Classical cryptographic protocols in a quantum world

Sean Hallgren Adam Smith Fang Song*

1 Motivation

Cryptographic protocols, such as protocols for secure function evaluation, have played a crucial role in the development of modern cryptography. Secure function evaluation (SFE) allows a group of players, each holding a secret input (e.g., a vote) to jointly evaluate some function of their inputs (say, the votes' tally) without revealing anything except the function's value. A special case of this is a zero-knowledge (ZK) proof system, which allows a prover P who knows a short proof of a statement to interactively prove the statement to a computationally-bounded verifier V without revealing anything except the statement's veracity. The very possibility of such protocols is counterintuitive. But a series of seminal results in the 1980's showed that under mild assumptions (roughly, the existence of secure public-key cryptosystems), SFE protocols exist for any polynomial-time function [22, 10, 3, 29], and ZK proof systems are possible for any language in NP [23]. Research into the design and analysis of these protocols is now a large subfield of cryptography; moreover, it has driven important advances in more traditional areas of cryptography such as the design of encryption, authentication and signature schemes.

The extensive theory of these protocols, however, deals almost exclusively with classical attackers. If we accept that quantum information processing is currently the most realistic model of physically feasible computation (we do), then we must ask: *what classical protocols remain secure against quantum attackers?*

Clearly not all protocols are secure: we can rule out anything based on the computational hardness of factoring, the discrete log [31], or the principal ideal problem [24]. More subtly, the basic techniques used to reason about security may not apply in a quantum setting. For example, some two-prover ZK protocols are analyzed by viewing the provers as long tables that are fixed before the verifier selects its queries; entanglement breaks that analysis and some protocols are insecure with quantum provers [15].

In the computational realm, *rewinding* is a key technique for reducing the security of a protocol to the hardness of some underlying problem. Rewinding proofs consist of mental experiments in which the adversary is run multiple times using carefully chosen variations of its inputs. At first glance, rewinding seems impossible with a quantum adversary since running the same circuit multiple times might modify its state's entanglement with some outside reference state and change the overall system's behavior. In a breakthrough paper, Watrous [36] showed that a specific type of zero-knowledge proof can be proven secure using a rewinding argument tailored to quantum adversaries. Damgård and Lunemann showed that a similar analysis can be applied to a variant of Blum's coin flipping protocol [19]. Some information-theoretically secure classical protocols are also known to resist quantum attacks [13, 2, 21, 35]. Finally, there is longer line of work on protocols that involve quantum communication (dating back to the Bennett-Brassard key exchange protocol). Overall, however, little is known about how much of the classical theory can be carried over to quantum settings (see "Related Work", below, for more detail).

[*] Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, U.S.A. An extended version of this abstract can be found at `http://www.cse.psu.edu/~fus121/cpq_qip.html`

2 Our Contributions

Our main contribution is showing the existence of classical two-party protocols for the secure evaluation (SFE) of any polynomial-time function that are secure against quantum attacks under reasonable computational assumptions (for example, it suffices that the learning with errors problem [30] be hard for quantum polynomial time). Our result shows that *the basic two-party feasibility picture from classical cryptography remains unchanged in a quantum world.* The only two-party general SFE protocols which had previously been analyzed in the presence of quantum attackers required quantum computation and communication on the part of the honest participants (e.g. [11]).

More precisely, we show that a large class of classical security analyses remain valid in the presence of quantum attackers as long as the underlying computational primitives (encryption schemes, pseudorandom generators, etc) resist quantum attack. In what follows, we distinguish two basic settings: in the *stand-alone* setting, protocols are designed to be run in isolation, without other protocols running simultaneously; in *network* settings, the protocols must remain secure even when the honest participants are running many other protocols (or copies of the same protocol) concurrently. Protocols that are secure in arbitrary network settings are called *universally composable*. Our contributions can be broken down as follows:

Modeling stand-alone security with quantum adversaries. We describe a security model for two-party protocols in the presence of a quantum attackers. Proving security in this model amounts to showing that a protocol for computing a function f behaves indistinguishably from an "ideal" protocol in which f is computed by a trusted third party. Our model is a quantum analogue of the model of stand-alone security developed by Canetti [7] in the classical setting. Our model is more restrictive than the quantum UC framework of Unruh [35], in that it does not provide any security guarantees when a protocol is executed concurrently with other protocols in a network; however, this also means that the model applies to a much broader class of protocols. Our model captures both classical and quantum protocols, though we only apply it to classical ones.

We also show a composition theorem for protocols analyzed in our model. Roughly, it states that one can design protocols modularly, treating sub-protocols as equivalent to their ideal versions when analyzing security of a high-level protocol (for instance, one can treat a coin-flipping protocol as a trusted party who hands all participants a uniformly random string).

The new model is significantly more general than existing stand-alone models of security; see "Related Work" below. In particular, the recent coin-flipping protocol of Damgård and Lunemann (DL) [19] fits our model. This allows us to design protocols assuming that all participants share a uniformly random common reference string (CRS). By the modular composition theorem, we can then use the DL coin-flipping protocol to generate the CRS.

Classical UC Protocols in a Quantum Context: Towards Unruh's Conjecture. We show that a large class of protocols which are UC-secure against computationally-bounded classical adversaries are also UC-secure against quantum adversaries. In his recent paper, Unruh [35] showed that any classical protocol which is proven UC secure against unbounded classical adversaries is also UC-secure against unbounded quantum adversaries. He conjectured (roughly, see [35] for the exact statement) that classical arguments of *computational* UC security should also go through as long as the underlying computational primitives are not easily breakable by quantum computers.

We provide some support for this conjecture by describing a class of classical security arguments that go through verbatim with quantum adversaries. We call these arguments "simple hybrid" arguments. Our observation allows us to port a general result of Canetti, Lindell, Ostrovsky and Sahai [9] to the quantum setting. We obtain the following: if there exists a classical protocol for zero-knowledge proofs that is UC-secure against quantum adversaries then, under reasonable computational assumptions, there exist classical protocols for the evaluation of any polynomial-time function f that are UC-secure against quantum adversaries. Finally, we describe a simple classical protocol for zero-knowledge proofs which is quantum-UC secure in a model where all participants have access to a common uniformly-distributed random string (known as the *CRS model*). Only one component of our ZK protocol, a construction of witness-indistinguishable proofs, does not fit the "simple hybrid" model; for that component we provide a direct proof of security.

The conclusion is that, as in the classical world, the availability of a common reference string allows for the implementation of UC-secure SFE protocols.

Implications. Combining our (stand-alone) modular composition result with the DL coin-flipping protocol and the UC-secure protocols in the CRS model, we get two interesting implications:

First, there exist classical SFE protocols in the plain model (without a shared random string) which are stand-alone-secure against quantum attackers.

Second, there exist classical proofs of knowledge which are "witness-extendable" [25] even against quantum adversaries, in the sense that one can simulate an interaction with a malicious prover while simultaneously extracting a witness to the statement whenever the prover is successful. This overcomes a limitation of the proofs of knowledge recently analyzed by Unruh [34].

3 Related Work

In addition to the previous work mentioned above, we expand here on two categories of related efforts.

Composition Frameworks for Quantum Protocols. Systematic investigations of the composition properties of quantum protocols are relatively recent.[1] Canetti's UC framework and Pfitzmann and Waidner's closely related *reactive functionality* framework were extended to the world quantum protocols and adversaries by Ben-Or and Mayers [27] and Unruh [32, 35]. These frameworks (which share similar semantics) provide extremely strong guarantees—security in arbitrary network environments. They were used to analyze a number of unconditionally-secure quantum protocols (key exchange [4] and multi-party computation with honest majorities [2])). However, many protocols are not universally composable, and Canetti [8] showed that classical protocols cannot UC-securely realize even basic tasks such as commitment and zero-knowledge proofs without some additional setup assumptions such as a CRS or public-key infrastructure.

The only general composition framework we know of for stand-alone protocols is that of Fehr and Schaffner [21], which applies only to information-theoretically secure protocols of a particular form (where quantum communication occurs only at the lowest levels of the modular composition). Our framework is significantly more general. It is expressive enough to capture computationally secure quantum protocols such as those of Watrous and Damgård-Lunemann.

Analyses of quantum protocols. The first careful proofs of security of quantum protocols were for key exchange (Mayers, Lo and Chau, Shor-Preskill, Beaver). Research on quantum protocols for two-party tasks such as coin-flipping, bit commitment and oblivious transfer dates back farther [6, 5] but many initially proposed protocols were insecure [26]. The first proofs of security of such protocols were based on computational assumptions [20, 12]. They were highly protocol-specific and it was not known how well the protocols composed. The first proofs of security using the simulation paradigm were for information-theoretically-secure protocols for multiparty computations assuming a strict majority of honest participants [13, 14, 2]. Subsequently, a line of work on the *bounded quantum storage* model [18, 17, 21, 16, 33] developed tools for reasoning about specific types of composition of two-party protocols, under assumptions on the size of the adversary's quantum storage. Unruh's UC security work, mentioned above, was the first we are aware of that was sufficiently general to encompass classical and quantum protocols and generic composition.

[1] Only last year, Fehr and Schaffner wrote: "It is still common practice in quantum cryptography that every paper proposes its own security denition of a certain task and proves security with respect to the proposed definition. However, it usually remains unclear whether these definitions are strong enough to guarantee any kind of composability, and thus whether protocols that meet the denition really behave as expected." [21]

References

[1] ACM. *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, 2-4 May 1988, Chicago, Illinois, USA*. ACM, 1988.

[2] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *FOCS*, pages 249–260. IEEE Computer Society, 2006.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC* [1], pages 1–10.

[4] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In J. Kilian, editor, *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406. Springer, 2005.

[5] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer. In J. Feigenbaum, editor, *CRYPTO*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 1991.

[6] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In A. Menezes and S. A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 49–61. Springer, 1990.

[7] R. Canetti. Security and composition of multiparty cryptographic protocols. *J. Cryptology*, 13(1):143–202, 2000.

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

[9] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party and multi-party secure computation. In *STOC*, pages 494–503, 2002.

[10] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *STOC* [1], pages 11–19.

[11] C. Crépeau, P. Dumais, D. Mayers, and L. Salvail. Computational collapse of quantum state with application to oblivious transfer. In Naor [28], pages 374–393.

[12] C. Crépeau, P. Dumais, D. Mayers, and L. Salvail. Computational collapse of quantum state with application to oblivious transfer. In Naor [28], pages 374–393.

[13] C. Crépeau, D. Gottesman, and A. Smith. Secure multi-party quantum computation. In *STOC*, pages 643–652, 2002.

[14] C. Crépeau, D. Gottesman, and A. Smith. Approximate quantum error-correcting codes and secret sharing schemes. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 285–301. Springer, 2005.

[15] C. Crépeau, L. Salvail, J.-R. Simard, and A. Tapp. Classical and quantum strategies for two-prover bit commitments. Manuscript, 2006.

[16] I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner. Improving the security of quantum protocols via commit-and-open. In S. Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 408–427. Springer, 2009.

[17] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and qkd in the bounded-quantum-storage model. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer, 2007.

[18] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.*, 37(6):1865–1890, 2008.

[19] I. Damgård and C. Lunemann. Quantum-secure coin-flipping and applications. In M. Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 52–69. Springer Berlin / Heidelberg, 2009.

[20] P. Dumais, D. Mayers, and L. Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In B. Preneel, editor, *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 300–315. Springer, 2000.

[21] S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. In O. Reingold, editor, *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2009.

[22] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC*, pages 218–229, New York City, 25–27 May 1987.

[23] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity for all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.

[24] S. Hallgren. Polynomial-time quantum algorithms for pell's equation and the principal ideal problem. *J. ACM*, 54(1), 2007.

[25] Y. Lindell. Parallel coin-tossing and constant-round secure two-party computation. *J. Cryptology*, 16(3):143–184, 2003.

[26] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, 2001.

[27] D. M. Michael Ben-Or. General security definition and composability for quantum and classical protocols, September 2004. Online available at `http://arxiv.org/abs/quant-ph/0409062`.

[28] M. Naor, editor. *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*. Springer, 2004.

[29] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). pages 73–85. ACM, 1989.

[30] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):1–40, 2009.

[31] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[32] D. Unruh. Simulatable security for quantum protocols. arXiv:quant-ph/0409125, 2004.

[33] D. Unruh. Concurrent composition in the bounded quantum storage model, April 2010. Preprint on IACR ePrint 2010/229.

[34] D. Unruh. Quantum proofs of knowledge, April 2010. Preprint on IACR ePrint 2010/212.

[35] D. Unruh. Universally composable quantum multi-party computation. In H. Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 486–505. Springer, 2010.

[36] J. Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.