Feasibility and Completeness of Cryptographic Tasks in the Quantum World

Serge Fehr[1], Jonathan Katz[2,⋆], Fang Song[3], Hong-Sheng Zhou[2,⋆⋆], and Vassilis Zikas[4,⋆⋆⋆]

[1] Centrum Wiskunde & Informatica (CWI)
serge.fehr@cwi.nl
[2] University of Maryland
{jkatz,hszhou}@cs.umd.edu
[3] Pennsylvania State University
fus121@cse.psu.edu
[4] UCLA
vzikas@cs.ucla.edu

Abstract. It is known that cryptographic feasibility results can change by moving from the classical to the quantum world. With this in mind, we study the feasibility of realizing functionalities in the framework of universal composability, with respect to both computational and information-theoretic security. With respect to computational security, we show that existing feasibility results *carry over unchanged* from the classical to the quantum world; a functionality is "trivial" (i.e., can be realized without setup) in the quantum world if and only if it is trivial in the classical world. The same holds with regard to functionalities that are *complete* (i.e., can be used to realize arbitrary other functionalities).

In the information-theoretic setting, the quantum and classical worlds differ. In the quantum world, functionalities in the class we consider are either complete, trivial, or belong to a family of simultaneous-exchange functionalities (e.g., XOR). However, other results in the information-theoretic setting remain roughly unchanged.

1 Introduction

In a *classical* setting of cryptography, participants in a protocol (both the honest parties and the adversary), are modeled as being able to perform classical computation only. In the *quantum* setting, however, parties are able to send and receive quantum states and process quantum information. It is well known that cryptographic feasibility results in these two settings differ; for example, key exchange with information-theoretic security is possible in the quantum world, but not in the classical world. In this paper we focus on protocols for

⋆ This work was supported by NSF awards #1111599 and #1223623.
⋆⋆ Supported by an NSF CI postdoctoral fellowship.
⋆⋆⋆ Work done while at the University of Maryland, and supported in part by a fellowship from the Swiss National Science Foundation (Project No. PBEZP2-134445).

A. Sahai (Ed.): TCC 2013, LNCS 7785, pp. 281–296, 2013.

universally composable two-party computation, and study the relationships between feasibility/impossibility results in the classical and quantum settings.

1.1 Universally Composable Computation in the Classical World

Our focus in on secure computation within the framework of universal composability [8], which provides strong composition guarantees when arbitrary protocols are executed concurrently. Soon after the introduction of this framework, Canetti and Fischlin [9] showed that, without honest majority, UC commitment is impossible to achieve. This was later extended to rule out protocols for securely achieving most other "interesting" tasks [10,32].

On the positive side, it is known that (under suitable cryptographic assumptions) any functionality can be securely computed, without honest majority, if we are willing to assume some form of trusted setup such as a common reference string [9,11]. Subsequent work has identified other *complete* setup assumptions [1,19,18,12]. Completeness results in the *information-theoretic* (or *statistical*) setting, where the adversary is computationally unbounded, have also been shown [21,18].

Maji et al. [28] proved a *zero/one law*: every two-party deterministic function with polynomial-size input domain is either *trivial*[1] (i.e, can be realized in the UC framework with no setup assumptions), or *complete* (i.e., sufficient for computing arbitrary other functions, under appropriate complexity assumptions). This characterization was extended by Katz et al. [20], who showed completeness for deterministic functions with exponential-size input domains, and by Rosulek [33], who showed completeness for randomized, reactive functions as well. In the setting of information-theoretic security, Kraschewski et al. [22] give a characterization of completeness for two-party deterministic functionalities, and show that a zero/one laws does not hold. In fact, Maji et al. [27] show there is an infinite hierarchy of function complexity in the statistical setting.

1.2 The Shift to a Quantum World

How do the results described in the previous section change when we move to the quantum world? The answer, *a priori*, is unclear. Feasibility results in the classical setting may not hold in the quantum setting since quantum adversaries are more powerful than classical ones. This is true even if "quantum-resistant" cryptographic assumptions are used, since techniques such as rewinding that are used to prove security against classical adversaries may not apply in the quantum setting. Even in the case of statistical security, feasibility results may not translate from the classical world to the quantum world [14].

In the other direction, impossibility results in the classical setting might potentially be circumvented in the quantum setting since honest parties can rely on quantum mechanics, too. As a notable example of this, statistically secure key exchange is possible in the quantum world [3] but not in the classical one.

[1] We use *trivial* and *feasible* exchangeably hereafter.

While several impossibility results for statistically secure two-party computation in the quantum setting are known [29,24,23,34,6], these results say nothing about the computational setting. They also say nothing about what might be possible given trusted setup. An example here, that also demonstrates the power of quantum protocols, arises in the context of building oblivious transfer (OT) from commitment. Classically, this is impossible [27]. However, there is a construction of OT from commitment in the quantum world [4,15,36,5]; as a consequence, commitment is complete for UC computation in that setting [36].

Given the above, the situation regarding triviality and completeness of functionalities within the *quantum* UC framework (see Section 2) is unclear, though partial answers are known. In the *statistical* setting, Unruh [36] gives a generic "lifting" theorem asserting that classically secure protocols remain (statistically) secure in the quantum world. So any functionalities that are classically trivial (in a statistical sense) are also trivial in a quantum setting. Moreover, any functionality that is classically *complete* in a statistical sense (and so in particular OT [36]) is complete with respect to the quantum UC framework as well. The situation is less clear with regard to computational security. A recent work by Hallgren et al. [17] "salvages" a few classically complete functionalities, showing that, for example, coin-flipping and zero-knowledge are still complete in the quantum world. But this does not rule out the possibility that some classically complete functionalities are no longer complete in the quantum setting.

1.3 Our Results

We study feasibility and completeness of an interesting class of two-party, deterministic functionalities on polynomial-size domains. We prove generic, *quantum-lifting* theorems and use them to show that feasibility in the quantum world is *equivalent* to classical feasibility, in both the computational and statistical settings. An important ingredient here is a quantum analogue of the Canetti-Fischlin result [9], showing that there is no quantum protocol realizing UC commitment against computationally bounded quantum adversaries in the plain model.[2] This result extends the known impossibility results mentioned earlier for statistically secure protocols in the quantum setting.

At the core of our quantum-lifting theorems is a quantum construction of statistically secure OT from the "2-bit cut-and-choose" functionality $\mathcal{F}_{\mathsf{2CC}}$. (Note that $\mathcal{F}_{\mathsf{2CC}}$ is not complete in the classical setting.) Our construction is a modification of the BBCS protocol [4], but existing techniques do not seem to apply for arguing its security. Instead, we introduce and analyze an *adaptive* version of the sampling technique from [5], and use this to prove the security of our OT protocol. The adaptive-sampling analysis may be of independent interest.

Our lifting theorems for the case of computational security, together with Unruh's lifting theorem for the statistical case [36], imply that any classically complete functionality remains complete in the quantum setting. On the other hand, we identify tasks that are statistically complete using quantum protocols but are incomplete classically. Our results show, roughly, that every functionality

[2] A similar result was stated in [31] with no proof.

in our class is either trivial or complete in the quantum computational setting; thus, the situation here is analogous to the classical case [28]. In the quantum *statistical* setting, however, functionalities fall into one of three different classes; this is in contrast with the (more complicated) classical picture [27,22].

1.4 Additional Related Work

Proving security of quantum protocols has been challenging and nontrivial. Indeed, it was only several years after the invention of quantum key-exchange protocols that rigorous proofs of security were given [30,25,35]. With regard to secure computation, the first broad feasibility results were in the setting of multi-party protocols with information-theoretic security, assuming honest majority [13,2]. Positive results for computational security in the quantum world, without honest majority, have only recently been shown [37,26,17,16].

1.5 Outline of the Paper

In Section 2, we describe the classical and the quantum UC models as well as our terminology. We prove our lifting theorems for completeness in Section 3, and for feasibility in Section 4. In Section 5, we apply our lifting theorems to classify the cryptographic complexity of functionalities in the class we consider.

2 The Model

In this section we describe the model and our terminology. We consider two types of security statements, namely classical and quantum. The classical statements are done in Canetti's (classical) UC framework [8]. For quantum statements we use the recently developed quantum-UC framework [36]. In this work, we assume *static*, i.e., non-adaptive corruption. Namely an adversary chooses the set of parties to corrupt before execution of the protocol.

The UC Framework. The security of protocols is argued via the simulation paradigm. Intuitively, a protocol *securely realizes* a given ideal functionality $\mathcal{F}$, if the adversary cannot gain more in the protocol (real-world) than what she could in an ideal-evaluation of $\mathcal{F}$ where a trusted party computes the function values and hand them to designated players (ideal-world). More formally, a protocol π securely realizes a functionality $\mathcal{F}$ if for every real-world adversary $\mathcal{A}$ there exists an ideal-world adversary $\mathcal{S}$, called the *simulator*, such that no environment can distinguish whether it is witnessing the real-world execution with adversary $\mathcal{A}$ or the ideal-world execution with simulator $\mathcal{S}$. The parties, the adversary, the simulator, the functionalities, and the environment, are modeled as interactive Turing-machines (ITMs). Depending on the assumed computing power of the adversaries and the environment we distinguish between *computational security*, where they are all considered to be polynomially bounded ITMs, and *information-theoretic (i.t.)*, also known as *statistical* security, where they are assumed to be computationally unbounded.

Universal Composability and the Hybrid Model. The most important feature of the simulation-based security definition is that it allows to argue about security of protocols in a composable way. In particular, let π be a protocol which securely realizes a functionality $\mathcal{F}$. If we can prove that a protocol π' securely realizes a functionality $\mathcal{F}'$ using invocations of $\mathcal{F}$ as in the ideal world, then it follows automatically that if we replace in π' the invocations of $\mathcal{F}$ by invocations of π, the resulting protocol also securely realizes $\mathcal{F}'$. Therefore we only need to prove the security of π' in the so-called $\mathcal{F}$-*hybrid* model, where the players run π' and are allowed to make invocations to $\mathcal{F}$.

Reductions and Cryptographic Complexity. For two ideal functionalities $\mathcal{F}$ and $\mathcal{F}'$, we say that $\mathcal{F}$ *computationally (classical) UC reduces to* $\mathcal{F}'$, denoted as $\mathcal{F} \sqsubseteq^{\text{CCOMP}} \mathcal{F}'$, if there exists a $\mathcal{F}'$-hybrid protocol $\pi^{\mathcal{F}'}$ which computationally securely realizes $\mathcal{F}$. If the protocol $\pi^{\mathcal{F}'}$ statistically securely realizes $\mathcal{F}$, then we say that $\mathcal{F}$ *statistically (classical) UC reduces to* $\mathcal{F}'$, denoted as $\mathcal{F} \sqsubseteq^{\text{CSTAT}} \mathcal{F}'$. As syntactic sugar, we say that $\mathcal{F}$ and $\mathcal{F}'$ are computationally (resp. statistically) UC equivalent, denoted as $\mathcal{F} \overset{\texttt{ccomp}}{\equiv} \mathcal{F}'$ (resp. $\mathcal{F} \overset{\texttt{cstat}}{\equiv} \mathcal{F}'$), if $\mathcal{F} \sqsubseteq^{\text{CCOMP}} \mathcal{F}'$ and $\mathcal{F}' \sqsubseteq^{\text{CCOMP}} \mathcal{F}$ (resp. $\mathcal{F} \sqsubseteq^{\text{CSTAT}} \mathcal{F}'$ and $\mathcal{F}' \sqsubseteq^{\text{CSTAT}} \mathcal{F}$).

The reduction-relation $\sqsubseteq$ is "transitive" in the sense that if $\mathcal{F}' \sqsubseteq \mathcal{F}$, then any task which is implementable in the $\mathcal{F}'$-hybrid world is also implementable in the $\mathcal{F}$-hybrid world. This implies a notion of cryptographic complexity for functions, where $\mathcal{F}' \sqsubseteq \mathcal{F}$ implies that $\mathcal{F}$ is at least as high in the hierarchy as $\mathcal{F}'$.

Feasibility and Completeness. Let $\mathcal{F}_{\texttt{SEC}}$ denote the secure channels functionality.We say that a functionality $\mathcal{F}$ is *computationally (resp. statistically) UC feasible* if $\mathcal{F} \sqsubseteq^{\text{CCOMP}} \mathcal{F}_{\texttt{SEC}}$ (resp. $\mathcal{F} \sqsubseteq^{\text{CSTAT}} \mathcal{F}_{\texttt{SEC}}$). Furthermore, we say that $\mathcal{F}$ is *computationally (resp. statistically) UC complete* if for any well-formed functionality $\mathcal{F}' : \mathcal{F}' \sqsubseteq^{\text{CCOMP}} \mathcal{F}$ (resp. $\mathcal{F}' \sqsubseteq^{\text{CSTAT}} \mathcal{F}$).

The Quantum UC Framework [36]. The quantum-UC framework generalizes the classical UC model, in which the players (including the adversaries and the environment) are quantum machines. A quantum universal composition theorem was proved in [36]. We point out that in this work we only consider ideal functionalities with classical inputs and outputs. For two ideal functionalities $\mathcal{F}$ and $\mathcal{F}'$, we say that $\mathcal{F}$ *computationally quantum-UC reduces to* $\mathcal{F}'$, denoted as $\mathcal{F} \sqsubseteq^{\text{QCOMP}} \mathcal{F}'$, if there exists a $\mathcal{F}'$-hybrid protocol $\pi^{\mathcal{F}'}$ which computationally securely realizes $\mathcal{F}$. If the protocol $\pi^{\mathcal{F}'}$ statistically securely realizes $\mathcal{F}$, then we say that $\mathcal{F}$ *statistically quantum-UC reduces to* $\mathcal{F}'$, denoted as $\mathcal{F} \sqsubseteq^{\text{QSTAT}} \mathcal{F}'$. We say that a functionality $\mathcal{F}$ is *computationally (resp. statistically) quantum-UC feasible* if $\mathcal{F}$ can be computationally (resp. statistically) quantum-UC realized in the plain quantum-UC model, i.e., without assuming any hybrids.[3] Furthermore, we say that $\mathcal{F}$ is *computationally (resp. statistically) quantum-UC complete* if for any well-formed (classical) functionality $\mathcal{F}' : \mathcal{F}' \sqsubseteq^{\text{QCOMP}} \mathcal{F}$ (resp. $\mathcal{F}' \sqsubseteq^{\text{QSTAT}} \mathcal{F}$).

[3] We point out that quantum secure channel is implied by authentication channel due to QKD protocols, which is by default provided in the quantum-UC framework, hence there is no need to assume quantum secure channels.

The definitions of computation and statistical quantum-UC equivalence is also analogous to the classical setting.

In [36] the so-called *(statistical) quantum lifting theorem* was proved which, roughly speaking shows that if a classical protocol is statistically UC secure then it is also statistically quantum-UC secure.

Fact 1 ([36, Theorem 15] – The Quantum Lifting Theorem). *If a protocol π statistically UC realizes a functionality $\mathcal{F}$, then π statistically quantum-UC realizes the functionality $\mathcal{F}$.*

Remark 1 (Polynomial Simulation). In all the security definitions considered in this work we explicitly require that the simulator's running time is polynomial to the running time of the adversary. We call this property *polynomial simulation*. The property ensures that when a protocol statistically realizes a functionality, then it also computationally realizes it [7,8]. We point out that the definition of statistical quantum-UC security in [36] explicitly requires *polynomial simulation*.

Ideal Functionalities and the Class $\mathcal{U}^-$. Ideally, we would like our statements to cover the whole class $\mathcal{U}$ of finite, deterministic, two-party functionalities, which is the central class studied in [27,28]. However, we were unable to prove or disprove (quantum-UC) neither completeness nor feasibility of the 1-bit cut-and-choose functionality $\mathcal{F}_{\mathtt{1cc}} \in \mathcal{U}$ (also denoted as $\mathcal{F}_{\mathtt{cc}}$). We were able to prove statistical quantum-UC completeness of its "closest sibling;" namely, the 2-bit cut-and-choose functionality $\mathcal{F}_{\mathtt{2cc}}$.[4] Therefore, our results are for the slightly smaller class $\mathcal{U}^-$ which is $\mathcal{U}$ excluding the small fraction of functionalities that are sufficient for (statistically classically) realizing $\mathcal{F}_{\mathtt{1cc}}$ but not for realizing $\mathcal{F}_{\mathtt{2cc}}$. Formally:

$$\mathcal{U}^- = \{\mathcal{F} \mid (\mathcal{F} \in \mathcal{U}) \wedge ((\mathcal{F}_{\mathtt{2cc}} \sqsubseteq^{\text{CSTAT}} \mathcal{F}) \vee (\mathcal{F}_{\mathtt{1cc}} \not\sqsubseteq^{\text{CSTAT}} \mathcal{F}))\}.$$

Note that, as demonstrated in [28], the missing fraction, i.e., $\mathcal{U} \setminus \mathcal{U}^-$, is indeed very small as, roughly, it corresponds to the lowest primitive of an infinite *strict* hierarchy of (statistically classically) incomplete "cut-and-choose" primitives.[5] Nevertheless, it remains an open problem to prove quantum-UC feasibility or completeness of $\mathcal{F}_{\mathtt{1cc}}$ (which would complete the characterization of $\mathcal{U}$) as it does not follow from any known classical or quantum results.

For completeness, we list a few two-party ideal functionalities that are used as setups in this work.Consistently with existing literature we use the names Alice and Bob for the parties:

• 1-out-of-2 Oblivious Transfer $\mathcal{F}_{\mathtt{0T}}$: Alice (the sender) inputs 2 bits (s_0, s_1) and Bob (the receiver) inputs a selection bit $c \in \{0, 1\}$. Bob receives s_c from $\mathcal{F}_{\mathtt{0T}}$.

[4] Our conjecture is that $\mathcal{F}_{\mathtt{1cc}}$ is also statistically quantum-UC complete. Recall that classically neither $\mathcal{F}_{\mathtt{cc}}$ nor $\mathcal{F}_{\mathtt{2cc}}$ is statistically UC complete [28].

[5] These are variations of $\mathcal{F}_{\mathtt{2cc}}$ parameterized by the size of Bob's input, i.e., $\mathcal{F}_{\mathtt{mcc}}$ behaves as $\mathcal{F}_{\mathtt{cc}}$ where Bob's input is a string of length m. ($\mathcal{F}_{\mathtt{1cc}}$ is the lowest and $\mathcal{F}_{\mathtt{2cc}}$ is the second lowest primitive in this hierarchy.) [28].

We also consider the more general string OT, where (s_0, s_1) are ℓ-bit strings. Our OT protocol in Sect. 3.1 realizes string OT.

• Commitment $\mathcal{F}_{\texttt{COM}}$: Alice (the committer) inputs a bit b and Bob (the receiver) receives from $\mathcal{F}_{\texttt{COM}}$ a notification that a bit was received. At a later point, Alice can input the command open to $\mathcal{F}_{\texttt{COM}}$ in which case Bob receives b.

• XOR $\mathcal{F}_{\texttt{XOR}}$: Alice and Bob input bits b_A and b_B, respectively. They both receive the output $y = b_A \oplus b_B$.

• 2-bit Cut-and-Choose $\mathcal{F}_{\texttt{2CC}}$: Bob inputs a 2-bit string $b = (b_0, b_1)$, an Alice inputs a selection bit s_A; informally, s_A indicates whether or not Alice wishes to learn b. Bob receives output s_A and Alice receives output b if $s_A = 1$, and receives $\perp$ if $s_A = 0$.

• Coin Tossing $\mathcal{F}_{\texttt{COIN}}$: Alice and Bob input a request to $\mathcal{F}_{\texttt{COIN}}$, and $\mathcal{F}_{\texttt{COIN}}$ randomly chooses a fair coin $r \in \{0, 1\}$ and it then sends delayed output r to both Alice and Bob.

Note that the functionalities $\mathcal{F}_{\texttt{OT}}$, $\mathcal{F}_{\texttt{XOR}}$, $\mathcal{F}_{\texttt{2CC}}$, and $\mathcal{F}_{\texttt{COM}}$ are in the set $\mathcal{U}^-$.

Notational Conventions. Throughout the paper we use small π to denote a classical protocol in classical UC model, while we use capital Π to denote a classical or quantum protocol in quantum UC model.

3 Quantum Lifting for Completeness

In this section we prove that statements about completeness of functionalities in the classical setting are preserved in the quantum setting. More precisely, we prove the following theorem:

Theorem 1. *For any $\mathcal{F} \in \mathcal{U}^-$ the following statements hold:*

1. *(Statistical Setting) If $\mathcal{F}$ is statistically classical-UC complete then $\mathcal{F}$ is statistically quantum-UC complete.*
2. *(Computational Setting) If $\mathcal{F}$ is computationally classical-UC complete under the semi-honest OT assumption* shOT *then $\mathcal{F}$ is computationally quantum-UC complete under the assumptions of existence of a quantum-secure pseudorandom generator and a dense encryption that is quantum IND-CPA.*

The statistical statement follows easily from Unruh's quantum lifting theorem (Fact 1) and the definition of completeness. In the remaining of this section we prove the computational statement. To this direction we follow a structure similar to that of [28]: First, in Section 3.1 we show that for any $\mathcal{F} \in \mathcal{U}^-$, either $\mathcal{F}$ is computationally quantum-UC feasible or for a functionality $\mathcal{F}' \in \{\mathcal{F}_{\texttt{XOR}}, \mathcal{F}_{\texttt{OT}}, \mathcal{F}_{\texttt{2CC}}, \mathcal{F}_{\texttt{COM}}\}$, there exists a statistically quantum-UC secure protocol which reduces $\mathcal{F}'$ to $\mathcal{F}$. Second, in Section 3.2, we show that $\mathcal{F}_{\texttt{XOR}}$, $\mathcal{F}_{\texttt{OT}}$, $\mathcal{F}_{\texttt{2CC}}$, and $\mathcal{F}_{\texttt{COM}}$ are computationally quantum-UC complete. Statement 2 of the theorem follows then immediately by combining the above steps and using the fact that any statistically quantum-UC secure protocol is also computationally quantum-UC secure.

3.1 Non-feasibility Implies $\mathcal{F}_{\mathtt{XOR}}$, $\mathcal{F}_{\mathtt{OT}}$, $\mathcal{F}_{\mathtt{2CC}}$, or $\mathcal{F}_{\mathtt{COM}}$

To show that every infeasible $\mathcal{F} \in \mathcal{U}^-$, there is some $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{COM}}\}$ such that $\mathcal{F}' \sqsubseteq^{\text{QCOMP}} \mathcal{F}$, we use the following result that is proved in [28, Theorems 1,4]: if $\mathcal{F} \in \mathcal{U}$ is not UC feasible, then for $\mathcal{F}' \sqsubseteq^{\text{CSTAT}} \mathcal{F}$. Using this result on $\mathcal{U}^-$ we obtain the following:

Fact 2 ([28]). *Let $\mathcal{F} \in \mathcal{U}^-$. If $\mathcal{F}$ is not compuationally (UC) feasible, then for some $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{COM}}\}$ the following holds: $\mathcal{F}' \sqsubseteq^{\text{CSTAT}} \mathcal{F}$.*

Because the reductions in Fact 2 are information-theoretic (with polynomial-simulation), the statement can be translated to the quantum-UC setting by Fact 1. This proves the following lemma:

Lemma 1. *Let $\mathcal{F} \in \mathcal{U}^-$. If $\mathcal{F}$ is not statistically quantum-UC feasible , then for some $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{COM}}\}$ the following holds: $\mathcal{F}' \sqsubseteq^{\text{QSTAT}} \mathcal{F}$.*

Proof. First observe that $\mathcal{F}$ is not statistically classical-UC feasible, because otherwise the lifting lemma (Fact 1) will impy that $\mathcal{F}$ is also statistically quantum-UC feasible, contradicting the assumption. Then by our lifting theorem for feasibility in later section (Sect. 4, Theorem 2), statistical UC infeasibility of $\mathcal{F}$ implies that $\mathcal{F}$ is *not* computationally UC feasible. Then Fact 2 tells us that for some $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{COM}}\} : \mathcal{F}' \sqsubseteq^{\text{CSTAT}} \mathcal{F}$, which, in turns implies that $\mathcal{F}' \sqsubseteq^{\text{QSTAT}} \mathcal{F}$ by Fact 1.

3.2 Quantum-UC Completeness of $\mathcal{F}_{\mathtt{XOR}}$, $\mathcal{F}_{\mathtt{OT}}$, $\mathcal{F}_{\mathtt{2CC}}$, and $\mathcal{F}_{\mathtt{COM}}$

We next prove that each of the functionalities $\mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}$ and $\mathcal{F}_{\mathtt{COM}}$ is computationally quantum-UC complete[6]. The quantum-UC completeness of $\mathcal{F}_{\mathtt{OT}}$ and $\mathcal{F}_{\mathtt{COM}}$ was proved in [36]:

Lemma 2. *$\mathcal{F}_{\mathtt{OT}}$ and $\mathcal{F}_{\mathtt{COM}}$ are statistically quantum-UC complete.*

This immediately gives us the desired computational quantum-UC completeness of $\mathcal{F}_{\mathtt{OT}}$ and $\mathcal{F}_{\mathtt{COM}}$. Next, we show completeness for the XOR functionality. To this direction we use the following idea: first we use the straight-forward classical $\mathcal{F}_{\mathtt{XOR}}$-hybrid coin-tossing protocol (each party chooses a random bit and sends it to $\mathcal{F}_{\mathtt{XOR}}$; the output of every party is the value they receive from $\mathcal{F}_{\mathtt{XOR}}$) to construct $\mathcal{F}_{\mathtt{COIN}}$; subsequently, we apply the results of [17] who proved computationally quantum-UC completeness of $\mathcal{F}_{\mathtt{COIN}}$ under proper assumptions.

Lemma 3. *Assuming existence of a quantum-secure pseudorandom generator and a dense encryption that is quantum IND-CPA, then $\mathcal{F}_{\mathtt{XOR}}$ is computationally quantum-UC complete.*

[6] Actually, as will be shown, $\mathcal{F}_{\mathtt{COM}}$, $\mathcal{F}_{\mathtt{OT}}$, $\mathcal{F}_{\mathtt{2CC}}$ are *statistically* quantum-UC complete.

The most involved completeness proof is the one concerning the cut-and-choose functionality $\mathcal{F}_{\mathtt{2CC}}$. In [28], they constructed a classical protocol realizing $\mathcal{F}_{\mathtt{COM}}$ from $\mathcal{F}_{\mathtt{1CC}}$. However, their security proof involves rewinding, and it is unclear how to make it go through against quantum adversaries.[7]

Instead, we demonstrate completeness of $\mathcal{F}_{\mathtt{2CC}}$ by constructing a *quantum* protocol that statistically quantum-UC realizes $\mathcal{F}_{\mathtt{OT}}$ in $\mathcal{F}_{\mathtt{2CC}}$-hybrid world (and then applying Lemma 2). The idea is motivated by the quantum OT construction in the $\mathcal{F}_{\mathtt{COM}}$ hybrid world by Bennett et al [4]. In this protocol, roughly speaking, $\mathcal{F}_{\mathtt{COM}}$ is used in a checking subroutine to ensure that malicious Bob measures his qubits upon arrival (and does not store them until Alice informs him about the bases used). More specifically, Alice sends several qubits encoded in random bases, and Bob measures all of them and commits, for each qubit, to the pair $(\tilde{x}_i^B, \tilde{\theta}_i^B)$, where $\tilde{x}_i^B$ is the outcome of the measurement of the i^{th} qubit and $\tilde{\theta}_i^B$ is the corresponding basis Bob used. Alice then asks Bob to open a randomly chosen subset of the committed pairs, and she checks consistency with how she had prepared the qubits. Intuitively, this indeed ensures that Bob has measures most of the qubits, as otherwise he would not know what to commit to. Formally proving this intuition turned out to be non-trivial, with the first rigorous proofs given in [15,36,5].

Our protocol uses, instead of commitments, invocations to $\mathcal{F}_{\mathtt{2CC}}$ to implement the checking step (see the protocol $\Pi_{\mathtt{QOT}}$ below). Intuitively, this should enforce Bob to measure all the qubits as in the original protocol based on commitments. Unfortunately, the formal proof does not carry over. The problem arises from the fact that in the original protocol, Bob has to commit to all the $\tilde{\theta}_i^B$ and $\tilde{x}_i^B$ *before* he gets to see the random subset that Alice chooses for testing consistency, whereas in our protocol based on $\mathcal{F}_{\mathtt{2CC}}$, Bob can make his input $(\tilde{\theta}_i^B, \tilde{x}_i^B)$ to $\mathcal{F}_{\mathtt{2CC}}$ *adaptively*, and *dependent* on which prior positions Alice has tested. Current proofs, like [15,5], cannot deal with that.

In order to deal with this issue, we introduce an *adaptive* version of the sampling framework of [5]. We then show, analogous to the static setting as in [5], that the security of the OT scheme reduces to the analysis of a quantum sampling problem in our adaptive sampling framework. Analyzing the quantum sampling problem can further be reduced to a classical probabilistic analysis, which can be handled by standard techniques (e.g., Azuma's inequality).

In the following, we describe the $\mathcal{F}_{\mathtt{2CC}}$-hybrid OT protocol $\Pi_{\mathtt{QOT}}$ and state its security in Lemma 4. The formal proof can be found in the full version.

Lemma 4. *There exists an $\mathcal{F}_{\mathtt{2CC}}$-hybrid protocol which statistically quantum-UC realizes $\mathcal{F}_{\mathtt{OT}}$.*

The following corollary follows from Lemma 4 and the completeness of $\mathcal{F}_{\mathtt{OT}}$ (Lemma 2), by applying the quantum-UC composition theorem.

[7] It is in general 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, which [28] actually satisfies. The subtlety is that the correctness of the simulator might still involve rewinding argument (e.g., in defining hybrid experiments).

Protocol $\Pi_{\mathtt{QOT}}$

Parameters: A family $\mathbf{F} = \{f : \{0,1\}^n \to \{0,1\}^\ell\}$ of universal hash functions.
Parties: The sender Alice and the recipient Bob.
Inputs: Alice gets two ℓ-bit strings s_0 and s_1, Bob gets a bit c.

1. (**Initialization**)
   1.1 Alice chooses $\tilde{x}^A = (\tilde{x}_1^A, \ldots, \tilde{x}_n^A) \in_R \{0,1\}^n$ and $\tilde{\theta}^A = (\tilde{\theta}_1^A, \ldots, \tilde{\theta}_n^A) \in_R \{+,\times\}^n$ uniformly at random and sends $|\tilde{x}^A\rangle_{\tilde{\theta}^A}$ to Bob who denotes the received state by $|\psi\rangle$.
   2.2 Bob chooses $\tilde{\theta}^B = (\tilde{\theta}_1^B, \ldots, \tilde{\theta}_n^B) \in_R \{+,\times\}^n$ uniformly at random and measures the qubits of $|\psi\rangle$ in the bases $\tilde{\theta}^B$; denote the result by $\tilde{x}^B := (\tilde{x}_1^B, \ldots, \tilde{x}_n^B)$.
2. (**Checking**)
   2.1 For $i = 1, \ldots n$ the following steps are executed sequentially:
      (a) Alice chooses a bit $b_i \in_R \{0,1\}$ uniformly at random.
      (b) Alice and Bob invoke $\mathcal{F}_{\mathtt{2CC}}$ with inputs b_i and $(\tilde{x}_i^B, \tilde{\theta}_i^B)$, respectively.
   2.2 If in some iteration i of Step 2.1 Alice receives $\tilde{\theta}_i^B = \tilde{\theta}_i^A$ but $\tilde{x}_i^B \neq \tilde{x}_i^A$, then Alice aborts. If in Step 2.1 Bob receives (as output of $\mathcal{F}_{\mathtt{2CC}}$) the bit $b_i = 1$ more than $3n/5$ times then Bob aborts.
   2.3 Let $\hat{x}^A$ be the string resulting from removing in $\tilde{x}^A$ the bits at positions i with $b_i = 1$. Define $\hat{\theta}^A$, $\hat{x}^B$, $\hat{\theta}^B$ analogously.
3. (**Partition Index Set**) Alice sends $\hat{\theta}^A$ to Bob. Bob sets $I_c := \{i : \hat{\theta}_i^A = \hat{\theta}_i^B\}$ and $I_{1-c} := \{i : \hat{\theta}_i^A \neq \hat{\theta}_i^B\}$. Then Bob sends (I_0, I_1) to Alice.
4. (**Secret Transferring**)
   4.1 Alice picks a function $f \in_R \mathbf{F}$; for $i = 0, 1$: Alice computes $m_i := s_i \oplus f(x_i')$, where x_i' is the n-bit string that consists of $\hat{x}^A|_{I_i}$ padded with zeros, and sends (f, m_0, m_1) to Bob.
   4.2 Bob outputs $s := m_c \oplus f(x_B')$, where x_B' is the n-bit string that consists of $\hat{x}^B|_{I_c}$ padded with zeros.

Corollary 1. *$\mathcal{F}_{\mathtt{2CC}}$ is statistically quantum-UC complete.*

The proof of Theorem 3 follows easily from Lemmas 1, 2, 3, and Corollary 1, by applying the quantum-UC composition theorem.

4 Quantum Lifting for Feasibility

In this section we show a bi-directional lifting theorem for feasibility statements. Informally, we show that if a functionality $\mathcal{F} \in \mathcal{U}^-$ is feasible in the classical UC setting, then $\mathcal{F}$ is also feasible in the quantum-UC setting and vise versa. In fact, we can even show a stronger statement, namely that the set of feasible functionalities in $\mathcal{U}^-$ is the same set *irrespective* of whether we are considering the classical or the quantum setting and independent of the level of security (i.e, computational or statistical). We point out that the computational statements in the following theorem are under that semi-honest OT assumption for the

classical setting, and under the assumptions of existence of a quantum-secure pseudorandom generator and a dense encryption that is quantum IND-CPA, for the quantum setting.

Theorem 2. *Let $\mathcal{F} \in \mathcal{U}^-$. The following statements are equivalent*

1. *$\mathcal{F}$ is computationally (classical) UC feasible.*
2. *$\mathcal{F}$ is statistically (classical) UC feasible.*
3. *$\mathcal{F}$ is statistically quantum-UC feasible.*
4. *$\mathcal{F}$ is computationally quantum-UC feasible.*

Proof. $(1 \Rightarrow 2)$ is already implicit in [28]. For $\mathcal{F} \in \mathcal{U}^-$, if $\mathcal{F}$ is computationally feasible, then such $\mathcal{F}$ is splittable and we can construct a trivial protocol [32]. Then we can show the same trivial protocol can realize $\mathcal{F}$ information theoretically, which means $\mathcal{F}$ is statistically feasible.

$(2 \Rightarrow 3)$ is immediate from Unruh's quantum lifting lemma. $(3 \Rightarrow 4)$ follows because we require poly-time simulation in statistical UC model, and hence statistical UC security in particular implies computational UC security. We are left to show $(4 \Rightarrow 1)$.

Assume for contradiction that $\mathcal{F}$ is computationally quantum-UC feasible but classically not computationally classical-UC feasible. Invoke Fact 2 again, we have that for some $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{COM}}, \mathcal{F}_{\mathtt{XOR}}\} : \mathcal{F}' \sqsubseteq^{\text{CSTAT}} \mathcal{F}$, which by Theorem 1, implies that $\mathcal{F}$ is computationally quantum-UC complete. This, combined with the assumption that $\mathcal{F}$ is computationally quantum-UC feasible, implies that every $\mathcal{F} \in \mathcal{U}^-$ is computationally quantum-UC feasible. This is a contradiction because one can prove that $\mathcal{F}_{\mathtt{COM}}$ is not computationally quantum-UC feasible, i.e., there exists no (quantum) protocol that realizes $\mathcal{F}_{\mathtt{COM}}$ with computational quantum-UC security. The argument is similar the classical impossibility proof of UC commitments [9], and the details can be found in the full version.

5 Putting it Together

In this section we bring the pieces together and describe the cryptographic-complexity landscape for $\mathcal{U}^-$ in the quantum world. In the case of computational quantum-UC security, we can derive a zero/one law in the flavor of [28]. For statistical quantum-UC security we show that, roughly speaking, every $\mathcal{F} \in \mathcal{U}^-$ is either statistically quantum-UC feasible, or $\mathcal{F}$ is statistically quantum-UC complete, or $\mathcal{F}_{\mathtt{XOR}}$ statistically quantum-UC reduces to $\mathcal{F}$.

5.1 Computational Security: A Zero/One Law

Our quantum lifting theorems for feasibility and completeness imply that all computational UC complete (resp. UC feasible) functionalities in $\mathcal{U}^-$ are also computational quantum-UC complete (resp. quantum-UC feasible). Using this fact along with the classical zero/one law, one can derive a zero-one law for the

computational quantum-UC setting in a straight-forward manner (under the assumptions of existence of a quantum-secure pseudorandom generator and a dense encryption that is quantum IND-CPA). This proves the following theorem (see Figure 1a):

Theorem 3 (A Computational Zero/One Law). *Every functionality $\mathcal{F} \in \mathcal{U}^-$ is either computationally quantum-UC feasible or computationally quantum-UC complete.*

As a straightforward corollary of the above theorem we can conclude that the quantum lifting theorem for completeness can be made bi-directional in the computational setting. Theorem 1 already states that computational completeness of some $\mathcal{F} \in \mathcal{U}^-$ in the classical setting implies computational completeness of $\mathcal{F}$ in the quantum setting. In the other direction, if $\mathcal{F}$ is quantumly-UC complete, then Theorem 3 implies that it is not quantum-UC feasible, which implies (by Theorem 2) that it is not (classically) UC feasible; hence, the computational (classical) zero/one law implies that $\mathcal{F}$ is computationally (classically) UC complete. This proves the following:

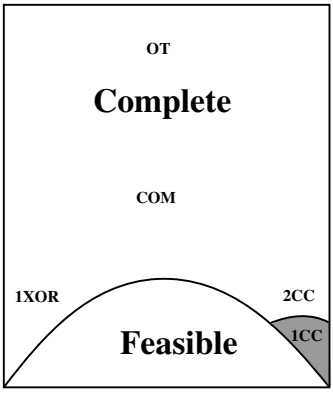
Corollary 2. *Let $\mathcal{F} \in \mathcal{U}^-$ be a functionality. $\mathcal{F}$ is computationally UC complete under the semi-honest OT assumption* $\mathtt{shOT}$ *if and only if $\mathcal{F}$ is computationally quantum-UC complete under the assumptions of existence of a quantum-secure pseudorandom generator and a dense encryption that is quantum IND-CPA.*

5.2 Statistical Security: Three Classes

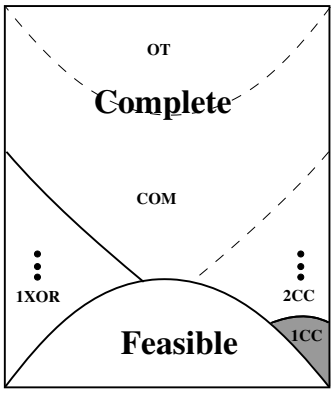
We next turn to the setting of statistical security. In the classical setting, the cryptographic-complexity landscape is complicated, as, apart from the complete/feasible functionalities, there is a partition of the set $\mathcal{U}^-$ in clusters for which the exact relation is not known. In contrast we can show a "[zero/xor/one]-law" in the statistical quantum-UC setting. In other words we can divide the class $\mathcal{U}^-$ into functionalities that are either complete, or feasible, or we can reduce $\mathcal{F}_{\mathtt{XOR}}$ to them. This considerably simplifies the landscape of the classical statistical setting, as the hierarchy of functionalities that we can reduce $\mathcal{F}_{\mathtt{2CC}}$ to collapses at the second level (i.e, to $\mathcal{F}_{\mathtt{2CC}}$) which as it follows from Lemma 4 is in fact complete in the quantum setting. This illustrates, as [36] mentioned also, that the inverse of the Unruh's quantum lifting lemma is in general not true. Namely, *there exist classical well-formed infeasible functionalities $\mathcal{F}$ and $\mathcal{F}'$ such that there exist an $\mathcal{F}$-hybrid quantum protocol which statistically quantum-UC securely realizes $\mathcal{F}'$, but there exists no $\mathcal{F}$-hybrid classical protocol which statistically classical-UC realizes $\mathcal{F}'$.*

The following theorem states the aforementioned zero/xor/one-law:

Theorem 4 (A [Zero/Xor/One]-Law for the Information-Theoretic Setting). *Let $\mathcal{F} \in \mathcal{U}^-$. Then exactly one of the following statements holds: (1) $\mathcal{F}$ is quantum-UC feasible, (2) $\mathcal{F}$ is quantum-UC complete, and (3) $\mathcal{F}$ is neither*



(a) Computational landscape: zero/one law. The picture is the same as in the classical-UC setting.



(b) Statistical landscape: zero/xor/one. The three dots represent an infinite hierarchy of functionalities.

Fig. 1. Cryptographic complexity in the quantum-UC framework: the box denotes the class of deterministic finite two-party functionalities. The set $\mathcal{U}^-$ corresponds to the white area. The solid lines represent separations between non-equivalent primitives. The dotted lines represent separations that exist only in the classical-UC setting.

quantum-UC complete nor quantum-UC feasible and $\mathcal{F}_{\mathtt{XOR}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$*. Furthermore, for each of the three statements, there exists at least one* $\mathcal{F} \in \mathcal{U}^-$ *which satisfies it.*

Proof (Sketch). By Lemma 2 and because statistically, $\mathcal{F}_{\mathtt{2CC}}$, $\mathcal{F}_{\mathtt{COM}}$ and $\mathcal{F}_{\mathtt{OT}}$ are quantum-UC complete and $\mathcal{F}_{\mathtt{XOR}}$ is not quantum-UC feasible (since otherwise $\mathcal{F}_{\mathtt{XOR}}$ is also classical-UC feasible, contradicting the classical impossibility result in [27]), we can see that that for any $\mathcal{F} \in \mathcal{U}^-$, either $\mathcal{F}$ is quantum-UC feasible, or at least one of the following two statements holds: (1) $\mathcal{F}$ is quantum-UC complete and (2) $\mathcal{F}_{\mathtt{XOR}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$.

We then show that $\mathcal{F}_{\mathtt{XOR}}$ is not quantum-UC complete by proving that there is *no* quantum protocol that UC realizes $\mathcal{F}_{\mathtt{COM}}$ in the $\mathcal{F}_{\mathtt{XOR}}$-hybrid world. Proof of this statement is reminiscence of Lo and Chau's proof that quantum protocols are impossible to implement commitment [24]. The essence there is a so called "purification" attack where a dishonest sender can purify the protocol in the commit phase which allows him to apply a transformation on his local system, by which he can open to a value other than what he committed to. In our case, the only difference is that a quantum protocol can use $\mathcal{F}_{\mathtt{XOR}}$ as an extra setup. However, $\mathcal{F}_{\mathtt{XOR}}$ is nothing but a classical fair-exchange channel. In particular, the classical information in the protocol is symmetric to both parties, and we can argue that a dishonest committer can make the overall quantum state pure conditioned on shared classical information at the end of commit phase, so that the purification attack still applies. We defer a formal proof to the full version.

Finally, [27] showed that classically the class of functionalities that $\mathcal{F}_{\texttt{XOR}}$ reduces to and are not complete, denoted $\mathcal{E}$, are exactly those of the form $\mathcal{F}_{\texttt{EXCH}}^{(\ell_1,\ell_2)}$: simultaneous exchange channels that trasmit ℓ_1 (resp. ℓ_2) bits from one party to the other. The above argument that $\mathcal{F}_{\texttt{XOR}}$ is not quantum-UC complete extends straightforwardly to all such $\mathcal{F}_{\texttt{EXCH}}$, thus we conclude that any functionality in the $\mathcal{F}_{\texttt{XOR}}$ family $\mathcal{E}$ are neither statistically quantum-UC complete nor statistically quantum-UC feasible. Thus we can derive the quantum-UC statistical landscape for $\mathcal{U}^-$ as in Figure 1b.

References

1. Barak, B., Canetti, R., Nielsen, J.B., Pass, R.: Universally composable protocols with relaxed set-up assumptions. In: 45th Annual Symposium on Foundations of Computer Science (FOCS), pp. 186–195. IEEE (October 2004)
2. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: 47th Annual Symposium on Foundations of Computer Science (FOCS), pp. 249–260. IEEE (October 2006)
3. Bennett, C., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp. 175–179 (December 1984)
4. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.-H.: Practical Quantum Oblivious Transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366. Springer, Heidelberg (1992)
5. Bouman, N.J., Fehr, S.: Sampling in a Quantum Population, and Applications. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 724–741. Springer, Heidelberg (2010)
6. Buhrman, H., Christandl, M., Schaffner, C.: Complete insecurity of quantum protocols for classical two-party computation. Phys. Rev. Lett. 109, 160501 (2012)
7. Canetti, R.: Security and composition of multiparty cryptographic protocols. Journal of Cryptology 13(1), 143–202 (2000)
8. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: 42nd Annual Symposium on Foundations of Computer Science (FOCS), pp. 136–145. IEEE (October 2001)
9. Canetti, R., Fischlin, M.: Universally Composable Commitments. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 19–40. Springer, Heidelberg (2001)
10. Canetti, R., Kushilevitz, E., Lindell, Y.: On the limitations of universally composable two-party computation without set-up assumptions. Journal of Cryptology 19(2), 135–167 (2006)
11. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: 34th Annual ACM Symposium on Theory of Computing (STOC), pp. 494–503. ACM Press (May 2002)
12. Canetti, R., Pass, R., Shelat, A.: Cryptography from sunspots: How to use an imperfect reference string. In: 48th Annual Symposium on Foundations of Computer Science (FOCS), pp. 249–259. IEEE (October 2007)
13. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: 34th Annual ACM Symposium on Theory of Computing (STOC), pp. 643–652. ACM Press (May 2002)

14. Crépeau, C., Salvail, L., Simard, J.-R., Tapp, A.: Two Provers in Isolation. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 407–430. Springer, Heidelberg (2011)
15. Damgård, I., Fehr, S., Lunemann, C., Salvail, L., Schaffner, C.: Improving the Security of Quantum Protocols via Commit-and-Open. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 408–427. Springer, Heidelberg (2009)
16. Dupuis, F., Nielsen, J.B., Salvail, L.: Actively Secure Two-Party Evaluation of Any Quantum Operation. In: Safavi-Naini, R. (ed.) CRYPTO 2012. LNCS, vol. 7417, pp. 794–811. Springer, Heidelberg (2012)
17. Hallgren, S., Smith, A., Song, F.: Classical Cryptographic Protocols in a Quantum World. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 411–428. Springer, Heidelberg (2011)
18. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding Cryptography on Oblivious Transfer – Efficiently. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 572–591. Springer, Heidelberg (2008)
19. Katz, J.: Universally Composable Multi-party Computation Using Tamper-Proof Hardware. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 115–128. Springer, Heidelberg (2007)
20. Katz, J., Kiayias, A., Kumaresan, R., Shelat, A., Zhou, H.-S.: From impossibility to completeness for deterministic two-party SFE (2011) (manuscript)
21. Kilian, J.: Founding cryptography on oblivious transfer. In: STOC, pp. 20–31. ACM (1988)
22. Kraschewski, D., Müller-Quade, J.: Completeness Theorems with Constructive Proofs for Finite Deterministic 2-Party Functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 364–381. Springer, Heidelberg (2011)
23. Lo, H.-K.: Insecurity of quantum secure computations. Physical Review A 56(2), 1154–1162 (1997)
24. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Physical Review Letters 78, 3410–3413 (1997)
25. Lo, H.-K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science 283(5410), 2050–2056 (1999)
26. Lunemann, C., Nielsen, J.B.: Fully Simulatable Quantum-Secure Coin-Flipping and Applications. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 21–40. Springer, Heidelberg (2011)
27. Maji, H.K., Prabhakaran, M., Rosulek, M.: Complexity of Multi-party Computation Problems: The Case of 2-Party Symmetric Secure Function Evaluation. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 256–273. Springer, Heidelberg (2009)
28. Maji, H.K., Prabhakaran, M., Rosulek, M.: A Zero-One Law for Cryptographic Complexity with Respect to Computational UC Security. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 595–612. Springer, Heidelberg (2010)
29. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Physical Review Letters 78, 3414–3417 (1997)
30. Mayers, D.: Unconditional security in quantum cryptography. J. ACM 48(3), 351–406 (2001)
31. Müller-Quade, J., Renner, R.: Composability in quantum cryptography. New J. Phys. 11, 085006 (2009)

32. Prabhakaran, M., Rosulek, M.: Cryptographic Complexity of Multi-Party Computation Problems: Classifications and Separations. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 262–279. Springer, Heidelberg (2008)
33. Rosulek, M.: Universal Composability from Essentially Any Trusted Setup. In: Safavi-Naini, R. (ed.) CRYPTO 2012. LNCS, vol. 7417, pp. 406–423. Springer, Heidelberg (2012)
34. Salvail, L., Schaffner, C., Sotáková, M.: On the Power of Two-Party Quantum Cryptography. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 70–87. Springer, Heidelberg (2009)
35. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85(2), 441–444 (2000)
36. Unruh, D.: Universally Composable Quantum Multi-party Computation. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 486–505. Springer, Heidelberg (2010)
37. Watrous, J.: Zero-knowledge against quantum attacks. SIAM J. Comput. 39(1), 25–58 (2009); Preliminary version in STOC 2006