Security proof for Quantum Key Recycling with noise

Daan Leermakers and Boris Škorić
d.leermakers.1@tue.nl, b.skoric@tue.nl

Abstract

Quantum Key Recycling aims to re-use the keys employed in quantum encryption and quantum authentication schemes. We consider QKR protocols where classical information is embedded in qubit states, as opposed to high-dimensional qudits. A security proof was given by Fehr and Salvail [1] in the case where there is practically no noise. A scheme for the noisy case was proposed by Škorić and de Vries [2], based on eight-state encoding, which reduces leakage. However, a security proof was not given.

In this paper we introduce a small protocol modification to [2] and provide a security proof. Our proof is based on a bound on the trace distance between the real quantum state of the system and a state in which the keys are completely secure. We determine how much privacy amplification is needed as a function of the tolerated bit error rate. It turns out that less privacy amplification is needed than suggested by previous results.

1 Introduction

1.1 Quantum Key Recycling

Quantum cryptography uses the properties of quantum physics to achieve security feats that are impossible with classical communication. Best known is Quantum Key Distribution (QKD), first described in the famous BB84 paper [3]. QKD establishes a random secret key known only to Alice and Bob, and exploits the no-cloning theorem for unknown quantum states [4] to detect any manipulation of the quantum states. Already two years before the invention of QKD, the possibility of Quantum Key Recycling (QKR) was considered [5]. Let Alice and Bob encrypt classical data as quantum states, using a classical key to determine the basis in which the data is encoded. If they do not detect any manipulation of the quantum states, then Eve has learned almost nothing about the encryption key, and hence it is safe for Alice and Bob to re-use the key. After the discovery of QKD, interest in QKR was practically nonexistent for a long time, despite the benefits that QKR can offer for communication complexity. QKR received some attention again in 2003 when Gottesman [6] proposed an Unclonable Encryption scheme with partially re-usable keys. In 2005 Damgård, Pedersen and Salvail introduced a scheme that allows for complete key recycling, based on mutually unbiased bases in a high-dimensional Hilbert space [7, 8]. Though elegant, their scheme unfortunately needs a quantum computer for encryption and decryption. In 2017 Fehr and Salvail [1] introduced a qubit-based QKR scheme (similar to [5]) that does not need a quantum computer, and they were able to prove its security in the regime of extremely low noise. Škorić and de Vries [2] proposed a variant with 8-state encoding, which drastically reduces the need for privacy amplification. It is meant to operate at the same noise levels as QKD, but the security was not proven. Attacks on the qubit-based QKR schemes of [1, 2] were studied in [9], but that did not yield a security proof.

1.2 Contributions and outline

We investigate qubit-based Quantum Key Recycling, taking an 'engineering' point of view: we do not aim for complete key re-use, but rather for a high ratio of message length versus expended key bits.

- We introduce a small modification in the QKR protocol of Škorić and de Vries [2]. We impose the condition that the one-time MAC function has key length equal to the tag length.
- We give a security proof. We use the EPR formulation of the protocol. First we consider attacks in which Eve collects quantum side information from one EPR pair at a time; then we apply the post-selection method in order to get security in the case of general attacks.
- The required amount of privacy amplification depends on the bit error rate β tolerated by the error-correcting code. When n qubits are sent, the amount of privacy amplification in the case of 8-state encoding is $2n \log[\sqrt{(1-\beta)(1-\frac{3}{2}\beta)} + \sqrt{\frac{1}{2}\beta(1-\beta)} + \beta\sqrt{2}]$ bits (asymptotically). This result is more favourable than the min-entropy analysis in [9] and straightforward generalisations of [1] to the noisy case.

The outline of the paper is as follows. In the preliminaries section we introduce notation; we briefly review proof techniques and methods for embedding classical bits in qubits, and we summarise known results regarding Eve's optimal extraction of information from a qubit into a four-dimensional ancilla state. In Section 3 we discuss the QKR protocol. Section 4 states the main theorems. The proofs are given in Sections 6 and 7. Section 5 contains a discussion of parameter choices, rates, comparison to the literature, handling of erasures, and suggestions for future work.

2 Preliminaries

2.1 Notation and terminology

Classical Random Variables (RVs) are denoted with capital letters, and their realisations with lowercase letters. The probability that a RV X takes value x is written as $\Pr[X=x]$. The expectation with respect to RV X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X=x] f(x)$. Sets are denoted in calligraphic font. We write $[n]$ for the set $\{1,\ldots,n\}$. For a string x and a set of indices $\mathcal{I}$ the notation $x_\mathcal{I}$ means the restriction of x to the indices in $\mathcal{I}$. The notation 'log' stands for the logarithm with base 2. The notation h stands for the binary entropy function $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. Bitwise XOR of binary strings is written as '$\oplus$'. The Kronecker delta is denoted as δ_{ab}. The inverse of a bit $b\in\{0,1\}$ is written as $\bar{b} = 1-b$. We will speak about 'the bit error rate β of a quantum channel'. This is defined as the probability that a classical bit g, sent by Alice embedded in a qubit, arrives at Bob's side as $\bar{g}$.
For quantum states we use Dirac notation, with the standard qubit basis states $|0\rangle$ and $|1\rangle$ represented as $\binom{1}{0}$ and $\binom{0}{1}$ respectively. The Pauli matrices are denoted as $\sigma_x, \sigma_y, \sigma_z$, and we write $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. The standard basis is the eigenbasis of σ_z, with $|0\rangle$ in the positive z-direction. We write $\mathbb{1}$ for the identity matrix. The notation 'tr' stands for trace. The Hermitian conjugate of an operator A is written as $A^\dagger$. The complex conjugate of z is denoted as z^*. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. The trace distance between matrices ρ and σ is denoted as $\delta(\rho;\sigma) = \frac{1}{2}||\rho-\sigma||_1$. It is a

generalisation of the statistical distance and represents the maximum possible advantage one can have in distinguishing ρ from σ.
Consider a uniform classical variable X and a mixed state ρ_X that depends on X. The combined classical-quantum state is $\rho^{\mathrm{XE}} = \mathbb{E}_x |x\rangle\langle x| \otimes \rho_x^{\mathrm{E}}$. The states of the sub-systems 'X' and 'E' are obtained by tracing out one subspace, and are given by $\rho^{\mathrm{X}} = \mathbb{E}_x |x\rangle\langle x|$ and $\rho^{\mathrm{E}} = \mathbb{E}_x \rho_x^{\mathrm{E}}$ respectively. The security of the variable X, given that Eve holds the 'E' subsystem, can be expressed in terms of a trace distance as follows [10],

$$d(X|\mathrm{E}) \stackrel{\mathrm{def}}{=} \delta\Big(\rho^{\mathrm{XE}} \; ; \;\; \rho^{\mathrm{X}} \otimes \rho^{\mathrm{E}}\Big) \tag{1}$$

i.e. the distance between the true classical-quantum state and a state in which the quantum state is decoupled from X. X is said to be ε-secure with respect to ρ if $d(X|\rho) \leq \varepsilon$. When this is the case, it can be considered that X is 'ideal' except with probability ε.
A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{T}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [11] if for all distinct pairs $x, x' \in \mathcal{X}$ and all pairs $y, y' \in \mathcal{T}$ it holds that $\Pr_{h \in H}[h(x) = y \wedge h(x') = y'] = |\mathcal{T}|^{-2}$. Here the probability is over random $h \in H$. Pairwise independence can be achieved with a hash family of size $|H| = |\mathcal{X}|$.

2.2 QKR proof structure

The protocol (see Section 3) has three basic steps. (i) Alice sends quantum states and classical data to Bob. (ii) Bob responds with a decision bit $c \in \{Accept, Reject\}$. (iii) In case of Accept, the key material K is re-used; in case of Reject, the key material is refreshed from K to K'.
We will use a recursive proof structure as in [1]. The starting situation is an 'ideal' state $\rho^{(0)} = \rho^{\mathrm{K}} \otimes \rho^{\mathrm{E}}$, in which the key material K is decoupled from Eve's state. After one round of QKR the state has evolved to $\rho_c^{(1)}$; this includes actions by Eve as well as potential key updates by Alice and Bob. Accept happens with probability P_{acc} and leads to a state $\rho_{\mathrm{acc}}^{(1)} = \mathbb{E}_k |k\rangle\langle k| \otimes \tilde{\rho}_k^{\mathrm{E}}$ in which Eve has potentially gained knowledge about K; Reject happens with probability P_{rej} and yields a state $\rho_{\mathrm{rej}}^{(1)} = \tilde{\rho}^{\mathrm{K}} \otimes \tilde{\rho}^{\mathrm{E}}$ which has factorised form due to the key refreshment.
The notion of secure key re-use is expressed as follows. Under known-plaintext conditions, a bound is derived on the distance between $\rho_c^{(1)}$ and the ideal state $\rho^{(0)}$, given that Eve observes the decision bit: $P_{\mathrm{acc}} \|\rho_{\mathrm{acc}}^{(1)} - \rho^{(0)}\|_1 + P_{\mathrm{rej}} \|\rho_{\mathrm{rej}}^{(1)} - \rho^{(0)}\|_1 \leq \varepsilon$, which is equivalent to $P_{\mathrm{acc}} \|\rho_{\mathrm{acc}}^{(1)} - \rho^{(0)}\|_1 \leq \varepsilon$.
By induction $\mathbb{E}_{c_1 \cdots c_N} \|\rho_{c_1 \cdots c_N}^{(N)} - \rho^{(0)}\|_1 \leq N\varepsilon$, where $\rho^{(N)}$ is the state after N rounds. This can be seen as follows. After two rounds the state is $\rho_{c_1 c_2}^{(2)}$, and the security quantity of interest is $\mathbb{E}_{c_1 c_2} \|\rho_{c_1 c_2}^{(2)} - \rho^{(0)}\|_1 = P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc,acc}}^{(2)} - \rho^{(0)}\|_1 + P_{\mathrm{rej}} P_{\mathrm{acc}} \|\rho_{\mathrm{rej,acc}}^{(2)} - \rho^{(0)}\|_1 = P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc,acc}}^{(2)} - \rho^{(0)}\|_1 + P_{\mathrm{rej}} P_{\mathrm{acc}} \|\rho_{\mathrm{acc}}^{(1)} - \rho^{(0)}\|_1 \leq P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc,acc}}^{(2)} - \rho^{(0)}\|_1 + P_{\mathrm{rej}} \varepsilon$. Using the triangle inequality the first term is upperbounded as $P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc,acc}}^{(2)} - \rho^{(0)}\|_1 \leq P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc,acc}}^{(2)} - \rho_{\mathrm{acc}}^{(1)}\|_1 + P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc}}^{(1)} - \rho^{(0)}\|_1 \leq P_{\mathrm{acc}}^2 \|\rho_{\mathrm{acc,acc}}^{(2)} - \rho_{\mathrm{acc}}^{(1)}\|_1 + P_{\mathrm{acc}} \varepsilon$. Finally it is used that the mapping from $\rho^{(i)}$ to $\rho^{(i+1)}$ is a CPTP map, which cannot increase distance. Hence $\|\rho_{\mathrm{acc,acc}}^{(2)} - \rho_{\mathrm{acc}}^{(1)}\|_1 \leq \|\rho_{\mathrm{acc}}^{(1)} - \rho^{(0)}\|_1$. It follows that $\mathbb{E}_{c_1 c_2} \|\rho_{c_1 c_2}^{(2)} - \rho^{(0)}\|_1 \leq 2\varepsilon$.

2.3 Post-selection

In a *collective attack* Eve acts on individual qudits. This is not the most general attack. For protocols that obey permutation symmetry, a post-selection argument [12] can be used

to show that ε-security against collective attacks implies ε'-security against general attacks, with $\varepsilon' = \varepsilon(n+1)^{d^4-1}$, where d is the dimension of the qudit space ($d = 2$ for qubits). Hence, by paying a modest price in terms of privacy amplification, e.g. changing the usual privacy amplification term $2\log\frac{1}{\varepsilon}$ to $2\log\frac{1}{\varepsilon} + 2(d^4-1)\log(n+1)$, one can 'buy' security against general attacks.

2.4 Encoding a classical bit in a qubit

We briefly review methods for embedding a classical bit $g \in \{0,1\}$ into a qubit state. The standard basis is $|0\rangle, |1\rangle$ with $|0\rangle$ the positive z-direction on the Bloch sphere. The set of bases used is denoted as $\mathcal{B}$, and a basis choice as $b \in \mathcal{B}$. The encoding of bit value g in basis b is written as $|\psi_{bg}\rangle$. In BB84 encoding we write $\mathcal{B} = \{0,1\}$, with $|\psi_{00}\rangle = |0\rangle$, $|\psi_{01}\rangle = |1\rangle$, $|\psi_{10}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|\psi_{11}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. In six-state encoding [13] the vectors are $\pm x$, $\pm y$, $\pm z$ on the Bloch sphere. We have $\mathcal{B} = \{0,1,2\}$ and

$$\begin{aligned} |\psi_{00}\rangle = |0\rangle \quad ; \quad |\psi_{01}\rangle = |1\rangle \qquad ; \qquad |\psi_{10}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad ; \quad |\psi_{11}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ |\psi_{20}\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \qquad ; \qquad |\psi_{21}\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \end{aligned} \tag{2}$$

For 8-state encoding [2] we have $\mathcal{B} = \{0,1,2,3\}$ and the eight states are the corner points of a cube on the Bloch sphere. We write $b = 2u + w$, with $u, w \in \{0,1\}$. The states are

$$|\psi_{uwg}\rangle = (-1)^{gu}\left[(-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g \oplus w\rangle + (-1)^u(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|\overline{g \oplus w}\rangle\right]. \tag{3}$$

The angle α is defined as $\cos\alpha = 1/\sqrt{3}$. For given g, the four states $|\psi_{uwg}\rangle$ are the Quantum One-Time Pad (QOTP) encryptions [14, 15, 16] of $|\psi_{00g}\rangle$. The 'plaintext' states $|\psi_{000}\rangle$, $|\psi_{001}\rangle$ correspond to the vectors $\pm(1,1,1)/\sqrt{3}$ on the Bloch sphere.

2.5 Eve's ancilla state

Attacks on QKR were studied in some detail in [9]. They formulated an EPR version of qubit-based QKR protocol. Instead of creating $|\psi_{b_i x_i}\rangle$ and sending it to Bob, Alice performs a measurement on one half an EPR singlet state (using basis b_i) while the other half goes to Bob. Eve may manipulate the EPR state. Any manipulation turns the pure EPR state into a mixed state. The noise symmetrisation technique of [17] was applied to simplify the state. If Eve's actions induce bit error probability β (defined as a bit mismatch in x_i between Alice and Bob), then this corresponds to a state of the AB subsystem of the form $\tilde{\rho}^{\mathrm{AB}} = (1-\frac{3}{2}\beta)|\Psi^-\rangle\langle\Psi^-| + \frac{\beta}{2}\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+|\right)$, where $|\Psi^\pm\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$ and $|\Phi^\pm\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$ denote the Bell basis states.[1] Eve's state is obtained by purifying $\tilde{\rho}^{\mathrm{AB}}$. The pure state is $|\Psi^{\mathrm{ABE}}\rangle = \sqrt{1-\frac{3}{2}\beta}|\Psi^-\rangle \otimes |m_0\rangle + \sqrt{\frac{\beta}{2}}\left(-|\Phi^-\rangle \otimes |m_1\rangle + i|\Psi^+\rangle \otimes |m_2\rangle + |\Phi^+\rangle \otimes |m_3\rangle\right)$, where $|m_i\rangle$ is some orthonormal basis in Eve's four-dimensional ancilla space. Let $\boldsymbol{v}$ be a 3-component vector on the Bloch sphere describing the '0' bit value in a certain basis. Let x be the bit value that Alice measures, and y Bob's bit value. (In the noiseless case we have

[1] For 4-state QKR an extra ingredient is needed to arrive at this expression: the use of decoy/test states so as to probe more than a circle on the Bloch sphere. This allows us to treat 4, 6 and 8-state encoding on an equal footing; the main theorem of this paper then also applies to 4-state encoding. (If the decoy/test states are not used in 4-state QKR, Eve has a more powerful attack and the ancilla states ω_x^b are modified.)

$y = \bar{x}$ because of the anti-correlation in the singlet state.) One of the results of [9] is an expression for Eve's mixed ancilla state when $\boldsymbol{v}, x, y$ are fixed,

$$\sigma_{xy}^{\boldsymbol{v}} \stackrel{\text{def}}{=} |E_{xy}^{\boldsymbol{v}}\rangle\langle E_{xy}^{\boldsymbol{v}}|. \tag{4}$$

$$\begin{aligned}
|E_{01}^{\boldsymbol{v}}\rangle &= \frac{1}{\sqrt{1-\beta}}\left[\sqrt{1-\tfrac{3}{2}\beta}|m_0\rangle + \sqrt{\tfrac{\beta}{2}}\left(v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle\right)\right] \\
|E_{10}^{\boldsymbol{v}}\rangle &= \frac{1}{\sqrt{1-\beta}}\left[\sqrt{1-\tfrac{3}{2}\beta}|m_0\rangle - \sqrt{\tfrac{\beta}{2}}\left(v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle\right)\right] \\
|E_{00}^{\boldsymbol{v}}\rangle &= \frac{1}{\sqrt{2(1-v_z^2)}}\left[(-v_xv_z - iv_y)|m_1\rangle + (-v_yv_z + iv_x)|m_2\rangle + (1-v_z^2)|m_3\rangle\right] \\
|E_{11}^{\boldsymbol{v}}\rangle &= \frac{1}{\sqrt{2(1-v_z^2)}}\left[(-v_xv_z + iv_y)|m_1\rangle + (-v_yv_z - iv_x)|m_2\rangle + (1-v_z^2)|m_3\rangle\right].
\end{aligned} \tag{5}$$

The E-vectors are not all orthogonal. We have $\langle E_{01}^{\boldsymbol{v}}|E_{10}^{\boldsymbol{v}}\rangle = \frac{1-2\beta}{1-\beta}$. (The rest of the inner products are zero.) It holds that $|\frac{-v_xv_z - iv_y}{\sqrt{1-v_z^2}}|^2 = 1 - v_x^2$ and $|\frac{-v_yv_z + iv_x}{\sqrt{1-v_z^2}}|^2 = 1 - v_y^2$. We have $|E_{10}^{\boldsymbol{v}}\rangle = |E_{01}^{-\boldsymbol{v}}\rangle$ and $|E_{11}^{\boldsymbol{v}}\rangle = |E_{00}^{-\boldsymbol{v}}\rangle$.
Eve is primarily interested in learning x. At given b, x Eve's state (averaged over y) is

$$\omega_x^b(\beta) \stackrel{\text{def}}{=} (1-\beta)\sigma_{x\bar{x}}^{\boldsymbol{v}(b)} + \beta\sigma_{xx}^{\boldsymbol{v}(b)} = (1-\beta)|E_{x\bar{x}}^{\boldsymbol{v}(b)}\rangle\langle E_{x\bar{x}}^{\boldsymbol{v}(b)}| + \beta|E_{xx}^{\boldsymbol{v}(b)}\rangle\langle E_{xx}^{\boldsymbol{v}(b)}|. \tag{6}$$

3 The QKR protocol

In this paper we consider the QKR scheme #2 proposed in [2], which is a slightly modified version of the QEMC* scheme of Fehr and Salvail [1]. This protocol can be executed with 4-state, 6-state or 8-state encoding, where 8-state has the advantage that it needs less Privacy Amplification [9]. We introduce a small change in the protocol:

- For efficiency reasons we demand that the one-time MAC function has a key size that equals the tag size.[2]

The key material shared between Alice and Bob consists of four parts: a basis sequence $b \in \mathcal{B}^n$, a MAC key $k_{\text{MAC}} \in \{0,1\}^\lambda$, an extractor key[3] $u \in \mathcal{U}$, and a classical OTP $k_{\text{SS}} \in \{0,1\}^a$ for protecting the secure sketch. The plaintext is $\mu \in \{0,1\}^\ell$.
Alice and Bob have agreed on a pairwise independent hash function $\texttt{Ext} : \mathcal{U}\times\{0,1\}^n \to \{0,1\}^\ell$, a MAC function $M : \{0,1\}^\lambda \times \{0,1\}^{n+\ell+a} \to \{0,1\}^\lambda$, a linear error-correcting code with syndrome function $S : \{0,1\}^n \to \{0,1\}^a$, and a Secure Sketch that uses this error-correcting code. The basis set $\mathcal{B}$, the functions $\texttt{Ext}, M, S$, and the Secure Sketch algorithm are publicly known.
Encryption
Alice performs the following steps. Generate random $x \in \{0,1\}^n$. Compute $s = k_{\text{SS}} \oplus S(x)$ and $z = \texttt{Ext}(u, x)$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $t = M(k_{\text{MAC}}, x||c||s)$.

[2] Alternatively, it is an arbitrary information-theoretically secure MAC and the MAC key is be re-used indefinitely; but then the tag has to be one-time padded and the pad has to be refreshed in every round. This construction leads to the same amount of key expenditure and involves a few more operations.

[3] The extractor key was not mentioned explicitly in [2].

Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_{b_i x_i}\rangle$ according to Section 2.4. Send $|\Psi\rangle$, s, c, t to Bob.

Decryption

Bob receives $|\Psi'\rangle$, s', c', t'. He performs the following steps. Measure $|\Psi'\rangle$ in the b-basis. This yields $x' \in \{0,1\}^n$. Recover $\hat{x}$ from x' and $k_{\mathrm{SS}} \oplus s'$ (by the reconstruction procedure of the Secure Sketch). Compute $\hat{z} = \mathtt{Ext}(u, \hat{x})$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if the Secure Sketch reconstruction succeeded and $t' = M(k_{\mathrm{MAC}}, \hat{x}||c'||s')$. Communicate Accept/Reject to Alice (publicly but with authentication).

Key update

Alice and Bob perform the following actions. If Bob Accepts, replace k_{SS} and k_{MAC}. If Bob Rejects, replace $k_{\mathrm{SS}}, k_{\mathrm{MAC}}, b, u$.

See Section 5.1 for a discussion of the balance between message length and key expenditure.

4 Main result

4.1 Attacker model and proof method

The attacker model is the one used in most works on QKD. Eve is able to manipulate the classical channel and the quantum channel between Alice and Bob in any way. Eve has no access to the private computations taking place in Alice and Bob's devices. Eve has unbounded (quantum) computation power and unbounded quantum memory.

First we consider attacks where Eve entangles her own quantum system with individual EPR pairs one at a time. Eve is allowed to postpone all measurements. For this limited class of attacks we derive a bound (Theorem 4.2) on the product $P_{\mathrm{acc}} \cdot \|\rho^{(1)} - \rho^{(0)}\|_1$ as explained in Section 2.2. Finally we invoke post-selection to extend the validity of the security proof to general attacks.

4.2 The result

Alice and Bob's shared key material consists of k_{SS}, k_{MAC}, b and u. The only keys open to attack are b and u, since k_{SS} and k_{MAC} get discarded after each round. Eve's classical side information consists of s (OTP'ed syndrome), t (authentication tag), and the ciphertext $c = z \oplus \mu$. The s and t carry no information about b and u. We assume that Eve knows the plaintext μ; this implies that she knows z.

Eve's quantum side information consists of her ancilla particles which have interacted with the EPR pairs. The state of the ancillas depends on x and b. Since $z = \mathtt{Ext}(u, x)$ and we are interested only in the coupling between Eve's state and the keys u, b, we will keep track only of z, u and b. After one accepted QKR round the joint state of the key material and Eve's system (at fixed z) is given by

$$\rho_z^{\mathrm{UBE}} = \mathbb{E}_{ub} |ub\rangle\langle ub| \otimes \rho_{zub}^{\mathrm{E}}, \tag{7}$$

where the states $|ub\rangle$ form an orthonormal basis for the classical variables u, b. We define $\rho_z^{\mathrm{E}} = \mathbb{E}_{ub} \rho_{zub}^{\mathrm{E}}$. Our main result puts an upper bound on the distance between the actual state and the 'ideal' state in which Eve has no information about U, B.

Theorem 4.1 *Let the function f be defined as $f(\beta) = \sqrt{(1-\beta)(1-\frac{3}{2}\beta)} + \sqrt{\frac{1}{2}\beta(1-\beta)} + \beta\sqrt{2}$. Let Eve know z and create ancilla states for each EPR pair individually, as specified*

in Section 2.5, under the constraint that she causes average bit error rate $\gamma \in [0, \frac{1}{2})$. Let Bob accept. Then it holds that

$$\mathbb{E}_z \|\rho_z^{\mathrm{UBE}} - \rho^{\mathrm{UB}} \otimes \rho_z^{\mathrm{E}}\|_1 < \sqrt{2^{\ell - n + 2n \log f(\gamma)}}. \tag{8}$$

The proof is given in Section 6.

Theorem 4.2 *Consider the same setting as in Theorem 4.1. Let σ be a security parameter. Let the length ℓ be chosen as*

$$\ell = n - 2n \log f(\beta) - 2\xi, \tag{9}$$

$$\xi \geq \min\left(\frac{f'(\beta)}{f(\beta)} \Big[\sigma + \sqrt{\sigma^2 + n \tfrac{2}{\ln 2} \beta \sigma} \Big], \ \sqrt{\frac{n\sigma}{\ln 2}} + \sigma \cdot 2\sqrt{2} \right) \tag{10}$$

where β is the bit error rate that the scheme is designed to resist. Let $P_{\text{re-use}}$ be the probability that Alice receives a decision bit with the value 'Accept'. Then it holds that

$$P_{\text{re-use}} \mathbb{E}_z \|\rho_z^{\mathrm{UBE}} - \rho^{\mathrm{UB}} \otimes \rho_z^{\mathrm{E}}\|_1 \leq 2 \cdot 2^{-\lambda} + 2^{-\sigma}. \tag{11}$$

The proof is given in Section 7.
Note that ξ scales as $\sqrt{n}$ for large n.

- For 8-state encoding, the result (11) suffices to prove the security of the protocol. (The Quantum One Time Pad protects the x perfectly as long as B is uniform.) See Section 2.2. Theorem 4.2 tells us that ℓ must be set smaller than approximately $n[1 - 2\log f(\beta)]$. Asymptotically ($n \gg 1$) this yields a balance of {message length minus key expenditure} that scales as $n[1 - 2\log f(\beta) - h(\beta)]$. See Section 5.1. This balance is positive up to $\beta \approx 0.09$, i.e. up to this noise level it makes sense to use the QKR protocol.
- In the case of 4-state and 6-state encoding, Eve has additional attacks. She may steal all the qubits (causing a Reject) and extract partial information about x from the stolen qubits. This was called the 'M1 attack' in [9]. This attack has to be countered by applying a proper amount of Privacy Amplification, i.e. choosing the correct value for the message length ℓ. Expressed in terms of min-entropy loss[4], 4-state encoding leaks $1 - \log(\cos\frac{\pi}{8})^{-2} \approx 0.77$ bits per qubit; 6-state encoding leaks $1 - \log(\cos\frac{\alpha}{2})^{-2} \approx 0.66$ bits per qubit, with α as defined in Section 2.4. This leakage does not depend on β. It exists already at $\beta = 0$.

As explained in Section 2.3, by invoking post-selection we can 'buy' security against general attacks by reducing the message length ℓ a bit. The bound (8) changes by a factor $(n+1)^{15}$, which can be compensated by shrinking ℓ from (9) to

$$\ell = n - 2n \log f(\beta) - 2\xi - 30 \log(n+1). \tag{12}$$

5 Discussion

5.1 QKR rate; Choosing the parameter values

We want to characterize the performance of 8-state QKR under ideal circumstances. Consider a sequence of QKR rounds with a large number of consecutive Accepts. Let $\varepsilon = 2 \cdot 2^{-\lambda} + 2^{-\sigma}$ be the 'imperfection' induced by one round of QKR. Let θ be the maximum distance that

[4]The min-entropy loss gives a conservative (and possibly too pessimistic) bound.

Alice and Bob are willing to tolerate between reality and the ideal state $\rho^{(0)}$. After $N = \lfloor \theta/\varepsilon \rfloor$ rounds they have to refresh *all* their key material. One can define a 'QKR rate' as {the total amount of message data sent in N rounds minus the key material expended} divided by the number of qubits and the number of rounds. The total message size is $N\ell$, with ℓ specified in (12). The total key expenditure consists of N times two λ-bit authentication tags[5], N a-bit OTPs that protect the syndromes (asymptotically $a \approx nh(\beta)$), $2n$ bits of basis key b, and n bits of extractor key u. This gives

$$\text{Rate} = 1 - \frac{a}{n} - 2\log f(\beta) - \frac{2\xi}{n} - \frac{30\log(n+1)}{n} - \frac{2\lambda}{n} - \frac{3}{\lfloor \theta/\varepsilon \rfloor}. \tag{13}$$

Note that ξ/n scales as $\sqrt{\sigma}/\sqrt{n}$, and that ε can be made exponentially small (N exponentially large) by increasing λ and σ. The asymptotic rate is

$$\text{for} \quad n \to \infty, N \to \infty: \quad \text{Rate} \to 1 - h(\beta) - 2\log f(\beta). \tag{14}$$

See Fig. 1. The asymptotic rate is positive up to $\beta \approx 0.09$. Up to this noise level using QKR makes sense.

It is possible to reduce the key expenditure. "Scheme #3" in [2] greatly reduces the key material spent on protecting the syndrome, but it increases the number of qubits needed to convey the message. It does not modify the rate (13).

Instead of pairwise independent hashing one may use 'almost pairwise independent' hashes. A small security penalty δ is incurred, but the length of the extractor key u is reduced from n to approximately $\min(n - \ell, \ell + 2\log \frac{1}{\delta})$.

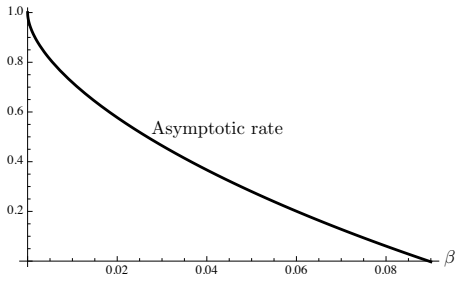

Figure 1: *The asymptotic rate* $1 - h(\beta) - 2\log f(\beta)$.

Typically θ is fixed. It makes sense to set $\lambda - 1 \approx \sigma$. Increasing one of the two parameters σ, λ far above the other one does not significantly reduce the sum $\varepsilon = 2^{-\lambda+1} + 2^{-\sigma}$. Then it remains to tune N (which via $\varepsilon = \theta/N$ fixes σ) and n as a function of (θ, β) so as to optimise the rate. In Fig. 2 the non-asymptotic rate is plotted for $\theta = 2^{-256}$ and various choices of β, N and n. We see that the asymptotic rate can be approached well for realistic values of N and n, especially for channels with a low bit error rate β.

5.2 Comparison to existing results

The proof technique of Fehr and Salvail [1] requires a special property ('key privacy') of the MAC function, and they have to keep track of the security of the MAC key. We avoid this complication at the cost of spending λ additional bits of key material per round. An

[5]Both the tag t and the Accept/Reject bit are authenticated using λ bits of key material.

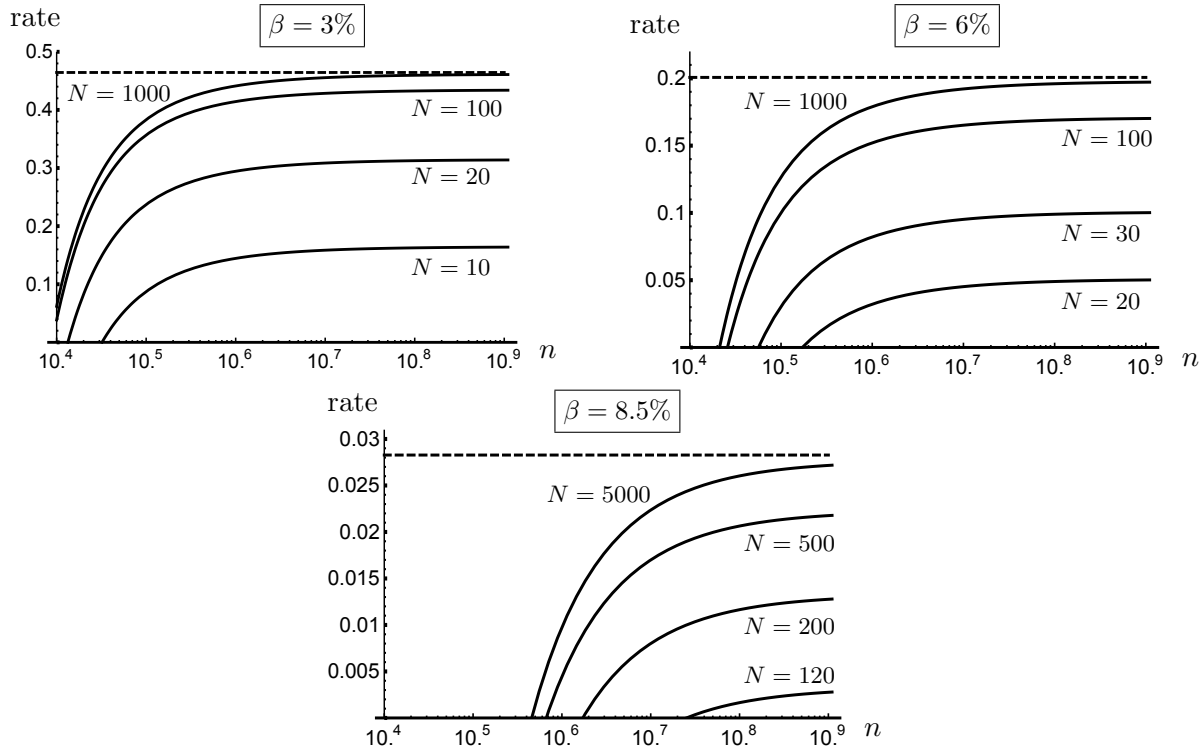

Figure 2: *Rate as a function of the number of qubits (n), for various values of the design parameter N and tolerated noise β. The security parameter θ is set to $\theta = 2^{-256}$. We have set $\lambda = \sigma + 1$. The dashed lines indicate the asymptotic rate (14).*

interesting difference with respect to [1] is that we capture the security of the basis key B and the extractor key U in a single quantity $d(UB|ZE)$, whereas [1] uses a min-entropy result for the basis key and a trace distance for the extractor key. In terms of QKR scheme construction, the main differences are of course (i) that [1] tolerates practically no noise, and (ii) that the use of 8-state encoding [2] as compared to 4-state (or 6-state) massively reduces the need for privacy amplification at low β. These differences were already noted in [2, 9].

The min-entropy analysis of attacks in [9] has turned out to be too pessimistic in certain respects. For the 'K2 attack' (a known-plaintext attack on b) a min-entropy loss of $\log(1 + \sqrt{6\beta(1 - \frac{3}{2}\beta)})$ bits per qubit was found for 8-state encoding; that is considerably more than our leakage result $2 \log f(\beta)$. Clearly min-entropy is too pessimistic as a measure of security in this context. Note that in [1] all security bounds are expressed in terms of min-entropy.

5.3 Dealing with erasures

Our analysis has not taken into account quantum channels with erasures. (Particles failing to arrive.) Consider a channel with erasure rate η and bit error rate β for the non-erased states. The Alice-to-Bob channel capacity is $(1 - \eta)(1 - h(\beta))$. A capacity-achieving linear error-correcting code that is able to deal with such a channel has a syndrome of size $nh(\beta) +$

$n\eta[1-h(\beta)]$. Imagine the QKR scheme of Section 3 employing such an error-correcting code. On the one hand, the key expenditure increases from $nh(\beta)$ to $nh(\beta)+n\eta[1-h(\beta)]$. On the other hand, the leakage increases. Every qubit not arriving at Bob's side must be considered to be in Eve's possession; since an erasure can be parametrised as a qubit with $\beta=\frac{1}{2}$, the leakage is 1 bit per erased qubit. Hence the leakage term $n\cdot 2\log f(\beta)$ in Theorem 4.1 changes to $n(1-\eta)2\log f(\beta)+n\eta$. The combined effect of the syndrome size and the leakage increase has a serious effect on the QKR rate. The asymptotic rate becomes $1-h(\beta)-\eta[1-h(\beta)]-(1-\eta)2\log f(\beta)-\eta$. For $\beta=0$ this is $1-2\eta$; at zero bit error rate no more than 50% erasures can be accommodated by the scheme. In long fiber optic cables the erasure rate can be larger than 90%. Under such circumstances the QKR scheme of Section 3 simply does not work. (Note that continuous-variable schemes have much lower erasure rates.)
One can think of a number of straightforward ways to make the QKR protocol erasure-resistant. Below we sketch a protocol variant in which Alice sends qubits, and Bob returns an authenticated and encrypted message.

1. Alice sends a random string $x\in\{0,1\}^m$ encoded in m qubits, with $m(1-\eta)>n$.
2. Bob receives qubits in positions $i\in\mathcal{I}$, $\mathcal{I}\subseteq[m]$ and measures x'_i in those positions. He aborts the protocol if $|\mathcal{I}|<n$. Bob selects a random subset $\mathcal{J}'\subset\mathcal{I}$, with $|\mathcal{J}'|=n$. He constructs a string $y'=x'_{\mathcal{J}'}$. He computes $s'=k_{\mathrm{SS}}\oplus S(y')$, $z'=\mathtt{Ext}(u,y')$, $c'=\mu\oplus z'$, $t'=M(k_{\mathrm{MAC}},\mathcal{J}'||y'||c'||s')$. He sends $\mathcal{J}',s',c',t'$.
3. Alice receives this data as $\mathcal{J},s,c,t$. She computes y by running the Secure Sketch's reconstruction algorithm on $x_{\mathcal{J}}$ and the syndrome $k_{\mathrm{SS}}\oplus s$. Then she computes $z=\mathtt{Ext}(u,y)$, $\hat{\mu}=z\oplus c$ and $\tau=M(k_{\mathrm{MAC}},\mathcal{J}||y||c||s)$. Alice Accepts the message $\hat{\mu}$ if $\tau=t$ and Rejects otherwise.

The security is not negatively affected by the existence of erasures. Assume that Eve holds all the qubits that have not reached Bob. Since the data in the qubits is random, and does not contribute to the computation of z', it holds that (i) it is not important if Eve learns the content of these bits, (ii) known plaintext does not translate to partial knowledge of the data content of these qubits, which would endanger the basis key b and the extractor key u.

Many protocol modifications are possible. For instance, if Alice sends the qubits *and* the message, then Bob needs to tell Alice where the erasures are before she can construct the ciphertext.

5.4 Future work

It is interesting to note that QKR protocols which first send a random string z and then use z for OTP encryption look a lot like Quantum Key Distribution, but with reduced communication complexity. This changes when the message is put directly into the qubits, e.g. as is done in Gottesman's Unclonable Encryption [6]. It remains a topic for future work to prove security of such a QKR scheme.
The QKR scheme of Section 3 can be improved and embellished in various ways. For instance, Alice's λ-bit key expenditure for one-time MACing may not be necessary. The authentication tag may simply be generated as part of the `Ext` function's output, and then the security of the MAC key can be proven just by proving the security of the extractor key u (similar to what is done in [1]).

Furthermore, as mentioned in Section 5.1, one may use 'scheme #3' of [2] which protects the syndrome by sending it through the quantum channel instead of classically OTP-ing it. This too reduces the key expenditure and does not affect the rate.
Another interesting option is to deploy the Quantum One Time Pad with approximately half the key length, which still yields information-theoretic security. This would improve the rate (13) by reducing the cost $\frac{2}{N}$ to approximately $\frac{1}{N}$.
We suspect that the inequality in (8) is not tight. Given the similarities between QKR and QKD we would intuitively expect that the required amount of privacy amplification is the same as for QKD. A known result for QKD, based on von Neumann entropy, is $-(1-\frac{3}{2}\beta)\log(1-\frac{3}{2}\beta)-\frac{3}{2}\beta\log\frac{\beta}{2}-h(\beta)$, which is less than the $2n\log f(\beta)$ of (8) for all β. Perhaps an improved proof technique can get closer to the QKD result.

6 Proof of Theorem 4.1

Our proof is similar to the derivation of the Leftover Hash Lemma (against quantum side information), but with the difference that we apply an operator inequality on the square root function and then compute the trace of a square root, instead of pulling the trace into the square root via a Jensen, Cauchy-Schwartz or Hölder inequality.

6.1 Rewriting Eve's state

We omit the superscript 'E' on Eve's state. We allow Eve to cause different bit error probabilities $\gamma_i \in [0, \frac{1}{2})$ in each qubit position i individually. We have

$$\rho_{zub} = \mathbb{E}_{x:z=\mathtt{Ext}(u,x)} \bigotimes_{i=1}^{n} \omega_{x_i}^{b_i}(\gamma_i) = 2^{\ell} \sum_{x\in\{0,1\}^n} \delta_{z,\mathtt{Ext}(u,x)} \bigotimes_{i=1}^{n} \tfrac{1}{2}\omega_{x_i}^{b_i}(\gamma_i), \tag{15}$$

where $\omega_{x_i}^{b_i}$ is defined as in (6). Using the properties of universal hash functions we get $\mathbb{E}_u \delta_{z,\mathtt{Ext}(u,x)} = 2^{-\ell}$, which yields

$$\rho_{\mathrm{av}} \stackrel{\mathrm{def}}{=} \mathbb{E}_u \rho_{zub} = \bigotimes_{i=1}^{n} \frac{\omega_0^{b_i}(\gamma_i) + \omega_1^{b_i}(\gamma_i)}{2}. \tag{16}$$

Note that ρ_{av} does not depend on z. In fact, it does not depend on b either! From (6) it follows that

$$\frac{\omega_0^b(\gamma) + \omega_1^b(\gamma)}{2} = (1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma}{2}(\mathbb{1} - |m_0\rangle\langle m_0|). \tag{17}$$

We have

$$\rho_{\mathrm{av}} = \bigotimes_{i=1}^{n} \Big\{ (1-\tfrac{3}{2}\gamma_i)|m_0\rangle\langle m_0| + \tfrac{\gamma_i}{2}(\mathbb{1} - |m_0\rangle\langle m_0|) \Big\}. \tag{18}$$

The special property holds that $\mathbb{E}_z \rho_{zub} = \mathbb{E}_u \rho_{zub} = \rho_{\mathrm{av}}$.

6.2 Bounding the distance

We start from $D \stackrel{\mathrm{def}}{=} \mathbb{E}_z \|\rho_z^{\mathrm{UBE}} - \rho^{\mathrm{UB}} \otimes \rho_z\|_1 = \mathbb{E}_{zub} \|\rho_{zub} - \rho_{\mathrm{av}}\|_1 = \mathbb{E}_{zub} \mathrm{tr}\sqrt{[\rho_{zub} - \rho_{\mathrm{av}}]^2}$. Here we have used the block structure of the state to pull the $\mathbb{E}_{ub}$ out of the trace norm. We use

the fact that the square root function is operator-concave in order to move $\mathbb{E}_u$ into the square root, and then use $\rho_{\rm av} = \mathbb{E}_u \rho_{zub}$.

$$D \leq \mathbb{E}_{bz} \mathrm{tr} \sqrt{\mathbb{E}_u [\rho_{zub} - \rho_{\rm av}]^2} = \mathbb{E}_{bz} \mathrm{tr} \sqrt{\mathbb{E}_u \rho_{zub}^2 - \rho_{\rm av}^2}. \tag{19}$$

Next we expand ρ_{zub} twice and write

$$\mathbb{E}_u \rho_{zub}^2 \;=\; \mathbb{E}_u 2^{2\ell} \sum_{xy} \delta_{z,\mathtt{Ext}(u,x)} \delta_{z,\mathtt{Ext}(u,y)} \bigotimes_{i=1}^n \tfrac{1}{4} \omega_{x_i}^{b_i}(\gamma_i) \omega_{y_i}^{b_i}(\gamma_i). \tag{20}$$

The $\mathbb{E}_u \delta\delta$ is evaluated using the properties of pairwise independent hash functions. An occurrence $x \neq y$ gives rise to $2^{-2\ell}$, whereas $x = y$ yields $2^{-\ell}$.

$$\begin{aligned}
\mathbb{E}_u \rho_{zub}^2 &= \sum_{xy} [2^\ell \delta_{xy} + (1 - \delta_{xy})] \bigotimes_{i=1}^n \tfrac{1}{4} \omega_{x_i}^{b_i}(\gamma_i) \omega_{y_i}^{b_i}(\gamma_i) && (21)\\
&= \sum_{xy} [(2^\ell - 1)\delta_{xy} + 1] \bigotimes_{i=1}^n \tfrac{1}{4} \omega_{x_i}^{b_i}(\gamma_i) \omega_{y_i}^{b_i}(\gamma_i) && (22)\\
&= (2^\ell - 1) \bigotimes_{i=1}^n \frac{[\omega_0^{b_i}(\gamma_i)]^2 + [\omega_1^{b_i}(\gamma_i)]^2}{4} + \bigotimes_{i=1}^n \Big(\frac{\omega_0^{b_i}(\gamma_i) + \omega_1^{b_i}(\gamma_i)}{2} \Big)^2 && (23)\\
&= (2^\ell - 1) \bigotimes_{i=1}^n \frac{[\omega_0^{b_i}(\gamma_i)]^2 + [\omega_1^{b_i}(\gamma_i)]^2}{4} + \rho_{\rm av}^2. && (24)
\end{aligned}$$

We define shorthand notation $|\boldsymbol{v} \cdot \boldsymbol{m}\rangle \stackrel{\rm def}{=} v_x |m_1\rangle + v_y |m_2\rangle + v_z |m_3\rangle$. Then

$$|E_{01}^{\boldsymbol{v}}\rangle = \sqrt{\frac{1 - \frac{3}{2}\gamma}{1 - \gamma}} |m_0\rangle + \sqrt{\frac{\frac{1}{2}\gamma}{1 - \gamma}} |\boldsymbol{v} \cdot \boldsymbol{m}\rangle. \tag{25}$$

Note that $|m_0\rangle$, $|\boldsymbol{v} \cdot \boldsymbol{m}\rangle$, $|E_{00}^{\boldsymbol{v}}\rangle$, $|E_{11}^{\boldsymbol{v}}\rangle$ form an orthonormal basis. We have

$$\begin{aligned}
[\omega_x^b(\gamma)]^2 &= (1 - \gamma)^2 \sigma_{x\bar{x}}^{\boldsymbol{v}(b)} + \gamma^2 \sigma_{xx}^{\boldsymbol{v}(b)} && (26)\\
[\omega_0^b(\gamma)]^2 + [\omega_1^b(\gamma)]^2 &= (1 - \gamma)^2 [\sigma_{01}^{\boldsymbol{v}(b)} + \sigma_{10}^{\boldsymbol{v}(b)}] + \gamma^2 [\sigma_{00}^{\boldsymbol{v}(b)} + \sigma_{11}^{\boldsymbol{v}(b)}]\\
&= 2(1 - \gamma)^2 \Big[\frac{1 - \frac{3}{2}\gamma}{1 - \gamma} |m_0\rangle\langle m_0| + \frac{\frac{1}{2}\gamma}{1 - \gamma} |\boldsymbol{v}(b) \cdot \boldsymbol{m}\rangle\langle \boldsymbol{v}(b) \cdot \boldsymbol{m}| \Big]\\
&\quad + \gamma^2 [\sigma_{00}^{\boldsymbol{v}(b)} + \sigma_{11}^{\boldsymbol{v}(b)}]. && (27)
\end{aligned}$$

The eigenvalues of $[(\omega_0^b)^2 + (\omega_1^b)^2]/2$ are

$$\lambda_1^{(i)} \stackrel{\rm def}{=} (1 - \gamma_i)(1 - \tfrac{3}{2}\gamma_i); \quad \lambda_2^{(i)} \stackrel{\rm def}{=} \tfrac{1}{2}\gamma_i (1 - \gamma_i); \quad \lambda_3^{(i)} \stackrel{\rm def}{=} \tfrac{1}{2}\gamma_i^2; \quad \lambda_4^{(i)} \stackrel{\rm def}{=} \tfrac{1}{2}\gamma_i^2. \tag{28}$$

Hence we get

$$\begin{aligned}
\mathrm{tr} \sqrt{\mathbb{E}_u \rho_{zub}^2 - \rho_{\rm av}^2} &= \sqrt{(2^\ell - 1)2^{-n}} \prod_{i=1}^n \Big[\sum_{j=1}^4 \sqrt{\lambda_j^{(i)}} \Big] = \sqrt{(2^\ell - 1)2^{-n}} \prod_{i=1}^n f(\gamma_i) && (29)\\
&< \sqrt{2^{\ell - n}} \prod_{i=1}^n f(\gamma_i) = \sqrt{2^{\ell - n + 2n \cdot \frac{1}{n} \sum_{i=1}^n \log f(\gamma_i)}} && (30)
\end{aligned}$$

with f as defined in Theorem 4.1. We substitute (30) into (19). As $\log f(\cdot)$ is a concave function it holds that $\frac{1}{n} \sum_{i=1}^n \log f(\gamma_i) \leq \log f(\frac{1}{n} \sum_i \gamma_i)$. $\square$

7 Proof of Theorem 4.2

We omit the superscript 'E' on Eve's state. We use shorthand notation $D \stackrel{\text{def}}{=} \mathbb{E}_z \|\rho_z^{\text{UBE}} - \rho^{\text{UB}} \otimes \rho_z\|_1$. Let γ be the noise parameter that Eve actually applies. The error rate tolerated by the error-correcting code is β. The probability that Bob accepts is denoted as P_{acc}. We distinguish between P_{acc} and $P_{\text{re-use}}$ because it is possible that Bob sends a Reject bit and Eve changes it to Accept, which leads to unintended key re-use. We have $P_{\text{re-use}} = 2^{-\lambda} + P_{\text{acc}}$, where $2^{-\lambda}$ is Eve's probability of forging Bob's MAC tag.

The P_{acc} consists of two contributions: a term $2^{-\lambda}$ from the possibility that Eve accidentally forges a correct tag on Alice's message, and a term $P_{\text{acc}}^{\text{ECC}}(\gamma,\beta) = \sum_{t \le n\beta} \binom{n}{t} \gamma^t (1-\gamma)^{n-t}$ representing the probability that the number of bit flips in x' remains below the threshold $n\beta$ that can be handled by the error-correcting code.[6]

In the two cases where Eve forges a tag we use the bound $D \le 1$. This yields the term $2 \cdot 2^{-\lambda}$ in (11). In the third case we use Theorem 4.1. Substitution of (9) into (8) yields

$$D < \Delta(\gamma,\beta) \stackrel{\text{def}}{=} \left[\frac{f(\gamma)}{f(\beta)}\right]^n 2^{-\xi}. \tag{31}$$

We define a parameter β_ξ such that $\Delta(\beta_\xi,\beta) = 1$. On the interval $\gamma \le \beta$ we use $P_{\text{acc}}^{\text{ECC}} \le 1$, which yields $P_{\text{acc}}^{\text{ECC}} D < 2^{-\xi} < 2^{-\sigma}$. (Here we have used that $\xi > \sigma$ for relevant values of β, i.e. the range that yields positive rate. See Section 5.1. In particular, we use that $f'(\beta)/f(\beta) > 1/2$.)

On the interval $\gamma > \beta_\xi$ we use $D \le 1$. Furthermore, $P_{\text{acc}}^{\text{ECC}}$ is a decreasing function of γ. Hence for $\gamma > \beta_\xi$ it holds that $P_{\text{acc}}^{\text{ECC}} D < P_{\text{acc}}^{\text{ECC}}(\beta_\xi,\beta)$.

On the interval $\gamma \in (\beta, \beta_\xi]$ we note that $P_{\text{acc}}^{\text{ECC}}(\gamma,\beta)\Delta(\gamma,\beta)$ is an increasing function of γ. We conclude that we can use the bound $P_{\text{acc}}^{\text{ECC}} D < P_{\text{acc}}^{\text{ECC}}(\beta_\xi,\beta)$ on the whole interval $\gamma > \beta$. The Chernoff bound yields $P_{\text{acc}}^{\text{ECC}}(\beta_\xi,\beta) \le \exp[-\frac{n}{2\beta_\xi}(\beta_\xi - \beta)^2]$.

First we define a parameter α_σ such that $\beta_\xi \ge \alpha_\sigma$ implies $P_{\text{acc}}^{\text{ECC}}(\beta_\xi,\beta) \le 2^{-\sigma}$. Solving for α_σ gives $\alpha_\sigma = \beta + \frac{\sigma \ln 2}{n} + \sqrt{(\frac{\sigma \ln 2}{n})^2 + 2\beta\frac{\sigma \ln 2}{n}}$.

Next we note that (31) gives us an expression for ξ as a function of β_ξ, namely $\xi = n \log \frac{f(\beta_\xi)}{f(\beta)}$. A sufficiently large value of ξ in order to achieve the desired security $2^{-\sigma}$ is given by

$$\xi_{\text{suff}} = n \log \frac{f(\alpha_\sigma)}{f(\beta)}. \tag{32}$$

We consider two ways to simplify (32).

1. The concavity of f allows us to write $f(\alpha_\sigma) \le f(\beta) + (\alpha_\sigma - \beta) f'(\beta)$. Substitution into (32) and using $\ln(1+u) \le u$ yields $\xi_{\text{suff}} \le \frac{n}{\ln 2} \frac{f'(\beta)}{f(\beta)} (\alpha_\sigma - \beta)$, which is precisely the first expression in (10).

2. ξ_{suff} is a decreasing[7] function of β. Hence we can upper bound it by the value taken at $\beta = 0$. This gives $\xi_{\text{suff}} \le \frac{n}{\ln 2} \ln f(\frac{2\sigma \ln 2}{n})$. Using $f(u) \le 1 + \sqrt{u/2} + u\sqrt{2}$ and $\ln(1+v) \le v$ we get $\xi_{\text{suff}} \le \frac{n}{\ln 2}[\sqrt{\frac{\sigma}{n} \ln 2} + \frac{\sigma}{n} 2\sqrt{2} \ln 2]$, which is the second expression in (10).

□

[6] We could allow Eve to apply a different γ_i for each EPR pair. However, the $P_{\text{acc}}^{\text{ECC}}$ is maximized by setting all γ_i equal to γ. Namely, $P_{\text{acc}}^{\text{ECC}} = \sum_{\mathcal{A} \subset [n] : |\mathcal{A}| \le n\beta} (\prod_{i \in \mathcal{A}} \gamma_i) \prod_{j \in \mathcal{A}^c} (1-\gamma_j)$. Using Jensen's inequality for the logarithm function it is readily verified that $\prod_{i \in \mathcal{A}} \gamma_i \le (\frac{1}{|\mathcal{A}|} \sum_{i \in \mathcal{A}} \gamma_i)^{|\mathcal{A}|}$ and similarly $\prod_{j \in \mathcal{A}^c} (1-\gamma_j) \le (1 - \frac{1}{|\mathcal{A}^c|} \sum_{j \in \mathcal{A}^c} \gamma_j)^{|\mathcal{A}^c|}$.

[7] This is easily verified by plotting $\frac{\mathrm{d}}{\mathrm{d}\beta} \frac{f(\alpha_\sigma)}{f(\beta)}$ and noting that it is always negative.

Acknowledgements

We thank Serge Fehr and Niek Bouman for helpful discussions. Part of this research was funded by NWO (CHIST-ERA project ID_IOT).

References

[1] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Eurocrypt*, pages 311–338, 2017.

[2] B. Škorić and M. de Vries. Quantum Key Recycling with eight-state encoding. (The Quantum One Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 2017.

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

[4] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[5] C.H. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13:453–458, 2014. Original manuscript 1982.

[6] D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581–602, 2003.

[7] I.B. Damgård, T.B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *CRYPTO*, pages 494–510, 2005.

[8] I.B. Damgård, T.B. Pedersen, and L. Salvail. How to re-use a one-time pad safely and almost optimally even if P = NP. *Natural Computing*, 13(4):469–486, 2014.

[9] D. Leermakers and B. Škorić. Optimal attacks on qubit-based Quantum Key Recycling. *Quantum Information Processing*, 2018.

[10] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.

[11] M.N. Wegman and J.W. Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22:265–279, 1981.

[12] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.

[13] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.

[14] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[15] D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.

[16] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.

[17] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.