Nat Comput (2014) 13:469–486
DOI 10.1007/s11047-014-9454-5

How to re-use a one-time pad safely and almost optimally even if $P = NP$

Ivan Damgård · Thomas Brochmann Pedersen · Louis Salvail

Published online: 21 August 2014

Abstract Assuming an insecure quantum channel, a quantum computer, and an authenticated classical channel, we propose an unconditionally secure scheme for encrypting classical messages under a shared key, where attempts to eavesdrop the ciphertext can be detected. If no eavesdropping is detected, we can securely re-use the entire key for encrypting new messages. If eavesdropping is detected, we must discard a number of key bits corresponding to the length of the message, but can re-use almost all of the rest. We show this is essentially optimal. Thus, provided the adversary does not interfere (too much) with the quantum channel, we can securely send an arbitrary number of message bits, independently of the length of the initial key. Moreover, the key-recycling mechanism only requires one-bit feedback. While ordinary quantum key distribution with a classical one time pad could be used instead to obtain a similar functionality, this would need more rounds of interaction and more communication.

Keywords key-recycling · Private-key encryption · Quantum cryptography · Unconditional security

1 Introduction

It is well known that only assuming a quantum channel and an authenticated classical channel, unconditionally secure secret keys can be generated between two parties using something like the BB84 quantum key distribution scheme (such a scheme will be denoted QKD in the following). If we want to use the key generated for encrypting classical messages, the simplest and safest approach is to use it as a one-time pad. This way, an m-bit key can be used to encrypt no more than m bits of message, since re-using the key would not be secure without extra assumptions. Some typical assumptions are: computational assumptions, requiring that $P \neq NP$, and the bounded storage assumption (Vadhan 2004; Dziembowski and Maurer 2004; Lu 2004).

However, if we allow the same communication model for message transmission as for key exchange—which seems quite natural—an obvious question is whether we might gain something by using the quantum channel to transmit ciphertexts. The reason why this might be a good idea is that the ciphertext is now a quantum state, and so by the laws of quantum mechanics, the adversary cannot avoid affecting the ciphertext when trying to eavesdrop. We may therefore hope being able to detect—at least with some probability—whether the adversary has interacted with the ciphertext. Clearly, if we know he has not, we can re-use the entire key. Even if he has, we may still be able to bound the amount of information he can obtain on the key, and hence we can still re-use part of the key. Note that the authenticated classical channel is needed in such a scheme,

The extended abstract version of this paper originally appears in Damgård et al. (2005) under the title: *A Quantum Cipher with Near Optimal Key-Recycling*.

I. Damgård
DAIMI, Aarhus University, Århus, Denmark
e-mail: ivan@cs.au.dk

T. B. Pedersen
TÜBİTAK UEKAE, P.O. Box 73, 41470 Gebze, Kocaeli, Turkey
e-mail: thomas.pedersen@tubitak.gov.tr

L. Salvail (✉)
Université de Montréal (DIRO), Montreal, QC, Canada
e-mail: salvail@iro.umontreal.ca

in order for the receiver to tell the sender whether the ciphertext arrived safely, and possibly also to exchange information needed to extract the part of the key that can be re-used. Such a system is called a *Quantum Key-Recycling Scheme* (QKRS).

A possible objection against QKRS is that since it requires interaction, we might as well use QKD (without the need for a quantum computer) to generate new key bits whenever needed. However, in the model where the authenticated classical channel is given as a black-box (i.e. not implemented via a shared key) QKD requires at least three messages: the quantum channel must be used, and the authenticated channel must be used in both directions, since otherwise the adversary could impersonate one of the honest parties. Further, in all QKD schemes known to the authors, each move requires a substantial amount of communication (if N qubits were transmitted then the two classical moves require $\Omega(N)$ classical bits each). Finally, N is typically larger than the length of the secret key produced. Hence, if we can build a QKRS scheme that is efficient, particularly in terms of how much key material can be re-used, this may be an advantage over straightforward use of QKD.

From a more theoretical point of view, our work can be seen as a study of the recycling capabilities of quantum ciphers in general. In particular, how many key bits can be recycled, and how much feedback information must go from receiver to sender in order to guarantee the security of the recycled key? How do these capabilities differ from those of classical (e.g. non-quantum) ciphers? In this paper we give precise answers to these questions.

The idea behind a QKRS originates from Bennett, Brassard, and Breidbart during the early days of quantum cryptography (Bennett et al. 1982). Although they did not provide any fully satisfying solution or security proof, their approach to the problem is very similar to our. Their idea was to encrypt a classical message together with some redundancy (i.e. an error-detection code) using a one-time pad with each bit encoded in two mutually unbiased bases (i.e. the BB84 bases) to detect eavesdropping. In our construction, we one-time encrypt the classical message together with a one-time classical authentication code. The classical encryption and the authentication code are then encoded using one basis (of the same dimension as the authenticated message) picked randomly among a set of 2^n mutually unbiased bases (Wootters and Fields 1989). Our work can then be seen as a way to use the idea of Bennett, Brassard, and Breidbart in a provably secure way. More recently, Leung studied recycling of quantum keys in a model where Alice and Bob are allowed three moves of interaction (Leung 2002). In this model however, quantum key distribution can be applied. Leung also suggested that classical keys can be recycled when no eavesdropping is detected. In Oppenheim and Horodecki (2003), a QKRS was proposed based on quantum authentication codes (Barnum et al. 2002). The key-recycling capabilities of their scheme can be described in terms of 2 parameters: the message length m and the security parameter ℓ. The scheme uses $2m + 2\ell$ bits of key, and is based on quantum authentication schemes that, as shown in Barnum et al. (2002), must always encrypt the message. The receiver first checks the authenticity of the received quantum state and then sends the result to the sender on the authenticated channel. Even when the receiver accepts, the adversary may still have obtained a small amount of information on the key. The receiver therefore also sends a universal hash function, and privacy amplification is used to extract a secure key of length $2m + \ell$ from the original key. If the receiver rejects then a secure key of length $m + \ell$ can be extracted. Hayden et al. (2011) present another QKRS based on the quantum authentication codes of (Barnum et al. 2002). Their scheme uses $2m + \ell$ (here ℓ is linear in m), and can recycle the first $2m$ bits unmodified when the authentication of the ciphertext is accepted. However, if the authentication fails the entire key is discarded. Contrary to our scheme, the QKRS in Hayden et al. (2011) can tolerate a noisy quantum channel.

In this paper, we propose a QKRS for encrypting classical messages. Our QKRS is based on a new technique where we append a k-bit classical authentication tag to the message, and then encrypt the $n = m + \ell$-bit plaintext using the W_n-quantum cipher introduced in Damgård et al. (2004). The authentication is based on universal hashing using an m-bit key. Encryption with the W_n-quantum cipher requires a quantum computer to encode a classical message in a state of one of a set of so called mutually unbiased bases. The cipher uses $2n = 2(m + \ell)$ bits of key, where $m + \ell$ bits are used as a one-time pad, and $m + \ell$ bits are used to select in which basis to send the result, out of a set of $2^{m+\ell}$ mutually unbiased bases. Thus, the entire key of the QKRS consists of $3m + 2\ell$ bits. The receiver decrypts and checks the authentication tag. If the tag is correct, we can show that the adversary has negligible information about the key, and the entire key can therefore be recycled. If the tag is incorrect, we can still identify $2m + \ell$ bits of the key, about which the adversary has no information, and they can therefore be re-used. Since this subset of bits is always the same, the receiver only needs to tell the sender whether he accepts or not.

Being able to recycle the entire key in case the receiver accepts is of course optimal. On the other hand, we can show that any QKRS must discard at least $m - 2$ bits of key in case the receiver rejects. Since m can be chosen to be much larger than ℓ, discarding $m + \ell$ bits, as we do, is almost optimal.

In comparison with earlier works, our technique completely eliminates the use of privacy amplification, and

hence reduces the communication on the authenticated channel to a single bit. Moreover, we can recycle the entire key when the receiver accepts the authentication tag. Hence, in scenarios where interference from the adversary is not too frequent, our keys can last much longer than with previous schemes, even though we initially start with a longer key.

Our results differ from those of Oppenheim and Horodecki (2003) and Hayden et al. (2011), since quantum authentication based QKRS do not guarantee the privacy of the authentication tag. Therefore, part of the key must be discarded even if the receiver accepts. Instead of quantum authentication, we use classical Wegman and Carter authentication codes (Carter and Wegman 1977) and a quantum encryption of classical messages (Damgård et al. 2004) applied to both the message and the tag. This construction allows to recycle the entire authentication key securely.

Our QKRS is sequentially self composable since the security is expressed in terms of distance between the distribution of the secret key, as seen from the eavesdropper's point of view, and the uniform distribution. The secret keys and plaintexts are private when, from the adversary's point of view, they look uniformly distributed.

We end this introduction with some remarks on the authenticated classical channel. Having such a channel given for free as a black-box may not be a realistic assumption, but it is well known that it can be implemented assuming the players initially have a (short) shared key.[1] In this model, the distinction between QKD and QKRS is not as clear as before, since we now assume an initial shared key for both primitives. Indeed, our QKRS can be seen as an alternative way to do QKD: we can form a message as the concatenation of new random key bits to be output and a short key for implementing the next usage of the authenticated channel. Having sent enough messages of this form successfully, we can generate a much larger number of secure key bits than we started from. Note that this is harder to achieve when using the earlier QKRS scheme since bits of the original key are lost even in successful transmissions.

2 Preliminaries

2.1 Notations

In the following, we call a function $f : \mathbb{N} \to \mathbb{R}^+$ *negligible in* n if $f(n) \leq 2^{-\alpha n}$ for some $\alpha > 0$ provided n is sufficiently large. Notice that this definition of negligible is more demanding than the usual requirement that $f(n) < 1/p(n)$ for any polynomial $p(\cdot)$. This only makes our security definition stronger.

For a set S, we denote its cardinality by $\#S$. In particular, for a function $r : \{0,1\}^n \to \{0,1\}^m$ and for $y \in \{0,1\}^m$, we denote by $\#r^{-1}(y)$ the number of elements $x \in \{0,1\}^n$ such that $r(x) = y$. When s is a bitstring, we write $|s|$ for its bit length.

2.2 Density operators and distance measures

For a discrete probability space (Ω, P), we write $P(\mathcal{E})$ for the probability of the event $\mathcal{E} \subset \Omega$, and we write P_X for the distribution of the random variable X according to (Ω, P). We use a similar notation for conditional probabilities and distributions. Henceforth, we will not refer to the probability space (Ω, P) but leave it implicitly defined by the joint probabilities of all considered events and random variables. We denote by $\mathcal{S}(\mathcal{H})$ the set of density operators on Hilbert space $\mathcal{H}$ (i.e. positive operators σ such that $\mathrm{tr}(\sigma) = 1$). In the following, $\mathcal{H}_n$ denotes the 2^n-dimensional Hilbert space over $\mathbb{C}$, $\mathbb{1}_n$ denotes the $2^n \times 2^n$ identity operator, and $\mathbb{I}_n = 2^{-n}\mathbb{1}_n$ denotes the completely mixed state. The trace-norm distance between two quantum states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ is defined as:

$$D(\rho, \sigma) = \frac{1}{2}\mathrm{tr}(|\rho - \sigma|),$$

where the right-hand side denotes half the sum over the absolute value of all eigenvalues of $\rho - \sigma$. The trace-norm distance is a metric over the set of density operators in $\mathcal{S}(\mathcal{H})$.

The behavior of a quantum state in a register Q is fully described by its density matrix ρ_{Q}. We often consider cases where a quantum state may depend on some classical random variable K, in that it is described by the density matrix ρ^k_{Q} if and only if $K = k$. For an observer having only access to the register Q but not to K, the behavior of the state is determined by the density matrix $\sum_k P_K(k)\rho^k_{\mathsf{Q}}$. The joint state, consisting of the classical register K and the quantum register Q is called a *cq-state*. A cq-state is described by the density operator $\sum_k P_K(k)|k\rangle\langle k| \otimes \rho^k_{\mathsf{Q}}$. To shorten the notation, we write

$$\rho_{K\mathsf{Q}} = \sum_k P_K(k)|k\rangle\langle k| \otimes \rho^k_{\mathsf{Q}} \quad \text{and} \quad \rho_{\mathsf{Q}} = \mathrm{tr}_K(\rho_{K\mathsf{Q}}) = \sum_k P_K(k)\rho^k_{\mathsf{Q}}\,.$$

More general, for any event $\mathcal{E}$, we write

$$\rho_{K\mathsf{Q}|\mathcal{E}} = \sum_k P_{K|\mathcal{E}}(k)|k\rangle\langle k| \otimes \rho^k_{\mathsf{Q}} \text{ and } \rho_{\mathsf{Q}|\mathcal{E}} = \mathrm{tr}_K(\rho_{K\mathsf{Q}|\mathcal{E}}) = \sum_k P_{K|\mathcal{E}}(k)\rho^k_{\mathsf{Q}}\,. \quad (1)$$

[1] Even in this case, QKD does something that is impossible classically, namely it generates a shared key that is longer than the initial one.

We also write $\rho_K = \sum_k P_K(k)|k\rangle\langle k|$ for the quantum representation of the classical random variable K (and similarly for $\rho_{K|\mathcal{E}}$).

This notation extends naturally to quantum states that depend on several classical random variables (i.e. to ccq-states, etc.), defining the density matrices $\rho_{KX\mathsf{Q}}$, $\rho_{KX\mathsf{Q}|\mathcal{E}}$, $\rho_{X\mathsf{Q}|K=k}$, etc. Note that writing $\rho_{K\mathsf{Q}} = \mathrm{tr}_X(\rho_{XK\mathsf{Q}})$ and $\rho_{\mathsf{Q}} = \mathrm{tr}_{KX}(\rho_{XK\mathsf{Q}})$ is consistent with the above notation. We also write $\rho_{K\mathsf{Q}|\mathcal{E}} = \mathrm{tr}_X(\rho_{XK\mathsf{Q}|\mathcal{E}})$ and $\rho_{\mathsf{Q}|\mathcal{E}} = \mathrm{tr}_{XK}(\rho_{XK\mathsf{Q}|\mathcal{E}})$, where one has to be aware that in contrast to (1), here the state of register Q may depend on the event $\mathcal{E}$ when given k (namely via X), so that $\rho_{\mathsf{Q}|\mathcal{E}} = \sum_k P_{K|\mathcal{E}}(k)\rho^k_{\mathsf{Q}|\mathcal{E}}$.

In the following we will abuse the previous notation by conditioning on measurement outcomes as well. This simplifies quite a lot the notation in our proofs. Let $\rho_{K\mathsf{Q}}$ be a cq-state. Let $\{\Pi_{\mathrm{ok}}, \Pi_{\mathrm{no}}\}$ be a two-outcome measurement acting on register Q where $\Pi_{\mathrm{no}} = \mathbb{1}_{\mathsf{Q}} - \Pi_{\mathrm{ok}}$. Let $\mathcal{A}_{\mathrm{ok}}$ and $\mathcal{A}_{\mathrm{no}}$ be the events corresponding to the outcome Π_{ok} and Π_{no} respectively when ρ_{Q} is measured. We write

$$\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}}} := \frac{(\mathbb{1}_K \otimes \Pi_{\mathrm{ok}})\rho_{K\mathsf{Q}}(\mathbb{1}_K \otimes \Pi_{\mathrm{ok}})}{\mathrm{tr}((\mathbb{1}_K \otimes \Pi_{\mathrm{ok}})\rho_{K\mathsf{Q}})},$$

to denote the resulting state when the observable Π_{ok} is obtained. Similarly, we write $\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{no}}}$ for outcome Π_{no}. As before, $\rho_{\mathsf{Q}|\mathcal{A}_{\mathrm{ok}}} = \mathrm{tr}_K(\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}}})$ and $\rho_{K|\mathcal{A}_{ok}} = \mathrm{tr}_{\mathsf{Q}}(\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}}})$. For an event $\mathcal{E}$ deterministic over the classical part of the cq-state $\rho_{K\mathsf{Q}}$ (i.e. $\Pr(\mathcal{E}|K=k) = 0$ or $\Pr(\mathcal{E}|K=k) = 1$ for every k), we write $\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}},\rho_{\mathsf{Q}|\mathcal{E}}=\mathrm{tr}_{XK}(\rho_{XK\mathsf{Q}|\mathcal{E}})}$ (resp. $\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{no}},\rho_{\mathsf{Q}|\mathcal{E}}=\mathrm{tr}_{XK}(\rho_{XK\mathsf{Q}|\mathcal{E}})}$) for the conditioning according to $\rho_{\mathsf{Q}|\mathcal{E}} = \mathrm{tr}_{XK}(\rho_{XK\mathsf{Q}|\mathcal{E}})$ of the cq-state $\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}}}$ (resp. $\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{no}}}$). Since in this case the measurement takes place on register Q, it is easy to verify that the conditioning on $\rho_{\mathsf{Q}|\mathcal{E}} = \mathrm{tr}_{XK}(\rho_{XK\mathsf{Q}|\mathcal{E}})$ commutes with the measurement:

$$\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}},\mathcal{E}} = \frac{(\mathbb{1}_K \otimes \Pi_{\mathrm{ok}})\rho_{K\mathsf{Q}|\mathcal{E}}(\mathbb{1}_K \otimes \Pi_{\mathrm{ok}})}{\mathrm{tr}((\mathbb{1}_K \otimes \Pi_{\mathrm{ok}})\rho_{K\mathsf{Q}|\mathcal{E}})},$$

and similarly for $\mathcal{A}_{\mathrm{no}}$. In other words, and as for normal conditioning, the order of the events (as far as there is only one measurement involved) is irrelevant, $\rho_{K\mathsf{Q}|\mathcal{A}_{\mathrm{ok}},\mathcal{E}} = \rho_{K\mathsf{Q}|\mathcal{E},\mathcal{A}_{\mathrm{ok}}}$. The same notation can be used the natural way for ccq-states, cccq-states, etc...

Obviously, $\rho_{K\mathsf{Q}} = \rho_K \otimes \rho_{\mathsf{Q}}$ if and only if the quantum part is independent of K (in that $\rho^k_{\mathsf{Q}} = \rho_{\mathsf{Q}}$ for any k), where the latter in particular implies that no information on K can be learned by observing only ρ_{Q}. Furthermore, if $\rho_{K\mathsf{Q}}$ and $\rho_K \otimes \rho_{\mathsf{Q}}$ are ϵ-close in terms of their trace distance $D(\rho, \sigma)$, then the real system $\rho_{K\mathsf{Q}}$ "behaves" as the ideal system $\rho_K \otimes \rho_{\mathsf{Q}}$ except with probability ϵ in that for any evolution of the system no observer can distinguish the real from the ideal one with advantage greater than ϵ (Renner and König 2005). Let K be a classical random variable and let $\rho_{K\mathsf{E}}$ be a cq-state. The *distance to uniform of K given ρ_{E}* is defined by

$$d(K|\rho_{\mathsf{E}}) = D(\rho_{K\mathsf{E}}, \mathbb{I}_K \otimes \rho_{\mathsf{E}}), \tag{2}$$

where $\mathbb{I}_K$ is the completely mixed state for the classical register K (i.e. uniform distribution for the classical register K). Suppose an eavesdropper holds register E in $\rho_{K\mathsf{E}}$ with $K \in \{0,1\}^n$. If $d(K|\rho_{\mathsf{E}}) \leq \epsilon(n)$ then we say that K is $\epsilon(n)$-*uniform*. Whenever $\epsilon(n)$ is a negligible function, we say that K is *statistically secure*.

2.3 Quantum Ciphers

A quantum encryption scheme for classical messages is the central part of any QKRS. Such schemes where introduced independently in Ambainis et al. (2000); Boykin and Roychowdhury (2003), and further studied Damgård et al. (2004)), where their performances were analyzed against known-plaintext attacks. We adopt a similar definition here except that we allow for the encryption to provide only statistical instead of perfect privacy. As in Ambainis et al. (2000), Boykin and Roychowdhury (2003), Damgård et al. (2004), we model encryption under key $k \in \{0,1\}^n$ by an appropriate unitary operator E_k acting upon an m-bit message and a possible ancilla of any size initially in state $|0\rangle$. Decryption is simply done by applying the inverse unitary.

For convenience, we write

$$\begin{aligned}\rho_{KX\mathsf{Q}} =& 2^{-n-m} \sum_{k\in\{0,1\}^n} \sum_{x\in\{0,1\}^m} |k\rangle\langle k| \otimes |x\rangle\langle x| \\ & \otimes E_k|x\rangle\langle x| \otimes |0\rangle\langle 0|E_k^\dagger,\end{aligned} \tag{3}$$

as the mixed state corresponding to the encryption of a random plaintext under a random key. The state

$$\rho_{\mathsf{Q}|X=x} = \mathrm{tr}_{KX}(\rho_{KX\mathsf{Q}|X=x}) = 2^{-n} \sum_{k\in\{0,1\}^n} E_k|x\rangle\langle x| \otimes |0\rangle\langle 0|E_k^\dagger$$

corresponds to the equal mixture of plaintext $x \in \{0,1\}^m$ encrypted under all possible keys with uniform probability. A quantum cipher is private if, given a cipherstate, almost no information can be extracted about the plaintext.

Definition 2.1 Let $\epsilon(n)$ be a non-negative function. An $\epsilon(n)$-*private* (n,m)-*quantum cipher* is a set consisting of 2^n unitary encryption operators $\{E_k\}_{k\in\{0,1\}^n}$, acting on a set of m-bit plaintexts and an arbitrary ancilla initially in state $|0\rangle$ such that,

$$(\forall x, x' \in \{0,1\}^m)[D(\rho_{\mathsf{Q}|X=x}, \rho_{\mathsf{Q}|X=x'}) < \epsilon(n)]\,.$$

If $\epsilon(n)$ is a negligible function of n we say that the scheme is *statistically private*.

The total mixture of ciphertexts associated with an ϵ-private (n,m)-quantum cipher with encryption operators $\{E_k\}_{k\in\{0,1\}^n}$ is defined as,

$$\rho_{\mathsf{Q}} = \mathrm{tr}_{KX}(\rho_{KX\mathsf{Q}}) = 2^{-n-m} \sum_{k\in\{0,1\}^n} \sum_{x\in\{0,1\}^m} E_k|x\rangle\langle x| \otimes |0\rangle\langle 0|E_k^\dagger\,. \tag{4}$$

The next technical lemma states that the total mixture of any ϵ-private quantum cipher is ϵ-close to any plaintext encryption under a random and private key.

Lemma 2.1 *Any ϵ-private (n,m)-quantum cipher satisfies that $D(\rho_{\mathsf{Q}}, \rho_{\mathsf{Q}|X=x}) < \epsilon$, for any $x \in \{0,1\}^m$.*

Proof Simply observe using (4) that,

$$\begin{aligned} D(\rho_{\mathsf{Q}}, \rho_{\mathsf{Q}|X=x}) &= D\left(2^{-m} \sum_{x'\in\{0,1\}^m} \rho_{\mathsf{Q}|X=x'}, \rho_{\mathsf{Q}|X=x}\right) \\ &\leq 2^{-m} \sum_{x'\in\{0,1\}^m} D(\rho_{\mathsf{Q}|X=x'}, \rho_{\mathsf{Q}|X=x}) \\ &< \epsilon\,, \end{aligned}$$

from the convexity of $D(\cdot,\cdot)$ and the ϵ-privacy of the quantum cipher. □

2.4 Mutually unbiased bases

A set $\mathcal{B}_n = \{B_1, \ldots, B_{2^t}\}$ of 2^t orthonormal bases in a Hilbert space of dimension 2^n is said to be *mutually unbiased* (we abbreviate mutually unbiased bases set as MUBS) if for all $|u\rangle \in B_i$ and $|v\rangle \in B_j$, for $i \neq j$, we have $|\langle u|v\rangle| = 2^{-n/2}$. Wootters and Fields (1989) have shown that there are MUBSs of up to $2^n + 1$ bases in a Hilbert space of dimension 2^n, and such sets are *maximum*. They also give a construction for a maximal MUBS in Hilbert spaces of prime-power dimensions. For $\mathcal{B}_n = \{B_b\}_{b\in\{0,1\}^t}$ a MUBS, $w \in \{0,1\}^n$, and $b \in \{0,1\}^t$, we denote by $|v_w^{(b)}\rangle$ the w-th state in basis $B_b \in \mathcal{B}_n$.

Lawrence et al. (2002) introduced an alternative construction for maximal MUBSs based on algebra in the Pauli group. Their construction plays an important role in the security analysis of our QKRS. The method for constructing a maximal MUBS in $\mathcal{H}_n$ relies on a special partitioning of all Pauli operators in $\mathcal{H}_n$. These operators form a vector space of dimension 4^n. Let $\Sigma = \{\sigma_x, \sigma_y, \sigma_z, \sigma_{\mathbb{1}}\}$ (where $\sigma_{\mathbb{1}} = \mathbb{1}_1$) be the set of Pauli operators in $\mathcal{H}_1$. This set forms a basis for all one-qubit operators. A basis for operators on n qubits is constructed as follows for $i \in \{0, \ldots, 4^n - 1\}$:

$$O_i = \sigma^1_{\mu(1,i)}\sigma^2_{\mu(2,i)}\cdots\sigma^n_{\mu(n,i)} = \prod_{k=1}^n \sigma^k_{\mu(k,i)}\,, \tag{5}$$

such that $\sigma^k_{\mu(k,i)}$ is an operator in Σ acting only on the k-th qubit. We use the convention $O_0 = \mathbb{1}_n$. The action of O_i on the k-th qubit is $\sigma_{\mu(k,i)}$ where $\mu(k,i) \in \{x, y, z, \mathbb{1}\}$. The basis described in (5) is orthogonal, $\mathrm{tr}(O_iO_j) = 2^n\delta_{i,j}$ where $i = j$ means that $\mu(k,i) = \mu(k,j)$ for any qubit k. Every Pauli operator O_i is such that $O_i^2 = \mathbb{1}_n$. Apart from the identity $\mathbb{1}_n$, all O_i's are traceless and have eigenvalues ± 1.

In Lawrence et al. (2002), it is first shown how to partition the set of $4^n - 1$ non-trivial Pauli operators $\{O_i\}_{i=1}^{4^n-1}$ into $2^n + 1$ subsets, each containing $2^n - 1$ commuting members. Second, each such partitioning is shown to define a maximal MUBS. Let us denote by $P^b_\beta = |v^{(b)}_\beta\rangle\langle v^{(b)}_\beta|$ the projector onto the β-th vector in basis B_b. Saying that $\mathcal{B}_n = \{B_i\}_i$ is a MUBS means that $\mathrm{tr}(P^a_\alpha P^b_\beta) = 2^{-n}$ when $a \neq b$ and $\mathrm{tr}(P^b_\beta P^b_{\beta'}) = \delta_{\beta,\beta'}$. Let $(\varepsilon_{b,\beta})_{b,\beta}$ be a $2^n \times 2^n$ matrix consisting of orthogonal rows, one of which is all $+1$, and the remaining ones all contain as many $+1$ as -1. The b-th partition of the non-trivial Pauli operators contains $\{O^b_\beta\}_{\beta=1}^{2^n-1}$ such that

$$O^b_\beta = \sum_{\alpha=1}^{2^n} \varepsilon_{\beta,\alpha} P^b_\alpha\,. \tag{6}$$

In the following, $(\varepsilon_{\beta,\alpha})_{\beta,\alpha}$ will always denote the operator $2^{n/2}H^{\otimes n}$ where $H^{\otimes n}$ is the n-qubit Hadamard transform, $\varepsilon_{\beta,\alpha} = (-1)^{\beta\cdot\alpha}$ where $\beta\cdot\alpha$ denotes the inner product between the binary representions of β and α.

The number of partitions $\{O^b_\beta\}_\beta$ defined by (6) is $2^n + 1$ when constructed from a maximal MUBS. Each partition contains $2^n - 1$ operators after discarding the identity (they all contain the identity). Each of these operators is traceless and has ± 1 eigenvalues as for the Pauli operators. It is easy to verify that for $a \neq b$,

$$\mathrm{tr}(O^a_\alpha O^b_\beta) = \sum_{\mu,\nu} \varepsilon_{\alpha,\mu}\varepsilon_{\beta,\nu}\mathrm{tr}(P^a_\mu P^b_\nu) = 0\,. \tag{7}$$

Moreover,

$$\mathrm{tr}(O^b_\beta O^b_{\beta'}) = \sum_{\mu,\nu} \varepsilon_{\beta,\mu}\varepsilon_{\beta',\nu}\mathrm{tr}(P^b_\mu P^b_\nu) = \sum_\mu \varepsilon_{\beta,\mu}\varepsilon_{\beta',\mu} = 2^n\delta_{\beta,\beta'}\,. \tag{8}$$

It follows from (7) and (8) that all operators in (6) are unitarily equivalent to Pauli operators. This essentially shows that partitioning the Pauli operators the way we want is always possible.

It remains to argue that any such partitioning defines a maximal MUBS. Notice that partition $\{O^b_1, \ldots, O^b_{2^n-1}\}$ (i.e. without the identity O^b_0) defines a unique basis $\{P^b_\beta\}_\beta$ where

$$P_\beta^b = 2^{-n} \sum_\mu \varepsilon_{\mu,\beta} O_\mu^b \,. \tag{9}$$

It is not difficult to verify that $\mathrm{tr}(P_\beta^b P_{\beta'}^b) = \delta_{\beta,\beta'}$ and for $a \neq b$, $\mathrm{tr}(P_\beta^b P_\alpha^a) = 2^{-n}$ thus leading to a maximal MUBS.

In other words, there is a one-to-one correspondence between maximal MUBSs and the partitionings $\{\{O_\beta^b\}_\beta\}_b$ of the $4^n - 1$ Pauli operators (except the identity), acting on n qubits, into $2^n + 1$ partitions $\{O_\beta^b\}_\beta$ of $2^n - 1$ commuting members. Each partition is a subgroup of the n-qubit Pauli group and is generated by n of these operators. Any Pauli operator anti-commutes with exactly half the operators in all partitions and commutes with all operators in the partition in which it belongs. See Lawrence et al. (2002) for more details.

2.5 The W_n-Cipher

In Damgård et al. (2004), quantum ciphers based on MUBSs were introduced and studied with respect to their secret key uncertainty against known-plaintext attacks. Our QKRS, presented in Sect. 5.1, uses one of these ciphers, the W_n-cipher, as its main building block. The W_n-cipher is a $(2n, n)$-quantum cipher, that is, it encrypts n-bit classical messages with the help of a $2n$-bit secret key. The W_n-cipher enjoys perfect privacy when the secret key is perfectly private. It is easy to verify that the cipher is ϵ-private if the secret key is only ϵ-uniform (Renner and König 2005).

Let $\mathcal{B}_n = \{B_b\}_{b\in\{0,1\}^n}$ be a MUBS of cardinality 2^n for $\mathcal{H}_n$. Remember that $|v_w^{(b)}\rangle$ denotes the w-th basis state in basis $B_b \in \mathcal{B}$. The secret key k for the W_n-cipher is conveniently written as $k = (z, b)$ where $z, b \in_R \{0,1\}^n$. Encryption with secret key $k = (z, b)$ of message $x \in \{0,1\}^n$ consists in preparing the following state:

$$E_k|x\rangle = E_{(z,b)}|x\rangle = |v_{x\oplus z}^{(b)}\rangle \in B_b \,.$$

In other words, the encryption process first applies the one-time pad to message x with key z and then maps the resulting state to basis B_b. Encryption and decryption can be performed efficiently on a quantum computer (Wootters and Fields 1989; Wootters and Sussman 2007; Mandayam et al. 2010; Damgård et al. 2004).

3 Key-recycling schemes

A QKRS is an encryption scheme with authentication. In addition, there are two key-recycling mechanisms, $\mathsf{R}_{\mathrm{ok}}^{n,s}$ and $\mathsf{R}_{\mathrm{no}}^{n,t}$, allowing one to recycle part of the secret key shared between Alice and Bob in case where the authentication succeeds and fails respectively. We model the recycling mechanism by privacy amplification. That is, $\mathsf{R}_{\mathrm{ok}}^{n,s}$ and $\mathsf{R}_{\mathrm{no}}^{n,t}$ are classes of hashing functions mapping the current key $k \in \{0,1\}^n$ into a recycled key $\tilde{k}$ of length s and t respectively. In order to apply privacy amplification, an *authentic classical feedback channel* is necessary for announcing Bob's random recycling function $r \in_R \mathsf{R}_{\mathrm{ok}}^{n,s}$ or $r \in_R \mathsf{R}_{\mathrm{no}}^{n,t}$ depending on the outcome of authentication. Alice and Bob then compute $\tilde{k} = r(k)$ as their recycled secret key. We do not allow further interaction between Alice and Bob since otherwise quantum key distribution could take place between them allowing not only to recycle their secret key but even to increase its length. Key-recycling should be inherently non-interactive from Bob to Alice since the authentication outcome should anyway be made available to Alice. For simplicity, we assume that the classical feedback channel between Bob and Alice is authenticated. In general, a small secret key could be used for providing classical message-authentication on the feedback channel if necessary.

Definition 3.1 An (n, m, s, t)-QKRS is defined by a pair $(\mathfrak{C}^{n,m}, (\mathsf{R}_{\mathrm{ok}}^{n,s}, \mathsf{R}_{\mathrm{no}}^{n,t}))$ where

- $\mathfrak{C}^{n,m}$ is an (n, m)-quantum cipher, and
- $(\mathsf{R}_{\mathrm{ok}}^{n,s}, \mathsf{R}_{\mathrm{no}}^{n,t})$ is a key-recycling mechanism.

For a QKRS to be secure, we require that even knowing the plaintext, the function r, and the authentication outcome, the adversary's view about the recycled key is at negligible distance to uniform. This should hold except for a negligible number of functions in $\mathsf{R}_{\mathrm{ok}}^{n,s}$ and $\mathsf{R}_{\mathrm{no}}^{n,t}$. Security against known plaintext attacks is an important property of good key-recycling mechanisms. Otherwise, extra conditions on the *a posteriori* probability distribution over plaintexts have to be enforced. In particular a recycled key could be compromised if a previous plaintext gets revealed to the adversary.

The adversary's view typically changes depending on whether the authentication succeeds or fails. Let $\mathcal{A}_{\mathrm{ok}}$ (resp. $\mathcal{A}_{\mathrm{no}}$) be the event consisting in a successful (resp. unsuccessful) authentication. Conditioned on $\mathcal{A}_{\mathrm{ok}}$, the adversary should have access only to very limited amount of information about the secret key. The better the authentication scheme is, the more key material the recycling mechanism can handle. When $\mathcal{A}_{\mathrm{no}}$ occurs, however, the adversary may hold the entire cipherstate. Let $\rho_{K\mathsf{X}\mathsf{Q}}$ be the ccq-state defined as in (3) for some (n, m, s, t)-QKRS. An attacker, seeing ρ_{Q} may interact with it after adding an extra quantum register E initially in state $|0\rangle$. Let U be the unitary transform implementing this interaction:

$$\tilde{\rho}_{\mathsf{E}\mathsf{Q}} = U|0\rangle\langle 0| \otimes \rho_{\mathsf{Q}} U^\dagger \,.$$

The attacker then keeps register E and forwards Q to the legitimate receiver. The legitimate receiver then verifies the authentication of the cipherstate Q resulting in event $\mathcal{A}_{\text{ok}}$ or $\mathcal{A}_{\text{no}}$ according to the outcome of the verification process.

The key-recycling mechanism then picks a random r in either $\mathsf{R}_{\text{ok}}^{n,s}$ or $\mathsf{R}_{\text{no}}^{n,t}$ depending upon the outcome $\mathcal{A}_{\text{ok}}$ or $\mathcal{A}_{\text{no}}$, respectively. The recycled key $\hat{K} = r(K)$ is then produced. The resulting mixed state is of the form $\tilde{\rho}_{\hat{K}RKX\mathsf{EQ}}$ where $\hat{K}$ stores the recycled secret key and R stores the hashing function used to generate it. In a known plaintext attack, the adversary has access to $\tilde{\rho}_{\mathsf{E}|X=x}$ (plus the outcome of the authentication process) and wants to get as much information as possible on the recycled key $\hat{K}$.

We define the following mixed state for the view of the adversary depending upon the output of the authentication process, the known plaintext $X = x$ encrypted in the cipherstate, and the function $R = r$ used for key-recycling (i.e. $r \in_R \mathsf{R}_{\text{ok}}^{n,s}$ if $\mathcal{A}_{\text{ok}}$ and $r \in_R \mathsf{R}_{\text{no}}^{n,t}$ if $\mathcal{A}_{\text{no}}$):

$$\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x,r) := \tilde{\rho}_{R\mathsf{E}|\mathcal{A}_{\text{ok}},X=x,R=r} = \text{tr}_{\hat{K}KX\mathsf{Q}}(\tilde{\rho}_{\hat{K}RKX\mathsf{EQ}|\mathcal{A}_{\text{ok}},X=x,R=r}),$$
$$\tilde{\rho}_{\mathsf{E}}^{\text{no}}(x,r) := \tilde{\rho}_{R\mathsf{E}|\mathcal{A}_{\text{no}},X=x,R=r} = \text{tr}_{\hat{K}KX\mathsf{Q}}(\tilde{\rho}_{\hat{K}RKX\mathsf{EQ}|\mathcal{A}_{\text{no}},X=x,R=r}).$$

A secure key-recycling mechanism will make sure that both

$$\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x,R) := \frac{1}{\#\mathsf{R}_{\text{ok}}^{n,s}} \sum_{r \in \mathsf{R}_{\text{ok}}^{n,s}} \tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x,r) \text{ and}$$
$$\tilde{\rho}_{\mathsf{E}}^{\text{no}}(x,R) := \frac{1}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{r \in \mathsf{R}_{\text{no}}^{n,t}} \tilde{\rho}_{\mathsf{E}}^{\text{no}}(x,r) \quad (10)$$

are essentially independent of $\hat{K}$. When the authentication succeeds (i.e. conditioned on $\mathcal{A}_{\text{ok}}$), we require that the recycled key $\hat{K}$ is independent of the adversary's view as long as the probability that the cipherstate forwarded to the receiver has a sufficiently high probability to result in $\mathcal{A}_{\text{ok}}$. Otherwise, the attack could be very unlikely to result in $\mathcal{A}_{\text{ok}}$ but, conditioned on $\mathcal{A}_{\text{ok}}$, the information on the recycled key could be non-negligible. An attack having negligible probability to result in $\mathcal{A}_{\text{ok}}$ is not considered a threat to a key-recycling scheme even though, conditioned on $\mathcal{A}_{\text{ok}}$, the recycled key is not safe.

Next, we define the security of the key-recycling mechanism whenever the secret key is initially uniform. That is, no eavesdropper has any *a priori* information about the secret key used for encrypting the next transmission. We shall discuss the composability of our security definition below in Sect. 3.1. It corresponds to using a secret key that may be only at negligible distance to uniform before the next transmission.

Definition 3.2 A key-recycling mechanism, $(\mathsf{R}_{\text{ok}}^{n,s}, \mathsf{R}_{\text{no}}^{n,t})$, is $(p_{\text{ok}}, \delta_{\text{ok}}, \delta_{\text{no}})$ *-indistinguishable* if, for all $x \in \{0,1\}^m$,

1. Any attack with a probability of successful authentication at least as large as p_{ok} is such that $d(\hat{K}|\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x,R)) \leq \delta_{\text{ok}}$, and
2. $d(\hat{K}|\tilde{\rho}_{\mathsf{E}}^{\text{no}}(x,R)) \leq \delta_{\text{no}}$,

whenever the secret key is initially uniform. For $p_{\text{ok}}, \delta_{\text{ok}}$, and δ_{no} all negligible functions of n, we say that the key-recycling mechanism is *statistically secure*. The key-recycling class of functions $\mathsf{R}_{\text{ok}}^{n,s}$ is said to be δ*-uniform* if condition 1 holds relative to δ for any $p_{\text{ok}} \geq \delta$. The key-recycling class of functions $\mathsf{R}_{\text{no}}^{n,t}$ is said to be δ *-uniform* if condition 2 holds relative to δ.

Notice that an equivalent definition could have been made along the same lines as in Barnum et al. (2002) where the security of quantum authentication schemes is defined. The two conditions of Definition 3.2 would then be expressed in our scenario as the requirement that, for any attack,

$$p_{\text{ok}} d(\hat{K}|\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x,R)) + (1 - p_{\text{ok}}) d(\hat{K}|\tilde{\rho}_{\mathsf{E}}^{\text{no}}(x,R)) \leq \delta',$$

for some negligible δ'. In the following, we rather use Definition 3.2 since it corresponds more directly to the way we prove the security of our scheme in Sect. 5, and the key-recycling bound of Sect. 4 (Theorem 4.1).

Finally, a QKRS is secure if it is a private encryption scheme together with a statistically secure key-recycling mechanism. In general,

Definition 3.3 An (n,m,s,t)-QKRS defined by $(\mathfrak{C}^{\mathfrak{n},\mathfrak{m}}, (\mathsf{R}_{\text{ok}}^{n,s}, \mathsf{R}_{\text{no}}^{n,t}))$ is said to be $(\epsilon, p_{\text{ok}}, \delta_{\text{ok}}, \delta_{\text{no}})$ *-secure* if

1. $\mathfrak{C}^{n,m}$ is ϵ-private,
2. $(\mathsf{R}_{\text{ok}}^{n,s}, \mathsf{R}_{\text{no}}^{n,t})$ is a $(p_{\text{ok}}, \delta_{\text{ok}}, \delta_{\text{no}})$-uniform key-recycling mechanism.

If the scheme is such that $\epsilon, p_{\text{ok}}, \delta_{\text{ok}}$, and δ_{no} are all negligible functions of n then we say that the scheme is *statistically secure*.

The efficiency of a QKRS is characterized by n, s and t. When authentication succeeds, $n - s$ bits of secret key must be thrown away while, when authentication fails, $n - t$ bits have to be discarded. Clearly, any purely classical key-recycling scheme must have $s, t \leq n - m$. This does not have to hold for quantum schemes. However, we show in Sect. 4 that quantum schemes suffer from the same limitations as classical ciphers when authentication fails.

3.1 On sequential self composability

Let us now discuss the security of key-recycling when composed sequentially with itself many times. Using a security

definition that characterizes the security of the recycled keys in terms of trace-norm distance to uniform allows for sequential composability as it was observed in Renner and König (2005). Here is how the argument goes in our case.

Assume any (n, m, s, t)-QKRS equipped with δ-uniform key-recycling mechanisms. Given one behavior of an eavesdropper, the authentication will be successful with some probability p_{ok}. Let $\tilde{\rho}_{K\mathsf{EQ}|X=x}$ be the joint state before key-recycling but after the transmission of register Q whenever the secret key is initially ϵ-uniform. Let $\tilde{\rho}^*_{K\mathsf{EQ}|X=x}$ be a joint state such that $D(\tilde{\rho}_{K\mathsf{EQ}|X=x}, \tilde{\rho}^*_{K\mathsf{EQ}|X=x}) \leq \epsilon$ and where the secret key is initially uniform. The recycled key can be seen as a quantum operation that, upon the outcome of authentication, produces a new key:

$$\begin{aligned}\tilde{\rho}_{K\mathsf{EQ}|X=x} \mapsto & p_{\text{ok}}\ \tilde{\rho}_{\hat{K}R\mathsf{EQ}|\mathcal{A}_{\text{ok}},X=x} + (1-p_{\text{ok}}) \\ & \tilde{\rho}_{\hat{K}R\mathsf{EQ}|\mathcal{A}_{\text{no}},X=x} =: \tilde{\rho}_{\hat{K}R\mathsf{EQ}|X=x}\,.\end{aligned} \tag{11}$$

On the other hand, if the state shared between Alice, Bob, and the eavesdropper was $\tilde{\rho}^*_{K\mathsf{EQ}|X=x}$ then the quantum operation corresponding to the key-recycling process would be[2]:

$$\begin{aligned}\tilde{\rho}^*_{K\mathsf{EQ}|X=x} \mapsto & p^*_{\text{ok}}\ \tilde{\rho}^*_{\hat{K}R\mathsf{EQ}|\mathcal{A}_{\text{ok}},X=x} + (1-p^*_{\text{ok}}) \\ & \tilde{\rho}^*_{\hat{K}R\mathsf{EQ}|\mathcal{A}_{\text{no}},X=x} =: \tilde{\rho}^*_{\hat{K}R\mathsf{EQ}|X=x}\,.\end{aligned} \tag{12}$$

Since a quantum operation cannot increase the trace-norm distance, we have that $D(\tilde{\rho}_{\hat{K}R\mathsf{E}|X=x}, \tilde{\rho}^*_{\hat{K}R\mathsf{E}|X=x}) \leq \epsilon$ (i.e. notice that we traced out register Q since it is irrelevant for this discussion). On the other hand, one can imagine an ideal functionality for key-recycling that, upon input p^*_{ok} by the adversary, produces a perfectly secure key $\hat{K}$ for Alice and Bob of length s with probability p^*_{ok}, and length t with probability $1-p^*_{\text{ok}}$ together with random variable R (i.e. chosen uniformly at random in either $\mathsf{R}^{n,s}_{\text{ok}}$ when $\mathcal{A}_{\text{ok}}$ or in $\mathsf{R}^{n,t}_{\text{no}}$ otherwise) to the eavesdropper. Let $\rho^{\text{id}}_{\hat{K}R}$ be the result of this ideal process and let $\rho^{\text{id}}_{\hat{K}R\mathsf{E}} = \rho^{\text{id}}_{\hat{K}R} \otimes \tilde{\rho}^*_{\mathsf{E}|X=x}$ be the ideal state including the state of the adversary. Since the QKRS-scheme has δ-uniform key-recycling mechanisms, it follows that $D(\tilde{\rho}^*_{\hat{K}R\mathsf{E}|X=x}, \rho^{\text{id}}_{\hat{K}R\mathsf{E}}) \leq \delta$. Notice that the ideal functionality $\rho^{\text{id}}_{\hat{K}R\mathsf{E}}$ and the state $\tilde{\rho}^*_{\hat{K}R\mathsf{E}|X=x}$ may differ greatly conditioned on $\mathcal{A}_{\text{ok}}$ whenever $p^{b,u}_{\text{ok}} < \delta$ since in this case, the key-recycling mechanism is not guarantee to produce a safe key. This is not a problem given that the probability of this event is upper bounded by a negligible δ. By the triangle inequality, we then have:

$$D(\tilde{\rho}_{\hat{K}R\mathsf{E}|X=x}, \rho^{\text{id}}_{\hat{K}R\mathsf{E}}) \leq \epsilon + \delta.$$

That is, the loss in security when using an initial ϵ-uniform secret key, rather than a perfect one, is only ϵ. The resulting recycled-key behaves exactly like the ideal process except with probability $\epsilon + \delta$. If ϵ is negligible then the same argument can be applied polynomially many times. It therefore suffices to prove security of a key-recycling scheme assuming the initial secret key is perfectly safe in order to conclude its sequential self composability (i.e. see Renner and König 2005; Ben-Or et al. 2005 for more details).

4 Upper bound on key-recycling

In this section, we show that any statistically secure QKRS must discard as many key-bits as the length of the plaintext (minus two bits) when the authentication fails. In other words, when authentication fails no QKRS does significantly better than the classical one-time-pad (up to a possible two bits saving). When authentication fails, the adversary may have kept the entire ciphertext and may know the plaintext $x \in \{0,1\}^m$ (i.e. the adversary mounts a known-plaintext attack). We show that in this case, the recycled key size must be shorter than the original key by at least $m-2$ bits.

Assume an arbitrary (n, m, s, t)-QKRS key-recycling scheme. To be statistically secure, condition 2 in Definition 3.2 requires that for any $x \in \{0,1\}^m$,

$$D(\tilde{\rho}^{\text{no}}_{\hat{K}\mathsf{E}}(x,R), \mathbb{I}_t \otimes \tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,R)) \leq \delta(n)\,, \tag{13}$$

for some negligible $\delta(n)$. Assume now that the adversary intercepts the whole cipherstate and forwards all qubits of register Q in state $|0\rangle$. We then have that for any $r \in \mathsf{R}^{n,t}_{\text{no}}$,

$$\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r) = \frac{1}{\#r^{-1}(\hat{k})} \sum_{k \in r^{-1}(\hat{k})} E_k|x\rangle\langle x| \otimes |0\rangle\langle 0| E_k^\dagger\,. \tag{14}$$

For convenience, we define:

$$\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,R) = \frac{1}{\#\mathsf{R}^{n,t}_{\text{no}}} \sum_{r \in \mathsf{R}^{n,t}_{\text{no}}} \tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r)\,. \tag{15}$$

If the QKRS is statistically secure then, according to condition 2 of Definition 3.2, we get that

$$\begin{aligned}\delta(n) &\geq d(\hat{K}|\tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,R)) = D(\tilde{\rho}^{\text{no}}_{\hat{K}\mathsf{E}}(x,R), \mathbb{I}_t \otimes \tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,R)) \\ &= D\left(\sum_{\hat{k}} P_{\hat{K}}(\hat{k})|\hat{k}\rangle\langle\hat{k}| \otimes \tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,R), \mathbb{I}_t \otimes \tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,R)\right) \qquad (16) \\ &\geq \frac{2^{-n}}{\#\mathsf{R}^{n,t}_{\text{no}}} \sum_{r \in \mathsf{R}^{n,t}_{\text{no}}} \sum_{\hat{k}} \#r^{-1}(\hat{k}) D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), \tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,r)) \qquad (17)\end{aligned}$$

[2] Remember that the key length of $\hat{K}$ is s conditioned on $\mathcal{A}_{\text{ok}}$ and t conditioned on $\mathcal{A}_{\text{no}}$.

$$= \frac{2^{-n}}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{r \in \mathsf{R}_{\text{no}}^{n,t}} \sum_{\hat{k}} \#r^{-1}(\hat{k}) D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), 2^{-n} \sum_{k} \rho_{\mathsf{Q}|K=k,X=x})$$

$$= \frac{2^{-n}}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{r \in \mathsf{R}_{\text{no}}^{n,t}} \sum_{\hat{k}} \#r^{-1}(\hat{k}) D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), \rho_{\mathsf{Q}|X=x}), \quad (18)$$

where (16) follows from (15). Equation (17) follows from the fact that in general $D(\rho,\sigma) = \max_{\{W_m\}_m} D(p(m), q(m))$ where the maximum is computed over all POVMs $\{W_m\}_m$ and $p(m) = \text{tr}(\rho W_m)$, $q(m) = \text{tr}(\sigma W_m)$ are probability distributions for the outcomes when applied to ρ and σ respectively (see for example Theorem 9.1 in Nielsen and Chuang 2000). In order to get (17) from (16) one only has to consider a POVM that first measures r and $\hat{k}$ before performing the POVM $\{W'_m\}_m$ (depending on r and $\hat{k}$) on the residual state that satisfies $D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), \rho_{\mathsf{Q}|X=x}) = d(p'(m), q'(m))$.

We are now ready to prove that when authentication fails, the recycled secret key for any secure QKRS must be $m-2$ bits shorter than the initial secret key:

Theorem 4.1 (Key-Recycling Bound) *Any statistically secure* (n,m,s,t)-QKRS *is such that* $t \le n - m + 2$.

In order to prove Theorem 4.1, we need the following lemma (Lemma 4.1) establishing that any statistically secure key-recycling applied when the authentication fails must be such that for any $X = x$, there exist $r_0 \in \mathsf{R}_{\text{no}}^{n,t}$ and $\hat{k}_0 \in \{0,1\}^t$ such that both $D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0), \rho_{\mathsf{Q}|X=x})$ is small and $\#r_0^{-1}(\hat{k}_0) \le 2^{n-t+1}$. We will then show that these conditions cannot be satisfied whenever $t \ge n - m + 2$ thus showing the desired result.

Lemma 4.1 *Let* $0 < c \le 1$ *be a constant and let* $\mathsf{R}_{\text{no}}^{n,t}$ *be a statistically secure key-recycling mechanism in case of authentication failure. Then, for all* $x \in \{0,1\}^m$ there exist $r_0 \in \mathsf{R}_{\text{no}}^{n,t}$ and $\hat{k}_0 \in \{0,1\}^t$ *such that*

1. $D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0), \rho_{\mathsf{Q}|X=x}) \le c$, and
2. $\#r_0^{-1}(\hat{k}_0) \le 2^{n-t+1}$.

Proof Suppose for a contradiction that for all $r \in \mathsf{R}_{\text{no}}^{n,t}$, all $\hat{k} \in \{0,1\}^t$ either

- $D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), \rho_{\mathsf{Q}|X=x}) > c$, or
- $\#r^{-1}(\hat{k}) > 2^{n-t+1}$.

Let $\delta(n)$ be a negligible function such that $\mathsf{R}_{\text{no}}^{n,t}$ is $\delta(n)$–uniform. We define $\mathcal{K}^*(r) = \{\hat{k} \mid D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), \rho_{\mathsf{Q}|X=x}) > c\}$ as the set of recycled keys for which condition 1 is not satisfied for r. Remember that $\Pr(\hat{K} = \hat{k} \mid R = r) = 2^{-n}\#r^{-1}(\hat{k})$ where $\hat{K}$ is the random variable for the recycled key. Using (18), we easily get

$$\begin{aligned}
\delta(n) &\ge \frac{1}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{R} \sum_{\hat{k}} 2^{-n} \#r^{-1}(\hat{k}) D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r), \rho_{\mathsf{Q}|X=x}) \\
&\ge \frac{1}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{r} \sum_{\hat{k} \in \mathcal{K}^*(r)} 2^{-n} \#r^{-1}(\hat{k}) \cdot c \\
&= \frac{c}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{r} \Pr(\hat{K} \in \mathcal{K}^*(r) \mid R = r) \\
&= c \cdot \Pr(\hat{K} \in \mathcal{K}^*(r)),
\end{aligned}$$

which implies

$$\Pr(\hat{K} \in \mathcal{K}^*(r)) \le \frac{\delta(n)}{c}. \quad (19)$$

On the other hand, when $\hat{K} \notin \mathcal{K}^*(r)$ then by assumption $\#r^{-1}(\hat{k}) > 2^{n-t+1}$ which implies that for all $\hat{k}$, $P_{\hat{K}}(\hat{k}) = 2^{-n}\#r^{-1}(\hat{k}) > 2^{-t+1}$. By definition of a statistically secure key-recycling mechanism, we have

$$\delta(n) \ge d(\hat{K} \mid \tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,R)) \ge d(\hat{K} \mid R) \quad (20)$$

$$\begin{aligned}
&\ge \frac{1}{2} \sum_{r} \frac{1}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{\hat{k} \notin \mathcal{K}^*(r)} |\Pr(\hat{K} = \hat{k} \mid R = r) \\
&\quad - 2^{-t}| \ge \frac{1}{2} \sum_{r} \frac{1}{\#\mathsf{R}_{\text{no}}^{n,t}} \sum_{\hat{k} \notin \mathcal{K}^*(r)} \frac{\Pr(\hat{K} = \hat{k} \mid R = r)}{2}
\end{aligned} \quad (21)$$

$$\ge \frac{1}{4}(1 - \Pr(\hat{K} \in \mathcal{K}^*(r))) \ge \frac{1}{4}\left(1 - \frac{\delta(n)}{c}\right), \quad (22)$$

where (20) follows since forgetting can only decrease the distance to uniform. Equation (21) is obtained from the fact that $\hat{K} \notin \mathcal{K}^*(r)$, as discussed in the previous paragraph. Finally, (22) follows from (19). Clearly, (22) leads to a contradiction when $\delta(n)$ is negligible. It follows that conditions 1 and 2 must be satisfied by some r_0 and $\hat{k}_0$. □

One last technical lemma is needed to prove Theorem 4.1. It establishes that for any $x \in \{0,1\}^m$ and $\hat{k}_0 \in \{0,1\}^t$ such that $\#r_0^{-1}(\hat{k}_0) \le 2^{m-1}$, the adversary's state $\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)$ (i.e. whenever the adversary keeps the whole cipherstate $\rho_{\mathsf{Q}|X=x}$) is such that $D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0), \rho_{\mathsf{Q}})$ is at least $\frac{1}{2}$.

Lemma 4.2 *Let* $r_0 \in \mathsf{R}_{\text{no}}^{n,t}$ *and* $\hat{k}_0 \in \{0,1\}^t$ *be such that* $\#r_0^{-1}(\hat{k}_0) \le 2^{m-1}$. *Then,*

$$D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0), \rho_{\mathsf{Q}}) \ge \frac{1}{2}.$$

Proof We lower bound the trace-norm distance between $\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)$ and ρ_{Q} using a similar argument as in the proof of Lemma IV.3.2 in Bhatia (1997). We rewrite the

operator $\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)-\rho_{\mathsf{Q}}$ as $P-N$, where P, and N are positive operators with orthogonal support. We then have,

$$D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}}(x,r_0),\rho_{\mathsf{Q}}) = \frac{1}{2}\text{tr}(|\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)-\rho_{\mathsf{Q}}|) = \frac{1}{2}\text{tr}(P+N)\,,$$

since P and N have orthogonal support. From $\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)-\rho_{\mathsf{Q}}=P-N$, we define the operator $C=\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)+N=\rho_{\mathsf{Q}}+P$ so that,

$$\begin{aligned}D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0),\rho_{\mathsf{Q}}) &= \frac{1}{2}\text{tr}(C-\rho_{\mathsf{Q}}+C-\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))\\ &\geq \frac{1}{2}\sum_i 2\lambda_i^{\downarrow}(C)-\lambda_i^{\downarrow}(\rho_{\mathsf{Q}})\\ &\quad -\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))\,,\end{aligned}$$

where $\lambda_i^{\downarrow}(C)$ are the eigenvalues of C in decreasing order. By Weyl's monotonicity theorem, $\lambda_i^{\downarrow}(C)\geq\lambda_i^{\downarrow}(\rho_{\mathsf{Q}})$ and $\lambda_i^{\downarrow}(C)\geq\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))$ for all i. Applying these inequalities and subtracting from $\lambda_i^{\downarrow}(C)$ the largest of the values $\lambda_i^{\downarrow}(\rho_{\mathsf{Q}})$ and $\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))$, lead to

$$\begin{aligned}&D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0),\rho_{\mathsf{Q}}) \geq \frac{1}{2}\sum_i \lambda_i^{\downarrow}(C)\\ &-\min\{\lambda_i^{\downarrow}(\rho_{\mathsf{Q}}),\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))\}\\ &\geq \frac{1}{2}\sum_i\Big(\max\{\lambda_i^{\downarrow}(\rho_{\mathsf{Q}}),\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))\}\\ &-\min\{\lambda_i^{\downarrow}(\rho_{\mathsf{Q}}),\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))\}\Big)\\ &=\frac{1}{2}\sum_i|\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0))-\lambda_i^{\downarrow}(\rho_{\mathsf{Q}})|. \qquad (23)\end{aligned}$$

The eigenvalues of ρ_{Q} are $\lambda(\rho_{\mathsf{Q}})=\lambda(\sum_k 2^{-n}M_k)$, where M_k is the rank 2^m matrix $\sum_x 2^{-m}E_k|x\rangle\langle x|\otimes|0\rangle\langle 0|E_k^{\dagger}$ with eigenvalues 2^{-m}. By Lidskii's theorem (see, for example, equation III.13 in Bhatia 1997) $\lambda^{\downarrow}(\sum_k 2^{-n}M_k)\prec\sum_k 2^{-n}\lambda^{\downarrow}(M_k)$ which is the vector where the first 2^m entries are 2^{-m}, and the remaining ones are all 0's[3] This means that the largest eigenvalue of ρ_{Q} is at most 2^{-m}. Since the rank of $\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)$ cannot exceed the cardinality of $r_0^{-1}(\hat{k}_0)$ which by assumption is 2^{m-1}, (23) is minimized when $\lambda_i^{\downarrow}(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0)))=2^{-m+1}$, for $i=1,\ldots,2^{m-1}$, and $\lambda_i^{\downarrow}(\rho_{\mathsf{Q}})=2^{-m}$, for $i=1,\ldots,2^m$. We finally get the desired result:

$$\begin{aligned}&D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0),\rho_{\mathsf{Q}})\geq\frac{1}{2}\left(2^{m-1}(2^{-m+1}-2^{-m})\right.\\ &\left.+(2^m-2^{m-1})2^{-m}\right)=\frac{1}{2}\,.\end{aligned}$$

□

The previous two lemmas allow to prove Theorem 4.1. We show that for any QKRS with $t\geq n-m+2$, Lemma 4.2 implies that both conditions of Lemma 4.1 cannot be satisfied allowing to conclude that the key-recycling mechanism $\mathsf{R}^{n,t}_{\text{no}}$ cannot be statistically secure.

Proof (of Theorem 4.1) Assume for a contradiction that $(\mathfrak{C}^{n,m},(\mathsf{R}^{n,s}_{\text{ok}},\mathsf{R}^{n,t}_{\text{no}}))$ is a statistically secure (n,m,s,t)-QKRS with $t>n-m+2$. Using the triangle inequality, we have:

$$\begin{aligned}D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0),\rho_{\mathsf{Q}}) &\leq D(\tilde{\rho}^{\text{no}}_{\mathsf{E}|\hat{K}=\hat{k}_0}(x,r_0),\rho_{\mathsf{Q}|X=x})\\ &\quad + D(\rho_{\mathsf{Q}|X=x},\rho_{\mathsf{Q}})\leq c+\epsilon(n)\,,\end{aligned} \qquad (24)$$

for $\hat{k}_0\in\{0,1\}^t$ and $r_0\in\mathsf{R}^{n,t}_{\text{no}}$ guaranteed by Lemma 4.1 (i.e. for any $0<c\leq 1$) together with Lemma 2.1 since the cipher is $\epsilon(n)$–private for some negligible function $\epsilon(n)$. However, since $t\geq n-m+2$ we have that $\#r_0^{-1}(\hat{k}_0)\leq 2^{n-t+1}\leq 2^{m-1}$, and Lemma 4.2 can be applied to the left hand-side of (24). We get,

$$\frac{1}{2}\leq c+\epsilon(n)\,,$$

providing the desired contradiction for any constant $c<\frac{1}{2}$ since $\epsilon(n)$ is negligible. □

We believe that a more careful analysis would show that statistically secure (n,m,s,t)-QKRS must satisfy $t\leq n-m$. Theorem 4.1 implies that recycling significantly more secret key bits than any classical scheme can only happen when the authentication succeeds.

5 A near optimal quantum key-recycling scheme

We introduce a QKRS, called $\mathsf{W}_n\mathsf{C}_m$, that recycles an almost optimal amount of key material. Moreover, the key-recycling mechanism does not use privacy amplification. Deterministic functions are sufficient to guarantee the statistical security of the recycled key. The scheme is introduced in Sect. 5.1. In Sect. 5.2, we present an EPR-version of the scheme and we prove it secure in the following three subsections. In Sect. 5.6, we reduce the security of $\mathsf{W}_n\mathsf{C}_m$ to that of the EPR-version.

5.1 The scheme

The $\mathsf{W}_n\mathsf{C}_m$-cipher encrypts a message together with its Wegman-Carter one-time authentication tag (Carter and

[3] $(x_1,\ldots,x_n)\prec(y_1,\ldots,y_n)$ means that vector x is majorized by vector y. That is, $\sum_{i=1}^{\ell}x_i\leq\sum_{i=1}^{\ell}y_i$ for all $1\leq\ell\leq n$.

Fig. 1 The $\mathsf{W}_n\mathsf{C}_m$ key-recycling scheme

Private-Key: $(z,b,u) \in_R \{0,1\}^{2n+m}$ where $n = m + \ell(m)$,
Plaintext: $x \in \{0,1\}^m$.

1. Alice creates the message $c = (x, h_u(x))$ where $h_u \in H^{\oplus}_{m,\ell(m)}$. She then encrypts this message with key (z,b) according to the W_n-cipher.
2. Bob decodes the received W_n-cipher with key (z,b) and gets $c' = (x', t')$. He then verifies the authentication tag $t' = h_u(x')$. Bob sends the result of the test to Alice through a classical authentic channel.
3. **[Key-Recycling]** If Bob accepts then Alice and Bob recycle the entire key (b,z,u). If Bob rejects then Alice and Bob recycle (b,u) and throw away $z \in \{0,1\}^n$.

Wegman 1977) using the W_n-cipher (Damgård et al. 2004). We need an authentication code constructed from XOR-universal classes of hash-functions:

Definition 5.1 (Carter and Wegman 1977) An XOR-*universal family of hash-functions* is a set of functions $H^{\oplus}_{m,\ell} = \{h_u : \{0,1\}^m \to \{0,1\}^\ell\}_u$ such that for all $a \neq b \in \{0,1\}^m$ and all $y \in \{0,1\}^\ell$, $\#\{h \in H^{\oplus}_{m,\ell} | h(a) \oplus h(b) = y\} = \frac{\#H^{\oplus}_{m,\ell}}{2^\ell}$.

There exists an XOR-universal class of hash-functions $H^{\oplus}_{m,\ell}$ (for any $m \geq \ell$) that requires only m bits to specify and such that picking a function at random can be done efficiently. In the following, we assume that $H^{\oplus}_{m,\ell}$ is such an XOR-universal family of hash-functions.

For the transmission of m-bit messages, $\mathsf{W}_n\mathsf{C}_m$ requires Alice and Bob to share a secret key of size $N = 2n + m$ bits where $n = m + \ell(m)$, and $\ell(m) \in \Omega(m)$ is the size of the Wegman-Carter authentication tag. We denote secret key k by the triplet: $k = (z,b,u)$ where $z,b \in \{0,1\}^n$ is the key for the W_n-cipher and $u \in \{0,1\}^m$ is the description of a random function $h_u \in H^{\oplus}_{m,\ell(m)}$. Encrypting message $x \in \{0,1\}^m$ is performed by first computing the Wegman-Carter one-time authentication tag $h_u(x)$. The message $(x, h_u(x)) \in \{0,1\}^n$ is then encrypted using the W_n-cipher with secret key (z,b). Bob decrypts the W_n-cipher and verifies that a message of the form $(x, h_u(x))$ is obtained. Bob announces to Alice the outcome of the authentication using the authenticated feedback channel. When it is successful, Alice and Bob recycle the whole secret key. If the authentication fails then Alice and Bob throw away the one-time-pad $z \in \{0,1\}^n$. The remaining part (b,u) is entirely recycled. In other words, $\mathsf{R}^{N,s}_{\text{ok}}$ is the identity with $s = N$ and $\mathsf{R}^{N,t}_{\text{no}}$ is deterministic with $t = N - n = N - m - \ell(m)$ (Fig. 1).

It is almost straightforward to show that our key-recycling function is perfectly secure when authentication fails.

Lemma 5.1 *Let* $N = 2n + m$ *where* $n = m + \ell(m)$, $\ell(m) > 0$ *be the key-length used in* $\mathsf{W}_n\mathsf{C}_m$ *and let* $r_{\text{no}}(z,b,u) = (b,u)$ *for* $z,b \in \{0,1\}^n$ *and* $u \in \{0,1\}^m$. *The key-recycling mechanism* $\mathsf{R}^{N,N-n}_{\text{no}} = \{r_{\text{no}}\}$ *is uniform.*

Proof Let $k = (z,b,u)$ be the secret key used to send a cipherstate. Even if the adversary holds the entire cipherstate $\rho_{\mathsf{Q}|X=x}$ we show that the recycled key $\hat{k} = (b,u) := r_{\text{no}}(k) := r_{\text{no}}(z,b,u)$ is indistinguishable from uniform. Let $\hat{k} = (b,u)$ and $\hat{k}' = (b',u')$ be two possible recycled keys. It is easy to verify that for any $x \in \{0,1\}^m$, $\hat{k}$ and $\hat{k}'$, we have that $\rho_{\mathsf{Q}|X=x,\hat{K}=\hat{k}} = \mathbb{I}_n = \rho_{\mathsf{Q}|X=x,\hat{K}=\hat{k}'}$. It follows that $d(\hat{K}|\tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,R)) = d(\hat{K}|\tilde{\rho}^{\text{no}}_{\mathsf{E}}(x,r_{\text{no}})) = d(\hat{K}|\rho_{\mathsf{Q}|X=x}) = 0$. □

Since $\mathsf{W}_n\mathsf{C}_m$ encrypts m-bit messages and recycles $N - n$ bits of key, the scheme is sub-optimal according to Theorem 4.1. In the next sections, we see that $\mathsf{W}_n\mathsf{C}_m$ remains statistically secure for any $\ell(m) \in \Omega(m)$. It follows that although sub-optimal, $\mathsf{W}_n\mathsf{C}_m$ is *nearly* optimal.

It remains to prove that when no eavesdropping is detected, the entire secret key can safely be recycled. This is the topic of next subsections.

5.2 An EPR variant of $\mathsf{W}_n\mathsf{C}_m$

We establish the security of the key-recycling mechanism in $\mathsf{W}_n\mathsf{C}_m$ when the authentication is successful. We prove this case using a Shor–Preskill argument (Shor and Preskill 2000) similar to the ones invoked in Oppenheim and Horodecki (2003) and Barnum et al. (2002) for key-recycling and quantum authentication respectively.

We first define a variant of $\mathsf{W}_n\mathsf{C}_m$, called EPR-$\mathsf{W}_n\mathsf{C}_m$, using EPR-pairs and having access to an additional authenticated and private classical channel. The key-recycling mechanism of EPR-$\mathsf{W}_n\mathsf{C}_m$ can be proven secure more easily since it has access to more powerful resources. Second, we show that the security of $\mathsf{W}_n\mathsf{C}_m$ follows from the security of EPR-$\mathsf{W}_n\mathsf{C}_m$.

In EPR-$\mathsf{W}_n\mathsf{C}_m$, Alice and Bob initially share an n-bit key b, and an m-bit key u. They agree on 2^n mutually unbiased bases in $\mathcal{H}_n$, and a family of XOR-universal hash-functions $H^{\oplus}_{m,\ell} = \{h_u\}_{u \in \{0,1\}^m}$. As for $\mathsf{W}_n\mathsf{C}_m$, the key b is used to

select in which of the bases of the MUBS the encryption will take place. The key u indicates the selection of the hash-function for authentication. The key z in EPR-$\mathsf{W}_n\mathsf{C}_m$ is not shared beforehand but will be implicitly generated by measuring the shared EPR-pairs. This corresponds to refreshing z before each round of EPR-$\mathsf{W}_n\mathsf{C}_m$.

In order for Alice to send classical message $x \in \{0,1\}^m$ to Bob, Alice and Bob proceeds as described in Fig. 2. The key-recycling mechanism of EPR-$\mathsf{W}_n\mathsf{C}_m$ only takes place when authentication succeeds. The quantum transmission in $\mathsf{W}_n\mathsf{C}_m$ is replaced by transmitting half of a maximally entangled state consisting of n EPR-pairs:

$$|\Psi^n\rangle = \sum_{w\in\{0,1\}^n} 2^{-n/2}|w\rangle^A|w\rangle^B = \sum_{w\in\{0,1\}^n} 2^{-n/2}|\xi_w^{(b)}\rangle^A|v_w^{(b)}\rangle^B, \tag{25}$$

for one of the MUBS $\{|v_w^{(b)}\rangle\}_w$, and some orthonormal basis $\{|\xi_w^{(b)}\rangle\}_w$.

Let Q' be Alice's register holding her half EPR-pairs. Any trace-preserving operator the adversary can apply to Bob's half EPR-pairs can be described in terms of the 4^n Pauli operators $\{O_i\}_i$,

$$\begin{aligned}\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}} &= \mathcal{E}(|\Psi^n\rangle\langle\Psi^n|)\\ &= \sum_{i=0}^{4^n-1}\sum_{j=0}^{4^n-1} c_i\overline{c_j}(\mathbb{1}_n\otimes O_i)|\Psi^n\rangle\langle\Psi^n|(\mathbb{1}_n\otimes O_j)^\dagger,\end{aligned} \tag{26}$$

where $O_0 = \mathbb{1}_n$. We can split (26) into the case where the error leaves the state untouched, and the case where the state is modified:

$$\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}} = |c_0|^2|\Psi^n\rangle\langle\Psi^n| + (1-|c_0|^2)\tilde{\rho}_{\mathcal{E}}, \tag{27}$$

where $\tilde{\rho}_{\mathcal{E}} = \sum_{(i,j)\neq(0,0)} \frac{c_i\overline{c_j}}{(1-|c_0|^2)}(\mathbb{1}_n\otimes O_i)|\Psi^n\rangle\langle\Psi^n|(\mathbb{1}_n\otimes O_j)^\dagger$, and $|c_0|^2$ is the probability that the state is left unchanged by $\mathcal{E}$.

The idea behind the security of the key-recycling mechanism is to show that conditioned on successful Wegman-Carter authentication, the eavesdropper has performed essentially no action upon Bob's system. Moreover, when no action took place, Alice's and Bob's entire secret key can be recycled since nothing the eavesdropper holds contains any information about it.

The probability that Bob accepts the authentication tag, when Alice and Bob share key (b,u), can be expressed by the observable projecting onto the space of states where Alice has her untouched EPR-halves, and Bob has anything that passes the authentication test:

$$\Pi_{\text{ok}}^{b,u} = \sum_{z\in\{0,1\}^n}\sum_{\hat{x}\in\{0,1\}^m} |\xi_{e_{z,u}(x)}^{(b)}\rangle\langle\xi_{e_{z,u}(x)}^{(b)}| \otimes |v_{e_{z,u}(\hat{x})}^{(b)}\rangle\langle v_{e_{z,u}(\hat{x})}^{(b)}|, \tag{28}$$

where $e_{z,u}(x) = z \oplus (x, h_u(x))$. We denote the probability that Bob accepts the authentication, when using key (b,u), is

$$p_{\text{ok}}^{b,u} := \text{tr}(\Pi_{\text{ok}}^{b,u}\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}}) = |c_0|^2 + (1-|c_0|^2)\text{tr}(\Pi_{\text{ok}}^{b,u}\tilde{\rho}_{\mathcal{E}}). \tag{29}$$

As mentioned in Sect. 2.4, all 4^n-1 Pauli operators (excluding the identity) are partitioned into 2^n+1 sets, each containing 2^n-1 commuting members. Each operator, O_i, appearing in (26), will be in one of the 2^n+1 partitions. In the partition or basis where an error operator O_i belongs, its action will leave all cipherstates unchanged. O_i will anti-commute with exactly half the operators (including the identity) in the remaining 2^n partitions. In these partitions or bases the action of O_i permutes the basis vectors (cipherstates). Since this permutation is independent of the authentication code, we can show that the probability for O_i to remain undetected is negligible when the class of Wegman-Carter authentication functions used is XOR-universal. Let $\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}|\mathcal{A}_{\text{ok}}}^{b,u}$ be the state $\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}}$ conditioned on $\mathcal{A}_{\text{ok}}$ for secret key (b,u):

$$\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}|\mathcal{A}_{\text{ok}}}^{b,u} := \frac{\Pi_{\text{ok}}^{b,u}\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}}\Pi_{\text{ok}}^{b,u}}{p_{\text{ok}}^{b,u}}, \tag{30}$$

where $p_{\text{ok}}^{b,u}$ is the re-normalization factor defined in (29).

Fig. 2 The EPR-$\mathsf{W}_n\mathsf{C}_m$-cipher using an extra private and authentic classical channel

Private-Key: $(b,u) \in_R \{0,1\}^{n+m}$,
Plaintext: $x \in \{0,1\}^m$.

1. Alice prepares the n EPR-pairs in state $|\Psi^n\rangle^{AB}$.
2. Alice sends the B-register to Bob.
3. Bob acknowledges receiving the state using the classical authentic feedback channel.
4. Alice measures her A-register in basis $\{|\xi_c^{(b)}\rangle\}_{c\in\{0,1\}^n}$ (See (25)). On classical outcome c, she computes $z := c \oplus (x, h_u(x))$.
5. Alice sends z to Bob through the additional private and authenticated classical channel.
6. Bob measures his B-register in the b-th basis of the MUBS, gets outcome c', and computes $(x',t') = c' \oplus z$. Bob verifies that $t' = h_u(x')$ and announces the result to Alice through the classical authenticated feedback channel.
7. If Bob accepts, Alice and Bob recycle the whole key (b,u).

5.3 Upper bounding the probability of successful authentication

The following Lemma relates the probability that Bob accepts the authentication to the probability that Eve did not modify the cipher forwarded to Bob. The result is obtained from the XOR-universality of $H^{\oplus}_{n,\ell(m)}$. This is the main technical lemma needed for concluding that the secret key can be safely re-used when authentication succeeds. The intuition being that the entire key can be safely re-used since authentication succeeds almost only when the cipherstate has not been tampered with during transmission. When no eavesdropping occurred, no information about the secret key is available to the adversary even in a known plaintext attack.

Lemma 5.2 *Let* $p_{\text{ok}} = 2^{-m-n}\sum_{b,u} p^{b,u}_{\text{ok}} = 2^{-m-n}\sum_{b,u} \text{tr}(\Pi^{b,u}_{\text{ok}}\tilde{\rho}_{\text{Q'Q}})$ *be the average probability that Bob accepts the authentication (when the probability is taken over all keys), and let* $|c_0|^2$ *be defined as in* (27)*.Then,* $p_{\text{ok}} \leq |c_0|^2 + 2^{-n+m+2}$,

which implies that $2^{-n-m}\sum_{(b,u)} \text{tr}(\Pi^{b,u}_{\text{ok}}\tilde{\rho}_{\mathcal{E}}) \leq 2^{-n+m+2}$.

Proof Equality (27) allows to write $\text{tr}(\Pi^{b,u}_{\text{ok}}\tilde{\rho}_{\text{Q'Q}}) = |c_0|^2$ tr $(|\Psi^n\rangle\langle\Psi^n|) + (1-|c_0|^2)\,\text{tr}(\Pi^{b,u}_{\text{ok}}\tilde{\rho}_{\mathcal{E}})$. We then get,

$$p_{\text{ok}} = |c_0|^2 + (1-|c_0|^2)2^{-n-m}\sum_{b\in\{0,1\}^n}\sum_{u\in\{0,1\}^m}\text{tr}(\Pi^{b,u}_{\text{ok}}\tilde{\rho}_{\mathcal{E}})\,. \tag{31}$$

Since

$\tilde{\rho}_{\mathcal{E}} = \sum_{(i,j)\neq(0,0)}\frac{c_i\overline{c_j}}{(1-|c_0|^2)}(\mathbb{1}_n\otimes O_i)|\Psi^n\rangle\langle\Psi^n|(\mathbb{1}_n\otimes O_j)^\dagger$, the trace on the right hand side of (31) is

$$\sum_{(i,j)\neq(0,0)}\frac{c_i\overline{c_j}\,2^{-n}}{(1-|c_0|^2)}$$
$$\times\sum_{k,l\in\{0,1\}^m}\text{tr}(\Pi^{b,u}_{\text{ok}}\left(|\xi^{(b)}_k\rangle\langle\xi^{(b)}_l|\otimes O_i|v^{(b)}_k\rangle\langle v^{(b)}_l|O_j^\dagger\right))\,. \tag{32}$$

Using the notation from Sect. 2.4 (i.e. $P^b_a := |v^{(b)}_a\rangle\langle v^{(b)}_a|$), and applying the equality $\text{tr}(A\otimes B) = \text{tr}(A)\text{tr}(B)$, the inner sum of (32) becomes

$$\sum_{k,l\in\{0,1\}^m}\text{tr}(\Pi^{b,u}_{\text{ok}}\left(|\xi^{(b)}_k\rangle\langle\xi^{(b)}_l|\otimes O_i|v^{(b)}_k\rangle\langle v^{(b)}_l|O_j^\dagger\right))$$
$$=\sum_{k,l,\hat{x}\in\{0,1\}^m}\sum_{z\in\{0,1\}^n}\text{tr}(|\xi^{(b)}_{e_{z,u}(x)}\rangle\langle\xi^{(b)}_{e_{z,u}(x)}||\xi^{(b)}_k\rangle\langle\xi^{(b)}_l|)$$
$$\times\,\text{tr}(|v^{(b)}_{e_{z,u}(\hat{x})}\rangle\langle v^{(b)}_{e_{z,u}(\hat{x})}|O_i|v^{(b)}_k\rangle\langle v^{(b)}_l|O_j^\dagger)$$
$$=\sum_{z\in\{0,1\}^n}\sum_{\hat{x}\in\{0,1\}^m}\text{tr}(P^b_{e_{z,u}(\hat{x})}O_iP^b_{e_{z,u}(x)}O_j^\dagger)\,, \tag{33}$$

where (33) is obtained easily after observing that $\text{tr}(|\xi^{(b)}_{e_{z,u}(x)}\rangle\langle\xi^{(b)}_{e_{z,u}(x)}||\xi^{(b)}_k\rangle\langle\xi^{(b)}_l|) = \langle\xi^{(b)}_{e_{z,u}(x)}|\xi^{(b)}_k\rangle\langle\xi^{(b)}_l|\xi^{(b)}_{e_{z,u}(x)}\rangle$ which is 1 if $k=l=e_{z,u}(x)$ and 0 otherwise. We can re-write the trace in (33) by expressing the two projectors as linear combinations of Pauli operators as in (9). This way, the trace in (33) becomes:

$$\begin{aligned}
&\text{tr}\left(\left(2^{-n}\sum_{\mu'\in\{0,1\}^n}\varepsilon_{(\mu',e_{z,u}(\hat{x}))}O^b_{\mu'}\right)O_i\left(2^{-n}\sum_{\mu\in\{0,1\}^n}\varepsilon_{(\mu,e_{z,u}(x))}O^b_{\mu}\right)O_j^\dagger\right)\\
&=2^{-2n}\sum_{\mu,\mu'\in\{0,1\}^n}\varepsilon_{(\mu',e_{z,u}(\hat{x}))}\varepsilon_{(\mu,e_{z,u}(x))}\text{tr}(O^b_{\mu'}O^b_{\mu}O_iO_j^\dagger)\\
&=2^{-2n}\sum_{\mu,\mu'\in\{0,1\}^n}\varepsilon_{(\mu',e_{z,u}(\hat{x}))}\varepsilon_{(\mu,e_{z,u}(x))}(-1)^{\text{Com}(O_i,O^b_\mu)}\text{tr}(O^b_{\mu'}O^b_{\mu}O_iO_j^\dagger)\,,
\end{aligned} \tag{34}$$

where $\text{Com}(O_i,O^b_\mu)$ is 0 if O_i and O^b_μ commute, and 1 if they anti-commute; notice that since both O_i and O^b_μ are Pauli operators they will either commute or anti-commute.

Using the fact that $(\varepsilon_{\alpha,\beta})_{\alpha,\beta} := 2^{n/2}H^{\otimes n}$ (i.e. $\varepsilon_{\alpha,\beta} = (-1)^{\alpha\cdot\beta}$), we see that,

$$\begin{aligned}
&\sum_{z\in\{0,1\}^n}\varepsilon_{(\mu',e_{z,u}(\hat{x}))}\varepsilon_{(\mu,e_{z,u}(x))}\\
&=\sum_{z\in\{0,1\}^n}(-1)^{\mu'\cdot(z\oplus(\hat{x},h_u(\hat{x})))}(-1)^{\mu\cdot(z\oplus(x,h_u(x)))}\\
&=(-1)^{\mu'\cdot(\hat{x},h_u(\hat{x}))\oplus\mu\cdot(x,h_u(x))}\sum_{z\in\{0,1\}^n}(-1)^{z\cdot(\mu\oplus\mu')}\\
&=2^n\delta_{\mu,\mu'}(-1)^{\mu'\cdot(\hat{x},h_u(\hat{x}))\oplus\mu\cdot(x,h_u(x))}\,.
\end{aligned} \tag{35}$$

We insert (34) into (33) using (35) together with the fact that $(O^b_\mu)^2 = \mathbb{1}_n$ to obtain:

$$\begin{aligned}
&\sum_{k,l\in\{0,1\}^m}\text{tr}(\Pi^{b,u}_{\text{ok}}|\xi^{(b)}_k\rangle\langle\xi^{(b)}_l|\otimes O_i|v^{(b)}_k\rangle\langle v^{(b)}_l|O_j^\dagger)\\
&=2^{-n}\sum_{\hat{x}\in\{0,1\}^m}\sum_{\mu\in\{0,1\}^n}(-1)^{\mu\cdot(\hat{x},h_u(\hat{x}))\oplus\mu\cdot(x,h_u(x))\oplus\text{Com}(O_i,O^b_\mu)}\text{tr}(O_iO_j^\dagger)\,,
\end{aligned} \tag{36}$$

which is non-zero only when $i=j$, since $\text{tr}(O_iO_j^\dagger) = \delta_{i,j}2^n$. Inserting (36) into (32), leads to

$$\begin{aligned}
\text{tr}(\Pi^{b,u}_{\text{ok}}\tilde{\rho}_{\mathcal{E}}) &= \sum_{i\neq 0}\frac{2^{-n}|c_i|^2}{(1-|c_0|^2)}\\
&\times\sum_{\hat{x}\in\{0,1\}^m}\sum_{\mu\in\{0,1\}^n}(-1)^{\mu\cdot((\hat{x},h_u(\hat{x}))\oplus(x,h_u(x)))\oplus\text{Com}(O_i,O^b_\mu)}.
\end{aligned} \tag{37}$$

Let $\mu_0\in\{0,1\}^m$ be the first m bits of μ, and $\mu_1\in\{0,1\}^{n-m}$ the last $n-m$ bits of μ. We can now use the fact that h_u is taken from a XOR-universal classes of hash-functions to upper bound

$$\sum_{\hat{x}\in\{0,1\}^m}\sum_{u\in\{0,1\}^m}(-1)^{\mu\cdot((\hat{x},h_u(\hat{x}))\oplus(x,h_u(x)))}\,. \tag{38}$$

When $\hat{x} = x$, the whole sum is 2^{2m} so (38) is

$$2^{2m} + \sum_{\hat{x}\in\{0,1\}^m, \hat{x}\neq x} (-1)^{\mu_0\cdot(\hat{x}\oplus x)} \sum_{u\in\{0,1\}^m} (-1)^{\mu_1\cdot(h_u(\hat{x})\oplus h_u(x))}. \tag{39}$$

If $\mu_1 = 0^{n-m}$ then the inner sum is 2^m else it is zero since, by definition of XOR-universal class of hash-functions, each $n-m$ bit string occurs the same number of times when generating by $h_u(\hat{x}) \oplus h_u(\hat{x}), x \neq \hat{x}$ over all possible choices for u. Equation (39) then becomes,

$$2^{2m} + \delta_{\mu_1,0} 2^m \sum_{\hat{x}\in\{0,1\}^m, \hat{x}\neq x} (-1)^{\mu_0\cdot(\hat{x}\oplus x)}. \tag{40}$$

The last sum in (40) is 2^m if $\mu_0 = 0^m$. Otherwise, it is -1 since the only element $\hat{x} \oplus x$ not included in the sum is the all zeros m-bitstring. Equation (38) can then be re-written using (40) as,

$$\sum_{\hat{x},u\in\{0,1\}^m} (-1)^{\mu\cdot((\hat{x},h_u(\hat{x}))\oplus(x,h_u(x)))} = 2^{2m} + \delta_{\mu_1,0^{n-m}} \times 2^m(\delta_{\mu_0,0^m} 2^m - (1-\delta_{\mu_0,0^m})) \leq 2^{2m} + \delta_{\mu,0^n}(2^{2m}+2^m). \tag{41}$$

After inserting (37) into (31) using (41), we get

$$\begin{aligned} p_{\text{ok}} &= |c_0|^2 + (1-|c_0|^2) 2^{-n-m} \sum_{b\in\{0,1\}^n} \sum_{u\in\{0,1\}^m} \text{tr}(\Pi_{\text{ok}}^{b,u} \tilde{\rho}_{\mathcal{E}}) \\ &= |c_0|^2 + 2^{-2n-m} \sum_{b\in\{0,1\}^n} \sum_{i\neq 0} |c_i|^2 \\ &\quad \sum_{\mu\in\{0,1\}^n} \sum_{\hat{x}\in\{0,1\}^m} \sum_{u\in\{0,1\}^m} (-1)^{\mu\cdot((\hat{x},h_u(\hat{x}))\oplus(x,h_u(x)))\oplus \text{Com}(\text{O}_i,\text{O}_\mu^b)} \\ &\leq |c_0|^2 + 2^{-2n-m} \sum_{b\in\{0,1\}^n} \sum_{i\neq 0} |c_i|^2 \\ &\quad \sum_{\mu} (2^{2m} + \delta_{\mu,0^n}(2^{2m}+2^m)) (-1)^{\text{Com}(\text{O}_i,\text{O}_\mu^b)}. \end{aligned} \tag{42}$$

When $\mu = 0^n, \text{Com}(O_i, O_\mu^b) = 0$ since $O_{0^n}^b = 11_n$ for all $b \in \{0,1\}^n$. For $\mu = 0^n$, (42) becomes:

$$2^{-2n-m} \sum_{b\in\{0,1\}^n} \sum_{i\neq 0} |c_i|^2 (2^{2m} + \delta_{0^n,0^n}(2^{2m}+2^m)) \times (-1)^{\text{Com}(\text{O}_i,\text{O}_{0^n}^b)} = 2^{-n-m} \sum_{i\neq 0} |c_i|^2 (2^{2m+1} + 2^m). \tag{43}$$

We now look at (42) when $\mu \neq 0^n$. The basis $b[i]$ for which $O_i \in \{O_\mu^{b[i]}\}_\mu$ is such that O_i commutes with all operators $O_\mu^{b[i]}$. It follows that summing $(-1)^{\text{Com}(\text{O}_i,\text{O}_\mu^{b[i]})}$ over terms $\mu \neq 0^n$ therefore results in $(2^n - 1)$. Remember that the Pauli operator O_i anti-commutes with exactly half the Pauli operators (including the identity and the extra $2^n + 1$-th basis that we are not using) contained in all bases (i.e. partitions). Summing $(-1)^{\text{Com}(\text{O}_i,\text{O}_\mu^b)}$ over all $b \neq b[i]$ and all $\mu \neq 0^n$ can therefore be at most $-(2^n - 1)$ since there are at least $2^n - 1$ more operators O_μ^b that anti commute with O_i (i.e. in the worst case O_i anti-commutes with all operators in the $2^n + 1$-th partition that we are not using) than commute with O_i since the identity $O_{0^n}^b$ is considered in the sums. Formally, the right-hand side of (42) with $\mu \neq 0^n$ can be upper-bounded as:

$$\begin{aligned} &2^{-2n-m} \sum_{b\in\{0,1\}^n} \sum_{i\neq 0} |c_i|^2 \sum_{\mu\neq 0} (2^{2m} + \delta_{\mu,0^n}(2^{2m}+2^m)) \\ &\times (-1)^{\text{Com}(\text{O}_i,\text{O}_\mu^b)} = 2^{-2n-m} \sum_{b\in\{0,1\}^n} \sum_{i\neq 0} |c_i|^2 \sum_{\mu\neq 0} 2^{2m} (-1)^{\text{Com}(\text{O}_i,\text{O}_\mu^b)} \\ &= 2^{-2n-m} \sum_{i\neq 0} |c_i|^2 2^{2m} \left((2^n - 1) + \sum_{b\neq b[i]} \sum_{\mu\neq 0} (-1)^{\text{Com}(\text{O}_i,\text{O}_\mu^b)} \right) \\ &\leq 2^{-2n-m} \sum_{i\neq 0} |c_i|^2 2^{2m} ((2^n - 1) - (2^n - 1)) = 0. \end{aligned} \tag{44}$$

Finally, inserting (43) and (44) in (42) results in

$$\begin{aligned} p_{\text{ok}} &\leq |c_0|^2 + 2^{-n-m} \sum_{i\neq 0} |c_i|^2 (2^{2m+1} + 2^m) \\ &\leq |c_0|^2 + 2^{-n+m+2} (1 - |c_0|^2) \leq |c_0|^2 + 2^{-n+m+2}. \end{aligned}$$

This completes the proof. □

5.4 Key Indistinguishability of EPR-$\mathsf{W}_n\mathsf{C}_m$

In this subsection we show (Theorem 5.1) that the state shared by Alice, Bob, and the eavesdropper upon successful authentication is at negligible distance to the state they would share if no eavesdropping had occurred. We start with the following easy consequence of Lemma 5.2:

Lemma 5.3 *Assume* $p_{\text{ok}} \geq 2^{-\frac{n-m-2}{2}}(1 + 2^{-\frac{n-m-2}{2}})$. Then,

$$2^{-n-m} \sum_{b\in\{0,1\}^n} \sum_{u\in\{0,1\}^m} \frac{p_{\text{ok}}^{b,u} - |c_0|^2}{p_{\text{ok}}^{b,u}} \leq 2^{-\frac{n-m-2}{2}}. \tag{45}$$

Proof The assumption on p_{ok} in the statement together with Lemma 5.2 allow to conclude:

$$\begin{aligned} &2^{-\frac{n-m-2}{2}}(1 + 2^{-\frac{n-m-2}{2}}) \leq p_{\text{ok}} \leq |c_0|^2 + 2^{-n+m+2} \\ &\Rightarrow |c_0|^2 \geq 2^{-\frac{n-m-2}{2}}. \end{aligned} \tag{46}$$

Let $p_{\mathcal{E}}^{b,u} := \text{tr}(\Pi_{\text{ok}}^{b,u} \tilde{\rho}_{\mathcal{E}})$ be the probability of a successful authentication whenever the adversary has non-trivially eavesdropped and the secret key is (b,u). We have,

$$2^{-n-m} \sum_{(b,u)} \frac{p_{\text{ok}}^{b,u} - |c_0|^2}{p_{\text{ok}}^{b,u}} = 2^{-n-m} \sum_{(b,u)} \frac{(1-|c_0|^2) p_{\mathcal{E}}^{b,u}}{p_{\text{ok}}^{b,u}} \tag{47}$$

$$\leq \frac{(1-|c_0|^2)}{|c_0|^2} 2^{-n-m} \sum_{(b,u)} p_{\mathcal{E}}^{b,u} \tag{48}$$

$$\leq \frac{2^{-n+m+2}}{|c_0|^2} \tag{49}$$

$$\leq 2^{-\frac{n-m-2}{2}}, \tag{50}$$

where (47) follows from (29), (48) uses the fact that $p_{\text{ok}}^{b,u} \geq |c_0|^2$, (49) invokes Lemma 5.2, and finally (50) uses (46). □

We now introduce the state held by the eavesdropper upon successful authentication. Remember that the random hashing function R in EPR-$\mathsf{W}_n\mathsf{C}_m$ is always the identity function. This allows to write

$$\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x) := \tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x,R)\,,$$

where the right hand side is the state of the eavesdropper as defined in (10). Assume now that the secret key $K=(b,u)$ is initially uniform. That is, prior to the quantum transmission K is uniformly distributed in $\{0,1\}^{n+m}$ from the eavesdropper's point of view. In this case, the joint state upon successful authentication $\tilde{\rho}_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}$, including the secret key, registers $\mathsf{Q}'\mathsf{Q}$ initially in state $|\Psi^n\rangle$, and the eavesdropper's register E, can be written as:

$$\tilde{\rho}_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}} := 2^{-n-m} \times \sum_{b\in\{0,1\}^n} \sum_{u\in\{0,1\}^m} |(b,u)\rangle\langle(b,u)| \otimes \tilde{\rho}_{\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}^{b,u}\,, \tag{51}$$

where $\text{tr}_{\mathsf{E}}(\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}^{b,u}) = \tilde{\rho}_{\mathsf{Q}'\mathsf{Q}|\mathcal{A}_{\text{ok}}}^{b,u}$ as defined in (30). We also have that $\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x) = \text{tr}_{K\mathsf{Q}'\mathsf{Q}}(\tilde{\rho}_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}})$ since the state sent $|\Psi^n\rangle$ is independent of the plaintext $X=x$. For a given view of the adversary, all plaintexts have the same probability to occur than before Alice's transmission given that $z = c \oplus (x, h_u(x))$ is sent through a private and authenticated channel from Alice to Bob. As far as the eavesdropper is concerned, nothing transmitted is correlated to the plaintext. In the following, we assume that the joint state of Alice, Bob, and the eavesdropper for a given secret key K is in pure state. This only provides the eavesdropper with more power.

Let $\sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}}$ be the state that Alice,Bob, and the eavesdropper would share if no eavesdropping occurred (and the secret key was initially uniform):

$$\sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}} := 2^{-n-m} \sum_{(b,u)\in\{0,1\}^{n+m}} |(b,u)\rangle\langle(b,u)| \otimes |\Psi^n\rangle\langle\Psi^n| \otimes \tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x)\,. \tag{52}$$

The following theorem establishes that $\tilde{\rho}_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}$ is close to be in state $\sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}}$ when the probability p_{ok} that $\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}}$ gets successfully authenticated is not too small. The proof is an easy consequence of Lemma 5.3.

Theorem 5.1 *Let $\tilde{\rho}_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}$ be defined as in (51). Assume that $p_{\text{ok}} \geq 2^{-\frac{n-m-2}{2}}(1+2^{-\frac{n-m-2}{2}})$ and that the secret key is initially uniform. Then,*

$$D(\tilde{\rho}_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}, \sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}}) \leq 2^{-\frac{n-m}{2}+2}\,.$$

Proof Remember from (30) that the state of register Q upon successful authentication using key $K=(b,u)$ is,

$$\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}|\mathcal{A}_{\text{ok}}}^{b,u} = \frac{|c_0|^2}{p_{\text{ok}}^{b,u}} |\Psi^n\rangle\langle\Psi^n| + \frac{(1-|c_0|^2)}{p_{\text{ok}}^{b,u}} \Pi_{\text{ok}}^{b,u} \tilde{\rho}_{\mathcal{E}} \Pi_{\text{ok}}^{b,u}\,. \tag{53}$$

Adding register E under our assumption that the entire joint system is in pure state allows to write:

$$\tilde{\rho}_{\mathsf{Q}'\mathsf{Q}\mathsf{E}|\mathcal{A}_{\text{ok}}}^{b,u} = \frac{|c_0|^2}{p_{\text{ok}}^{b,u}} |\Psi^n\rangle\langle\Psi^n| \otimes |e_*\rangle\langle e_*| + \frac{(1-|c_0|^2)}{p_{\text{ok}}^{b,u}} |\widetilde{e_{b,u}}\rangle\langle\widetilde{e_{b,u}}|, \tag{54}$$

for some pure state $|e_*\rangle$ for register E and some unnormalized pure state $|\widetilde{e_{b,u}}\rangle$ for registers $\mathsf{Q}'\mathsf{Q}\mathsf{E}$ such that $p_{\mathcal{E}}^{b,u} = \text{tr}(|\widetilde{e_{b,u}}\rangle\langle\widetilde{e_{b,u}}|) = \text{tr}(\Pi_{\text{ok}}^{b,u}\tilde{\rho}_{\mathcal{E}})$. In order to shorten the notation, let $\tilde{\varrho}_{\mathcal{E}}^{b,u} = |\widetilde{e_{b,u}}\rangle\langle\widetilde{e_{b,u}}|$ and let $\varrho_{\mathcal{E}}^{b,u} := \frac{\tilde{\varrho}_{\mathcal{E}}^{b,u}}{p_{\mathcal{E}}^{b,u}}$ be its normalized version. Notice that from (54) we have for all $x\in\{0,1\}^m$,

$$\begin{aligned}\tilde{\rho}_{\mathsf{E}}^{\text{ok}}(x) &= \frac{|c_0|^2}{p_{\text{ok}}^{b,u}} |e_*\rangle\langle e_*| + \frac{1-|c_0|^2}{p_{\text{ok}}^{b,u}} 2^{-n-m} \sum_{b,u} \text{tr}_{\mathsf{Q}'\mathsf{Q}}(\tilde{\varrho}_{\mathcal{E}}^{b,u}) \\ &= \frac{|c_0|^2}{p_{\text{ok}}^{b,u}} |e_*\rangle\langle e_*| + \frac{1-|c_0|^2}{p_{\text{ok}}^{b,u}} 2^{-n-m} \sum_{b,u} p_{\mathcal{E}}^{b,u} \text{tr}_{\mathsf{Q}'\mathsf{Q}}(\varrho_{\mathcal{E}}^{b,u})\,.\end{aligned}$$

Let us define $\sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}}^* = 2^{-n-m} \sum_{(b,u)\in\{0,1\}^{n+m}} |(b,u)\rangle\langle(b,u)| \otimes |\Psi^n\rangle\langle\Psi^n| \otimes |e_*\rangle\langle e_*|$. We have,

$$\begin{aligned}D(\sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}}^*, \sigma_{K\mathsf{Q}'\mathsf{Q}\mathsf{E}}) = 2^{-n-m-1} \quad \text{tr} \Bigg| &\sum_{b,u} |(b,u)\rangle\langle(b,u)| \\ &\otimes |\Psi^n\rangle\langle\Psi^n| \\ &\otimes \left(\frac{p_{\text{ok}}^{b,u} - |c_0|^2}{p_{\text{ok}}^{b,u}} |e_*\rangle\langle e_*| - \frac{p_{\mathcal{E}}^{b,u}(1-|c_0|^2)\text{tr}_{\mathsf{Q}'\mathsf{Q}}(\varrho_{\mathcal{E}}^{b,u})}{p_{\text{ok}}^{b,u}} \right) \Bigg|.\end{aligned} \tag{55}$$

The trace in (55) is maximized whenever $|e_*\rangle\langle e_*|$ and $\text{tr}_{\mathsf{Q}'\mathsf{Q}}(\varrho_{\mathcal{E}}^{b,u})$ are orthogonal for all (b,u). Using the fact that $p_{\text{ok}}^{b,u} = |c_0|^2 + (1-|c_0|^2)p_{\mathcal{E}}^{b,u}$, we get

$$D(\sigma^*_{KQ'QE}, \sigma_{KQ'QE}) \le 2^{-n-m-1} \sum_{b,u} \frac{2(p^{b,u}_{ok} - |c_0|^2)}{p^{b,u}_{ok}} = 2^{-n-m} \sum_{b,u} \frac{p^{b,u}_{ok} - |c_0|^2}{p^{b,u}_{ok}} \le 2^{-\frac{n-m-2}{2}}, \quad (56)$$

where (56) follows from Lemma 5.3 given the assumption that $p_{ok} \ge 2^{-\frac{n-m}{2}+1}(1 + 2^{-\frac{n-m}{2}+1})$. On the other hand, using a similar argument, we get

$$\begin{aligned} D(\tilde{\rho}_{KQ'QE|\mathcal{A}_{ok}}, \sigma^*_{KQ'QE}) &= \frac{2^{-n-m}}{2} \mathrm{tr} \Bigg| \sum_{(b,u)} |(b,u)\rangle\langle(b,u)| \\ &\otimes \left(\frac{|c_0|^2}{p^{b,u}_{ok}} |\Psi^n\rangle\langle\Psi^n| \otimes |e_*\rangle\langle e_*| + \frac{(1-|c_0|^2)}{p^{b,u}_{ok}} \tilde{\varrho}^{b,u}_{\mathcal{E}} \right) \\ &- \sigma^*_{KQ'QE} \Bigg| = \frac{2^{-n-m}}{2} \mathrm{tr} \Bigg| \sum_{(b,u)} \left(\frac{p^{b,u}_{ok} - |c_0|^2}{p^{b,u}_{ok}} |(b,u)\rangle\langle(b,u)| \right. \\ &\left. \otimes (\varrho^{b,u}_{\mathcal{E}} - |\Psi^n\rangle\langle\Psi^n| \otimes |e_*\rangle\langle e_*|) \right) \Bigg| \\ &\le 2^{-n-m} \sum_{(b,u)} \frac{p^{b,u}_{ok} - |c_0|^2}{p^{b,u}_{ok}} \le 2^{-\frac{n-m-2}{2}}, \end{aligned} \quad (57)$$

where (57) is obtained using the fact that the final trace is maximized when, for each (b,u), $\tilde{\rho}^{b,u}_{\mathcal{E}}$ and $|\Psi^n\rangle\langle\Psi^n|$ are orthogonal. In this case, the trace is no larger than $\sum_{(b,u)} \frac{2(p^{b,u}_{ok} - |c_0|^2)}{p^{b,u}_{ok}}$, which from Lemma 5.3 and the assumption that $p_{ok} \ge 2^{-\frac{n-m}{2}+1}(1 + 2^{-\frac{n-m}{2}+1})$, gives the desired upper bound. The proof of the statement follows using the triangle inequality with (56) and (57),

$$D(\tilde{\rho}_{KQ'QE|\mathcal{A}_{ok}}, \sigma_{KQ'QE}) \le D(\tilde{\rho}_{KQ'QE|\mathcal{A}_{ok}}, \sigma^*_{KQ'QE}) + D(\sigma^*_{KQ'QE}, \sigma_{KQ'QE}) \le 2^{-\frac{n-m}{2}+2}.$$

□

5.5 Security of key-recycling in EPR-$\mathsf{W}_n\mathsf{C}_m$

Theorem 5.1 establishes that, upon successful authentication and provided the secret key is initially uniform, the state shared between Alice, Bob, and the eavesdropper is at negligible distance (i.e. provided p_{ok} is large enough) to the state they would share if no eavesdropping at all occurred. The statistical security of the key-recycling mechanism follows when $\ell(m) = n - m \in \Omega(n)$ as shown in the next theorem.

Theorem 5.2 *Assume that the secret key K used by Alice and Bob for one transmission of message x using* EPR-$\mathsf{W}_n\mathsf{C}_m$ *is initially uniform. Then, for all adversary strategies for which $p_{ok} \ge 2^{-\frac{n-m}{2}+1}(1 + 2^{-\frac{n-m}{2}+1})$, we have that:*

$$d(K|\tilde{\rho}^{ok}_{E}(x)) \le 2^{-\frac{n-m}{2}+2}.$$

Proof As usual, we denote by $\sigma_{KE} := \mathrm{tr}_{Q'Q}(\sigma_{KQ'QE})$ the state held by the eavesdropper together with the secret key shared by Alice and Bob when no active eavesdropping occurred and the secret key is initially uniform. We have,

$$\begin{aligned} d(K|\tilde{\rho}^{ok}_{E}(x)) &:= D(\tilde{\rho}_{KE|\mathcal{A}_{ok}}, \mathbb{I}_{n+m} \otimes \tilde{\rho}^{ok}_{E}(x)) \\ &\le D(\tilde{\rho}_{KE|\mathcal{A}_{ok}}, \sigma_{KE}) + D(\sigma_{KE}, \mathbb{I}_{n+m} \otimes \tilde{\rho}^{ok}_{E}(x)) \end{aligned} \quad (58)$$

$$= D(\tilde{\rho}_{KE|\mathcal{A}_{ok}}, \sigma_{KE}) \quad (59)$$

$$\le D(\tilde{\rho}_{KQ'QE|\mathcal{A}_{ok}}, \sigma_{KQ'QE}) \quad (60)$$

$$\le 2^{-\frac{n-m}{2}+2}, \quad (61)$$

where inequality (58) comes from the triangle inequality, (59) follows since $D(\sigma_{KE}, \mathbb{I}_{n+m} \otimes \tilde{\rho}^{ok}_{E}(x)) = 0$ when the secret key is initially uniform, and (60) comes from the fact that tracing out cannot increase the distance between two states. Finally, (61) is obtained from Theorem 5.1 given that $p_{ok} \ge 2^{-\frac{n-m}{2}+1}(1 + 2^{-\frac{n-m}{2}+1})$. □

Theorem 5.2 establishes the security of the key-recycling mechanism when authentication succeeds. The entire key can be re-used since, from the point of view of the eavesdropper, the secret key is indistinguishable from uniform even after the transmission of the cipherstate.

5.6 Back to $\mathsf{W}_n\mathsf{C}_m$

We now show that Theorem 5.2 also applies to $\mathsf{W}_n\mathsf{C}_m$. Similarly to other Shor–Preskill arguments (Shor and Preskill 2000; Barnum et al. 2002; Oppenheim and Horodecki 2003), we transform EPR-$\mathsf{W}_n\mathsf{C}_m$ into $\mathsf{W}_n\mathsf{C}_m$ by simple modifications leaving the adversary's view unchanged. It goes as follows.

In Step 4 of EPR-$\mathsf{W}_n\mathsf{C}_m$, Alice measures her part of the entangled pair in order to extract $c \in \{0,1\}^n$. Instead, she could have measured already in Step 1 since the measurement commutes with everything the adversary and Bob do up to Step 4. Measuring half the EPR-pairs immediately after creating them is equivalent to Alice preparing $c \in_R \{0,1\}^n$ before sending $|v^{(b)}_c\rangle$ in Step 2.

Instead of picking $c \in_R \{0,1\}^n$ in Step 1, Alice could choose $z \in_R \{0,1\}^n$ at random before sending $|v^{(b)}_{z \oplus (x, h_u(x))}\rangle$

to Bob. All these modifications change nothing to the adversary's view.

Now, sending z through the private and authenticated classical channel in Step 5 becomes unnecessary if Alice and Bob share z before the start of the protocol (thus making z part of the key). We have now removed the need for the private and authenticated classical channel.

The resulting protocol is such that Bob first acknowledges receiving the cipher, then measures it, and finally replies with either accept or reject. The acknowledgment of Step 3 is unnecessary and can safely be postponed to Bob's announcement in Step 6. The EPR-$\mathsf{W}_n\mathsf{C}_m$-cipher has now been fully converted into the $\mathsf{W}_n\mathsf{C}_m$-cipher without interfering with the eavesdropper's view. It follows directly that Theorem 5.2 also applies to $\mathsf{W}_n\mathsf{C}_m$.

Theorem 5.2 shows that one use of the $\mathsf{W}_n\mathsf{C}_m$-cipher leaves the secret key at negligible distance to uniform when it was initially uniform. Our main result follows from Lemma 5.1 and Theorem 5.2:

Theorem 5.3 (Main Result) The $\mathsf{W}_n\mathsf{C}_m$*-cipher, with* $n = m + \ell(m)$, *is a statistically secure* QKRS *for any* $\ell(m) \in \Omega(n)$.

The discussion of Sect. 3.1 allows to conclude that the $\mathsf{W}_n\mathsf{C}_m$–cipher can be composed a super-polynomial number of times provided some new key material is injected each time authentication fails. No new key material whatsoever has to be introduced as long as the authentication succeeds and the scheme is used polynomially many times.

6 Conclusion and open questions

We have shown that the $\mathsf{W}_n\mathsf{C}_m$-cipher is an almost optimal key-recycling cipher with one-bit feedback. There are many possible improvements of our scheme. In this paper, we assume noiseless quantum communication. This is of course an unrealistic assumption. Our scheme can easily be made resistant to noise by encoding the quantum cipher using a quantum error-correcting code. Since a quantum error-correcting code is also a secret-sharing (Cleve et al. 1999), it can be shown that when authentication succeeds almost no information about the cipherstate is available to the eavesdropper. On the other hand, if the eavesdropper gains information about the cipherstate then authentication will fail similarly to the case where no error-correction is used.

It would be interesting to show that, when authentication fails, the key-recycling bound of Theorem 4.1 can be improved to $t = n - m$ (instead of $n - m + 2$) as for classical schemes. Remember that the $\mathsf{W}_n\mathsf{C}_m$–cipher is slightly sub-optimal since $t = n - m - \ell(m)$ and $\ell(m) \in \Omega(n)$. However, in order to have statistically secure key-recycling schemes it could be the case that t must satisfy $t/(n-m) \in \Omega(n)$. It would be interesting to know whether any key-recycling mechanism that recycles t bits with $t/(n-m) \in o(n)$ when authentication fails can have an optimal statistically secure key-recycling mechanism when authentication succeeds. If the answer was no then our scheme could be optimal. It seems difficult to have both $t = n - m - o(n)$ and $s = n$ in any secure key-recycling scheme since, in order for $s = n$, one seems to need adding redundancy to the plaintext before encrypting both the plaintext and the redundancy to resist known-plaintext attacks.

It is also possible to allow for more key-recycling mechanisms associated to different output values for the authentication process. Such a generalized scheme would allow to recycle key-material as a function of the adversary's available information but would require more than one-bit feedback.

Acknowledgments Thomas Brochmann Pedersen was partially funded by European projects PROSECCO and SECOQC. Louis Salvail was supported by Canada's NSERC and the QuantumWorks Network.

References

Advances in Cryptology—EUROCRYPT '04 (2004) vol. 3027 of Lecture Notes in Computer Science, Springer, New York

Ambainis A, Mosca M, Tapp A, de Wolf R (2000) Private quantum channels. In: 41st annual IEEE symposium on foundations of computer science (FOCS), pp 547–553

Barnum H, Crépeau C, Gottesman D, Smith A, Tapp A (2002) Authentication of quantum messages. In: 43rd annual IEEE symposium on foundations of computer science (FOCS), pp 449–458

Ben-Or M, Horodecki M, Leung DW, Mayers D, Oppenheim J (2005) The universal composable security of quantum key distribution. In: Theory of cryptography conference (TCC) (Theory of Cryptography Conference (TCC) 2005), pp 386–406

Bennett CH, Brassard G, Breidbart S (1982) Quantum cryptography II: How to re-use a one-time pad safely even if P = NP.

Bhatia R (1997) Matrix analysis, graduate texts in mathematics. Springer, New York

Boykin PO, Roychowdhury V (2003) Optimal encryption of quantum bits. Phys Rev A 67(4):042317

Carter JL, Wegman MN (1977) Universal classes of hash functions. In: 9th annual ACM symposium on theory of computing (STOC), pp 106–112

Cleve R, Gottesman D, Lo H-K (1999) How to share a quantum secret. Phys Rev Lett 83(3):648–651

Damgård IB, Pedersen TB, Salvail L (2004) On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. In: Advances in Cryptology–EUROCRYPT '04 (Advances in Cryptology—EUROCRYPT '04 2004), pp 91–108

Damgård IB, Pedersen TB, Salvail L (2005) A quantum cipher with near optimal key-recycling. In: Advances in Cryptology–CRYPTO '05', vol. 3621 of Lecture Notes in Computer Science, Springer, New York, pp 494–510

Dziembowski S, Maurer UM (2004) On generating the initial key in the bounded-storage model. In: Advances in Cryptology–EUROCRYPT '04 (Advances in Cryptology—EUROCRYPT '04 2004), pp 126–137

Hayden P, Leung D, Mayers D (2011) Authentication of quantum messages. Imaging Appl Opt

Hayden P, Leung D, Mayers D (2004) Authentication of quantum messages. J Cryptol 17:386–406

Lawrence J, Brukner Č (2002) Mutually unbiased binary observable sets on N qubits. Phys Rev A 65(3):5

Leung DW (2002) Quantum vernam cipher. Quantum Inf Comput 2(1):14–34

Lu C-J (2004) Encryption against storage-bounded adversaries from on-line strong extractors. J Cryptol 17:27–42

Mandayam P, Balachandran N, Wehner S (2010) A transform of complementary aspects with applications to entropic uncertainty relations. J Math Phys 51(8):082201

Nielsen MA, Chuang IL (2000) Quantum computation and quantum information. Cambridge university press, Cambridge

Oppenheim J, Horodecki M (2003) How to reuse a one-time pad and other notes on authentication, encryption and protection of quantum information. http://arxiv.org/abs/quant-ph/0306161

Renner R, König R (2005) Universally composable privacy amplification against quantum adversaries. In: Theory of cryptography conference (TCC) (Theory of Cryptography Conference (TCC) 2005), pp 407–425

Shor PW, Preskill J (2000) Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett 85(2):441–444

Theory of Cryptography Conference (TCC) (2005) vol. 3378 of Lecture Notes in Computer Science, Springer, New York

Vadhan SP (2004) On constructing locally computable extractors and cryptosystems in the bounded storage model. J Cryptol 17:43–77

Wootters WK, Fields BD (1989) Optimal state-determination by mutually unbiased measurements. Ann Phys 191(2):363–381

Wootters WK, Sussman DM (2007) Discrete phase space and minimum-uncertainty states. In: Proceedings of the eighth international conference on quantum communication, measurement and computing, pp 296–274