Classical Cryptographic Protocols in a Quantum World

Sean Hallgren*, Adam Smith**, and Fang Song

Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, U.S.A.

Abstract. Cryptographic protocols, such as protocols for secure function evaluation (SFE), have played a crucial role in the development of modern cryptography. The extensive theory of these protocols, however, deals almost exclusively with classical attackers. If we accept that quantum information processing is the most realistic model of physically feasible computation, then we must ask: what classical protocols remain secure against quantum attackers?
Our main contribution is showing the existence of classical two-party protocols for the secure evaluation of any polynomial-time function under reasonable computational assumptions (for example, it suffices that the learning with errors problem 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.

1 Introduction

Cryptographic protocols, such as protocols for secure function evaluation (SFE), have played a crucial role in the development of modern cryptography. Goldreich, Micali and Wigderson [25], building on the development of zero-knowledge (ZK) proof systems [27,26], showed that SFE protocols exist for any polynomial-time function under mild assumptions (roughly, the existence of secure public-key cryptosystems). Research into the design and analysis of such protocols is now a large subfield of cryptography; it has also 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. However, given our current understanding of physics, quantum information processing is the most realistic model of physically feasible computation. It is natural to ask: *what classical protocols remain secure against quantum attackers?* In many cases, even adversaries with modest quantum computing capabilities, such as the ability to share and store entangled photon pairs, are not covered by existing proofs of security.

Clearly not all protocols are secure: we can rule out anything based on the computational hardness of factoring, the discrete log [43], or the principal ideal problem [28]. More subtly, the basic techniques used to reason about security may not apply in a

* Partially supported by National Science Foundation award CCF-0747274 and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-08-1-0298.

** Partially supported by National Science Foundation award CCF-0747294.

quantum setting. For example, some information-theoretically secure two-prover ZK and commitment protocols are analyzed by viewing the provers as long tables that are fixed before queries are chosen by the verifier; quantum entanglement breaks that analysis and some protocols are insecure against colluding quantum provers (Crépeau *et al.*, [17]).

In the computational realm, *rewinding* is a key technique for basing the security of a protocol on the hardness of some underlying problem. Rewinding proofs consist of a mental experiment in which the adversary is run multiple times using careful variations of a given input. At first glance, rewinding seems impossible with a quantum adversary since running it multiple times might modify the entanglement between its internal storage and an outside reference system, thus changing the overall system's behavior.

In a breakthrough paper, Watrous [49] showed that a specific type of zero-knowledge proof (3-round, GMW-style protocols) can be proven secure using a rewinding argument tailored to quantum adversaries. Damgård and Lunemann [21] showed that a similar analysis can be applied to a variant of Blum's coin flipping protocol. Hallgren *et al.* [29] showed certain classical transformations from honest-verifier to malicious-verifier ZK can be modified to provide security against malicious quantum verifiers. Some information-theoretically secure classical protocols are also known to resist quantum attacks [15,5,23,47]. Finally, there is a longer line of work on protocols that involve quantum communication, dating back to the Bennett-Brassard key exchange paper. 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.

1.1 Our Contributions

Our main contribution is showing the existence of classical two-party protocols for the secure evaluation of any polynomial-time function under reasonable computational assumptions (for example, it suffices that the learning with errors problem [42] 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. [14,18]).

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 other protocols (or copies of the same protocol) concurrently. Protocols proven secure in the *universal composability* (UC) model [11] are secure in arbitrary network settings, but UC-security is impossible to achieve in many settings.

Our contributions can be broken down as follows:

Classical Zero-knowledge Arguments of Knowledge Secure Against Quantum Adversaries. We construct a classical zero-knowledge argument of knowledge (ZKAoK) protocol that can be proven secure in our model. In particular it means that our construction is "witness-extendable" [33] in the sense that one can simulate an interaction with a malicious prover and simultaneously extracting a witness of the statement whenever

the prover succeeds. Our construction overcomes a limitation of the proofs of knowledge recently analyzed by Unruh [46], where a simulator for the prover is not given, and thus it is unclear how to analyze security when using his proof of knowledge as a subprotocol. As in the classical case, our ZKAoK protocol is an important building block in designing general SFE protocols.

The main idea behind our construction is to have the prover and verifier first execute a weak coin-flipping protocol to generate a public key for a special type of encryption scheme. The prover encrypts his witness with respect to this public key and proves consistency of his ciphertext with the statement x using the ZK protocols analyzed by Watrous [49]. A simulator playing the role of the verifier can manipulate the coin-flipping phase to generate a public key for which she knows the secret key, thus allowing her to extract the witness without needing to rewind the prover. A simulator playing the role of the prover, on the other hand, cannot control the coin flip (to our knowledge) but can ensure that the public key is nearly random. If the encryption scheme satisfies additional, non-standard properties (that can be realized under widely used lattice-type assumptions), we show that the verifier's view can nonetheless be faithfully simulated. Lunemann and Nielsen [36] independently gave a similarly-flavored construction of ZKAoK for quantum adversaries; see "Related Work".

(More) General modeling of 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, which we call the ideal functionality $\mathcal{F}$. Our model is a quantum analogue of the model of stand-alone security developed by Canetti [10] in the classical setting. It slightly generalizes the existing model of Damgård *et al.*[18] in two ways. First, our model allows for protocols in which the ideal functionalities that process quantum information (rather than only classical functionalities). Second, it allows for adversaries that take arbitrary quantum advice, and for arbitrary entanglement between honest and malicious players' inputs.

We also show a sequential modular composition theorem for protocols analyzed in our model. Roughly, it states that one can design protocols modularly, treating subprotocols as equivalent to their ideal versions when analyzing security of a high-level protocol. While the composition results of Damgaard *et al.* allow only for classical high-level protocols, our result holds for arbitrary quantum protocols.

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 [47] 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 [47] 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 support for this conjecture by describing a family of classical security arguments that go through verbatim with quantum adversaries. We call these arguments

"simple hybrid arguments". They use rewinding neither in the simulation nor in any of the steps that show the correctness of simulation.[1]

Our observation allows us to port a general result of Canetti, Lindell, Ostrovsky and Sahai [13] to the quantum setting. We obtain the following: in the $\mathcal{G}_{ZK}$-hybrid model, where an ideal functionality $\mathcal{G}_{ZK}$ implementing ZKAoK is available, there exist classical protocols for the evaluation of any polynomial-time function f that are UC-secure against quantum adversaries under reasonable computational assumptions.

As an immediate corollary, we get a classical protocol that quantum UC-emulates ideal functionality $\mathcal{G}_{CF}$ for coin-flipping. Adapting ideas from [33], we also give a direct construction of coin-flipping from ZK. More interestingly, we can develop the converse by describing a simple classical protocol for ZKAoK that is UC-secure against quantum adversaries in the $\mathcal{G}_{CF}$-hybrid model (a.k.a the *common reference string model* where all participants have access to a common, uniformly distributed bit string). The "simple hybrid arguments" mentioned above do not suffice for proving the security of the UC-secure ZKAoK protocol. Specifically, one component of our protocol, a construction of a *witness-indistinguishable* proof system, needs a new proof of security. The basic strategy is still a hybrid argument, but its analysis requires breaking the space of possible executions into pieces (classically, this involves conditioning on complementary events; quantumly, this involves projecting onto orthogonal subspaces) and arguing that (a) the adversary cannot have a significant advantage in either piece and (b) the original state was a mixture, not a superposition, of the two pieces. This establishes the equivalence between $\mathcal{G}_{ZK}$ and $\mathcal{G}_{CF}$ in the UC model, which may be of independent interest, e.g., in simplifying protocol designs.

Implications. The modular composition theorem in our stand-alone model allows us to get the general feasibility result below by combining our stand-alone ZKAoK protocol and the UC-secure protocols in $\mathcal{G}_{ZK}$-hybrid model:

Under standard assumptions, *there exist* classical *SFE protocols in the plain model (without a shared random string) which are stand-alone-secure against static* quantum *adversaries*. This parallels the classic result of Goldreich, Micali and Wigderson [25].

The equivalence of zero-knowledge and coin-flipping functionalities in the UC model also gives rise to interesting implications. First, the availability of a common reference string suffices for implementing quantum UC-secure protocols. Secondly, given our stand-alone ZKAoK protocol, we get a quantum stand-alone coin-flipping protocol due to the aforementioned equivalence.

Independently of our work, Lunemann and Nielsen [36] obtained similar results to ours. See the discussion at the end of "Related Work".

1.2 Related work

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

[1] In general, it is hard to clearly define what it means for a security proof to "not use rewinding". It is not enough for the protocol to have a straight-line simulator, since the proof of the simulator's correctness might still employ rewinding. Simple hybrid arguments provide a clean, safe subclass of arguments that go through with quantum adversaries.

Composition Frameworks for Quantum Protocols. Systematic investigations of the composition properties of quantum protocols are relatively recent. Canetti's UC framework and Pfitzmann and Waidner's closely related *reactive functionality* framework were extended to the world of quantum protocols and adversaries by Ben-Or and Mayers [7] and Unruh [45,47]. 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 [6] and multi-party computation with honest majorities [5]). However, many protocols are not universally composable, and Canetti [11] 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.

Damgård *et al.*[18], building on work by Fehr and Schaffner [23], proposed a general composition framework which applies only to secure quantum protocols of a particular form (where quantum communication occurs only at the lowest levels of the modular composition). As noted earlier, our model is more general and captures both classical and quantum protocols. That said, understanding the exact relationship between the models is delicate, and connected to basic questions in complexity theory such as the power of quantum advice (BQP/poly vs BQP/qpoly). We defer further discussion of this relationship to the full version.

Analyses of quantum protocols. The first careful proofs of security of quantum protocols were for key exchange (Mayers [37], Lo and Chau [35], Shor and Preskill [44], Beaver [2]). Research on quantum protocols for two-party tasks such as coin-flipping, bit commitment and oblivious transfer dates back farther [9,8] but many initially proposed protocols were insecure [37]. The first proofs of security of such protocols were based on computational assumptions [22,14]. 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 multi-party computations assuming a strict majority of honest participants [15,16,5]. Subsequently, a line of work on the *bounded quantum storage* model [20,19,23,48] 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.

Straight-line simulators and code-based games. As mentioned above, we introduce "simple hybrid arguments" to capture a class of straightforward security analyses that go through against quantum adversaries. Several formalisms have been introduced in the past to capture classes of "simple" security arguments. To our knowledge, none of them is automatically compatible with quantum adversaries. For example, *straight-line black-box simulators* [32] do not rewind the adversary nor use an explicit description of its random coins; however, it may be the case that rewinding is necessary to prove that the straight-line simulator is actually correct. In a different vein, the *code-based games* of Bellare and Rogaway [4] capture a class of hybrid arguments that can be encoded in a clean formal language; again, however, the arguments concerning each step of the hybrid may still require rewinding.

Independent Work: Lunemann and Nielsen [36]. Lunemann and Nielsen [36] independently obtained similar results to the ones described here, via a slightly different route. Specifically, they start by constructing a stand-alone coin-flipping protocol that is fully simulatable against quantum poly-time adversaries. Then they use the coin-flipping protocol to construct a stand-alone ZKAoK protocol, and finally by plugging into the GMW construction, they get quantum stand-alone-secure two-party SFE protocols as well. The computational assumptions in the two works are similar and the round complexities of the stand-alone SFE protocols are both polynomial in the security parameter. Our approach to composition is more general, however, leading to results that also apply (in part) to the UC model.

Organization. The rest of the paper is organized as follows: Section 2 reviews basic notations and definitions. In Section 3, we propose our quantum stand-alone security model. A quantum stand-alone-secure ZKAoK protocol is developed in Section 4. Section 5 studies a family of classical analysis that go through in the quantum UC model, and then Section 6 discusses equivalence of $\mathcal{G}_{ZK}$ and $\mathcal{G}_{CF}$. Finally in Section 7, we obtain, among other consequences, classical SFE that are quantum stand-alone-secure with no set-up assumptions. We conclude with future directions.

2 Preliminaries

For $m \in \mathbb{N}$, $[m]$ denotes the set $\{1,\ldots,m\}$. We use $n \in \mathbb{N}$ to denote a *security parameter*. The security parameter, represented in unary, is an implicit input to all cryptographic algorithms; we omit it when it is clear from the context. Quantities derived from protocols or algorithms (probabilities, running times, etc) should be thought of as functions of n, unless otherwise specified. A function $f(n)$ is said to be negligible if $f = o(n^{-c})$ for any constant c, and $negl(n)$ is used to denote an unspecified function that is negligible in n. We also use $poly(n)$ to denote an unspecified function $f(n) = O(n^c)$ for some constant c. Let $\mathbf{X} = \{X_n\}_{n\in\mathbb{N}}$ and $\mathbf{Y} = \{Y_n\}_{n\in\mathbb{N}}$ be two ensembles of binary random variables. We call $\mathbf{X}$, $\mathbf{Y}$ *indistinguishable*, denoted $\mathbf{X} \approx \mathbf{Y}$, if $|\Pr(X_n = 1) - \Pr(Y_n = 1)| \leq negl(n)$.

We assume the reader is familiar with the basic concepts of quantum information theory (see, e.g., [39]). We use a capital letter (e.g. X) to denote a quantum register and for each n, we use script letter (e.g., $\mathcal{X}(n)$) to denote the corresponding Hilbert space. Let $D(\mathcal{H})$ be the set of density operators acting on space $\mathcal{H}$. Let $\{\rho_n\}_{n\in\mathbb{N}}$ denote an ensemble of mixed states where $\rho_n \in D(\mathcal{H}_n)$ and $\mathcal{H}_n$ is a $poly(n)$-qubit space.

Quantum Machine Model. We adapt Unruh's machine model in [47] with minor changes. A *quantum interactive machine* (QIM) M is an ensemble of circuits $\{M_n\}_{n\in\mathbb{N}}$, for each value n of the security parameter. M operates on three registers: a state register S used for input and workspace; an output register O; and a network register N for communicating with other machines. We say the size (or running time) of M is $t(n)$, if there is a deterministic classical Turing machine that computes the description of M_n in time $t(n)$ on input 1^n. We say a machine is polynomial time if $t(n) = poly(n)$.

When two QIMs M and M' interact, their network register N is shared. The circuits M_n and ${M'}_n$ are executed alternately. When three or more machines interact, the machines may share different parts of their network registers (for example, a private

channel consists of a register shared between only two machines; a broadcast channel is a register shared by all machines). The order in which machines are activated may be either specified in advance (as in a synchronous network) or adversarially controlled.

A noninteractive quantum machine (referred to as QTM hereafter) is a QIM M with no network register that runs for only one round (for all n). This is equivalent to the *quantum Turing machine* model (see [50]). A classical interactive machine is a special case of a QIM, where the registers only store classical strings and all circuits are classical. Classical polynomial-time QIMs are equivalent to polynomial-time interactive Turing machines.

Indistinguishability of Quantum States. Recall Watrous's notion of indistinguishability of quantum states.

Definition 1. *((t,ϵ)-indistinguishable quantum states. [49, Definition 2]) We say two quantum state ensembles $\rho = \{\rho_n\}_{n\in\mathbb{N}}$ and $\eta = \{\eta_n\}_{n\in\mathbb{N}}$ are (t,ϵ)-quantum-indistinguishable, denoted $\rho \approx_Q^{t,\epsilon} \eta$, if for every $t(n)$-time QTM $\mathcal{Z}$ and every mixed state $\sigma_n \in \mathcal{W}(n)$, $\mathcal{W}(n)$ is a $t(n)$-qubit auxiliary system,*

$$|\Pr[\mathcal{Z}(\rho_n \otimes \sigma_n) = 1] - \Pr[\mathcal{Z}(\eta_n \otimes \sigma_n) = 1]| \leq \epsilon(n).$$

The states ρ and η are called *quantum computationally indistinguishable*, denoted $\rho \approx_Q \eta$, if for every $t(n) \leq poly(n)$, there exists a negligible $\epsilon(n)$ such that ρ_n and η_n are (t,ϵ)-indistinguishable. This definition subsumes classical distributions, since classical distributions can be represented by density matrices that are diagonal with respect to the standard basis.

Indistinguishability of quantum machines. Next we define indistinguishability of quantum interactive machines. Let $\mathcal{Z}, M$ be two QIMs, we denote $\langle \mathcal{Z}(\sigma), M\rangle$ as the process that $\mathcal{Z}$ with auxiliary input σ, interacts with M and finally $\mathcal{Z}$ outputs one classical bit 1 or 0.

Definition 2 ((t,ϵ)-indistinguishable QIMs). *We say two QIMs M_1 and M_2 are (t,ϵ)-*interactively indistinguishable*, denoted $M_1 \approx_I^{t,\epsilon} M_2$, if for any quantum $t(n)$-time interactive machine $\mathcal{Z}$ and every mixed state σ_n on $t(n)$ qubits, $\mathbf{X_1} \approx \mathbf{X_2}$, where $\mathbf{X}_i = \{\langle \mathcal{Z}(\sigma_n), M_i\rangle\}_{n\in\mathbb{N}}$ for $i = 1,2$. QIMs M_1 and M_2 are called* interactively indistinguishable*, denoted $M_1 \approx_I M_2$, if for every $t(n) \leq poly(n)$, there exists a negligible $\epsilon(n)$ such that M_1 and M_2 are (t,ϵ)-interactively indistinguishable.*

Finally we state the computational assumptions that we make in this work.

Assumption 1 *There exists a classical pseudorandom generator secure against quantum distinguishers.*

Based on this assumption and the construction of [38], we can obtain a statistically binding and quantum computationally hiding commitment scheme $(\mathbf{comm}, \mathbf{decom})$. All commitment scheme we use afterwards refers to this one. This assumption also suffices for Watrous's ZK proof system for any NP-language against quantum attacks.

Assumption 2 *There exists a* dense *classical public-key cryptosystem that is IND-CPA (chosen-plaintext attack) secure against quantum distinguishers. A public-key cryptosystem is dense if a valid public key is indistinguishable in quantum poly-time from a uniformly random string of the same length.*

Although it is likely that standard reductions would show that Assumption 2 implies Assumption 1, we chose to keep the assumptions separate because the instantiation one would normally use of the pseudorandom generator would not be related to the public-key system (instead, it would typically be based on a symmetric-key block or stream cipher). Both assumptions hold, for instance, assuming the hardness of *leaning with errors* (LWE) problem [42].

In one of our constructions (stand-alone ZKAoK), we need an encryption scheme that has one extra property than the one in Assumption 2.

Assumption 3 *There exists a dense classical public-key cryptosystem that is IND-CPA secure against quantum distinguishers. In addition, encryptions of two messages under a uniformly random string are statistically indistinguishable.*

Note that the *dense* property already implies encryptions under a random string are quantum computationally indistinguishable. Assumption 3 strengthens this requirement to be statistically indistinguishable. This allows "cheating" in the sense that if a ciphertext is generated under a uniformly random string, we can then claim it to be an encryption of an arbitrary message. This type of encryption scheme is sometimes called Meaningful/Meaningless encryption (e.g., see [31]). Again, the LWE assumption implies Assumption 3.

3 Quantum Stand-alone Security and Modular Composition

In this section, we propose a stand-alone security model for two-party protocols in the presence of quantum attacks and show that modular composition holds in our model. Our definition can be viewed in two ways: either as a quantum analogue of Canetti's classical stand-alone model [10] or as a relaxed notion of a variant of Unruh's quantum UC security [47].

3.1 Security Definition

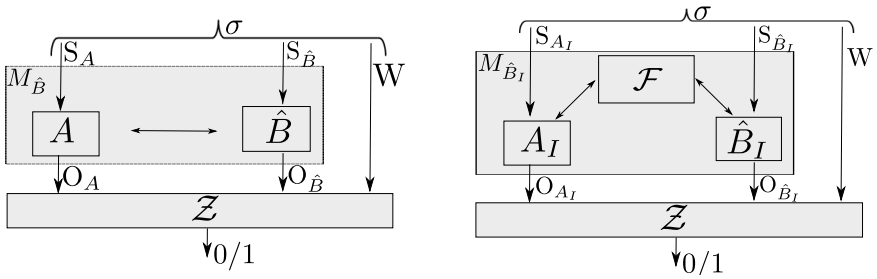
A two-party protocol Π consists of two quantum interactive machines $\mathbf{A}$ and $\mathbf{B}$. Two players Alice and Bob that execute Π are called honest if they run machines $\mathbf{A}$ and $\mathbf{B}$ respectively. An adversary in Π is one entity that corrupts some player and controls its behavior. We consider both *semi-honest* (a.k.a. *honest-but-curious*) and *malicious* adversaries. In the quantum setting, a semi-honest adversary runs the honest protocol *coherently*, that is, replacing measurements and classical operations with unitary equivalents.

We consider only *static* adversaries, which corrupt a set of players before the protocol execution starts, but do not perform further corruptions during the protocol execution. For ease of exposition, we merge the identities of an adversary and the party it corrupts. Machines run by an adversary are indicated by a $\hat{}$ symbol (e.g., $\hat{\mathbf{B}}$).

Our definition of security follows the *simulation paradigm* where we compare two modes of execution called *real-world* and *ideal-world*. A *real-world* execution is an interaction between an honest player and a real-world adversary, e.g., $\mathbf{A}$ and $\hat{\mathbf{B}}$. In an *ideal world*, there is a trusted party that communicates with $\mathbf{A}_I$ and $\mathbf{B}_I$ (subscript I indicates entities in the ideal world) through private channels and completes the desired task. We model the trusted party as a quantum interactive machine, and call it an *ideal functionality* $\mathcal{F}$. For example, in the secure evaluation of a function f, an ideal functionality $\mathcal{F}$ would take inputs (x,y) from $\mathbf{A}_I$ and $\mathbf{B}_I$ respectively, compute $(f_A, f_B) = f(x,y)$ and give f_A to $\mathbf{A}_I$ and f_B to $\mathbf{B}_I$. We then say a protocol Π securely realizes a given task, formulated by an ideal functionality $\mathcal{F}$, if for any adversary $\hat{\mathbf{B}}$ attacking a real-world execution, there exists an ideal-world adversary $\hat{\mathbf{B}}_I$ emulating "equivalent" attacks in the ideal-world. Equivalent means on any input state the output states of the players in the real world and ideal world are indistinguishable.

To be more specific, in the real world we initialize $\mathrm{S}_{\mathbf{A}}$, $\mathrm{S}_{\hat{\mathbf{B}}}$ and an auxiliary register W with a quantum state $\sigma_n \in \mathcal{S}_{\mathbf{A}}(n) \otimes \mathcal{S}_{\hat{\mathbf{B}}}(n) \otimes \mathcal{W}(n)$. Then $\mathbf{A}$ and $\hat{\mathbf{B}}$ interact, and end up with a state $\sigma'_n \in \mathcal{O}_{\mathbf{A}}(n) \otimes \mathcal{O}_{\hat{\mathbf{B}}}(n) \otimes \mathcal{W}(n)$. Finally a QTM $\mathcal{Z}$, which we call an *environment*, takes σ'_n as input and outputs one classical bit. Abstractly, we treat $\mathbf{A}$ and $\hat{\mathbf{B}}$ collectively as a noninteractive machine $M_{\hat{\mathbf{B}}}$ with state space $\mathcal{S}_{\mathbf{A}} \otimes \mathcal{S}_{\hat{\mathbf{B}}}$ and output space $\mathcal{O}_{\mathbf{A}} \otimes \mathcal{O}_{\hat{\mathbf{B}}}$. Analogously, for each ideal world adversary $\hat{\mathbf{B}}_I$, we can model $\mathbf{A}_I$, $\hat{\mathbf{B}}_I$ and $\mathcal{F}$ as a single QTM $M_{\hat{\mathbf{B}}_I}$ with state space $\mathcal{S}_{\mathbf{A}_I} \otimes \mathcal{S}_{\hat{\mathbf{B}}_I}$ and output space $\mathcal{O}_{\mathbf{A}_I} \otimes \mathcal{O}_{\hat{\mathbf{B}}_I}$. Then let $\mathbf{EXEC}_{\Pi,\hat{\mathbf{B}},\mathcal{Z}} := \{\mathcal{Z}((M_{\hat{\mathbf{B}}} \otimes \mathbb{1}_{\mathcal{W}(n)})\sigma_n)\}_{n\in\mathbb{N}}$ and $\mathbf{IDEAL}_{\mathcal{F},\hat{\mathbf{B}}_I,\mathcal{Z}} := \{\mathcal{Z}((M_{\hat{\mathbf{B}}_I} \otimes \mathbb{1}_{\mathcal{W}(n)})\sigma_n)\}_{n\in\mathbb{N}}$ be the binary distribution ensembles of $\mathcal{Z}$'s output in the real-world execution and in the ideal-world execution respectively. See Fig. 1 for an illustration of real-world and ideal-world executions.

Fig. 1. Real-world and Ideal-world Executions



(a) Real-world execution $\mathbf{EXEC}_{\Pi,\hat{\mathbf{B}},\mathcal{Z}}$ (b) Ideal-world execution $\mathbf{IDEAL}_{\mathcal{F},\hat{\mathbf{B}}_I,\mathcal{Z}}$

Definition 3. *(Quantum Stand-alone Secure Emulation). Let $\mathcal{F}$ be a two-party functionality and let Π be a two-party protocol. We say* Π quantum stand-alone-emulates *$\mathcal{F}$, if for any poly-time QIM $\hat{\mathbf{B}}$, there is a poly-time QIM $\hat{\mathbf{B}}_I$, such that for any poly-time QTM $\mathcal{Z}$, and for any $\sigma = \{\sigma_n : \sigma_n \in \mathcal{S}_{\mathbf{A}}(n) \otimes \mathcal{S}_{\hat{\mathbf{B}}}(n) \otimes \mathcal{W}(n)\}_{n\in\mathbb{N}}$, $\mathbf{EXEC}_{\Pi,\hat{\mathbf{B}},\mathcal{Z}} \approx \mathbf{IDEAL}_{\mathcal{F},\hat{\mathbf{B}}_I,\mathcal{Z}}$.*

Remark. (I) Equivalently, the definition can be formulated as: for any $\hat{\mathbf{B}}$, there exists $\hat{\mathbf{B}}_I$, such that QTMs $M_{\hat{\mathbf{B}}}$ and $M_{\hat{\mathbf{B}}_I}$ are indistinguishable, as per Definition 2 restricting to non-interactive machines. (II) We focus on computational security in this work, and the model extends to information-theoretical setting straightforwardly. (III) We stress that σ not only encodes the inputs to the players, but also contains auxiliary system $\mathcal{W}$ that might be entangled with the inputs and moreover serves as quantum advice to later assist $\mathcal{Z}$ in distinguishing the two worlds. There are other possible choices in the definition, e.g., disallowing auxiliary system $\mathcal{W}$ and only giving $\mathcal{Z}$ classical advice, which may give rise to variants that coincide with or subsume existing models. See the full version for a thorough discussion. (IV) For technical reasons, we require functionalities to be *well-formed* and protocols to be *nontrivial*, which are satisfied by all functionalities and protocols in our paper. (See [13, Sect.3] for details.) Aside from that, $\mathcal{F}$ could be as general as randomized, reactive, and evaluating quantum circuits, though in this work we concentrate on SFE of classical functions.

3.2 Modular Composition

It is common practice in the design of large protocols that we break a given task into subtasks, accomplish these subtasks and then use these modules as building blocks (subroutines) in a solution for the initial task. We formalize this paradigm by *hybrid models*[2]. A protocol in the *$\mathcal{G}$-hybrid model*, denoted $\Pi^{\mathcal{G}}$, has access to a trusted party that implements ideal functionality $\mathcal{G}$. As before, for each adversary $\hat{\mathbf{B}}_H$ (subscript H indicates entities in a hybrid model) in the $\mathcal{G}$-hybrid model, we can define $M_{\hat{\mathbf{B}}_H}$ and $\mathbf{EXEC}_{\Pi^{\mathcal{G}},\hat{\mathbf{B}}_H,\mathcal{Z}}$ likewise. Then we say $\Pi^{\mathcal{G}}$ quantum stand-alone-emulates ideal functionality $\mathcal{F}$ in the $\mathcal{G}$-hybrid model if $\mathbf{EXEC}_{\Pi^{\mathcal{G}},\hat{\mathbf{B}}_H,\mathcal{Z}} \approx \mathbf{IDEAL}_{\mathcal{F},\hat{\mathbf{B}}_I,\mathcal{Z}}$ for all poly-time QTMs $\mathcal{Z}$ and all σ.

Now suppose we have $\Pi_1^{\mathcal{G}}$ in the $\mathcal{G}$-hybrid model and a protocol Π_2 realizing $\mathcal{G}$. The operation of replacing an invocation of $\mathcal{G}$ with an invocation of Π_2 is done in the natural way: machines in Π_1 initialize machines in Π_2 and pause; machines in Π_2 execute Π_2 and generate outputs; then Π_1 resumes with these outputs. We denote the composed protocol $\Pi_1^{\Pi_2}$.

Theorem 1. *(Modular Composition Theorem) Let $\Pi_1^{\mathcal{G}}$ be a two-party protocol that quantum stand-alone-emulates $\mathcal{F}$ in the $\mathcal{G}$-hybrid model and let Π_2 be a two-party protocol that quantum stand-alone-emulates $\mathcal{G}$. Then the composed protocol $\Pi_1^{\Pi_2}$ quantum stand-alone-emulates $\mathcal{F}$.*

Remark. See the full version for its proof. It is easy to extend our analysis to a more general case where Π can invoke $\mathcal{G}$ multiple times and also access polynomially many ideal functionalities ($\mathcal{G}_1, \mathcal{G}_2, \ldots$). However, we stress that at each round, only one functionality is invoked for at most once.

[2] In contrast, we call it a *plain model* if there are no trusted parties and no trusted setup assumptions like common reference string or public-key infrastructure, etc.

4 Quantum Stand-Alone-Secure ZK Arguments of Knowledge

A very important building block in cryptographic protocols is *Zero-Knowledge Arguments of Knowledge* (ZKAoK) for NP, formulated below as the ideal functionality $\mathcal{G}_{ZK}$. In this section we provide a construction that quantum stand-alone-emulates $\mathcal{G}_{ZK}$. Let $L \in$ NP and let $R_L = \{(x,w)|w \text{ is a witness of } x\}$. Assume the length of the witness is bounded above by a polynomial $w(n)$.

Ideal Functionality $\mathcal{G}_{ZK}$: prover $\mathbf{P}_I$; verifier $\mathbf{V}_I$; NP-relation R_L

- Upon receiving (x,w) from $\mathbf{P}_I$, $\mathcal{G}_{ZK}$ verifies $(x,w) \stackrel{?}{\in} R_L$. If yes, it sends x to $\mathbf{V}_I$; otherwise it halts.

Notice that this is indeed an argument of knowledge, since the prover has to explicitly show a valid witness to the trusted party.

Let $\mathcal{E} =$ (**Gen**, **Enc**, **Dec**) be a cryptosystem as in Assumption 3.

ZKAoK Protocol Π_{ZK}

Phase 1

1. $\mathbf{V}$ chooses $a \leftarrow \{0,1\}^n$ at random, and sends $\mathbf{P}$ a commitment of a: $c = \mathbf{comm}(a)$.
2. $\mathbf{P}$ sends $b \leftarrow \{0,1\}^n$ to $\mathbf{V}$.
3. $\mathbf{V}$ sends $\mathbf{P}$ string a.
4. $\mathbf{V}$ proves to $\mathbf{P}$ that c is indeed a commitment of a using Watrous's ZK protocol.
5. $\mathbf{P}$ and $\mathbf{V}$ set $pk = a \oplus b$ and interpret it as a public key.

Phase 2

1. $\mathbf{P}$, holding an instance x and a witness w, encrypts w under pk. Let $e = \mathbf{Enc}_{pk}(w)$. $\mathbf{P}$ sends (x,e) to $\mathbf{V}$.
2. $\mathbf{P}$ proves to $\mathbf{V}$ that e encodes a witness of x using Watrous's ZK protocol. $\mathbf{V}$ outputs x if it accepts in this ZK protocol. Otherwise it halts.

Theorem 2. *Protocol* Π_{ZK} *quantum stand-alone-emulates* $\mathcal{G}_{ZK}$.

The key idea lies in the inherent power of the simulator $\mathbf{S}$ of Watrous's ZK protocol. Namely, we can use $\mathbf{S}$ to generate a bogus proof that is indistinguishable from a real ZK proof run by a prover and a verifier, when we don't know a witness of a statement, or even when there isn't one, i.e., the statement is false. Specifically, an ideal-world $\hat{\mathbf{V}}_I$, receiving a true statement x from $\mathcal{G}_{ZK}$, needs to convince $\hat{\mathbf{V}}$ of the validity of x without knowing a witness. We do know that on true instances, i.e., the ciphertext e indeed encodes a witness w, $\mathbf{S}$ simulates a proof successfully by definition. The trouble then boils down to generating an encryption of w without knowing w. This might sound contradictory, but it is actually very natural. For instance, suppose a function f maps all strings to 0, then generating $f(r)$ without knowing r is trivial–just output 0! Our situation is more sophisticated, yet shares the same spirit. We need the fact that encryptions under a uniform string are statistically close. This implies, in particular, that encryption of any string under a uniform string pk, will coincide with $\mathbf{Enc}_{pk}(w)$ with high probability. In addition, if we let $\hat{\mathbf{V}}_I$ play an honest prover in Phase 1, the outcome pk will be guaranteed uniformly random. This shows how we handle corrupted verifiers.

On the other hand, in the case of a corrupted prover $\hat{\mathbf{P}}$, an ideal-world $\hat{\mathbf{P}}_I$ needs to extract a witness w from e when $\hat{\mathbf{P}}$ provides an accepting proof in Phase 2. The trick is that $\hat{\mathbf{P}}_I$ can use $\mathbf{S}$ to cheat in Phase 1 and force the outcome to be a real public key pk

of which he knows a corresponding secret key sk, so that $\hat{\mathbf{P}}_I$ can decrypt e to recover w in the end. The difficulty is that $\hat{\mathbf{P}}_I$ wants to make $a = pk \oplus b$, but it has to commit to a before seeing b. It turns out we could commit to 0^n, and later run $\mathbf{S}$ on the *false* statement that $\mathbf{comm}(0^n)$ is a commitment of a. $\mathbf{S}$ must behave equally well as if it is given a true statement $(\mathbf{comm}(a), a)$, because otherwise $\mathbf{S}$ will break the hiding property of the commitment scheme. The formal proof can be found in the full version.

5 Classical Protocols with Quantum UC Security

In this section, we investigate classical protocols in the quantum Universal Composability (UC) model. We propose a framework, *simple hybrid arguments*, to capture a large family of classical security analyses that also go through against quantum adversaries (under reasonable computational assumptions). Applying our framework to the classical results of Canetti et el. [13], we get classical protocols that quantum UC-securely realize two-party SFE in the $\mathcal{G}_{ZK}$-hybrid model.

Universally Composable (UC) security, proposed in the classical context by Canetti [11], differs from the stand-alone definition of security in that the environment is allowed to be *interactive*: during the execution of the protocol, the environment may provide inputs and receive the outputs of the honest players, and exchange arbitrary messages with the adversary. In contrast, the environment in the stand-alone model runs only at the end of the protocol execution (and, implicitly, before the protocol starts, to prepare the inputs to all parties). UC-secure protocols enjoy a property called *general* (or *universal*) *composition*[3]: loosely speaking, the protocol remains secure even if it is run concurrently with an unbounded number of other arbitrary protocols (whereas proofs of security in the stand-alone model only guarantee security when only a single protocol at a time is running).

Earlier work on defining UC security and proving universal composition in the quantum setting appears in [7,45]. We will adapt the somewhat simpler formalism of Unruh [47]. Modulo a small change in Unruh's model (quantum advice, discussed below), our stand-alone model is exactly the restriction of Unruh's model to a *non-interactive* environment, that is one which is idle from the start to the finish of the protocol. [4]

We make one change to Unruh's model in order to be consistent with our earlier definitions and the work of Watrous on zero-knowledge [49]: we allow the environment

[3] There is a distinction between UC security (a definition that may be satisfied by a specific protocol and ideal functionality) and universal composition (a property of the class of protocols that satisfy a security definition). Not all definitions that admit universal composition theorems are equivalent to UC security. See [30,34] for discussion.

[4] The only apparent difference in the models is that in the UC model, the environment runs for some time before the protocol starts to prepare inputs, while in Section 3.1 we simply quantify over all joint states σ of the honest players' and adversary's inputs and the auxiliary input W to the distinguisher. This difference is only cosmetic, though: the state σ can be taken to be the joint state of the outputs and internal memory of the environment at the time the protocol begins.

to take quantum advice, rather than only classical advice. See the full version for details. This modification of Unruh's definition does not change the proof of the universal composition theorem:

Theorem 3. *(Quantum UC Composition Theorem [47, Theorem 11]) Let* Π_1, Π_2 *and* Π *be quantum-polynomial-time protocols. Assume that* Π_1 *quantum UC-emulates* Π_2. *Then* Π^{Π_1} *quantum UC-emulates* Π^{Π_2}.

5.1 Classical Proofs for Quantum Adversaries: Simple Hybrid Argument

The goal of this section is to analyze a class of protocols, including the protocol of Canetti *et al.* [13] for two- and multi-party computation (referred to in the sequel as CLOS). These are classical protocols, proven secure in the classical UC model. We will show that these protocols remain secure in the presence of quantum adversaries as long as the underlying primitives (pseudorandom generators and a special kind of public-key encryption scheme) are secure against quantum adversaries. Specifically, we show:

Theorem 4. *Let* $\mathcal{F}$ *be a well-formed two-party functionality. Under Assumptions 1 and 2, there exists a nontrivial classical protocol that UC-emulates* $\mathcal{F}$ *in the* $\mathcal{G}_{ZK}$*-hybrid model in the presence of polynomial-time malicious, static* quantum *adversaries.*

To prove Theorem 4, we propose an abstraction that captures a family of classical security arguments in the UC model which remains valid in the quantum setting (as long as the underlying primitives are secure against quantum adversaries).

We use the term *experiment* loosely to describe a well-defined probability experiment which results in 0 or 1. The arguments described here could also be cast in the more stringent formalism of code-based games [4]; however, because the experiments we use are ultimately fairly simple, we have chosen a less formal exposition.

We'll use the following fact about UC-secure protocols, classical [11, Claim 10] and quantum [47, Lemma 10]: the adversary can be taken to be a "dummy" adversary, which simply relays messages faithfully to and from the environment without doing any actual processing. Because we will only discuss protocols with classical communication, we can assume w.l.o.g. that the adversary in our experiments is a known, classical machine; in particular, all quantum processing can be deferred to the environment. Note that ideal world adversaries will also be classical. Consequently, we can treat the process external to the environment as a whole, and view it as a classical interactive machine M. Namely, we let M describe the process $\langle world, dummy\text{-}adv \rangle$ or $\langle world, simulator \rangle$ where *world* is an ideal world, a real world or an execution in a hybrid model. (Recall that $\langle M_1, M_2 \rangle$ denotes the interaction between M_1 and M_2. It is itself an interactive machine whose inputs are the inputs expected by M_1 and M_2 together with messages expected by M_1 and M_2 from other entities. The outputs of $\langle M_1, M_2 \rangle$ are the outputs of M_1 and M_2 together with any messages sent by them to other entities.) Thus, all the experiments (real-world executions, ideal-world executions with simulators or without, executions in hybrid models, etc) we will analyze in this section have the form $\langle M, \mathcal{Z} \rangle$, where M is a classical interactive machine *which depends only on the protocol description* as we described above and $\mathcal{Z}$ is an adversarial environment.

Definition 4 (Simply related machines). *We say two QIMs M_a and M_b are* (t,ϵ)-simply related *if there is a classical time-t machine M and a pair of classical distributions D_a, D_b such that*

1. $M(D_a) \equiv M_a$ *(for two QIMs N_1 and N_2, we say $N_1 \equiv N_2$ if the two machines behave identically on all inputs, that is, if they can be described by the same circuits),*
2. $M(D_b) \equiv M_b$, *and*
3. $D_a \approx_Q^{2t,\epsilon} D_b$.

Definition 5 (Simple hybrid argument). *Two machines M_0 and M_ℓ are related by a* (t,ϵ)-simple hybrid argument of length ℓ *if there is a sequence of intermediate machines $M_1, M_2, ..., M_{\ell-1}$ such that each adjacent pair M_{i-1}, M_i of machines, $i = 1,\ldots,\ell$, is $(t, \frac{\epsilon}{\ell})$-simply related.*

Lemma 1. *For any t,ϵ and ℓ, if two machines are related by a (t,ϵ)-simple hybrid argument of length ℓ, then the machines are (t,ϵ)-interactively indistinguishable.*

Proofs of all the statements from this section are deferred to the full version.

Observation 5 (CLOS proof structure) *Except for the proof of security of protocol compilation from semi-honest to malicious adversaries, all the security proofs for static adversaries in CLOS consist of either (a) simple hybrid arguments with $t = poly(n)$ and $\epsilon = negl(n)$, or (b) applications of the UC composition theorem.*

Moreover, the underlying indistinguishable distributions in the CLOS arguments consist of either (i) switching between a real public key and a uniformly random string, (ii) changing the plaintext of an encryption, or (iii) changing the message in the commit phase of a commitment protocol.

From this observation, we get the corollary below, where $\mathcal{G}_{CP}$ denotes the "commit-and-prove" functionality of Canetti *et al.* [13, Figure 8].

Corollary 6 (CLOS—simple hybrids) *Under Assumptions 1 and 2,*

1. *In the $\mathcal{G}_{ZK}$-hybrid model, there is a nontrivial protocol that UC-emulates $\mathcal{G}_{CP}$ in the presence of polynomial-time* malicious *static* quantum *adversaries.*
2. *Let $\mathcal{F}$ be a well-formed two-party functionality. In the plain model, there is a protocol that UC-emulates $\mathcal{F}$ in the presence of polynomial-time* semi-honest *static* quantum *adversaries.*

It remains to discuss the proof of the security of the compiler from semi-honest to malicious adversaries in the $\mathcal{G}_{CP}$ model. The proof structure is only slightly different from the hybrid proofs above. Let Π be a protocol designed for the semi-honest model and let $Comp(\Pi)$ be the result of applying the CLOS compiler to Π to get a protocol in the (malicious) $\mathcal{G}_{CP}$-hybrid model. We use the following result from Canetti *et al.* [13]:

Proposition 7 (Canetti *et al.* [13, Proposition 8.1]) *Let Π be any real-world protocol designed for the semi-honest model. For every classical adversary $\hat{\mathbf{B}}$, there exists a classical adversary $\hat{\mathbf{B}}'$ with running time polynomial in that of $\hat{\mathbf{B}}$ such that the interaction of $\hat{\mathbf{B}}$ with honest players running $Comp(\Pi)$ in the $\mathcal{G}_{CP}$-hybrid model is* identical *to the interaction of $\hat{\mathbf{B}}'$ with Π in the semi-honest model; that is, $\langle Comp(\Pi), \hat{\mathbf{B}}\rangle \equiv \langle \Pi, \hat{\mathbf{B}}'\rangle$.*

Combining the previous proposition with the simpler arguments from CLOS (Corollary 6, above) we can prove Theorem 4. See the full version for further details.

6 Equivalence Between $\mathcal{G}_{ZK}$ and $\mathcal{G}_{CF}$

In this section, we sketch the UC equivalence of zero-knowledge and coin-flipping in the quantum setting. The fact that coin-flipping can be realized in the $\mathcal{G}_{ZK}$ hybrid model follows from the general result of CLOS, discussed in the previous section. In the full version, we also give a direct construction of coin-flipping from ZK inspired by the parallel coin-flipping protocol of Lindell [33]. The direct construction relies only on the assumption of a quantum-secure PRG. More interestingly, we give a construction of $\mathcal{G}_{ZK}$ in the $\mathcal{G}_{CF}$-hybrid model which resists attacks by quantum adversaries.

Proposition 8 *1. Under Assumption 1, there is a constant-round protocol $\Pi_{CF}^{\mathcal{G}_{ZK}}$ that quantum UC-emulates $\mathcal{G}_{CF}$ in the $\mathcal{G}_{ZK}$-hybrid model.*

2. Under Assumptions 1 and 2, there is a constant-round protocol $\Pi_{ZK}^{\mathcal{G}_{CF}}$ that quantum UC-emulates $\mathcal{G}_{ZK}$ in the $\mathcal{G}_{CF}$-hybrid model.

This implies that in the stand-alone model, it suffices to construct a secure (simulatable) coin-flipping protocol to obtain secure SFE protocols for arbitrary functions. This gives a different avenue for constructing secure protocols, which might produce protocols that rely on assumptions weaker than (or incomparable to) those in our work, or that use fewer rounds. The related work of Lunemann and Nielsen [36] starts by constructing a coin-flipping protocol rather than a ZKAoK, though they rely on assumptions very similar to ours and have similar round complexity.

Our $\Pi_{ZK}^{\mathcal{G}_{CF}}$ protocol uses a standard transformation to get a ZKAoK from a witness-indistinguishable (WI) proof system in the CRS model. The main technical step in our analysis is showing that Blum's 3-round ZK protocol for Hamiltonian Cycle is in fact WI against a *malicious* quantum adversary. Our proof avoids rewinding, and is reminiscent of proofs that certain WI protocols can be composed concurrently. Details can be found in the full version.

7 Applications and Discussions

We first recap the results that we have obtained so far and derive a couple of straightforward yet important corollaries about two-party SFE in presence of quantum attacks.

1. Under Assumptions 1 and 2, for any well-formed two-party functionality $\mathcal{F}$, there is a classical protocol $\Pi^{\mathcal{G}_{ZK}}$ quantum UC-emulating $\mathcal{F}$ in the $\mathcal{G}_{ZK}$-hybrid model. (Theorem 4)
2. $\mathcal{G}_{ZK}$ and $\mathcal{G}_{CF}$ are equivalent in the quantum UC model. (Prop. 8)
3. There exists classical protocol Π_{ZK} that quantum stand-alone-emulates $\mathcal{G}_{ZK}$. (Theorem 2)

Applying modular composition theorem in the stand-alone model to item 1 and 3 we have:

Corollary 9 *For any well-formed classical two-party functionality $\mathcal{F}$, there exists a classical protocol Π that quantum stand-alone-emulates $\mathcal{F}$ with no set-up assumptions.*

Note that item 2 immediately implies equivalence of $\mathcal{G}_{ZK}$ and $\mathcal{G}_{CF}$ in the quantum stand-alone model. Combining with item 3 we get:

Corollary 10 *There exists a classical protocol Π_{CF} that quantum stand-alone-emulates $\mathcal{G}_{CF}$ with no set-up assumptions.*

Discussion. Our work suggests a number of straightforward conjectures. For example, it is likely that our techniques in fact apply to all the results in CLOS (multi-party, adaptive adversaries) and to corresponding results in the "generalized" UC model [12]. Essentially all protocols in the semi-honest model seem to fit the simple hybrids framework, in particular protocols based on Yao's garbled-circuits framework (e.g. [3]). It is also likely that existing proofs in security models which allow super-polynomial simulation (e.g., [40,41,1]) will carry through using a similar line of argument to the one here.

However, our work leaves open some basic questions: for example, can we construct constant-round ZK with negligible completeness and soundness errors against quantum verifiers? Watrous's technique does not immediately answer it since sequential repetition seems necessary in his construction to reduce the soundness error. A quick look at classical constant-round ZK (e.g., [24]) suggests that witness-indistinguishable proofs of knowledge are helpful. Is it possible to construct constant-round witness-extendable WI proofs of knowledge? Do our analyses apply to extensions of the UC framework, such the *generalized UC* framework of Canetti *et al.* [12]? Finally, more generally, which other uses of rewinding can be adapted to quantum adversaries? Aside from the original work by Watrous [49], Damgård and Lunemann [21] and Unruh [46] have shown examples of such adaption.

Acknowledgments

This work was informed by insightful discussions with many colleagues, notably Michael Ben-Or, Claude Crépeau, Ivan Damgård and Daniel Gottesman. Several of the results were obtained while A.S. was at the Institute for Pure and Applied Mathematics (IPAM) at UCLA in the fall of 2006. He gratefully acknowledges Rafi Ostrovksy and the IPAM staff for making his stay there pleasant and productive.

References

1. B. Barak and A. Sahai. How to play almost any mental game over the net - concurrent composition via super-polynomial simulation. In *FOCS*, pages 543–552. IEEE, 2005.
2. D. Beaver. On deniability in quantum key exchange. In *EUROCRYPT*, pages 352–367. Springer, 2002.
3. D. Beaver, S. Micali, and P. Rogaway. The round complexity of secure protocols. In *STOC*, pages 503–513. ACM, 1990.

4. M. Bellare and P. Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *EUROCRYPT*, pages 409–426. Springer, 2006.
5. 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, 2006.
6. M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *TCC*, pages 386–406. Springer, 2005.
7. M. Ben-Or and D. Mayers. General security definition and composability for quantum and classical protocols, September 2004. arxiv:quant-ph/0409062v2.
8. C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer. In *CRYPTO*, pages 351–366. Springer, 1991.
9. G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *CRYPTO*, pages 49–61. Springer, 1990.
10. R. Canetti. Security and composition of multiparty cryptographic protocols. *J. Cryptology*, 13(1):143–202, 2000.
11. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–145. IEEE, 2001.
12. R. Canetti, Y. Dodis, R. Pass, and S. Walfish. Universally composable security with global setup. In *TCC*, pages 61–85. Springer, 2007.
13. R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party and multi-party secure computation. In *STOC*, pages 494–503. ACM, 2002.
14. C. Crépeau, P. Dumais, D. Mayers, and L. Salvail. Computational collapse of quantum state with application to oblivious transfer. In *TCC*, pages 374–393. Springer, 2004.
15. C. Crépeau, D. Gottesman, and A. Smith. Secure multi-party quantum computation. In *STOC*, pages 643–652. ACM, 2002.
16. C. Crépeau, D. Gottesman, and A. Smith. Approximate quantum error-correcting codes and secret sharing schemes. In *EUROCRYPT*, pages 285–301. Springer, 2005.
17. C. Crépeau, L. Salvail, J.-R. Simard, and A. Tapp. Classical and quantum strategies for two-prover bit commitments. In *Quantum Information Processing (QIP)*, 2006. Online available at `http://crypto.cs.mcgill.ca/~crepeau/PDF/CSST06.pdf`.
18. I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner. Improving the security of quantum protocols via commit-and-open. In *CRYPTO*, pages 408–427. Springer, 2009. Full version at arXiv:0902.3918v4.
19. I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and qkd in the bounded-quantum-storage model. In *CRYPTO*, pages 342–359. Springer, 2007.
20. I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.*, 37(6):1865–1890, 2008.
21. I. Damgård and C. Lunemann. Quantum-secure coin-flipping and applications. In *ASIACRYPT*, pages 52–69. Springer, 2009.
22. P. Dumais, D. Mayers, and L. Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *EUROCRYPT*, pages 300–315. Springer, 2000.
23. S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. In *TCC*, pages 350–367. Springer, 2009.
24. U. Feige and A. Shamir. Zero knowledge proofs of knowledge in two rounds. In *CRYPTO*, pages 526–544. Springer, 1990.
25. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *STOC*, pages 218–229. ACM, 1987.
26. 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.
27. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18:186–208, 1989.

28. S. Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *J. ACM*, 54(1):1–19, 2007.
29. S. Hallgren, A. Kolla, P. Sen, and S. Zhang. Making classical honest verifier zero knowledge protocols secure against quantum attacks. In *ICALP*, pages 592–603. Springer, 2008.
30. D. Hofheinz and D. Unruh. Simulatable security and polynomially bounded concurrent composability. In *Symposium on Security and Privacy*, pages 169–183. IEEE, 2006.
31. G. Kol and M. Naor. Games for exchanging information. In *STOC*, pages 423–432. ACM, 2008.
32. E. Kushilevitz, Y. Lindell, and T. Rabin. Information-theoretically secure protocols and security under composition. *SIAM J. Comput.*, 39(5):2090–2112, 2010.
33. Y. Lindell. Parallel coin-tossing and constant-round secure two-party computation. *J. Cryptology*, 16(3):143–184, 2003.
34. Y. Lindell. General composition and universal composability in secure multiparty computation. *J. Cryptology*, 22(3):395–428, 2009.
35. H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.
36. C. Lunemann and J. B. Nielsen. Fully simulatable quantum-secure coin-flipping and applications. In *Africacrypt*, February 2011. arXiv:1102.0887.
37. D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, 2001.
38. M. Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991.
39. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
40. R. Pass. Simulation in quasi-polynomial time, and its application to protocol composition. In *EUROCRYPT*, pages 160–176. Springer, 2003.
41. M. Prabhakaran and A. Sahai. New notions of security: achieving universal composability without trusted setup. In *STOC*, pages 242–251. ACM, 2004.
42. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009. Preliminary version in STOC 2005.
43. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
44. P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, Jul 2000.
45. D. Unruh. Simulatable security for quantum protocols, 2004. arXiv:quant-ph/0409125v2.
46. D. Unruh. Quantum proofs of knowledge, April 2010. IACR ePrint 2010/212.
47. D. Unruh. Universally composable quantum multi-party computation. In *EUROCRYPT*, pages 486–505. Springer, 2010. arXiv:0910.2912v1.
48. D. Unruh. Concurrent composition in the bounded quantum storage model. In *EUROCRYPT*, pages 467–486. Springer, 2011.
49. J. Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version in STOC 2006.
50. A. C.-C. Yao. Quantum circuit complexity. In *FOCS*, pages 352–361. IEEE, 1993.