数理解析研究所講究録
第1554巻 2007年 117-124

Quantum Asymmetric-Key Cryptosystems Secure Against Computationally Unbounded Adversaries

Akinori Kawachi * Christopher Portmann *

Abstract— In this paper we propose quantum asymmetric-key cryptosystems, which do not rely on a computationally hard problem for security, but on uncertainty principles of quantum mechanics, thus obtaining security against computationally unbounded adversaries. 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. [3, 2] 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. [11] 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 [11], which allows the receiver to produce exponentially more encryption keys.

Keywords: quantum cryptography, asymmetric-key cryptography, universal composability, information-theoretic 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 [17]. And new paradigms have to be found.

Where quantum computation makes existing protocols insecure, it also provides new protocols. BB84 [4] 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 [12] 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 [7], quantum string commitment [5] or quantum digital signatures [8], 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 [14], or quantum protocols as in [11]. 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

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

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 quantum asymmetric-key cryptosystems.

Model The first quantum encryption scheme using the same model as ours was proposed by Kawachi et al. in [10]. In this model, which is illustrated in Figure 1 and will be described in more detail in Section 2, Alice distributes a quantum state, ρ_ν, 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., [1] 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.)

Security Alice can perform a measurement to decrypt the message sent to her by Bob, because she knows how she constructed her encryption key ρ_ν, she knows the decryption key ν, so she knows how to measure it. But to the adversary the encryption key looks like a mixture of all possible ρ_ν, and as a measurement destroys the state and quantum mechanics does not allow cloning [12], 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 bellow 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. [10], and its extension in [11], was proved by Hayashi, Kawachi and Kobayashi in [9].

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 [6] and adapted to the quantum setting by Mayers et al. [3, 2] and in parallel by Unruh [18]. 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 [11], which improves the previous best bound on the number of encryption-key states which can be released [9], 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 [3, 2], and proved the scheme secure according to this condition.

More precisely, Hayashi et al. found in [9], 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 [11], 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, 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.

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.

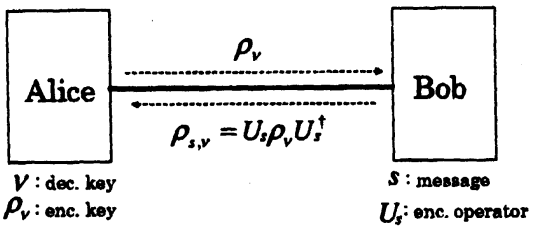

Figure 1: Encryption scheme

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 ρ_ν, 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 ν. 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 ν, which we will refer to as the *correctness* of the protocol. More precisely, we want the probability of Alice decoding the message correctly, $\mathrm{tr}(E_s^\nu \rho_{\nu,s})$, 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 ν, 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 [1], 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

[12] for an overview of these techniques) can be used.

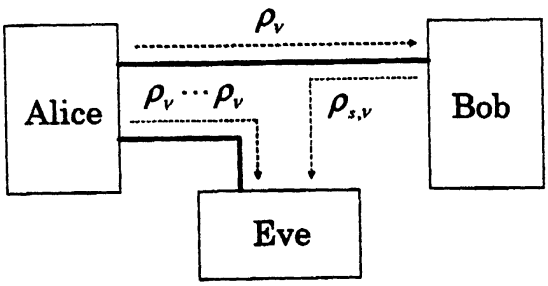

Figure 2: The adversary's attack

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[1] 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 ν 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 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 [6] 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 [6] was extended to the quantum setting by Ben-Or and Mayers in [3] and adapted to quantum key distribution in [2]. 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 [2] and was applied to quantum privacy amplification [16] and quantum key distribution [15]. 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 , 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 [9] for the quantum asymmetric-key cryptosystem proposed in [11].

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 ρ_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

[1] 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.

described by the following density operator:

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

where $\{|s\rangle\}_{s \in S}$ is an orthonormal basis of some Hilbert space $\mathcal{H}_S$. With an ideal protocol $\mathcal{P}_\mathcal{I}$, 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

$$\rho_U \otimes \rho_E, \tag{2}$$

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 ρ_E is the adversary's state, namely

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

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

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

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

According to the work done in [3, 2], 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 ϵ. The protocol $\mathcal{P}$ is said to *ϵ-securely realize* the ideal functionality $\mathcal{P}_\mathcal{I}$, and by the composition theorem from [3, 2], any protocol $\mathcal{Q}$ which is ϵ'-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 [15], if Eq. (4) is respected, the secret S is said to be *ϵ-secure* with respect to $\mathcal{H}_E$. The ideal and real situations are ϵ-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 ν uniformly at random from a set Γ and publishes k copies of the encryption key ρ_ν, the adversary's system conditioned on the secret message being s is then in the state

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

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 ρ_ν, 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*

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

where d is the dimension of ρ_ν and I is the identity operator of dimension d, and if the non-uniformity[2] 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.,

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

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

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

Because $\rho_{\nu,s}$ is obtained from ρ_ν by applying the unitary U_s, and because a unitary operation does

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

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 ρ_{SE} and ρ_E with their exact values (Eqs. (1), (3) and (5)), we get

$$\left\| \sum_{s\in S} P_S(s)|s\rangle\langle s| \otimes \left(\frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu\in\Gamma} \rho_\nu^{\otimes k} + \sigma_s \right) - \frac{1}{|S|} I \otimes \sum_{s\in S} P_S(s) \left(\frac{1}{d} I \otimes \frac{1}{|\Gamma|} \sum_{\nu\in\Gamma} \rho_\nu^{\otimes k} + \sigma_s \right) \right\|_1$$

$$\leq \left\| \sum_{s\in S} P_S(s)|s\rangle\langle s| - \frac{1}{|S|} I \right\|_1 + \left\| \sum_{s\in S} P_S(s)|s\rangle\langle s| \otimes \sigma_s \right\|_1 + \left\| \frac{1}{d} I \otimes \frac{1}{|S|} \sum_{s\in S} \sigma_s \right\|_1 \leq \delta + \frac{\epsilon}{2} + \frac{\epsilon}{2}.$$

□

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 ρ_ν 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 proprieties. 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. 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.

In the following lemma (which is a slight modification of Theorem 2.4 in [9]) and Corollary 6 just after, we substitute coset states $\{\rho_H\}_{H\in\mathrm{H}}$ of subgroups $H \in \mathrm{H}$ 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 ρ_H which can be released, so that the environment can only distinguish with probability ϵ between an encryption key drawn at random and the fully mixed state when provided with k extra copies of it.

Lemma 5. *If* $k \leq \frac{2\log\epsilon + \log|\mathrm{H}|}{\log \max_{H\in\mathrm{H}}|H|} - 1$, *then*

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

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

Proof. Simply by expanding the coset states and using the triangle inequality with a similar argument of [9], we obtain

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

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 ϵ, if $k \leq \frac{2\log\epsilon + \log|\mathrm{H}|}{\log \max_{H\in\mathrm{H}}|H|} - 1$. □

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

$$k \leq \frac{2\log\epsilon + \log|\mathrm{H}|}{\log|H|} - 1. \tag{9}$$

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 ϵ-secure, for an ϵ 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 ρ_π, where π is the decryption key.

Definition 7. Let $\mathcal{K}_n^m \subseteq S_n$, be the set composed of n/m disjoint cyclic permutations. We now define the encryption-key state ρ_π, where the decryption key π is chosen uniformly at random from $\mathcal{K}_n^m$, as

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

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

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 ρ_π, 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., $S = \{0,\cdots,m-1\}$. To encrypt the message s in the state ρ_π defined previously, let Bob apply the unitary

$$U_s := \sum_{x=0}^{m-1} e^{2\pi i s x/m}|x\rangle\langle x|. \tag{11}$$

This unitary is only defined on a space of dimension m and acts on the first register of the encryption-key state ρ_π, 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. (11) 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 ρ_π are only defined with values of the first register $0 \leq x \leq m-1$, so for all decryption keys π 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. (11) take any encryption-key state ρ_π 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 σ, and by linearity the algorithm can extract s from $\rho_{\pi,s}$.

By applying to $|\Phi_{\pi,s}^\sigma\rangle$ the controlled-π^{-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 π^{-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. □

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 ϵ-secure, if the number k of encryption keys released is $k \leq \frac{6\log\epsilon + n\log n}{3\log m}$*

Thus, if the number k of the released encryption keys is at most $n\log n/3\log m - O(n/\log m)$, we can guarantee $\epsilon = 2^{-\Theta(n)}$ by this theorem.

References

[1] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In Proc. FOCS 2002, pages 449–458, 2002.

[2] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In Proc. TCC 2005, pages 386–406, 2005.

[3] M. Ben-Or and D. Mayers. General security definition and composability for quantum & classical protocols. quant-ph/0409062, 2004.

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

[5] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner. On the (im)possibility of quantum string commitment. quant-ph/0504078, 2005.

[6] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In Proc. FOCS 2001, pages 136–145, 2001.

[7] C. Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.

[8] D. Gottesman and I. Chuang. Quantum digital signatures. quant-ph/0105032, 2001.

[9] M. Hayashi, A. Kawachi, and H. Kobayashi. Quantum measurements for hidden subgroup problems with optimal sample complexity. quant-ph/0604174, 2006.

[10] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In Proc. EUROCRYPT 2005, LNCS 3494, pages 268–284, 2005.

[11] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami. Computational indistinguishability between quantum states and its cryptographic application. Full version of [10], quant-ph/0403069, 2006.

[12] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[13] T. Okamoto, K. Tanaka, and S. Uchiyama. Quantum public-key cryptosystems. In Proc. CRYPTO 2000, LNCS 1880, pages 147–165, 2000.

[14] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In Proc. STOC 2005, pages 84–93, 2005.

[15] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology Zurich, September 2005.

[16] R. Renner and R. Koenig. Universally composable privacy amplification against quantum adversaries. In Proc. TCC 2005, LNCS 3378, pages 407–425, 2005.

[17] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SICOMP*, 26(5):1484–1509, 1997.

[18] D. Unruh. Simulatable security for quantum protocols. quant-ph/0409125, 2004.