

On the Power of Quantum Encryption Keys

Akinori Kawachi* and Christopher Portmann†

Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan.

August 21, 2008

Abstract

The standard definition of quantum state randomization, which is the quantum analog of the classical one-time pad, consists in applying some transformation to the quantum message conditioned on a classical secret key k . We investigate encryption schemes in which this transformation is conditioned on a quantum encryption key state ρ_k instead of a classical string, and extend this symmetric-key scheme to an asymmetric-key model in which copies of the same encryption key ρ_k may be held by several different people, but maintaining information-theoretical security.

We find bounds on the message size and the number of copies of the encryption key which can be safely created in these two models in terms of the entropy of the decryption key, and show that the optimal bound can be asymptotically reached by a scheme using classical encryption keys.

This means that the use of quantum states as encryption keys does not allow more of these to be created and shared, nor encrypt larger messages, than if these keys are purely classical.

1 Introduction

1.1 Quantum Encryption

To encrypt a quantum state σ , the standard procedure consists in applying some (unitary) transformation U_k to the state, which depends on a classical string k . This string serves as secret key, and anyone who knows this key can perform the reverse operation and obtain the original state. If the transformations U_1, U_2, \dots are chosen with probabilities p_1, p_2, \dots , such that when averaged over all possible choices of key,

$$\mathcal{R}(\sigma) = \sum_k p_k U_k \sigma U_k^\dagger, \quad (1)$$

the result looks random, i.e., close to the fully mixed state, $\mathcal{R}(\sigma) \approx \text{id}/d$, this cipher can safely be transmitted on an insecure channel. This procedure is

*kawachi@is.titech.ac.jp

†portmann.c.aa@m.titech.ac.jp

called *approximate quantum state randomization* or *approximate quantum one-time pad* [1, 2, 3] or *quantum one-time pad*, *quantum Vernam cipher* or *quantum private channel* in the case of perfect security [4, 5, 6], and is the quantum equivalent of the classical one-time pad.

An encryption scheme which uses such a randomization procedure is called *symmetric*, because the same key is used to encrypt and decrypt the message. An alternative paradigm is *asymmetric-key cryptography*, in which a different key is used for encryption and decryption. In such a cryptosystem the encryption key may be shared amongst many different people, because possessing this key is not sufficient to perform the reverse operation, decryption. This can be seen as a natural extension of symmetric-key cryptography, because this latter corresponds to the special case in which the encryption and decryption keys are identical and can be shared with only one person.

Although the encryption model given in Eq. (1) is symmetric, by replacing the classical encryption key with a quantum state we can make it asymmetric. To see this, let us rewrite Eq. (1) as

$$\mathcal{R}(\sigma) = \sum_k p_k \operatorname{tr}_K \left[U \left(|k\rangle\langle k|^K \otimes \sigma^S \right) U^\dagger \right], \quad (2)$$

where $U := \sum_k |k\rangle\langle k| \otimes U_k$. The encryption key in Eq. (2), $|k\rangle\langle k|$, is diagonal in the computational basis, i.e., classical, but an arbitrary quantum state, ρ_k , could be used instead, e.g.,

$$\mathcal{R}(\sigma) = \sum_k p_k \operatorname{tr}_K \left[U \left(\rho_k^K \otimes \sigma^S \right) U^\dagger \right], \quad (3)$$

for some set of quantum encryption keys $\{\rho_k\}_k$.

If the sender only holds such a quantum encryption key state ρ_k without knowing the corresponding decryption key k , then the resulting model is asymmetric in the sense that possessing this copy of the encryption key state is enough to perform the encryption, but not to decrypt. So many different people can hold copies of the encryption key without compromising the security of the scheme. It is generally impossible to distinguish between non-orthogonal quantum states with certainty (we refer to the textbook by Nielsen and Chuang [7] for an introduction to quantum information), so measuring a quantum state cannot tell us precisely what it is, and possessing a copy of the encryption key state does not allow us to know how the quantum message got transformed, making it impossible to guess the message, except with exponentially small probability.

Up to roughly $\log N$ copies of a state can be needed to discriminate between N possible states [8], so such a scheme could allow the same encryption key to be used several times, if multiple copies of this quantum key state are shared with any party wishing to encrypt a message. The scheme will stay secure as long as the number of copies created stays below a certain threshold. What is more, the security which can be achieved is information-theoretic like for standard quantum state randomization schemes [9], not computational like most asymmetric-key encryption schemes.

Such an asymmetric-key cryptosystem is just a possible application of a quantum state randomization scheme which uses quantum keys. It is also interesting to study quantum state randomization with quantum keys for itself (in the symmetric-key model), without considering other parties holding extra

copies of the same encryption key. In this paper we study these schemes in both the symmetric-key and asymmetric-key models, and compare their efficiency in terms of message size and number of usages of the same encryption key to quantum state randomization schemes which use only classical keys.

1.2 Related Work

Quantum one-time pads were first proposed in [4, 5] for perfect security, then approximate security was considered in, e.g., [1, 2, 3]. All these schemes assume the sender and receiver share some secret classical string which is used only once to perform the encryption. We extend these models in the symmetric-key case by conditioning the encryption operation on a quantum key and considering security with multiple uses of the same key, and then in the asymmetric-key case by considering security with multiple users holding copies of the same encryption key.

The first scheme using quantum keys in an asymmetric-key model was proposed by Kawachi et al. [10], although they considered the restricted scenario of classical messages. Their scheme can encrypt a 1 bit classical message, and their security proof is computational, as it reduces the task of breaking the scheme to a graph automorphism problem. They extended their scheme to a multi-bit version [11], but without security proof. Hayashi et al. [9] then gave an information-theoretical security proof for [11]. The quantum asymmetric-key model we consider is a generalization and extension of that of [10, 11].

1.3 Main Contributions

The main result of this paper is that using quantum encryption keys has no advantage over classical keys with respect to the number of copies of the encryption key which can be safely created and to the size of the messages which can be encrypted, both in the symmetric and asymmetric-key models. Contrary to what was believed and motivated previous works with quantum keys, the intrinsic indistinguishability of quantum states does not allow more of these to be created and shared as encryption keys, than if these keys are purely classical.

To show this, we first find an upper bound on the quantum message size and on the number of copies of the encryption key which can be securely produced. We show that if t copies of the key are created and if the quantum messages encrypted are of dimension d , then they have to be such that $t \log d \lesssim H(\mathcal{K})$ for the scheme to be secure, where $H(\mathcal{K})$ is the entropy of the decryption key.

We then construct a quantum state randomization scheme and show that it meets this upper bound in both the symmetric and asymmetric-key models. The encryption keys this scheme uses are however all diagonal in the same basis, i.e., classical. This means that the scheme with classical keys is optimal in terms of message size and number of usages of the same key, and no scheme with quantum keys can perform better.

We also show how to extend quantum asymmetric-key encryption schemes for classical message (such as [11]) to encrypt quantum messages as well. To do this, we combine these schemes for classical messages with a standard quantum one-time pad, and prove that the resulting scheme is still secure.

1.4 Organization of the Paper

In Section 2 we develop the encryption models with quantum keys sketched in this introduction. We first redefine quantum state randomization schemes using quantum keys instead of classical keys in Section 2.1 and generalize the standard security definition for multiple usage of the same key in this symmetric-key model. In Section 2.2 we then show how to construct an asymmetric-key cryptosystem using such a quantum state randomization scheme with quantum keys and define its security. Section 2.3 contains a few notes about the special case of classical messages, which are relevant for the rest of the paper.

In Section 3 we find an upper bound on the message size and number of copies of the encryption key which can be created, both for the symmetric and asymmetric-key models.

In Section 4 we construct a quantum state randomization scheme which uses classical encryption keys, but which meets the optimality bounds for quantum keys from the previous section in both models. We give this construction in three steps. First in Section 4.1 we construct a scheme which can randomize classical messages only. Then in Section 4.2 we show how to combine this scheme for classical messages with a standard approximate quantum one-time pad to randomize any quantum state. And finally in Section 4.3 we calculate the key size of the scheme proposed and show that it corresponds to the bound found in Section 3.

We conclude in Section 5 with a brief summary and further comments about the results.

2 Encryption Model

2.1 Quantum Encryption Keys

Let us consider a setting in which we have two parties, a sender and a receiver, who wish to transmit a quantum state, σ , from one to the other in a secure way over an insecure channel. If they share a secret classical string, k , they can apply some completely positive, trace-preserving (CPTP) map \mathcal{E}_k to the quantum message and send the cipher $\mathcal{E}_k(\sigma)$. If the key k was chosen with probability p_k , to any person who does not know this key the transmitted state is

$$\mathcal{R}(\sigma) = \sum_k p_k \mathcal{E}_k(\sigma), \quad (4)$$

which will look random for “well chosen” maps \mathcal{E}_k . This is the most general form of quantum state randomization [6].

If instead the sender has a quantum state ρ_k , he can apply some CPTP map \mathcal{E} to both the shared state and the quantum message, and send $\mathcal{E}(\rho_k \otimes \sigma)$. So for someone who does not know ρ_k the state sent is

$$\mathcal{R}(\sigma) = \sum_k p_k \mathcal{E}(\rho_k \otimes \sigma). \quad (5)$$

It is clear that Eqs. (4) and (5) produce equivalent ciphers, because for every set of CPTP maps $\{\mathcal{E}_k\}_k$ there exists a map \mathcal{E} and set of states $\{\rho_k\}_k$ such that for all messages σ , $\mathcal{E}_k(\sigma) = \mathcal{E}(\rho_k \otimes \sigma)$, and vice versa. The difference lies in

the knowledge needed to perform the encryption. In the first case (Eq. (4)) the sender needs to know the secret key k to know which CPTP map \mathcal{E}_k to apply. In the second case (Eq. (5)) the sender only needs to hold a copy of the encryption key ρ_k , he does not need to know what it is or what secret key k it corresponds to. This allows us to construct in Section 2.2 a quantum asymmetric-key cryptosystem in which copies of the same encryption key ρ_k can be used by many different users. In this section we focus on the symmetric-key model and define quantum state randomization (QSR) schemes with quantum encryption keys and their security in this model.

Definition 1. Let $\mathcal{B}(\mathcal{H})$ denote the set of linear operators on \mathcal{H} .

A quantum state randomization (QSR) scheme with quantum encryption keys consists of the following tuple,

$$\mathbb{T} = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E}).$$

$\rho_k \in \mathcal{B}(\mathcal{H}_K)$ are density operators on a Hilbert space \mathcal{H}_K . They are called *encryption keys* and are indexed by elements $k \in \mathcal{K}$ called *decryption keys*.

$P_{\mathcal{K}}(\cdot)$ is a probability distribution over the set of decryption keys \mathcal{K} , corresponding to the probability with which each en/decryption key-pair should be chosen.

$\mathcal{E} : \mathcal{B}(\mathcal{H}_K \otimes \mathcal{H}_S) \rightarrow \mathcal{B}(\mathcal{H}_C)$, is a completely positive, trace-preserving (CPTP) map from the set of linear operators on the joint system of encryption key and message Hilbert spaces, \mathcal{H}_K and \mathcal{H}_S respectively, to the set of linear operators on the cipher Hilbert space \mathcal{H}_C , and is called *encryption operator*.

To encrypt a quantum message given by its density operator $\sigma \in \mathcal{B}(\mathcal{H}_S)$ with the encryption key ρ_k , the encryption operator is applied to the key and message, resulting in the cipher

$$\rho_{k,\sigma} := \mathcal{E}(\rho_k \otimes \sigma).$$

Definition 1 describes how to encrypt a quantum message, but for such a scheme to be useful, it must also be possible to decrypt the message for someone who knows which key k was used, i.e., it must be possible to invert the encryption operation.

Definition 2. A QSR scheme given by the tuple $\mathbb{T} = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E})$ is said to be *invertible on the set* $\mathcal{S} \subseteq \mathcal{B}(\mathcal{H}_S)$ if for every $k \in \mathcal{K}$ with $P_{\mathcal{K}}(k) > 0$ there exists a CPTP map $\mathcal{D}_k : \mathcal{B}(\mathcal{H}_C) \rightarrow \mathcal{B}(\mathcal{H}_S)$ such that for all density operators $\sigma \in \mathcal{S}$,

$$\mathcal{D}_k \mathcal{E}(\rho_k \otimes \sigma) = \sigma.$$

Furthermore, a QSR scheme must – as its name says – randomize a quantum state. We define this in the same way as previous works on approximate quantum state randomization [1, 2, 3], by bounding the distance between the ciphers averaged over all possible choices of key and some state independent from the message. We however generalize this to encrypt t messages with the same key, because the asymmetric-key model we define Section 2.2 will need this. It is always possible to consider the case $t = 1$ in the symmetric-key model, if multiple uses of the same key are not desired.

We will use the trace norm as distance measure between two states, because it is directly related to the probability that an optimal measurement can distinguish between these two states, and is therefore meaningful in the context of

eavesdropping. The trace norm of a matrix A is defined by $\|A\|_{\text{tr}} := \text{tr} |A| = \text{tr} \sqrt{A^\dagger A}$, which is also equal to the sum of the singular values of A .

Definition 3. A QSR scheme given by the tuple $\mathbb{T} = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E})$ is said to be (t, ϵ) -randomizing on the set $\mathcal{S} \subseteq \mathcal{B}(\mathcal{H}_S)$ if there exists a density operator $\tau \in \mathcal{B}(\mathcal{H}_C^{\otimes t})$ such that for all t -tuples of message density operators $\omega = (\sigma_1, \dots, \sigma_t) \in \mathcal{S}^{\times t}$

$$\|\mathcal{R}(\omega) - \tau\|_{\text{tr}} \leq \epsilon, \quad (6)$$

where $\mathcal{R}(\omega) = \sum_k P_{\mathcal{K}}(k) \rho_{k, \sigma_1} \otimes \dots \otimes \rho_{k, \sigma_t}$ and $\rho_{k, \sigma_i} = \mathcal{E}(\rho_k \otimes \sigma_i)$.

2.2 Quantum Asymmetric-Key Cryptosystem

As announced in the previous section, the idea behind the quantum asymmetric-key cryptosystem model is that many different people hold a copy of some quantum state ρ_k which serves as encryption key, and anyone who wishes to send a message to the originator of the encryption keys uses a quantum state randomization scheme, as described in Definition 1. This is depicted in Figure 1.

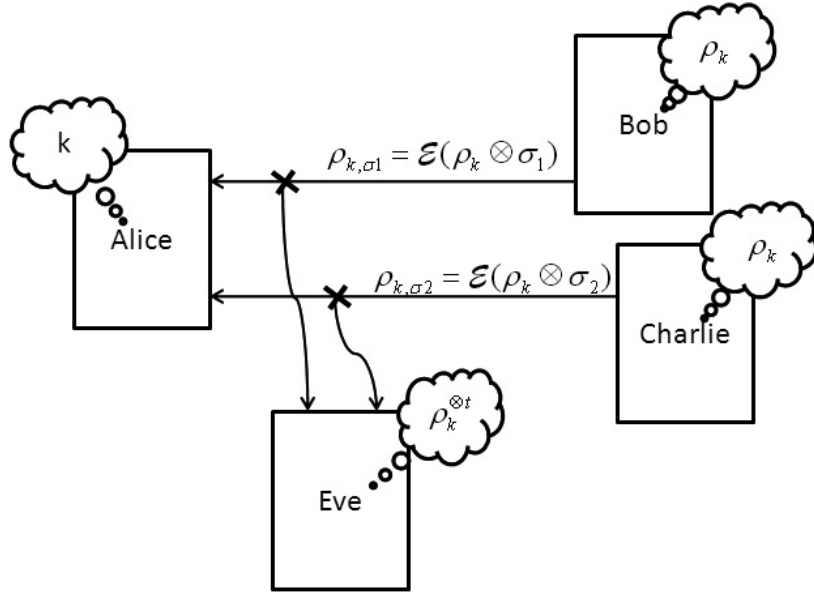


Figure 1: *Quantum asymmetric-key cryptosystem model.* Bob and Charlie hold copies of Alice's encryption key ρ_k . To send her a message, they encrypt it with the key and a given QSR scheme, and send the resulting cipher to her. An eavesdropper, Eve, may intercept the ciphers as well as possess some copies of the encryption key herself.

If the QSR scheme used to encrypt the messages is (t, ϵ) -randomizing and no more than t copies of the encryption key were released, an eavesdropper who intercepts the ciphers will not be able to distinguish them from some state independent from the messages, so not get any information about these messages. This is however not the only attack he may perform.

As we consider a scenario in which copies of the encryption key are shared between many different people, the adversary could hold one or many of them. If a total of t copies of the encryption key were produced and t_1 were used to encrypt messages $\omega = (\sigma_1, \dots, \sigma_{t_1})$, in the worst case we have to assume that the adversary has the $t_2 := t - t_1$ remaining unused copies of the key. So his total state is

$$\rho_\omega^E := \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, \sigma_1} \otimes \dots \otimes \rho_{k, \sigma_{t_1}} \otimes \rho_k^{\otimes t_2}, \quad (7)$$

where ρ_{k, σ_i} is the cipher of the message σ_i encrypted with the key ρ_k . This leads to the following security definition.

Definition 4. We call a quantum asymmetric-key cryptosystem (t, ϵ) -*indistinguishable on the set* $\mathcal{S} \subseteq \mathcal{B}(\mathcal{H}_S)$ if for all $t_1 \in \{0, 1, \dots, t\}$, $t_2 := t - t_1$, there exists a density operator $\tau \in \mathcal{B}(\mathcal{H}_C^{\otimes t_1} \otimes \mathcal{H}_K^{\otimes t_2})$ such that for all t_1 -tuples of message density operators $\omega = (\sigma_1, \dots, \sigma_{t_1}) \in \mathcal{S}^{\times t_1}$,

$$\|\rho_\omega^E - \tau\|_{\text{tr}} \leq \epsilon,$$

where ρ_ω^E is the state the adversary obtains as defined in Eq. (7).

Remark 5. Definition 4 is clearly more general than the security criteria of Definition 3 ((t, ϵ) -randomization) as this latter corresponds to the special case $t_1 = t$. However, for the scheme constructed in Section 4 the two are equivalent, and proving one proves the other. This is the case in particular if the encryption key is equal to the cipher of some specific message σ_0 , i.e., $\rho_k = \rho_{k, \sigma_0} = \mathcal{E}(\rho_k \otimes \sigma_0)$, in which case holding an extra copy of the encryption key does not give more information about the decryption key than holding an extra cipher state.

2.3 Classical Messages

In the following sections we will also be interested in the special case of schemes which encrypt classical messages only. Classical messages can be represented by a set of mutually orthogonal quantum states, which we will take to be the basis states of the message Hilbert space and denote by $\{|s\rangle\}_{s \in \mathcal{S}}$. So these schemes must be invertible and randomizing on the set of basis states of the message Hilbert space.

When considering classical messages only, we will simplify the notation when possible and represent a message by a string s instead of by its density matrix $|s\rangle\langle s|$, e.g., the cipher of the message s encrypted with the key ρ_k is

$$\rho_{k, s} := \mathcal{E}(\rho_k \otimes |s\rangle\langle s|).$$

Remark 6. Definition 2 (invertibility) can be simplified when only classical messages are considered: a QSR scheme given by the tuple $\mathbb{T} = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E})$ is invertible for the set of classical messages \mathcal{S} , if for every $k \in \mathcal{K}$ with $P_{\mathcal{K}}(k) > 0$ the ciphers $\{\rho_{k, s}\}_{s \in \mathcal{S}}$ are mutually orthogonal, where $\rho_{k, s} := \mathcal{E}(\rho_k \otimes |s\rangle\langle s|)$ for some orthonormal basis $\{|s\rangle\}_{s \in \mathcal{S}}$ of the message Hilbert space \mathcal{H}_S .

We will also use a different but equivalent definition to measure how well a scheme can randomize a message when dealing with classical messages. This new security criteria allows us to simplify some proofs.

Definition 7. A QSR scheme given by the tuple $\mathbb{T} = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E})$ is said to be (t, ϵ) -secure for the set of classical messages \mathcal{S} if for all probability distributions $P_{\mathcal{S}^t}(\cdot)$ over the set of t -tuples of messages $\mathcal{S}^{\times t}$,

$$\left\| \rho^{S^t C^t} - \rho^{S^t} \otimes \rho^{C^t} \right\|_{\text{tr}} \leq \epsilon, \quad (8)$$

where $\rho^{S^t C^t}$ is the state of the joint systems of t -fold message and cipher Hilbert spaces, and ρ^{S^t} and ρ^{C^t} are the result of tracing out the cipher respectively message systems. I.e.,

$$\begin{aligned} \rho^{S^t C^t} &= \sum_{s \in \mathcal{S}^{\times t}} P_{\mathcal{S}^t}(s) |s\rangle\langle s| \otimes \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}, \\ \rho^{S^t} &= \sum_{s \in \mathcal{S}^{\times t}} P_{\mathcal{S}^t}(s) |s\rangle\langle s|, \\ \rho^{C^t} &= \sum_{s \in \mathcal{S}^{\times t}} P_{\mathcal{S}^t}(s) \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}, \end{aligned}$$

where $s = (s_1, \dots, s_t)$.

This security definition can be interpreted the following way. No matter what the probability distribution on the secret messages is – let the adversary choose it – the message and cipher spaces are nearly in product form, i.e., the cipher gives next to no information about the message.

The following lemma proves that this new security definition is equivalent to the previous one (Definition 3) up to a constant factor.

Lemma 8. *If a QSR scheme is (t, ϵ) -randomizing for a set of classical messages \mathcal{S} , then it is $(t, 2\epsilon)$ -secure for \mathcal{S} . If a QSR scheme is (t, ϵ) -secure for a set of classical messages \mathcal{S} , then it is $(t, 2\epsilon)$ -randomizing for \mathcal{S} .*

Proof. In order to simplify the notation we will set $s := (s_1, \dots, s_t)$ and $\rho_{k, s} := \rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}$. The left-hand side of Eq. (8) can then be rewritten as

$$\begin{aligned} & \left\| \rho^{S^t C^t} - \rho^{S^t} \otimes \rho^{C^t} \right\|_{\text{tr}} \\ &= \left\| \sum_{s \in \mathcal{S}^{\times t}} P_{\mathcal{S}^t}(s) |s\rangle\langle s| \otimes \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s} \right. \\ & \quad \left. - \sum_{s \in \mathcal{S}^{\times t}} P_{\mathcal{S}^t}(s) |s\rangle\langle s| \otimes \sum_{\substack{r \in \mathcal{S}^{\times t} \\ k \in \mathcal{K}}} P_{\mathcal{K}}(k) P_{\mathcal{S}^t}(r) \rho_{k, r} \right\|_{\text{tr}} \\ &= \sum_{s \in \mathcal{S}^{\times t}} P_{\mathcal{S}^t}(s) \left\| \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s} - \sum_{\substack{r \in \mathcal{S}^{\times t} \\ k \in \mathcal{K}}} P_{\mathcal{K}}(k) P_{\mathcal{S}^t}(r) \rho_{k, r} \right\|_{\text{tr}}. \quad (9) \end{aligned}$$

If this must be less than ϵ for all probability distributions $P_{\mathcal{S}^t}$ then for the distribution $P_{\mathcal{S}^t}(s_1) = P_{\mathcal{S}^t}(s_2) = 1/2$ for any two elements $s_1, s_2 \in \mathcal{S}^{\times t}$ we have from Eq. (9)

$$\frac{1}{2} \left\| \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_1} - \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_2} \right\|_{\text{tr}} \leq \epsilon.$$

This immediately implies $(t, 2\epsilon)$ -randomization.

To prove the converse we apply the triangle inequality to Eq. (9) and get

$$\left\| \rho^{S^t C^t} - \rho^{S^t} \otimes \rho^{C^t} \right\|_{\text{tr}} \leq \sum_{s \in \mathcal{S}^{\times t}} P_{S^t}(s) \sum_{r \in \mathcal{S}^{\times t}} P_{S^t}(r) \left\| \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k,s} - \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k,r} \right\|_{\text{tr}}.$$

By the definition of (t, ϵ) -randomization (Definition 3) and the triangle inequality we know that

$$\left\| \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k,s} - \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k,r} \right\|_{\text{tr}} \leq 2\epsilon,$$

for all $r, s \in \mathcal{S}^{\times t}$, which concludes the proof. \square

3 Lower Bounds on the Key Size

It is intuitively clear that the more copies of the encryption key state ρ_k are created, the more information the adversary gets about the decryption key $k \in \mathcal{K}$ and the more insecure the scheme becomes. As it turns out, the number of copies of the encryption key which can be safely used is directly linked to the size of the decryption key, i.e., the cardinality of the decryption key set \mathcal{K} .

Let us assume a QSR scheme with quantum encryption keys is used to encrypt classical messages of size m . Then if t copies of the encryption key state are released and used, the size of the total message encrypted with the same decryption key k is tm . We prove in this section that the decryption key has to be of the same size as the total message to achieve information-theoretical security, i.e., $\log |\mathcal{K}| \gtrsim tm$. In Section 4 we then give a scheme which reaches this bound asymptotically.

Theorem 9. *If a QSR scheme given by the tuple $\mathbb{T} = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E})$ is invertible for the set of classical messages \mathcal{S} , then when t messages (s_1, \dots, s_t) are chosen from \mathcal{S} with (joint) probability distribution $P_{S^t}(s_1, \dots, s_t)$ and encrypted with the same key,*

$$\left\| \rho^{S^t C^t} - \rho^{S^t} \otimes \rho^{C^t} \right\|_{\text{tr}} \geq \frac{H(S^t) - H(\mathcal{K}) - 2}{4t \log |S|}, \quad (10)$$

where $H(\cdot)$ is the Shannon entropy and $\rho^{S^t C^t}$ is the state of the t -fold message and cipher systems:

$$\begin{aligned} \rho^{S^t C^t} &= \sum_{s \in \mathcal{S}^{\times t}} P_{S^t}(s) |s\rangle\langle s| \otimes \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k,s_1} \otimes \dots \otimes \rho_{k,s_t}, \\ \rho^{S^t} &= \sum_{s \in \mathcal{S}^{\times t}} P_{S^t}(s) |s\rangle\langle s|, \\ \rho^{C^t} &= \sum_{s \in \mathcal{S}^{\times t}} P_{S^t}(s) \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k,s_1} \otimes \dots \otimes \rho_{k,s_t}, \end{aligned} \quad (11)$$

where $s = (s_1, \dots, s_t)$.

Proof. A theorem by Alicki and Fanes [12] tells us that for any two states ρ^{AB} and σ^{AB} on the joint system $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $\delta := \|\rho^{AB} - \sigma^{AB}\|_{\text{tr}} \leq 1$ and $d_A := \dim \mathcal{H}_A$,

$$|\text{S}(\rho^{AB}|\rho^B) - \text{S}(\sigma^{AB}|\sigma^B)| \leq 4\delta \log d_A + 2h(\delta), \quad (12)$$

where $\text{S}(\rho^{AB}|\rho^B) := \text{S}(\rho^{AB}) - \text{S}(\rho^B)$ is the conditional Von Neumann entropy and $h(p) := p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$ is the binary entropy. $h(\delta) \leq 1$, so from Eq. (12) we get

$$\|\rho^{AB} - \sigma^{AB}\|_{\text{tr}} \geq \frac{|\text{S}(\rho^{AB}|\rho^B) - \text{S}(\sigma^{AB}|\sigma^B)| - 2}{4 \log d_A}.$$

By applying this to the left-hand side of Eq. (10) we obtain

$$\left\| \rho^{S^t C^t} - \rho^{S^t} \otimes \rho^{C^t} \right\|_{\text{tr}} \geq \frac{\text{S}(\rho^{S^t}) + \text{S}(\rho^{C^t}) - \text{S}(\rho^{S^t C^t}) - 2}{4t \log |\mathcal{S}|}.$$

To prove this theorem it remains to show that

$$\text{S}(\rho^{S^t}) + \text{S}(\rho^{C^t}) - \text{S}(\rho^{S^t C^t}) \geq \text{H}(\mathcal{S}^t) - \text{H}(\mathcal{K}).$$

For this we will need the two following bounds on the Von Neumann entropy (see e.g, [7]):

$$\begin{aligned} \text{S}\left(\sum_{x \in \mathcal{X}} p_x \rho_x\right) &\geq \sum_{x \in \mathcal{X}} p_x \text{S}(\rho_x), \\ \text{S}\left(\sum_{x \in \mathcal{X}} p_x \rho_x\right) &\leq \text{H}(\mathcal{X}) + \sum_{x \in \mathcal{X}} p_x \text{S}(\rho_x). \end{aligned}$$

Equality is obtained in the second equation if the states $\{\rho_x\}_{x \in \mathcal{X}}$ are all mutually orthogonal. By using these bounds and Eq. (11) we see that

$$\begin{aligned} \text{S}(\rho^{S^t C^t}) &= \text{H}(\mathcal{S}^t) + \sum_{s \in \mathcal{S}^t} P_{\mathcal{S}^t}(s) \text{S}\left(\sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}\right) \\ &\leq \text{H}(\mathcal{S}^t) + \text{H}(\mathcal{K}) + \sum_{\substack{s \in \mathcal{S}^t \\ k \in \mathcal{K}}} P_{\mathcal{K}}(k) P_{\mathcal{S}^t}(s) \text{S}(\rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}), \\ \text{S}(\rho^{S^t}) &= \text{H}(\mathcal{S}^t), \\ \text{S}(\rho^{C^t}) &\geq \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \text{S}\left(\sum_{s \in \mathcal{S}^t} P_{\mathcal{S}^t}(s) \rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}\right) \\ &= \text{H}(\mathcal{S}^t) + \sum_{\substack{s \in \mathcal{S}^t \\ k \in \mathcal{K}}} P_{\mathcal{K}}(k) P_{\mathcal{S}^t}(s) \text{S}(\rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}). \end{aligned}$$

We have equality in the last line because the scheme is invertible on \mathcal{S} , i.e., by Definition 2 and Remark 6 the states $\{\rho_{k, s_1} \otimes \cdots \otimes \rho_{k, s_t}\}_{s_1, \dots, s_t \in \mathcal{S}}$ are mutually orthogonal. By putting this all together we conclude the proof. \square

Corollary 10. *For a QSR scheme to be (t, ϵ) -randomizing or (t, ϵ) -indistinguishable, it is necessary that*

$$H(\mathcal{K}) \geq (1 - 8\epsilon)t \log d - 2, \quad (13)$$

where d is the dimension of the message Hilbert space \mathcal{H}_S and $H(\mathcal{K})$ is the entropy of the decryption key.

Proof. Definition 7 says that for a scheme to be (t, ϵ) -secure we need

$$\left\| \rho^{S^t C^t} - \rho^{S^t} \otimes \rho^{C^t} \right\|_{\text{tr}} \leq \epsilon$$

for all probability distributions P_{S^t} . So for the uniform distribution we get from Theorem 9 that for a scheme to be (t, ϵ) -secure we need

$$H(\mathcal{K}) \geq (1 - 4\epsilon)t \log |\mathcal{S}| - 2.$$

By Lemma 8 we then have the condition

$$H(\mathcal{K}) \geq (1 - 8\epsilon)t \log |\mathcal{S}| - 2$$

for the scheme to be (t, ϵ) -randomizing for the classical messages \mathcal{S} . And as classical messages are a subset of quantum messages – namely an orthonormal basis of the message Hilbert space – this bound extends to the case of quantum messages on a Hilbert space of dimension $d_S = |\mathcal{S}|$.

As (t, ϵ) -randomization is a special case of (t, ϵ) -indistinguishability, namely for $t_1 = t$, it is immediate that this lower bound also applies to (t, ϵ) -indistinguishability. \square

Remark 11. Approximate quantum one-time pad schemes usually only consider the special case in which the cipher has the same dimension as the message [1, 3]. A more general scenario in which an ancilla is appended to the message is however also possible. It was proven in [6] that for perfect security such an extended scheme needs a key of the same size as in the restricted scenario, namely $2 \log d$. Corollary 10 for $t = 1$ shows the same for approximate security, namely roughly $\log d$ bits of key are necessary, just as when no ancilla is present.

4 Near-Optimal Scheme

To simplify the presentation of the QSR scheme, we first define it for classical messages in Section 4.1, show that it is invertible and find a bound on t , the number of copies of the encryption key which can be released, for it to be (t, ϵ) -randomizing for an exponentially small ϵ . In Section 4.2 we extend the scheme to encrypt any quantum message of a given size, and show again that it is invertible and randomizing. And finally in Section 4.3 we calculate the size of the key necessary to encrypt a message of a given length, and show that it is nearly asymptotically equal to the lower bound found in Section 3.

4.1 Classical Messages

Without loss of generality, let the message space be of dimension $\dim \mathcal{H}_S = 2^m$. The classical messages can then be represented by strings of length m , $\mathcal{S} := \{0, 1\}^m$. We now define a QSR scheme which uses encryption key states of dimension $\dim \mathcal{H}_K = 2^{m+n}$, where n is a security parameter, i.e., the scheme will be (t, ϵ) -randomizing for $\epsilon = 2^{-\Theta(n)}$.

We define the set of decryption keys to be the set of all $(m \times n)$ binary matrices,

$$\mathcal{K} := \{0, 1\}^{m \times n}. \quad (14)$$

This set has size $|\mathcal{K}| = 2^{mn}$ and each key is chosen with uniform probability.

For every decryption key $A \in \mathcal{K}$ the corresponding encryption key is defined as

$$\rho_A := \frac{1}{2^n} \sum_{x \in \{0, 1\}^n} |Ax, x\rangle\langle Ax, x|, \quad (15)$$

where Ax is the multiplication of the matrix A with the vector x .

The encryption operator $\mathcal{E} : \mathcal{B}(\mathcal{H}_K \otimes \mathcal{H}_S) \rightarrow \mathcal{B}(\mathcal{H}_C)$ consists in applying the unitary

$$U := \sum_{\substack{x \in \{0, 1\}^n \\ s, y \in \{0, 1\}^m}} |y \oplus s, x\rangle\langle y, x|^K |s\rangle\langle s|^S$$

and tracing out the message system S , i.e.,

$$\rho_{A, s} := \text{tr}_S \left(U \left(\rho_k^K \otimes |s\rangle\langle s|^S \right) U^\dagger \right).$$

This results in the cipher for the message s being

$$\rho_{A, s} = \frac{1}{2^n} \sum_{x \in \{0, 1\}^n} |Ax \oplus s, x\rangle\langle Ax \oplus s, x|. \quad (16)$$

These states are mutually orthogonal for different messages s so by Remark 6 this scheme is invertible.

We now show that this scheme is (t, ϵ) -randomizing for $\epsilon = 2^{-\delta n + 1}$ and $t = (1 - \delta)n$, $0 < \delta < 1$.

Theorem 12. *For the QSR scheme defined above in Eqs. (14), (15) and (16) there exists a density operator $\tau \in \mathcal{B}(\mathcal{H}_C^{\otimes t})$ such that for all t -tuples of messages $s = (s_1, \dots, s_t) \in \mathcal{S}^{\times t}$, if $t = (1 - \delta)n$, $0 < \delta < 1$, then*

$$\|\gamma_s - \tau\|_{tr} \leq 2^{-\delta n + 1},$$

where γ_s is the encryption of s with this scheme averaged over all possible keys, i.e.,

$$\gamma_s = \sum_{A \in \mathcal{K}} P_{\mathcal{K}}(A) \rho_{A, s_1} \otimes \dots \otimes \rho_{A, s_t}. \quad (17)$$

Proof. The τ in question is the fully mixed state $\tau = \frac{1}{2^{t(m+n)}} \text{id}$. By placing the values of the ciphers from Eq. (16) in Eq. (17) we get

$$\gamma_s = \frac{1}{2^{mn} 2^{tn}} \sum_{\substack{A \in \{0, 1\}^{m \times n} \\ x_1, \dots, x_t \in \{0, 1\}^n}} |\dots, Ax_i \oplus s_i, x_i, \dots\rangle\langle \dots, Ax_i \oplus s_i, x_i, \dots|.$$

A unitary performing bit flips can take γ_s to γ_r for any $s, r \in \mathcal{S}^t$, so

$$\left\| \gamma_s - \frac{1}{2^{t(m+n)}} \text{id} \right\|_{\text{tr}} = \left\| \gamma_r - \frac{1}{2^{t(m+n)}} \text{id} \right\|_{\text{tr}},$$

and it is sufficient to evaluate

$$\left\| \gamma_0 - \frac{1}{2^{t(m+n)}} \text{id} \right\|_{\text{tr}} = \sum_{e \in \text{EVec}(\gamma_0)} \left| w_e - \frac{1}{2^{t(m+n)}} \right|, \quad (18)$$

where e are the eigenvectors of γ_0 and w_e the corresponding eigenvalues.

So we need to calculate the eigenvalues of

$$\gamma_0 = \frac{1}{2^{mn} 2^{tn}} \sum_{\substack{A \in \{0,1\}^{m \times n} \\ x_1, \dots, x_t \in \{0,1\}^n}} |Ax_1, x_1, \dots, Ax_t, x_t\rangle \langle Ax_1, x_1, \dots, Ax_t, x_t|. \quad (19)$$

Let us fix x_1, \dots, x_t . It is immediate from the linearity of Ax that if exactly d of the vectors $\{x_i\}_{i=1}^t$ are linearly independent, then

$$\sum_{A \in \{0,1\}^{m \times n}} |Ax_1, x_1, \dots, Ax_t, x_t\rangle \langle Ax_1, x_1, \dots, Ax_t, x_t|$$

uniformly spans a space of dimension 2^{dm} , and for different values of x_1, \dots, x_t these subspaces are all mutually orthogonal. Let D_t be the random variable representing the number of independent vectors amongst t binary vectors of length n , when chosen uniformly at random, and let $P_{D_t}(d) = \Pr[D_t = d]$ be the probability that exactly d of these vectors are linearly independent. The matrix given in Eq. (19) then has exactly $2^{tn} P_{D_t}(d) 2^{dm}$ eigenvectors with eigenvalue $\frac{1}{2^{dm} 2^{tn}}$, for $0 \leq d \leq t$. The remaining eigenvectors have eigenvalue 0.

So Eq. (18) becomes

$$\begin{aligned} \sum_{e \in \text{EVec}(\rho_0^E)} \left| w_e - \frac{1}{2^{t(m+n)}} \right| &= 2 \sum_{d=0}^t 2^{tn} P_{D_t}(d) 2^{dm} \left(\frac{1}{2^{dm} 2^{tn}} - \frac{1}{2^{t(m+n)}} \right) \\ &= 2 \sum_{d=0}^t P_{D_t}(d) \left(1 - 2^{-(t-d)m} \right) \\ &\leq 2 \sum_{d=0}^{t-1} P_{D_t}(d) = 2(1 - P_{D_t}(t)) \\ &\leq 2^{t-n+1}. \end{aligned}$$

For $t = (1 - \delta)n$, $0 < \delta < 1$, we have for all $s \in \mathcal{S}^t$, $\|\gamma_s - \tau\|_{\text{tr}} \leq 2^{-\delta n+1}$. \square

Corollary 13. *An asymmetric-key cryptosystem using this QSR scheme is (t, ϵ) -indistinguishable (Definition 4) for $\epsilon = 2^{-\delta n+1}$ and $t = (1 - \delta)n$, $0 < \delta < 1$.*

Proof. As noted in Section 2.2 this scheme is such that the encryption keys are identical to the ciphers of the message 0, $\rho_{k,0} = \rho_k = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |Ax, x\rangle \langle Ax, x|$. So if t_1 copies of the encryption key were used to encrypt the messages $s =$

(s_1, \dots, s_{t_1}) and the adversary holds these ciphers and the $t_2 = t - t_1$ extra copies of the encryption key,

$$\rho_s^E = \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_1} \otimes \dots \otimes \rho_{k, s_{t_1}} \otimes \rho_k^{\otimes t_2}.$$

Then $\rho_s^E = \gamma_r$ for $r = (s_1, \dots, s_{t_1}, 0, \dots, 0)$ and by Theorem 12, $\|\gamma_r - \tau\|_{\text{tr}} \leq \epsilon$. \square

4.2 Quantum Messages

We will now extend the encryption scheme given above to encrypt any quantum state, not only classical ones. To do this we will show how to combine a QSR scheme with quantum keys which is (t, ϵ_1) -randomizing for classical messages (like the one from Section 4.1) with a QSR scheme with classical keys which is $(1, \epsilon_2)$ -randomizing for quantum states (which is the case of any standard QSR scheme, e.g., [4, 5, 1, 2, 3, 6]) to produce a QSR scheme which is $(t, \epsilon_1 + t\epsilon_2)$ -randomizing. The general idea is to choose a classical key for the second scheme at random, encrypt the quantum message with this scheme, then encrypt the classical key with the quantum encryption key of the first scheme, and send both ciphers.

Theorem 14. *Let a QSR scheme with quantum keys be given by the tuple $\mathbb{T}_1 = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{E})$, where $\mathcal{E} : \mathcal{B}(\mathcal{H}_K \otimes \mathcal{H}_S) \rightarrow \mathcal{B}(\mathcal{H}_C)$, and let a QSR scheme with classical keys be given by the tuple $\mathbb{T}_2 = (P_{\mathcal{S}}, \{\mathcal{F}_s\}_{s \in \mathcal{S}})$, where $\mathcal{F}_s : \mathcal{B}(\mathcal{H}_R) \rightarrow \mathcal{B}(\mathcal{H}_D)$. We combine the two to produce the QSR scheme with quantum encryption keys given by $\mathbb{T}_3 = (P_{\mathcal{K}}, \{\rho_k\}_{k \in \mathcal{K}}, \mathcal{G})$, where $\mathcal{G} : \mathcal{B}(\mathcal{H}_K \otimes \mathcal{H}_R) \rightarrow \mathcal{B}(\mathcal{H}_C \otimes \mathcal{H}_D)$ is defined by*

$$\mathcal{G}(\rho_k \otimes \sigma) := \sum_{s \in \mathcal{S}} P_{\mathcal{S}}(s) \mathcal{E}(\rho_k \otimes |s\rangle\langle s|) \otimes \mathcal{F}_s(\sigma). \quad (20)$$

If \mathbb{T}_1 forms a quantum asymmetric-key cryptosystem which is invertible and (t, ϵ_1) -indistinguishable (respectively randomizing) for the basis states of \mathcal{H}_S and \mathbb{T}_2 is an invertible and $(1, \epsilon_2)$ -randomizing QSR scheme for any state on \mathcal{H}_R , then \mathbb{T}_3 forms an invertible and $(t, \epsilon_1 + t\epsilon_2)$ -indistinguishable (respectively randomizing) cryptosystem for all density operator messages on \mathcal{H}_R .

Proof. The invertibility of the scheme formed with \mathbb{T}_3 is immediate. To prove the indistinguishability we need to show that for all $t_1 \in \{0, 1, \dots, t\}$, $t_2 := t - t_1$, there exists a density operator $\tau \in \mathcal{B}(\mathcal{H}_C^{\otimes t_1} \otimes \mathcal{H}_K^{\otimes t_2} \otimes \mathcal{H}_D^{\otimes t_1})$ such that for all t_1 -tuples of message density operators $\omega = (\sigma_1, \dots, \sigma_{t_1}) \in \mathcal{B}(\mathcal{H}_R)^{\times t_1}$, $\|\rho_{\omega}^E - \tau\|_{\text{tr}} \leq \epsilon$, where $\rho_{\omega}^E = \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \mathcal{G}(\rho_k \otimes \sigma_1) \otimes \dots \otimes \mathcal{G}(\rho_k \otimes \sigma_{t_1}) \otimes \rho_k^{\otimes t_2}$.

Let us write $\gamma_s := \sum_{k \in \mathcal{K}} P_{\mathcal{K}}(k) \rho_{k, s_1} \otimes \dots \otimes \rho_{k, s_{t_1}} \otimes \rho_k^{\otimes t_2}$, where $s = (s_1, \dots, s_{t_1})$ and $\rho_{k, s_i} = \mathcal{E}(\rho_k \otimes |s_i\rangle\langle s_i|)$, and $\mu_{\sigma} := \sum_{s \in \mathcal{S}} P_{\mathcal{S}}(s) \mathcal{F}_s(\sigma)$. And let τ_1 and τ_2 be the two states such that $\|\gamma_s - \tau_1\|_{\text{tr}} \leq \epsilon_1$ and $\|\mu_{\sigma} - \tau_2\|_{\text{tr}} \leq \epsilon_2$ for all s and σ respectively. We define $\delta_s := \gamma_s - \tau_1$ and $\tau := \tau_1 \otimes \tau_2^{\otimes t_1}$. Then by the triangle

inequality and changing the order of the registers

$$\begin{aligned}
\|\rho_\omega^E - \tau\|_{\text{tr}} &\leq \left\| \sum_{s \in \mathcal{S}^{\times t_1}} P_{\mathcal{S}^t}(s) \delta_s \otimes \mathcal{F}_{s_1}(\sigma_1) \otimes \cdots \otimes \mathcal{F}_{s_{t_1}}(\sigma_{t_1}) \right\|_{\text{tr}} \\
&\quad + \|\tau_1 \otimes \mu_{\sigma_1} \otimes \cdots \otimes \mu_{\sigma_{t_1}} - \tau\|_{\text{tr}} \\
&\leq \sum_{s \in \mathcal{S}^{\times t_1}} P_{\mathcal{S}^t}(s) \|\delta_s\|_{\text{tr}} + \sum_{i=1}^{t_1} \|\mu_{\sigma_i} - \tau_2\|_{\text{tr}} \\
&\leq \epsilon_1 + t_1 \epsilon_2.
\end{aligned}$$

As (t, ϵ) -randomization is a special case of (t, ϵ) -indistinguishability, namely for $t_1 = t$, it is immediate from Theorem 14 that \mathbb{T}_3 is also $(t, \epsilon_1 + t\epsilon_2)$ -randomizing. \square

4.3 Key Size

To construct the QSR scheme for quantum messages as described in Section 4.2 we combine the scheme for classical messages from Section 4.1 and the approximate one-time pad scheme of Dickinson and Nayak [3].

The scheme from Section 4.1 is (t, ϵ_1) -randomizing for $t = (1 - \delta)n$ and $\epsilon_1 = 2^{-\delta n + 1}$, and uses a key with entropy $H(\mathcal{K}) = nm = (t + \log \frac{1}{\epsilon_1} + 1)m$. The scheme of Dickinson and Nayak [3] is $(1, \epsilon_2)$ -randomizing and uses a key with entropy $m = \log d + \log \frac{1}{\epsilon_2} + 4$ to encrypt a quantum state of dimension d . So by combining these our final scheme is $(t, \epsilon_1 + t\epsilon_2)$ -randomizing and uses a key with entropy

$$H(\mathcal{K}) = (t + \log \frac{1}{\epsilon_1} + 1)(\log d + \log \frac{1}{\epsilon_2} + 4)$$

to encrypt t states of dimension d . By choosing ϵ_1 and ϵ_2 to be polynomial in $\frac{1}{t}$ and $\frac{1}{\log d}$ respectively, the key has size $H(\mathcal{K}) = t \log d + o(t \log d)$, which nearly reaches the asymptotic optimality found in Eq. (13), namely $H(\mathcal{K}) \geq (1 - 8\epsilon)t \log d - 2$. Exponential security can be achieved at the cost of a slightly reduced asymptotic efficiency. For $\epsilon_1 = 2^{-\delta_1 t}$ and $\epsilon_2 = d^{-\delta_2}$ for some small $\delta_1, \delta_2 > 0$, the key has size $H(\mathcal{K}) = (1 + \delta_1)(1 + \delta_2)t \log d + o(t \log d)$.

5 Consequence for Quantum Keys

The scheme presented in Section 4 uses the encryption keys

$$\rho_A = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |Ax, x\rangle \langle Ax, x|, \quad (21)$$

for some $(m \times n)$ -matrix decryption key A . Although these keys are written as quantum states using the bra-ket notation to fit in the framework for QSR schemes with quantum keys developed in the previous sections, the states from Eq. (21) are all diagonal in the computational basis. So they are classical and could have been represented by a classical random variable \mathcal{X}_A which takes the value (Ax, x) with probability 2^{-n} .

This scheme meets the optimality bound on the key size from Section 3. This bound tells us that for a given set of decryption keys \mathcal{K} , no matter how the encryption keys $\{\rho_k\}_{k \in \mathcal{K}}$ are constructed, the number of copies of the encryption keys which can be created, t , and the dimension of the messages which can be encrypted, d , have to be such that $t \log d \lesssim H(\mathcal{K})$ for the scheme to be information-theoretically secure. From the construction of the scheme in Section 4 we know that this bound is met by a scheme using classical keys. Hence no scheme using quantum keys can perform better. So using quantum keys in a quantum state randomization scheme has no advantage with respect to the message size and number of usages of the same key over classical keys.

This result applies to both the symmetric-key and asymmetric-key models as the optimality was shown with respect to both (t, ϵ) -randomization (Definition 3) and (t, ϵ) -indistinguishability (Definition 4), the security definitions for the symmetric-key and asymmetric-key models respectively.

Quantum keys may however have other advantages over classical keys. For example, the scheme proposed in Section 4 is not optimal in the dimension of the encryption keys ρ_k . If the dimension of these keys can be reduced and quantum memory becomes the norm, they could be less resource consuming than classical keys. So encryption schemes using quantum keys cannot yet be dismissed.

Acknowledgements

The authors thank Renato Renner for helpful suggestions, in particular for the proof of Theorem 9.

This work is partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Young Scientists (B) No.17700007, 2005 and for Scientific Research (B) No. 18300002, 2006.

References

- [1] Patrick Hayden, Debbie Leung, Peter W. Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250:371–391, Sep 2004. [doi:10.1007/s00220-004-1087-6, arXiv:quant-ph/0307104v3].
- [2] Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *Proceedings of the 8th International Workshop on Randomization and Computation, RANDOM 2004*, volume 3122 of *Lecture Notes in Computer Science*, pages 249–260. Springer, 2004. [arXiv:quant-ph/0404075].
- [3] Paul Dickinson and Ashwin Nayak. Approximate randomization of quantum states with fewer bits of key. In *AIP Conference Proceedings*, volume 864, pages 18–36, 2006. [arXiv:quant-ph/0611033].
- [4] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67:042317, 2003. [doi:10.1103/PhysRevA.67.042317, arXiv:quant-ph/0003059].

- [5] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *FOCS '00: Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, page 547, Washington, DC, USA, 2000. IEEE Computer Society. [arXiv:quant-ph/0003101].
- [6] Ashwin Nayak and Pranab Sen. Invertible quantum operations and perfect encryption of quantum states. *Quantum Information and Computation*, 7:103–110, 2007. [arXiv:quant-ph/0605041].
- [7] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [8] Aram W. Harrow and Andreas Winter. How many copies are needed for state discrimination? eprint, 2006. [arXiv:quant-ph/0606131].
- [9] Masahito Hayashi, Akinori Kawachi, and Hirotada Kobayashi. Quantum measurements for hidden subgroup problems with optimal sample complexity. *Quantum Information and Computation*, 8:345–358, 2008. [arXiv:quant-ph/0604174].
- [10] 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, pages 268–284. Springer, 2005. [doi:10.1007/11426639_16].
- [11] Akinori Kawachi, Takeshi Koshihara, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. Full version of [10], 2006. [arXiv:quant-ph/0403069].
- [12] R. Alicki and M. Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37:L55–L57, February 2004. [doi:10.1088/0305-4470/37/5/L01].