational binding error against malicious committers. We refer the readers to the related discussions in Yan's work [Yan22] for more details.

2   Preliminaries

2.1   Quantum information

We refer the reader to [NC10] for a comprehensive reference on the basics of quantum information and quantum computation. We use standard Dirac notation for quantum states.

We recall the notion of density matrices, which are PSD trace-1 matrices that represent the complete characterization of a state of a quantum system. The state of a system can be "pure", i.e. in the form of a state $|\psi\rangle$, in which case the density matrix is $|\psi\rangle\langle\psi|$ (i.e. of rank 1), or "mixed" which corresponds to a distribution over pure states, and is represented by a density matrix of rank > 1. Two quantum states are identical if and only if their density matrices are equal, and the distance between quantum states is also expressed as a function of their density matrices, as explained below.

We recall that quantum operations can always be expressed as unitary operators on *some* quantum system, and they act on the density matrix of this quantum system via conjugation. We may sometimes refer to a quantum operation that uses some auxiliary registers, or that removes ("traces out") registers during the computation. Such a general quantum operation is known as a *quantum channel*. (Mathematically, a quantum channel can be expressed as a completely-positive trace-preserving (CPTP) map on the space of density matrices, but this formulation will not be required for our purposes.)

We use $\mathcal{D}(\mathcal{H})$ to denote the set of density matrices on a Hilbert space $\mathcal{H}$. Let $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ be density matrices. We write $\mathrm{TD}(\rho, \sigma)$ to denote the trace distance between them, i.e.,

$$\mathrm{TD}(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1$$

where $\|X\|_1 = \mathrm{Tr}(\sqrt{X^\dagger X})$ denotes the trace norm. We also use $F(\rho, \sigma) = \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right)^2$ to denote the fidelity of ρ and σ.

Fact 2.1. *For any two mixed states ρ, σ, $(F(\rho, \sigma))^2 + (\mathrm{TD}(\rho, \sigma))^2 \leq 1$.*

Theorem 2.2 (Holevo–Helstrom [Hol73, Hel69])**.** *The best success probability to (inefficiently) distinguish two mixed states ρ, σ is given by $\frac{1}{2}(1 + \mathrm{TD}(\rho, \sigma))$. The measurement that achieves this success probability is called the* Helstrom measurement.

Corollary 2.3. *For any mixed states ρ, σ and integer $n > 0$,*

$$\mathrm{TD}(\rho^{\otimes n}, \sigma^{\otimes n}) \geq 1 - \exp(-n\,\mathrm{TD}(\rho, \sigma)/2).$$

We recall that $\rho^{\otimes n}$ is the state containing n-copies of the state represented by ρ.

Proof. We prove this by building a majority-vote distinguisher. Let D be the distinguisher optimally distinguishing ρ from σ by Holevo–Helstrom theorem. We apply D on each copy, and take the majority vote. Corollary follows by applying Hoeffding's inequality and Holevo–Helstrom again. $\qquad\square$

2.2 Quantum algorithms

A quantum algorithm A is a family of generalized quantum circuits $\{A_n\}_{n\in\mathbb{N}}$ over a discrete universal gate set (such as $\{CNOT, H, T\}$). By generalized, we mean that such circuits can have a subset of input qubits that are designated to be initialized in the zero state, and a subset of output qubits that are designated to be traced out at the end of the computation. Thus a generalized quantum circuit A_n corresponds to a *quantum channel*. When we write $A_n(\rho)$ for some density matrix ρ, we mean the output of the generalized circuit A_n on input ρ. If we only take the quantum gates of A_n and ignore the subset of input/output qubits that are initialized to zeroes/traced out, then we get the *unitary part* of A_n, which corresponds to a unitary operator which we denote by $\hat{A}_n$. The *size* of a generalized quantum circuit is the number of gates in it, plus the number of input and output qubits.

We say that $A = \{A_n\}_n$ is a *quantum polynomial-time (QPT) algorithm* if there exists a polynomial p such that the size of each circuit A_n is at most $p(n)$. We furthermore say that A is *uniform* if there exists a deterministic polynomial-time Turing machine M that on input 1^n outputs the description of A_n.

We also define the notion of a *non-uniform* QPT algorithm A that consists of a family $\{(A_n, \rho_n)\}_n$ where $\{A_n\}_n$ is a polynomial-size family of circuits (not necessarily uniformly generated), and for each n there is additionally a subset of input qubits of A_n that are designated to be initialized with the density matrix ρ_n of polynomial length. This is intended to model nonuniform quantum adversaries who may receive quantum states as advice.

The notation we use to describe the inputs/outputs of quantum algorithms will largely mimic what is used in the classical cryptography literature. For example, for a state generator algorithm G, we write $G_n(k)$ to denote running the generalized quantum circuit G_n on input $|k\rangle\langle k|$, which outputs a state ρ_k.

Ultimately, all inputs to a quantum circuit are density matrices. However, we mix-and-match between classical, pure state, and density matrix notation; for example, we may write $A_n(k, |\theta\rangle, \rho)$ to denote running the circuit A_n on input $|k\rangle\langle k| \otimes |\theta\rangle\langle\theta| \otimes \rho$. In general, we will not explain all the input and output sizes of every quantum circuit in excruciating detail; we will implicitly assume that a quantum circuit in question has the appropriate number of input and output qubits as required by context.

We assume that all parties are quantum algorithms with (noiseless) quantum communication. Furthermore, all algorithms run with the same security parameter.

A function $f : \mathbb{N} \to \mathbb{R}^{\geq 0}$ is negligible, if for any polynomial p, $f(\lambda) \leq 1/p(\lambda)$ for all sufficiently large $\lambda \in \mathbb{N}$. Otherwise, we say it is noticeable, or equivalently when it is infinitely often at least $1/p(\lambda)$.

Definition 2.4 (Computational indistinguishability). *For two families of mixed states $\{\rho_\lambda\}_\lambda, \{\sigma_\lambda\}_\lambda$, we say that they are computationally indistinguishable (against* BQP/qpoly*), if for any QPT algorithm D, there exists a negligible function ε such that for any security parameter λ and advice state $\alpha = (\alpha_\lambda)_\lambda$,*

$$|\Pr[D(\alpha_\lambda, \rho_\lambda) = 1] - \Pr[D(\alpha_\lambda, \sigma_\lambda) = 1]| \leq \varepsilon(\lambda).$$

Extending the standard cryptographic convention, the above definition considers adversaries with non-uniform quantum advice. The definition can be adapted to the uniform setting by simply requiring fixing $\alpha = \perp$. We note that the reductions shown in this work are all uniform, or "advice preserving": given an adversary with some advice, the generated adversary uses the same advice.

3 EFI pairs of states

We define the main object considered in this work, namely pairs of efficiently generatable mixed quantum states that are statistically far and yet computationally indistinguishable:

Definition 3.1. *We call $\xi = (\xi_{b,\lambda})$ a pair of EFI states if it satisfies the following criteria:*

1. ***Efficient generation****: There exists a uniform QPT quantum algorithm A that on input $(1^\lambda, b)$ for some integer λ and $b \in \{0, 1\}$, outputs the mixed state $\xi_{b,\lambda}$.*
2. ***Statistically Far****: $\mathrm{TD}(\xi_{0,\lambda}, \xi_{1,\lambda})$ as a function of λ is at least inverse polynomial.*
3. ***Computational Indistinguishability****: $(\xi_{0,\lambda})_\lambda$ is computationally indistinguishable to $(\xi_{1,\lambda})_\lambda$.*

Here we require exact generation of the mixed state. Since we only care about the existence of such object, this requirement does not make a difference. In particular, if we can approximately synthesize a certain family of states with inverse-exponential fidelity, then taking the output of the circuit directly would also satisfy the requirement.

4 Commitments and semi-honest oblivious transfer

4.1 Commitments

In this work, we without loss of generality focus on the canonical form of quantum commitment schemes [Yan22, Definition 5]. A commitment scheme consists of two phases. In the commitment phase of a canonical commitment scheme, Alice (the committer) chooses a bit b, and runs a uniform QPT circuit $Q_{\lambda,b}$ on all zeroes, which outputs two registers C, R; she then proceeds to send the register C to Bob (the receiver). Later in the reveal phase, Alice sends the other register R and the bit b to Bob; Bob accepts the opening if he performs $Q_{\lambda,b}^\dagger$ on two registers and measures all zeroes in the computational basis. We now recall the requirements on the commitment schemes, specialized to canonical forms for convenience. It will be convenient to define the commitment message $\rho_{\lambda,b} := \mathrm{Tr}_\mathsf{R}(Q_{\lambda,b} |0\rangle\langle 0| Q_{\lambda,b}^\dagger)$.

Definition 4.1 (Computational hiding). *A commitment scheme satisfies computational hiding, if $\rho_{\lambda,0}$ is computationally indistinguishable to $\rho_{\lambda,1}$.*

We are going to consider a specific more restricted variant of statistical binding called honest binding. We refer the readers to related works [YWLQ15, FUYZ20, MY22, Yan22] for a more thorough discussion on this variant (and how it is equivalent to statistical binding for canonical commitment schemes).

Definition 4.2 (Honest binding). *A canonical commitment scheme satisfies honest computational (resp. statistical) binding if for any auxiliary state $|\psi\rangle$ and any polynomial-time (resp. physically) realizable unitary U, we have that*

$$\left\| \left(Q_{\lambda,1} \, |0\rangle\langle 0|_{\mathsf{CR}} \, Q_{\lambda,1}^\dagger \otimes I_{\mathsf{Z}} \right) \left(I_{\mathsf{C}} \otimes U_{\mathsf{RZ}} \right) \left(Q_{\lambda,0} \, |0\rangle_{\mathsf{CR}} \otimes |\psi\rangle_{\mathsf{Z}} \right) \right\|_2$$

is negligible.

4.2 Oblivious transfer and semi-honest adversaries

In an oblivious transfer protocol, Bob (the sender) chooses two bits x_0, x_1 to send to Alice, and Alice (the receiver) chooses the bit b to receive. At the end of the protocol, Alice is able to recover x_b. Here, we assume the protocol is able to transmit x_b with probability 1.

Here, we say a (quantum) party is semi-honest (or secure against purified adversaries, analogous to the classical honest-but-curious security), if they follow the protocol (without abort) except that they can purify (without loss of generality) all measurements. We in addition also allow Bob (the sender) to purify his randomness for x_0, x_1 if he was to sample them randomly; on the other hand, we require Alice (the receiver) to specify a classical input to make it easier to define security. (Looking ahead, this is also needed to invoke the semi-honest inefficient attack [CGS16].) At the end, they output their residual state as their view for the distinguisher as usual.

Definition 4.3 (Statistical security against semi-honest Alice). *We say an oblivious transfer protocol is P_A^*-secure against semi-honest Alice, if for every bits b, c, at the end of the protocol with Alice's input being b, a semi-honest Alice's view when $x_b = c$ and $x_{1-b} = 0$ is at most P_A^*-close to that when $x_b = c$ and $x_{1-b} = 1$ in trace distance.*

Definition 4.4 (Statistical security against semi-honest Bob). *We say an oblivious transfer protocol is P_B^*-secure against semi-honest Bob, if for every possible (purified) Bob's inputs (meaning an arbitrary bipartite quantum state where the first part is a qubit indicating the input choice bit), at the end of the protocol, a semi-honest Bob's view when $b = 0$ is at most P_B^*-close to that when $b = 1$ in trace distance.*

Computational security against semi-honest Alice and Bob can be similarly defined, except considering these two views to be computationally indistinguishable instead of statistically indistinguishable.

We recall the impossibility due to Chailloux, Gutoski, and Sikora showing that oblivious transfer protocols that are statistically secure against both parties do not exist. While the "semi-honest" definition they have is different from here, we could open the proof and check that the cheating strategies constructed there are indeed semi-honest according to our definition.

Theorem 4.5 ([CGS16, Theorem 1.1]). *For any oblivious transfer protocol, it holds that $2P_B^* + P_A^* \geq 2$, where Alice chooses the choice bit uniformly at random (classically) and Bob chooses the two bits as uniform superposition $\left(\frac{1}{2} \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right) \right)$, and P_A^* is the best probability that a semi-honest Alice is able to predict Bob's choice correctly, and P_B^* is the best probability that a semi-honest Bob is able to predict both bits being sent by Alice correctly.*

We briefly recall the cheating strategies constructed in their proof. Alice's strategy is the following [CGS16, Section 2.1]: she randomly chooses b and then follows the protocol semi-honestly

according to our definition; at the end, she performs a gentle measurement to learn x_b (it is gentle since by completeness she is supposed to be able to learn x_b with almost certainty), and then performs the Helstrom measurement (Theorem 2.2) to learn x_{1-b}. Similarly, Bob's strategy is the following [CGS16, Section 2.2]: he follows the protocol semi-honestly, purifying all measurements including the uniform sampling of x_0, x_1; at the end, he performs a post-processing to try to guess b. Let the success probability of Alice and Bob be p_a, p_b respectively. They establish that for these two strategies, $2p_b + p_a \geq 2$, and thus the theorem follows.

4.3 Equivalence theorem

Theorem 4.6. *The following assumptions are equivalent.*

1. *Existence of EFI states.*
2. *Existence of statistically binding (canonical-form) commitment schemes.*
3. *Existence of commitment schemes.*
4. *Existence of semi-honest oblivious transfer.*

Proof. $1 \Rightarrow 2$ is shown in Lemma 4.7. $3 \Rightarrow 4$ is shown in Lemma 4.9. $4 \Rightarrow 1$ is shown in Lemma 4.10. Finally, $2 \Rightarrow 3$ is trivial. $\square$

Lemma 4.7. *Assuming the existence of pairs of EFI states, there exists statistically binding commitments.*

Proof. Let A_0, A_1 be the two quantum channels that generate two parts of the EFI state pair respectively. Without loss of generality, we assume that their statistical distance is negligibly close to 1, in particular, at least $1 - e^{-\lambda/2}$ — by Corollary 2.3, let $\delta = \mathrm{TD}(A_0(1^\lambda), A_1(1^\lambda))$, then taking λ/δ copies of their outputs suffices since $1/\delta$ by assumption is polynomial; on the other hand, computational indistinguishability still holds by a straightforward hybrid argument.

Let the unitary part of $A_i(1^\lambda)$ be $\hat{A}_i$ for $i = 0, 1$, which acts on registers CR where the output register is C and the auxiliary register is R. The construction of canonical bit commitment scheme is simply running the unitary part as specified above.

It is easy to see that this scheme satisfies computational hiding since by construction $A_b(1^\lambda) = \mathrm{Tr}_\mathsf{A}\left(A_b \, |0\rangle\langle 0| \, A_b^\dagger\right)$ and thus Bob after the commitment phase sees exactly $A_b(1^\lambda)$. On the other hand, since by Fact 2.1,

$$F\left(A_0(1^\lambda), A_1(1^\lambda)\right) \leq \sqrt{1 - (\mathrm{TD}(A_0(1^\lambda), A_1(1^\lambda)))^2} \leq \sqrt{2} e^{-\lambda/4}$$

is negligible, it also satisfies honest-binding by Uhlmann's theorem. Finally, it is known that honest binding for canonical form commitment schemes do imply the more general statistical binding property [Yan22, Theorems 2 and 3]. $\square$

To construct semi-honest oblivious transfer from commitments, we need the following lemma by Yan, which is originally developed to use computational binding property of a canonical form commitment in order to construct statistically binding quantum commitments from statistically hiding quantum commitments. On a high level, it reduces the collapsing property of an honest commitment to the computational binding property.

Lemma 4.8 (Computational collapse theorem [Yan22, Theorem 8]). *Let Q a canonical computationally binding quantum bit commitment scheme. Then for every polynomial m, and every normalized quantum state $\sum_{s \in \{0,1\}^m} \alpha_s |s\rangle |\psi_s\rangle$ (of polynomial length), every projector Π,*

$$\left| \left\| \Pi \sum_{s \in \{0,1\}^m} \alpha_s |s\rangle (Q_s |0\rangle)_{\mathsf{CR}^{\otimes m}} |\psi_s\rangle \right\|^2 - \sum_{s \in \{0,1\}^m} \|\alpha_s \Pi |s\rangle (Q_s |0\rangle)_{\mathsf{CR}^{\otimes m}} |\psi_s\rangle\|^2 \right|$$

is negligible, given that Π does not act on the registers $\mathsf{C}^{\otimes m}$ and is efficient.

Lemma 4.9. *Assuming the existence of commitment schemes, there exists a two-message semi-honest quantum oblivious transfer.*

Proof. The semi-honest oblivious transfer scheme is the following. The sender, on input x_0, x_1, sends $|x_0\rangle \otimes H |x_1\rangle$; in other words, the sender encodes x_0 in the standard basis and x_1 in the Hadamard basis and send these two qubits to the receiver. The receiver measures both qubits in standard basis if $b = 0$, or in Hadamard basis if $b = 1$. Let x_0, x_1 be the measurement outcomes. The receiver commits to both of them using the commitment scheme in canonical form[5], and outputs x_b.

Semi-honest security against semi-honest sender is easy to see, by a simple hybrid argument invoking the hiding property of the commitment twice, replacing each commitment to committing to 0; furthermore, this reduction even extends if the sender chooses an arbitrary purified input. Semi-honest security against receiver follows immediately from collapsing. Formally, without loss of generality, we assume the choice bit $b = 0$ and thus the receiver should measure in the standard basis. As the goal of the adversary is to extract x_1, we can for simplicity remove x_0 from the view. The second qubit (denoted by register X) the receiver sends is $\frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_1} |1\rangle)$. After the purified protocol concludes, the probability of an efficient distinguisher outputting 1 is

$$\left\| \Pi \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x_1 y} |y\rangle (Q_y |0\rangle)_{\mathsf{CR}} |\psi_y\rangle \right\|^2$$

for some auxiliary states $|\psi_0\rangle, |\psi_1\rangle$ (possibly containing the distinguisher's advice and auxiliary registers), where Π denotes the projector for the distinguisher outputting 1 acting on everything but the C register. By the computational collapse theorem, this is negligibly close to

$$\frac{1}{2} \sum_{y \in \{0,1\}} \left\| \Pi |y\rangle (Q_y |0\rangle)_{\mathsf{CR}} |\psi_y\rangle \right\|^2,$$

which is independent of x_1. This concludes the proof. $\qquad\square$

We remark that we construct semi-honest OT here instead of considering the CLS scheme directly because (1) semi-honest OT suffices for the following lemma but also (2) as observed by Yan [Yan22], it is not clear whether the CLS scheme indeed satisfy malicious (indistinguishability) security when instantiated with a commitment scheme that is only computationally binding but not statistically binding nor extractable, due to the difficulties in using computational binding for a quantum commitment scheme.

---

[5]We use canonical form only because we want the commitment to be non-interactive. Even if it is an interactive quantum commitment, everything else could still be extended minus the round complexity.

Also this semi-honest OT protocol fully intentionally ends with a receiver message to erase the information about the other bit from the distinguisher. For a classical OT, if the last message comes from a receiver, it can always be removed without impacting the scheme (semi-honest or malicious); this is certainly not the case here.

Finally, this protocol has the minimum round complexity for semi-honest OT. This can be seen from the following argument. Even with trusted setup, 1-message protocols are impossible: the message has to be sent by the sender as otherwise the receiver cannot recover the output; however, this means that a semi-honest receiver can always extract both bits efficiently via correctness and gentle measurement. Without trusted setup, 1-round protocols (two parties exchanging a single message simultaneously) are also impossible: this can be seen as the receiver message is useless and thus reduces to the impossibility above. Finally, if the sender and the receiver share two EPR pairs, then there is a variant of the protocol above that is 1-round: the receiver is the same but acts on his halves of EPR pairs instead of sender's message, and the sender measures his part of EPR pairs, the first qubit in standard basis and the second qubit in Hadamard basis, obtaining y_0, y_1, and send $x_0 \oplus y_0, x_1 \oplus y_1$ to the receiver. The correctness and security of this protocol can be argued with the same proof techniques as above.

Lemma 4.10. *Assuming the existence of semi-honest oblivious transfer, there exists a pair of EFI states.*

Proof. Let us consider both parties to be semi-honest, i.e. purifying all the measurements. Then their final state would be given by $U_{x_0,x_1,b} |0\rangle_{\mathsf{AB}}$, for some efficient unitaries $U_{x_0,x_1,b}$ for $x_0, x_1, b = 0, 1$, and at the end Alice holds register A and Bob holds register B. By Theorem 4.5, we know that either $P_A^* \geq \frac{2}{3}$ or $P_B^* \geq \frac{2}{3}$ for every security parameter λ. In particular, either a semi-honest Alice who chooses the choice bit uniformly at random could achieve P_A^*, or a semi-honest Bob who chooses the two input bits to be uniform superposition could achieve P_B^*.

Fix any security parameter λ. If $P_A^* \geq \frac{2}{3}$, we construct EFI generators G_y for $y = 0, 1$ that outputs

$$\frac{1}{2} \cdot \operatorname*{Tr}_{\mathsf{B}}\left(\mathbb{E}_x \left[|0\rangle\langle 0| \otimes U_{x,y,0} |0\rangle\langle 0| U_{x,y,0}^\dagger + |1\rangle\langle 1| \otimes U_{y,x,1} |0\rangle\langle 0| U_{y,x,1}^\dagger \right] \right).$$

Note that G_y is exactly Alice's view when she chooses a random choice bit (and remembers the bit in the first register), and Bob sends y in the other slot not chosen by Alice, and thus computational indistinguishability follows by semi-honest security of oblivious transfer. On the other hand, they are statistically far since there exists a distinguisher that achieves advantage at least $\frac{1}{6}$ by our assumption.

Otherwise if $P_B^* \geq \frac{2}{3}$, we construct EFI generators H_b for $b = 0, 1$ that outputs $\operatorname{Tr}_{\mathsf{A}}(|\phi_b\rangle\langle\phi_b|)$, where $|\phi_b\rangle$ is defined to be

$$\frac{1}{2} \sum_{x,y} (U_{x,y,b} |0\rangle)_{\mathsf{AB}} \otimes |x\rangle |y\rangle .$$

Note that H_b is exactly Bob's view when Alice wants to choose the slot b, and thus computational indistinguishability follows by semi-honest security of oblivious transfer. On the other hand, they are statistically far since there exists a distinguisher that achieves advantage at least $\frac{1}{6}$ by our assumption.

Putting everything together, we get that $G_0 \otimes H_0$ and $G_1 \otimes H_1$ generate EFI pairs: statistical farness follows as at least one of G_b, H_b have trace distance $\geq \frac{1}{6}$ for all security parameters, and computational indistinguishability follows from a direct hybrid argument. $\square$

5   Dichotomy for secure two party computations

In this section, we study secure two party computations with quantum parties for classical functionalities. A secure two-party computation protocol consists of two (interactive uniform quantum) algorithms A, B, where they receive (implicitly) the security parameter λ and their respective inputs a, b, take turns to run and exchange a message register back and forth; in the end, we denote their joint state as $\langle A, B \rangle (a, b)$. We can also denote Alice's state to be $\langle A, B \rangle (a, b)_A$ and Bob's to be $\langle A, B \rangle (a, b)_B$. Without loss of generality, we consider the protocol so that only Bob gets the output and otherwise they do not learn any other information [BMM99, Definition 1]. In this case, $\langle A, B \rangle (a, b)$ would simply be $(\bot, z)$ as Alice outputs nothing and Bob outputs the evaluated result z. In particular, this evaluated result could be the output of any efficient quantum channel [DNS12]. We can also define the output state $\langle A^*, B \rangle (a, b)$ for a malicious Alice (and analogously for Bob), where the malicious Alice can output anything she wants and not necessarily $\bot$.

We now describe the definition for malicious simulation security.

Definition 5.1 (Malicious simulation security). *Let $f = (f_\lambda)_\lambda$ be a quantum channel computable by a polynomial-size quantum circuit. A protocol computing f satisfies malicious simulation security for Alice, if the following holds. For any (malicious) QPT algorithm A^*, there exists a QPT simulator S such that for any QPT distinguisher D, there exists a negligible function ε such that for all security parameter λ, non-uniform bipartite advice state ρ_{AD}, and Bob's input b (permissible by f_λ),*

$$|\Pr[D(\langle A^*, B \rangle (\rho_A, b), \rho_D) = 1] - \Pr[D(S_f(\rho_A, b), \rho_D) = 1]| \leq \varepsilon(\lambda),$$

where $S_f(\rho_A, b)$ is the following algorithm:

- *The two-stage algorithm $S(1^\lambda, \rho_A)$ is run, which outputs some a^*.*
- *Compute $(z_a, z_b) \leftarrow f_\lambda(a^*, b)$ to be the output of f. (In our setup, $z_a = \bot$ but z_b is the actual output.)*
- *Finish executing S with input z_a, which in the end outputs a certain state σ.*
- *Output (σ, z_b).*

Malicious simulation security for Bob can be defined in the same way as above, except exchanging the role of Alice and Bob.

We say the malicious simulation security is statistical if it holds even against any unbounded algorithms A^* and D, and in this case there need not be a running time bound on the simulator.

In this work, we focus on secure two-party computations although the consequences also generalize to secure multi-party computations where possibly more than two parties are involved and all of them could receive outputs. We refer the readers to the prior work [BCKM21] for related literature.

Combining our equivalence theorem from before and existing work constructing one-sided statistically secure 2PC from statistically binding (quantum) commitments [BCKM21, AQY22, WW06], we immediately get the following corollary.

Corollary 5.2. *Assuming EFI state pairs exist, then any P/poly functionalities can be computed with full malicious security and one-sided statistical security.*

For the rest of the section, we show EFI states are also implied by non-trivial 2PC protocols. For that purpose, we focus on 2PC protocols for finite functionalities. By "finite", we mean that the

function to be computed is a fixed-size function independent of the security parameter, say Yao's millionaires' problem.

Definition 5.3 (Insecure minor). *Let S_1, S_2, S_3 be finite sets and $f : S_1 \times S_2 \to S_3$ be a (finite) function. Then we say f contains an insecure minor, if there exists $x_0, x_1 \in S_1$ and $y_0, y_1 \in S_2$ such that $f(x_0, y_0) = f(x_1, y_0)$ and $f(x_0, y_1) \neq f(x_1, y_1)$.*

Lemma 5.4 ([BMM99, Claim 1]). *If a function $f(\cdot, \cdot)$ does not contain an insecure minor, then there is a classical one-message perfectly secure computation protocol for f.*

Lemma 5.5. *If a function $f(\cdot, \cdot)$ contains an insecure minor, then we can build an semi-honest OT protocol from an semi-honest secure computation protocol for f.*

Proof. This essentially follows from the work of Beimel, Malkin, and Micali [BMM99, Claim 3]. Since the original proof is black-box, it also immediately generalizes to our setting when the parties are quantum. As the precise definition of semi-honest is different in our case, we give the proof for completeness.

Let x_0, x_1, y_0, y_1 be the values guaranteed by the insecure minor, and let Π_f be the semi-honest secure computation protocol for f. The (semi-honest) oblivious transfer protocol described in that proof works as follows:

- (Recall) Alice gets as input a_0, a_1 and Bob gets as input a choice bit b.
- Execute Π_f on input x_{a_0}, y_{1-b}, and Bob gets output z_0.
- Execute Π_f on input x_{a_1}, y_b, and Bob gets output z_1.
- Bob outputs 0 if $z_b = f(x_0, y_1)$, otherwise Bob outputs 1.

Correctness follows directly since the construction is black-box. A semi-honest Alice's view only consists of her semi-honest view from two protocol executions, and thus Alice does not learn anything about b. Similarly, a semi-honest Bob's view only consists of his semi-honest view from two protocol executions, and thus semi-honest security also follows from the property of insecure minor and Alice's privacy against semi-honest Bob for Π_f. □

Combining this with Theorem 4.5, we immediately get the following:

Corollary 5.6. *If a function $f(\cdot, \cdot)$ contains an insecure minor, then f cannot be computed by statistically-secure semi-honest protocols.*

Combining our equivalence theorem with Lemmas 5.4 and 5.5, we obtain the following dichotomy theorem. We shall remark that this theorem, similar to the classical proof [BMM99], is non-black-box in the use of the functionalities [CK88, Kil91, KKMO00] due to the use of the equivalence theorem.

Theorem 5.7. *If there is a semi-honest two-party secure computation protocol for a classical finite functionality $f(\cdot, \cdot)$, then either f can be computed perfectly securely in a single message or EFI states exist.*

6 Quantum computational zero knowledge proofs

The existence of one-way functions implies that all of PSPACE admit a computational zero knowledge proof [BGG+88, Sha92], and NP admits computational zero-knowledge proofs where proofs can be efficiently generated given a witness for membership [GMW86]. Furthermore, the existence of computational zero-knowledge proofs for *any* non-trivial (i.e., average-case easy) language implies the existence of (infinitely-often) one-way functions [OW93]. In this section, we use our equivalence theorem to establish the quantum analogue of these classical results.

Definition 6.1. *A language L is in QCZK if there is a (quantum) interactive protocol between an unbounded prover and a QPT verifier (specified by an interactive quantum Turing machine V) such that the following holds:*

- *Completeness: For any $x \in L$, there is an unbounded prover strategy P that would make V accept with probability at least $1 - 2^{|x|}$.*
- *Soundness: For any $x \notin L$ and any unbounded prover strategy, V accepts with probability at most $2^{|x|}$.*
- *Computational zero knowledge: For any malicious QPT verifier V^*, there exists a QPT simulator S such that for any QPT distinguisher D and non-uniform bipartite advice state ρ_{AD}, there exists a negligible function ε such that for any $x \in L$,*

$$|\Pr[D(\langle P, V^*(\rho_A)\rangle(x,x)_{V^*}, \rho_D) = 1] - \Pr[D(S(x, \rho_A), \rho_D) = 1]| \leq \varepsilon(|x|).$$

We can also consider a (much) weaker variant of this zero knowledge requirement called computationally zero knowledge against purified verifiers *with abort* (or "honest verifier"), where we restrict the malicious V^* to only purifying his state and aborting after any fixed number of rounds[6]. We call the corresponding class QCZK$_{HV}$, similar to QSZK$_{HV}$ with respect to QSZK for statistical zero knowledge [Wat02].

Note that here, unlike semi-honest OT where we disallow a semi-honest party to prematurely abort, here we must allow a purified verifier to abort prematurely (this makes the complexity class smaller). This is because otherwise we can even show the corresponding class (for even quantum *perfect* zero knowledge) is trivially equal to IP, by simply asking the IP verifier at the end to destroy all the other information he has learned by measuring them in Hadamard basis and then returning them to the prover.

Fact 6.2 ([Sha92, Wat02, JJUW11] and Theorem 6.7). BQP $\subseteq$ QSZK = QSZK$_{HV}$ $\subseteq$ QCZK = QCZK$_{HV}$ $\subseteq$ QIP = IP = PSPACE.

6.1 With EFI, everything provable is provable in QCZK

We first consider QCZK protocols with efficient provers (in which case the largest complexity class we can consider is QMA), and then move on to QCZK with inefficient provers. The work by Broadbent and Grilo on QCZK [BG20] show how to build a commit-and-open zero knowledge protocol for QCZK using a commitment scheme, and thus combining it with a quantum commitment scheme, we get a QCZK proof, but it requires multiple copies of the advice to boost the soundness to negligible. We

---

[6]Formally, we require that for a k-round protocol, there exists a simulator S whose output is computationally indistinguishable to $\rho_1 \otimes \cdots \otimes \rho_k$, where ρ_i for $i \in [k]$ is the purified verifier's state immediately after receiving i-th message from the prover.

strengthen this to show that we can achieve the same thing from the same assumption, but with a single copy of the witness.

Theorem 6.3. *If EFI states exist, then any language in* QMA *has a quantum computational zero knowledge proof with negligible soundness and with an efficient prover that uses only a single copy of the witness.*

Proof. By our equivalence theorem, we get maliciously-secure quantum 2PC for any *quantum* functionality (any quantum channel) with one-sided statistical security via existing works [DNS12]. Formally, the protocol is simply the prover and the verifier engaging in the following secure two-party computation for the following quantum functionality that is statistically secure against the prover:

- Prover's input: The witness state.
- Verifier's input: None.
- The functionality computes whether the amplified verifier (so that the completeness-soundness gap is exponentially close to 1 [MW05]) accepts the witness. If so then output 1 to the verifier, otherwise output 0. The prover gets no output.

Completeness follows from the correctness of 2PC. Soundness follows from the statistical security of 2PC; in particular, we can extract the witness used by the prover and have the guarantee that this extracted witness passes verification with probability negligibly different from the success probability of the original malicious prover. For zero knowledge, we simply tell the 2PC simulator to simulate the malicious verifier's view given the ideal functionality outputting 1. Since the amplified verifier has completeness exponentially close to 1, the output of 2PC is unchanged with overwhelming probability, and thus invoking the security of 2PC, this change is computationally indistinguishable. □

Theorem 6.4. *If EFI states exist, then* QCZK = QIP.

Proof. By our equivalence theorem, we get a maliciously-secure quantum 2PC for any (classical) *reactive* functionality with one-sided statistical security via existing works [CGT95, IPS08]. By reactive, we mean that the functionality can interact with the two parties and keep private states. Given any language $L \in$ QIP, let Π be a (classical many-round) Merlin–Arthur interactive proof protocol for L with completeness 1. The zero knowledge protocol is simply the prover and the verifier engaging in the following secure two-party computation for the following reactive functionality that is statistically secure against the prover:

- Π is executed in the following way: for every prover message, the functionality remembers the message and only sends $\top$ to the verifier; and for every verifier message, the functionality forwards it to the prover. (Both parties are able to participate in the protocol as usual since the prover sees all the messages and the verifier only needs to flip random coins.)
- At the end, if the verifier for Π accepts the transcript, we output 1 to the verifier; otherwise we output 0. The prover gets no output.

Similarly as before, completeness follows from completeness of Π and the correctness of 2PC. Soundness follows from the soundness of the original IP protocol and the statistical security of 2PC; in particular, we can use the 2PC simulator to come up with a malicious prover for Π and have the guarantee that this malicious prover has success probability negligibly different from the success

probability of the original malicious prover. For zero knowledge, we simply invoke the 2PC simulator for the verifier, and tell the simulator that the ideal functionality outputs 1. Since the protocol has completeness 1, the output of 2PC is unchanged no matter what the verifier's input is, and thus invoking the security of 2PC, this change is computationally indistinguishable. □

6.2 EFI pairs are essential for non-trivial QCZK

Theorem 6.5. *If there is a language in* $\mathsf{QCZK_{HV}}$ *that is hard on average for* BQP *for some* BQP-*samplable distribution D, i.e. any* BQP *algorithm has negligible success probability in deciding L on average over D and the algorithm's randomness, then EFI state pairs (secure against uniform* BQP *adversaries) exist.*

As is the classical case [OW93], the other direction is more involved. Since we could not use one-way functions like the classical proof, we instead use ideas from the works of Ong and Vadhan [Vad06, OV08]. On a high level, they also study the equivalence between zero-knowledge and commitments in the classical setting, but their proof goes through universal one-way hash functions. We adapt their high-level proof ideas but replace certain ingredients with quantum techniques originally developed by Watrous when studying quantum statistical zero knowledge proofs [Wat02]. In particular, we are going to take their idea of considering instance-dependent probability ensembles/commitments, and propose the quantum analogue of instance-dependent probability ensembles in the following lemma, showing the equivalence between a language being inside QCZK and the existence of an instance-dependent computational indistinguishability for that language[7].

Lemma 6.6. *If a language L admits a* $\mathsf{QCZK_{HV}}$ *proof, then there are instance-dependent mixed states* $\{\xi_{b,x}\}_{b,x}$ *for L where* $b = 0, 1$ *and* $x \in \{0, 1\}^*$ *such that:*

- *There is a uniform QPT procedure that on input* b, x *generates* $\xi_{b,x}$.
- *For every nonuniform QPT distinguisher D, there is a negligible function* ε *such that for all* $x \in L$,

$$|\Pr[D(x, \xi_{0,x}) = 1] - \Pr[D(x, \xi_{1,x}) = 1]| \leq \varepsilon(|x|).$$

- *There is some constant c such that for every* $x \notin L$, $\mathrm{TD}(\xi_{0,x}, \xi_{1,x}) \geq c$.

Proof. The mixed states that we consider is due to Watrous [Wat02, Theorem 7], who introduced these states while finding a complete problem for QSZK. We are given a k-round computational zero knowledge protocol, where each round consists of the verifier sending a message followed by the prover sending a response. In Watrous's work, γ_0 and γ_1 are defined to be $\gamma_0 = \rho_1 \otimes \cdots \otimes \rho_k$ and $\gamma_1 = \xi_1 \otimes \cdots \otimes \xi_k$, where ρ_i corresponds to the simulated purified verifier's state if he aborts at the end of round i and then trace out the prover's message, and ξ_i corresponds to the simulated purified verifier's state if he aborts immediately before sending the i-th round's message and then trace out the verifier's message (more formally, this is taken to be the simulated output after $(i-1)$-th message from the prover, apply the verifier's action in i-th round and then trace out the message register). Efficient generation is immediate and trace distance for NO instances follows from the soundness of the protocol as in the case for QSZK [Wat02, Lemma 8].

Finally, computational indistinguishability for YES instances follows from a straightforward hybrid argument, invoking the computational zero knowledge property. This is because in the

---

[7]We only formally show one direction, but the other direction follows the same proof as the classical case via constructing zero-knowledge proofs from instance-dependent commitments.

honest execution (for a YES instance), the verifier's (unsimulated) states corresponding to ρ_i and γ_i are identical since they only differ by an action from the prover, which does not act on the verifier's private register that we are not outputting. More formally, let $\gamma_2 = \psi_1 \otimes \cdots \otimes \psi_k$, where ψ_i is the purified verifier's state after i rounds of interaction with the real prover. By semi-honest zero knowledge, we immediately have that γ_0 is computationally indistinguishable to γ_2. Invoking semi-honest zero knowledge again, we have that γ_1 is computationally indistinguishable to a state that is identical to γ_2, by our discussion above. This completes the proof via hybrid argument. $\quad\square$

We first sketch how this object is powerful enough for us to give the following alternative proof for an unconditional result about $\mathsf{QCZK_{HV}}$ originally established by Kobayashi [Kob08].

Theorem 6.7 ([Kob08])**.** $\mathsf{QCZK_{HV}} = \mathsf{QCZK}$ *holds unconditionally.*

Proof sketch. By definition, $\mathsf{QCZK} \subseteq \mathsf{QCZK_{HV}}$. Using the lemma above with Lemma 4.7, for any language $L \in \mathsf{QCZK_{HV}}$, we obtain instance-dependent quantum commitments, which is statistically binding when x is not in the language and computationally hiding when x is in the language. This is sufficient to obtain an instance-dependent 2PC for reactive functionalities via known compilers [BCKM21, AQY22, WW06, CGT95, IPS08], where it is statistically secure against the prover when x is not in the language and computationally secure against the verifier when x is in the language. This can be then plugged into Theorem 6.4 to give a QCZK proof for L. $\quad\square$

Proof of Theorem 6.5. Assume that there exists L that admits a QCZK proof but (L, D) is hard on average against BQP for some efficiently samplable distribution D. By Lemma 6.6, we get instance-dependent mixed states.

Since D is hard-on-average, it is easy to see that YES and NO instances are of at least $1/3$ fraction for all sufficiently large instance lengths, as otherwise a trivial machine that outputs a constant decides this language with a noticeable advantage (infinitely often). Given that this is the case, it is easy to see that the mixed states $(x, \xi_{b,x})$ taken average over this distribution for x is still statistically far.

We now assume for contradiction that this EFI state pair does not satisfy computational indistinguishability, i.e. there is a BQP algorithm M that distinguishes $(x, \xi_{0,x})$ from $(x, \xi_{1,x})$. In particular, without loss of generality that it outputs 1 with probability $c(|x|)$ when $b = 1$ but $s(|x|)$ when $b = 0$ over $|x|$, where $c - s$ is noticeable.

We now give a QPT algorithm for L: on input x, generate the instance-dependent mixed states with b uniformly chosen from random; if M correctly predicts b then reject, otherwise accept. When the input is a YES instance, we accept correctly with probability within $\left[\frac{1}{2} - \varepsilon(|x|), \frac{1}{2} + \varepsilon(|x|)\right]$ for some universal negligible function ε as otherwise we can use this algorithm to break computational indistinguishability of the instance-dependent mixed states. Since the algorithm predicts correctly with non-negligible probability over the entire domain of D, it must be the case that almost all the prediction advantages are from NO instances[8]. Therefore, for NO instances, this algorithm correctly rejects with probability noticeably more than $\frac{1}{2}$. This breaks the average-case hardness of (L, D), a contradiction. $\quad\square$

Theorem 6.8. *If* $\mathsf{BQP} \neq \mathsf{QCZK}$ *then auxiliary-input EFI state pairs exist, where the definition of auxiliary-input EFI state pairs is the following:*

---

[8]We cannot argue this fact directly from the non-existence of EFI states since the distribution conditioning on the input being a NO instance might not be efficiently samplable.

1. **Efficient generation**: *There exists a uniform QPT quantum algorithm A that on input (x, b) outputs the mixed state $\xi_{b,x}$.*
2. **Statistically Far**: *There exists an infinite set $S \subseteq \{0, 1\}^*$ and some polynomial p, such that for any $x \in S$, we have that $\mathrm{TD}(\xi_{0,x}, \xi_{1,x}) \geq 1/p(|x|)$.*
3. **Computational Indistinguishability**: *For any uniform QPT distinguisher D and every polynomial q, there exists $x \in S$ such that $|\mathrm{Pr}[D(x, \xi_{0,x}) = 1] - \mathrm{Pr}[D(x, \xi_{1.x}) = 1]| \leq 1/q(|x|)$.*

Proof. The proof works similarly as before. Given a QCZK language L, we start by constructing instance-dependent mixed states $\xi_{b,x}$. Consider $S = \bar{L}$. If S is finite then L is trivial then we are done. Otherwise, by the non-existence of auxiliary-input EFI states, we get that there exists a uniform BQP distinguisher D such that for every $x \in S$, the BQP distinguisher distinguishes these two distributions with inverse polynomial probability. Using the same BQP decider as the proof above, we get that this decider (after parallel repetition and majority vote) is correct with probability at least $2/3$ except on finitely many instances. Therefore, $L \in$ BQP. $\qquad\square$

Acknowledgements

References

[AA13]   Scott Aaronson and Alex Arkhipov. "The Computational Complexity of Linear Optics". In: *Theory of Computing* 9.4 (2013), pp. 143–252. DOI: 10.4086/toc.2013.v009a004 (cit. on p. 10).

[Aar16]   Scott Aaronson. *The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes.* 2016. arXiv: 1607.05256 (cit. on p. 9).

[AB09]   Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach.* 1st. Cambridge University Press, 2009. ISBN: 0521424267 (cit. on p. 9).

[AC17]   Scott Aaronson and Lijie Chen. "Complexity-Theoretic Foundations of Quantum Supremacy Experiments". In: *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia.* Vol. 79. 2017, 22:1–22:67. DOI: 10.4230/LIPIcs.CCC.2017.22 (cit. on p. 10).

[AIK22]   Scott Aaronson, DeVon Ingram, and William Kretschmer. "The Acrobatics of BQP". In: *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA.* Vol. 234. 2022, 20:1–20:17. DOI: 10.4230/LIPIcs.CCC.2022.20 (cit. on p. 4).

[AK07]   Scott Aaronson and Greg Kuperberg. "Quantum Versus Classical Proofs and Advice". In: *Theory of Computing* 3.7 (2007), pp. 129–157. DOI: 10.4086/toc.2007.v003a007 (cit. on p. 10).

[AQY22]   Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I.* Vol. 13507. 2022, pp. 208–236. DOI: `10.1007/978-3-031-15802-5_8` (cit. on pp. 2, 3, 5, 7, 18, 23).

[BB21]   Nir Bitansky and Zvika Brakerski. "Classical Binding for Quantum Commitments". In: *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I.* Vol. 13042. 2021, pp. 273–298. DOI: `10.1007/978-3-030-90459-3_10` (cit. on p. 2).

[BB84]   Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of International Conference on Computers, Systems & Signal Processing, Dec. 9-12, 1984, Bangalore, India.* 1984, pp. 175–179. arXiv: `2003.06557` (cit. on p. 2).

[BBCS91]   Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. "Practical Quantum Oblivious Transfer". In: *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings.* Vol. 576. 1991, pp. 351–366. DOI: `10.1007/3-540-46766-1_29` (cit. on pp. 6, 7).

[BCH+21]   Fernando G.S.L. Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. "Models of Quantum Complexity Growth". In: *PRX Quantum* 2 (3 2021), p. 030316. DOI: `10.1103/PRXQuantum.2.030316` (cit. on p. 10).

[BCKM21]   James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. "One-Way Functions Imply Secure Computation in a Quantum World". In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I.* Vol. 12825. 2021, pp. 467–496. DOI: `10.1007/978-3-030-84242-0_17` (cit. on pp. 2, 3, 7, 18, 23).

[BFV20]   Adam Bouland, Bill Fefferman, and Umesh V. Vazirani. "Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract)". In: *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA.* Vol. 151. 2020, 63:1–63:2. DOI: `10.4230/LIPIcs.ITCS.2020.63` (cit. on p. 10).

[BG20]   Anne Broadbent and Alex B. Grilo. "QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge". In: *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020.* 2020, pp. 196–205. DOI: `10.1109/FOCS46700.2020.00027` (cit. on pp. 7, 20).

[BGG+88]   Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, and Phillip Rogaway. "Everything Provable is Provable in Zero-Knowledge". In: *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings.* Vol. 403. 1988, pp. 37–56. DOI: `10.1007/0-387-34799-2_4` (cit. on pp. 8, 20).

[BJSW20] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. "Zero-Knowledge Proof Systems for QMA". In: *SIAM Journal on Computing* 49.2 (2020), pp. 245–283. DOI: `10.1137/18M1193530` (cit. on p. 7).

[BM84] Manuel Blum and Silvio Micali. "How to Generate Cryptographically Strong Sequences of Pseudorandom Bits". In: *SIAM Journal on Computing* 13.4 (1984), pp. 850–864. DOI: `10.1137/0213053` (cit. on p. 1).

[BMM99] Amos Beimel, Tal Malkin, and Silvio Micali. "The All-or-Nothing Nature of Two-Party Secure Computation". In: *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings.* Vol. 1666. 1999, pp. 80–97. DOI: `10.1007/3-540-48405-1_6` (cit. on pp. 3, 7, 18, 19).

[BS18] Adam R. Brown and Leonard Susskind. "Second law of quantum complexity". In: *Phys. Rev. D* 97 (8 2018), p. 086015. DOI: `10.1103/PhysRevD.97.086015` (cit. on p. 10).

[BS19] Zvika Brakerski and Omri Shmueli. "(Pseudo) Random Quantum States with Binary Phase". In: *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I.* Vol. 11891. 2019, pp. 229–250. DOI: `10.1007/978-3-030-36030-6_10` (cit. on p. 2).

[BS20] Zvika Brakerski and Omri Shmueli. "Scalable Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II.* Vol. 12171. 2020, pp. 417–440. DOI: `10.1007/978-3-030-56880-1_15` (cit. on p. 2).

[CGS16] André Chailloux, Gus Gutoski, and Jamie Sikora. "Optimal bounds for semi-honest quantum oblivious transfer". In: *Chicago Journal of Theoretical Computer Science* 2016.13 (2016). DOI: `10.4086/cjtcs.2016.013` (cit. on pp. 6, 14, 15).

[CGT95] Claude Crépeau, Jeroen 5 Graaf, and Alain Tapp. "Committed Oblivious Transfer and Private Multi-Party Computation". In: *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings.* Vol. 963. 1995, pp. 110–123. DOI: `10.1007/3-540-44750-4_9` (cit. on pp. 7, 8, 21, 23).

[CK88] Claude Crépeau and Joe Kilian. "Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract)". In: *29th Annual Symposium on Foundations of Computer Science, White Plains, New York, USA, 24-26 October 1988.* 1988, pp. 42–52. DOI: `10.1109/SFCS.1988.21920` (cit. on pp. 6, 19).

[CKR11] André Chailloux, Iordanis Kerenidis, and Bill Rosgen. "Quantum Commitments from Complexity Assumptions". In: *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I.* Vol. 6755. 2011, pp. 73–85. DOI: `10.1007/978-3-642-22006-7_7` (cit. on pp. 4, 9).

[CLS01]   Claude Crépeau, Frédéric Légaré, and Louis Salvail. "How to Convert the Flavor of a Quantum Bit Commitment". In: *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding.* Vol. 2045. 2001, pp. 60–77. DOI: `10.1007/3-540-44987-6_5` (cit. on pp. 2, 5–7).

[Cré94]   Claude Crépeau. "Quantum Oblivious Transfer". In: *Journal of Modern Optics* 41.12 (1994), pp. 2445–2454. DOI: `10.1080/09500349414552291` (cit. on pp. 6, 7).

[DH76]   W. Diffie and M. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: `10.1109/TIT.1976.1055638` (cit. on p. 1).

[DNS12]   Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. "Actively Secure Two-Party Evaluation of Any Quantum Operation". In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings.* Vol. 7417. 2012, pp. 794–811. DOI: `10.1007/978-3-642-32009-5_46` (cit. on pp. 7, 8, 18, 21).

[FUYZ20]   Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. *How to Base Security on the Perfect/Statistical Binding Property of Quantum Bit Commitment?* 2020. Cryptology ePrint Archive: `2020/621` (cit. on pp. 4, 6, 13).

[GL89]   Oded Goldreich and Leonid A. Levin. "A Hard-Core Predicate for all One-Way Functions". In: *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA.* 1989, pp. 25–32. DOI: `10.1145/73007.73010` (cit. on p. 1).

[GLSV21]   Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. "Oblivious Transfer Is in MiniQCrypt". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II.* Vol. 12697. 2021, pp. 531–561. DOI: `10.1007/978-3-030-77886-6_18` (cit. on pp. 2, 7).

[GMW86]   Oded Goldreich, Silvio Micali, and Avi Wigderson. "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design". In: *27th Annual Symposium on Foundations of Computer Science (sfcs 1986).* 1986, pp. 174–187. DOI: `10.1109/SFCS.1986.47` (cit. on p. 20).

[Gol90]   Oded Goldreich. "A note on computational indistinguishability". In: *Information Processing Letters* 34.6 (1990), pp. 277–281. DOI: `10.1016/0020-0190(90)90010-U` (cit. on pp. 2, 10).

[Hel69]   Carl W. Helstrom. "Quantum detection and estimation theory". In: *Journal of Statistical Physics* 1.2 (1969), pp. 231–252. DOI: `10.1007/BF01007479` (cit. on p. 11).

[HFK+22]   Jonas Haferkamp, Philippe Faist, Naga B. T. Kothakonda, Jens Eisert, and Nicole Yunger Halpern. "Linear growth of quantum circuit complexity". In: *Nature Physics* 18.5 (2022), pp. 528–532. DOI: `10.1038/s41567-022-01539-6` (cit. on p. 10).

[HILL99]   Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. "A Pseudorandom Generator from any One-way Function". In: *SIAM Journal on Computing* 28.4 (1999), pp. 1364–1396. DOI: `10.1137/S0097539793244708` (cit. on p. 1).

[Hol73]   A.S Holevo. "Statistical decision theory for quantum systems". In: *Journal of Multi-variate Analysis* 3.4 (1973), pp. 337–394. DOI: `10.1016/0047-259X(73)90028-6` (cit. on p. 11).

[ILL89]   R. Impagliazzo, L. A. Levin, and M. Luby. "Pseudo-Random Generation from One-Way Functions". In: *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing.* 1989, pp. 12–24. DOI: `10.1145/73007.73009` (cit. on p. 2).

[IPS08]   Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. "Founding Cryptography on Oblivious Transfer - Efficiently". In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings.* Vol. 5157. 2008, pp. 572–591. DOI: `10.1007/978-3-540-85174-5_32` (cit. on pp. 7, 8, 21, 23).

[IR89]   R. Impagliazzo and S. Rudich. "Limits on the Provable Consequences of One-Way Permutations". In: *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing.* 1989, pp. 44–61. DOI: `10.1145/73007.73012` (cit. on p. 2).

[JJUW11]   Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. "QIP = PSPACE". In: *J. ACM* 58.6 (2011). DOI: `10.1145/2049697.2049704` (cit. on pp. 8, 20).

[JLS18]   Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III.* Vol. 10993. 2018, pp. 126–152. DOI: `10.1007/978-3-319-96878-0_5` (cit. on p. 2).

[Kil91]   Joe Kilian. "A General Completeness Theorem for Two Party Games". In: *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing.* 1991, pp. 553–560. DOI: `10.1145/103418.103475` (cit. on pp. 4, 19).

[KKMO00]   Joe Kilian, Eyal Kushilevitz, Silvio Micali, and Rafail Ostrovsky. "Reducibility and Completeness in Private Computations". In: *SIAM Journal on Computing* 29.4 (2000), pp. 1189–1208. DOI: `10.1137/S0097539797321742` (cit. on p. 19).

[KKNY12]   Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami. "Computational Indistinguishability Between Quantum States and Its Cryptographic Application". In: *Journal of Cryptology* 25.3 (2012), pp. 528–555. DOI: `10.1007/s00145-011-9103-4` (cit. on p. 10).

[Kob08]   Hirotada Kobayashi. "General Properties of Quantum Zero-Knowledge Proofs". In: *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.* Vol. 4948. 2008, pp. 107–124. DOI: `10.1007/978-3-540-78524-8_7` (cit. on p. 23).

[Kre21]   William Kretschmer. "Quantum Pseudorandomness and Classical Complexity". In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference.* Vol. 197. 2021, 2:1–2:20. DOI: `10.4230/LIPIcs.TQC.2021.2` (cit. on pp. 2–4, 9).

[MP12]   Mohammad Mahmoody and Rafael Pass. "The Curious Case of Non-Interactive Commitments - On the Power of Black-Box vs. Non-Black-Box Use of Primitives". In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings.* Vol. 7417. 2012, pp. 701–718. DOI: `10.1007/978-3-642-32009-5_41` (cit. on p. 2).

[MW05]   Chris Marriott and John Watrous. "Quantum Arthur–Merlin games". In: *computational complexity* 14.2 (2005), pp. 122–152. DOI: `10.1007/s00037-005-0194-x` (cit. on p. 21).

[MY22]   Tomoyuki Morimae and Takashi Yamakawa. "Quantum Commitments and Signatures Without One-Way Functions". In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I.* Vol. 13507. 2022, pp. 269–295. DOI: `10.1007/978-3-031-15802-5_10` (cit. on pp. 2, 10, 13).

[Nao91]   Moni Naor. "Bit commitment using pseudorandomness". In: *Journal of Cryptology* 4.2 (1991), pp. 151–158. DOI: `10.1007/BF00196774` (cit. on p. 4).

[NC10]   Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010. DOI: `10.1017/CBO9780511976667` (cit. on p. 11).

[OV08]   Shien Jin Ong and Salil P. Vadhan. "An Equivalence Between Zero Knowledge and Commitments". In: *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.* Vol. 4948. 2008, pp. 482–500. DOI: `10.1007/978-3-540-78524-8_27` (cit. on pp. 8, 22).

[OW93]   R. Ostrovsky and A. Wigderson. "One-way functions are essential for non-trivial zero-knowledge". In: *The 2nd Israel Symposium on Theory and Computing Systems.* 1993, pp. 3–17. DOI: `10.1109/ISTCS.1993.253489` (cit. on pp. 8, 20, 22).

[REN08]   RENATO RENNER. "SECURITY OF QUANTUM KEY DISTRIBUTION". In: *International Journal of Quantum Information* 06.01 (2008), pp. 1–127. DOI: `10.1142/S0219749908003256` (cit. on p. 2).

[Sha83]   Adi Shamir. "On the Generation of Cryptographically Strong Pseudorandom Sequences". In: *ACM Trans. Comput. Syst.* 1.1 (1983), pp. 38–44. DOI: `10.1145/357353.357357` (cit. on p. 1).

[Sha92]   Adi Shamir. "IP = PSPACE". In: *J. ACM* 39.4 (1992), pp. 869–877. DOI: `10.1145/146585.146609` (cit. on pp. 8, 20).

[Vad06]   Salil P. Vadhan. "An Unconditional Study of Computational Zero Knowledge". In: *SIAM Journal on Computing* 36.4 (2006), pp. 1160–1214. DOI: `10.1137/S0097539705447207` (cit. on pp. 8, 22).

[Wat02]   John Watrous. "Limits on the Power of Quantum Statistical Zero-Knowledge". In: *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings.* 2002, p. 459. DOI: `10.1109/SFCS.2002.1181970` (cit. on pp. 4, 9, 20, 22).

[WW06]   Stefan Wolf and Jürg Wullschleger. "Oblivious Transfer Is Symmetric". In: *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*. Vol. 4004. 2006, pp. 222–232. DOI: `10.1007/11761679_14` (cit. on pp. 18, 23).

[Yan22]   Jun Yan. *General Properties of Quantum Bit Commitments*. 2022. Cryptology ePrint Archive: `2020/1488/20221017:032232` (cit. on pp. 2–7, 11, 13, 15, 16).

[Yao82]   Andrew C. Yao. "Theory and application of trapdoor functions". In: *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. 1982, pp. 80–91. DOI: `10.1109/SFCS.1982.45` (cit. on p. 1).

[YWLQ15]   Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. "Quantum Bit Commitment with Application in Quantum Zero-Knowledge Proof (Extended Abstract)". In: *Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings*. Vol. 9472. 2015, pp. 555–565. DOI: `10.1007/978-3-662-48971-0_47` (cit. on pp. 2, 4, 9, 13).