

# Research Reports on Mathematical and Computing Sciences

Quantum Asymmetric-Key Cryptosystem Secure  
Against A Computationally Unbounded Adversary

Christopher Portmann and Akinori Kawachi

December 2006, C-238

Department of  
Mathematical and  
Computing Sciences  
Tokyo Institute of Technology

SERIES **C**: Computer Science

# Quantum Asymmetric-Key Cryptosystem Secure Against A Computationally Unbounded Adversary

Christopher Portmann\* and Akinori Kawachi

Dept. of Mathematical and Computing Sciences  
Tokyo Institute of Technology  
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan  
{christo5, kawachi}@is.titech.ac.jp

December 15, 2006

## Abstract

In this paper we propose a quantum asymmetric-key cryptosystem, which does not rely on a computationally hard problem for security, but on uncertainty principles of quantum mechanics, thus obtaining security against a computationally unbounded adversary. We first propose a universally composable security criteria for quantum asymmetric-key cryptosystems by adapting the universally composable security of quantum key distribution by Mayers et al. [4, 3] to the context of quantum asymmetric-key encryption. We then give a specific implementation using this security notion, which improves the quantum asymmetric-key cryptosystem of Kawachi et al. [15] in the sense of information-theoretic security. We prove that the information leak on the decryption key from the multiple copies of the encryption keys released in our scheme is exponentially smaller than that in [15], which allows Alice to produce exponentially more encryption keys.

**Keywords:** Quantum Asymmetric-Key Cryptosystem, Information-Theoretic Security, Universally Composable Security.

## 1 Introduction

Public-key cryptography is the most used cryptographic paradigm. In contrast to secret-key schemes, where the key used to encrypt messages must be kept hidden from the adversary and communicated secretly to anyone wishing to send a secret message, in public-key cryptography the encryption key can be announced publicly and given to any party who wishes it, because knowledge of this key is not sufficient to perform the reverse operation, decryption, efficiently. But the person who generated the public key, also generated a secret key, the decryption key, which he keeps private and uses to decrypt any message sent to him, which was encrypted with the public key he published.

The most famous public-key cryptosystem is RSA, which relies on the difficulty of factoring large numbers to make the attack inefficient for anyone who does not have knowledge of the secret key. Any classical public-key cryptosystem must similarly rely on the computational difficulty of some problem. But with the advent of quantum computers, a lot of these difficult problems have been proved to be efficiently solvable [23]. And new paradigms have to be found.

---

\*Supported in part by NTT Information Sharing Platform Laboratories and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 16092206.

Where quantum computation makes existing protocols insecure, it also provides new protocols. BB84 [5] marked the breakthrough of quantum cryptography, a quantum key-distribution protocol which is unconditionally secure, when classical key-distribution protocols are only computationally secure and vulnerable to quantum adversaries. Instead of relying on the difficulty of some computational problem, as classical key distribution does, QKD uses fundamental principles of quantum mechanics, such as the indistinguishability of non-orthogonal quantum states and the fact that eavesdropping produces noise (we refer to the textbook by Nielsen and Chuang [18] for an introduction to quantum information), to ensure that the eavesdropper has no information on the quantum communication between Alice and Bob. Other protocols with security relying on the fundamental principles of quantum mechanics were developed, such as quantum oblivious transfer [8], quantum string commitment [6] or quantum digital signatures [10], often leading to unconditional security. But little has been done in this area for quantum asymmetric-key cryptosystems.

The development of quantum key distribution allows the usage of secret-key cryptosystems which are secure against a computationally unbounded quantum adversary. But public-key cryptosystems have advantages which we want to preserve. To make them secure against quantum attacks, a possible solution is to develop schemes which rely on problems thought to be hard even on quantum computers, e.g., NP-hard problems, either classical protocols as in [13, 1, 20], or quantum protocols as in [19, 14, 15]. But such schemes are still only computationally secure, and thus vulnerable to further development of (quantum) computation. The alternative solution is to design protocols which are secure by virtue of quantum mechanical principles, and thus produce a scheme which is secure against a computationally unbounded adversary. In this paper we propose such a quantum asymmetric-key cryptosystem.

## Model

The first quantum encryption scheme using the same model as ours was proposed by Kawachi et al. in [14]. In this model, which is illustrated in Figure 1 on page 4 and will be described in more detail in Section 2, Alice distributes a quantum state,  $\rho_\nu$ , which serves as an encryption key and corresponds to a decryption key, to anyone who wants to send her a secret message. She also publishes some encoding operations  $\{U_s\}_{s \in S}$ , which Bob applies to Alice's state when he wants to send her the message  $s$ . He thus creates the state  $\rho_{\nu,s} = U_s \rho_\nu U_s^\dagger$ , and sends it back to Alice. She then measures it to detect which operator  $U_s$  was applied, i.e., decrypt Bob's message  $s$ .

Public-key cryptosystems are vulnerable to man-in-the-middle attacks, in which an adversary intercepts or modifies the public key sent by Alice to Bob, and replaces it by her own. So some authentication protocol is necessary, to ensure that the key Bob receives really is the one Alice sent. As authentication is out of the scope of this work, the model we consider requires an authentic quantum channel as cryptographic primitive for the distribution of the encryption-key states (which can be realized with unconditional security, see, e.g., [2] and Section 2.2 for further discussion). The adversary can not tamper with the encryption-key states before they are received by Bob, but she can intercept the cipher he sends back to Alice and all other encryption-key states, and has unbounded computational power. (See Figure 2 on page 5.)

## Security

Alice can perform a measurement to decrypt the message sent to her by Bob, because she knows how she constructed her encryption key  $\rho_\nu$ , she knows the decryption key  $\nu$ , so she knows how to measure it. But to the adversary the encryption key looks like a mixture of all possible  $\rho_\nu$ , and as a measurement destroys the state and quantum mechanics does not allow cloning [18], the adversary is very dependent on the number of copies of the encryption key released by Alice, to measure it precisely, extract the decryption key and thus find a way to measure Bob's cipher state,  $\rho_{\nu,s}$ . So by keeping the number of copies of the encryption key released below a certain threshold, the

secrecy is guaranteed even against a computationally unbounded adversary. A proof of security based on that idea for the scheme by Kawachi et al. [14], and its extension in [15], was proved by Hayashi, Kawachi and Kobayashi in [11].

The previous paragraph briefly sketches how the adversary could try to extract the decryption key from multiple copies of the encryption key to break the cryptosystem. This is one strategy amongst many, and the security criteria, which is discussed in detail in Section 3, has to encompass any possible attack allowed by the model. But what is more, we want the encryption scheme to still be secure — or at least as secure as an ideal functionality — if the adversary gets some partial information about the message or which may be leaked if this protocol is combined with others, e.g., if Alice publishes part of the message she received, or encrypts it a second time to send it to someone else, the rest of the message should still be secure. This notion is captured by what is called *universal composability*, which was first proposed by Canetti [7] and adapted to the quantum setting by Mayers et al. [4, 3] and in parallel by Unruh [24]. So in Section 3 we use such a universally composable security notion for this encryption scheme.

## Main Results

Our main result is a new encryption scheme based on [15], which improves the previous best bound on the number of encryption-key states which can be released [11], by a factor exponential in the length of the message which Bob can send. We also derived a new universal security criteria for the quantum asymmetric-key cryptosystem considered, based on the universal composability framework in [4, 3], and proved the scheme secure according to this condition.

More precisely, Hayashi et al. found in [11], that Alice can safely produce  $k = o\left(\frac{n \log n}{m \log m}\right)$  encryption keys for the quantum asymmetric-key cryptosystem proposed in [15], where  $m$  is the number of messages Bob can send, i.e.,  $\log m$  is the length of the secret message in bits, and  $n$  is a security parameter, polynomial in the size of the encryption-key state. Their security criteria was the indistinguishability of any two cipher states, which is weaker than the universal security criteria we use, but their work can be adapted to meet the same criteria as ours and still keep the same bound on  $k$ . Our scheme allows Alice to produce  $k \leq \frac{n \log n}{3 \log m} - O\left(\frac{n}{\log m}\right)$  copies of the encryption-key state (Eq. (14)), thus improving the bound by a factor  $m/3$ , which is exponential in the length of the message. This allows Alice to produce that many more encryption keys and receive that many more messages.

## Organization of the Paper

This paper is structured as follows. In Section 2 we define the model considered, the assumptions on channels available and adversary power. We also detail the encryption scheme which was briefly sketched in the introduction, defining precisely the states, unitaries and operations needed, and how they fit together in the protocol. In Section 3 we discuss the security notions and requirements for the scheme, introduce universally composable security more precisely, and derive a condition for universal security for this asymmetric-key cryptosystem. And finally in Section 4 we give an implementation of the scheme, prove its correctness and find the bound stated previously on the number of encryption keys which can be released, so that the scheme is secure according to the notion discussed in Section 3.

## 2 Model

### 2.1 Scheme

The following two definitions describe the states and operations required by the encryption scheme (illustrated in Figure 1), which were sketched in the introduction. Definition 1 describes the various

quantum states, operations and measurements which the cryptosystem needs, and which need to be defined when an implementation of the model is given. Definition 2 describes how the protocol is executed and how the elements fit together.

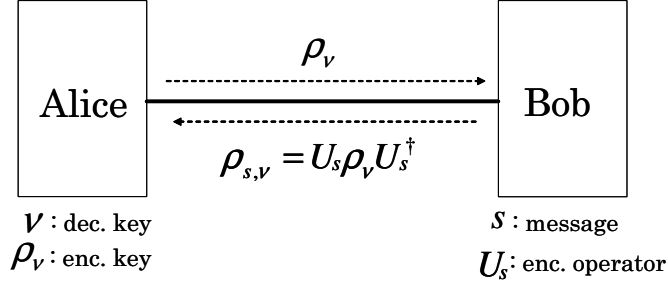


Figure 1: Encryption scheme

**Definition 1.** The asymmetric-key cryptosystem model considered consists of a tuple of three elements,  $\mathcal{M}_{AKC} = (\{\rho_\nu\}_{\nu \in \Gamma}, \{U_s\}_{s \in S}, \{\mathbb{E}_\nu\}_{\nu \in \Gamma})$ , where

- $\{\rho_\nu\}_{\nu \in \Gamma}$  is a set of quantum states lying in a Hilbert space  $\mathcal{H}_d$  of dimension  $d$ , which we will call *encryption keys*, indexed by elements  $\nu \in \Gamma$ , which we will call *decryption keys*.
- $\{U_s\}_{s \in S}$  is a set of unitary operators of dimension  $d$ , which we will call *encoding operators*, indexed by elements  $s \in S$ , which we will call *secret messages*.
- $\{\mathbb{E}_\nu\}_{\nu \in \Gamma}$  is a set of POVMs, which we will call *decoding measurements*, where  $\mathbb{E}_\nu = \{E_s^\nu\}_{s \in S}$  are the POVM elements, indexed by the decryption keys and secret messages respectively.

Although we have specified a set of POVMs as decoding measurements in this definition, practically we will give a protocol, or a set of unitary operations followed by a measurement, which are equivalent to a POVM.

**Definition 2.** The protocol consists of three steps, which use the states and operations given in Definition 1, namely key generation, encryption and decryption.

**Key generation:** Alice chooses an element  $\nu \in \Gamma$  uniformly at random, and creates copies of the encryption key  $\rho_\nu$ , which she sends to any party who asks for one on an authentic quantum channel. She also publishes the set of encoding operations  $\{U_s\}_{s \in S}$ .

**Encryption:** To encode the message  $s$ , Bob applies the unitary  $U_s$  to the encryption key, and obtains  $\rho_{\nu,s} = U_s \rho_\nu U_s^\dagger$ , which he sends back to Alice.

**Decryption:** Alice measures  $\rho_{\nu,s}$  with the POVM  $\mathbb{E}_\nu = \{E_s^\nu\}_{s \in S}$ , corresponding to her choice of decryption key  $\nu$ . She obtains the result  $s'$  which is her guess of Bob's message.

For such a scheme to be useful three things are required. First of all it is necessary for Alice to be able to distinguish between the possible ciphers sent by Bob,  $\rho_{\nu,s}$ , for all messages  $s \in S$  and a given decryption key  $\nu$ , which we will refer to as the *correctness* of the protocol. More precisely, we want the probability of Alice decoding the message correctly,  $\text{tr}(E_s^\nu \rho_{\nu,s})$ , to be close to 1 for every  $\nu \in \Gamma$  and  $s \in S$ . But it must be hard for Eve to distinguish between them when she has no or only partial information on the decryption key  $\nu$ , on Bob's message  $s$ , or any other kind of information she might obtain. This latter condition is the *security* of the protocol, which we will discuss in the next section. And thirdly, we want the protocol to be *efficient*, i.e., the encoding and decoding operations have to be implementable by a polynomial-time quantum algorithm.

## 2.2 Channels and Adversary

An adversary, Eve, could perform a man-in-the-middle attack, and replace the encryption-key state sent by Alice to Bob by her own state. If Alice and Bob do not run some authentication protocol, to ensure that the key Bob receives really is the one Alice sent, then any cipher state sent back to Alice by Bob, which is encrypted using the unauthenticated encryption key he received, could be readable by the adversary.

In this work we study the feasibility of encrypting messages into quantum states of which the adversary has copies. We do not consider the protocols which allow these states to be distributed. We therefore require an authentic quantum channel as cryptographic primitive. Such a channel could be realized with a non-interactive protocol if a decryption key is shared by the two parties, as proposed in [2], in which case this scheme can be seen as turning a secret key into a public one. Alternatively, an interactive protocol involving entanglement distillation or quantum error correction (see [18] for an overview of these techniques) can be used.

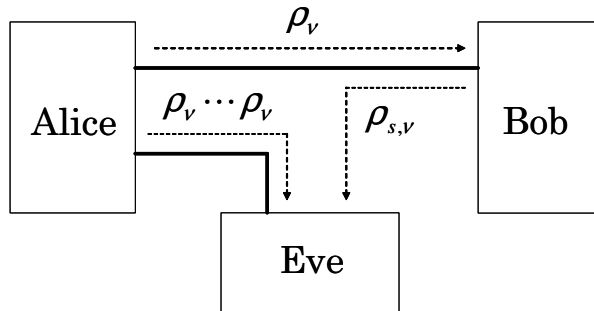


Figure 2: The adversary's attack

In this model we therefore have an authentic quantum channel for the distribution of the encryption-key state, and a totally insecure quantum channel for sending the cipher state. Thus the adversary cannot tamper with the encryption key, but he can make a copy of it<sup>1</sup> and can intercept the cipher state and all of the other encryption keys published, as illustrated in Figure 2. The adversary is also computationally unbounded, and can perform any operation and measurement allowed by quantum mechanics on the states she intercepted.

## 3 Security

The security of the general scheme presented in the previous section relies on the indistinguishability of non-orthogonal quantum states. For a given decryption key  $\nu \in \Gamma$ , the encodings of the possible messages  $s \in S$  must be near-orthogonal, so that Alice can distinguish between them with high probability. But when  $\nu$  is not known, the possible ciphers over all possible decryption keys must be highly non-orthogonal, so that Eve cannot distinguish between them without knowing in which basis to measure Bob's message.

Each encryption key Alice publishes is information leaked to the adversary. With sufficient copies of it, Eve can measure it precisely and thus discover how to measure Bob's message in order to extract the secret message. So it is necessary to find a bound on the number of encryption keys Alice can release, so that Eve only gets negligible information on Bob's message.

Yet as such, this security notion is not strong enough. Eve may obtain information from other sources or in subsequent protocols, which combined with what is leaked by this protocol reveal

<sup>1</sup>Cloning of a quantum state is generally impossible. But as we use an authentic quantum channel as a black box, by assuming the adversary gets a copy of the state we upper bound the information he might obtain.

too much of Bob's message, although individually neither this protocol nor the subsequent leaks give any non-negligible amount of information to Eve. This stronger security notion is captured by what is called *universally composable security*.

Universal composability was first introduced by Canetti in [7] for classical cryptography. The idea is to ensure that a cryptographic protocol is still secure when combined in a complex system with other protocols, and that the developer of such a system only needs to consider the ideal functionalities the protocols are trying to implement, and not the details of the implementations, when combining them together. The framework proposed in [7] was extended to the quantum setting by Ben-Or and Mayers in [4] and adapted to quantum key distribution in [3]. In these works, a protocol is considered secure if the environment, which comprises all adversaries and the inputs and outputs of the protocol, can only distinguish with negligible probability between the real protocol and the ideal functionality the protocol is trying to implement. The ideal functionality can thus be substituted for the real protocol in the analysis of any other cryptographic protocol which uses it as a subroutine, as the two cannot be distinguished.

A slightly different approach to quantum universal security by Renner lead to the same definition for the security of secret keys as [3] and was applied to quantum privacy amplification [22] and quantum key distribution [21]. Here the question asked is whether the scheme is still secure if the adversary postpones the measurement of whatever information he possesses encoded in a quantum state until a later time when he might have gathered extra information, e.g., part of the message, telling him how to perform the measurement, thus unlocking much more information than he could have obtained initially<sup>2</sup>. This extra information the adversary might get, could be from another protocol, when several are combined together. So these two approaches are basically the same. But the latter can also be seen as a generalization of other specific security requirements, such as wanting the last bit of the key to still be secret if the rest of it is revealed, or not wanting the adversary to be able to distinguish between any two possible ciphers, which was the security criteria used in [11] for the quantum asymmetric-key cryptosystem proposed in [15].

Very generally, let  $S$  be a secret (e.g., a key or message) with distribution  $P_S$ , which consists of the input or output of a protocol  $\mathcal{P}$ , and let  $\rho_E^s$  be the adversary's system after the execution of this protocol, when the secret takes the value  $s$ , for any element  $s$  of  $S$ . The resulting system can be described by the following density operator:

$$\rho_{SE} = \sum_{s \in S} P_S(s) |s\rangle\langle s| \rho_E^s, \quad (1)$$

where  $\{|s\rangle\}_{s \in S}$  is an orthonormal basis of some Hilbert space  $\mathcal{H}_S$ . With an ideal protocol  $\mathcal{P}_I$ , the adversary's system would be uncorrelated to the secret. Thus not only he gets no direct information about the secret, but if this protocol is combined with others which share the same secret input or output and leak some information about it, the adversary cannot use this extra information to help him extract the secret from the states this protocol leaked. I.e., the system would be in the state

$$\rho_U \otimes \rho_E, \quad (2)$$

where  $\rho_U = \frac{1}{|S|} I = \frac{1}{|S|} \sum_{s \in S} |s\rangle\langle s|$  is the fully mixed state in the Hilbert space of the secret  $\mathcal{H}_S$ , and  $\rho_E$  is the adversary's state, namely

$$\rho_E = \text{tr}_S(\rho_{SE}) = \sum_{s \in S} P_S(s) \rho_E^s. \quad (3)$$

We want the distance between the real situation (Eq. (1)) and the ideal one (Eq. (2)) to be small. Therefore

$$\|\rho_{SE} - \rho_U \otimes \rho_E\|_1 \leq \epsilon, \quad (4)$$

---

<sup>2</sup>This phenomenon, sometimes called *locking of classical correlation*, has been studied in other contexts, see, e.g., [9, 12].

where the distance measure used, known as the 1-distance, is defined as  $\|\rho - \sigma\|_1 := \text{tr}(|\rho - \sigma|)$ .

According to the work done in [4, 3], if Eq. (4) is respected, then the environment cannot distinguish between the real protocol  $\mathcal{P}$  and the ideal functionality  $\mathcal{P}_{\mathcal{I}}$ , except with probability  $\epsilon$ . The protocol  $\mathcal{P}$  is said to  $\epsilon$ -securely realize the ideal functionality  $\mathcal{P}_{\mathcal{I}}$ , and by the composition theorem from [4, 3], any protocol  $\mathcal{Q}$  which is  $\epsilon'$ -secure when using the ideal functionality  $\mathcal{P}_{\mathcal{I}}$  as subroutine, is  $(\epsilon' + \epsilon)$ -secure when using the real protocol  $\mathcal{P}$  as subroutine. In [21], if Eq. (4) is respected, the secret  $S$  is said to be  $\epsilon$ -secure with respect to  $\mathcal{H}_E$ . The ideal and real situations are  $\epsilon$ -close, and as the 1-distance cannot increase when applying an arbitrary quantum operator, it will remain so for any further evolution of the world.

We therefore take Eq. (4) as our definition of universally composable security, and adapt it to the particular context of our encryption scheme. The secret which maybe be seen as both input and output of the encryption protocol is Bob's message  $s$ . Alice or Bob may publish part of it, or encrypt it again to send it to another party. It can be used by any super protocol which accesses this encryption scheme as subroutine. Alice's secret key on the other hand is kept secret by Alice. No matter how other protocols use this one, they do not have access to her secret key, so no extra information will ever be leaked about it. The adversary's system consists of all the encryption keys and the intercepted cipher state  $\rho_{\nu,s}$  from Bob, as defined in Section 2. If Alice chooses the decryption key  $\nu$  uniformly at random from a set  $\Gamma$  and publishes  $k$  copies of the encryption key  $\rho_{\nu}$ , the adversary's system conditioned on the secret message being  $s$  is then in the state

$$\rho_E^s = \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu,s} \otimes \rho_{\nu}^{\otimes k}. \quad (5)$$

By placing Eq. (5) in Eq. (4), we get a universal security criteria for the scheme. It depends however not only on the choice of the encryption-key states  $\rho_{\nu}$ , but also on the way the encoding of the message  $s$  is done and the resulting cipher states  $\rho_{\nu,s}$ . In Theorem 3 we will show that the universal security of the encryption-key scheme only depends on a near-uniform distribution of the messages  $s \in S$  and the security of the encryption-key state, namely the difficulty to distinguish it from the fully mixed state when drawn uniformly at random, given  $k$  extra copies of it.

**Theorem 3.** *If*

$$\left\| \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu}^{\otimes(k+1)} - \frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu}^{\otimes k} \right\|_1 \leq \frac{\epsilon}{2}, \quad (6)$$

where  $d$  is the dimension of  $\rho_{\nu}$  and  $I$  is the identity operator of dimension  $d$ , and if the non-uniformity<sup>3</sup> of the message probability distribution is less than  $\frac{\delta}{2}$ , then an asymmetric-key cryptosystem as described in Section 2, i.e., which leaves the adversary's system in the state  $\rho_E^s = \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu,s} \otimes \rho_{\nu}^{\otimes k}$  (Eq. (5)) when the message is  $s$  and the encryption key is chosen uniformly at random from  $\{\rho_{\nu}\}_{\nu \in \Gamma}$ , then such a scheme is  $(\delta + \epsilon)$ -secure with respect to the Hilbert space  $\mathcal{H}_E$ , i.e.,

$$\|\rho_{SE} - \rho_U \otimes \rho_E\|_1 \leq \delta + \epsilon. \quad (7)$$

*Proof.* Let

$$\sigma_s := \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu,s} \otimes \rho_{\nu}^{\otimes k} - \frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu}^{\otimes k},$$

then

$$\frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu,s} \otimes \rho_{\nu}^{\otimes k} = \frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_{\nu}^{\otimes k} + \sigma_s. \quad (8)$$

---

<sup>3</sup>The non-uniformity of a probability distribution  $P_X$  is its variational distance from the uniform distribution, i.e.,  $d(P_X) = \frac{1}{2} \sum_{x \in X} \left| P_X(x) - \frac{1}{|X|} \right|$

Because  $\rho_{\nu,s}$  is obtained from  $\rho_\nu$  by applying the unitary  $U_s$ , and because a unitary operation does not change the 1-distance, we have  $\|\sigma_{s_1}\| = \|\sigma_{s_2}\|$  for any  $s_1, s_2 \in S$ . Then by the hypothesis of this lemma (Eq. (6)),  $\|\sigma_s\|_1 \leq \frac{\epsilon}{2}$ .

By placing Eq. (8) in the left-hand side of Eq. (7) and replacing  $\rho_{SE}$  and  $\rho_E$  with their exact values (Eqs. (1), (3) and (5)), we get

$$\begin{aligned}
& \left\| \sum_{s \in S} P_S(s) |s\rangle\langle s| \otimes \left( \frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_\nu^{\otimes k} + \sigma_s \right) \right. \\
& \qquad \qquad \qquad \left. - \frac{1}{|S|} I \otimes \sum_{s \in S} P_S(s) \left( \frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_\nu^{\otimes k} + \sigma_s \right) \right\|_1 \\
&= \left\| \left( \sum_{s \in S} P_S(s) |s\rangle\langle s| - \frac{1}{|S|} I \right) \otimes \frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu \in \Gamma} \rho_\nu^{\otimes k} \right. \\
& \qquad \qquad \qquad \left. + \sum_{s \in S} P_S(s) |s\rangle\langle s| \otimes \sigma_s - \frac{1}{d} I \otimes \sum_{s \in S} P_S(s) \sigma_s \right\|_1 \\
&\leq \left\| \sum_{s \in S} P_S(s) |s\rangle\langle s| - \frac{1}{|S|} I \right\|_1 + \left\| \sum_{s \in S} P_S(s) |s\rangle\langle s| \otimes \sigma_s \right\|_1 + \left\| \frac{1}{d} I \otimes \frac{1}{|S|} \sum_{s \in S} \sigma_s \right\|_1 \\
&\leq \delta + \frac{\epsilon}{2} + \frac{\epsilon}{2}.
\end{aligned}$$

□

We can require from Bob that the non-uniformity of the distribution of his messages  $s \in S$  be negligible. So the sufficient conditions for universal security expressed in Theorem 3 are reduced to Eq. (6). From the universal composability viewpoint, this criteria can be seen as a universal security requirement for the encryption key, namely a negligible probability that the environment can distinguish between the encryption key  $\rho_\nu$  drawn uniformly at random from all possible key-states and the fully mixed state, given  $k$  extra copies of the key.

This criteria can be used to find bounds on the number of copies  $k$  of the encryption key which can safely be released, for particular instances or family of instances of states and encoding operations implementing Definition 1, which is what we do in the next section.

## 4 Instances

In Section 4.2 we will give a specific implementation of encryption key, encoding-operation and measurement tuple, with a precise bound on the security. But before that, in Section 4.1, we will study a family of good encryption key candidates, namely what is known as coset states of a subgroup of prime order (see Definition 4). This allows us to derive a bound on the number of encryption-key states which can be released for the universal security criteria found in Section 3 (Eq. (6)), for a specific family of states with common properties. The final scheme we propose in Section 4.2 is a particular instance of this family of states, and we can directly use the security bound derived in Section 4.1.

## 4.1 Coset States

**Definition 4.** Let  $G$  be a finite group and  $H$  a subgroup of  $G$ . The *coset state* of  $H$  is then

$$\rho_H = \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH| = \frac{|H|}{|G|} \sum_{g \in G/H} |gH\rangle\langle gH|,$$

with

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle,$$

where  $\{|g\rangle\}_{g \in G}$  is an orthonormal basis of some Hilbert space  $\mathcal{H}_G$ , and  $gh$  is the composition of  $g$  and  $h$  with the group operation.

These coset states appear in what is known as the *standard method* to solve the *hidden subgroup problem*, which is one of the central issues in quantum computation, introduced for revealing the structure behind exponential speedups in quantum computation [17]. Let  $G$  be a finite group, and  $H$  a hidden subgroup of  $G$ . Given a map  $f_H$  from  $G$  to a finite set  $S$  such that  $f_H(g) = f_H(gh)$  if and only if  $h \in H$ , the hidden subgroup problem (HSP) is the problem of outputting a set of generators for the hidden subgroup  $H$ .

The standard method to solve the HSP consists in constructing several copies of the coset state of  $H$  (using the map  $f_H$ ) and then measuring these states to identify the hidden subgroup. General solutions to Abelian HSPs have been given [16, 17], but non-Abelian HSPs are much harder and most important cases of non-Abelian HSPs are not known to have efficient solutions. Although our problem at hand is slightly different, it is still very interesting to use coset states as encryption keys, as it seems a hard problem to identify them exactly without a large number of copies.

In the following lemma (which is a slight modification of Theorem 2.4 in [11]) and Corollary 6 just after, we substitute coset states  $\{\rho_H\}_{H \in \mathcal{H}}$  of subgroups  $H \in \mathcal{H}$  with prime cardinality for the encryption-key states  $\{\rho_\nu\}_{\nu \in \Gamma}$  in Eq. (6), and find an upper bound on the number of copies  $k$  of the coset state  $\rho_H$  which can be released, so that the environment can only distinguish with probability  $\epsilon$  between an encryption key drawn at random and the fully mixed state when provided with  $k$  extra copies of it.

**Lemma 5.** *If*

$$k \leq \frac{2 \log \epsilon + \log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|} - 1,$$

*then*

$$\left\| \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \rho_H^{\otimes(k+1)} - \frac{1}{|G|} I \otimes \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \rho_H^{\otimes k} \right\|_1 \leq \epsilon,$$

*for  $H \in \mathcal{H}$  with prime cardinality.*

*Proof.* Simply by expanding the coset states and using the triangle inequality, we obtain

$$\begin{aligned} & \left\| \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \rho_H^{\otimes(k+1)} - \frac{1}{|G|} I \otimes \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \rho_H^{\otimes k} \right\|_1 \\ &= \left\| \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \frac{1}{|G|^{k+1}} \sum_{g_0, \dots, g_k \in G} \sum_{h_0, \dots, h_k \in H} (|g_0, \dots, g_k\rangle\langle g_0 h_0, \dots, g_k h_k| \right. \\ & \quad \left. - |g_0, g_1, \dots, g_k\rangle\langle g_0, g_1 h_1, \dots, g_k h_k|) \right\|_1 \end{aligned}$$

$$\begin{aligned}
&= \left\| \frac{1}{|\mathcal{H}|} \frac{1}{|G|^{k+1}} \sum_{g_0, \dots, g_k \in G} \sum_{H \in \mathcal{H}} \sum_{\substack{h_0, \dots, h_k \in H \\ h_0 \neq id}} |g_0, \dots, g_k\rangle \langle g_0 h_0, \dots, g_k h_k| \right\|_1 \\
&\leq \frac{1}{|\mathcal{H}| |G|^{k+1}} \sum_{g_0, \dots, g_k \in G} \|\langle g_0, \dots, g_k \|_2 \left\| \sum_{H \in \mathcal{H}} \sum_{\substack{h_0, \dots, h_k \in H \\ h_0 \neq id}} |g_0 h_0, \dots, g_k h_k\rangle \right\|_2 \\
&= \frac{1}{|\mathcal{H}|} \sqrt{\sum_{H, H' \in \mathcal{H}} |H \cap H'|^k (|H \cap H'| - 1)} \\
&\leq \sqrt{\frac{\max_{H \in \mathcal{H}} |H|^{k+1}}{|\mathcal{H}|}},
\end{aligned}$$

where  $\|\cdot\|_2$  is the L2-norm. The last inequality is obtained by using the fact that the subgroups considered have prime cardinality which implies that  $|H \cap H'| = 1$  if  $H \neq H'$ .

The last inequality is then smaller than  $\epsilon$ , if

$$k \leq \frac{2 \log \epsilon + \log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|} - 1. \quad \square$$

**Corollary 6.** *If we use coset states  $\{\rho_H\}_{H \in \mathcal{H}}$  as encryption keys  $\{\rho_\nu\}_{\nu \in \Gamma}$  in the scheme described in Section 2, and each  $H \in \mathcal{H}$  has the same cardinality, then the scheme is  $\epsilon$ -secure if the number of copies  $k$  of the encryption key released is*

$$k \leq \frac{2 \log \epsilon + \log |\mathcal{H}|}{\log |H|} - 1. \quad (9)$$

## 4.2 Implementation with Cyclic Permutations

We now propose a particular instance for the scheme discussed so far, namely cosets of subgroups of the group  $G = \mathbb{Z}_m \times S_n$ , where  $\mathbb{Z}_m$  is the set of natural numbers smaller than  $m$  and the group operation is addition modulo  $m$ , and  $S_n$  is the set of all permutations of an  $n$ -tuple and the group operation is permutation composition.  $n$  and  $m$  are two parameters such that  $m$  is prime and  $m$  divides  $n$ , but for the rest they can be chosen freely. As it will become clear as we define the encryption scheme more precisely,  $m$  is the number of messages which can be encoded, and  $n$  is a security parameter. By choosing  $n$  big enough, we will be able to make the scheme  $\epsilon$ -secure, for an  $\epsilon$  exponentially small in  $n$ .

In Section 4.2.1 we will define the encryption-key states, encoding operations and decoding measurements precisely, and show that the scheme is correct, i.e., that Alice can decode Bob's message with probability 1 if the adversary does not intervene. In Section 4.2.2 we will then prove that the scheme is secure and find a bound on the number of encryption keys which can be released.

### 4.2.1 Correctness

The following definition specifies the encryption-key state  $\rho_\pi$ , where  $\pi$  is the decryption key.

**Definition 7.** Let

$$\mathcal{K}_n^m = \{h : h = (a_1 \cdots a_m) \cdots (a_{n-m+1} \cdots a_n), a_i \in \{1, \dots, n\}, a_i \neq a_j (i \neq j)\},$$

$\mathcal{K}_n^m \subseteq S_n$ , be the set composed of  $n/m$  disjoint cyclic permutations. We now define the encryption-key state  $\rho_\pi$ , where the decryption key  $\pi$  is chosen uniformly at random from  $\mathcal{K}_n^m$ , as

$$\rho_\pi := \frac{1}{n!} \sum_{\sigma \in S_n} |\Phi_\pi^\sigma\rangle\langle\Phi_\pi^\sigma|, \quad (10)$$

where

$$|\Phi_\pi^\sigma\rangle = \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |x, \sigma\pi^x\rangle. \quad (11)$$

Alice will send this state to Bob, or any party who wishes it. To send a message  $s$  to Alice, Bob will apply a unitary  $U_s$  to the encryption key  $\rho_\pi$ , obtaining  $\rho_{\pi,s} = U_s \rho_\pi U_s^\dagger$ , which he sends back to Alice. The operations  $U_s$  are defined as follows.

**Definition 8.** Let the message set  $S$ , which the scheme allows Bob to send, have cardinality  $m$ ,  $|S| = m$ , and let us represent them by the natural numbers, i.e.,  $S = \{0, \dots, m-1\}$ . To encrypt the message  $s$  in the state  $\rho_\pi$  defined previously, let Bob apply the unitary

$$U_s := \sum_{x=0}^{m-1} e^{2\pi i s x/m} |x\rangle\langle x|. \quad (12)$$

This unitary is only defined on a space of dimension  $m$  and acts on the first register of the encryption-key state  $\rho_\pi$ , so it needs to be padded by an identity operator of dimension  $n!$  to be formally correct. But we will omit it for simplicity and allow ourselves to write  $\rho_{\pi,s} = U_s \rho_\pi U_s^\dagger$  instead of  $\rho_{\pi,s} = (U_s \otimes I) \rho_\pi (U_s^\dagger \otimes I)$ .

If the first register is represented by  $\lceil \log m \rceil$  qubits, Eq. (12) can be rewritten as  $\hat{U}_s = \bigotimes_{j=0}^{\lceil \log m \rceil - 1} U_{s,j}$ , where

$$U_{s,j} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i s 2^j/m} \end{pmatrix}.$$

Note that  $\hat{U}_s$  differs slightly from  $U_s$ , in that it is defined on a space of dimension  $2^{\lceil \log m \rceil}$  and also modifies the first register if it takes a value  $m \leq x \leq 2^{\lceil \log m \rceil} - 1$ . But the encryption-key states  $\rho_\pi$  are only defined with values of the first register  $0 \leq x \leq m-1$ , so for all decryption keys  $\pi$  and messages  $s$ ,  $U_s \rho_\pi U_s^\dagger = \hat{U}_s \rho_\pi \hat{U}_s^\dagger$ . The operators  $\{U_s\}_{s \in S}$  can thus be efficiently implemented.

The operators  $U_s$  defined in Eq. (12) take any encryption-key state  $\rho_\pi$  to mutually orthogonal subspaces, which allows them to be distinguished by Alice with probability 1, as the following theorem shows.

**Theorem 9.** *There exists a polynomial-time quantum algorithm that, for each  $\pi \in \mathcal{K}_n^m$ , decrypts  $\rho_{\pi,s} = U_s \rho_\pi U_s^\dagger$  to  $s$  with probability 1.*

*Proof.*

$$\rho_{\pi,s} = \frac{1}{n!} \sum_{\sigma \in S_n} |\Phi_{\pi,s}^\sigma\rangle\langle\Phi_{\pi,s}^\sigma|,$$

where

$$|\Phi_{\pi,s}^\sigma\rangle = \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} e^{2\pi i s x/m} |x, \sigma\pi^x\rangle.$$

This state is a superposition of the pure states  $|\Phi_{\pi,s}^\sigma\rangle$ . So it is sufficient to give a polynomial-time quantum algorithm which can extract  $s$  from any  $|\Phi_{\pi,s}^\sigma\rangle$  independently from  $\sigma$ , and by linearity the algorithm can extract  $s$  from  $\rho_{\pi,s}$ .

By applying to  $|\Phi_{\pi,s}^\sigma\rangle$  the controlled- $\pi^{-1}$  operator,

$$C_{\pi^{-1}} = \sum_{x=0}^{m-1} \sum_{\sigma \in S_n} |x, \sigma \pi^{-x}\rangle \langle x, \sigma|,$$

which applies  $x$  times the permutation  $\pi^{-1}$  to the second register, when the first register contains  $x$ , we obtain:

$$C_{\pi^{-1}} |\Phi_{\pi,s}^\sigma\rangle = \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} e^{2\pi i s x/m} |x\rangle |\sigma\rangle.$$

The second register is now un-entangled from the first, and by applying the inverse Fourier transform on the first register we get  $s$ .

The efficiency of this algorithm is straightforward from its construction.  $\square$

Theorem 9 not only proves that the cipher states  $\rho_{\pi,s}$  can be decoded, but it also gives an explicit efficient algorithm to do it, which serves as the decoding POVMs required by the definition of the scheme (Definition 1 in Section 2).

#### 4.2.2 Security

To prove that a scheme using the encryption key defined in the previous section (Definition 7) is secure, we will show that it is a coset state, and then we apply the bound from Eq. (9) from Corollary 6.

**Theorem 10.** *An encryption scheme as defined in Section 2 using the encryption keys given in Definition 7 is  $\epsilon$ -secure, if the number  $k$  of encryption keys released is*

$$k \leq \frac{6 \log \epsilon + n \log n}{3 \log m}$$

*Proof.* The encryption-key state defined in Eqs. (10) and (11) is a coset state, as the following calculation shows.

Let  $H_\pi = \{(0, id), (1, \pi), \dots, (m-1, \pi^{m-1})\}$ , where  $\pi \in \mathcal{K}_n^m$ .  $H_\pi$  is a subgroup of  $\mathbb{Z}_m \times S_n$ , and its coset state is

$$\rho_{H_\pi} = \frac{1}{mn!} \sum_{a \in \mathbb{Z}_m, \sigma \in S_n} |\Phi_\pi^{a,\sigma}\rangle \langle \Phi_\pi^{a,\sigma}|,$$

where

$$|\Phi_\pi^{a,\sigma}\rangle = \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |a+x, \sigma \pi^x\rangle.$$

But by setting  $x' = a+x$  and  $\sigma' = \sigma \pi^{-a}$ , we get

$$\frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |a+x, \sigma \pi^x\rangle = \frac{1}{\sqrt{m}} \sum_{x'=0}^{m-1} |x', \sigma' \pi^{x'}\rangle,$$

which is identical to the expression in Eq. (11). As we are summing over all  $a \in \mathbb{Z}_m$  and all  $\sigma \in S_n$ , we get  $\rho_{H_\pi} = \rho_\pi$ .

By the standard counting method we find that  $|\mathcal{K}_n^m| = \frac{n!}{(n/m)! m^{n/m}}$ , and using the bounds  $\sqrt{2\pi n} \left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2\pi n} \left(\frac{n}{e}\right)^{n+\frac{1}{12n}}$  we get

$$|\mathcal{K}_n^m| \geq \frac{m^{\frac{1}{2} + \frac{m}{12n}} n^{n - \frac{n}{m} - \frac{m}{12n}}}{e^{n - \frac{n}{m} - \frac{m}{12n}}}.$$

We can now put this into Eq. (9) from Corollary 6 and we find that our scheme is  $\epsilon$ -secure if

$$k \leq \frac{2 \log \epsilon + \left(\frac{m}{12n} - \frac{1}{2}\right) \log m + \left(n - \frac{n}{m} - \frac{m}{12n}\right) (\log n - \log e)}{\log m}. \quad (13)$$

As  $\left(\frac{n}{m} + \frac{m}{12n}\right) \log n + \left(n - \frac{n}{m} - \frac{m}{12n}\right) \log e + \frac{1}{2} \log m \leq \frac{2n}{3} \log n$  for  $m \geq 2$  and  $n \geq 24$ , the theorem is proved.  $\square$

**Corollary 11.** *An encryption scheme as defined in Section 2 using the encryption keys given in Definition 7 is  $\epsilon$ -secure for an exponentially small  $\epsilon$ , namely  $\epsilon = 2^{-\Theta(n)}$ , if the number  $k$  of encryption keys released is*

$$k \leq \frac{n \log n}{3 \log m} - O\left(\frac{n}{\log m}\right). \quad (14)$$

## 5 Concluding Remarks and Further Work

We have proposed a model for a quantum asymmetric-key cryptosystem in Section 2 and given an instance of it in Section 4, with a bound on the number of encryption keys which can be released (Eq. (14)), which is exponentially better in the length of the messages which can be sent than the previously known bound for a quantum asymmetric-key cryptosystem [15, 11]. The notion of security we use is universally composable (Section 3), which guarantees that no matter what information the adversary might get at a later stage or from another protocol which is composed with this encryption scheme, the real system is still  $\epsilon$ -close to the ideal system, for a negligible  $\epsilon$ . (Exponentially small in our specific instance, see Corollary 11.)

An open question is how much the bound on the number of encryption keys which can be released can be improved — if possible at all. This bound is a strict lower bound on the number of copies of the encryption-key state the adversary needs to break the encryption scheme. By finding an upper bound on the number of copies necessary to break the scheme, no matter what encryption-key states are chosen (as long as there exist encoding operations with which they fulfill the correctness condition), we would have a bound beyond which this model of quantum asymmetric-key cryptosystem cannot be improved.

Another line of research is to circumvent the authentic quantum channel requirement. Clearly the encryption keys still need to be distributed authentically. But by including this operation in the scheme, it might be possible to perform it in a less costly way than by invoking a separate protocol.

## References

- [1] Miklos Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the 29th annual ACM Symposium on Theory of Computing*, pp. 284–293, 1997. See also ECCC TR96-065.
- [2] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *FOCS '02: Proceedings of the 43rd Symposium on Foundations of Computer Science*, pp. 449–458, Washington, DC, USA, 2002. IEEE Computer Society. [quant-ph/0205128].
- [3] Michael Ben-Or, Michael Horodecki, Debbie Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography, Second Theory of Cryptography Conference*, pp. 386–406. Springer, 2005. [quant-ph/0409078].

- [4] Michael Ben-Or and Dominic Mayers. General security definition and composability for quantum & classical protocols. eprint, 2004. [quant-ph/0409062].
- [5] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984.
- [6] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. On the (im)possibility of quantum string commitment. eprint, 2005. [quant-ph/0504078].
- [7] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS '01: Proceedings of the 42nd IEEE symposium on Foundations of Computer Science*, p. 136, Washington, DC, USA, 2001. IEEE Computer Society.
- [8] Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.
- [9] David DiVincenzo, Michal Horodecki, Debbie Leung, John Smolin, and Barbara Terhal. Locking classical correlation in quantum states. *Physical Review Letters*, 92:067902, 2004. [quant-ph/0303088].
- [10] Daniel Gottesman and Isaac Chuang. Quantum digital signatures. eprint, 2001. [quant-ph/0105032].
- [11] Masahito Hayashi, Akinori Kawachi, and Hirotsada Kobayashi. Quantum measurements for hidden subgroup problems with optimal sample complexity. eprint, 2006. [quant-ph/0604174].
- [12] Patrick Hayden, Debbie Leung, Peter W. Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250:371, 2004. [doi:10.1007/s00220-004-1087-6].
- [13] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. *Journal of Cryptology*, 9(4):199–216, 1996.
- [14] Akinori Kawachi, Takeshi Koshihara, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In *Advances in Cryptology - EUROCRYPT '05*, LNCS 3494, pp. 268–284. Springer, 2005.
- [15] Akinori Kawachi, Takeshi Koshihara, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. Full version of [14], 2006. [quant-ph/0403069].
- [16] Alexei Kitaev. Quantum measurements and the abelian stabilizer problem. eprint, 1995. [quant-ph/9511026].
- [17] Michele Mosca and Artur Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication*, LNCS 1501, pp. 174–188. Springer, 1999.
- [18] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [19] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryptosystems. In *Advances in Cryptology - CRYPTO 2000*, LNCS 1880, pp. 147–165. Springer, 2000.

- [20] Oded Regev. New lattice-based cryptographic constructions. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pp. 407–416, 2003.
- [21] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology Zurich, September 2005. [quant-ph/0512258].
- [22] Renato Renner and Robert Koenig. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Second Theory of Cryptography Conference, TCC 2005*, volume 3378 of *LNCS*, pp. 407–425. Springer, February 2005. [quant-ph/0403133].
- [23] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
- [24] Dominique Unruh. Simulatable security for quantum protocols. eprint, September 2004.