Feasibility and Completeness of Cryptographic Tasks in the Quantum World

Serge Fehr* Jonathan Katz† Fang Song‡ Hong-Sheng Zhou†§
Vassilis Zikas†

June 12, 2014

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.

*Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands. Email: serge.fehr@cwi.nl.

†Department of Computer Science, University of Maryland, College Park, MD 20742, USA. Email: {jkatz,hszhou,vzikas}@cs.umd.edu. This work is supported in part by NSF award #1111599 and DARPA.

‡Department of Computer Science & Engineering, Pennsylvania State University, University Park, PA 16802, USA. Email: fus121@cse.psu.edu.

§Supported by an NSF CI postdoctoral fellowship.

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 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 [Can01], which provides strong composition guarantees when arbitrary protocols are executed concurrently. Soon after the introduction of this framework, Canetti and Fischlin [CF01] 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 [CKL06, PR08].

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 [CF01, CLOS02]. Subsequent work has identified other *complete* setup assumptions [BCNP04, Kat07, IPS08, CPS07]. Completeness results in the *information-theoretic* (or *statistical*) setting, where the adversary is computationally unbounded, have also been shown [Kil88, IPS08].

Maji et al. [MPR10] 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. [KKK+11], who showed completeness for deterministic functions with exponential-size input domains, and by Rosulek [Ros12], who showed completeness for randomized, reactive functions as well. In the setting of information-theoretic security, Kraschewski et al. [KMQ11] 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. [MPR09] 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 [CSST11].

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 [BB84] but not in the classical one. While several impossibility results for statistically secure two-party computation in the quantum setting are known [May97, LC97, Lo97, SSS09, BCS12], 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

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

is impossible [MPR09]. However, there is a construction of OT from commitment in the quantum world [BBCS92, DFL$^+$09, Unr10, BF10]; as a consequence, commitment is complete for UC computation in that setting [Unr10].

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 [Unr10] 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 [Unr10]) 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. [HSS11] "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 [CF01], 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 [BBCS92], 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 [BF10], 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 [Unr10], 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 in our class is either trivial or complete in the quantum computational setting; thus, the situation here is analogous to the classical case [MPR10]. In the quantum *statistical* setting, however, functionalities fall into one of three different classes; this is in contrast with the (more complicated) classical picture [MPR09, KMQ11].

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 [May01, LC99, SP00]. 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 [CGS02, BOCG$^+$06]. Positive results for computational security in the quantum world, without honest majority, have only recently been shown [Wat09, LN11, HSS11, DNS12].

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,

[2] A similar result was stated in [MQR09] with no proof.

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 [Can01]. For quantum statements we use the recently developed quantum-UC framework [Unr10]. A high-level description of the models can be found in Appendix B. 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 [Unr10]. 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 [Unr10]. 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. $\mathcal{F}' \sqsubseteq^{\text{QSTAT}} \mathcal{F}$). The definitions of computation and statistical quantum-UC equivalence is also analogous to the classical setting.

In [Unr10] 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 ([Unr10, 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 [Can00, Can01]. We point out that the definition of statistical quantum-UC security in [Unr10] 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(we refer to Appendix B.4 for a formal definition), which is the central class studied in [MPR09, MPR10]. 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 [MPR10], 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; a formal description can be found in Appendix B.5.Consistently with existing literature we use the names Alice and Bob for the parties:

• Secure Function Evaluation $\mathcal{F}_{\mathtt{SFE}}$: An SFE functionality $\mathcal{F}_{\mathtt{SFE}}$ is specified by a pair of functions (f_A, f_B) over a finite input domain $X \times Y$. Alice inputs value $x \in X$ and Bob inputs $y \in Y$. Then Alice receives $f_A(x, y)$ while Bob obtains $f_B(x, y)$.

[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.

[4] Our conjecture is that $\mathcal{F}_{\mathtt{1cc}}$ is also statistically quantum-UC complete. Recall that classically neither $\mathcal{F}_{\mathtt{cc}}$ not $\mathcal{F}_{\mathtt{2cc}}$ is statistically UC complete [MPR10].

[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.) [MPR10].

• 1-out-of-2 Oblivious Transfer $\mathcal{F}_{\mathtt{OT}}$: 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 $\mathcal{F}_{\mathtt{OT}}$. 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 $\mathcal{F}_{\mathtt{COM}}$: Alice (the committer) inputs a bit b and Bob (the receiver) receives from $\mathcal{F}_{\mathtt{COM}}$ a notification that a bit was received. At a later point, Alice can input the command open to $\mathcal{F}_{\mathtt{COM}}$ in which case Bob receives b.

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

• Fair (Simultaneous) Exchange $\mathcal{F}_{\mathtt{EXCH}}$: Alice and Bob input strings b_A and b_B, respectively, and receive outputs $y_A = b_B$ and $y_B = b_A$, respectively.

• 2-bit Cut-and-Choose $\mathcal{F}_{\mathtt{2CC}}$: 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 $\mathcal{F}_{\mathtt{COIN}}$: Alice and Bob input a request to $\mathcal{F}_{\mathtt{COIN}}$, and $\mathcal{F}_{\mathtt{COIN}}$ 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 $\mathcal{F}_{\mathtt{OT}}$, $\mathcal{F}_{\mathtt{XOR}}$, $\mathcal{F}_{\mathtt{2CC}}$, and $\mathcal{F}_{\mathtt{COM}}$ 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 2 (Quantum Lifting of Completeness)**.** *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.*[6]

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 [MPR10]: 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 $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{COM}}\}$, there exists a statistically quantum-UC secure protocol which reduces $\mathcal{F}'$ to $\mathcal{F}$. Second, in Section 3.2, we show that $\mathcal{F}_{\mathtt{XOR}}$, $\mathcal{F}_{\mathtt{OT}}$, $\mathcal{F}_{\mathtt{2CC}}$, and $\mathcal{F}_{\mathtt{COM}}$ 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.

[6] For a concrete description of the assumptions we refer to Appendix C.

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 [MPR10, 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 ([MPR10])**.** *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 3. *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 8), statistically 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[7]. The quantum-UC completeness of $\mathcal{F}_{\mathtt{OT}}$ and $\mathcal{F}_{\mathtt{COM}}$ was proved in [Unr10]:

Lemma 4. *The OT functionality $\mathcal{F}_{\mathtt{OT}}$ and the commitment functionality $\mathcal{F}_{\mathtt{COM}}$ 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 [HSS11] who proved computationally quantum-UC completeness of $\mathcal{F}_{\mathtt{COIN}}$ under proper assumptions. The more detailed proof can be found in Appendix C.

Lemma 5. *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.*

The most involved completeness proof is the one concerning the cut-and-choose functionality $\mathcal{F}_{\mathtt{2CC}}$. In [MPR10], 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.[8]

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 4). The idea is motivated by the quantum OT construction in the $\mathcal{F}_{\mathtt{COM}}$ hybrid world by Bennett et al [BBCS92]. In this protocol, roughly speaking, $\mathcal{F}_{\mathtt{COM}}$ is used in a checking subroutine to ensure that malicious

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

[8] 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 [MPR10] actually satisfies. The subtlety is that the correctness of the simulator might still involve rewinding argument (e.g., in defining hybrid experiments).

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 [DFL$^+$09, Unr10, BF10].

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 [DFL$^+$09, BF10], cannot deal with that.

In order to deal with this issue, we introduce an *adaptive* version of the sampling framework of [BF10]. We then show, analogous to the static setting as in [BF10], 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 6. The formal proof can be found in Appendix D.

Lemma 6. *There exists an $\mathcal{F}_{\mathtt{2CC}}$-hybrid protocol which statistically quantum-UC realizes $\mathcal{F}_{\mathtt{OT}}$.*

The following corollary follows from Lemma 6 and the completeness of $\mathcal{F}_{\mathtt{OT}}$ (Lemma 4), by applying the quantum-UC composition theorem.

Corollary 7. *$\mathcal{F}_{\mathtt{2CC}}$ is statistically quantum-UC complete.*

The proof of Theorem 3 follows easily from Lemmas 3, 4, 5, and Corollary 7, 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 8 (Quantum Bi-Lifting of Feasibility)**.** *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.*

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.

4. $\mathcal{F}$ is computationally quantum-UC feasible.

In the remaining of this section we prove the above theorem, by showing that for each $i \in \{1,2,3\}$ Statement i implies Statement $i+1$, and, finally, that Statement 4 implies Statement 1.

For the first implication (i.e., that Statement 1 implies Statement 2) we use the following result about classical functionalities implied by [MPR10, Theorems 1,4]:

Fact 3 ([MPR10, Theorems 1,4])**.** *The functionalities $\mathcal{F}_{\mathtt{OT}}$, $\mathcal{F}_{\mathtt{2CC}}$, $\mathcal{F}_{\mathtt{COM}}$, and $\mathcal{F}_{\mathtt{XOR}}$ are computationally (classical) UC complete.*[9]

Claim 1. *If $\mathcal{F} \in \mathcal{U}^-$ is computationally (classical) UC feasible then $\mathcal{F}$ is statistically (classical) UC feasible.*

Proof (sketch). Assume, for contradiction, that $\mathcal{F}$ is not statistically (classical) UC feasible. Then, Fact 2 implies that for some $\mathcal{F}' \in \{\mathcal{F}_{\mathtt{OT}}, \mathcal{F}_{\mathtt{2CC}}, \mathcal{F}_{\mathtt{XOR}}, \mathcal{F}_{\mathtt{COM}}\}$: $\mathcal{F}' \sqsubseteq^{\text{CCOMP}} \mathcal{F}$, which, by the claim's

[9] Observe that [MPR10] proved completeness of $\mathcal{F}_{\mathtt{cc}}$ instead of $\mathcal{F}_{\mathtt{2cc}}$; however, this directly implies completeness of $\mathcal{F}_{\mathtt{2cc}}$ as $\mathcal{F}_{\mathtt{cc}} \sqsubseteq^{\text{COMP}} \mathcal{F}_{\mathtt{2cc}}$.

assumption, that $\mathcal{F}$ is computationally UC feasible, implies that $\mathcal{F}'$ is feasible contradicting the results from [MPR10, Theorem 4]. □

The second implication (i.e., the proof that Statement 2 implies Statement 3) follows directly by using Unruh's quantum lifting theorem, whereas the third implication (i.e., the proof that Statement 3 implies Statement 4) follows from the fact that statistical feasibility implies computational feasibility. In the remaining of this section we prove the last implication (i.e., the proof that Statement 4 implies Statement 1). In order to prove this implication we first prove that there exist functionalities in $\mathcal{U}^-$ which are *not* computationally quantum-UC feasible. Specifically, we prove an extension of the (classical) impossibility of UC commitments [CF01] to the quantum-UC setting. Notice that this claim was briefly stated previously in [MQR09] but with no proof. For completeness, we give a proof in Appendix E which follows the structure of the classical impossibility proof.

Lemma 9. *There exists no protocol in the plain model which computationally quantum-UC realizes the commitment functionality* $\mathcal{F}_{\mathtt{COM}}$.

We now prove the last implication which completes the proof of Theorem 8.

Claim 2. *If* $\mathcal{F} \in \mathcal{U}^-$ *is computationally quantum-UC feasible then* $\mathcal{F}$ *is computationally (classical) UC feasible.*

Proof. Assume, towards contradiction, that $\mathcal{F}$ is not computationally (classical) UC feasible. Then, Fact 2 implies 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 2, implies that $\mathcal{F}$ is computationally quantum-UC complete. This, combined with the claim's assumption that $\mathcal{F}$ is computationally quantum-UC feasible, implies that every $\mathcal{F} \in \mathcal{U}^-$ is computationally quantum-UC feasible contradicting the impossibility of $\mathcal{F}_{\mathtt{COM}}$. □

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 [MPR10]. 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. This proves the following theorem :

Theorem 10 (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 2 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 10 implies that it is not quantum-UC feasible, which implies (by Theorem 8) 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 11 (Quantum Bi-lifting of Computational Completeness)**.** *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 6 is in fact complete in the quantum setting. This illustrates, as [Unr10] mentioned also, that the inverse of the Unruh's quantum lifting lemma is in general not true, which is formalized in the following lemma:

Lemma 12. *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 (classic) UC realizes $\mathcal{F}'$.*

Proof (sketch). For the cut-and-choose functionality $\mathcal{F}_{\mathtt{2CC}}$, it is shown in [MPR09] that $\mathcal{F}_{\mathtt{2CC}}$ is not statistically UC complete, which implies that there exists no $\mathcal{F}_{\mathtt{2CC}}$-hybrid protocol which statistically UC securely realizes the oblivious transfer functionality $\mathcal{F}_{\mathtt{OT}}$. Indeed, the existence of such a protocol together with the statistical UC completeness of $\mathcal{F}_{\mathtt{OT}}$ would imply statistical UC completeness of $\mathcal{F}_{\mathtt{2CC}}$. However, as shown in Lemma 6 there exists a quantum $\mathcal{F}_{\mathtt{2CC}}$-hybrid protocol which statistically quantum-UC securely realizes $\mathcal{F}_{\mathtt{OT}}$. □

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

Theorem 13 (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 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). The proof proceeds in two steps: First (Claim 3) we show that 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) $\mathcal{F}_{\mathtt{XOR}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$. In a second step, (Claim 4) we show that $\mathcal{F}_{\mathtt{XOR}}$ is not UC complete. Because (1) $\mathcal{F}_{\mathtt{XOR}}$ is also not statistically quantum-UC feasible (otherwise, this would imply that it is also computationally (classical) UC feasible contradicting the results of [MPR10].) and (2) statistically quantum-UC feasible functionalities are not statistically quantum-UC complete (as implied by Lemma 9), we can deduce that there is at least one functionality that satisfies each case.

Claim 3. *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) $\mathcal{F}_{\mathtt{XOR}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$.*

Proof. Fact 2 combined with Lemma 6 and the completeness of $\mathcal{F}_{\mathtt{COM}}$ from [Unr10] imply that when $\mathcal{F}$ is not feasible then $\mathcal{F}_{\mathtt{OT}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$ or $\mathcal{F}_{\mathtt{XOR}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$. The statistical UC completeness of $\mathcal{F}_{\mathtt{OT}}$ implies (Theorem 2) statistical quantum-UC completeness of $\mathcal{F}_{\mathtt{OT}}$, hence, $\mathcal{F}_{\mathtt{OT}} \sqsubseteq^{\mathrm{QSTAT}} \mathcal{F}$ implies that $\mathcal{F}$ is statistically quantum-UC complete. Furthermore, the feasibility quantum lifting theorem (Theorem 8) implies that $\mathcal{F}_{\mathtt{OT}}$ and $\mathcal{F}_{\mathtt{XOR}}$ are not statistically quantum-UC feasible (as this would imply that they are computationally (classical) UC feasible contradicting the results of [MPR10].) □

Claim 4. *The functionality $\mathcal{F}_{\texttt{XOR}}$ is* not *statistically quantum-UC complete.*

Proof. The proof proceeds in two steps: In a first step we show that $\mathcal{F}_{\texttt{XOR}}$ is statistically quantum-UC equivalent[10] to the simultaneous exchange functionality $\mathcal{F}_{\texttt{EXCH}}$ which allows two parties each having input one bit to fairly and securely exchange their inputs (for a detailed description we refer to Appendix B.4). In a second step, we show that $\mathcal{F}_{\texttt{EXCH}}$ is not quantum-UC complete, which, as $\mathcal{F}_{\texttt{EXCH}}$ is equivalent to $\mathcal{F}_{\texttt{XOR}}$, implies the $\mathcal{F}_{\texttt{XOR}}$ is also not quantum-UC complete.

Step 1: One can classically implement $\mathcal{F}_{\texttt{EXCH}}$ from $\mathcal{F}_{\texttt{XOR}}$ as follows: Alice and Bob input their bits b_A and b_B, respectively, into the $\mathcal{F}_{\texttt{XOR}}$ functionality and obtain the output y. Alice outputs $y_A = y \oplus b_A$ and Bob outputs $y_B = y \oplus b_B$. Similarly, one can classically implement $\mathcal{F}_{\texttt{XOR}}$ from $\mathcal{F}_{\texttt{EXCH}}$ as follows: Alice and Bob input their bits b_A and b_B, respectively, into the $\mathcal{F}_{\texttt{EXCH}}$ functionality and obtain their respective outputs y_A and y_B; they both output $y = y_A \oplus y_B$. Both implementations are trivially statistically (in fact, even perfectly) UC secure in the classical stetting; hence, the quantum lifting Theorem [Unr10] implies that there are also statistically quantum-UC secure reductions between $\mathcal{F}_{\texttt{EXCH}}$ and $\mathcal{F}_{\texttt{XOR}}$.

Step 2: For proving that $\mathcal{F}_{\texttt{EXCH}}$ (hence also $\mathcal{F}_{\texttt{XOR}}$) is not statistically quantum-UC complete, it suffices to prove that one cannot construct a quantumly secure commitment scheme assuming $\mathcal{F}_{\texttt{EXCH}}$ (on top of regular communication). This is an easy extension of the impossibility proof of quantum commitment by Lo and Chau [LC97]: the key idea in [LC97] is that a dishonest committer (Alice) could purify her operations and make sure at the end of the committing phase, the joint state with the receiver (Bob) will be a pure state $|\Psi^b_{AB}\rangle$, where b is the bit Alice is supposed to commit. But the hiding property, which we assume is perfect for simplicity, requires that $tr_A(|\Psi^0_{AB}\rangle\langle\Psi^0_{AB}|) = tr_A(|\Psi^1_{AB}\rangle\langle\Psi^1_{AB}|) =: \rho_B$. This immediately implies that $|\Psi^0_{AB}\rangle$ and $|\Psi^1_{AB}\rangle$ are just two possible purifications of the same ρ_B and by Uhlmann's theorem, there exists a unitary U_A operating on Alice's system alone that transforms $|\Psi^b_{AB}\rangle$ into $|\Psi^{1-b}_{AB}\rangle$. Thus Alice breaks binding completely. Here we use a generalization by Winkler et al. [WTHR11], claiming that if the joint state is pure conditioned on the symmetric classical information available to both Alice and Bob, then analogous transformation also exists. Now observe that, given any quantum protocol with a classical fair-exchange channel $\mathcal{F}_{\texttt{EXCH}}$, the classical information will always be symmetric to two parties, and a dishonest Alice can as well purify her operations and apply the transformation, guaranteed by [WTHR11], to break the binding property.

This completes the proof of the theorem. □

To complete the picture in Figure 1 we need to show that not only $\mathcal{F}_{\texttt{XOR}}$ is not complete, but the whole "exchange-like hierarchy" from [MPR09] consists of incomplete primitives. This hierarchy is a family of primitives, denoted by $\mathcal{E}$, that correspond to simultaneously exchange channels (of the type of $\mathcal{F}_{\texttt{EXCH}}$) for different input lengths. In other words, $\mathcal{E}$ consists of two-party functionalities ${\mathcal{F}_{\texttt{EXCH}}}^{(\ell_1,\ell_2)}$, where $(\ell_1, \ell_2) \in \mathbb{N}^2$, defined as follows: ${\mathcal{F}_{\texttt{EXCH}}}^{(\ell_1,\ell_2)}$ takes from Alice a message $x_A \in \{0,1\}^{\ell_1}$ and from Bob a message $x_B \in \{0,1\}^{\ell_2}$; it returns to Alice x_B and to Bob x_A. Note that all the primitives in this hierarchy are sufficient for implementing $\mathcal{F}_{\texttt{XOR}}$ and, therefore, are not UC-feasible. Additionally, it is straight-forward to verify that the proof of Claim 4 goes through even if we replace $\mathcal{F}_{\texttt{XOR}}$ by any of the primitives in $\mathcal{E}$.

This proves the following:

Lemma 14. *For any ${\mathcal{F}_{\texttt{EXCH}}}^{(\ell_1,\ell_2)} \in \mathcal{E}$: ${\mathcal{F}_{\texttt{EXCH}}}^{(\ell_1,\ell_2)}$ is neither statistically quantum-UC complete nor statistically quantum-UC feasible.*

[10] By this we mean that there exists a protocol statistically quantum-UC realize $\mathcal{F}_{\texttt{XOR}}$ from $\mathcal{F}_{\texttt{EXCH}}$ and vise versa.

References

[BB84] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India*, pages 175–179, December 1984.

[BBCS92] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In Joan Feigenbaum, editor, *Advances in Cryptology — Crypto '91*, volume 576 of *LNCS*, pages 351–366. Springer, 1992.

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *FOCS*, pages 449–458, 2002.

[BCNP04] Boaz Barak, Ran Canetti, Jesper Buus Nielsen, and Rafael Pass. Universally composable protocols with relaxed set-up assumptions. In *45th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 186–195. IEEE, October 2004.

[BCS12] Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Phys. Rev. Lett.*, 109:160501, Oct 2012.

[BF10] Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications. In *Advances in Cryptology — Crypto 2010*, volume 6223 of *LNCS*, pages 724–741. Springer, 2010.

[Blu82] Manuel Blum. Coin flipping by telephone. In Allen Gersho, editor, *Advances in Cryptology — Crypto '81*, volume ECE Report 82-04, pages 11–15. U.C. Santa Barbara, Dept. of Elec. and Computer Engineering, 1982.

[BOCG+06] Michael Ben-Or, Claude Crépeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *47th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 249–260. IEEE, October 2006.

[Bra06] Gilles Brassard. Brief history of quantum cryptography: A personal perspective, April 2006. arxiv:quant-ph/0604072.

[Can00] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 136–145. IEEE, October 2001.

[Can05] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2005. `http://eprint.iacr.org/`.

[CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In Joe Kilian, editor, *Advances in Cryptology — Crypto 2001*, volume 2139 of *LNCS*, pages 19–40. Springer, 2001.

[CGS02] Claude Crépeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. In *34th Annual ACM Symposium on Theory of Computing (STOC)*, pages 643–652. ACM Press, May 2002.

[CKL06] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *Journal of Cryptology*, 19(2):135–167, April 2006.

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *34th Annual ACM Symposium on Theory of Computing (STOC)*, pages 494–503. ACM Press, May 2002.

[CPS07] Ran Canetti, Rafael Pass, and Abhi Shelat. Cryptography from sunspots: How to use an imperfect reference string. In *48th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 249–259. IEEE, October 2007.

[CSST11] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. LNCS, pages 407–430. Springer, 2011.

[DFL+09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In Shai Halevi, editor, *Advances in Cryptology — Crypto 2009*, volume 5677 of *LNCS*, pages 408–427. Springer, 2009.

[DNS12] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In *Advances in Cryptology - Crypto 2012*, volume 7417 of *LNCS*, pages 794–811. Springer, 2012.

[HSS11] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *Advances in Cryptology — Crypto 2011*, volume 6841 of *LNCS*, pages 411–428. Springer, 2011.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *Advances in Cryptology — Crypto 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, 2008.

[Kat07] Jonathan Katz. Universally composable multi-party computation using tamper-proof hardware. In Moni Naor, editor, *Advances in Cryptology — Eurocrypt 2007*, volume 4515 of *LNCS*, pages 115–128. Springer, 2007.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *STOC*, pages 20–31. ACM, 1988.

[KKK+11] Jonathan Katz, Aggelos Kiayias, Ranjit Kumaresan, Abhi Shelat, and Hong-Sheng Zhou. From impossibility to completeness for deterministic two-party SFE, 2011. Manuscript.

[KMQ11] Daniel Kraschewski and Jörn Müller-Quade. Completeness theorems with constructive proofs for finite deterministic 2-party functions. In *8th Theory of Cryptography Conference — TCC 2011*, volume 6597 of *LNCS*, pages 364–381. Springer, 2011.

[LC97] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410–3413, 1997.

[LC99] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[LN11] Carolin Lunemann and Jesper Buus Nielsen. Fully simulatable quantum-secure coin-flipping and applications. LNCS, pages 21–40, 2011.

[Lo97] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, 2001.

[MPR09] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In *6th Theory of Cryptography Conference — TCC 2009*, volume 5444 of *LNCS*, pages 256–273. Springer, 2009.

[MPR10] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. A zero-one law for cryptographic complexity with respect to computational UC security. In *Advances in Cryptology — Crypto 2010*, volume 6223 of *LNCS*, pages 595–612. Springer, 2010.

[MQR09] Jörn Müller-Quade and Renato Renner. Composability in quantum cryptography. *New J. Phys. 11 085006*, 2009.

[PR08] Manoj Prabhakaran and Mike Rosulek. Cryptographic complexity of multi-party computation problems: Classifications and separations. In David Wagner, editor, *Advances in Cryptology — Crypto 2008*, volume 5157 of *LNCS*, pages 262–279. Springer, 2008.

[Rab81] Michael Rabin. How to exchange secrets by oblivious transfer, 1981. Technical Memo TR-81, Aiken Computation Laboratory, Harvard University.

[Ren05] Renato Renner. Security of quantum key distribution, January 2005. arXiv:quant-ph/0512258.

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *2nd Theory of Cryptography Conference — TCC 2005*, volume 3378 of *LNCS*, pages 407–425. Springer, February 2005.

[Ros12] Mike Rosulek. Universal composability from essentially any trusted setup. In *Advances in Cryptology - Crypto 2012*, volume 7417 of *LNCS*, pages 406–423. Springer, 2012.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, Jul 2000.

[SSS09] Louis Salvail, Christian Schaffner, and Miroslava Sotáková. On the power of two-party quantum cryptography. In *Advances in Cryptology — Asiacrypt 2009*, volume 5912 of *LNCS*, pages 70–87. Springer, December 2009.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology — Eurocrypt 2010*, volume 6110 of *LNCS*, pages 486–505. Springer, 2010.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version in STOC 2006.

[WTHR11] Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner. Impossibility of growing commitments. *Physical Review Letters*, 107, 2011.

A Figures

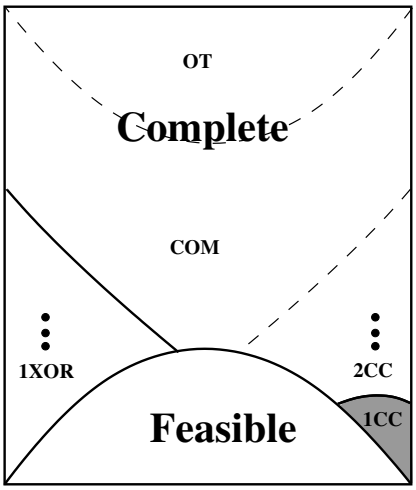

Figure 1: The feasibility/completeness landscape for the class of deterministic finite two-party functionalities in the *statistical* quantum-UC setting. The set $\mathcal{U}^-$ corresponds to the white area. The solid lines represent separations between non-equivalent primitives which exist both in the quantum-UC and in the classical-UC setting. The dotted lines represent separations that exist only in the classical-UC setting. The three dots over 1XOR (resp. 2CC) represent the infinite hierarchy of XOR (resp. CC) primitives which was proved by [MPR09, KMQ11]. Note that in the classical setting both hierarchies are *strict*, i.e., lower primitives are separated from higher, but in the quantum setting the CC hierarchy collapses at the second level, as 2CC is quantum-UC complete (Corollary 7).

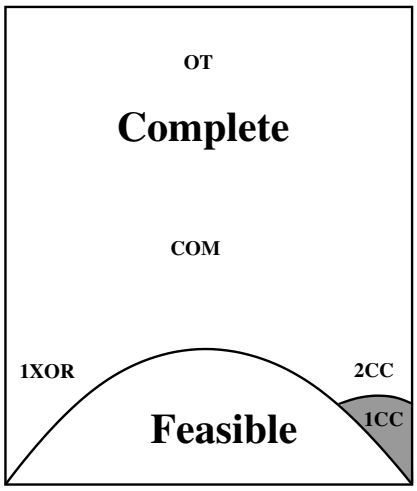

Figure 2: The feasibility/completeness landscape for the class of deterministic finite two-party functionalities in the *computational* quantum-UC setting. The set $\mathcal{U}^-$ corresponds to the white area. The solid lines represent separations between non-equivalent primitives. The picture is the same in the quantum-UC and in the classical-UC setting.

B Universal Composition (UC) Framework

We give a very brief introduction to the UC model in classical setting and in quantum setting, and refer readers to [Can05] and [Unr10] respectively for more details.

B.1 Classical UC Model

Machines. The basic entities involved in the UC model are players $P_1, \ldots, P_n$ where n is in polynomial of security parameter κ, an adversary $\mathcal{A}$, and an environment $\mathcal{Z}$. Each entity is modeled as a interactive Turing machine (ITM), where $\mathcal{Z}$ could have an additional non-uniform string as advice. Each P_i has identity i assigned to it, while $\mathcal{A}$ and $\mathcal{Z}$ have special identities $id_{\mathcal{A}} := \texttt{adv}$ and $id_{\mathcal{Z}} := \texttt{env}$.

Protocol Execution. A protocol specifies the programs for each P_i, which we denote as $\pi = (\pi_1, \ldots, \pi_n)$. The execution of a protocol is coordinated by the environment $\mathcal{Z}$. It starts by preparing inputs to all players, who then run their respective programs on the inputs and exchange messages of the form $(id_{\texttt{sender}}, id_{\texttt{receiver}}, \texttt{msg})$. $\mathcal{A}$ can corrupt an arbitrary set of players and control them later on. In particular, $\mathcal{A}$ can instruct a corrupted player sending messages to another player and also read messages that are sent to the corrupted players. During the course of execution, the environment $\mathcal{Z}$ also interacts with $\mathcal{A}$ in an arbitrary way. In the end, $\mathcal{Z}$ receives outputs from all the other players and generates one bit output. We use $\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \pi]$ denote the distribution of the environment $\mathcal{Z}$'s (single-bit) output when executing protocol π with $\mathcal{A}$ and the P_i's.

Ideal Functionality and Dummy Protocol. Ideal functionality $\mathcal{F}$ is a trusted party, modeled by an ITM again, that perfectly implements the desired multi-party computational task. We consider an "dummy protocol", denoted $P^{\mathcal{F}}$, where each party has direct communication with $\mathcal{F}$, who accomplishes the desired task according to the messages received from the players. The execution of $P^{\mathcal{F}}$ with environment $\mathcal{Z}$ and an adversary, usually called the simulator $\mathcal{S}$, is defined analogous as above, in particular, $\mathcal{S}$ monitors the communication between corrupted parties and the ideal functionality $\mathcal{F}$. Similarly, we denote $\mathcal{Z}$'s output distribution as $\mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, P^{\mathcal{F}}]$.

Definition 15. *(Classical UC-secure Emulation) We say π (classically) UC-emulates π' if for any adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$ such that for all environments $\mathcal{Z}$,*

$$\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \pi] \approx \mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, \pi']^{11}$$

If $\mathcal{A}$ and $\mathcal{Z}$ are computationally bounded, we call it computational UC-security; if $\mathcal{A}$ and $\mathcal{Z}$ are computationally unbounded, we call it statistical UC-security. In both cases, we require the running time $\mathcal{S}$ is polynomial in that of $\mathcal{A}$. We call this property Polynomial Simulation.

As a typical case, Let $\mathcal{F}$ be a well-formed two party functionality. We say π (classically) UC-emulates realizes $\mathcal{F}$ if for all adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$ such that for all environments $\mathcal{Z}$, $\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \pi] \approx \mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, P^{\mathcal{F}}]$.

UC-secure protocols admit a general composition property, demonstrated in the following universal composition theorem.

Theorem 16 (UC Composition Theorem [Can05])**.** *Let π, π' and σ be n-party protocols. Assume that π UC-emulates π'. Then σ^{π} UC-emulates $\sigma^{\pi'}$.*

[11] We say two binary distributions $\mathbf{X}$ and $\mathbf{Y}$ are *indistinguishable*, denoted $\mathbf{X} \approx \mathbf{Y}$, if $|\Pr(X_n = 1) - \Pr(Y_n = 1)| \leq \mathrm{negl}(n)$.

B.2 Quantum UC Model

Next we proceed to a high-level description of Unruh's quantum Universal-Composable model.

Quantum Machine. In the quantum UC model, all players are modeled as quantum machines. A quantum machine is a sequence of quantum circuits $\{M^\kappa\}_{\kappa\in\mathbb{N}}$, for each security parameter κ. M^κ is a completely positive trace preserving operator on space $\mathcal{H}^{\mathtt{state}} \otimes \mathcal{H}^{\mathtt{class}} \otimes \mathcal{H}^{\mathtt{quant}}$, where $\mathcal{H}^{\mathtt{state}}$ represents the internal workspace of M^κ and $\mathcal{H}^{\mathtt{class}}$ and $\mathcal{H}^{\mathtt{quant}}$ represent the spaces for communication, where for convenience we divide the messages into classical and quantum parts. We allow a non-uniform quantum advice[12] to the machine of the environment $\mathcal{Z}$, while all other machines are uniformly generated.

Protocol Execution. In contrast to the communication policy in classical UC model, we consider a network $\mathbf{N}$ which contains the space $\mathcal{H}_{\mathbf{N}} := \mathcal{H}^{\mathtt{class}} \otimes \mathcal{H}^{\mathtt{quant}} \otimes_i \mathcal{H}_i^{\mathtt{state}}$. Namely, each machine maintains individual internal state space, but the communication space is shared among all . We assume $\mathcal{H}^{\mathtt{class}}$ contains the message $(id_{\mathtt{sender}}, id_{\mathtt{receiver}}, \mathtt{msg})$ which specifies the sender and receiver of the current message, and the receiver then process the quantum state on $\mathcal{H}^{\mathtt{quant}}$. Note that this communication model implicitly ensures authentication. In a protocol execution, $\mathcal{Z}$ is activated first, and each round one player applies the operation defined by its machine M^κ on $\mathcal{H}^{\mathtt{class}} \otimes \mathcal{H}^{\mathtt{quant}} \otimes \mathcal{H}^{\mathtt{state}}$. In the end $\mathcal{Z}$ generates one-bit output. Denote $\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \Pi]$ the output distribution of $\mathcal{Z}$.

Remark 17 (Secure Communication). In [Unr10] secure channels are implicitly assumed. However, whenever we want to make the assumption of such channels explicit we shall denote them as $\mathcal{Q}_{\mathtt{SEC}}$. Note that as in the quantum setting secure (i.e., authenticated and private) channels can be obtained from (only) authenticated channels [BB84, BCG$^+$02]. Hence, one can use $\mathcal{Q}_{\mathtt{AUTH}}$ and $\mathcal{Q}_{\mathtt{SEC}}$, interchangeably.

Ideal Functionality. All functionality we consider in this work is classical, i.e., the inputs and outputs are classical, and its program can be implemented by a classical Turing machine. Here in quantum UC model, ideal functionality $\mathcal{F}$ is still modeled as a quantum machine for consistency, but it only applies classical operations. Namely, it measures any input message in the computational basis to get an classical bit-string, and implements the operations specified by the classical computational task.

Definition 18. *(Quantum UC-secure Emulation) We say* Π *quantum-UC-emulates* Π' *if for any quantum adversary* $\mathcal{A}$*, there exists a (quantum) simulator* $\mathcal{S}$ *such that for all quantum environments* $\mathcal{Z}$*,*

$$\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \Pi] \approx \mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, \Pi']$$

If $\mathcal{A}$ *and* $\mathcal{Z}$ *are computationally bounded, we call it (quantum) computational UC-security; if* $\mathcal{A}$ *and* $\mathcal{Z}$ *are computationally unbounded, we call it (quantum) statistical UC-security. In both cases, we require the running time* $\mathcal{S}$ *is polynomial in that of* $\mathcal{A}$*. We call this property* Polynomial Simulation*.*

As a typical case, Let $\mathcal{F}$ be a well-formed two party functionality. We say Π quantum-UC-emulates $\mathcal{F}$ if for all quantum adversary $\mathcal{A}$, there exists a (quantum) simulator $\mathcal{S}$ such that for all quantum environments $\mathcal{Z}$, $\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \Pi] \approx \mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, P^{\mathcal{F}}]$.

Quantum UC-secure protocols also admit general composition:

Theorem 19 (Quantum UC Composition Theorem [Unr10, Theorem 11])**.** *Let* Π, Π' *and* Σ *be quantum-polynomial-time protocols. Assume that* Π *quantum UC-emulates* Π'*. Then* Σ^Π *quantum UC-emulates* $\Sigma^{\Pi'}$*.*

[12] Unruh's model only allows classical advice, but we tend to take the most general model. It is easy to justify that almost all results remain unchanged, including the composition theorem. See [HSS11, Section 5] for more discussion.

B.3 Feasible Functionalities

Definition 20 (Classical Feasibility [PR08])**.** *We say a functionality $\mathcal{F}$ is* classically feasible *if there exists a classic protocol π that UC-realizes $\mathcal{F}$ in the plain UC model where basic communication such as secure and authenticated channels are available.*

Definition 21 (Quantum Feasibility)**.** *We say a functionality $\mathcal{F}$ is quantumly feasible if there exists a classical or quantum protocol Π that quantum-UC-securely realizes $\mathcal{F}$ in the quantum plain model where basic communication such as secure and authenticated quantum channels are available.*

B.4 Deterministic Finite Functionalities

For completeness, we give a formal description for the class of functionalities we consider in this work.

Definition 22. *(Deterministic Finite SFE.) Let $\mathcal{F} := \{f_\kappa\}_{\kappa\in\mathbb{N}}$ be a two-party SFE functionality: $f_\kappa : D_\kappa \times D'_\kappa \to R_\kappa \times R'_\kappa, \kappa \in \mathbb{N}$, where $D_\kappa, D'_\kappa, R_\kappa$ and R'_κ are all subsets in $\{0,1\}^\kappa$. We call $\mathcal{F}$* finite deterministic *if for all except finite number of $\kappa \in \mathbb{N}$, there exist polynomials $p(\cdot)$ and $q(\cdot)$ such that*

1. *$|D_\kappa| + |D'_\kappa| \le p(\kappa)$;*
2. *f_κ is computable on a deterministic Turing machine in time at most $q(\kappa)$.*

A *reactive* functionality $\mathcal{F}$ can be described as a sequence of SFEs $\mathcal{F}_1 \circ \mathcal{F}_2 \circ \cdots \circ \mathcal{F}_m$ which might share a joint state.We call $\mathcal{F}$ deterministic finite reactive, if each of these $\mathcal{F}_i$'s is deterministic and finite.

Finally, we denote $\mathcal{U} := \{\mathcal{F} : \mathcal{F}$ is a deterministic finite SFE or reactive functionality$\}$ be the collection of finite deterministic two-party functionalities. Then define $\mathcal{U}^- = \{\mathcal{F} | \mathcal{F} \in \mathcal{U} \wedge (\mathcal{F}_{\mathtt{2CC}} \sqsubseteq^{\text{CSTAT}} \mathcal{F} \vee \mathcal{F}_{\mathtt{CC}} \not\sqsubseteq^{\text{CSTAT}} \mathcal{F})\}$.

B.5 Ideal Functionalities

We introduce several classical two-party functionalities used in the paper.

Secure Function Evaluation, $\mathcal{F}_{\mathtt{SFE}}$. A secure function evaluation (SFE) functionality $\mathcal{F}_{\mathtt{SFE}}$ is specified by a pair of functions (f_A, f_B) over a finite input domain $X \times Y$; Please see a formal definition of the functionality below:

Functionality $\mathcal{F}_{\mathtt{SFE}}$

The functionality interacts with players Alice and Bob, and is parameterized with functions (f_A, f_B) over a finite input domain $X \times Y$.

- Upon receiving input $x \in X$ from Alice and input $y \in Y$ from Bob, return delayed output $f_A(x, y)$ to Alice and delayed output $f_B(x, y)$ to Bob.

We say that the functionality is symmetric SFE (SSFE) if $f_A = f_B$.

Oblivious transfer $\mathcal{F}_{\mathtt{OT}}$. There are many equivalent variants of oblivious transfer[13]. In this paper we use the standard 1-out-of-2 oblivious bit transfer, defined as follows:

[13]There is an interesting story about the invention of OT. Arguably, Wiesner was the first to propose (in disguised form) 1-out-of-2 OT in his notion of "quantum multiplexing" channel, which would allow one party to send two messages to messages to another in a way that the receiver can choose which message to process and the other one will be destroyed automatically. Michael Rabin independently introduced his original concept about ten years later [Rab81], which is more widely recognized by the theoretical computer science community and found great significance is cryptography. See [Bra06] for a vivid story.

Functionality $\mathcal{F}_{\mathtt{OT}}$

The functionality is parameterized by players Alice and Bob.

- Upon receiving input $(x_0, x_1) \in \{0,1\}^2$ from Alice, and input $b \in \{0,1\}$ from Bob, return delayed output x_b to Bob, and delayed output (receipt) to Alice.

Commitment $\mathcal{F}_{\mathtt{COM}}$. $\mathcal{F}_{\mathtt{COM}}$ is a reactive functionality including two stages, the committing stage and then an opening stage. Below we give a formal definition. $\mathcal{F}_{\mathtt{COM}}$ was shown impossible to achieve in classic UC plain model by Canetti and Fischlin [CF01]. In this paper, we extend their impossibility result into quantum setting, and show $\mathcal{F}_{\mathtt{COM}}$ cannot be securely realized in quantum UC plain model.

Functionality $\mathcal{F}_{\mathtt{COM}}$

The functionality is parameterized by committer Alice and receiver Bob.

- Upon receiving input (commit, b) from Alice, where $b \in \{0,1\}$, internally record such b and send delayed output (receipt) to Bob.
- Upon receiving input (open) from Alice, if a bit b has been internally recorded, send delayed output (open, b) to Bob.

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

Functionality $\mathcal{F}_{\mathtt{XOR}}$

The functionality is parameterized by players Alice and Bob.

- Upon receiving input $b_A \in \{0,1\}$ from Alice, and input $b_B \in \{0,1\}$ from Bob, $y = b_A \oplus b_B$ and return delayed output y to both Alice and Bob.

Cut-and-Choose. First define 1-bit Cut-and-Choose functionality $\mathcal{F}_{\mathtt{1CC}}$. Bob inputs a bit b, 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 $b \cdot s_A$.

Functionality $\mathcal{F}_{\mathtt{1CC}}$

The functionality is parameterized by players Alice and Bob.

- Upon receiving input $s_A \in \{0,1\}$ from Alice, and input $b \in \{0,1\}$ from Bob; return delayed output s_A to Bob; return delayed output b to Alice if $s_A = 1$; otherwise return delayed output $\perp$ to Alice if $s_A = 0$.

Similarly, we can define 2-bit Cut-and-Choose functionality $\mathcal{F}_{\mathtt{2CC}}$ as follows:

Functionality $\mathcal{F}_{\mathtt{2CC}}$

The functionality is parameterized by players Alice and Bob.

- Upon receiving input $s_A \in \{0,1\}$ from Alice, and input a 2-bit string $b \in \{0,1\}^2$ from Bob; return delayed output s_A to Bob; return delayed output b to Alice if $s_A = 1$; otherwise return delayed output $\perp$ to Alice if $s_A = 0$.

Coin Tossing $\mathcal{F}_{\mathtt{COIN}}$. Blum [Blu82] first showed how to flip a coin over phone line. A formal definition of coin tossing functionality can be found as follows:

Functionality $\mathcal{F}_{\mathtt{COIN}}$

The functionality is parameterized by players Alice and Bob.

- Upon receiving input (request) from both Alice and Bob, randomly choose a fair coin $r \in \{0,1\}$ and send delayed output r to both Alice and Bob.

Secure channel and authenticated channel. In [Can05], generic communication channel, secure message transmission functionality $\mathcal{F}_{\mathtt{SMT}}$ is presented. Here we present secure channel $\mathcal{F}_{\mathtt{SEC}}$ and authenticated channel $\mathcal{F}_{\mathtt{AUTH}}$, which can be viewed as special instantiations of $\mathcal{F}_{\mathtt{SMT}}$.

Functionality $\mathcal{F}_{\mathtt{SEC}}$

The functionality is parameterized by players Alice and Bob, and a length function $l : \{0,1\}^* \to \{0,1\}^*$.

- Upon receiving an input (send, x) from party Alice, send $(\mathsf{sent}, l(x))$ to the adversary, and issue a *private* delayed output (sent, x) for Bob.

Functionality $\mathcal{F}_{\mathtt{AUTH}}$

The functionality is parameterized by Alice and Bob.

- Upon receiving an input (send, x) from Alice, issue a *public* delayed output (sent, x) to Bob.

Simultaneous exchange channel. This is a secure and fair bidirectional (bit-)channel, i.e., Alice and Bob can send each other bits which are delivered in a fair-manner, i.e., any of the parties receives the the other party's bit only after inputting his own bit into the channel.

Functionality $\mathcal{F}_{\mathtt{EXCH}}$

The functionality is parameterized by Alice and Bob.

- Upon receiving input $b_A \in \{0,1\}$ from Alice, and input $b_B \in \{0,1\}$ from Bob, return delayed outputs $y_A = b_B$ to Alice and $y_B = b_A$ to Bob.

C Complementary Material For Section 3

C.1 Computational Completeness of $\mathcal{F}_{\mathtt{COIN}}$ [HSS11]

Here we state the result, which is implicit but immediate from [HSS11], that under proper computational assumptions, $\mathcal{F}_{\mathtt{COIN}}$ suffices to realize all well-formed functionalities. We first specify the computational assumptions needed in [HSS11].

Assumption 23. *There exists a classical pseudorandom generator secure against quantum distinguishers.*

Assumption 24. *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.*

Theorem 25 ([HSS11, Theorem 4])**.** *Let $\mathcal{F}$ be a well-formed two-party functionality. Under Assumptions 23 and 24, there exists a nontrivial classical protocol that UC-emulates $\mathcal{F}$ in the $\mathcal{F}_{\mathtt{ZK}}$-hybrid model in the presence of polynomial-time malicious, static* quantum *adversaries.*

Theorem 26 ([HSS11, Prop.8, Part 1])**.** *Under Assumption 23, there is a constant-round protocol $\pi^{\mathcal{F}_{\mathtt{ZK}}}$ that quantum UC-emulates $\mathcal{F}_{\mathtt{COIN}}$ in the $\mathcal{F}_{\mathtt{ZK}}$-hybrid model.*

Then by Unruh's quantum universal composition theorem, Theorem 19, we get

Theorem 27. *Let $\mathcal{F}$ be a well-formed two-party functionality. Under Assumptions 23 and 24, there exists a nontrivial classical protocol that UC-emulates $\mathcal{F}$ in the $\mathcal{F}_{\mathtt{COIN}}$-hybrid model in the presence of polynomial-time malicious, static* quantum *adversaries.*

C.2 Proof of Lemma 5

Proof (sketch). In [HSS11] it was shown that under the assumptions of the lemma there exists a quantum protocol which statically computationally quantum-UC realizes any well-formed functionality in the $\mathcal{F}_{\mathtt{COIN}}$-hybrid model. Hence to prove the lemma it suffices the to provide an $\mathcal{F}_{\mathtt{XOR}}$-hybrid protocol which computationally quantum-UC realizes $\mathcal{F}_{\mathtt{COIN}}$ (the statement of the lemma follows then by the quantum universal composition theorem [Unr10]. To this direction we observe that the following trivial (classical) $\mathcal{F}_{\mathtt{XOR}}$-hybrid protocol $\pi^{\mathcal{F}_{\mathtt{XOR}}}$ statistically (classic) UC realizes $\mathcal{F}_{\mathtt{COIN}}$: 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 XOR. It is straight-forward to verify that $\pi^{\mathcal{F}_{\mathtt{XOR}}}$ statistically UC realizes the coin-flip functionality $\mathcal{F}_{\mathtt{COIN}}$. By using the quantum lifting theorem, we deduce that $\pi^{\mathcal{F}_{\mathtt{XOR}}}$ also statistically quantum-UC realizes $\mathcal{F}_{\mathtt{COIN}}$, which in terms implies that $\pi^{\mathcal{F}_{\mathtt{XOR}}}$ computationally quantum-UC realizes $\mathcal{F}_{\mathtt{COIN}}$. □

D Security Proof of Protocol $\Pi_{\mathtt{QOT}}$

Notation

- Alphabet $\Sigma = \{0,1\}$
- Hamming weight $wt(\cdot)$: $wt(x) :=$ number of 1s in $x \in \{0,1\}^*$
- Relative Hamming weight $w(\cdot)$: $w(x) := \frac{wt(x)}{|x|}$, where $|x|$ is the length of x.
- Index set $I \subseteq [n]$, where $[n] := \{1, \ldots, n\}$
- Complement of a string $t \in \{0,1\}^n$: $\bar{t} = \bar{t}_1 \ldots \bar{t}_n$, i.e., bit-wise flip.
- Restriction of $x \in \{0,1\}^n$ to a substring w.r.t. an index set $I \subseteq [n]$: $x|_I := x_{i_1} \ldots x_{i_k}$, with $i_j \in I$
- Restriction of $x \in \{0,1\}^n$ to a substring w.r.t. a string $t \in \{0,1\}^n$: $x_t := x_{i_1} \ldots x_{i_k}$, with $t_{i_j} = 1$.
- Computational basis $+$: identified with 0.
- Hadamard basis $\times$: identified with 1.
- Trace distance $D(\cdot,\cdot)$: $D(\rho,\sigma) := \frac{1}{2}\mathrm{tr}\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}$

We show how to construct an ideal-world simulator $\mathcal{S}$ for an adversary corrupting Alice or Bob respectively in the quantum UC model.

D.1 Corrupted Alice

Intuitively, security against corrupted Alice requires that Alice should not be able to figure out Bob's chosen bit c. This is conceivable, noting that Alice does not learn anything about the bases Bob used for the unchecked qubits. This is because at these positions, Alice inputs $b_i = 0$ to $\mathcal{F}_{\mathtt{2CC}}$ and hence always gets output $\perp$ from $\mathcal{F}_{\mathtt{2CC}}$. Therefore, from Alice's view, the index sets I_0 and I_1 received from Bob will be a random partition. Formally, we need to construct a simulator $\mathcal{S}$ in the ideal world who produces a transcript indistinguishable from that in the real protocol, without knowing the chosen bit of (honest) Bob. One main task $\mathcal{S}$ needs to accomplish is extracting two secret strings (s_0, s_1) from corrupted Alice, so that $\mathcal{S}$ could feed them to the external $\mathcal{F}_{\mathtt{OT}}$ functionality. The idea is that $\mathcal{S}$ can "cheat" in the checking phase by only measuring the qubits that the adversary asks to. $\mathcal{S}$ can do so without being caught , and thus not disturbing the transcript (also adversary's view), because in the ideal world, $\mathcal{F}_{\mathtt{2CC}}$ is simulated internally by $\mathcal{S}$ and he thus sees the checking bit b_i that corrupted Alice sends to $\mathcal{F}_{\mathtt{2CC}}$ and can decide afterwards whether it is necessary to respond to Alice honestly. As a result, once $\mathcal{S}$ receives the bases $\hat{\theta}^A$ after the checking phase, he can measure the remaining qubits in $\hat{\theta}^A$ and thus know all of $\hat{x}^A$. This allows him to recover both s_0 and s_1 from $m_i = s_i \oplus f(\hat{x}^A|_{I_i})$.

Simulating corrupted Alice. Given adversary $\mathcal{A}$ that corrupts Alice, we construct a simulator $\mathcal{S}$ as follows.

Proposition 28. *For any unbounded $\mathcal{Z}$, $\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \Pi_{\mathtt{QOT}}] = \mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, \mathcal{F}_{\mathtt{OT}}]$, and $\mathcal{S}$ runs in polynomial of the running time of $\mathcal{A}$.*

The proof is straightforward and follows the very same lines as in the standard protocol for quantum OT from commitment. We omit the formal proof.

Simulator $\mathcal{S}$ (when Alice is corrupted)

Inputs: Environment $\mathcal{Z}$ generates inputs: chosen bit c is given to honest (dummy) Bob; and input to $\mathcal{A}$ is passed through $\mathcal{S}$.

1. (Initialization) $\mathcal{S}$ behaves as an honest Bob does in the real protocol $\Pi_{\mathtt{QOT}}$.
2. (Checking)

   2.1 For $i = 1, \ldots n$ the following steps are executed *sequentially*:
   - (a) $\mathcal{S}$ internally simulates $\mathcal{F}_{\mathtt{2CC}}$, so when $\mathcal{A}$ inputs b_i to $\mathcal{F}_{\mathtt{2CC}}$, $\mathcal{S}$ records it.
   - (b) If $b_i = 0$, $\mathcal{S}$ sends $\perp$ to $\mathcal{A}$.
   - (c) If $b_i = 1$, $\mathcal{S}$ measures the i^{th} qubit in a randomly chosen basis $\tilde{\theta}_i^B \in_R \{+, \times\}$ and send both $\tilde{\theta}_i^B$ and the outcome $\tilde{x}_i^B$ to $\mathcal{A}$.

   2.2 $\mathcal{S}$ aborts if any time $\mathcal{A}$ aborts or $\mathcal{S}$ sees more that $3n/5$ i with $b_i = 1$.
3. (Partition Index Set) Let $\hat{\theta}^A$ be the basis received from $\mathcal{A}$. $\mathcal{S}$ measures the remaining qubits under θ^A, and obtains $\hat{x}^B$. $\mathcal{S}$ then randomly partitions the indices into I_0 and I_1 and sends them to $\mathcal{A}$.
4. (Secret Transferring) Once receiving (f, m_0, m_1), $\mathcal{S}$ computes $s'_0 := m_0 \oplus f(\hat{x}^B|_{I_0})$ and $s'_1 := m_1 \oplus f(\hat{x}^B|_{I_1})$. $\mathcal{S}$ gives $\mathcal{F}_{\mathtt{OT}}$ the pair (s'_0, s'_1). Outputs whatever $\mathcal{A}$ outputs in the end.

Figure 3: Simulating corrupted Alice.

D.2 Corrupted Bob

The case that Bob is corrupted is much more challenging. Basically, we want to prevent a malicious Bob from learning s_{1-c} in addition to his chosen secret s_c. We know that s_{1-c} is masked by $f(\hat{x}^A|_{I_{1-c}})$, to ensure that Bob learns nothing about s_{1-c}, it thus suffices to show that $f(\hat{x}^A|_{I_{1-c}})$ is close to uniformly random, or equivalently, due to privacy amplification (cf. [Ren05, RK05]) that $\hat{x}^A|_{I_{1-c}}$ has sufficient min-entropy even conditioned on Bob's view in the protocol.

In order to derive such a claim, we first describe an variant[14] $\Pi_{\mathtt{QOT}}^{\mathtt{EPR}}$ of $\Pi_{\mathtt{QOT}}$, which is based on EPR-pairs and is equivalent to $\Pi_{\mathtt{QOT}}$ from Bob's perspective. It then allows us to adapt a sampling framework proposed by Bouman and Fehr [BF10] to argue about a lower bound on the min-entropy we are interested in. The high-level approach is:

- Interpret the checking phase in $\Pi_{\mathtt{QOT}}^{\mathtt{EPR}}$ as a sampling game (to be defined shortly) over qubits.
- Analysis of the sampling game will imply that if Bob passes the checking phase, then the *real* joint state of Alice and Bob after the checking phase in the protocol will be negligibly close to an *ideal* state.
- Finally we argue that if one measured Alice's system in the *ideal* state and gets a string x, then no matter how Bob partitions the index sets (I_0, I_1), there exists a c such that high amount of min-entropy is preserved in $x|_{I_{1-c}}$.

Thus we see that if Bob indeed passes the checking phase in the real protocol, $f(\hat{x}^A|_{I_{1-c}})$ will be statistically close to uniform, except with negligible probability.

[14] This is a standard proof trick in the literature used in proving BB84-type quantum cryptographic protocols, dating back to [SP00].

However, the sampling framework in [BF10] is not immediately applicable in our setting because it seems to be specific to a *static* sampling scenario, where the classical string or quantum state is fixed before the sampling starts. Our checking phase, using $\mathcal{F}_{\mathtt{2CC}}$ in sequential, resembles an adaptive-type sampling, where data are coming in an on-line fashion, and in particular could be generated adaptively based on the information about which previous data have been chosen as samples. To cope with this, we generalize their framework to capture an adaptive sampling setting, and subsumes most of their results as a special case. This extension may be useful independently in other applications. is an upper bound on the classical error probability of the sampling strategy buried in our checking phase of the protocol $\Pi_{\mathtt{QOT}}$[15].

We now describe the EPR-based protocol $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$ in Fig. 4; note that Bob's actions are as in $\Pi_{\mathtt{QOT}}$ and thus omitted in the description of $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$. Also recall that $\hat{\theta}^A$ denotes the restriction of $\tilde{\theta}^A$ to those positions with $b_i = 0$.

Protocol $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$

Inputs: Alice gets input two ℓ-bit strings s_0 and s_1, Bob gets a bit c.

1. (Initialization) Alice generates n pairs of EPR $|\Psi\rangle^{\otimes n} = [\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)]^{\otimes n}$, and sends Bob n halves of these EPR pairs. Alice chooses $\tilde{\theta}^A \in \{+, \times\}^n$ at random, but doesn't measure her shares of the EPR pairs.
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 call $\mathcal{F}_{\mathtt{2CC}}$ with inputs b_i and $(\tilde{x}^B_i, \tilde{\theta}^B_i)$, respectively.
   - 2.2 For every $i \in \{1, \ldots, n\}$ with $b_i = 1$, Alice measures her qubit of the i-th EPR pair in basis $\tilde{\theta}^B_i$ (not $\tilde{\theta}^A_i$) to obtain bit $\tilde{x}^A_i$. If $\tilde{x}^A_i \neq \tilde{x}^B_i$ for some i with $b_i = 1$ and $\tilde{\theta}^A_i = \tilde{\theta}^B_i$, then Alice aborts. If not, then Alice continues and measures her remaining qubits under $\hat{\theta}^A$ to obtain $\hat{x}^A$.
3. (Partition Index Set) Same as $\Pi_{\mathtt{QOT}}$.
4. (Secret Transferring) Same as $\Pi_{\mathtt{QOT}}$.

Figure 4: Protocol $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$ for OT

Claim 5. *$\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$ and $\Pi_{\mathtt{QOT}}$ are equivalent from Bob's view, i.e., $\Pi_{\mathtt{QOT}}$ is quantum-UC secure against malicious Bob if and only if $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$ is.*

Proof. Note that if Alice were to measure her EPR halves in random bases $\tilde{\theta}^A$ right after step 1, it's equivalent to encoding a random n-bit string into n qubits under random bases, and that is what happens in $\Pi_{\mathtt{QOT}}$. But Alice's measuring operations commute with Bob's operations up to step 2.2, since they operate on different spaces. Therefore, from Bob's perspective there is no effect of postponing Alice's measurements to step 2.2. Then the only difference left is that Alice measures all those where $b_i = 1$ and $\tilde{\theta}^A_i \neq \tilde{\theta}^B_i$ under $\tilde{\theta}^B_i$, whereas in $\Pi_{\mathtt{QOT}}$ she measures them in $\tilde{\theta}^A_i$. However,

[15] Actually, the analysis will be applied on an equivalent (From Bob's perspective) protocol $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$. See the proof below.

these qubits are not used anyway, and they are discarded thereafter. Hence Bob will not notice any difference. □

As a result, it suffices that we show how to simulate an arbitrary adversary $\mathcal{A}$ that corrupts Bob in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$, which comes next.

Simulating corrupted Bob. Given adversary $\mathcal{A}$ in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$ that corrupts Bob, we construct a simulator $\mathcal{S}$ as follows.

Simulator $\mathcal{S}$ (when Bob is corrupted)

Inputs: Environment $\mathcal{Z}$ generates inputs: s_0 and s_1 are given to honest (dummy) Alice; and input to $\mathcal{A}$ is passed through $\mathcal{S}$.

1. (Initialization) $\mathcal{S}$ initializes an execution with corrupted Bob, just as in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$.
2. (Checking) $\mathcal{S}$ does the checking procedure as in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$. Note that in the present situation, $\mathcal{S}$ simulates each $\mathcal{F}_{\mathtt{2CC}}$ internally, and thus he sees all $(\tilde{x}^B_i, \tilde{\theta}^B_i)$ that corrupted Bob sent to $\mathcal{F}_{\mathtt{2CC}}$.
3. (Partition Index Set) $\mathcal{S}$ expects to receive (I_0, I_1) from $\mathcal{A}$.
4. (Secret Transferring) Alice sends (s_0, s_1) to the ideal functionality $\mathcal{F}_{\mathtt{OT}}$. $\mathcal{S}$ sets $c \in \{0,1\}$ to be such that $wt(\hat{\theta}^A|_{I_c} \oplus \hat{\theta}^B|_{I_c}) \leq wt(\hat{\theta}^A|_{I_{1-c}} \oplus \hat{\theta}^B|_{I_{1-c}})$. (That is, the Hamming distance between $\hat{\theta}^A$ and $\hat{\theta}^B$, restricted to I_{1-c}, is larger.) Send c to the (external) $\mathcal{F}_{\mathtt{OT}}$ and obtain s_c. $\mathcal{S}$ then sends $f \in_R \mathbf{F}$, $m_c := s_c \oplus f(x^A|_{I_c})$ and $m_{1-c} \in_R \{0,1\}^\ell$ to $\mathcal{A}$. Output whatever $\mathcal{A}$ outputs in the end.

Figure 5: Simulating corrupted Bob in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$

Proposition 29. *For any unbounded $\mathcal{Z}$ and $\mathcal{A}$ corrupting Bob, $\mathsf{EXEC}[\mathcal{Z}, \mathcal{A}, \Pi^{\mathtt{EPR}}_{\mathtt{QOT}}] \approx \mathsf{EXEC}[\mathcal{Z}, \mathcal{S}, \mathcal{F}_{\mathtt{OT}}]$, and $\mathcal{S}$ runs in polynomial of the running time of $\mathcal{A}$.*

Proof. Observe that the simulation of $\mathcal{S}$ differs from the real-world execution only in the last *secret transferring* phase: in both cases $m_c = s_c \oplus f(\hat{x}^A|_{I_c})$, but $m_{1-c} = s_{1-c} \oplus f(\hat{x}^A|_{I_{1-c}})$ in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$, while during simulation $\mathcal{S}$ sets $m_{1-c} \in_R \{0,1\}^\ell$. However, as we will argue formally in Theorem 30, after checking phase, Alice's system A restricted to I_{1-c} has high min-entropy even conditioned on the adversary's view. Hence f will effectively extract ℓ uniformly random bits. □

Theorem 30. *If $\ell = \lambda n$, where λ is a constant strictly smaller than $\frac{1}{8}$, then the following holds. Let M_0 and M_1 be the two message systems generated by Alice in $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$. Then, there exists $c \in \{0,1\}$ such that M_{1-c} is close to uniformly random and independent of Bob's view:*

$$D(\rho_{M_{1-c}M_cB}, \frac{1}{2^\ell}\mathbb{I} \otimes \sigma_{M_cB}) \leq negl(n) \ .$$

Proving Theorem 30 is the most technically challenging part of our paper. In the following sections, we will develop the technical tools and give a proof.

D.2.1 An Adaptive Sampling Framework

In this section, we introduce an *adaptive* version of the (classical and quantum) sampling framework of [BF10]. This will give us the right tool to prove security of our OT protocol based on the $\mathcal{F}_{\mathsf{2cc}}$ functionality.

In the (non-adaptive) sampling framework from [BF10], the goal is to estimate the Hamming distance of a fixed but unknown string x (over the binary or some other finite alphabet) to a fixed and known reference string $\hat{x}$ by sampling and "looking" at a few randomly chosen positions of x.[16] Actually, for technical reasons, the goal is to estimate the Hamming distance of the *remainders* of the strings x and $\hat{x}$, when the sampled positions are removed. For later convenience, it is useful to think of x and $\hat{x}$ being chosen by a party Bob in an arbitrary way, and the sampling being performed by some other party Alice. In the quantum version, the string x is replaced by an n-qubit (or qudit) state A, and the sampling is done by sampling and *measuring* a few randomly chosen positions of A, using a fixed reference basis $\hat{\theta}$. As shown in [BF10], if the observed sample is close to $\hat{x}$ (in the sampled positions), then the state of the remaining qubits is close to a superposition of strings (encoded into quantum states) with small Hamming distance to $\hat{x}$ (on the unsampled positions). Furthermore, the error is related to the error probability of the corresponding classical sampling procedure.

We extend these results to an adaptive setting, where x and $\hat{x}$ are chosen in an adaptive way: position by position, Bob fixes x_i and $\hat{x}_i$ and Alice announces whether she chooses the position i as part of the sample or not. Hence, Bob can choose x_i and $\hat{x}_i$ depending on which previous positions Alice chose. For the quantum version, Bob still has to fix the state in advance, but he can choose $\hat{\theta}$ and $\hat{x}$ adaptively, position by position.

We now make this formal, and we show that the results of [BF10] still hold in this adaptive setting. Let $n \in \mathbb{N}$ be a positive integer and Σ be a finite alphabet. A sampling strategy is specified by the distribution according to which Alice chooses the sample, and the (possibly randomized) function that she uses to process the sample.

Definition 31. *(Sampling Strategy). A sampling strategy Ψ consists of a triple (P_T, P_S, f), where P_T is a distribution over $\{0,1\}^n$, P_S is a distribution over an arbitrary finite set $\mathcal{S}$, and f is a function $f : \Sigma^* \times \{0,1\}^n \times \mathcal{S} \to \mathbb{R}$.*

This definition coincides with the definition in [BF10]; the adaptivity comes into the picture when defining the *error probability*, which captures how well a sampling strategy performs when applied to an adaptive or a non-adaptive setting. Although our results hold more generally, in the remainder we restrict to the binary setting where $\Sigma = \{0,1\}$.

Informally, a sampling strategy $\Psi = (P_T, P_S, f)$ is to be interpreted in that Alice chooses $t \in \{0,1\}^n$ according to P_T, "looks" at the positions x_i of x with $t_i = 1$, and computes $f(x_t \oplus \hat{x}_t, t, s)$ as estimate for the relative Hamming weight $w(x_{\bar{t}} \oplus \hat{x}_{\bar{t}})$, where s is chosen according to P_S, and x_t stands for the restriction of x to those positions with $t_i = 1$ (and correspondingly for $\hat{x}_t, x_{\bar{t}}$ etc.). A canonical example sampling strategy is as follows.

Example 1. P_T is the uniform distribution over $\{0,1\}^n$, $\mathcal{S}$ is empty, and $f(x_t \oplus \hat{x}_t, t) = w(x_t \oplus \hat{x}_t)$, i.e., Alice samples a random subset and computes the relative Hamming distance within the sample.

A less canonical example, but one that is important for us, is as follows.

Example 2. As above, Alice samples a random subset, but then she computes her estimate for $w(x_{\bar{t}} \oplus \hat{x}_{\bar{t}})$ as $f(x_t \oplus \hat{x}_t, t, s) = w(x_s \oplus \hat{x}_s)$ for a random $s \in \{0,1\}^n$ subject to $t_i = 0 \Rightarrow s_i = 0$. In other words, she only uses a random subset of the random sample to compute the estimate.

[16] Without loss of generality, $\hat{x}$ is set to the all-0 string in [BF10].

In order to define the error probability of a given sampling strategy $\Psi = (P_T, P_S, f)$ in the adaptive setting, we consider the following adaptive sampling game, given in Figure 7, that is associated to Ψ. The game should be understood in that Bob may choose each pair $(x_i, \hat{x}_i)$ in an arbitrary and adaptive way, depending on what he has seen so far, and Alice only "looks" at those positions where $t_i = 1$, and computes her estimate based on those positions.

Adaptive Sampling Game $\mathcal{G}$

1. Alice chooses $t \in \{0,1\}^n$ according to P_T, and $s \in \mathcal{S}$ according to P_S.
2. For $i = 1, \ldots n$ the following steps are executed *sequentially*:
   (a) Bob generates and sends to Alice $x_i, \hat{x}_i \in \Sigma^n$.
   (b) Alice sends t_i to Bob.
3. Alice outputs $\mu_{t,s} := f(x_t \oplus \hat{x}_t, t, s)$.

Figure 6: Adaptive sampling game.

We point out once more that the difference to the non-adaptive sampling game considered in [BF10] is that in the non-adaptive case, Bob has to provide all x_i and $\hat{x}_i$'s *in advance*, before (or without) learning t. Additionally, [BF10] assumes without loss of generality that $\hat{x}_i = 0$; this, we could do here as well, but here we do not.

Intuitively, a sampling strategy Ψ is "good" if in the above adaptive sampling game, $\mu_{t,s} = f(x_t \oplus \hat{x}_t, t, s)$ provides a good estimate of $w(x_{\bar{t}} \oplus \hat{x}_{\bar{t}})$, the relative Hamming distance between $x_{\bar{t}}$ and $\hat{x}_{\bar{t}}$. We now make this precise. For a given sampling strategy Ψ, and for any $\hat{x} \in \Sigma^n$, $t \in \{0,1\}^n$, $s \in \mathcal{S}$ and $\delta > 0$, we define the set

$$B^{\delta}_{t,s,\hat{x}}(\Psi) := \{x \in \Sigma^n : |w(x_{\bar{t}} \oplus \hat{x}_{\bar{t}}) - f(x_t \oplus \hat{x}_t, t, s)| < \delta\}.$$

$B^{\delta}_{t,s,\hat{x}}(\Psi)$ consists of all the strings x for which Alice's estimate is δ-close to being accurate in case she samples t and s and Bob provides the reference string $\hat{x}$. If Ψ is clear from the context, we may simply write $B^{\delta}_{t,s,\hat{x}}$.

Note that for any fixed strategy $\mathcal{B}$ for Bob in the adaptive sampling game, the random variables T, S, X and $\hat{X}$ that describe the choices of t, s, x and $\hat{x}$ in the adaptive sampling game are well defined, and so is the random variable $B^{\delta}_{T,S,\hat{X}}(\Psi)$, which takes on sets as values. The adaptive error probability of a sampling strategy Ψ is defined as the maximal probability that X lies outside the set $B^{\delta}_{T,S,\hat{X}}$, i.e., that Alice's estimate is far off, maximized over the possible strategies of Bob.

Definition 32 (Classical adaptive error probability)**.** *The* classical adaptive probability *of a sampling strategy $\Psi = (P_T, P_S, f)$ is defined as*

$$\bar{\varepsilon}^{\delta}_{c}(\Psi) := \max_{\mathcal{B}} \Pr[X \notin B^{\delta}_{T,S,\hat{X}}(\Psi)]$$

parameterized by $0 < \delta < 1$, where the max is over all strategies $\mathcal{B}$ for Bob.

Note that the randomness is over the choices of T and S, and the (adaptive) choices of X and $\hat{X}$, specified by the strategy $\mathcal{B}$.

We now extend our study to sampling of quantum states. We define a quantum sampling game as follows.

Following [BF10], we want to understand what can be concluded on the state of the unmeasured qubits from the estimate $\mu_{t,s}$. For this, for a given strategy $\mathcal{B}$ for Bob, let $|\phi^{t,s,\hat{x},\hat{\theta}}_{AE}\rangle$ be the state of

Quantum Adaptive Sampling Game $\mathcal{G}_q$

1. Bob prepares an arbitrary state $|\phi_{AE}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E$, where A consists of n qubits and E is arbitrary, and sends A to Alice. Alice chooses $t \in \{0,1\}^n$ according to P_T, and $s \in \mathcal{S}$ according to P_S.
2. For $i = 1, \ldots n$ the following steps are executed *sequentially*:
   (a) Bob generates (possibly by processing E) $\hat{\theta}_i, \hat{x}_i \in \Sigma$, and sends them to Alice.
   (b) Alice sends t_i to Bob.
3. For every i with $t_i = 1$, Alice measures the i-th qubit of A in basis $\hat{\theta}_i$ to obtain x_i, and she outputs $\mu_{t,s} := f(x_t \oplus \hat{x}_t, t, s)$.

Figure 7: Quantum adaptive sampling game.

the joint system AE right before step 3. Also taking into account the randomized classical data $t, s, \hat{x}, \hat{\theta}$, we can describe the joint state before step 3 by means of the density matrix

$$\rho_{TS\hat{X}\hat{\Theta}AE} = \sum_{t,s} P_{TS\hat{X}\hat{\Theta}AE}(t,s,\hat{x},\hat{\theta}) |t,s,\hat{x},\hat{\theta}\rangle\langle t,s,\hat{x},\hat{\theta}| \otimes |\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle\langle\phi_{AE}^{t,s,\hat{x},\hat{\theta}}|$$

Note that in the non-adaptive setting [BF10], $\hat{X}$ and $\hat{\Theta}$ are *fixed* (without loss of generality to all 0's, both), and systems TS and AE are *independent*. Here, due to the adaptive sampling game, $\hat{X}$ and $\hat{\Theta}$ may be randomized as well, and there may be some dependency between TS and AE.

We compare the above *real* state $\rho_{TS\hat{X}\hat{\Theta}AE}$ with an *ideal* state, which is a state of the form

$$\tilde{\rho}_{TS\hat{X}\hat{\Theta}AE} = \sum_{t,s} P_{TS\hat{X}\hat{\Theta}AE}(t,s,\hat{x},\hat{\theta}) |t,s,\hat{x},\hat{\theta}\rangle\langle t,s,\hat{x},\hat{\theta}| \otimes |\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle\langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}|$$

with

$$|\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle \in \mathrm{span}_{\hat{\theta}}(B^{\delta}_{t,s,\hat{x}}) \otimes \mathcal{H}_E$$

for all $t, s, \hat{x}$ and $\hat{\theta}$, where

$$\mathrm{span}_{\hat{\theta}}(B^{\delta}_{t,s,\hat{x}}) := \mathrm{span}\{|x\rangle_{\hat{\theta}} : x \in B^{\delta}_{t,s,\hat{x}}\} = \mathrm{span}\{|x\rangle_{\hat{\theta}} : |w(x_{\bar{t}} \oplus \hat{x}_{\bar{t}}) - f(x_t \oplus \hat{x}_t, t, s)| < \delta\},$$

and where $|x\rangle_\theta$ means each bit x_i in x is encoded in basis θ_i.

Essentially by definition of the ideal state, if step 3 of the quantum adaptive sampling game is done on the ideal rather than the real state, then the resulting state $\tilde{\rho}_{TS\hat{X}\hat{\Theta}X_T A_{\overline{T}}E}$ after Alice has measured the qubits with $t_i = 1$ satisfies

$$\tilde{\rho}_{A_{\overline{T}}E|T=t,S=s,\hat{X}=\hat{x},\hat{\Theta}=\hat{\theta},X_T=x_t} = |\tilde{\phi}_{A_{\bar{t}}E}^{t,s,\hat{x},\hat{\theta},x_t}\rangle\langle\tilde{\phi}_{A_{\bar{t}}E}^{t,s,\hat{x},\hat{\theta},x_t}|$$

with $|\tilde{\phi}_{A_{\bar{t}}E}\rangle$ (where we leave the dependency of the state on t, s etc. implicit) of the form

$$|\tilde{\phi}_{A_{\bar{t}}E}\rangle = \sum_y \alpha_y |y\rangle_{\hat{\theta}} |\tilde{\phi}_E^y\rangle$$

where the sum is over all $y \in \{0,1\}^{wt(\bar{t})}$ with relative Hamming distance to $\hat{x}_{\bar{t}}$ at most δ-away from $\mu_{s,t} = f(x_t \oplus \hat{x}_t, t, s)$. In other words, it is a superposition over a "small" number of sets if $\mu_{s,t}$ is close or equal to 0 (as will be the case in the analysis of $\Pi_{\mathtt{QOT}}$)

Definition 33 (Quantum adaptive error probability)**.** *The* quantum adaptive error probability *of a sampling strategy* $\Psi = (P_T, P_S, f)$ *is defined as*

$$\bar{\varepsilon}_q^\delta(\Psi) = \max_{\mathcal{B}_q} \min_{\tilde{\rho}_{TS\hat{X}\hat{\Theta}AE}} D(\rho_{TS\hat{X}\hat{\Theta}AE}, \tilde{\rho}_{TS\hat{X}\hat{\Theta}AE})$$

parameterized by $0 < \delta < 1$*. The max is over all possible strategies* $\mathcal{B}_q$ *for Bob, and the minimum is over all ideal states of the form as* $\tilde{\rho}_{TS\hat{X}\hat{\Theta}AE}$*.*

By definition, if the quantum error probability is small then the resulting quantum state of $\mathcal{G}_q$ will behave, except with probability at most $\bar{\varepsilon}_q^\delta$, as an ideal state in which the unmeasured part of system A is in a superposition over a small set of orthogonal states.

Similar to the non-adaptive case of [BF10], we show the following relation between $\bar{\varepsilon}_q^\delta$ and $\bar{\varepsilon}_c^\delta$, for any sampling strategy.

Proposition 34. *For any sampling strategy* Ψ *and for any* $0 < \delta < 1$, $\bar{\varepsilon}_q^\delta(\Psi) \leq \sqrt{\bar{\varepsilon}_c^\delta(\Psi)}$.

The proof makes use of the following simple fact. For any strategy $\mathcal{B}_q$ for Bob in the quantum sampling game $\mathcal{G}_q$, there exists an associated strategy $\mathcal{B}$ for Bob in the classical sampling game $\mathcal{G}$, where Bob chooses $|\phi_{AE}\rangle$ and the $\hat{\theta}_i$ and $\hat{x}_i$'s as in $\mathcal{B}_q$, but he keeps the qubits A, and instead of sending $\hat{\theta}_i$ in step i, he measures the i-th qubit of A in basis $\hat{\theta}_i$ and sends the measurement outcome x_i to Alice (along with $\hat{x}_i$).

Proof. We show that for any strategy for Bob resulting in the (real) state $\rho_{TS\hat{X}\hat{\Theta}AE}$, there exists a suitable ideal state $\tilde{\rho}_{TS\hat{X}\hat{\Theta}AE}$ with $D(\rho_{TS\hat{X}\hat{\Theta}AE}, \tilde{\rho}_{TS\hat{X}\hat{\Theta}AE}) \leq \sqrt{\bar{\varepsilon}_c^\delta}$. We construct $\tilde{\rho}_{TS\hat{X}\hat{\Theta}AE}$ as required, where the $|\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle$'s are defined by the following decomposition into orthogonal components: $|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle = \Pi_{t,s,\hat{x},\hat{\theta}}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle + \Pi_{t,s,\hat{x},\hat{\theta}}^\perp|\phi_{AE}^{t,s,\hat{x},\hat{\theta}\perp}\rangle = \langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle|\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle + \langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}\perp}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle|\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}\perp}\rangle$, where

$$\Pi_{t,s,\hat{x},\hat{\theta}} = \sum_{x \in B_{t,s,\hat{x}}^\varepsilon} |x\rangle\langle x|_{\hat{\theta}} \otimes I \qquad \text{and} \qquad \Pi_{t,s,\hat{x},\hat{\theta}}^\perp = \sum_{x \notin B_{t,s,\hat{x}}^\varepsilon} |x\rangle\langle x|_{\hat{\theta}} \otimes I$$

are the orthogonal projections into $\mathrm{span}_{\hat{\theta}}(B_{t,s,\hat{x}}^\varepsilon) \otimes \mathcal{H}_E$ and the orthogonal complement $\mathrm{span}_{\hat{\theta}}(B_{t,s,\hat{x}}^\varepsilon)^\perp \otimes \mathcal{H}_E$, and $|\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle$ and $|\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}\perp}\rangle$ are the renormalized projections of $|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle$.

Consider the random variable X that describes the measurement outcome if Alice was to measure *all* qubits of A in step 2. We stress that she only measures the ones pointed to by t, but we may still consider what happens if she measures all of them. Formally, we set

$$\Pr[X = x | T = t, S = s, \hat{X} = \hat{x}, \hat{\Theta} = \hat{\theta}] = \langle\phi_{AE}^{t,s,\hat{x},\hat{\theta}}|(|x\rangle\langle x|_{\hat{\theta}} \otimes I)|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle\,.$$

It holds that $\Pr[X \notin B_{T,S,\hat{X}}^\delta] \leq \bar{\varepsilon}_c^\delta$. This follows from the fact that it has no impact on the joint distribution of these random variables *who* computes the qubits A, and if we let Bob measure the qubits then this results in the associated strategy $\mathcal{B}$ for the *classical* sampling game, for which the above holds by definition of the error probability $\bar{\varepsilon}_c^\delta$. By this observation, it is sufficient to relate $D(\rho_{TS\hat{X}\hat{\Theta}AE}, \tilde{\rho}_{TS\hat{X}\hat{\Theta}AE})$ to $\Pr[X \notin B_{T,S,\hat{X}}^\delta]$, which we do below. First, using elementary properties

of the trace distance, we obtain that

$$\begin{aligned}
D\big(\rho_{TS\hat{X}\hat{\Theta}AE}, \tilde{\rho}_{TS\hat{X}\hat{\Theta}AE}\big) &= \sum_{t,s,\hat{x},\hat{\theta}} P_{TS\hat{X}\hat{\Theta}AE}(t,s,\hat{x},\hat{\theta}) D\big(|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle\langle\phi_{AE}^{t,s,\hat{x},\hat{\theta}}|, |\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle\langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}|\big) \\
&= \sum_{t,s,\hat{x},\hat{\theta}} P_{TS\hat{X}\hat{\Theta}AE}(t,s,\hat{x},\hat{\theta}) \sqrt{1 - |\langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}}|\varphi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle|^2} \\
&= \sum_{t,s,\hat{x},\hat{\theta}} P_{TS\hat{X}\hat{\Theta}AE}(t,s,\hat{x},\hat{\theta}) |\langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}\perp}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle| \\
&\leq \sqrt{\sum_{t,s,\hat{x},\hat{\theta}} P_{TS\hat{X}\hat{\Theta}AE}(t,s,\hat{x},\hat{\theta}) |\langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}\perp}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle|^2}\,,
\end{aligned}$$

where the last inequality follows from Jensen's inequality. But since

$$\begin{aligned}
|\langle\tilde{\phi}_{AE}^{t,s,\hat{x},\hat{\theta}\perp}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle|^2 = \langle\phi_{AE}^{t,s,\hat{x},\hat{\theta}}|\Pi^{\perp}_{t,s,\hat{x},\hat{\theta}}|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle &= \sum_{x\notin B^{\varepsilon}_{t,s,\hat{x}}} \langle\phi_{AE}^{t,s,\hat{x},\hat{\theta}}|(|x\rangle\langle x|_{\hat{\theta}}\otimes I)|\phi_{AE}^{t,s,\hat{x},\hat{\theta}}\rangle \\
&= \Pr[X\notin B^{\delta}_{t,s,\hat{x}} | T=t, S=s, \hat{X}=\hat{x}, \hat{\Theta}=\hat{\theta}]\,,
\end{aligned}$$

it follows that the term in the square root equals $\Pr[X \notin B^{\delta}_{T,S,\hat{X}}]$. This proves the claim. □

D.2.2 Completing the Security Proof of $\Pi_{\mathtt{QOT}}$

Proof of Theorem 30. Consider the joint state $|\phi_{AE}\rangle$ right before the checking phase of $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$, consisting of the n EPR pairs plus potentially some additional quantum system on Bob's side. The crucial observation now is that the checking phase of $\Pi^{\mathtt{EPR}}_{\mathtt{QOT}}$ follows exactly the lines of the adaptive quantum sampling game $\mathcal{G}_q$ in that Bob specifies $\hat{\theta}_i = \tilde{\theta}_i^B$ and $\hat{x}_i = \tilde{x}_i^B$ sequentially and adaptively, depending on the previous selection bits $t_i = b_i$'s, which determine whether Alice uses position i for checking or not.

It follows that for any constant $\delta > 0$, the real state, after Alice has measured the selected qubits, is ε-close to an ideal state that is a superposition over a small number of basis vectors with respect to the basis $\hat{\theta}^B$, in the sense as discussed in the previous section, with $\varepsilon \leq \bar{\varepsilon}_q(\Psi) \leq \sqrt{\bar{\varepsilon}_c^{\delta}(\Psi)}$, where Ψ is the sampling strategy from Example 2.

The remainder of the proof now goes along the lines of the commitment-based proof of QOT in [BF10]. We give it here for completeness. The resulting (ideal) state being a superposition over a small number of basis vectors with respect to the basis $\hat{\theta}^B$ still holds after Bob announces the sets I_0 and I_1, and it also still holds if we view the qubits A_{I_c} as part of the adversarial system E, where $c \in \{0,1\}$ is such that $wt(\hat{\theta}^A|_{I_c} \oplus \hat{\theta}^B|_{I_c}) \leq wt(\hat{\theta}^A|_{I_{1-c}} \oplus \hat{\theta}^B|_{I_{1-c}})$. Note that (by Hoeffding's inequality) except with probability $negl(n)$, the number of positions $i \in I_{1-c}$ with $\hat{\theta}_i^A \neq \hat{\theta}_i^B$ is at least $\frac{1}{2}(\frac{1}{4} - \delta)n$.

It follows from Fact 4 below that (for the ideal state)

$$\mathbf{H}_{min}(\hat{X}_{1-c}|A_{I_c}E) \geq \frac{1}{2}(\frac{1}{4} - \delta)n - h(\delta)n\,,$$

except with negligible probability, where $\hat{X}_{1-c} = \hat{X}^A|_{I_{1-c}}$ and the left hand side should be understood as conditioned on all the common classical information, $\hat{\theta}^A, \hat{\theta}^B$ etc. By basic properties of the min-entropy, the same bound also applies to $\mathbf{H}_{min}(\hat{X}_{1-c}|\hat{X}_c E)$. It then follows from privacy amplification [Ren05, RK05] that if $\ell \leq \frac{1}{2}(\frac{1}{4} - 2\delta)n - h(\delta)n$ (and concretely in our protocol, we set $\ell = \lambda n$ with $\lambda < \frac{1}{8}$), then the extracted string S_{1-c} is $negl(n)$-close to uniform given X_c (and hence also given S_c), the quantum system E, and all common classical information. Collecting all

the "errors" encountered on the way, the distance to uniform becomes $negl(n) + \sqrt{\bar{\varepsilon}_c^\delta(\Psi)}$. Below we analyze $\bar{\varepsilon}_c^\delta(\Psi)$ and show that it is $negl(n)$ as well; this then proves the claim.

□

Fact 4 ([BF10, Corollary 1])**.** *Let $|\phi_{AE}\rangle$ be a superposition on states of the form $|x\rangle_{\theta'}|\phi_E\rangle$ with $|w(x)| \leq \delta$ and $\delta < 1/2$, and let the random variable X be the outcome of measuring A in basis $\theta \in \{+, \times\}^n$. Then*

$$\mathbf{H}_{min}(X|E) \geq wt(\theta \oplus \theta') - h(\delta)n.$$

where $h(p) := -p \log p - (1-p)\log(1-p)$ is the Shannon binary entropy.

D.2.3 Analyzing the classical adaptive error probability

We now derive an upper bound on the classical error probability $\bar{\varepsilon}_c^\delta$ of the sampling strategy from Example 2.

Proposition 35. *For $\Psi = (P_T, P_S, f)$ from Example 2, and for any $\delta > 0$, it holds that $\bar{\varepsilon}_c^\delta(\Psi) \leq 6\exp(-\delta^2 n/144)$.*

Proof. WLOG, we assume $\hat{x}_i = 0$ in the sampling game $\mathcal{G}$ and speak of (relative) Hamming weight instead of (relative) Hamming distance. We use capital letters T_i, S_i and X_i to represent these random variables in the game, where the randomness comes from Alice playing according to (P_T, P_S) and arbitrary (possibly randomized) strategy $\mathcal{B}$ of Bob. Let $D_i := (1-T_i)X_i - 2T_iS_iX_i$ for $i = 1, \ldots, n$. Define $M_0 := 0$ and $M_k := \sum_{i=1}^k D_i, k = 1 \ldots n$. Notice that

$$\begin{aligned}\mathbb{E}[M_k|M_0, \ldots, M_{k-1}] - M_{k-1} &= \mathbb{E}[M_{k-1} + D_k|M_0, \ldots, M_{k-1}] - M_{k-1} \\ &= \mathbb{E}[D_k|M_0, \ldots, M_{k-1}] = (\mathbb{E}[1-T_k] - 2\mathbb{E}[T_kS_k]) \cdot \mathbb{E}[X_k|M_0, \ldots, M_{k-1}] = 0\end{aligned}$$

using the fact that T_k and S_k are independent of $M_0, \ldots, M_{k-1}$ and X_k, and $\mathbb{E}[T_kS_k] = \frac{1}{4}, \mathbb{E}[T_k] = \frac{1}{2}$. Hence $\{M_k\}_{k=0}^n$ forms a Martingale sequence. Also, by construction, $M_n = wt(X_{\overline{T}}) - 2wt(X_S)$. Next observe that $|M_k - M_{k-1}| = |D_k| \leq |(1-T_k)X_k| + 2|T_kS_kX_k| \leq 2$, therefore we can apply Azuma's inequality and obtain that, for any constant $\beta > 0$,

$$\Pr[|M_n| \geq \beta n] \leq 2\exp(\frac{-\beta^2 n^2}{2\sum_{k=1}^n 2^2}) = 2\exp(-\beta^2 n/8)$$

Now we analyze $\Pr[|w(X_{\overline{T}}) - w(X_S)| \geq \delta]$, which will give us an upper bound for $\bar{\varepsilon}_c^\delta(\Psi)$. For some constant $\varepsilon > 0$, define the event $E := [wt(\overline{T}) \in (\frac{1}{2} \pm \varepsilon)n \wedge wt(S) \in (\frac{1}{4} \pm \varepsilon)n]$, i.e., the event that $wt(\overline{T})$ and $wt(S)$ are concentrated around their respective expectations. Applying Hoeffding's inequality immediately tells us $\Pr[E] \geq 1 - 4\exp(-2\varepsilon^2 n)$. Conditioned on this event E, it holds that

$$|2wt(X_{\overline{T}}) - n \cdot w(X_{\overline{T}})| = |2wt(\overline{T})w(X_{\overline{T}}) - n \cdot w(X_{\overline{T}})| \leq |2wt(\overline{T}) - n| \cdot |w(X_{\overline{T}})| \leq 2\varepsilon n$$

and, similarly, that $|4wt(X_S) - n \cdot w(X_S)| \leq 4\varepsilon n$. Hence, conditioned on E and $|M_n| < \beta n$, it holds that

$$|w(X_{\overline{T}}) - w(X_S)| \leq \frac{1}{n}|2wt(X_{\overline{T}}) - 4wt(X_S)| + 6\varepsilon \leq 2\beta + 6\varepsilon\,.$$

It follows that

$$\Pr[|w(X_{\overline{T}}) - w(X_S)| \geq 2\beta + 6\varepsilon] \leq \Pr[\neg E \vee |M_n| \geq \beta n] \leq 4\exp(-2\varepsilon^2 n) + 2\exp(-\beta^2 n/8)\,.$$

Finally, picking[17] $\varepsilon = \delta/12$ and $\beta = \delta/4$, we conclude that

$$\bar{\varepsilon}_c^\delta(\Psi) \leq \Pr[|w(X_{\overline{T}}) - w(X_S)| \geq \delta] \leq 6\exp(-\delta^2 n/144)$$

□

For completeness, we include some of the technical facts we used in this section.

[17] Our purpose here is simplifying the expression, and it is not necessarily tight though.

Fact 5 (Hoeffding's inequality)**.** *Let $x \in \{0,1\}^n$ be a bit string with relative Hamming weight $\mu := w(x)$. Let $X_1, \ldots, X_k$ be sampling k bits from x independently without replacement. Then for any $\delta > 0$, $\overline{X} := \frac{1}{k}\sum_i X_i$ satisfies*

$$\Pr[|\overline{X} - \mu| > \delta] \leq 2\exp(-2\delta^2 k)$$

Fact 6 (Azuma's inequality)**.** *Let $X_j : j = 0, \ldots, n$ be a martingale and $|X_j - X_{j-1}| < c_j$, then*

$$\Pr[|X_n - X_0| \geq t] \leq 2\exp(\frac{-t^2}{2\sum_{j=1}^n c_j^2})$$

Fact 7 (Privacy Amplification [RK05, Theorem 1])**.** *Let ρ_{XE} be a hybrid state with classical X with the form $\rho_{XE} = \sum_{x\in\mathcal{X}} P_X|x\rangle\langle x| \otimes \rho_E^x$. Let $\mathbf{F}$ be a family of universal hash functions with range $\{0,1\}^\ell$, and F be chosen randomly from $\mathbf{F}$. Then $K = F(X)$ satisfies*

$$D(\rho_{KFE}, \frac{1}{2^\ell}\mathbb{I}_K \otimes \rho_{FE}) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(\mathbf{H}_{min}(X|E)-\ell)}$$

E Impossibility of Quantum UC Commitment

Canetti and Fischlin [CF01] show the impossibility of realizing $\mathcal{F}_{\mathtt{COM}}$ in the plain model achieving computationally classical UC security[18]. Roughly speaking, if a protocol π UC-realizes $\mathcal{F}_{\mathtt{COM}}$, then an ideal world simulator $\mathcal{S}$ should be able to be constructed and satisfy the following properties:

- When the committer is corrupted (i.e., controlled by the adversary), $\mathcal{S}$ must be able to "extract" the committed value once the commitment phase is done. That is, $\mathcal{S}$ has to come up with a value x such that the committer will almost never be able to successfully decommit to any $x' \neq x$. This is so since in the ideal process $\mathcal{S}$ has to explicitly provide $\mathcal{F}_{\mathtt{COM}}$ with a committed value.
- When the receiver is uncorrupted, $\mathcal{S}$ has to be able to generate a simulated commitment c that looks like a real commitment and yet can be opened to any value, to be determined at the time of opening. This is so since S has to provide adversary $\mathcal{A}$ and environment $\mathcal{Z}$ with the simulated commitment c before the value committed to is known. All this needs to be done without rewinding the environment $\mathcal{Z}$.

Intuitively, these requirements look impossible to meet: A simulator that has the above abilities can be used by a dishonest receiver to "extract" the committed value from an honest committer. This intuition can indeed be formalized to show that in the plain model it is impossible to UC-realize $\mathcal{F}_{\mathtt{COM}}$ by any two-party protocol. This idea extends to the quantum UC setting naturally, and we can show the following theorem.

Lemma 36 (restate Lemma 9)**.** *There exists no protocol in the plain model which computationally quantum-UC realizes the commitment functionality $\mathcal{F}_{\mathtt{COM}}$.*

Proof. Suppose, for contradiction, that there exists (possibly quantum) protocol Π that quantum-UC-emulates $\mathcal{F}_{\mathtt{COM}}$. Assume at the end of the commitment phase, receiver acknowledges the committer by a receipt message. Consider an execution of π by an adversarial committer $\mathcal{A}_C$ and an honest receiver R, and WLOG we assume that the adversary merely forwards the communication messages between the environment $\mathcal{Z}_C$ and the honest receiver R (Note that this adversarial behavior is implementable by a quantum adversary as the adversary does not need to apply any transformation on the state and merely forwards it). Here $\mathcal{Z}_C$ privately chooses a random bit b at the beginning and then runs the protocol of the honest committer based on input bit b and R's answers, and then in the name of the committer sends the generated messages to R. Once $\mathcal{Z}_C$ received a receipt message from R at the end of committing stage, it starts running the honest opening protocol in the name of the committer, and receives bit b' from R at the end of opening stage. Finally, $\mathcal{Z}_C$ outputs 1 iff $b' = b$. We know that if both committer and receiver are honest in an execution of π, then in the opening phase the receiver always outputs the bit committed to by the committer, i.e., $b' = b$ always holds. By assumption that π quantum-UC-emulates $\mathcal{F}_{\mathtt{COM}}$, there should exist an ideal world simulator $\mathcal{S}$ that interacts with $\mathcal{F}_{\mathtt{COM}}$ and generates a view for $\mathcal{Z}_C$ that is indistinguishable from a real execution with π. We note that the view could consist of quantum messages and/or classic messages. In particular, $\mathcal{S}$ must make sure $b = b'$ almost always, where b' is the bit that $\mathcal{S}$ sends to $\mathcal{F}_{\mathtt{COM}}$. This means that the simulator $\mathcal{S}$ must be able to generate the correct bit b before the opening phase.

Next based on this $\mathcal{S}$, we are able to construct another environment, $\mathcal{Z}_R$, and a corrupted receiver $\mathcal{A}_R$, such that $\mathcal{Z}_R$ successfully distinguishes between an execution of π and an interaction with $\mathcal{F}_{\mathtt{COM}}$

[18] Note that, statistically, commitment is impossible from scratch even in the stand-alone model [May97, LC97, May01].

for any simulator $\mathcal{S}_R$. $\mathcal{Z}_R$ and $\mathcal{A}_R$ proceed as follows: $\mathcal{Z}_R$ chooses a random bit b and hands b as input to the honest committer C; $\mathcal{A}_R$ simply runs $\mathcal{S}$ and forwards all interaction between the committer and $\mathcal{S}$ (again this strategy is implementable by a quantum adversary as the adversary does not need to apply any transformation on the state); once $\mathcal{A}_R$ receives a bit b', it is passed to $\mathcal{Z}_R$ who then outputs 1 iff. $b = b'$.

Note that $\mathcal{S}$ can extract the committed bit b almost always, without rewinding or any additional information. In contrast, when $\mathcal{Z}_R$ interacts with $\mathcal{F}_{\mathtt{COM}}$, the $\mathcal{S}_R$'s view is independent of b, and thus $b = b'$ with probability exactly one half. Therefore, $\mathcal{Z}_R$ can tell the difference between its interaction with the real world or with $\mathcal{F}_{\mathtt{COM}}$ and ideal world for any $\mathcal{S}_R$.

□

Protocol $\Pi^{\mathtt{COM}}_{\mathtt{QOT}}$

Parameters: Integers $n, m > n, \ell$, a family $\mathbf{F}$ of universal hash functions.

Parties: The sender Alice and the recipient Bob.

Inputs: Alice gets input two ℓ-bit strings s_0 and s_1, Bob gets a bit c.

1. Alice chooses $\tilde{x}^A \in \{0,1\}^m$ and $\tilde{\theta}^A \in \{+,\times\}^m$ and sends $|\tilde{x}^A\rangle_{\tilde{\theta}^A}$ to Bob.
2. Bob receives the state $|\Psi\rangle$ sent by the sender. Then Bob chooses $\tilde{\theta}^B \in \{+,\times\}^m$ and measures the qubits of $|\Psi\rangle$ in the bases $\tilde{\theta}^B$. Call the result $\tilde{x}^B$.
3. For each i, Bob commits to $\tilde{\theta}^B_i$ and $\tilde{x}^B_i$ using one instance of $\mathcal{F}_{\mathtt{COM}}$ each.
4. Alice chooses a set $T \subseteq \{1,\ldots,m\}$ of size $m-n$ and sends T to Bob.
5. Bob opens the commitments of $\tilde{\theta}^B_i$ and $\tilde{x}^B_i$ for all $i \in T$.
6. Alice checks $\tilde{x}^A_i = \tilde{x}^B_i$ and $\tilde{\theta}^A_i = \tilde{\theta}^B_i$ for all i with $i \in T$. If this test fails, Alice aborts.
7. Let $\hat{x}^A$ be the n-bit string resulting from removing the bits at positions $i \in T$ from $\tilde{x}^A$. Define $\hat{\theta}^A$, $\hat{x}^B$, $\hat{\theta}^B$ analogously.
8. Alice sends θ^A to Bob.
9. Bob sets $I_c := \{i : \hat{\theta}^A_i = \hat{\theta}^B_i\}$ and $I_{1-c} := \{i : \hat{\theta}^A_i \neq \hat{\theta}^B_i\}$. Then Bob sends (I_0, I_1) to Alice.
10. 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.
11. 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.

Figure 8: Protocol $\Pi^{\mathtt{COM}}_{\mathtt{QOT}}$ for 1-out-of-2 OT in the $\{\mathcal{F}_{\mathtt{COM}}\}$-hybrid world.