Composability in quantum cryptography

Jörn Müller-Quade\textsuperscript{1} and Renato Renner\textsuperscript{2,3}

\textsuperscript{1} Institut für Kryptographie und Sicherheit, Karlsruhe Institute of Technology, Germany
\textsuperscript{2} Institute for Theoretical Physics, ETH Zurich, Switzerland
E-mail: mueller-quade@kit.edu and renner@phys.ethz.ch

\textit{New Journal of Physics} 11 (2009) 085006 (22pp)
Received 2 March 2009
Published 21 August 2009
Online at \url{http://www.njp.org/}
doi:10.1088/1367-2630/11/8/085006

Abstract. If we combine two secure cryptographic systems, is the resulting system still secure? Answering this question is highly nontrivial and has recently sparked a considerable research effort, in particular, in the area of classical cryptography. A central insight was that the answer to the question is yes, but only within a well-specified \textit{composability framework} and for carefully chosen security definitions.

In this article, we review several aspects of composability in the context of quantum cryptography. The first part is devoted to key distribution. We discuss the security criteria that a quantum key distribution (QKD) protocol must fulfill to allow its safe use within a larger security application (e.g. for secure message transmission); and we demonstrate—by an explicit example—what can go wrong if conventional (non-composable) security definitions are used. Finally, to illustrate the practical use of composability, we show how to generate a continuous key stream by sequentially composing rounds of a QKD protocol.

In the second part, we take a more general point of view, which is necessary for the study of cryptographic situations involving, for example, mutually distrustful parties. We explain the universal composability (UC) framework and state the composition theorem that guarantees that secure protocols can securely be composed to larger applications. We focus on the secure composition of quantum protocols into unconditionally secure classical protocols. However, the resulting security definition is so strict that some tasks become impossible without additional security assumptions. Quantum bit commitment is impossible in the UC framework even with mere computational security. Similar problems arise in the quantum bounded storage model and we observe a trade-off between the UC and the use of the weakest possible security assumptions.

\textsuperscript{3} Author to whom any correspondence should be addressed.
1. Introduction

Provable security, even for complex security applications, is desirable. However, giving one monolithic security proof for a larger cryptosystem is error prone, and a modular design is usually advantageous. But this comes with a major difficulty, namely that security definitions are not generally closed under composition. Therefore, an application may be insecure even if the individual components it consists of are secure. During the past few years, finding solutions to this problem has been a main focus of research in cryptography. This research effort has resulted in the development of frameworks in which security definitions are universally composable.

We review several aspects of composability in the context of quantum cryptography and structure our exposition into two parts. Section 2 considers the security and composability of quantum key distribution (QKD), which is the most prominent application of quantum cryptography. In the second part, starting with section 3, we consider the problem of composability for general security applications.

The reason for this organization of the paper is that for the usual treatment of QKD, one assumes a fixed adversary structure, i.e. Alice and Bob are always honest (in particular, they trust each other), while only a third party with access to the communication channels
is malicious. This avoids many of the problems that arise in the more general considerations outlined in sections 3 through 5, where arbitrary parties may be corrupted.

2. Quantum key distribution (QKD)

2.1. QKD in a nutshell

QKD is the art of distributing a secret key to two distant parties, Alice and Bob, connected by an insecure quantum channel. Technically, a secret key is simply a random bitstring for which there is a certain guarantee that its value is unknown to an adversary, Eve. Such a key may be used for a variety of cryptographic tasks. The most prominent among them is certainly the secure transmission of secret messages over an insecure channel. Here, the key typically serves as a one-time-pad for message encryption.

In the past two decades, numerous QKD schemes have been proposed. Although they differ in many aspects (such as their realizability with current technology), they still very much resemble the original protocols put forward by Bennett and Brassard [5] (based on ideas by Wiesner [44]) and by Ekert [15]. We will not attempt here to give a description of these protocols. In fact, for the purpose of this article, it is sufficient to take a rather abstract point of view, where the internal workings of the protocols are unimportant. (The reader interested in the concrete protocols is referred to the original articles [5, 15] as well as the recent review articles [36] and references therein.)

The security of QKD basically relies on an intrinsic property of quantum mechanics, namely that it is generally impossible to copy the state of a system without disturbing the original. For cryptography, this means that any attempt of an attacker to ‘steal’ appropriately encoded information can, in principle, be detected. This also motivates the basic structure of QKD protocols: first, Alice and Bob send random signals over the quantum channel and then, in a second step, perform tests to check for disturbances in the signals, which may be a sign of an attack. Depending on this test, the protocol typically has one of two different outcomes. Either the disturbances are found to be too large, in which case the protocol aborts with the declaration that no key can be generated. Otherwise, if there are no (or only small) disturbances, Alice and Bob use the randomness in the distributed signals to generate a key.

Although QKD is often said to be unconditionally secure, there are still a few assumptions needed to prove security of the generated keys. The first (usually implicit in the literature) is that Alice and Bob are honest, meaning that they both follow their respective part of the protocol. Secondly, it is assumed that Alice and Bob can exchange classical messages authentically, i.e. it is impossible for an adversary to alter the classical messages exchanged between Alice and Bob. In practice, this is usually achieved by invoking an authentication scheme (see, e.g. [42]), which, however, requires Alice and Bob to share a short initial key. Because of this latter assumption, QKD is sometimes called key growing rather than key distribution.

---

4 More precisely, it is impossible to build a physical device that takes as input an unknown quantum state and outputs two copies of it. This impossibility is also known as non-cloning theorem. For QKD, it is important to have a quantitative version of this statement, sometimes called information-disturbance trade-off.

5 More generally, a protocol may generate keys whose length depends on an estimate of the maximum amount of information that an adversary may have gained by an eavesdropping attack.

6 Dropping this assumption leads to the additional problem of generating randomness by mutually mistrustful parties, which is known as coin flipping [7].

New Journal of Physics 11 (2009) 085006 (http://www.njp.org/)
After this brief introduction, we are now ready to have a closer look at the notion of security used in the context of QKD. We introduce an explicit definition (section 2.2) and then show its composability (section 2.3). As an example, we discuss the problem of generating a continuous key stream by sequentially composing many rounds of a QKD protocol (section 2.4). We then conclude the part on QKD with an example that pinpoints the problems arising when employing a non-composable security definition, which incidentally has been widely used in the literature (section 2.5).

2.2. Security criteria

To define security, we first need to have a clearer picture of what a QKD protocol is supposed to do. We start with a list of the properties we expect an ideal protocol to have and then, in a second step, define security of real protocols by their indistinguishability from the ideal case. In accordance with the terminology used in the context of multi-party computation, we call these properties secrecy, correctness and robustness (see also [21]). We denote by $S_A$ and $S_B$ the final outputs of the protocol on Alice and Bob’s side, respectively. Following the discussion above, the protocol may either generate keys, in which case $S_A$ and $S_B$ are two identical random bitstrings of a certain fixed length $\ell$, or it may abort, in which case we set $S_A = \perp$ and $S_B = \perp$. Furthermore, we denote by $E$ the entire (quantum) system controlled by an adversary. In particular, $E$ contains all the information that the adversary acquires during the run of the protocol.

We consider here the strongest type of security, namely security against general attacks. This means that an adversary may arbitrarily tamper with the signals exchanged between Alice and Bob over the quantum channel. In addition, she may eavesdrop (but not alter) the classical communication. We also introduce the notion of a passive adversary, who does not disturb the quantum communication. Formally, this simply means that the behavior of the quantum channel is described by a fixed noise model. For QKD based on qubit-systems, for instance, the standard is to consider channels that introduce random bit- and phase-flips (with a given probability).

2.2.1. Perfect security. We now say that a QKD scheme is perfectly secure if the following holds for any attack.

**Correctness:** The outputs of the protocol on Alice and Bob’s side are identical (i.e. $S_A = S_B$).

**Secrecy:** If the protocol produces a key $S_A$ (i.e. if $S_A \neq \perp$) then $S_A$ is uniformly distributed and independent of the state of the system $E$ held by the adversary.

**Robustness:** If the adversary is passive then a key is generated (i.e. $S_A \neq \perp$).

Alternatively, the length $\ell$ of the generated key may be determined during the run of the protocol, with $\ell = 0$ if the protocol aborts (see, e.g. [3]). For practical applications, however, it is usually more convenient to work with a fixed key length.

One sometimes restricts the security analysis to more restricted types of attacks. An example is collective attacks [6], where it is assumed that the adversary acts on each of the signals sent through the channel independently and identically. For most protocols, security against collective attacks implies security against general attacks [31, 32].

Because of the correctness property, it is sufficient to require secrecy for either $S_A$ or $S_B$.

Note that this property is always relative to a given noise model of the quantum channel.
It is easy to see that none of these criteria can be dropped without making the task trivial. In fact, without the correctness requirement, a protocol may just produce uncorrelated randomness on Alice and Bob’s side. Similarly, without the robustness requirement, a protocol may always output $S_A = S_B = \perp$.

### 2.2.2. Approximate security.

Unfortunately, it is (provably) impossible to design a QKD protocol that is perfectly secure according to the above definition. One thus typically considers a relaxation where the requirement is that the behavior of the scheme is similar (but not necessarily equal) to an idealized scheme that is perfectly secure. This can be made precise using the notion of indistinguishability.

More specifically, one considers a hypothetical device, called distinguisher, which interacts with either the real protocol, in the following denoted $P_{\text{real}}$, or an ideal protocol, $P_{\text{ideal}}$, and then outputs a guess bit $B$. The distinguisher may have access to all regular inputs and outputs of the protocol (in our case, we only have outputs, namely $S_A$ and $S_B$) as well as to the system $E$ normally controlled by the adversary. We say that $P_{\text{real}}$ and $P_{\text{ideal}}$ are $\varepsilon$-indistinguishable for $\varepsilon \geq 0$ if, for any such distinguisher,

$$\Pr[B = 1 | P_{\text{real}}] - \Pr[B = 1 | P_{\text{ideal}}] \leq \varepsilon.$$  

(1)

Here $\Pr[B = 1 | P_{\text{real}}]$ and $\Pr[B = 1 | P_{\text{ideal}}]$ denote the probabilities that the distinguisher’s output $B$ equals 1 when interacting with $P_{\text{real}}$ and $P_{\text{ideal}}$, respectively.

The notion of $\varepsilon$-indistinguishability naturally leads to the following definition of $\varepsilon$-security.

**Definition 1.** A QKD protocol $P_{\text{real}}$ is $\varepsilon$-secure if it is $\varepsilon$-indistinguishable from a (hypothetical) protocol $P_{\text{ideal}}$ which is perfectly secure, i.e. $P_{\text{ideal}}$ satisfies the correctness, the secrecy and the robustness criteria above.

Intuitively, the parameter $\varepsilon$ can be understood as the maximum failure probability of the protocol $P_{\text{real}}$, i.e. the maximum probability that $P_{\text{real}}$ deviates from the behavior of the ideal protocol $P_{\text{ideal}}$. For practical considerations, it is often useful to quantify the correctness, secrecy and robustness of a protocol separately. The following definition is an obvious generalization of the above.

**Definition 2.** A QKD protocol is $\varepsilon$-correct, $\varepsilon$-secret, or $\varepsilon$-robust if it is $\varepsilon$-indistinguishable from a perfectly correct, secure, or robust scheme, respectively.

**Remark 3.** One can show that, if a protocol is $\varepsilon_c$-correct, $\varepsilon_s$-secret and $\varepsilon_r$-robust then it is $\varepsilon$-secure, for $\varepsilon = \varepsilon_c + \varepsilon_s + \varepsilon_r$.

The requirements of the different parameters are generally quite diverse. Typically, a relatively large value $\varepsilon_r$ for the robustness (e.g. $\varepsilon_r = 0.1$) can be tolerated, because the protocol may just be repeated in case it does not generate a key. In contrast, the parameter $\varepsilon_s$ for the secrecy can be interpreted as the (maximum) probability by which an adversary may get secret information without being detected, which one typically wants to keep small (e.g. $\varepsilon_s = 10^{-10}$).

It is easy to see that $\varepsilon$-correctness is equivalent to the requirement that the outputs $S_A$ and $S_B$ produced by the protocol on Alice and Bob’s side differ only with small probability,

$$\Pr[S_A \neq S_B] \leq \varepsilon.$$  

(2)

\[11\] This intuition can be made precise in a purely classical context [25].
Similarly, for $\varepsilon$-robustness, the requirement is that
\[ \Pr[S_A = \bot] \leq \varepsilon \] 
holds whenever the adversary is passive. The situation is a bit more subtle (and more interesting) for the secrecy criterion, which can be made more concrete as follows.

Let $S := \{0, 1\}^{\ell}$ be the key space, i.e. the output $S_A$ takes values in the set $S \cup \{\bot\}$. Furthermore, for any fixed value $s \in S \cup \{\bot\}$ of $S_A$, let the state of the system $E$ be denoted by $\rho_E$. The joint state of $S_A$ and $E$ can then be represented as a cq-state:

\[ \rho_{S_AE} = \sum_{s \in S \cup \{\bot\}} p_s |s\rangle\langle s| \otimes \rho_E^s, \]

where $p_s$ is the probability that $S_A = s$ and where $\{|s\rangle\}_{s \in S \cup \{\bot\}}$ is a family of orthonormal vectors.

It is easy to see that, for any attack, the state resulting from the run of a perfectly secure scheme has the form

\[ \rho_{S_AE}^\text{perfect} = (1 - p_{\bot}) \sum_{s \in S} \frac{1}{|S|} |s\rangle\langle s| \otimes \rho_E^s + p_{\bot} |\bot\rangle\langle \bot| \otimes \rho_E^{\prime\prime}, \]

where $p_{\bot} \in [0, 1]$ and where $\rho_E^s$ and $\rho_E^{\prime\prime}$ are density operators. With these definitions, we arrive at a reformulation of $\varepsilon$-secrecy in terms of the trace distance.

Lemma 4. A QKD protocol is $\varepsilon$-secret if and only if, for any attack, the cq-state $\rho_{S_AE}$ describing the joint state of the protocol output $S_A$ and the system $E$ held by the adversary satisfies

\[ \frac{1}{2} \| \rho_{S_AE} - \rho_{S_AE}^\text{perfect} \|_1 \leq \varepsilon \]

for some state $\rho_{S_AE}^\text{perfect}$ of the form (4).

In security proofs, correctness and secrecy are usually established by separate arguments. While the correctness parameter $\varepsilon_c$ is essentially determined by the quality of the error correction procedure used to reconcile the raw keys, the secrecy $\varepsilon_s$ rests upon various other elements of the protocol. In the simplest case, $\varepsilon_s$ is a function of the accuracy of the estimation procedure, which measures the disturbances of the transmitted signals, as well as of the parameters of the privacy amplification step, which is used to transform the (partially secret) raw key into a final secret key satisfying (5).

2.3. Composing QKD with other cryptographic primitives

Since a secret random string is of little interest by itself, QKD is almost never used as a stand-alone application. Instead, one typically is interested in higher cryptographic tasks such as secure message transmission. QKD then just serves as a mechanism to provide the key material needed by the application. In addition, QKD often is built on top of other cryptographic primitives such as authentication schemes, whose task is to make sure the adversary cannot alter the classical messages sent over the insecure channel. Hence, composability of the underlying security definitions is vital in the context of QKD.

---

12 The state of a bipartite system is called classical–quantum (cq) if the first subsystem is purely classical (in the sense that its states are perfectly distinguishable).

13 Lemma 4 is an immediate consequence of the well-known one-to-one relation between the indistinguishability of two quantum states and their trace distance.
2.3.1. What does composability mean? To get a more precise understanding of the notion of composability in the context of QKD, we consider a situation where the key produced by a QKD protocol $\mathcal{P}_{\text{real}}$ is later used in an application $\mathcal{A}_{\text{real}}$, e.g. an encryption scheme. Assume that the protocol $\mathcal{P}_{\text{real}}$ is $\varepsilon_1$-secure, and let the application $\mathcal{A}_{\text{real}}$ be $\varepsilon_2$-secure, i.e. $\varepsilon_2$-indistinguishable from an idealized application $\mathcal{A}_{\text{ideal}}$. The claim then is that the composite system, denoted $\mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{real}}$, where the application $\mathcal{A}_{\text{real}}$ is fed with the key produced by $\mathcal{P}_{\text{real}}$, is $\varepsilon$-secure, for $\varepsilon = \varepsilon_1 + \varepsilon_2$.

The claim becomes even simpler in the special case where $\mathcal{A}_{\text{real}}$ is based on one-time-pad encryption. When being fed with a perfectly secret key, one-time-pad encryption is indistinguishable from a perfect encryption procedure, which simply produces a ciphertext that is statistically independent of the message. We thus have $\varepsilon_2 = 0$. Hence, according to the above claim, when one-time-pad encryption is combined with an $\varepsilon_1$-secure QKD protocol $\mathcal{P}_{\text{real}}$, the resulting scheme is $\varepsilon_1$-secure. That is, it produces ciphertexts which are $\varepsilon_1$-indistinguishable from uniform randomness.

2.3.2. Why is our definition composable? Roughly speaking, the security parameters $\varepsilon_1$ and $\varepsilon_2$ can be understood as the maximum failure probabilities of $\mathcal{P}_{\text{real}}$ and $\mathcal{A}_{\text{real}}$, respectively (see the paragraph after definition 1). Hence, according to the union bound, if one combines $\mathcal{P}_{\text{real}}$ and $\mathcal{A}_{\text{real}}$, the total failure probability cannot be larger than $\varepsilon = \varepsilon_1 + \varepsilon_2$. This already gives an intuitive understanding of why the combined scheme $\mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{real}}$ is $\varepsilon$-secure, as claimed above.

We will now give a slightly more rigorous argument for this claim. Assume by contradiction that the composite system $\mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{real}}$ is not $\varepsilon$-indistinguishable from $\mathcal{A}_{\text{ideal}} \circ \mathcal{P}_{\text{ideal}}$, i.e. there exists a distinguisher $\mathcal{D}$ whose output $B$ satisfies

$$\Pr[B = 1 | \mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{real}}] - \Pr[B = 1 | \mathcal{A}_{\text{ideal}} \circ \mathcal{P}_{\text{ideal}}] > \varepsilon = \varepsilon_1 + \varepsilon_2 \tag{6}$$

(cf equation (1)). Assume now that we use the same distinguisher $\mathcal{D}$ to distinguish $\mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{real}}$ from $\mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{ideal}}$, where the latter denotes the composite scheme consisting of the real application fed with a key produced by a perfect QKD scheme. Because $\mathcal{A}_{\text{real}}$ is identical in both cases, we can alternatively treat $\mathcal{A}_{\text{real}}$ as part of a (more complex) distinguisher $\mathcal{D}'$ which now interacts with either $\mathcal{P}_{\text{real}}$ or $\mathcal{P}_{\text{ideal}}$ (see figure 1). Because, by assumption, $\mathcal{P}_{\text{real}}$ is $\varepsilon_1$-secure and, hence, $\varepsilon_1$-indistinguishable from $\mathcal{P}_{\text{ideal}}$, we find

$$\Pr[B = 1 | \mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{real}}] - \Pr[B = 1 | \mathcal{A}_{\text{real}} \circ \mathcal{P}_{\text{ideal}}] \leq \varepsilon_1 \tag{7}$$
Figure 2. Generation of a continuous key stream by sequential composition of rounds of a QKD protocol. The scheme starts with an initial key pair $S^0 = (S^0_A, S^0_B)$. In each round $i$, the QKD protocol $P_i$ generates a fresh pair $S^i = (S^i_A, S^i_B)$ of keys of length $\ell + \ell_i$, using $\ell_{i-1}$ bits of existing key material for authentication. $\ell$ bits of the fresh key are added to the key stream, whereas $\ell_i$ bits are passed to the next round for authentication.

Similarly, because $A^{\text{real}}$ is $\varepsilon$-indistinguishable from $A^{\text{ideal}}$, we find

$$\Pr[B = 1 | A^{\text{real}} \circ P^{\text{ideal}}] - \Pr[B = 1 | A^{\text{ideal}} \circ P^{\text{ideal}}] \leq \varepsilon_2.$$ (8)

Combining (7) and (8) contradicts (6) and, hence, concludes our proof of composability.

2.4. Example application: generating a continuous key stream

As already mentioned, composability of the keys produced by a QKD scheme is crucial because these are typically used in further applications. Here, we consider their use for authentication in subsequent rounds of a QKD protocol. The method described below can be employed to generate a continuous stream of key material. This may be of interest for various practical applications, such as the encryption of a continuous stream of data.

2.4.1. Description of the scheme. We are looking at the (realistic) situation where the communication channels connecting Alice and Bob may be completely insecure, so that not even authenticity is guaranteed. Instead, we assume that Alice and Bob hold an initial key pair $(S^0_A, S^0_B)$ of length $\ell_0$ which is $\varepsilon_0$-secure. They then repeat the following for any $i \in \mathbb{N}$ (see figure 2). A QKD protocol $P_i$ is invoked, which uses the first $\ell_{i-1}$ bits of the key pair $(S^i_{A^{-1}}, S^i_{B^{-1}})$ for authentication. The protocol generates a new (longer) key pair $(S^i_A, S^i_B)$ of length $\ell_i + \ell$, of which the first $\ell_i$ bits are stored for use in the next round, while the last $\ell$ bits form part of the output stream.

2.4.2. Security analysis. In the following, we are going to analyze the security of the key stream. Because of composability, this is conceptually very easy—we simply need to add up the security parameters. If the protocol $P_i$ executed in each round $i$ is $\varepsilon_i$-secure then the security $\varepsilon$ of the final stream is always bounded by

$$\varepsilon \leq \sum_{i=0}^{\infty} \varepsilon_i.$$ (9)

In order to get a reasonable value for $\varepsilon$, we need to make sure that the parameters $\varepsilon_i$ are sufficiently small. However, making $\varepsilon_i$ small generally comes at the cost of increasing the communication complexity of the protocol as well as the length $\ell_{i-1}$ of the initial key used for
authentication. As a rough estimate of the performance of a typical QKD protocol, we use here a bound of the form

$$\varepsilon_i \leq e^{-\gamma(n_i - \ell_i - \ell)} + e^{-\nu\ell_i + \log n_i},$$

(10)

where \(n_i\) denotes the number of quantum signals exchanged during the protocol and where \(\gamma, \rho,\) and \(\nu\) are positive constants. The first term corresponds to the security of the protocol if used with an authentic classical channel. Note that the exponent critically depends on the length \(\ell_i + \ell\) of the key that is generated. The second term is due to the imperfectness of the authentication scheme.

To make sure that (9) converges, it is necessary to increase the number \(n_i\) of exchanged signals in each round of the protocol. For the purpose of illustration, we set

$$n_i := n + ci \quad \text{and} \quad \ell_i := \ell + c \rho_i / 2$$

for some constants \(n \in \mathbb{N}\) and \(c > 0\). Inserting this into (10) results in a bound on \(\varepsilon_i\) such that the sum over \(i\) is a geometric series. Hence, by appropriately choosing the constants \(\ell, n\) and \(c\), the security parameter \(\varepsilon\) of the key stream can be made arbitrarily small.

2.5. An explicit attack exploiting non-composability

The necessity of composable security definitions has only been realized recently. In fact, most of the original security proofs proposed in the literature were relative to a security criterion that is not composable. The main purpose of this section is to illustrate what can go wrong if such a non-composable security definition is used.

2.5.1. Measuring secrecy. As we have seen in section 2.2, the correctness and the robustness property are rather unproblematic. In particular, both of them can be expressed as the condition that certain probabilities are small (cf equations (2) and (3)). This is different for the secrecy property. Intuitively, a key \(S_A\) is secret if an adversary has only little information about it, in the sense of (5). There are, however, a variety of alternative information measures, and this is indeed the source of the problem we are going to describe now.

One such information measure is the accessible information, denoted \(I_{\text{acc}}(\cdot : \cdot)\). It is particularly suitable to quantify the information a quantum system (in our case the system \(E\) held by the adversary) gives about a classical value (the key \(S_A\)). The accessible information is defined in terms of the Shannon mutual information, \(I(\cdot : \cdot)\),

$$I_{\text{acc}}(S_A : E) := \max_Z I(S_A : Z),$$

where the maximum is taken over all random variables \(Z\) that can be obtained by measuring the quantum system \(E\).

Recall that, according to lemma 4, the key \(S_A\) generated by a QKD protocol is \(\varepsilon\)-secret if and only if

$$\frac{1}{2} \|\rho_{S_A E} - \sum_s \frac{1}{|S|} |s\rangle \langle s| \otimes \rho'_E\|_1 \leq \varepsilon$$

(11)

\footnote{Values of \(\rho = 10^{-2}\) and \(\nu = \nu = 10^{-3}\) may be realistic for textbook protocols such as BB84 with single photons. We refer to [8, 37] for a more detailed numerical analysis of the performance of QKD protocols.}

\footnote{The example should be understood as a proof of principle. We have not attempted to optimize parameters.}
holds for some $\rho'_E$. (We assume here for simplicity that the protocol always outputs a key, i.e. $p_\perp = 0$.) Since a measurement cannot increase the trace distance, this immediately gives a bound on the distance between the joint distribution $P_{S_AZ}$ of the key $S_A$ and the outcome $Z$ of any measurement applied to $E$, and a distribution of the form $P_S \times P'_Z$, where $P_S$ denotes a uniform distribution over the key space,

$$\frac{1}{2}\|P_{S_AZ} - P_U \times P'_Z\|_1 \leq \varepsilon. \tag{12}$$

For small values of $\varepsilon$, Fano’s inequality implies that $I(S : Z)$ and, hence, the accessible information $I_{acc}(S_A : E)$, is small, too\footnote{More precisely, (11) implies $I_{acc}(S_A : E) \leq 2n\varepsilon + 4h(\varepsilon)$, where $n$ is the key length and $h$ is the binary entropy. (Since $\varepsilon$ is usually chosen exponentially small in $n$, the same is true for the term $2n\varepsilon$.)}. In other words, the secrecy criterion (11) is at least as strong as a criterion based on the accessible information.

The converse, however, is not true. To illustrate this, we construct an explicit example quantum state $\rho_{S_AE}$ for which the accessible information is (arbitrarily) small, whereas the key $S_A$ is insecure when being used for one-time pad encryption. The state $\rho_{S_AE}$ thus necessarily violates the (composable) secrecy criterion (11). From this, we conclude that small accessible information does not imply secrecy in the sense of definition 2.

2.5.2. Construction of the example. Our example consists of a uniformly distributed $(n + 1)$-bit key $S_A = (S_1, \ldots, S_{n+1})$ and an $n$-qubit system $E$. Furthermore, we consider an $n$-tuple of bits $R = (R_1, \ldots, R_n)$ whose sum modulo 2 equals $S_{n+1}$,

$$R_1 \oplus \cdots \oplus R_n = S_{n+1}, \tag{13}$$

but which are otherwise completely random. Then, for any fixed $S_A = s = (s_1, \ldots, s_n, s_{n+1})$ and $R = r = (r_1, \ldots, r_n)$ satisfying (13), we define the state $|\phi^{s,r}\rangle$ of $E$ by

$$|\phi^{s,r}\rangle := |r_1\rangle_{s_1} \otimes \cdots \otimes |r_n\rangle_{s_n},$$

where $|r_i\rangle_{s_i}$, for any $i = 1, \ldots, n$, denotes the state of a qubit encoding the classical bit $r_i$ in either some specified standard basis $\{|0\rangle, |1\rangle\}$ (if $s_i = 0$) or the corresponding diagonal basis (if $s_i = 1$), i.e.

$$|0\rangle_0 = |0\rangle, \quad |1\rangle_0 = |1\rangle, \quad |0\rangle_1 = \sqrt{\frac{1}{2}}(|0\rangle + |1\rangle), \quad |1\rangle_1 = \sqrt{\frac{1}{2}}(|0\rangle - |1\rangle).$$

In particular, the density operator $\rho_E^s$ describing the state of $E$ conditioned on $S_A = s$ (but randomized over $R$) is given by

$$\rho_E^s = 2^{-(n-1)} \sum_{(r_1, \ldots, r_n) \atop r_1 \oplus \cdots \oplus r_n = s_{n+1}} |\phi^{s,r}\rangle \langle \phi^{s,r}|.$$
2.5.3. Small accessible information. We do not attempt here to give a rigorous proof of the above claim but rather describe the intuition for it. For the details of the argument we refer to [22].

In order to prove that $I_{\text{acc}}(S_A : E)$ is small, we need to argue that any outcome $Z$ of a measurement applied to $E$ has only negligible correlation with $S_A$. To simplify this task, we split $S_A = (S_1, \ldots, S_n)$ into two parts and make use of the chain rule for the mutual information,

$$I(S_A : Z) = I(S_1 \cdots S_n : Z) + I(S_{n+1} : Z|S_1 \cdots S_n).$$

Note that the state of each qubit of $E$ is an encoding of a random bit $R_i$, where only the basis depends on $S_i$. The overall state of $E$ conditioned on $(S_1, \ldots, S_n)$ is thus fully mixed and, hence, independent of the value of $(S_1, \ldots, S_n)$. This immediately implies $I(S_1 \cdots S_n : Z) = 0$ and it thus remains to be shown that $I(S_{n+1} : Z|S_1 \cdots S_n)$ is small.

For this, let us first assume that the measurement giving $Z$ consists of $n$ independent measurements applied to the individual qubits of $E$. Each of them would then result in an estimate for the value of a bit $R_i$, for $i = 1, \ldots, n$. However, since each bit $R_i$ is encoded in a random basis determined by $S_i$, and since the bit $S_i$ is unknown at the time of the measurement, the maximum probability $p$ of obtaining the correct outcome $R_i$ is bounded away from 1, i.e. $p < 1$.

Now, recall that the key bit $S_{n+1}$ is equal to the sum modulo 2 of the random bits $R_1, \ldots, R_n$. Hence, using the measurement strategy described above, the correct value of $S_{n+1}$ can only be obtained if all the individual measurements are successful. The probability that this happens can be shown to be exponentially small in $n$.[17] We thus conclude that the correlation between the key bit $S_{n+1}$ and the measurement outcome $Z$ is small.

This argument can be generalized to arbitrary measurement strategies [22]. It turns out that the above individual strategy is essentially optimal, i.e. $I(S_{n+1} : Z|S_1 \cdots S_n)$ is small for any measurement. In fact, a quantitative analysis[18] (for a slightly modified example) gives

$$I(S_A, Z) < 2^{-(n-2)/\theta}$$

and, hence, $I_{\text{acc}}(S_A : E) \leq 2^{-(n-2)/\theta}$.

2.5.4. The attack. Let us now have a look at what happens if we use the key $S_A = (S_1, \ldots, S_{n+1})$ for one-time-pad encryption. By definition, for any message $M = (M_1, \ldots, M_{n+1})$, the ciphertext $C = (C_1, \ldots, C_{n+1})$ is given by $C_i = M_i \oplus S_i$. In the following, we assume that the adversary has full access to $C$.

To understand the relevance of the example, it is important to realize that we can, in general, not assume that the message $M$ is uniformly distributed[19]. To the contrary, almost any realistic message will consist of biased bits or bits that are (partially) known to an adversary. In fact, the history of cryptography is full of examples where prior knowledge about the structure of the messages has been exploited for attacks. For our specific attack, we consider the extreme case where the adversary already knows the first $n$ message bits $(M_1, \ldots, M_n)$ but tries to get

[17] More precisely, given $Z$, the probability of correctly guessing $S_{n+1}$ is not larger than the probability of guessing an independent random bit, except with probability exponentially small in $n$.

[18] For technical reasons, the argument of [22] is based on an extended construction where the bits $R_i$ are encoded with respect to three (rather than two) different mutually unbiased bases.

[19] It is possible to design encryption schemes whose security is based on the additional assumption that the distribution of the messages is highly random from the adversary’s point of view [34] (this is also known as entropic security). Interestingly, these schemes only require a short key.
information about the bit $M_{n+1}$. For example, the first $n$ bits may contain standardized header information, while the actual message starts with the $(n+1)$th bit.

Given the first $n$ bits of both the message and the ciphertext, the adversary can obviously determine the first $n$ key bits $S_1, \ldots, S_n$ by $S_i = M_i \oplus C_i$. This by itself would not be problematic because, after all, the very nature of a one-time-pad is that it is only used once. However, the adversary may now use her knowledge of $S_1, \ldots, S_n$ to extract further information from the quantum system $E$. More precisely, because by construction the bits $S_1, \ldots, S_n$ determine the basis in which the values $R_i$ are encoded in $E$, the adversary can apply a measurement that produces the outcomes $R_1, \ldots, R_n$. From this, she may determine the $(n+1)$th key bit $S_{n+1} = R_1 \oplus \cdots \oplus R_n$ and, in particular, the message bit $M_{n+1} = S_{n+1} \oplus C_{n+1}$ with certainty.

2.5.5. Discussion. Our example shows that the accessible information is an inappropriate measure for quantifying secrecy: even though the accessible information $I_{\text{acc}}(S_A; E)$ that an adversary has on the key $S_A$ is small, the key $S_A$ cannot safely be used for tasks such as one-time-pad encryption.

The example also answers a question raised by Ben-Or et al in [3]. They have shown that a QKD protocol that generates an $n$-bit key $S_A$ is $\epsilon$-secure whenever

$$I_{\text{acc}}(S_A; E) \leq 2^{-(n+2)\epsilon^2}.$$ 

An immediate implication of our argument above is that this result is essentially tight. In other words, in order to get (composable) security from a bound on $I_{\text{acc}}(S_A; E)$, this bound must be exponentially small in the key size. Unfortunately, however, this criterion is not met by most known security proofs that refer to the accessible information (see [22] for references).

In order to prove security of a given QKD scheme, it is thus more advisable to directly derive a bound on the trace distance in (11) (rather than on the accessible information). Such a bound can, for instance, be obtained by a modification of the well-known argument by Shor and Preskill [38], which applies to protocols based on qubits. A more generic approach is the use of more recent results on privacy amplification. As shown in [33], the output of an appropriately chosen hash function satisfies (11), provided it is applied to a raw key with sufficiently high entropy.

3. Composability of general secure applications

In the following sections, which constitute the second part of the article, we consider security definitions for general cryptographic tasks and the problem of composing secure protocols to complex security applications.

We will describe a quantum model of security [4, 41], which gives strong composability guarantees. The composition theorem (see section 5.1) states that a protocol secure in this model can be used in an arbitrary application without lowering the overall security. Furthermore an arbitrary number of protocols proven secure in this model can be used concurrently and remain secure in the model. We will have to neglect many details (already [9] has 128 pages and describes the classical case). Our treatment will be on a more intuitive and abstract level. For details please see [4, 41].

One could argue that this topic need not be discussed in an article about quantum cryptography as the most important building blocks of general applications, i.e. protocols.
like coin flipping, bit commitment, or oblivious transfer, can in quantum cryptography not be achieved with unconditional security \[1, 24, 26\]. However, there still are enough interesting applications for quantum cryptography. Even if some tasks are impossible to achieve, in principle, it is possible to achieve them relative to security assumptions that are independent of the computational assumptions of classical cryptography \[13, 35\]. Furthermore, many of the assumptions possible, like the adversary being able to store only a limited amount of qubits or the adversary being unable to maintain coherency for large quantum states, are very reasonable.

In addition, a quantum model of security is not only useful to analyze or prove the security of quantum protocols, but it can also be used to investigate the security of classical protocols against quantum adversaries. It was in the context of composability that the question of whether quantum attacks on classical protocols give more power to the adversary than a mere speed up of computations was answered \[40\] (see section 5.5).

4. Defining security

Key exchange and secure message transmission are one of the most important prerequisites of general security applications; however, general applications can require further security properties. As examples consider secure authentication, digital signatures, online banking, or remote voting. One of the big differences of such applications from key exchange is that the protocol participants are mutually mistrusting. Secure function evaluation \[16, 45\] is a generalization of such cryptographic applications: in a secure function evaluation a set of players \(P_1, \ldots, P_n\) wishes to evaluate a function \(f\) on inputs \(x_1, \ldots, x_n\) they hold, respectively, such that corrupted players cannot change the outcome of the computation (other than choosing a different input) and corrupted players do not learn more about the input of honest players than can be derived from their own input and the output of the function evaluation. These two properties of secure function evaluation are called correctness and privacy. However, it turned out that these two properties alone do not cover what one intuitively requires from a secure computation. Additional properties were added, like the independence of inputs, which demands that it should not be possible for a corrupted player to choose his own input dependent on the secret inputs of honest parties. It is easy to see that the property of independence of inputs is not logically implied by privacy or correctness if one does not demand that each protocol participant knows its input from the start. There are more security properties that are not implied by privacy and correctness: robustness requires that no corrupted player may abort the protocol, fairness demands that even if an abort cannot be prevented it should not be possible for the adversary to learn more about the result of the computation than the honest players, and zero knowledge is the property that a real protocol transcript could also have been generated by a single machine without knowledge of any secret involved in the protocol. Defining security via a list of security properties became known as the list approach; however, researchers got the impression that one might never know if the list of security properties is complete.

4.1. The simulation paradigm

A new security definition was needed. It should be convincing and (as general applications are to be considered) independent of the specific goals the attacker might have. The first step towards
this new definition was the discovery of zero knowledge proofs [17] where the simulation paradigm was introduced.

Instead of considering different security properties the new notion was based on indistinguishability. Intuitively speaking, a real protocol is compared to an ideal protocol where a trusted party collects the inputs from the protocol participants, computes the output and distributes the output to the participants. If the real protocol and the ideal protocol have an indistinguishable input–output behavior the real protocol is said to be at least as secure as the ideal protocol. Such a definition of security defines security of a real protocol relative to an idealization. The level of security reached thus also depends on the specification of the ideal protocol.

In the case of QKD, we have already seen a security definition that compares a real key exchange with an ideal situation; however, in contrast to the general case it was possible to reduce this security notion to the fulfillment of separate security properties (see section 2.2).

In the real model, the protocol is attacked by a real attacker which may corrupt protocol participants, pools all their data and lets the corrupted participants deviate from the protocol in an arbitrary way. In the ideal protocol there is an ideal attacker (also called a simulator) which must be able to provide an output indistinguishable from the output of the real attacker while having access only to the inputs and outputs of the corrupted players. As the ideal attacker does not learn any real protocol messages or secrets that cannot be derived from the input and output of the corrupted players the indistinguishability guarantees that the real protocol does not leak any secrets to the real attacker.

However, there are certain ‘attacks’ that cannot be prevented, e.g. an adversary could replace his input by a different value. These inevitable attacks are not considered to violate the security and hence we must be able to model these attacks in the ideal protocol as well. These inevitable attacks will be carried out by the simulator, too. The ideal attacker may corrupt protocol participants in the ideal model, but all the ideal attacker can do is to replace local inputs or to replace local outputs. If the real attacker may corrupt more than a minority of the protocol participants then the attacker can always abort the computation and we have to give this ability to the ideal adversary as well.

Stating the exact definition here goes beyond the scope of this article (it can be found in [16]), especially because this notion of security does not yet allow for composition as we will illustrate below.

Note that this definition of security requires the ideal attacker (simulator) to provide his output only after termination of the protocol, i.e. in retrospect and thus with the benefit of hindsight. This gives a certain ‘advantage’ to the ideal attacker without which a simulation would become impossible in most cases. The ability to provide a simulation of a real protocol without any advantage over a real attacker would in many cases imply the complete insecurity of the real protocol as the real attacker could use the program of the simulator to cheat in the real execution of the protocol. What is important in this context is that this advantage of the simulator should not invalidate the ‘idealness’ of the ideal model.

This simulation in retrospect does not violate the ‘idealness’, because the result of an ideal protocol is not altered by this (the protocol remains correct) and no secrets of honest participants are leaked. However, as we will see in section 4.3, this ability of simulating in retrospect does not play well with composition or with protocols that accept inputs not only at the start but also at later times (protocols realizing so-called reactive functionalities, which are a generalization of secure function evaluation).
4.2. A motivating example: secure composition as a problem

Below we will give two examples illustrating what can happen when protocols are composed. The first is a classical example from classical cryptography where a message from one subprotocol of a larger application is fed into another subprotocol and the overall application becomes insecure. The second example shows that quantum information can be used in different subprotocols such that entanglement spans over different subprotocols.

4.2.1. Malleability—a classical example. A very simple example of this kind is an (simplified) auction protocol. We assume a trusted auctioneer in possession of a RSA public key \((n, e)\). For an auction, the auctioneer accepts bids which are encrypted with his public key. After receiving all the bids the auctioneer decrypts the cipher texts with his secret key \(d\) and publishes the highest bid together with the winner of the auction. The RSA encryption keeps eavesdroppers from learning bids of competitors. This seems to imply that the bids of the dishonest participants must be chosen independently of the bids of the honest participants. However, astonishingly this is not necessarily the case: given an honest Alice, a dishonest Bob and let all encryptions be done by ‘textbook RSA\(^{20}\). If now Alice bids the amount \(m\) then she sends \(c = m^e \mod n\) to the auctioneer. Bob can, after learning this ciphertext \(c\) compute \(2^e \times c \mod n\) which equals an encryption of \(2 \times m\) with the public key \((n, e)\).

So without knowing the amount of Alice’s bid Bob is able to compute a ciphertext which encrypts a higher bid and so he will win the auction. This security weakness is called malleability [14] and it is not \textit{per se} a weakness of textbook RSA, but becomes a problem when textbook RSA is used in certain larger applications.

4.2.2. Quantum superpositions can span over several subprotocols. Quantum bit commitment, i.e. the cryptographic equivalent to a sealed envelope, has been shown to be impossible with unconditional security. However, it is tempting to try to circumvent this impossibility theorem of Mayers [26] and Lo/Chau [24] by a clever composition of possible quantum protocols. One could try to build up a secure bit commitment from weaker primitives like cheat sensitive commitments [18]. However, the impossibility theorem rules this out and therefore shows that composing quantum protocols can be counter intuitive. One cannot treat the subprotocols as being ‘atomic’ and quantum superpositions being limited to occur only within the subprotocols. It is possible to keep all quantum information in the different subprotocols in one large superposition and the attack of Mayers and Lo/Chau does exactly that.

4.3. Types of protocol composition

Two kinds of protocol composition can be distinguished:

\textit{Simple composition} for which an example was given in the previous section. In simple composition, a single instance of a cryptographic primitive is replaced by a real subprotocol. Now messages from the surrounding protocol, which may depend on secrets of uncorrupted parties can be injected into the subprotocol or vice versa: a corrupted player can use messages from within a subprotocol outside of this subprotocol. This access to protocol messages that may depend on secrets of uncorrupted parties give an enormous strength to the adversary not

\(^{20}\) This refers to the originally published version of RSA where a ciphertext \(c\) for a message \(m\) is deterministically computed via \(c = m^e \mod n\) and decryption is done via \(m = c^d \mod n\).
present in stand alone models of security. In the quantum world, it is additionally possible to entangle messages used in different protocols.

In the case of concurrent composition many instances of the same protocol with correlated inputs are run concurrently. Apart from the problems of simple composition that messages from one protocol could be fed into another [28], an additional problem occurs if one allows more than a constant number of protocol instances to be run concurrently. Even though each single instance of the protocol is secure in the sense of simulatability it could be that the multiple rounds of the different protocol instances are interleaved in a way that messages in one instance of the protocol affect messages in other protocols and no polynomial time simulation strategy to obtain a consistent simulation for all protocols is known.

So in a notion of security allowing for secure composition, the simulator should work even if the protocol is run in an arbitrary application context. This implies that the simulation cannot be done in retrospect as the real adversary could feed information into surrounding protocols at any time. This requirement of a straight line simulator is very strict; however, according to [23] it is close to the minimal requirement if one wants to combine the requirements of stand alone simulatability and the notion of security being preserved if run in arbitrary applications.

5. The universal composability (UC) framework

The basic idea of the UC framework and why this notion of security allows for secure composition is that the stand alone simulatability definition of security from [16] is enriched by an additional machine, an environment machine that interacts with the protocol and the attacker while it can emulate arbitrary surrounding protocols\(^ {21}\). Starting from this classical UC framework [9] and independently discovered concept of reactive simulatability [2, 29] two quantum models of security were defined in [4, 41]. Both models follow the same motivation, but differ in details which are not of importance in this overview.

The model of [41] is described in three steps. First the machines and their network is defined, next the behavior of the machines is defined according to their roles in a protocol, then the security definition is given based on the indistinguishability of two protocols (the real and the ideal protocol). In our overview many details have to be omitted. For details consult [41].

5.1. Machines and networks

Quantum machines have internal states that may be quantum and the state transition operator is a trace preserving superoperator on the Hilbert space spanned by the tensor product of the possible internal states, the possible inputs and the possible outputs of the machine. The machines are connected by an asynchronous quantum network, i.e. (quantum) messages between machines may be blocked or delayed. Only one machine may be active at any time and the scheduling is message driven, i.e. a machine sending away a message is switching to a waiting state while the receiving machine is activated\(^ {22}\).

The scheduling is classical, i.e. machines are not active and inactive in superposition nor are messages sent and not sent in superposition. This makes the model usable, but it excludes the possibility of certain protocols detecting a traffic analysis [27, 39].

\(^{21}\) In section 2.3, this environment was only implicit, because the interaction with other protocols is simpler than in the general case: key distribution has no input and guarantees no security if one of the parties is corrupted.

\(^{22}\) One distinguished machine, called master scheduler, will be invoked if this rule does not apply.

New Journal of Physics 11 (2009) 085006 (http://www.njp.org/)
5.2. Protocol, adversary, and environment

Apart from the protocol participants that are specified by the protocol there are two more machines taking part in the protocol execution. The adversary $A$ (or $S$ in the ideal model) is the machine coordinating all corrupted participants analogous to the stand-alone model in section 4.1. The environment machine $Z$ chooses the inputs, sees the outputs, and may communicate with the adversary at any time. The environment machine can emulate arbitrary surrounding protocols and can hence detect vulnerabilities which would result from protocol composition.

5.3. The security definition

We demand the environment machine to produce a classical output and we say that a protocol $\pi$ implements an ideal protocol $F$ with perfect security if for every adversary $A$ there exists an ideal adversary $S$ such that for every environment machine $Z$ the distribution of the outputs of $Z$ when interacting with $A$ and $\pi$ equals the distribution of the outputs of $Z$ when interacting with $S$ and $F$. A protocol $\pi$ realizes $F$ with statistical security if the output distribution of $Z$ when interacting with $A$ and $\pi$ is statistically indistinguishable from the output distribution of $Z$ when interacting with $F$ and $S$.

Quantum cryptography usually aims at achieving statistical security where the adversary may be limited only by the laws of quantum mechanics. It does, however, make sense to also define computational security in the quantum setting, because quantum cryptography can realize tasks with computational security which are believed to be impossible classically.

A machine is said to be quantum polynomial time if it can be invoked only a polynomial number of times in the security parameter $k$ and the input output behavior of the machine can be simulated by a quantum Turing machine in polynomial time in $k$. If now all protocol participants, the adversary and the environment machine are quantum polynomial machines then we say that a protocol $\pi$ realizes $F$ with quantum computational security if for all $A$ there exists a $S$ such that for all $Z$ the output distribution of $Z$ when interacting with $A$ and $\pi$ is indistinguishable in quantum polynomial time from the output distribution of $Z$ when interacting with $F$ and $S$. That is, if we denote by $\text{out}_{\pi,A,Z}$ the random variable of the output of $Z$ in the real protocol and by $\text{out}_{F,S,Z}$ the corresponding random variable for the ideal model then we demand that for every quantum polynomial machine $D$ it holds that $|P(D(\text{out}_{\pi,A,Z}) \rightarrow 1) - P(D(\text{out}_{F,S,Z}) \rightarrow 1)|$ is negligible in the security parameter (where a function $\varepsilon$ is called negligible if it is asymptotically smaller than any $1/k^n$ for every constant $n$).

5.4. The composition theorem

The UC framework is a very strict notion of security and for a protocol $\rho$ securely realizing an ideal protocol $F$ in the UC framework strong composition guarantees can be guaranteed. We denote by $\pi^F$ that a protocol $\pi$ invokes a protocol $F$ as a subprotocol and by $\pi^\rho$ that $F$ has

\footnote{In the case of a reactive functionality inputs can also depend on previous outputs or on protocol messages.}

\footnote{In the case of key distribution this amounts to approximate security with $\varepsilon$ negligible, i.e. asymptotically smaller than any $1/k^n$.}

\footnote{For example, realizing oblivious transfer from a one way function \cite{20, 46}.}
been replaced by a protocol \( \rho \). We write \( \pi \geq \rho \) to denote that the protocol \( \pi \) securely realizes \( \rho \) in the UC framework. Now the (simple) composition theorem (see [41]) states that if \( \rho \geq \mathcal{F} \) then \( \pi^\rho \) securely realizes \( \pi^\mathcal{F} \). Especially if \( \pi^\mathcal{F} \) securely realizes a functionality \( \mathcal{G} \) then also \( \pi^\rho \) realizes \( \mathcal{G} \).

If we denote by \( \rho^* \) the concurrent composition of (polynomially many) instances of \( \rho \) and by \( \mathcal{F}^* \) the concurrent composition of (polynomially many) instances of \( \mathcal{F} \). Then the (concurrenct) composition theorem guarantees that if \( \rho \geq \mathcal{F} \) it also holds that \( \rho^* \geq \mathcal{F}^* \).

Combining simple and concurrent composition we obtain the composition theorem where a larger application \( \pi \) may use multiple instances of a subprotocol; given a protocol \( \rho \) which securely realizes a protocol \( \mathcal{F} \) in the UC framework, then a protocol \( \pi^\rho \) securely realizes \( \pi^\mathcal{F} \) in the UC framework.

The UC framework is to a certain extent a minimal requirement for the composition theorem. In the classical case it was shown in [23] that a security notion comparable to the UC framework naturally arises if one demands stand alone simulatability (see section 4.1) and the existence of a composition theorem.

5.5. Information theoretical security and quantum adversaries

One very interesting result proven in the quantum UC framework regards the security of classical protocols with respect to a quantum adversary. Given a protocol which is proven to be statistically secure against a classic adversary. Does it remain secure under quantum attacks? Is the speed-up of quantum computing the only threat to classical protocols or could a quantum attacker together with a quantum environment use entangled quantum information to break classical protocols?

In [40] it was shown by Dominique Unruh that whenever a protocol \( \rho \) realizes some ideal protocol \( \mathcal{F} \) with respect to statistical security in the UC framework, then \( \rho \) securely realizes \( \mathcal{F} \) in the quantum composability setting.

This result is very useful. QKD is composable (cf section 2.3) and from QKD one can obtain composable secure communication [30]. Hence secure channels based on quantum cryptography can be used instead of idealized secure channels in many cryptographic settings, such as secure multiparty computations in the presence of an honest majority [11].

5.6. Impossibility of bit commitment

Additionally to the impossibility of unconditionally secure bit commitment in quantum cryptography [24, 26] a new impossibility result is introduced by the UC framework: without additional security assumptions bit commitment cannot be realized with computational security [10]. This result generalizes to many more cryptographic tasks like coin flipping or oblivious transfer and it also holds in the quantum case.

The reason for this impossibility result is that the simulator may no longer act in retrospect and without additional assumptions every simulation strategy for \( \mathcal{S} \) could be turned into a cheating strategy for the adversary \( \mathcal{A} \) in the real protocol.

The additional assumptions used to allow for a computationally secure bit commitment can be a trusted authority providing randomness to the protocol participants before the start of the protocol (the common reference string), a trusted authority setting up a trusted public key infrastructure, or the availability of tamper proof hardward. What is worse such set-up
assumptions are needed in quantum cryptography, too. The impossibility result of [10] directly carries over to the quantum case; thus in the UC framework quantum cryptographic protocols cannot even achieve a computationally secure bit commitment without additional security assumptions.

So for many cryptographic tasks where the protocol participants are mutually mistrusting one has a trade-off between the strength of the composability guarantees and the strength of the assumptions needed to achieve these tasks. For certain applications the threats introduced by the additional assumptions (e.g. the trusted authorities) weigh heavier than the threats introduced by improper composition of protocols and it seems that for this case there is no security notion which is without a compromise.

As we will see in the next subsection the above impossibility result also affects the composability of protocols in the bounded quantum storage model [13]. To allow for simulatable security in the bounded quantum storage model the memory restrictions have to be different in the real and in the ideal model, which results in difficulties when applying the composition theorem multiple times.

5.7. Composability in the bounded quantum memory model

Even though many interesting cryptographic tasks are not realizable from scratch these tasks can be realized under very reasonable security assumptions, e.g. that the adversary is limited in performing large coherent operations [35] or that the adversary has a quantum memory which is bounded in size [13]. It was shown that the protocols in the bounded quantum storage model do compose sequentially [43]; however, the protocols as stated do not allow general composition. With an example we will illustrate that this seems to be a general problem. To have a useful composition theorem we need that the at least as secure as relation ($\geq$) is transitive, because otherwise we cannot repeatedly apply the composition theorem in the modular design of a cryptographic protocol. To be able to conclude from $\pi \geq \rho$ and $\rho \geq F$ that $\pi$ securely realizes $F$ we need that the simulator in the protocol $\rho$ should be admitted as a real adversary for $\rho$ if this protocol is to be compared with $F$. In [19] it is shown that it is possible to achieve oblivious transfer (and hence bit commitment) if the real adversary is restricted to have no quantum memory at all. However, the simulator for this protocol needs quantum memory for the simulation. So if we restrict the simulator to have no quantum memory oblivious transfer is not realizable any more and having different restrictions for the real attacker and the simulator results in $\geq$ not being transitive.

6. Conclusions

This work reviewed composable security in quantum cryptography. In the first part of the paper the focus was on QKD, the most prominent application of quantum cryptography. We discussed the requirements that a composable security definition must fulfill and illustrated the importance of these requirements by an attack that exploits a typical weakness of a non-composable (but widely used) definition for secrecy. To show the utility of composable security, we constructed a scheme to generate a continuous key stream by sequentially composing rounds of a QKD protocol.

The second part of the work took a more general point of view, which is necessary for the study of security applications involving general tasks as well as mutually distrustful
parties. We explained the UC framework and stated its composition theorem, which gives strong
composability guarantees. Of special interest was the secure composition of quantum protocols
into unconditionally secure classical protocols. This shows that every unconditionally secure
protocol possible in the secure channel model is also possible with QKD and does not even
need a new proof.

However, there are open problems left. A drawback of the UC framework is that some
tasks become impossible there without adding new security assumptions. For example, quantum
bit commitment is impossible in the UC framework even with mere computational security or
with respect to an attacker in the bounded quantum storage model. Hence, we observe a trade-
off between the strong guarantees provided by UC and the possibility of using fewer security
assumptions. Addressing this trade-off remains an open problem.

Another open question regards a weakness inherent to most existing security proofs in
quantum cryptography. These proofs typically rely on a specific model for the hardware the
scheme is built on (e.g. the photon sources and detectors used for optical QKD). Obviously,
the security claims derived for such a model generally only apply to implementations that
strictly match the model. This, however, is almost never the case in practice. Indeed, explicit
attacks exploiting the deviation of the implementation from the theoretical model have been
demonstrated recently (see, e.g. [47]). It would thus be desirable to have a (composable)
framework that allows a more flexible modeling of the underlying hardware devices.

Acknowledgment

We would like to thank Gilles Brassard for helpful comments on an earlier version of the
manuscript.

References

[1] Ambainis A, Buhrmann H, Dodis Y and Röhrig H 2004 Multiparty quantum coin flipping Proc. 19th
Annual IEEE Conf. on Computational Complexity (CCC 2004), 21–24 June 2004, Amherst, MA, USA
(Los Alamitos, CA: IEEE Computer Society) pp 250–9
[2] Backes M, Pfitzmann B and Waidner M 2007 The reactive simulatability (rsim) framework for asynchronous
systems Inf. Comput. 205 1685–720
[3] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 The universal composable security of
quantum key distribution Second Theory of Cryptography Conf. TCC (Lecture Notes in Computer Science
vol 3378) (Berlin: Springer) pp 386–406
[4] Ben-Or M and Mayers D 2004 General security definition and composability for quantum and classical
protocols arXiv:quant-ph/0409062
[5] Bennett C H and Brassard G 1984 Quantum cryptography: public-key distribution and coin tossing Proc.
IEEE Int. Conf. on Computers, Systems and Signal Processing pp 175–9
[6] Biham E and Mor T 1997 Security of quantum cryptography against collective attacks Phys. Rev. Lett.
78 2256–9
[7] Blum M 1983 Coin flipping by telephone: a protocol for solving impossible problems ACM SIGACT News
15 23–7
[8] Cai R Y Q and Scarani V 2008 Finite-key analysis for practical implementations of quantum key distribution
arXiv:0811.2628

New Journal of Physics 11 (2009) 085006 (http://www.njp.org/)
[9] Canetti R 2001 Universally composable security: a new paradigm for cryptographic protocols Proc. 42nd Annual Symp. on Foundations of Computer Science, FOCS 2001 (Las Vegas, Nevada, USA) (Los Alamitos, CA: IEEE Computer Society) pp 136–45

[10] Canetti R and Fischlin M 2001 Universally composable commitments Proc. Advances in Cryptology—CRYPTO 2001 Santa Barbara, California, USA, August 2001 (Lecture Notes in Computer Science vol 2139) (Berlin: Springer) pp 19–40

[11] Chaum D, Crépeau C and Damgård I 1988 Multiparty unconditionally secure protocols (extended abstract) Proc. 20th Annual ACM Symp. on Theory of Computing (STOC) (Chicago, Illinois, USA, May 1988) (New York: ACM) pp 11–9

[12] Cover T M and Thomas J A 1991 Elements of Information Theory (Wiley Series in Telecommunications) (New York: Wiley)

[13] Damgård I B, Fehr S, Salvail L and Schaffner C 2005 Cryptography in the bounded quantum-storage model Proc. 46th Annual IEEE Symp. on Foundations of Computer Science (FOCS) (Pittsburgh, PA, USA, October 2005) (Los Alamitos, CA: IEEE Computer Society) pp 449–58

[14] Dolev D, Dwork C and Naor M 2000 Nonmalleable cryptography SIAM J. Comput. 30 391–437

[15] Ekert A 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661–3

[16] Goldreich O 2004 Foundations of Cryptography—II Basic Applications vol 2 (Cambridge: Cambridge University Press)

[17] Goldwasser S, Micali S and Rackoff C 1985 The knowledge complexity of interactive proof-systems Proc. 17th Annual ACM Symp. on Theory of Computing (STOC) (Providence, Rhode Island, USA, May 1985) (New York: ACM) pp 291–304

[18] Hardy L and Kent A 2004 Cheat sensitive quantum bit commitment Phys. Rev. Lett. 92 157901

[19] Hofheinz D and Müller-Quade J 2003 A paradox of quantum universal composability 4th European QIPC Workshop, 2003 poster abstract online at http://www.quiprocone.org/Oxford/Abstracts.htm

[20] Impagliazzo R and Rudich S 1988 Limits on the provable security of one-way permutations Proc. Advances in Cryptology—CRYPTO ’88, LNCS (Santa Barbara, California, USA, August 1988) ed S Goldwasser (Berlin: Springer)

[21] Kao M-Y (ed) 2008 Quantum key distribution Encyclopedia of Algorithms (Berlin: Springer)

[22] König R, Renner R, Bariska A and Maurer U 2007 Small accessible quantum information does not imply security Phys. Rev. Lett. 98 140502

[23] Lindell Y 2003 General composition and universal composability in secure multi-party computation Proc. 44th Symp. on Foundations of Computer Science (FOCS 2003) (Cambridge, MA, USA, October 2003) (Los Alamitos, CA: IEEE Computer Society)

[24] Lo H-K and Chau H F 1998 Why quantum bit commitment and ideal quantum coin tossing are impossible PhysComp96: Proc. 4th Workshop on Physics and Computation (Amsterdam, The Netherlands) (Amsterdam: Elsevier) pp 177–87

[25] Maurer U 2002 Indistinguishability of random systems Advances in Cryptology—EUROCRYPT ’02 (Lecture Notes in Computer Science vol 2332) ed L Knudsen (Berlin: Springer) pp 110–32

[26] Mayers D 1997 Unconditionally secure bit commitment is impossible Phys. Rev. Lett. 78 3414–7

[27] Müller-Quade J and Steinwandt R 2003 On the problem of authentication in a quantum protocol to detect traffic analysis Quantum Inf. Comput. 3 48–54

[28] Müller-Quade J and Unruh D 2007 Long-term security and universal composability Theory of Cryptography, 4th Theory of Cryptography Conf. TCC 2007, LNCS (Amsterdam, The Netherlands, February 2007) (Berlin: Springer) pp 41–60

[29] Pfitzmann B and Waidner M 2001 A model for asynchronous reactive systems and its application to secure message transmission Proc. 2001 IEEE Symp. on Security and Privacy

[30] Raub D, Steinwandt R and Müller-Quade J 2005 On the security and composability of the one time pad Proc. 31st Conf. on Current Trends in Theory and Practice of Computer Science, SOFSEM 2005 (Lecture Notes in Computer Science vol 3381) (Berlin: Springer) pp 288–97
[31] Renner R 2005 Security of quantum key distribution PhD Thesis Swiss Federal Institute of Technology (ETH), Zurich (arXiv:quant-ph/0512258)

[32] Renner R 2007 Symmetry of large physical systems implies independence of subsystems Nat. Phys. 3 645–9

[33] Renner R and König R 2005 Universally composable privacy amplification against quantum adversaries Second Theory of Cryptography Conf. TCC (Lecture Notes in Computer Science vol 3378) (Berlin: Springer) pp 407–25

[34] Russell A and Wang H 2002 How to fool an unbounded adversary with a short key EUROCRYPT 2002 (Amsterdam, April) (Lecture Notes in Computer Science vol 2332) (Berlin: Springer) pp 133–48

[35] Salvail L 1998 Quantum bit commitment from a physical assumption Proc. Advances in Cryptology—CRYPTO ’98 (Lecture Notes in Computer Science vol 1462) (Santa Barbara, California, USA, August 1998) (Berlin: Springer) pp 338–53

[36] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dütsch M, Lütkenhaus N and Peev M 2008 The security of practical quantum key distribution arXiv:0802.4155

[37] Scarani V and Renner R 2008 Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing Phys. Rev. Lett. 100 200501

[38] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol Phys. Rev. Lett. 85 441–4

[39] Steinwandt R, Janzing D and Beth T 2001 On using quantum protocols to detect traffic analysis Quantum Inf. Comput. 1 62–9

[40] Unruh D 2004 Relating formal security for classical and quantum protocols Isaac Newton Institute for Mathematical Sciences, Cambridge (UK), Workshop on Quantum Information Science, September 2004 invited talk

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

[42] Wegman M N and Carter J L 1981 New hash functions and their use in authentication and set equality J. Comput. Syst. Sci. 22 265–79

[43] Wehner S and Wullschleger J 2008 Composable security in the bounded-quantum-storage model Proc. 35th International Colloquium, Automata, Languages and Programming, ICALP 2008 (Reykjavik, Iceland, July 2008) (Berlin: Springer) pp 604–15

[44] Wiesner S 1983 Conjugate coding ACM SIGACT News 15 78–88

[45] Yao A C C 1982 Protocols for secure computations (extended abstract) Proc. 14th Annual ACM Symp. on Theory of Computing (STOC) (San Francisco, California, USA) (New York: ACM)

[46] Yao A C C 1995 Security of quantum protocols against coherent measurements Proc. 26th Annual ACM Symp. on the Theory of Computing (STOC) (Las Vegas, Nevada, June 1995) (New York: ACM) pp 67–75

[47] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 Quantum hacking: experimental demonstration of time shift attack against practical quantum key-distribution systems Phys. Rev. A 78 042333