Composing Quantum Protocols in a Classical Environment

Serge Fehr[*] and Christian Schaffner[**]

Centrum Wiskunde & Informatica (CWI)
Amsterdam, The Netherlands
{S.Fehr,C.Schaffner}@cwi.nl

Abstract. We propose a general security definition for cryptographic quantum protocols that implement classical non-reactive two-party tasks. The definition is expressed in terms of simple quantum-information-theoretic conditions which must be satisfied by the protocol to be secure. The conditions are uniquely determined by the ideal functionality $\mathcal{F}$ defining the cryptographic task to be implemented. We then show the following composition result. If quantum protocols $\pi_1, \ldots, \pi_\ell$ securely implement ideal functionalities $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ according to our security definition, then any purely *classical* two-party protocol, which makes sequential calls to $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$, is equally secure as the protocol obtained by replacing the calls to $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ with the respective quantum protocols $\pi_1, \ldots, \pi_\ell$. Hence, our approach yields the minimal security requirements which are strong enough for the typical use of quantum protocols as subroutines within larger classical schemes. Finally, we show that recently proposed quantum protocols for secure identification and oblivious transfer in the bounded-quantum-storage model satisfy our security definition, and thus compose in the above sense.

1 Introduction

Background. Finding the right security definition for a cryptographic task is a non-trivial fundamental question in cryptography. From a theoretical point of view, one would like definitions to be as strong as possible in order to obtain strong composability guarantees. However, this often leads to impossibility results or to very complex and inefficient schemes. Therefore, from a practical point of view, one may also consider milder security definitions which allow for efficient schemes, but still offer "good enough" security.

It is fair to say that in computational cryptography, the question of defining security and the trade-offs that come along with these definitions are by now quite well understood. The situation is different in quantum cryptography. For instance, it was realized only recently that the standard security definition of quantum key-agreement does not guarantee the desired kind of security

[*] Supported by the Dutch Organization for Scientific Research (NWO).

[**] Supported by the EU fifth framework project QAP IST 015848 and the Dutch Organization for Scientific Research (NWO).

and some work was required to establish the right security definition [13, 23, 2, 22, 17]. Security definitions for general quantum protocols have first been proposed in [14] and subsequently been refined for the case of quantum multi-party computation in [26]. In [3, 27], strong security definitions for general quantum protocols were proposed by translating Canetti's universal-composability framework and Backes, Pfitzmann and Waidner's reactive-simulatability model, respectively, into the quantum setting. The resulting security definitions are very strong and guarantee full composability. However, they are complex and hard to achieve. Indeed, so far they have been actually used and shown to be achievable only in a couple of isolated cases: quantum key distribution [2] and quantum multi-party computation with dishonest minority [1]. It is still common practice in quantum cryptography that every paper proposes its own security definition of a certain task and proves security with respect to the proposed definition. However, it usually remains unclear whether these definitions are strong enough to guarantee any kind of composability, and thus whether protocols that meet the definition really behave as expected.

Contribution. We propose a general security definition for quantum protocols that implement cryptographic two-party tasks. The definition is in terms of simple quantum-information-theoretic security conditions that must be satisfied for the protocol to be secure. In particular, the definition does not involve additional entities like a "simulator" or an "environment". The security conditions are uniquely determined by the *ideal functionality* that defines the cryptographic task to be realized. Our definition applies to any *non-reactive, classical* ideal functionality $\mathcal{F}$, which obtains classical (in the sense of non-quantum) input from the two parties, processes the provided input according to its specification, and outputs the resulting classical result to the parties. A typical example for such a functionality/task is oblivious transfer (OT). Reactive functionalities, i.e. functionalities that have several phases (like e.g. bit commitment), or functionalities that take quantum input and/or produce quantum output are not the scope of this paper.

We show the following composition result. If quantum protocols $\pi_1, \ldots, \pi_\ell$ securely implement ideal functionalities $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ according to our security definition, then any purely *classical* two-party protocol, which makes sequential calls to $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$, is equally secure as the protocol obtained by replacing the calls to $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ with the respective quantum subroutines $\pi_1, \ldots, \pi_\ell$. We stress that our composition theorem, respectively our security definition, only allows for the composition of quantum sub-protocols into a *classical* outer protocol. This is a trade-off which allows for milder security definitions (which in turn allows for simpler and more efficient implementations) but still offers security in realistic situations. Indeed, current technology is far from being able to execute quantum algorithms or protocols which involve complicated quantum operations and/or need to keep a quantum state "alive" for more than a tiny fraction of a second. Thus, the best one can hope for in the near future in terms of practical quantum algorithms is that certain small subroutines, like key-distribution or OT, may be implemented by quantum protocols, while the more complex outer protocol remains classical. From a more theoretical point of view, our general security definition expresses what security properties a quantum protocol must satisfy in order to be able to instantiate a basic cryptographic primitive upon which an information-theoretic cryptographic construction is based. For instance, it expresses the security properties a quantum OT[1] needs to satisfy so that Kilian's classical[2] construction of general secure function evaluation based on OT [15] remains secure when instantiating the OT primitive by a quantum protocol.

Finally, we show that the *ad-hoc* security definitions proposed by Damgård, Fehr, Salvail and Schaffner for their 1-2 OT and secure-identification protocols in the bounded-quantum-storage model [7, 9] imply (and are likely to be equivalent) to the corresponding security definitions obtained from our approach.[3] This implies composability in the above sense for these quantum protocols in the bounded-quantum-storage model.

Related work. In the classical setting, Crépeau *et al.* proposed information-theoretic conditions for two-party secure function evaluation [5], though restricted to the *perfect* case, where the protocol is not allowed to make any error. They show equivalence to a simulation-based definition that corresponds to the standard framework of Goldreich [12]. Similar conditions have been subsequently found by Crépeau and Wullschleger for the case of non-perfect classical protocols [6]. Our work can be seen as an extension of [5, 6] to the setting where classical subroutines are implemented by quantum protocols.

As pointed out and discussed above, general frameworks for universal composability in the quantum setting have been established in [3, 27]. The composability of protocols in the bounded-quantum-storage model has recently been investigated by Wehner and Wullschleger [29]. They propose security definitions that guarantee sequential composability of quantum protocols within *quantum* protocols. This is clearly a stronger composition result than we obtain (though restricted to the bounded-quantum-storage model) but comes at the price of a more demanding security definition. And indeed, whereas we show that the simple definitions used in [8, 7] already guarantee composability into classical protocols without any modifications to the original parameters and proofs, [29] need to strengthen the quantum-memory bound (and re-do the security proof) in order to show that the 1-2 OT protocol from [7] meets their strong security definition. As we argued above, this is an overkill in many situations.

[1] We are well aware that quantum OT is impossible without any restriction on the adversary, but it becomes possible for instance when restricting the adversary's quantum memory [8, 7].

[2] Here, "classical" can be understood as "non-quantum" as well as "being a classic".

[3] Interestingly, this is not true for the definition of Rabin OT given in the first paper in this line of research [8], and indeed in the full version of that paper, it is mentioned that their definition poses some "composability problems" (this problem though has been fixed in the journal version [10]). This supports our claim that failure of satisfying our security definition is strong evidence for a security problem of a quantum protocol (or the definition used).

2 Notation

Quantum States. We assume the reader's familiarity with basic notation and concepts of quantum information processing [21].

Given a bipartite quantum state ρ_{XE}, we say that X is *classical* if ρ_{XE} is of the form $\rho_{XE} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \rho_E^x$ for a probability distribution P_X over a finite set $\mathcal{X}$. This can be understood in that the state of the quantum register E depends on the classical random variable X, in the sense that E is in state ρ_E^x exactly if $X = x$. For any event $\mathcal{E}$ defined by $P_{\mathcal{E}|X}(x) = P[\mathcal{E}|X = x]$ for all x, we may then write

$$\rho_{XE|\mathcal{E}} := \sum_x P_{X|\mathcal{E}}(x) |x\rangle\langle x| \otimes \rho_E^x \ . \tag{1}$$

When we omit registers, we mean the partial trace over these register, for instance $\rho_{E|\mathcal{E}} = \mathrm{tr}_X(\rho_{XE|\mathcal{E}}) = \sum_x P_{X|\mathcal{E}}(x)\rho_E^x$, which describes E given that the event $\mathcal{E}$ occurs.

This notation extends naturally to states that depend on several classical random variables X, Y etc., defining the density matrices ρ_{XYE}, $\rho_{XYE|\mathcal{E}}$, $\rho_{YE|X=x}$ etc. We tend to slightly abuse notation and write $\rho_{YE}^x = \rho_{XE|X=x}$ and $\rho_{YE|\mathcal{E}}^x = \rho_{YE|X=x,\mathcal{E}}$, as well as $\rho_E^x = \mathrm{tr}_Y(\rho_{YE}^x)$ and $\rho_{E|\mathcal{E}}^x = \mathrm{tr}_Y(\rho_{YE|\mathcal{E}}^x)$. Given a state ρ_{XE} with classical X, by saying that "there exists a classical random variable Y such that ρ_{XYE} satisfies some condition", we mean that ρ_{XE} can be understood as $\rho_{XE} = \mathrm{tr}_Y(\rho_{XYE})$ for some state ρ_{XYE} with classical X and Y, and that ρ_{XYE} satisfies the required condition.

X is independent of E (in that ρ_E^x does not depend on x) if and only if $\rho_{XE} = \rho_X \otimes \rho_E$, which in particular implies that no information on X can be learned by observing only E. Similarly, X is random and independent of E if and only if $\rho_{XE} = \frac{1}{|\mathcal{X}|}\mathbb{I} \otimes \rho_E$, where $\frac{1}{|\mathcal{X}|}\mathbb{I}$ is the density matrix of the fully mixed state of suitable dimension.

We also need to express that a random variable X is independent of a quantum state E *when given a random variable* Y. This means that when given Y, the state E gives no additional information on X. Yet another way to understand this is that E is obtained from X and Y by solely processing Y. Formally, adopting the notion introduced in [9], this is expressed by requiring that ρ_{XYE} equals $\rho_{X \leftrightarrow Y \leftrightarrow E}$, where the latter is defined as

$$\rho_{X \leftrightarrow Y \leftrightarrow E} := \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^y \,.$$

In other words, $\rho_{XYE} = \rho_{X \leftrightarrow Y \leftrightarrow E}$ precisely if $\rho_E^{x,y} = \rho_E^y$ for all x and y. This notation naturally extends to $\rho_{X \leftrightarrow Y \leftrightarrow E|\mathcal{E}} = \sum_{x,y} P_{XY|\mathcal{E}}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_{E|\mathcal{E}}^y$.

Full (conditional) independence is often too strong a requirement, and it usually suffices to be "close" to such a situation. Closeness of two states ρ and σ is measured in terms of their trace distance $\delta(\rho, \sigma) = \frac{1}{2}\,\mathrm{tr}(|\rho - \sigma|)$, where for any operator A, $|A|$ is defined as $|A| := \sqrt{AA^\dagger}$. We write $\rho \approx_\varepsilon \sigma$ to denote that $\delta(\rho, \sigma) \leq \varepsilon$, and we then say that ρ and σ are ε-close. It is known that

ε-closeness is preserved under any quantum operation; this in particular implies that if $\rho \approx_\varepsilon \sigma$ then no observer can distinguish ρ from σ with advantage greater than ε [23]. For states ρ_{XE} and $\rho_{X'E'}$ with classical X and X', it is not hard to see that $\delta(\rho_{XE}, \rho_{X'E'}) = \sum_x \delta(P_X(x)\rho_E^x, P_{X'}(x)\rho_{E'}^x)$, and thus $\delta(\rho_{XE}, \rho_{X'E'}) = \sum_x P_X(x)\delta(\rho_E^x, \rho_{E'}^x)$ if $P_X = P_{X'}$. In case of purely classical states ρ_X and $\rho_{X'}$, the trace distance coincides with the statistical distance of the random variables X and X': $\delta(\rho_X, \rho_{X'}) = \frac{1}{2}\sum_x |P_X(x) - P_{X'}(x)|$, and we then write $P_X \approx_\varepsilon P_{X'}$, or $X \approx_\varepsilon X'$, instead of $\rho_X \approx_\varepsilon \rho_{X'}$.

We will make use of the following lemmas whose proofs are given in the full version [11] of this paper.

Lemma 2.1. *1. If $\rho_{XYZE} \approx_\varepsilon \rho_{X\leftrightarrow Y\leftrightarrow ZE}$ then $\rho_{XYZE} \approx_{2\varepsilon} \rho_{X\leftrightarrow YZ\leftrightarrow E}$.*
2. If $\rho_{XZE} \approx_\varepsilon \rho_X \otimes \rho_{ZE}$ then $\rho_{XZE} \approx_{2\varepsilon} \rho_{X\leftrightarrow Z\leftrightarrow E}$.
3. If $\rho_{XZE} \approx_\varepsilon \mathbb{I}/|\mathcal{X}| \otimes \rho_{ZE}$, then $\rho_{XZE} \approx_{4\varepsilon} \rho_{X\leftrightarrow Z\leftrightarrow E}$.

Lemma 2.2. *If $\rho_{XYE} \approx_\varepsilon \rho_{X\leftrightarrow Y\leftrightarrow E}$ then $\rho_{Xf(X,Y)YE} \approx_\varepsilon \rho_{Xf(X,Y)\leftrightarrow Y\leftrightarrow E}$ for any function f.*

Lemma 2.3. *For an event $\mathcal{E}$ which is completely determined by the random variable Y, i.e. for all y, the probability $\Pr[\mathcal{E}|Y = y]$ either vanishes or equals one, we can decompose the density matrix $\rho_{X\leftrightarrow Y\leftrightarrow E}$ into*[4]

$$\rho_{X\leftrightarrow Y\leftrightarrow E} = \Pr[\mathcal{E}] \cdot \rho_{X\leftrightarrow Y\leftrightarrow E|\mathcal{E}} + \Pr[\overline{\mathcal{E}}] \cdot \rho_{X\leftrightarrow Y\leftrightarrow E|\overline{\mathcal{E}}} \,.$$

3 Protocols and Functionalities

Quantum Protocols. We consider *two-party quantum protocols* $\pi = (\mathsf{A}, \mathsf{B})$, consisting of interactive quantum algorithms A and B. For convenience, we call the two parties who run A and B *Alice* and *Bob*, respectively. There are different approaches to formally define interactive quantum algorithms and thus quantum two-party protocols, in particular when we restrict in- and outputs (of honest participants) to be classical. For instance such a formalization can be done by means of quantum circuits, or by means of a classical Turing machine which outputs unitaries that are applied to a quantum register. For our work, the specific choice of the formalization is immaterial; what is important is that such a two-party quantum protocol, formalized in whatever way, uniquely specifies its input-output behavior. Therefore, in this work, we capture quantum protocols by their input-output behavior, which we formalize by a quantum operation, i.e. a trace-preserving completely-positive map, which maps the common two-partite input state ρ_{UV} to the common two-partite output state ρ_{XY}. We denote this operation by $\rho_{XY} = \pi\, \rho_{UV}$ or, when we want to emphasize that π is executed by *honest* Alice and Bob, also by $\rho_{XY} = \pi_{\mathsf{A},\mathsf{B}}\, \rho_{UV}$. If one of the players, say Bob, is *dishonest* and follows a malicious strategy B', then we slightly abuse notation and write $\pi_{\mathsf{A},\mathsf{B}'}$ for the corresponding operator.

[4] One is tempted to think that such a decomposition holds for *any* event $\mathcal{E}$; however, this is not true. See Lemma 2.1 of [9] for another special case where the decomposition does hold.

Protocols and Functionalities with Classical In- and Output. In this work, we focus on quantum protocols $\pi = (\mathsf{A}, \mathsf{B})$ with *classical in- and output* for the honest players. This means that we assume the common input state ρ_{UV} to be classical, i.e. of the form $\rho_{UV} = \sum_{u,v} P_{UV}(u,v)|u\rangle\langle u| \otimes |v\rangle\langle v|$ for some probability distribution P_{UV}, and the common output state $\rho_{XY} = \pi_{\mathsf{A},\mathsf{B}}\,\rho_{UV}$ is then guaranteed to be classical as well, i.e., $\rho_{XY} = \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y|$. In this case we may understand U and V as well as X and Y as random variables, and we also write $(X,Y) = \pi(U,V)$. Note that the input-output behavior of the protocol is uniquely determined by the conditional probability distribution $P_{XY|UV}$. If one of the players, say Bob, is dishonest and follows a malicious strategy B', then we may allow his part of the input to be quantum and denote it as V', i.e. $\rho_{UV'} = \sum_u P_U(u)|u\rangle\langle u| \otimes \rho_{V'|U=u}$, and we allow his part Y' of the common output state $\rho_{XY'} = \pi_{\mathsf{A},\mathsf{B}'}\,\rho_{UV'}$ to be quantum, i.e. $\rho_{XY'} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_{Y'|X=x}$. We write $\rho_{UV'}$ as $\rho_{U\emptyset} = \rho_U \otimes \rho_\emptyset = \rho_U$ if V' is empty, i.e. if B' has no input at all, and we write it as $\rho_{UZV'}$ if part of his input, Z, is actually classical.

A classical non-reactive two-party *ideal functionality* $\mathcal{F}$ is given by a conditional probability distribution $P_{\mathcal{F}(U,V)|UV}$, inducing a pair of random variables $(X,Y) = \mathcal{F}(U,V)$ for every joint distribution of U and V. We also want to take into account ideal functionalities which allow the dishonest player some additional—though still limited—capabilities (as for instance in Section 6). We do this as follows. We specify $\mathcal{F}$ not only for the "proper" domains $\mathcal{U}$ and $\mathcal{V}$, over which U and V are supposed to be distributed, but we actually specify it for some larger domains $\tilde{\mathcal{U}} \supseteq \mathcal{U}$ and $\tilde{\mathcal{V}} \supseteq \mathcal{V}$. The understanding is that U and V provided by honest players always lie in $\mathcal{U}$ and $\mathcal{V}$, respectively, whereas a dishonest player, say Bob, may select V from $\tilde{\mathcal{V}} \setminus \mathcal{V}$, and this way Bob may cause $\mathcal{F}$, if specified that way, to process its inputs differently and/or to provide a "more informative" output Y to Bob. For simplicity though, we often leave the possibly different domains for honest and dishonest players implicit.

We write $(X,Y) = \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}}(U,V)$ or $\rho_{XY} = \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}}\,\rho_{UV}$ for the execution of the "ideal-life" protocol, where Alice and Bob forward their inputs to $\mathcal{F}$ and output whatever they obtain from $\mathcal{F}$. And we write $\rho_{XY'} = \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}\,\rho_{UV'}$ for the execution of this protocol with a dishonest Bob with strategy $\hat{\mathsf{B}}'$ and quantum input V'. Note that Bob's possibilities are very limited: he can produce some classical input V for $\mathcal{F}$ (distributed over $\tilde{\mathcal{V}}$) from his input quantum state V', and then he can prepare and output a quantum state Y' which might depend on $\mathcal{F}$'s reply Y.

Classical Hybrid Protocols. A two-party *classical hybrid* protocol $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell} = (\hat{\mathsf{A}}, \hat{\mathsf{B}})$ between Alice and Bob is a protocol which makes a bounded number k of sequential oracle calls to possibly different ideal functionalities $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$. We allow $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ to make several calls to independent copies of the same $\mathcal{F}_i$, but we require from $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}$ that for every possible execution, there is always agreement between $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ on when to call which functionality; for instance we may assume that $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ exchange the index i before they call $\mathcal{F}_i$ (and stop if there is disagreement).

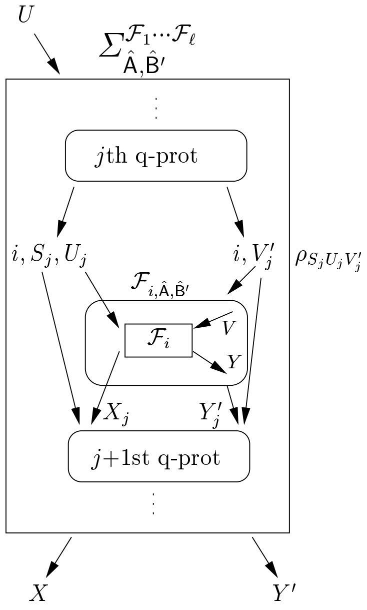
U
$\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$
jth q-prot
i, S_j, U_j
i, V'_j
$\rho_{S_jU_jV'_j}$
$\mathcal{F}_{i,\hat{\mathsf{A}},\hat{\mathsf{B}}'}$
$\mathcal{F}_i$
V
Y
X_j
Y'_j
j+1st q-prot
X
Y'

Fig. 1. Hybrid protocol $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$

Formally, such a classical hybrid protocol is given by a sequence of $k+1$ quantum protocols formalized by quantum operators with classical in- and output for the honest players, see Figure 1. For an honest player, say Alice, the j-th protocol outputs an index i indicating which functionality is to be called, classical auxiliary (or "state") information information S_j and a classical input U_j for $\mathcal{F}_i$. The $(j+1)$-st protocol expects as input S_j and Alice's classical output X_j from $\mathcal{F}_i$. Furthermore, the first protocol expects Alice's classical input U to the hybrid protocol, and the last produces the classical output X of the hybrid protocol. In case of a dishonest player, say Bob, all in- and outputs may be quantum states V'_j respectively Y'_j. By instantiating the j-th call to a functionality $\mathcal{F}$ (where we from now on omit the index for simpler notation) in the obvious way by the corresponding "ideal-life" protocol $\mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}}$ (respectively $\mathcal{F}_{\hat{\mathsf{A}}',\hat{\mathsf{B}}}$ or $\mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$ in case of a dishonest Alice or Bob), we obtain the instantiated hybrid protocol formally described by quantum operator $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}},\hat{\mathsf{B}}}$ (respectively $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}}',\hat{\mathsf{B}}}$ or $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$).[5]

For the hybrid protocol to be *classical*, we mean that it has classical in- and output (for the honest players), but also that all communication between Alice and Bob is classical.Since we have not formally modeled the communication within (hybrid) protocols, we need to formalize this property as a property of the quantum operators that describe the hybrid protocol: Consider a dishonest player, say Bob, with no input, and consider the common state $\rho_{S_jU_jV'_j}$ at any point during the execution of the hybrid protocol when a call to functionality $\mathcal{F}_i$ is made. The requirement for the hybrid protocol to be *classical* is now expressed in that there exists a classical Z_j—to be understood as consisting of $\hat{\mathsf{B}}'$'s classical communication with $\hat{\mathsf{A}}$ and with the $\mathcal{F}_{i'}$'s up to this point—such that given Z_j, Bob's quantum state V'_j is uncorrelated with (i.e. independent of) Alice' classical input and auxiliary information: $\rho_{S_jU_jZ_jV'_j} = \rho_{S_jU_j\leftrightarrow Z_j\leftrightarrow V'_j}$. Furthermore, we require that we may assume Z_j to be part of V'_j in the sense that for any $\hat{\mathsf{B}}'$ there exists $\hat{\mathsf{B}}''$ such that Z_j is part of V'_j. This definition is motivated by the observation that if Bob can communicate only classically with Alice, then he can correlate his quantum state with information on Alice's side only by means of the classical communication.

[5] Note that for simpler notation, we are a bit sloppy and give the same name, like $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}'$, to honest Alice's and dishonest Bob's strategy within different (sub)protocols.

We also consider the protocol we obtain by replacing the ideal functionalities by quantum two-party sub-protocols $\pi_1, \ldots, \pi_\ell$ with classical in- and outputs for the honest parties: whenever $\Sigma^{\mathcal{F}_1 \cdots \mathcal{F}_\ell}$ instructs $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ to execute $\mathcal{F}_{i\hat{\mathsf{A}},\hat{\mathsf{B}}}$, they instead execute $\pi_i = (\mathsf{A}_i, \mathsf{B}_i)$ and take the resulting outputs. We write $\Sigma^{\pi_1 \cdots \pi_\ell} = (\mathsf{A}, \mathsf{B})$ for the real-life quantum protocol we obtain this way.

4 Security for Two-Party Quantum Protocols

4.1 The Security Definition

Framework. We use the following framework for defining security of a quantum protocol π with classical in- and output. We distinguish three cases and consider the respective output states obtained by executing π in case of honest Alice and honest Bob, in case of honest Alice and dishonest Bob, and in case of dishonest Alice and honest Bob. For each of these cases we require some security conditions on the output state to hold. More precisely, for honest Alice and Bob, we fix an arbitrary joint probability distribution P_{UV} for the inputs U and V, resulting in outputs $(X, Y) = \pi_{\mathsf{A},\mathsf{B}}(U, V)$ with a well defined joint probability distribution P_{UVXY}. For an honest Alice and a dishonest Bob, we fix an arbitrary distribution P_U for Alice's input and an arbitrary strategy B' *with no input* for Bob, and we consider the resulting joint output state

$$\rho_{UXY'} = \big(\mathrm{id}_U \otimes \pi_{\mathsf{A},\mathsf{B}'}\big)\rho_{UU\emptyset} = \sum_u P_U(u)|u\rangle\langle u| \otimes \pi_{\mathsf{A},\mathsf{B}'}(|u\rangle\langle u|\otimes\rho_\emptyset)$$

augmented with Alice's input U, where U and X are classical and Y' is in general quantum. And, correspondingly, for a dishonest Alice and an honest Bob, we fix an arbitrary distribution P_V for Bob's input and an arbitrary strategy A' *with no input* for Alice, and we consider the resulting joint output state $\rho_{VX'Y} = \big(\mathrm{id}_V \otimes \pi_{\mathsf{A}',\mathsf{B}}\big)\rho_{V\emptyset V}$ augmented with Bob's input V. Then, security is defined by specific information-theoretic conditions on P_{UVXY}, $\rho_{UXY'}$ and $\rho_{VX'Y}$, where the conditions depend on the functionality $\mathcal{F}$ which π is implementing. Definition 4.1 below for a general functionality $\mathcal{F}$, as well as the definitions studied later for specific functionalities (Definitions 6.1), are to be understood in this framework. In particular, the augmented common output states are to be understood as defined above.

We stress once more that the framework assumes that dishonest players have no input at all. This might appear too weak at first glance; one would expect a dishonest player, say Bob, to at least get the input V of the honest Bob. The justification for giving dishonest players no input is that on the one hand, we will show that this "minimalistic approach" is good enough for the level of security we are aiming for (see Theorem 5.1), and on the other hand, our goal is to keep the security definitions as simple as possible.

Restricting the Adversary. Since essentially no interesting two-party task can be implemented securely by a quantum protocol against unbounded quantum attacks [20, 19, 18, 16], one typically has to put some restriction upon the dishonest player's capabilities, like to limit his quantum-storage capabilities [8, 7, 9, 28] or the size of coherent measurements he can do [24]. Throughout, we let $\mathfrak{A}$ and $\mathfrak{B}$ be subfamilies of all possible strategies A' and B' of a dishonest Alice and a dishonest Bob, respectively. In order to circumvent pathological counter examples, we need to assume the following two natural consistency conditions on $\mathfrak{A}$, and correspondingly on $\mathfrak{B}$. If a dishonest strategy $\mathsf{A}' \in \mathfrak{A}$ expects as input some state $\rho_{ZU'}$ with classical Z, then for any z and for any $\rho_{U'|Z=z}$, the strategy $\mathsf{A}'_{z,\rho_{U'|Z=z}}$, which has z hard-wired and prepares the state $\rho_{U'|Z=z}$ as an initial step but otherwise runs like A', is in $\mathfrak{A}$ as well. And, if $\mathsf{A}' \in \mathfrak{A}$ is a dishonest strategy for a protocol Σ^{π} which makes a call to a sub-protocol π, then the corresponding "sub-strategy" of A', which is active during the execution of π, is in $\mathfrak{A}$ as well. It is for instance clear that bounding the quantum memory leads to a family of strategies that satisfies these conditions.

Defining Security. Following the framework described above, we propose the following security definition for two-party quantum protocols with classical in- and output. The proposed definition implies strong simulation-based security when using quantum protocols as sub-protocols in classical outer protocols (Theorem 5.1), yet it is expressed in a way that is as simple and as weak as seemingly possible, making it as easy as possible to design and prove quantum cryptographic schemes secure according to the definition.

Definition 4.1. *A two-party quantum protocol* π ε-securely implements *an ideal classical functionality* $\mathcal{F}$ *against* $\mathfrak{A}$ *and* $\mathfrak{B}$ *if the following holds:*

Correctness: *For any joint distribution of the input U and V, the resulting common output $(X,Y) = \pi(U,V)$ satisfies $(U,V,X,Y) \approx_{\varepsilon} (U,V,\mathcal{F}(U,V))$.*

Security for Alice: *For any $\mathsf{B}' \in \mathfrak{B}$ (with no input), and for any distribution of U, the resulting common output state $\rho_{UXY'}$ (augmented with U) is such that there exist*[6] *classical random variables V, Y such that $P_{UV} \approx_{\varepsilon} P_U \cdot P_V$, $(U,V,X,Y) \approx_{\varepsilon} (U,V,\mathcal{F}(U,V))$, and $\rho_{UXVYY'} \approx_{\varepsilon} \rho_{UX \leftrightarrow VY \leftrightarrow Y'}$.*

Security for Bob: *For any $\mathsf{A}' \in \mathfrak{A}$ (with no input), and for any distribution of V, the resulting common output state $\rho_{VX'Y}$ (augmented with V) is such that there exist classical random variables U, X such that $P_{UV} \approx_{\varepsilon} P_U \cdot P_V$, $(U,V,X,Y) \approx_{\varepsilon} (U,V,\mathcal{F}(U,V))$, and $\rho_{VYUXX'} \approx_{\varepsilon} \rho_{VY \leftrightarrow UX \leftrightarrow X'}$.*

The three conditions for dishonest Bob (and similarly for dishonest Alice) express that, up to a small error, V is independent of U, X and Y are obtained by applying $\mathcal{F}$, and the quantum state Y' is obtained by locally processing V and Y.

We would like to point out that Definition 4.1 requires existence of the dishonest party's input, and as such prohibits the dishonest party to execute π in superposition with several inputs and to obtain a superposition of the corresponding outputs. Indeed, it is interesting to note that from a superposition of outputs, the dishonest party can typically extract "forbidden information" [4,

[6] as defined in Section 2.

25].This is another way to see that without any restriction on the adversary, non-trivial quantum two-party computation is not possible [18].

4.2 Equivalent Formulations

As already mentioned, Definition 4.1 appears to guarantee security only in a very restricted setting, where the honest player has no information beyond his input, and the dishonest player has no (auxiliary) information at all. Below, we argue that Definition 4.1 actually implies security in a somewhat more general setting, where the dishonest player is allowed as input to have arbitrary classical information Z as well as a quantum state which only depends on Z. For completeness, although this is rather clear, we also argue that not only the honest player's input is protected, but also any classical "side information" S he might additionally have but does not use.

Proposition 4.2. *Let π be a two-party protocol that ε-securely implements $\mathcal{F}$ against $\mathfrak{A}$ and $\mathfrak{B}$. Let $\mathsf{B}' \in \mathfrak{B}$ be a dishonest Bob who takes as input a classical Z and a quantum state V' and outputs (the same) Z and a quantum state Y'. Then, for any $\rho_{SUZV'}$ with $\rho_{SUZV'} = \rho_{SU \leftrightarrow Z \leftrightarrow V'}$, the resulting overall output state (augmented with S and U) $\rho_{SUXZY'} = \big(\mathrm{id}_{SU} \otimes \pi_{\mathsf{A},\mathsf{B}'}\big)\rho_{SUUZV'}$ is such that there exist classical random variables V, Y such that $P_{SUZV} \approx_\varepsilon P_{SU \leftrightarrow Z \leftrightarrow V}$, $(S, U, V, X, Y, Z) \approx_\varepsilon (S, U, V, \mathcal{F}(U, V), Z)$ and $\rho_{SUXVYZY'} = \rho_{SUX \leftrightarrow VYZ \leftrightarrow Y'}$. The corresponding holds for a dishonest Alice.*

The proof of Proposition 4.2, as well as the proof of Proposition 4.3 below, can be found in the full version [11].

Note the restriction on the adversary's quantum input V', namely that it is only allowed to depend on the honest player's input U (and side information S) "through" Z. It is this limitation which prohibits quantum protocols satisfying Definition 4.1 to securely compose into outer quantum protocols but requires the outer protocol to be classical. Indeed, within a quantum protocol that uses quantum communication, a dishonest player may be able to correlate his quantum state with classical information on the honest player's side; however, within a classical protocol, he can only do so through the classical communication so that his state is still independent when given the classical communication.

The following proposition shows equivalence to a simulation-based definition; this will be a handy formulation in order to prove the composition theorem.

Proposition 4.3. *Let π be a two-party protocol that ε-securely implements $\mathcal{F}$ against $\mathfrak{A}$ and $\mathfrak{B}$. Let $\mathsf{B}' \in \mathfrak{B}$ be a dishonest Bob who takes as input a classical Z and a quantum state V', engages into π with honest Alice and outputs Z and a quantum state Y'. Then, for any $\rho_{SUZV'}$ with $\rho_{SUZV'} = \rho_{SU \leftrightarrow Z \leftrightarrow V'}$ there exists $\hat{\mathsf{B}}'$ such that*

$$\big(\mathrm{id}_S \otimes \pi_{\mathsf{A},\mathsf{B}'}\big)\rho_{SUZV'} \approx_{3\varepsilon} \big(\mathrm{id}_S \otimes \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}\big)\rho_{SUZV'} \,.$$

The corresponding holds for a dishonest Alice.

Recall that $\mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$ is the execution of the "ideal-life" protocol, where honest $\hat{\mathsf{A}}$ relays in- and outputs, and the only thing dishonest $\hat{\mathsf{B}}'$ can do is modify the input and the output. Note that we do not guarantee that $\hat{\mathsf{B}}'$ is in $\mathfrak{B}$; we will comment on this after Theorem 5.1.

5 Composability

We show the following composition result. If quantum protocols $\pi_1, \ldots, \pi_\ell$ securely implement ideal functionalities $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ according to Definition 4.1, then any two-party *classical* hybrid protocol $\Sigma^{\mathcal{F}_1,\ldots,\mathcal{F}_\ell}$ which makes sequential calls to $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ is essentially equally secure as the protocol obtained by replacing the calls to $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ by the respective quantum subroutines $\pi_1, \ldots, \pi_\ell$.

We stress that the $\mathcal{F}_i$'s are *classical* functionalities, i.e., even a dishonest player $\hat{\mathsf{A}}'$ or $\hat{\mathsf{B}}'$ can only input a classical value to $\mathcal{F}_i$, and for instance cannot execute $\mathcal{F}_i$ with several inputs in superposition. This makes our composition result stronger, because we give the adversary less power in the "ideal" (actually hybrid) world.

Theorem 5.1 (Composition Theorem). *Let $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell} = (\hat{\mathsf{A}}, \hat{\mathsf{B}})$ be a classical two-party hybrid protocol which makes at most k oracle calls to the functionalities, and for every $i \in \{1, \ldots, \ell\}$, let protocol π_i be an ε-secure implementation of $\mathcal{F}_i$ against $\mathfrak{A}$ and $\mathfrak{B}$. Then, the following holds.*

Correctness: *For every (distribution of) U and V*

$$\delta\Big(\Sigma_{\mathsf{A},\mathsf{B}}^{\pi_1\cdots\pi_\ell}\rho_{UV}, \Sigma_{\hat{\mathsf{A}},\hat{\mathsf{B}}}^{\mathcal{F}_1\cdots\mathcal{F}_\ell}\rho_{UV}\Big) \leq k\varepsilon\,.$$

Security for Alice: *For every $\mathsf{B}' \in \mathfrak{B}$ there exists $\hat{\mathsf{B}}'$ such that for every U*

$$\delta\Big(\Sigma_{\mathsf{A},\mathsf{B}'}^{\pi_1\cdots\pi_\ell}\rho_{U\emptyset}, \Sigma_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}^{\mathcal{F}_1\cdots\mathcal{F}_\ell}\rho_{U\emptyset}\Big) \leq 3k\varepsilon\,.$$

Security for Bob: *For every $\mathsf{A}' \in \mathfrak{A}$ there exists $\hat{\mathsf{A}}'$ such that for every V*

$$\delta\Big(\Sigma_{\mathsf{A}',\mathsf{B}}^{\pi_1\cdots\pi_\ell}\rho_{\emptyset V}, \Sigma_{\hat{\mathsf{A}}',\hat{\mathsf{B}}}^{\mathcal{F}_1\cdots\mathcal{F}_\ell}\rho_{\emptyset V}\Big) \leq 3k\varepsilon\,.$$

Before going into the proof, we would like to point out the following observations. First of all, note that in contrast to typical composition theorems, which per-se guarantee security when replacing *one* functionality by a sub-protocol and where in case of several functionalities security then follows by induction, Theorem 5.1 is stated in such a way that it directly guarantees security when replacing all functionalities by sub-protocols. The reason for this is that the assumption that the outer protocol is classical is not satisfied anymore once the first functionality is replaced by a quantum sub-protocol, and thus the inductive reasoning does not work directly. We stress that our composition theorem nevertheless allows for several levels of compositions (see Corollary 5.2 and the preceding discussion).

Also, note that in Theorem 5.1 we assume the dishonest party to have no input. As in Section 4.2, this can be relaxed to a dishonest party, say Bob, that has an auxiliary input, consisting of a classical part Z and a quantum part V', as long as the quantum part V' depends on Alice' input U only through Z: $\rho_{UZV} = \rho_{U\leftrightarrow Z\leftrightarrow V}$; i.e., dishonest Bob has only classical side-information on Alice' input. This restriction is motivated by our model which captures a classical world except for specific designated quantum sub-protocols, and as such provides dishonest Bob a priori only with classical side-information.

Furthermore, note that we do not guarantee that the hybrid adversary $\hat{\mathsf{B}}'$ is in $\mathfrak{B}$ (and similarly for $\hat{\mathsf{A}}'$). For instance the specific $\hat{\mathsf{B}}'$ we construct in the proof is more involved with respect to classical resources (memory and computation), but less involved with respect to quantum resources: essentially it follows B', except that it remembers all classical communication and except that the actions during the sub-protocols are replaced by sampling a value from some distribution and preparing a quantum state (of a size that also B' has to handle); the descriptions of the distribution and the state have to be computed by $\hat{\mathsf{B}}'$ from the stored classical communication. By this, natural restrictions on B' concerning its *quantum capabilities* propagate to $\hat{\mathsf{B}}'$. For instance if B' has a quantum memory of bounded size, so has $\hat{\mathsf{B}}'$. Furthermore, in many cases the classical hybrid protocol is actually *unconditionally* secure against classical dishonest players and as such in particular secure against unbounded quantum dishonest players (because every dishonest quantum strategy can be simulated by an unbounded classical adversary), so no restriction on $\hat{\mathsf{B}}'$ is needed.

Finally, note that we do not specify what it means for the hybrid protocol to be secure; Theorem 5.1 guarantees that *whatever* the hybrid protocol achieves, essentially the same is achieved by the real-life protocol with the oracle calls replaced by protocols. But of course in particular, if the hybrid protocol *is* secure in the sense of Definition 4.1, then so is the real-life protocol, and as such it could itself be used as a quantum sub-protocol in yet another classical outer protocol.

Corollary 5.2. *If $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}$ is a δ-secure implementation of $\mathcal{G}$ against $\mathfrak{A}$ and $\mathfrak{B}$, and if π_i is an ε-secure implementation of $\mathcal{F}_i$ against $\mathfrak{A}$ and $\mathfrak{B}$ for every $i \in \{1,\ldots,\ell\}$, then $\Sigma^{\pi_1\cdots\pi_\ell}$ is a $(\delta{+}3k\varepsilon)$-secure implementation of $\mathcal{G}$.*

Proof (of Theorem 5.1). Correctness is obvious. We show security for Alice; security for Bob can be shown accordingly. Consider a dishonest B'. First we argue that for every distribution for Alice's input U, there exists a $\hat{\mathsf{B}}'$ as claimed (which though may depend on P_U). Then, in the end, we show how to make $\hat{\mathsf{B}}'$ independent of P_U.

Let A's input U be arbitrarily distributed. We prove the claim by induction on k. The claim holds trivially for protocols that make zero oracle calls. Consider now a protocol $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}$ with at most $k > 0$ oracle calls. For simplicity, we assume that the number of oracle calls equals k, otherwise we instruct the players to makes some "dummy calls". Let $\rho_{S_k U_k V_k'}$ be the common state right before the k-th and thus last call to one of the sub-protocols $\pi_1,\ldots,\pi_\ell$ in the execution of the real protocol $\Sigma^{\pi_1,\ldots,\pi_\ell}$. To simplify notation in the rest of the proof, we omit the index k and write $\rho_{\bar{S}\bar{U}\bar{V}'}$ instead; see Figure 2. We know from the induction hypothesis for $k-1$ that there exists $\hat{\mathsf{B}}'$ such that $\rho_{\bar{S}\bar{U}\bar{V}'} \approx_{3(k-1)\varepsilon} \sigma_{\bar{S}\bar{U}\bar{V}'}$ where $\sigma_{\bar{S}\bar{U}\bar{V}'}$ is the common state right before the k-th call to a functionality in the execution of the hybrid protocol $\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}\rho_{U\emptyset}$. As described in Section 3, $\bar{S}, \bar{U}$ and $\bar{V}'$ are to be understood as follows. $\bar{S}$ denotes A's (respectively $\hat{\mathsf{A}}$'s) classical auxiliary information to be "remembered" during the call to the functionality. $\bar{U}$ denotes A's (respectively $\hat{\mathsf{A}}$'s) input to the sub-protocol (respectively functionality) that is to be called next, and $\bar{V}'$ denotes the dishonest player's current quantum state. For simplicity, we assume that the index i, which determines the sub-protocol π_i (functionality $\mathcal{F}_i$) to be called next, is *fixed* and we just write π and $\mathcal{F}$ for π_i and $\mathcal{F}_i$, respectively. If this is not the case, we consider $\rho_{\bar{S}\bar{U}\bar{V}'|\bar{I}=i}$ and $\sigma_{\bar{S}\bar{U}\bar{V}'|\bar{I}=i}$ instead, and reason as below for any i, where $\bar{I}$ denotes the index of the sub-protocol (functionality) to be called. Note that conditioning on $\bar{I}=i$ means that we allow $\hat{\mathsf{B}}'$ to depend on i, but this is legitimate since $\bar{I}$ is known to the dishonest party.

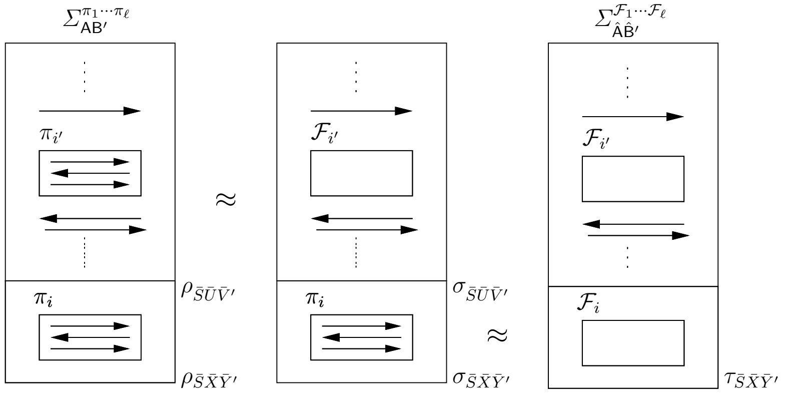
$\Sigma^{\pi_1\cdots\pi_\ell}_{\mathsf{AB}'}$
$\Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}}\hat{\mathsf{B}}'}$
$\pi_{i'}$
$\mathcal{F}_{i'}$
$\mathcal{F}_{i'}$
$\approx$
π_i
π_i
$\mathcal{F}_i$
$\rho_{\bar{S}\bar{U}\bar{V}'}$
$\sigma_{\bar{S}\bar{U}\bar{V}'}$
$\approx$
$\rho_{\bar{S}\bar{X}\bar{Y}'}$
$\sigma_{\bar{S}\bar{X}\bar{Y}'}$
$\tau_{\bar{S}\bar{X}\bar{Y}'}$

Fig. 2. Steps of the Composability Proof

Consider now the evolution of the state $\sigma_{\bar{S}\bar{U}\bar{V}'}$ when executing $\mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$ (as prescribed by the hybrid protocol) with a strategy for $\hat{\mathsf{B}}'$ yet to be determined and when executing $\pi_{\mathsf{A},\mathsf{B}'}$ instead. Let $\sigma_{\bar{S}\bar{X}\bar{Y}'}$ and $\tau_{\bar{S}\bar{X}\bar{Y}'}$ denote the corresponding states after the execution of respectively $\pi_{\mathsf{A},\mathsf{B}'}$ and $\mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}$, see Figure 2. We show that $\sigma_{\bar{S}\bar{X}\bar{Y}'}$ and $\tau_{\bar{S}\bar{X}\bar{Y}'}$ are 3ε-close; this then proves the result by the fact that evolution does not increase the trace distance and by the triangle inequality:

$$\begin{aligned}\rho_{\bar{S}\bar{X}\bar{Y}'} = (\mathrm{id}_{\bar{S}} \otimes \pi_{\mathsf{A},\mathsf{B}'})\,\rho_{\bar{S}\bar{U}\bar{V}'} &\approx_{3(k-1)\varepsilon} (\mathrm{id}_{\bar{S}} \otimes \pi_{\mathsf{A},\mathsf{B}'})\,\sigma_{\bar{S}\bar{U}\bar{V}'} = \sigma_{\bar{S}\bar{X}\bar{Y}'}\\ &\approx_{3\varepsilon} \tau_{\bar{S}\bar{X}\bar{Y}'} = (\mathrm{id}_{\bar{S}} \otimes \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'})\,\sigma_{\bar{S}\bar{U}\bar{V}'}\,.\end{aligned}$$

Let $\sigma_{\bar{S}\bar{U}\bar{Z}\bar{V}'}$, $\sigma_{\bar{S}\bar{X}\bar{Z}\bar{Y}'}$ and $\tau_{\bar{S}\bar{X}\bar{Z}\bar{Y}'}$ be the extensions of the respective states $\sigma_{\bar{S}\bar{U}\bar{V}'}$, $\sigma_{\bar{S}\bar{X}\bar{Y}'}$ and $\tau_{\bar{S}\bar{X}\bar{Y}'}$ when we also consider $\bar{Z}$ (which collects the classical communication dictated by $\Sigma^{\mathcal{F}_1,\ldots,\mathcal{F}_\ell}$ as well as $\hat{\mathsf{B}}'$'s classical inputs to and outputs from the previous oracle calls), which is guaranteed to exist by our formalization of a *classical* hybrid protocol, so that $\bar{Z}$ is without loss of generality contained in $\bar{V}'$ and $\sigma_{\bar{S}\bar{U}\bar{Z}\bar{V}'} = \sigma_{\bar{S}\bar{U}\leftrightarrow\bar{Z}\leftrightarrow\bar{V}'}$. It thus follows from Proposition 4.3 that $\sigma_{\bar{S}\bar{X}\bar{Z}\bar{Y}'}$ and $\tau_{\bar{S}\bar{X}\bar{Z}\bar{Y}'}$ are 3ε-close for a proper strategy of $\hat{\mathsf{B}}'$. Note that the strategy of $\hat{\mathsf{B}}'$ may depend on the state $\sigma_{\bar{S}\bar{U}\bar{Z}\bar{V}'}$, but since P_U as well as $\hat{\mathsf{A}}$'s behavior are fixed, $\sigma_{\bar{S}\bar{U}\bar{Z}\bar{V}'}$ is also fixed.

It remains to argue that we can make $\hat{\mathsf{B}}'$ independent of P_U. We use an elegant argument due to Crépeau and Wullschleger [6]. We know that for any P_U there exists a $\hat{\mathsf{B}}'$ (though depending on P_U) as required. For any value u that U may take on, let then

$$\varepsilon_u = \delta\Big(\Sigma^{\pi_1\cdots\pi_\ell}_{\mathsf{A},\mathsf{B}'} \rho_{U\emptyset|U=u}, \Sigma^{\mathcal{F}_1\cdots\mathcal{F}_\ell}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'} \rho_{U\emptyset|U=u} \Big) .$$

Then, $\sum_u P_U(u)\varepsilon_u = 3k\varepsilon$. The ε_u's depend on P_U, and thus we also write $\varepsilon_u(P_U)$. Consider now the function F which maps an arbitrary distribution P_U for U to a new distribution defined as $F(P_U)(u) := \frac{1+\varepsilon_u(P_U)}{1+3k\varepsilon} P_U(u)$. Function F is continuous and maps a non-empty, compact, convex set onto itself. Thus, by Brouwer's Fixed Point Theorem, it must have a fixed point: a distribution P_U with $F(P_U) = P_U$, and thus $\varepsilon_u(P_U) = 3k\varepsilon$ for any u. It follows that $\hat{\mathsf{B}}'$ which works for that particular distribution P_U in fact works for any specific value for U and so for any distribution of U. □

6 Example: Secure Identification

We show that the information-theoretic security definition proposed by Damgård *et al.* for their secure-identification quantum protocol in the bounded-quantum-storage model [9] implies security in our sense for a proper functionality $\mathcal{F}_{ID}$; this guarantees composability as in Theorem 5.1 for their protocol. In the full version [11] of this paper, we also show the corresponding for the 1-2 OT scheme [7] and for other variants of OT.

A secure identification scheme allows a user Alice to identify herself to server Bob by securely checking whether the supplied password agrees with the one stored by Bob. Specifically, on respective input strings $W_A, W_B \in \mathcal{W}$ provided by Alice and Bob, the functionality outputs the bit $Y = (W_A \overset{?}{=} W_B)$ to Bob. A dishonest server B' should learn essentially no information on W_A beyond that he can come up with a guess W' for W_A and learns whether $W' = W_A$ or not, and similarly a dishonest user A' succeeds in convincing Bob essentially only if she guesses W_B correctly. If her guess is incorrect then the only thing she might learn is that her guess is incorrect. The corresponding ideal functionality is depicted in Figure 3. Note that if dishonest A' provides the "correct" input $W_A = W_B$, then $\mathcal{F}_{ID}$ allows A' to learn this while she may still enforce Bob to reject (by setting the "override bit" D to 0). In [11] we study a slightly stronger variant, which does not allow this somewhat unfair option for A'.[7]

[7] The reason we study here the weaker version is that this corresponds to the security guaranteed by the definition proposed in [9], as we show.

Functionality $\mathcal{F}_{ID}$: Upon receiving strings W_A and W_B from user Alice and from server Bob, $\mathcal{F}_{ID}$ outputs the bit $W_A \overset{?}{=} W_B$ to Bob.

If Alice is dishonest, she may input an additional "override bit" D. Then, $\mathcal{F}_{ID}$ outputs the bit $W_A \overset{?}{=} W_B$ to Alice and the bit $(W_A \overset{?}{=} W_B) \wedge D$ to Bob.

Fig. 3. The Ideal Password-Based Identification Functionality.

We recall the security definition from [9] for a secure identification scheme. The definition is in the framework described in Section 4.1; thus, it considers a single execution of the protocol with an arbitrary distribution for the honest players inputs and with no input for dishonest players, and security is defined by information-theoretic conditions on the resulting output states. For consistency with the above notation (and the notation used in [9]), Alice and Bob's inputs are denoted by W_A and W_B, respectively, rather than U and V. Furthermore, note that honest Alice's output X is empty: $X = \emptyset$.

Definition 6.1 (Secure Identification). *A password-based quantum identification scheme is ε-*secure *(against $\mathfrak{A}$ and $\mathfrak{B}$) if the following properties hold.*

Correctness: *For honest user Alice and honest server Bob, and for any joint input distribution $P_{W_A W_B}$, Bob learns whether their input is equal, except with probability ε.*

Security for Alice: *For any dishonest server $\mathsf{B}' \in \mathfrak{B}$, and for any distribution of W_A, the resulting common output state $\rho_{W_A Y'}$ (augmented with W_A) is such that there exists a classical W' that is independent of W_A and such that*

$$\rho_{W_A W' Y' | W_A \neq W'} \approx_\varepsilon \rho_{W_A \leftrightarrow W' \leftrightarrow Y' | W_A \neq W'} \quad ,$$

Security for Bob: *For any dishonest user $\mathsf{A}' \in \mathfrak{A}$, and for any distribution of W_B, the resulting common output state $\rho_{W_B Y X'}$ (augmented with W_B) is such that there exists a classical W' independent of W_B, such that if $W_B \neq W'$ then $Y = 1$ with probability at most ε, and*

$$\rho_{W_B W' X' | W' \neq W_B} \approx_\varepsilon \rho_{W_B \leftrightarrow W' \leftrightarrow X' | W' \neq W_B} \quad .$$

Proposition 6.2. *A quantum protocol satisfying Definition 6.1 3ε-securely implements the functionality $\mathcal{F}_{ID}$ from Figure 3 according to Definition 4.1.*

Proof. Correctness follows immediately.

Security for Alice: Consider W' which is guaranteed to exist by Definition 6.1. Let us define $V = W'$ and let Y be the bit $W_A \overset{?}{=} W'$. By the requirement of Definition 6.1, W' is independent of Alice's input W_A. Furthermore, we have

$$\big(W_A, W', \emptyset, Y\big) = \big(W_A, W', \mathcal{F}_{ID}(W_A, W')\big)$$

by the definition of $\mathcal{F}_{\mathsf{ID}}$. Finally, we note that Y completely determines the event $\mathcal{E} := \{W_A \neq W'\}$ and therefore, we conclude using Lemma 2.3 that

$$\begin{aligned}
&\rho_{W_A \emptyset W' Y Y'} \\
&\quad = \Pr[W_A \neq W'] \cdot \rho_{W_A \emptyset W' Y Y' | W_A \neq W'} + \Pr[W_A = W'] \cdot \rho_{W_A \emptyset W' Y Y' | W_A = W'} \\
&\quad = \Pr[W_A \neq W'] \cdot \rho_{W_A \emptyset W' Y Y' | W_A \neq W'} + \Pr[W_A = W'] \cdot \rho_{W_A \leftrightarrow W' Y \leftrightarrow Y' | W_A = W'} \\
&\quad \approx_\varepsilon \Pr[W_A \neq W'] \cdot \rho_{W_A \leftrightarrow W' Y \leftrightarrow Y' | W_A \neq W'} + \Pr[W_A = W'] \cdot \rho_{W_A \leftrightarrow W' Y \leftrightarrow Y' | W_A = W'} \\
&\quad = \rho_{W_A \leftrightarrow W' Y \leftrightarrow Y'} .
\end{aligned}$$

Security for Bob: Consider the random variable W' which is guaranteed to exist by Definition 6.1. Let us define U and X as follows. We let $U = (W', D)$ where we define $D = Y$ if $W_B = W'$, and else we choose D "freshly" to be 0 with probability $\Pr[Y = 0 | W_B = W']$ and to be 1 otherwise. Furthermore, we let $X = (W' \overset{?}{=} W_B)$. Recall that by the requirement of Definition 6.1, W' is independent of Bob's input W_B. Furthermore by construction, $D = 0$ with probability $\Pr[Y = 0 | W_B = W']$, independent of the value of W_B (and independent of whether $W_B = W'$ or not). Thus, U is perfectly independent of W_B.

Since by Definition 6.1 the probability for Bob to decide that the inputs are equal, $Y = 1$, does not exceed ε if $W_B \neq W'$, we have that

$$\begin{aligned}
P_{U W_B X Y} &= \Pr[W_B = W'] \cdot P_{U W_B X Y | W_B = W'} + \Pr[W_B \neq W'] \cdot P_{U W_B X Y | W_B \neq W'} \\
&= \Pr[W_B = W'] \cdot P_{U W_B \mathcal{F}_{\mathsf{ID}}(U, W_B) | W_B = W'} + \Pr[W_B \neq W'] \cdot P_{U W_B X Y | W_B \neq W'} \\
&\approx_\varepsilon \Pr[W_B = W'] \cdot P_{U W_B \mathcal{F}_{\mathsf{ID}}(U, W_B) | W_B = W'} + \Pr[W_B \neq W'] \cdot P_{U W_B \mathcal{F}_{\mathsf{ID}}(U, W_B) | W_B \neq W'} \\
&= P_{U W_B \mathcal{F}_{\mathsf{ID}}(U, W_B)} .
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\rho_{W_B Y U X X'} = \Pr[W_B \neq W'] &\cdot \rho_{W_B Y W' D X X' | W_B \neq W'} \\
+ \Pr[W_B = W'] &\cdot \rho_{W_B Y W' D X X' | W_B = W'} .
\end{aligned}$$

In the case $W_B = W'$, we have by construction that $D = Y$ and therefore, we obtain that $\rho_{W_B Y W' D X X' | W_B = W'} = \rho_{W_B Y \leftrightarrow W' D \leftrightarrow X X' | W_B = W'}$. If $W_B \neq W'$, it follows from Definition 6.1 and the fact that D is sampled independently that $\rho_{W_B W' D X' | W' \neq W_B} \approx_\varepsilon \rho_{W_B \leftrightarrow W' D \leftrightarrow X' | W' \neq W_B}$. Furthermore, the bit X is fixed to 0 in case $W_B \neq W'$ and we only make an error of at most ε assuming that Bob's output Y is always 0 and therefore,

$$\begin{aligned}
&\rho_{W_B Y W' D X X' | W_B \neq W'} \approx_\varepsilon \rho_{W_B (Y=0) W' D (X=0) X' | W_B \neq W'} \\
&\quad \approx_\varepsilon \rho_{W_B (Y=0) \leftrightarrow W' D (X=0) \leftrightarrow X' | W_B \neq W'} \approx_\varepsilon \rho_{W_B Y \leftrightarrow W' D X \leftrightarrow X' | W_B \neq W'}
\end{aligned}$$

Putting things together, we obtain

$$\begin{aligned}
\rho_{W_B Y U X X'} \approx_{3\varepsilon} \Pr[W_B \neq W'] &\cdot \rho_{W_B Y \leftrightarrow W' D X \leftrightarrow X' | W_B \neq W'} \\
+ \Pr[W_B = W'] &\cdot \rho_{W_B Y \leftrightarrow W' D \leftrightarrow X X' | W_B = W'} \\
= \rho_{W_B Y \leftrightarrow (W' D) X \leftrightarrow X'} &,
\end{aligned}$$

where we used Lemma 2.1 and 2.3 in the last step.

□

7 Conclusion

We proposed a general security definition for quantum protocols in terms of simple quantum-information-theoretic conditions and showed that quantum protocols fulfilling the definition do their job as expected when used as subroutines in a larger classical protocol. The restriction to classical "outer" protocols fits our currently limited ability for executing quantum protocols, but can also be appreciated in that our security conditions pose *minimal* requirements for a quantum protocol to be useful beyond running it in isolation.

Acknowledgements

We would like to thank Jürg Wullschleger for sharing a draft of [6] and pointing out how to avoid the dependency of the dishonest player in the ideal model from the honest player's input distribution.

References

1. M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 249–260, 2005.
2. M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406. Springer, 2005.
3. M. Ben-Or and D. Mayers. General security definition and composability for quantum and classical protocols, September 2004. `http://arxive.org/abs/quant-ph/0409062`.
4. R. Colbeck. The impossibility of secure two-party classical computation. http://arxiv.org/abs/0708.2843, August 2007.
5. C. Crépeau, G. Savvides, C. Schaffner, and J. Wullschleger. Information-theoretic conditions for two-party secure function evaluation. In *Advances in Cryptology—EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 538–554. Springer, 2006.
6. C. Crépeau and J. Wullschleger. Statistical security conditions for two-party secure function evaluation. In *Third International Conference on Information Theoretic Security (ICITS)*, pages 86–99, 2008.
7. I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2007.
8. I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 449–458, 2005. Full version available at: `http://arxiv.org/abs/quant-ph/0508222v2`.

9. I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer, 2007.
10. I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.
11. S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. `http://arxiv.org/abs/0804.1059`, 2008.
12. O. Goldreich. *Foundations of Cryptography*, volume II: Basic Applications. Cambridge University Press, 2004.
13. D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003. `http://arxiv.org/abs/quant-ph/0105121`.
14. J. v. d. Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Université de Montréal, 1997.
15. J. Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 20–31, 1988.
16. A. Kitaev. Quantum coin-flipping. presented at QIP'03. A review of this technique can be found in `http://lightlike.com/~carlosm/publ`, 2003.
17. R. Koenig, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(140502), Apr. 2007.
18. H.-K. Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.
19. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, April 1997.
20. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997.
21. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2000.
22. R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich (Switzerland), September 2005. `http://arxiv.org/abs/quant-ph/0512258`.
23. R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005.
24. L. Salvail. Quantum bit commitment from a physical assumption. In *Advances in Cryptology—CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 338–353. Springer, 1998.
25. L. Salvail, M. Sotáková, and C. Schaffner. On the power of two-party quantum cryptography. submitted, 2008.
26. A. Smith. Multi-party quantum computation. Master's thesis, MIT, 2001.
27. D. Unruh. Simulatable security for quantum protocols. `http://arxiv.org/abs/quant-ph/0409125`, 2004.
28. S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.
29. S. Wehner and J. Wullschleger. Composable security in the bounded-quantum-storage model. In *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008*, volume 5126 of *Lecture Notes in Computer Science*, pages 604–615. Springer, 2008.