One-Way Functions Imply Secure Computation in a Quantum World

James Bartusek   Andrea Coladangelo   Dakshita Khurana   Fermi Ma

The complexity of cryptographic primitives has been central to the study of cryptography. Much of the work in the field focuses on establishing *reductions* between different primitives, typically building more sophisticated primitives from simpler ones. Reductions imply relative measures of complexity among different functionalities, and over the years have resulted in an expansive hierarchy of assumptions and primitives, as well as separations between them.

At the center of cryptographic complexity lie one-way functions (OWFs): their existence is the minimal assumption necessary for nearly all classical cryptography [IL89, LR86, IL89, ILL89]. One-way functions are equivalent to so-called "minicrypt" primitives like pseudorandom generators, pseudorandom functions and symmetric encryption; but provably cannot imply key exchange when used in a black-box way [IR90, BM09][1]. Thus, the existence of key exchange is believed to be a stronger assumption than the existence of one-way functions. Oblivious transfer (OT) — equivalently, secure computation — is believed to be *even stronger*: it implies key exchange, but cannot be obtained from black-box use of a key exchange protocol [MMP14].

The importance of OT stems from the fact that it can be used to achieve secure computation, which is a central cryptographic primitive with widespread applications. In a nutshell, secure computation allows mutually distrusting participants to compute any public function over their joint private inputs while revealing no private information beyond the output of the computation.

The Quantum Landscape. The landscape of cryptographic possibilities changes significantly when participants have quantum computation and communication capabilities. For one, *unconditionally* secure key distribution (*quantum key distribution*/QKD) becomes possible [BB84, May96]. Moreover, *quantum* oblivious transfer (QOT) is known to be achievable from special types of commitments, as we discuss next.

Bennett, Brassard, Crepeau and Skubiszewska [BBCS92] first proposed a protocol for QOT by using quantum bit commitments. The central idea in these QKD and QOT protocols is the use of (what are now known as) "BB84 states". These are single qubit states encoding either 0 or 1 in either the computational or Hadamard basis. Crucially, measuring (or essentially attempting to copy the encoded bit) in the wrong basis completely destroys information about the encoded bit. The original [BBCS92] paper heuristically argued security of the proposed OT protocol, and subsequently, Mayers and Salvail [MS94] proved that the protocol from [BBCS92] is secure against a restricted class of attackers that only perform single-qubit measurements. This was later improved by Yao [Yao95], who extended this result to handle general quantum adversaries.

By an unfortunate historical accident, the aforementioned security proofs claimed the [BBCS92] QOT could be *information-theoretically secure*, since at the time it was believed that information-theoretic quantum bit commitment was possible [BCJL93]. Several years later, Mayers [May97] and Lo and Chau [LC97] independently proved the impossibility of information-theoretic quantum bit commitment, and as a consequence, the precise security of [BBCS92] QOT was once again unclear. This state of affairs remained largely unchanged until 2009, when Damgard, Fehr, Lunemann, Salvail, and Schaffner [DFL$^+$09] proved that bit commitment schemes satisfying certain additional properties, namely *extraction and equivocation*, suffice to

[1] In particular, [IR90, BM09] showed that there cannot exist a key exchange protocol that only has oracle access to the input/output behavior of a one-way function, and makes no additional assumptions. Then [Dac16] ruled out the possibility of certain types of key exchange protocols that also make use of the *code* of a one-way function. Constructions of key exchange from one-way functions have eluded researchers for decades. This, combined with the aforementioned negative results, is considered to be evidence that key exchange is a qualitatively stronger primitive than one-way functions in the classical regime. In fact, Impagliazzo [Imp95] stipulates that we live in one of five possible worlds, of which *Minicrypt* is one where one-way functions exist but classical public-key cryptographic primitives do not.

obtain QOT [BBCS92]. [DFL+09] called their commitments *dual-mode* commitments, and provided a construction based on the quantum hardness of the learning with errors (QLWE) assumption. We remark that assumptions about the hardness of specific problems like QLWE are qualitatively even worse than general assumptions like QOWFs and QOT. Thus, the following basic question remains:

Do quantum-hard one-way functions suffice for quantum oblivious transfer?

Quantum OT: The Basis of Secure Quantum Computation. There is a natural extension of secure computation to the quantum world, where Alice and Bob wish to compute a *quantum* circuit on (possibly entangled) *quantum* input states. This setting, usually referred to as secure *quantum* computation, has been previously studied and in fact has a strong tradition in the quantum cryptography literature.

Secure quantum computation was first studied by [CGS02, BCG+06], who obtained unconditional maliciously-secure general *multi-party* quantum computation with honest majority. The setting where half (or more) of the players are malicious requires computational assumptions due to the impossibility of unconditionally secure quantum bit commitment [May97, LC97].

In this computational setting, [DNS10, DNS12] showed the feasibility of two-party quantum computation (2PQC) assuming post-quantum OT. More recently, [DGJ+20] constructed maliciously-secure general multi-party quantum computation (MPQC) secure against a *dishonest* majority from any maliciously-secure post-quantum multi-party computation (MPC) protocol for classical functionalities, which can itself be obtained from post-quantum OT [ABG+20].

Nevertheless, the following natural question has remained unanswered:

Can secure (quantum) computation be obtained from quantum-hard one-way functions?

Our Results

Our main result is the following:

Quantum oblivious transfer can be based on the assumption that quantum-hard one-way functions exist.

This in turn implies secure two party computation of classical functionalities, in the presence of quantum computation and communication capabilities, from the same assumption [Kil88]. The latter can then be used to obtain secure two-party *quantum* computation, by relying on the work of [DNS12]. QOT can also be used to obtain *multi-party* secure computation of all classical functionalities [IPS08], in the presence of quantum computation and communication capabilities, and additionally assuming the existence of authenticated channels. By relying on [DGJ+20], this also implies multi-party secure *quantum* computation.

In summary, our main result implies that: (1) quantum-hard OWFs imply 2PQC and (2) assuming the existence of authenticated channels, quantum-hard OWFs imply MPQC.

This provides a further potential separation between the complexity of cryptographic primitives in the classical and quantum worlds. In the former, (two-party) secure computation is only known from special types of enhanced public-key encryption schemes or from the hardness of specific problems, both of which are believed to be much stronger assumptions than one-way functions. But in the quantum world, prior to our work, (two-party) secure computation was only known from the commitments required in the protocol of [DFL+09], which can be based on QLWE following [DFL+09], or post-quantum OT (implicit in [HSS11, ABG+20]) — but were not known to be achievable from quantum-hard one-way functions.

Primary Tool: Stand-Alone Extractable and Equivocal Commitments. As discussed earlier in the introduction, [DFL+09] show that simulation-secure OT can be obtained from commitments satisfying certain properties, namely *extraction* and *equivocation*.

- Extraction informally requires that there exist an efficient quantum “extractor”, that with access to a quantum committer, is able to extract its committed value.

- Equivocality informally requires that there exist an efficient quantum simulator, that with access to a quantum receiver, is able to open a commitment to any value of its choice.

The two properties are crucial for proving simulation security of the [BBCS92] OT protocol: extraction for receiver security, and equivocality for sender security. Our key technical contribution, that may be of independent interest, is the following:

Extractable and equivocal commitments can be based on the assumption that quantum-hard one-way functions exist.

We obtain this result via the following technical steps.

- *Quantum Extractable Commitments from Quantum-Hard One-Way Functions.* We build on the [BBCS92, DFL+09, BF10] protocols to obtain an extractable commitment that leverages quantum communication and can be based on the existence of quantum-hard one-way functions. This is in contrast to existing approaches (eg., [HSS11]) that rely on qualitatively stronger assumptions like classical OT with post-quantum security.

- *From Extractable Commitments to Extractable and* Equivocal *Commitments.* Our second technical contribution is a generic unconditional compiler from quantum extractable commitments to quantum extractable and *equivocal* commitments. Such compilers are known in the classical setting, but break down in the setting of quantum communication due to the need to make non-black-box use of the underlying commitment. For example, one way to obtain the equivocality property is as follows. In the opening phase, to open to a bit b, the committer does not send the randomness used to commit to b in the clear. Instead, the committer sends a zero-knowledge proof for the NP statement that there exist randomness consistent with the commitment, and opening to b.

  Unfortunately, this technique fails when the commitment involves *quantum* communication, since the statement to be proven is no longer an NP statement (nor a QMA statement). Therefore, we build a new protocol that only makes black-box use of the underlying commitment, and leverages Watrous's rewinding lemma in the proof of equivocality [Wat06].

Plugging our quantum commitments into the [BBCS92] framework yields a final QOT protocol with an interaction pattern that readers familiar with [BB84, BBCS92] may find curious: the sender sends the receiver several BB84 states, after which the receiver proves to the sender that it has honestly measured the sender's BB84 states by *generating more BB84 states of their own and asking the sender to prove that they have measured the receiver's BB84 states!* An intriguing open question is whether obtaining QOT from one-way functions *requires* two-way quantum communication or, alternatively, quantum memory.[2]

Additional Related Work. The protocol in [DFL+09] can be instantiated [BF10, FUYZ20] with weaker types of commitments (in particular, statistically binding, computationally hiding commitments) to obtain a weaker version of OT, which only satisfies *indistinguishability-based* security, and not the standard notion of *simulation-based* security. Such commitments can be obtained from quantum-hard one-way functions. But this weaker notion is not typical in the classical OT literature and falls short of guaranteeing that the view of a quantum polynomial-time adversary can be efficiently simulated given the input and/or output of the protocol. More crucially, this notion is not known to imply standard (simulation-based) notions of secure multi-party computation. Our focus in this work is on achieving the (standard) simulation-based notion of security for OT – this suffices to instantiate the aforementioned compilers and achieve standard simulation-based secure quantum computation. Achieving simulation-based OT, specifically one that admits an *efficient* (quantum) simulator involves developing multiple new protocols, that we discuss in the technical overview of the main paper.

[2] Removing one direction of quantum communication would require the honest parties to be entangled and subsequently perform quantum teleportation.

References

[ABG$^+$20] Amit Agarwal, James Bartusek, Vipul Goyal, Dakshita Khurana, and Giulio Malavolta, *Post-quantum multi-party computation*, Cryptology ePrint Archive, Report 2020/1395, 2020, https://eprint.iacr.org/2020/1395.

[BB84] Charles H Bennett and Gilles Brassard, *Proceedings of the ieee international conference on computers, systems and signal processing*, 1984.

[BBCS92] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska, *Practical quantum oblivious transfer*, CRYPTO'91 (Joan Feigenbaum, ed.), LNCS, vol. 576, Springer, Heidelberg, August 1992, pp. 351–366.

[BCG$^+$06] Michael Ben-Or, Claude Crépeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith, *Secure multiparty quantum computation with (only) a strict honest majority*, 47th FOCS, IEEE Computer Society Press, October 2006, pp. 249–260.

[BCJL93] Gilles Brassard, Claude Crépeau, Richard Jozsa, and Denis Langlois, *A quantum bit commitment scheme provably unbreakable by both parties*, 34th FOCS, IEEE Computer Society Press, November 1993, pp. 362–371.

[BF10] Niek J. Bouman and Serge Fehr, *Sampling in a quantum population, and applications*, CRYPTO 2010 (Tal Rabin, ed.), LNCS, vol. 6223, Springer, Heidelberg, August 2010, pp. 724–741.

[BM09] Boaz Barak and Mohammad Mahmoody-Ghidary, *Merkle puzzles are optimal - an $O(n^2)$-query attack on any key exchange from a random oracle*, CRYPTO 2009 (Shai Halevi, ed.), LNCS, vol. 5677, Springer, Heidelberg, August 2009, pp. 374–390.

[CGS02] Claude Crépeau, Daniel Gottesman, and Adam Smith, *Secure multi-party quantum computation*, 34th ACM STOC, ACM Press, May 2002, pp. 643–652.

[Dac16] Dana Dachman-Soled, *Towards non-black-box separations of public key encryption and one way function*, Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II, 2016, pp. 169–191.

[DFL$^+$09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner, *Improving the security of quantum protocols via commit-and-open*, CRYPTO 2009 (Shai Halevi, ed.), LNCS, vol. 5677, Springer, Heidelberg, August 2009, pp. 408–427.

[DGJ$^+$20] Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner, *Secure multi-party quantum computation with a dishonest majority*, EUROCRYPT 2020, Part III (Anne Canteaut and Yuval Ishai, eds.), LNCS, vol. 12107, Springer, Heidelberg, May 2020, pp. 729–758.

[DNS10] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail, *Secure two-party quantum evaluation of unitaries against specious adversaries*, CRYPTO 2010 (Tal Rabin, ed.), LNCS, vol. 6223, Springer, Heidelberg, August 2010, pp. 685–706.

[DNS12] ______, *Actively secure two-party evaluation of any quantum operation*, CRYPTO 2012 (Reihaneh Safavi-Naini and Ran Canetti, eds.), LNCS, vol. 7417, Springer, Heidelberg, August 2012, pp. 794–811.

[FUYZ20] Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou, *How to base security on the perfect/statistical binding property of quantum bit commitment?*, Cryptology ePrint Archive, Report 2020/621, 2020, https://eprint.iacr.org/2020/621.

[HSS11] Sean Hallgren, Adam Smith, and Fang Song, *Classical cryptographic protocols in a quantum world*, CRYPTO 2011 (Phillip Rogaway, ed.), LNCS, vol. 6841, Springer, Heidelberg, August 2011, pp. 411–428.

[IL89] Russell Impagliazzo and Michael Luby, *One-way functions are essential for complexity based cryptography (extended abstract)*, 30th FOCS, IEEE Computer Society Press, October / November 1989, pp. 230–235.

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby, *Pseudo-random generation from one-way functions (extended abstracts)*, 21st ACM STOC, ACM Press, May 1989, pp. 12–24.

[Imp95] Russell Impagliazzo, *A personal view of average-case complexity*, Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995, 1995, pp. 134–147.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai, *Founding cryptography on oblivious transfer - efficiently*, CRYPTO 2008 (David Wagner, ed.), LNCS, vol. 5157, Springer, Heidelberg, August 2008, pp. 572–591.

[IR90] Russell Impagliazzo and Steven Rudich, *Limits on the provable consequences of one-way permutations*, CRYPTO'88 (Shafi Goldwasser, ed.), LNCS, vol. 403, Springer, Heidelberg, August 1990, pp. 8–26.

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

[LC97] Hoi-Kwong Lo and Hoi Fung Chau, *Is quantum bit commitment really possible?*, Physical Review Letters **78** (1997), no. 17, 3410.

[LR86] Michael Luby and Charles Rackoff, *Pseudo-random permutation generators and cryptographic composition*, 18th ACM STOC, ACM Press, May 1986, pp. 356–363.

[May96] Dominic Mayers, *Quantum key distribution and string oblivious transfer in noisy channels*, CRYPTO'96 (Neal Koblitz, ed.), LNCS, vol. 1109, Springer, Heidelberg, August 1996, pp. 343–357.

[May97] Dominic Mayers, *Unconditionally secure quantum bit commitment is impossible*, Physical review letters **78** (1997), no. 17, 3414.

[MMP14] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran, *On the power of public-key encryption in secure computation*, TCC 2014 (Yehuda Lindell, ed.), LNCS, vol. 8349, Springer, Heidelberg, February 2014, pp. 240–264.

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

[Wat06] John Watrous, *Zero-knowledge against quantum attacks*, 38th ACM STOC (Jon M. Kleinberg, ed.), ACM Press, May 2006, pp. 296–305.

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

Oblivious Transfer is in MiniQCrypt

Alex B. Grilo* Huijia Lin† Fang Song‡ Vinod Vaikuntanathan¶

Quantum computing and modern cryptography have enjoyed a highly productive relationship since the conception of both fields. On the one hand, quantum computers can be used to break many widely used cryptosystems [38]. On the other hand, quantum resources have helped us realize cryptographic tasks that are otherwise impossible [4, 9, 12, 41, 43].

Notably, the groundbreaking protocol for quantum key-distribution [4] raised the *tantalizing* possibility of realizing cryptographic primitives *unconditionally* with quantum resources. A natural next target is oblivious transfer (OT), a versatile cryptographic primitive, which in particular enables secure multiparty computation (MPC) of any polynomial-time computable function [20, 28, 29]. Oblivious transfer allows a receiver Bob to obtain one out of two secret bits that the sender Alice owns. The OT protocol must ensure that Alice does not learn which of the two bits Bob received, and that Bob learns only one of Alice's bits and no information about the other.

Bennett, Brassard, Crépeau and Skubiszewska (BBCS) [5] constructed a quantum OT protocol given an *ideal* bit commitment protocol. Unfortunately, *unconditionally secure* commitment [32, 34] and *unconditionally secure* OT [11, 31] were soon shown to be impossible even with quantum resources.

However, given that bit commitment can be constructed from one-way functions (OWF) [23, 35], the hope remains that OT, and therefore a large swathe of cryptography, can be based on only *OWF* together with simple quantum computation/communication.[1] Drawing our inspiration from Impagliazzo's five worlds in cryptography [25], we call such a world, where post-quantum secure one-way functions (pqOWF) exist and quantum computation and communication are possible, Mini**Q**Crypt. The question that motivates this paper is:

Do OT and MPC exist in MiniQCrypt?

Without the quantum power, this is widely believed to be impossible. That is, given only OWFs, there are no *black-box* constructions of OT or even key exchange protocols [26, 37]. The fact that [4] overcome this barrier and construct a key exchange protocol with quantum communication (without the help of OWFs!) reinvigorates our hope to do the same for OT. In this work, we finally give a positive answer to the previous question, by showing that OT and MPC do exist in MiniQCrypt.

Aren't We Done Already? At this point, the reader may wonder why we did not have an affirmative answer to this question already before, by combining the BBCS protocol based on bit commitments, with a construction of bit commitments from pqOWF [23, 35]. Although this possibility was mentioned already in [5], where they note that "...computational complexity based quantum cryptography is interesting since it allows to build oblivious transfer around one-way functions.", attaining this goal remains elusive as we explain below.

First, proving the security of the [5] OT protocol (regardless of the assumptions) turns out to be a marathon. After early proofs against limited adversaries [33, 44], it is relatively recently that we have a clear picture with formal proofs against arbitrary quantum polynomial-time adversaries [8, 13, 14, 39]. Based on these results, we can summarize the state of the art as follows.

*Sorbonne Université, CNRS, LIP6 † University of Washington ‡ Portland State University ¶ MIT

[1] In particular, in the BBCS protocol, the parties only need to create, send and measure BB84 states.

Using Ideal Commitments: If we assume an *ideal* commitment protocol, formalized as universally composable (UC) commitment, then the quantum OT protocol can be proven secure in strong simulation-based models, admitting secure sequential composition or even concurrent composition in a network setting (i.e., the quantum UC model) [8, 13, 18, 39]. However, UC commitments, in contrast to vanilla computationally-hiding and statistically-binding commitments, are powerful objects that do not live in (classical) Minicrypt. In particular, UC commitments give us key exchange protocols and are therefore black-box separated from Minicrypt.

Using Vanilla Commitments: If in the [5] quantum OT protocol we use a *vanilla* statistically-binding and computationally hiding commitment scheme, which exists assuming a pqOWF, the existing proofs, for example [8], fall short in two respects.

First, for a malicious receiver, the proof of [8] constructs only an *in*efficient simulator. Roughly speaking, this is because the OT receiver in [5] acts as a committer, and vanilla commitments are not extractable (explained shortly below). Hence, we need an inefficient simulator to extract the committed value by brute force. Inefficient simulation makes it hard, if not impossible, to use the OT protocol to build other protocols (even if we are willing to let the resulting protocol have inefficient simulation). Our work will focus on achieving the standard ideal/real notion of security [19] with efficient simulators.

Secondly, it is unclear how to construct a simulator (even ignoring efficiency) for a malicious sender. Roughly, the issue is that simulation seems to require that the commitment scheme used in [5] be secure against selective opening attacks, which vanilla commitments do not guarantee [3].

Using Extractable Commitments: It turns out that the first difficulty above can be addressed if we assume a commitment protocol that allows *efficient extraction* of the committed value – called extractable commitments. Constructing extractable commitments is surprisingly challenging in the quantum world because of the difficulty of rewinding quantum adversaries. Moreover, to plug into the quantum OT protocol, we need a strong version of extractable commitments from which the committed values can be extracted efficiently *without destroying or even disturbing the quantum states of the malicious committer,*[2] a property that is at odds with quantum unclonability and rules out several extraction techniques used for achieving arguments of knowledge such as in [40]. In particular, we are not aware of a construction of such extractable commitments without resorting to stronger assumptions such as LWE [1, 6] or PKE in the *common reference string* (CRS) model, which takes us out of Minicrypt.

To summarize, as tempting as it appears, securely realizing quantum OT from pqOWFs remains unaccomplished.

Our results. In this paper, we finally prove the longstanding (but previously unproved) claim.

Theorem 1 (Informal). *Assuming that pqOWFs exists, there exists a quantum protocol for oblivious transfer in the plain model that is simulation-secure against malicious quantum poly-time adversaries.*

Our main technical contribution consists of showing a construction of an extractable commitment scheme based solely on pqOWFs and using quantum communication. Our construction involves three ingredients. The first is vanilla post-quantum commitment schemes which exist assuming that pqOWFs exist [35]. The second is post-quantum zero-knowledge protocols which also exist assuming that pqOWFs exist [42]. The third and final ingredient is a special multiparty computation protocol called conditional disclosure of secrets (CDS) constructing which in turns requires OT. This might seem circular as this whole effort was to construct an OT protocol to begin with! Our key observation is that the CDS protocol is only required to have a mild type of security, namely *unbounded simulation*, which *can* be

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

achieved with a slight variant of the [5] protocol. Numerous difficulties arise in our construction, and in particular proving consistency of a protocol execution involving quantum communication appears difficult: how do we even write down an statement (e.g., NP or QMA) that encodes consistency? Overcoming these difficulties constitutes the bulk of our technical work.

We notice that just as in [4,5], the honest execution of our protocols does not need strong quantum computational power, since one only needs to create, send, and measure BB84 states.

In turn, plugging our OT protocol into the protocols of [16,17,28,39] (and using the sequential composition theorem [22]) gives us secure two-party computation and multi-party computation (with a dishonest majority) protocols, even for quantum channels.

Theorem 2 (Informal)**.** *Assuming that pqOWFs exist, for every classical two-party and multi-party functionality $\mathcal{F}$, there is a quantum protocol in the plain model that is simulation-secure against malicious quantum poly-time adversaries. Under the same assumptions, there is a quantum two-party and multi-party protocol for any quantum circuit Q.*

Finally, we note that our OT protocol runs in $\mathsf{poly}(\lambda)$ number of rounds, where λ is a security parameter, and that is only because of the Zero-Knowledge (ZK) proof. Watrous' ZK proof system [42] involves repeating a classical ZK proof [7,21] *sequentially*. A recent work of Bitansky and Shmueli [6] for the first time constructs a *constant-round* quantum ZK protocol (using only classical resources) but they rely on the strong LWE assumption, which does not live in Minicrypt. Nevertheless, in the common random string (CRS) model, we can instantiate the zero-knowledge protocol using a Witness Indistinguishability (WI) protocol, which can be implemented in a constant number of rounds based on pqOWF. Moreover, this modification allows us to achieve *straigh-line simulators*, leading to *universally-composable* (UC) security [10]. Therefore, this modification would give us the following statement.

Theorem 3 (Informal)**.** *Constant-round oblivious transfer protocols in the common random string (CRS) model that are UC-simulation-secure against malicious quantum poly-time adversaries exist assuming that post-quantum one-way functions exist and that quantum communication is possible.*

Why MiniQCrypt? Minicrypt is one of five Impagliazzo's worlds [25] where OWFs exist, but public-key encryption (PKE) schemes do not.

Minicrypt is robust *and* efficient. It is robust because there is an abundance of candidates for OWFs that draw from a variety of sources of hardness, and most do not fall to quantum attacks. In contrast, Cryptomania, the world where PKE schemes do exist, seems fragile and, to some skeptics, even endangered due to the abundance of subexponential and quantum attacks, except for a handful of candidates. It is efficient because the operations are combinatorial in nature and amenable to very fast implementations; and the key lengths are relatively small owing to OWFs against which the best known attacks are essentially brute-force key search.

Consequently, much research in (applied) cryptography has been devoted to minimizing the use of public-key primitives in advanced cryptographic protocols [2,27]. However, complete elimination seems hard. In the classical world, we can construct pseudorandom generators and digital signatures in Minicrypt, but not key exchange, PKE, OT or secure computation protocols. With quantum *communication* becoming a reality [15,24,30,36], we have the ability to reap the benefits of robustness and efficiency that Minicrypt affords us, *and* construct powerful primitives such as oblivious transfer and secure computation that were so far out of reach.

References

[1] Prabhanjan Ananth and Rolando L. La Placa. Secure quantum extraction protocols. *CoRR*, abs/1911.07672, 2019.

[2] Donald Beaver. Correlated pseudorandomness and the complexity of private computations. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 479–488. ACM, 1996.

[3] Mihir Bellare, Dennis Hofheinz, and Scott Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 1–35. Springer, Heidelberg, April 2009.

[4] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *EEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8, 1984.

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

[6] Nir Bitansky and Omri Shmueli. Post-quantum zero knowledge in constant rounds. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *STOC 2020*, pages 269–279. ACM, 2020.

[7] Manuel Blum. How to prove a theorem so no one else can claim it. Proceedings of the International Congress of Mathematicians, 1986.

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

[9] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Mikkel Thorup, editor, *FOCS 2018*, pages 320–331. IEEE Computer Society, 2018.

[10] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–145. IEEE, 2001.

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

[12] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. Ph.D. Thesis, Trinity College, University of Cambridge, 2009.

[13] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In *Advances in Cryptology – CRYPTO 2009*, pages 408–427. Springer, 2009.

[14] Ivan B Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advanced in Cryptology – CRYPTO 2007*, pages 360–378. Springer, 2007.

[15] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Optics Express*, 16(23):18790, Oct 2008.

[16] Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner. Secure multi-party quantum computation with a dishonest majority. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 729–758. Springer, Heidelberg, May 2020.

[17] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In *Advances in Cryptology – CRYPTO 2012*, pages 794–811. Springer, 2012.

[18] Serge Fehr and Christian Schaffner. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference – TCC 2009*, pages 350–367. Springer, 2009.

[19] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, USA, 1st edition, 2009.

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

[21] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to prove all NP-statements in zero-knowledge, and a methodology of cryptographic protocol design. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 171–185. Springer, Heidelberg, August 1987.

[22] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. *International Journal of Quantum Information*, 13(04):1550028, 2015. Preliminary version in Crypto 2011.

[23] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[24] P A Hiskett, D Rosenberg, C G Peterson, R J Hughes, S Nam, A E Lita, A J Miller, and J E Nordholt. Long-distance quantum key distribution in optical fibre. *New Journal of Physics*, 8(9):193–193, Sep 2006.

[25] R. Impagliazzo. A personal view of average-case complexity. In *Structure in Complexity Theory Conference, Annual*, page 134, Los Alamitos, CA, USA, jun 1995. IEEE Computer Society.

[26] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In David S. Johnson, editor, *STOC 1989*, pages 44–61. ACM, 1989.

[27] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 145–161. Springer, 2003.

[28] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, Heidelberg, August 2008.

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

[30] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, and et al. Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120(3), Jan 2018.

[31] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, Aug 1997.

[32] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, Apr 1997.

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

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

[35] Moni Naor. Bit commitment using pseudo-randomness. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 128–136. Springer, Heidelberg, August 1990.

[36] Christopher J Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Jeongwan Jin, Nigar Sultana, Sascha Agne, Elena Anisimova, Vadim Makarov, Eric Choi, Brendon L Higgins, and et al. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology*, 2(2):024009, Jun 2017.

[37] Steven Rudich. The use of interaction in public cryptosystems. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 242–251, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[38] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 1994*, pages 124–134. IEEE Computer Society, 1994.

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

[40] Dominique Unruh. Quantum proofs of knowledge. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, Heidelberg, April 2012.

[41] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: Or, true random number generation secure against quantum adversaries. In *STOC '12*, page 61–76. Association for Computing Machinery, 2012.

[42] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version in STOC 2006.

[43] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

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