Security proof for quantum key recycling with noise

Quantum Information and Computation, Vol. 0, No. 0 (2019) 000–000

SECURITY PROOF FOR QUANTUM KEY RECYCLING WITH NOISE

DAAN LEERMAKERS
Department of Mathematics and Computer Science, Eindhoven University of Technology
5600MB Eindhoven, The Netherlands

BORIS ŠKORIĆ
Department of Mathematics and Computer Science, Eindhoven University of Technology
5600MB Eindhoven, The Netherlands

Received (received date)
Revised (revised date)

Quantum Key Recycling aims to re-use the keys employed in quantum encryption and quantum authentication schemes. QKR protocols can achieve better round complexity than Quantum Key Distribution. We consider a QKR protocol that works with qubits, 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 high-rate scheme for the noisy case was proposed by Škorić and de Vries [2], based on eight-state encoding. However, a security proof was not given. In this paper we introduce a protocol modification to [2] and provide a security proof. The modified protocol has high rate not only for 8-state encoding, but also 6-state and BB84 encoding. 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. It turns out that the rate is higher than suggested by previous results. Asymptotically the rate equals the rate of Quantum Key Distribution with one-way postprocessing.

Keywords: Quantum Key Recycling; quantum cryptogtraphy
Communicated by: to be filled by the Editorial

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. A QKR protocol can achieve better round complexity than QKD, since communication about basis choices is avoided. After the discovery of QKD, interest in QKR was practically nonexistent for a long time. 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 and tolerates higher noise levels, 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 modification in the QKR protocol of Škorić and de Vries [2]. The basis key now gets refreshed even in case of an Accept; the key update is done by hashing the payload of the qubits into the old key, without using up existing key material. Furthermore, we modify the privacy amplification: instead of deriving a classical one-time pad from the qubits' payload solely, we compress the payload and the old basis key together. For simplicity we combine the privacy amplification and the key refreshment into a single hashing operation.
- We provide a security proof. Our proof technique differs from [1]. We treat all keys on the same footing and show that they remain close to uniform given Eve's side information, whereas in [1] some keys become non-uniform.

  Our approach is as follows. We switch to an EPR formulation of our protocol. First we consider attacks in which Eve collects quantum side information from one EPR pair at a time; we apply symmetrisation of the noisy Alice-Bob system as introduced in [10, 11]. We upper bound the trace distance between the real state and an ideal state in which all the keys are decoupled from the subsystem available to Eve. Finally we invoke the post-selection method [12] in order to obtain security against general attacks.

  For asymptotically large n (number of qubits) the steps in our derivation are very similar to [13, 14]; we make use of smooth Rényi entropies, which asymptotically tend to the von Neumann entropy. For finite n we present a separate result without smoothing, based on straightforward diagonalisation.
- The QKR rate is defined as the message length minus the key expenditure, divided by n. From our bound on the trace distance we obtain an expression for the QKR rate as a function of n and the tolerated bit error rate (β). For $n \to \infty$ the rate equals the rate of QKD with one-way postprocessing (i.e. without two-way advantage distillation). This means that whenever it is possible to do one-way-postprocessing-QKD, it is also possible to do QKR at the same asymptotic rate and hence get the benefit of reduced communication complexity.

For finite n, our approach without smoothing yields a rate $\approx 1-h(\beta)-2\log[\sqrt{(1-\frac{3}{2}\gamma)(1-\gamma)}+\sqrt{\frac{3}{2}\gamma(1+\gamma)}]$, where h is the binary entropy function. Both these results are more favourable than what one would expect based on the min-entropy analysis in [9] and straightforward generalisations of [1] to the noisy case.

It is interesting to note that the asymptotic equivalence of the QKR and QKD rate holds not only for 8-state encoding. For 6-state and 4-state (BB84) encoding there is a severe leakage of the qubit payload if Eve intercepts the whole cipherstate. From [2] and [9] it would seem that this leakage necessarily implies low QKR rate. However, in our protocol the leak is masked by the secret key that is used for privacy amplification.

The outline of the paper is as follows. In the preliminaries section we introduce notation; we briefly review smooth Rényi entropies, 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 motivate why we depart from the entanglement-monogamy based proof technique. In Section 4 we present the modified QKR protocol. Section 5 states the main theorems and discusses rates and optimal parameter choices. In Section 6 we compare to existing results, discuss erasures, and suggest topics 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 $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. Sometimes we will write $h(\{p_1,\ldots,p_k\})$ meaning $\sum_i p_i \log\frac{1}{p_i}$. 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 $\bar{b} = 1-b$. The Hamming weight of a binary string x is written as $|x|$. We will speak about 'the bit error rate γ 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 $\sigma_x, \sigma_y, \sigma_z$. 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 uniform classical variables X, Y and a quantum system labeled 'E' (under Eve's control) that depends on X and Y. The combined classical-quantum state is $\rho^{\mathrm{XYE}} =$

$\mathbb{E}_{xy}|xy\rangle\langle xy| \otimes \rho^{\mathrm{E}}_{xy}$. The state of a sub-system is obtained by tracing out a subspace, e.g. $\rho^{\mathrm{YE}} = \mathrm{tr}_X \rho^{\mathrm{XYE}} = \mathbb{E}_y |y\rangle\langle y| \otimes \rho^E_y$, with $\rho^E_y = \mathbb{E}_x \rho^E_{xy}$. The fully mixed state of subsystem X is denoted as μ^X. The security of the variable X, given that Eve holds the 'E' subsystem, can be expressed in terms of a trace distance as follows [13],

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

i.e. the distance between the true classical-quantum state and a state in which X is completely unknown to Eve. X is said to be ε-secure with respect to ρ if $d(X|E) \leq \varepsilon$. 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) [15] 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 Smooth Rényi entropies

Let ρ be a mixed state. The von Neumann entropy of ρ is $S(\rho) = -\mathrm{tr}\,\rho \log \rho$. The ε-smooth Rényi entropy of order α is defined as [13]

$$\text{For } \alpha \in (0,1) \cup (1,\infty): \qquad S^\varepsilon_\alpha(\rho) \stackrel{\mathrm{def}}{=} \frac{1}{1-\alpha} \log \min_{\bar\rho:\, \|\bar\rho - \rho\|_1 \leq \varepsilon} \mathrm{tr}\,\bar\rho^\alpha, \tag{2}$$

where the density operator $\bar\rho$ may be sub-normalised. Furthermore $S^\varepsilon_0(\rho) = \lim_{\alpha\to 0} S^\varepsilon_\alpha(\rho)$ and $S^\varepsilon_\infty(\rho) = \lim_{\alpha\to\infty} S^\varepsilon_\alpha(\rho)$ It has been shown that the smooth Rényi entropy of factor states $\rho^{\otimes n}$ asymptotically approaches the von Neumann entropy.

Lemma 1 *Let ρ be a density matrix.*

$$S^\varepsilon_2(\rho^{\otimes n}) \;\; \geq \;\; nS(\rho) - (2\log \mathrm{rank}(\rho) + 3)\sqrt{n \log \tfrac{2}{\varepsilon}}. \tag{3}$$

$$S^\varepsilon_0(\rho^{\otimes n}) \;\; \leq \;\; nS(\rho) + \mathcal{O}(\sqrt{n \log \tfrac{1}{\varepsilon}}). \tag{4}$$

This lemma follows from [10] (Corollary 3.3.7 and the comment above Theorem 3.3.6), combined with $S^\varepsilon_2 \geq S^\varepsilon_\infty$.

2.3 QKR security definition and proof structure

The aim of QKR is to send private authenticated messages, with a better round complexity than QKD. The protocol (see Section 4) 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, most of the key material K is re-used; in case of Reject, the key material is refreshed from K to K'.

In order to be considered secure, a QKR protocol must satisfy two properties: (1) even if Eve intercepts everything that Alice sends, she must learn only negligible information about the message; (2) if Eve knows the plaintext and Bob Accepts, Eve's knowledge about the keys used in the next round should be negligible.

For the security of the keys under known-plaintext 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 $\rho^{(1)}_c$;

this includes actions by Eve as well as key updates by Alice and Bob. Accept happens with probability $P_{\rm acc}$ and leads to a state $\rho^{(1)}_{\rm acc} = \mathbb{E}_k |k\rangle\langle k| \otimes \tilde{\rho}^{\rm E}_k$ in which Eve has potentially gained knowledge about K; Reject happens with probability $P_{\rm rej}$ and yields a state $\rho^{(1)}_{\rm rej} = \tilde{\rho}^{\rm K} \otimes \tilde{\rho}^{\rm E}$ 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 $\rho^{(1)}_c$ and the ideal state $\rho^{(0)}$, given that Eve observes the decision bit: $P_{\rm acc}\|\rho^{(1)}_{\rm acc} - \rho^{(0)}\|_1 + P_{\rm rej}\|\rho^{(1)}_{\rm rej} - \rho^{(0)}\|_1 \leq \varepsilon$, which is equivalent to $P_{\rm acc}\|\rho^{(1)}_{\rm acc} - \rho^{(0)}\|_1 \leq \varepsilon$.

By induction $\mathbb{E}_{c_1\cdots c_N}\|\rho^{(N)}_{c_1\cdots c_N} - \rho^{(0)}\|_1 \leq N\varepsilon$, where $\rho^{(N)}$ is the state after N rounds. This can be seen as follows. After two rounds the state is $\rho^{(2)}_{c_1c_2}$, and the security quantity of interest is $\mathbb{E}_{c_1c_2}\|\rho^{(2)}_{c_1c_2} - \rho^{(0)}\|_1 = P^2_{\rm acc}\|\rho^{(2)}_{\rm acc,acc} - \rho^{(0)}\|_1 + P_{\rm rej}P_{\rm acc}\|\rho^{(2)}_{\rm rej,acc} - \rho^{(0)}\|_1 = P^2_{\rm acc}\|\rho^{(2)}_{\rm acc,acc} - \rho^{(0)}\|_1 + P_{\rm rej}P_{\rm acc}\|\rho^{(1)}_{\rm acc} - \rho^{(0)}\|_1 \leq P^2_{\rm acc}\|\rho^{(2)}_{\rm acc,acc} - \rho^{(0)}\|_1 + P_{\rm rej}\varepsilon$. Using the triangle inequality the first term is upperbounded as $P^2_{\rm acc}\|\rho^{(2)}_{\rm acc,acc} - \rho^{(0)}\|_1 \leq P^2_{\rm acc}\|\rho^{(2)}_{\rm acc,acc} - \rho^{(1)}_{\rm acc}\|_1 + P^2_{\rm acc}\|\rho^{(1)}_{\rm acc} - \rho^{(0)}\|_1 \leq P^2_{\rm acc}\|\rho^{(2)}_{\rm acc,acc} - \rho^{(1)}_{\rm acc}\|_1 + P_{\rm acc}\varepsilon$. Finally it is used that the mapping from $\rho^{(i)}$ to $\rho^{(i+1)}$ is a CPTP map, which cannot increase distance. Hence $\|\rho^{(2)}_{\rm acc,acc} - \rho^{(1)}_{\rm acc}\|_1 \leq \|\rho^{(1)}_{\rm acc} - \rho^{(0)}\|_1$. It follows that $\mathbb{E}_{c_1c_2}\|\rho^{(2)}_{c_1c_2} - \rho^{(0)}\|_1 \leq 2\varepsilon$.

2.4 Post-selection

In a *collective attack* Eve acts on individual qudits. This is not the most general attack. For protocols that are invariant under permutation of the qubits, 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 ($d = 2$ 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.

2.5 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 [16] the vectors are $\pm x$, $\pm y$, $\pm z$ on the Bloch sphere. 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

$$|\psi_{uwg}\rangle = (-1)^{gu}\left[(-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g\oplus w\rangle + (-1)^u(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|\overline{g\oplus w}\rangle\right]. \tag{5}$$

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 [17, 18, 19] 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.

2.6 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 $|\psi_{b_ix_i}\rangle$ 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; this turns the pure EPR state into a mixed state. The noise symmetrisation technique of [11] was applied to simplify the state. If Eve's actions induce bit error probability γ (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 $\tilde{\rho}^{\mathrm{AB}} = (1-\frac{3}{2}\gamma)|\Psi^-\rangle\langle\Psi^-| + \frac{\gamma}{2}\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+|\right)$, 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.[a] Eve's state is obtained by purifying $\tilde{\rho}^{\mathrm{AB}}$. The pure state is $|\Psi^{\mathrm{ABE}}\rangle = \sqrt{1-\frac{3}{2}\gamma}|\Psi^-\rangle\otimes|m_0\rangle + \sqrt{\frac{\gamma}{2}}\left(-|\Phi^-\rangle\otimes|m_1\rangle + i|\Psi^+\rangle\otimes|m_2\rangle + |\Phi^+\rangle\otimes|m_3\rangle\right)$, where $|m_i\rangle$ is an orthonormal basis in Eve's four-dimensional ancilla space. Let $\boldsymbol{v} = (v_1, v_2, v_3)$ be a 3-component vector on the Bloch sphere describing the '0' bit value in a certain basis. Let $|\boldsymbol{v}\cdot\boldsymbol{m}\rangle$ be shorthand notation for $v_1|m_1\rangle + v_2|m_2\rangle + v_3|m_3\rangle$. Let x be the bit value that Alice measures, and y Bob's bit value. (In the noiseless case we have $y = \bar{x}$ 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,

$$\sigma^{\boldsymbol{v}}_{xy} \stackrel{\mathrm{def}}{=} |E^{\boldsymbol{v}}_{xy}\rangle\langle E^{\boldsymbol{v}}_{xy}|, \tag{6}$$

$$\begin{aligned}
|E^{\boldsymbol{v}}_{01}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\tfrac{3}{2}\gamma}|m_0\rangle + \sqrt{\tfrac{\gamma}{2}}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\right] \\
|E^{\boldsymbol{v}}_{10}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\tfrac{3}{2}\gamma}|m_0\rangle - \sqrt{\tfrac{\gamma}{2}}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\right] \\
|E^{\boldsymbol{v}}_{00}\rangle &= \frac{1}{\sqrt{2(1-v_3^2)}}\left[(-v_1v_3 - iv_2)|m_1\rangle + (-v_2v_3 + iv_1)|m_2\rangle + (1-v_3^2)|m_3\rangle\right] \\
|E^{\boldsymbol{v}}_{11}\rangle &= \frac{1}{\sqrt{2(1-v_3^2)}}\left[(-v_1v_3 + iv_2)|m_1\rangle + (-v_2v_3 - iv_1)|m_2\rangle + (1-v_3^2)|m_3\rangle\right].
\end{aligned} \tag{7}$$

The E-vectors are not all orthogonal. We have $\langle E^{\boldsymbol{v}}_{01}|E^{\boldsymbol{v}}_{10}\rangle = \frac{1-2\gamma}{1-\gamma}$. (The rest of the inner products are zero.) It holds that $|\frac{-v_1v_3-iv_2}{\sqrt{1-v_3^2}}|^2 = 1-v_1^2$ and $|\frac{-v_2v_3+iv_1}{\sqrt{1-v_3^2}}|^2 = 1-v_2^2$. We have $|E^{\boldsymbol{v}}_{10}\rangle = |E^{-\boldsymbol{v}}_{01}\rangle$ and $|E^{\boldsymbol{v}}_{11}\rangle = |E^{-\boldsymbol{v}}_{00}\rangle$. The state $|E^{\boldsymbol{v}}_{00}\rangle$ looks complicated, but the projector is given by the more simple expression $|E^{\boldsymbol{v}}_{00}\rangle\langle E^{\boldsymbol{v}}_{00}| = \frac{1}{2}\sum_{j=1}^3|m_j\rangle\langle m_j| - \frac{1}{2}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}| + i\sum_{jkp=1}^3\varepsilon_{jkp}v_j|m_k\rangle\langle m_p|$, where ε_{jkp} stands for the antisymmetric Levi-Civita symbol. For a given basis set $\mathcal{B}$ and $b\in\mathcal{B}$ we will write σ^b_{xy} instead of $\sigma^{\boldsymbol{v}}_{xy}$, as the vector $\boldsymbol{v}$ is implicitly defined by the pair $(\mathcal{B}, b)$. The following useful identity holds,

$$\mathbb{E}_{xy}\sigma^b_{xy} = (1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma}{2}\sum_{j=1}^3|m_j\rangle\langle m_j|. \tag{8}$$

3 Motivation

It is possible to add noise tolerance to the construction of Fehr and Salvail [1], but this leads to a result that is unsatisfactory in two respects. (i) For 4-state and 6-state encoding the scheme has a low rate. Even at zero noise the rate is below 1. (ii) For 8-state encoding it is

[a] For 4-state QKR an extra ingredient is needed to arrive at this expression: the use of test states so as to probe more than a circle on the Bloch sphere.

known [9] that the zero-noise rate should be 1, but the proof technique of [1] does not show it. We explain this below.

A straightforward way of adding more noise tolerance to the construction of Fehr and Salvail [1] is as follows. Alice sends to Bob an encrypted syndrome. The encryption is done with a one-time pad, i.e. a certain amount of existing key material has to be spent. Let the number of qubits be n; the length of the secret after privacy amplification is ℓ; the tolerated bit error rate is β. The proof technique in [1] is based on an entanglement monogamy game [20]. It yields a trace distance $\sqrt{2^\ell p_{\rm win}}$ between ideality and reality, where $p_{\rm win}$ is the winning probability, $p_{\rm win} \leq \mu^n 2^{nh(\beta)}$ (asymptotically), where $\mu = \frac{1}{|\mathcal{B}|} + \frac{|\mathcal{B}|-1}{|\mathcal{B}|}\sqrt{\max_{bb'\in\mathcal{B}:b'\neq b} \max_{xx'} \|F_x^b F_{x'}^{b'}\|_\infty}$. Here F_x^b is the projection operator that corresponds to data bit $x \in \{0,1\}$ in the basis b. The value of μ is given by $\mu_4 = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} \approx 0.85$, $\mu_6 = \frac{1}{3} + \frac{2}{3}\sqrt{\frac{1}{2}} \approx 0.80$, $\mu_8 = \frac{1}{4} + \frac{3}{4}\sqrt{\frac{2}{3}} \approx 0.86$ for 4-state, 6-state and 8-state encoding respectively.[b] Given that an amount $nh(\beta)$ of key material has to be spent, the asymptotic QKR rate $\frac{\ell-\text{expenditure}}{n}$ is upper bounded by $1-\log(2\mu)-2h(\beta)$. This bound on the rate is unfavourable for the 8-state case, even though it is known that QKR with 8-state encoding has good properties [9], e.g. no leakage of the qubit payload at zero noise. Our aim is to obtain a tighter bound on the rate, for all encoding schemes.

4 Our adapted 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]. We introduce a small change in the protocol:

- Some key refreshment of the basis key occurs even in case of an Accept.
- The one time pad is derived not only from the qubits' payload but also from the basis key.

The key material shared between Alice and Bob consists of four parts: a basis sequence $b \in \mathcal{B}^n$, a MAC key $k_{\rm MAC} \in \{0,1\}^\lambda$, an extractor key[c] $u \in \mathcal{U}$, and a classical OTP $k_{\rm syn} \in \{0,1\}^a$ for protecting the syndrome. The plaintext is $m \in \{0,1\}^\ell$.

Alice and Bob have agreed on a pairwise independent hash function $\texttt{Ext} : \mathcal{U} \times \{0,1\}^n \times \mathcal{B}^n \to \{0,1\}^\ell \times \mathcal{B}^n$, a MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^{n+\ell+a} \to \{0,1\}^\lambda$, and a linear error-correcting code with syndrome function $\texttt{Syn} : \{0,1\}^n \to \{0,1\}^a$ and decoder $\texttt{SynDec}$: $\{0,1\}^a \to \{0,1\}^n$. For efficiency reasons we take a one-time MAC function whose key size does not exceed the tag size.[d]

The basis set $\mathcal{B}$ and the functions $\texttt{Ext}, \Gamma, \texttt{Syn}, \texttt{SynDec}$ are publicly known.

Encryption

Alice performs the following steps. Generate random $x \in \{0,1\}^n$. Compute $s = k_{\rm syn} \oplus \texttt{Syn}(x)$ and $z||b' = \texttt{Ext}(u, x||b)$. Compute the ciphertext $c = m \oplus z$ and authentication tag $\tau = \Gamma(k_{\rm MAC}, x||c||s)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{b_i x_i}\rangle$ according to Section 2.5. Send $|\Psi\rangle$, s, c, τ to Bob.

[b] We note that the $p_{\rm win}$ obtained numerically with Semidefinite Programming is the same for 6-state and 8-state.

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

[d] Alternatively, it is an arbitrary information-theoretically secure MAC and the MAC key is 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.

Decryption
Bob receives $|\Psi'\rangle$, s', c', τ'. He performs the following steps. Measure $|\Psi'\rangle$ in the b-basis. This yields $x' \in \{0,1\}^n$. Recover $\hat{x} = x' \oplus \mathtt{SynDec}(k_{\mathrm{syn}} \oplus s' \oplus \mathtt{Syn}\, x')$. Compute $\hat{z}||b'' = \mathtt{Ext}(u, \hat{x}||b)$ and $\hat{m} = c' \oplus \hat{z}$. Accept only if $\tau' = \Gamma(k_{\mathrm{MAC}}, \hat{x}||c'||s')$ holds and the syndrome decoding was successful. Communicate Accept/Reject to Alice (publicly but with authentication).
Key update
Alice and Bob perform the following actions.

- In case of Reject: Take new keys $k_{\mathrm{syn}}, k_{\mathrm{MAC}}, b, u$.
- In case of Accept: Take new keys k_{syn} and k_{MAC}. The key u is re-used. Alice replaces b by b'. Bob replaces b by b''.

The replacement of k_{MAC} consumes a small constant amount of existing secret key material shared between Alice and Bob. The replacement of k_{syn} on the other hand consumes a noise-dependent amount of key material proportional to n. See Section 5.6 for a discussion of the balance between message length and key expenditure.

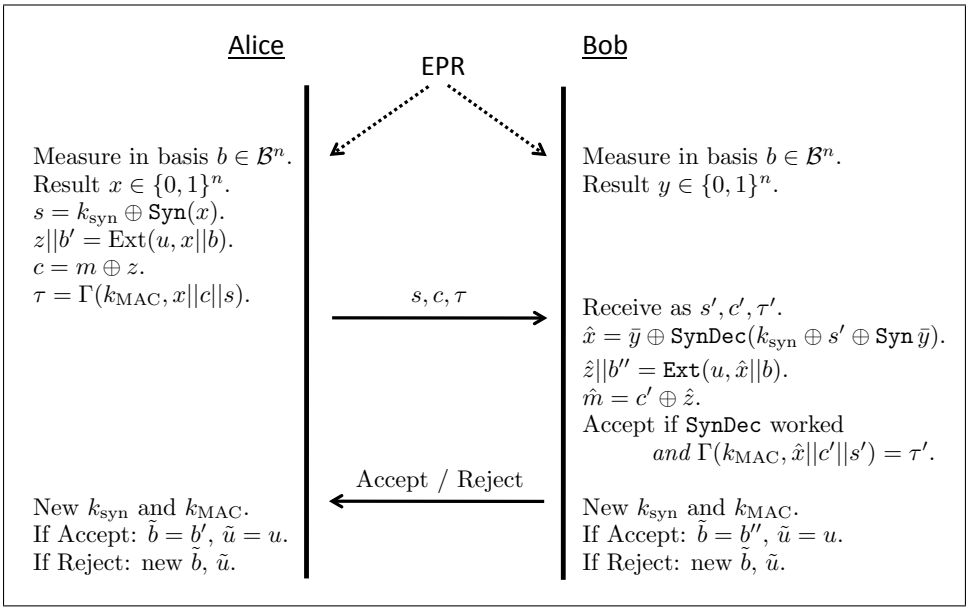

Fig. 1. *EPR version of the QKR protocol. The EPR pairs are in the singlet state.*

5 Main result

5.1 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.

We work with the EPR version of the protocol (Fig. 1). The protocol steps are practically the same as in Section 4. The only difference is that Alice does not prepare the state $|\Psi\rangle$;

instead Eve hands the parts of a noisy EPR pair to Alice and Bob whereupon Alice performs a measurement in the b-basis, resulting in a state $|\Psi\rangle$ with random payload x.

First we consider attacks where Eve entangles her quantum system with individual EPR pairs. Eve is allowed to postpone measurements. For this limited class of attacks we derive a bound (Theorems 1 and 2) on the trace distance between the real state and an ideal state, as explained in Section 2.3. Finally we invoke post-selection to extend the validity of the security proof to general attacks.

In Section 5.4 we present an asymptotic result for $n \to \infty$. We follow proof steps as in [13, 14]. Smoothing is introduced, after which the trace distance is upperbounded in a number of steps. First the trace operation and the average over the hashing key u are pulled into the square root using Jensen's inequality; then the properties of pairwise independent hashes are used to evaluate the average over u; this results in an expression that can be written in terms of smooth Rényi entropies S_0^ε and S_2^ε. Finally Lemma 1 is invoked to make the transition from smooth Rényi entropies to non-smooth von Neumann entropies, which are then easily evaluated.

In Section 5.5 we present a non-asymptotic result without smoothing. The proof follows similar steps up to and including the average over u, except that the trace operation is kept outside the square root. The operator square root is evaluated explicitly, which is feasible because of the diagonal form of the operator. No use is made of entropies.

5.2 What to prove

Alice and Bob's shared key material consists of $k_{\rm syn}, k_{\rm MAC}, b, u$. The only keys open to attack are b and u, since $k_{\rm syn}$ and $k_{\rm MAC}$ get discarded after each round. Eve's classical side information consists of s (OTP'ed syndrome), τ (authentication tag), the ciphertext $c = z \oplus m$, and the Accept/Reject bit. The s and τ carry no information about b, u, x. Hence we will need to prove (i) that μ, b, u are safe given c, the Accept/Reject bit and Eve's quantum side information; (ii) that b, u are safe given c, known plaintext m, the Accept/Reject bit and Eve's quantum side information.

Eve's quantum side information consists of her ancilla particles which have interacted with the EPR pairs. The state of the i'th ancilla depends on x_i, y_i, b_i and is given by the 4-dimensional matrix $\sigma^{b_i}_{x_i y_i}$ as specified in (6). We introduce the binary variable Ω, with $\Omega = 1$ indicating that Alice receives a properly authenticated Accept message from Bob. The keys after execution of one QKR round are denoted with a tilde, i.e. $\tilde{u}, \tilde{b}$. We work with quantum-classical states; each classical variable is assigned a quantum register, indicated as a capital-letter superscript on the state ρ. Eve's ancillas are denoted as the subsystem "E". The two quantities of interest are the trace distances $\|\rho^{\tilde{B}\tilde{U}MC\Omega E} - \mu^{\tilde{B}\tilde{U}M} \otimes \rho^{C\Omega E}\|_1$ and $\|\rho^{\tilde{B}\tilde{U}MC\Omega E} - \mu^{\tilde{B}\tilde{U}} \otimes \rho^{MC\Omega E}\|_1$. Below we will see that they reduce to the same expression.

We introduce a binary variable θ_{xy} which indicates whether the error correction succeeds.

$$\theta_{xy} \stackrel{\rm def}{=} \begin{cases} 1 & \text{if Hamm}(x \oplus \bar{y}) \leq t \\ 0 & \text{otherwise} \end{cases} . \tag{9}$$

(Note that $\bar{y}$ appears instead of y, because of the *anti*-correlation in the singlet state.) We write $p_{xy} = p_x p_{y|x}$ with $p_x = 2^{-n}$ and $p_{y|x} = \gamma^{|x \oplus \bar{y}|}(1-\gamma)^{n-|x\oplus\bar{y}|}$. The probability that the

error correction succeeds is given by

$$P_{\mathrm{corr}}(t,\gamma) = \sum_{xy} p_{xy}\theta_{xy} = \sum_{c=0}^{t} \binom{n}{c} \gamma^c (1-\gamma)^{n-c}. \tag{10}$$

Alice will re-use keys ($\Omega = 1$) if she receives an authenticated Accept bit from Bob. The probability of this event can be bounded as $P_{\mathrm{acc}}(t,\gamma) \leq P_{\mathrm{corr}}(t,\gamma) + 2 \cdot 2^{-\lambda}$. Here λ is the size of the authentication tag. One term $2^{-\lambda}$ comes from the possibility that Eve forges Alice's MAC. Another term $2^{-\lambda}$ comes from the possibility that Eve forges Bob's MAC on a Reject message and turns it into an Accept message. In the rest of the paper we will ignore these MAC forgery complications when writing down states, but it is understood that we will always have to add a term $2 \cdot 2^{-\lambda}$ to the trace distance.

5.3 Description of the state

We introduce notation $\mathbb{E}_b \stackrel{\mathrm{def}}{=} \sum_{b\in\mathcal{B}^n} |\mathcal{B}|^{-n}$, $\mathbb{E}_u \stackrel{\mathrm{def}}{=} \sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|}$, and in slight abuse of notation we define $\mathbb{E}_{\tilde{b}}, \mathbb{E}_{\tilde{u}}$ in the same way. Furthermore we introduce $\mathbb{E}_{xy} \stackrel{\mathrm{def}}{=} \sum_{x,y\in\{0,1\}^n} p_{xy}$. The full quantum-classical state of all the relevant classical variables and Eve's system together is

$$\begin{aligned}\rho^{BB'\tilde{B}U\tilde{U}MXYZC\Omega E} \quad = \quad & \mathbb{E}_{bumxy} \sum_{b'\tilde{b}\tilde{u}cz\omega} \delta_{z||b',\mathrm{Ext}(u,x||b)} \delta_{c,m\oplus z} [\delta_{\omega 1}\theta_{xy}\delta_{\tilde{b}b'}\delta_{\tilde{u}u} + \frac{\delta_{\omega 0}\overline{\theta_{xy}}}{|\mathcal{B}^n \times \mathcal{U}|}] \\ & |bb'\tilde{b}u\tilde{u}mxyzc\omega\rangle\langle bb'\tilde{b}u\tilde{u}mxyzc\omega| \otimes \rho^E_{bxy}. \end{aligned} \tag{11}$$

Here the case of successful error correction ($\theta_{xy} = 1$) leads to Accept ($\omega = 1$), key re-use $\tilde{u} = u$ and refresh $b \mapsto \tilde{b} = b'$. Failure of the error correction yields a Reject and completely random keys $\tilde{b}, \tilde{u}$ (the factor $1/|\mathcal{B}^n \times \mathcal{U}|$).

Note that in (11) we have written ρ^E_{bxy} without dependence on the classical variable c, which is in principle available to Eve at the moment when she creates the "E" subsystem. (And m, z in case of known plaintext). We are allowed to do this because the pairwise independent hash function Ext completely decouples x from z. It holds that $\Pr_U[Z = z|X = x, B = b] = 2^{-\ell}$, where U is the random variable. This implies that X given Z is also uniform. When Eve acts on the individual EPR pairs, she has no information that could lead her to treat any position $i \in [n]$ differently from the other positions. Thus we have $\rho^E_{bxy} = \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i}$, with σ^b_{xy} as defined in (6).[e]

By applying the appropriate partial traces to (11) we get

$$\rho^{\tilde{B}\tilde{U}MC\Omega E} \quad = \quad \mathbb{E}_{\tilde{b}\tilde{u}m} \sum_{c\omega} 2^{-\ell} |\tilde{b}\tilde{u}mc\omega\rangle\langle\tilde{b}\tilde{u}mc\omega| \otimes [\delta_{\omega 1}\rho^E_{\tilde{b}\tilde{u}mc,\omega=1} + \delta_{\omega 0}\rho^E_{\tilde{b}\tilde{u}mc,\omega=0}] \tag{12}$$

$$\rho^E_{\tilde{b}\tilde{u}mc,\omega=1} \quad = \quad \mathbb{E}_{xy}\theta_{xy} 2^{\ell} \sum_{b} \delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x||b)} \rho^E_{bxy} \tag{13}$$

$$\rho^E_{\tilde{b}\tilde{u}mc,\omega=0} \quad = \quad \mathbb{E}_{xy}\overline{\theta_{xy}}\mathbb{E}_b \rho^E_{bxy} \tag{14}$$

[e] One may want to formally write ρ^E_{bxycm} instead of ρ^E_{bxy}. Then this notation can be kept in the derivation below up to (27), where it becomes necessary to use the fact that the ancilla states do not actually depend on c and m.

and further tracing yields

$$\rho^{MC\Omega E} = \mu^{MC} \otimes \sum_{\omega} |\omega\rangle\langle\omega| \otimes [\delta_{\omega 1}\rho^E_{\omega=1} + \delta_{\omega 0}\rho^E_{\omega=0}], \tag{15}$$

$$\rho^E_{\omega=1} = \mathbb{E}_{xy}\theta_{xy}\mathbb{E}_b\rho^E_{bxy} \tag{16}$$

$$\rho^E_{\omega=0} = \mathbb{E}_{xy}\overline{\theta_{xy}}\mathbb{E}_b\rho^E_{bxy}. \tag{17}$$

Here we have used the property $\mathbb{E}_u\delta_{z||b',\mathrm{Ext}(u,x||b)} = 2^{-\ell}|\mathcal{B}|^{-n}$ of the pairwise independent hash function. Note that $\mu^{\tilde{B}\tilde{U}M} \otimes \rho^{C\Omega E} = \mu^{\tilde{B}\tilde{U}} \otimes \rho^{MC\Omega E}$, which means that the security of $\tilde{B}\tilde{U}M$ given $C\Omega E$ is the same as the security of $\tilde{B}\tilde{U}$ given $MC\Omega E$.

5.4 Asymptotic result

Theorem 1 *Consider one round of the QKR protocol (Section 4) with 6-state or 8-state encoding. Let Eve cause noise described by parameter γ as discussed in Section 2.6. Let t be the number of errors that can be corrected by the error-correcting code. In the limit $n \to \infty$ it holds that*

$$d(\tilde{B}\tilde{U}|MC\Omega E) \leq 2^{1-\lambda} + \min\left(P_{\mathrm{corr}}(t,\gamma),\ \sqrt{2^{\ell-1-n+nh(\{1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}\})-nh(\gamma)}}\right) \tag{18}$$

with P_{corr} as defined in (10).

Let $\beta \stackrel{\mathrm{def}}{=} t/n$. For $\gamma > \beta$ the probability P_{corr} is exponentially small. For $\gamma \leq \beta$, the second expression can be made exponentially small for $\ell < n + nh(\gamma) - nh(\{1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}\})$.

Asymptotically the length of the syndrome is $a = nh(\beta)$, and the $\mathcal{O}(\log n)$ contribution from post-selection (Section 2.4) becomes negligible compared to n. The QKR rate $\frac{\ell-a-\mathcal{O}(\log n)}{n}$ goes to

$$\text{asymptotic rate} = 1 - h(\{1-\tfrac{3}{2}\beta,\tfrac{\beta}{2},\tfrac{\beta}{2},\tfrac{\beta}{2}\}), \tag{19}$$

which is exactly the asymptotic rate of 6-state QKD.

Proof of Theorem 1: First of all there is the contribution $2^{1-\lambda}$ from the possibility of forging the MACs, as explained in Section 5.2. Next we write $D \stackrel{\mathrm{def}}{=} \|\rho^{\tilde{B}\tilde{U}MC\Omega E} - \mu^{\tilde{B}\tilde{U}} \otimes \rho^{MC\Omega E}\|_1$. We introduce smoothing as in [13, 10, 14] by allowing states $\bar{\rho}$ that are ε-close to ρ in terms of trace distance. This yields $D \leq 2\varepsilon + \bar{D}$, with $\bar{D} \stackrel{\mathrm{def}}{=} \|\bar{\rho}^{\tilde{B}\tilde{U}MC\Omega E} - \mu^{\tilde{B}\tilde{U}} \otimes \bar{\rho}^{MC\Omega E}\|_1$. Substituting (12,15) into this expression gives[f]

$$\bar{D} = \mathbb{E}_{\tilde{b}\tilde{u}mc}\|\bar{\rho}^E_{\tilde{b}\tilde{u}mc,\omega=1} - \bar{\rho}^E_{\omega=1}\|_1. \tag{20}$$

In slight abuse of notation we have written $\mathbb{E}_c(\cdots) \stackrel{\mathrm{def}}{=} \sum_c 2^{-\ell}(\cdots)$. The $\bar{\rho}^E_{\tilde{b}\tilde{u}mc,\omega=1}$ and $\bar{\rho}^E_{\omega=1}$ are both sub-normalised states; their trace equals $P_{\mathrm{corr}}(t,\gamma)$. Hence it holds that $\bar{D} \leq 2P_{\mathrm{corr}}(t,\gamma)$. This corresponds to the first expression in the 'min' in (18). For $\gamma \leq t/n$ we

[f] The $\omega = 0$ part disappears, since the Reject event of the real protocol is identical to the Reject in the 'ideal' case. Even in case of a Reject the plaintext M is secure; no matter how much leaks about X, the X is masked by U, which is then discarded.

derive a bound as follows.

$$\begin{aligned}
\bar{D} &\leq \mathbb{E}_{\tilde{b}\tilde{u}mc}\|\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E\|_1 = \mathbb{E}_{\tilde{b}\tilde{u}mc}\mathrm{tr}\sqrt{(\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E)^2} && (21)\\
&\overset{\text{Jensen}}{\leq} \mathbb{E}_{\tilde{b}\tilde{u}mc}\sqrt{\mathrm{rank}([\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E]^2)}\sqrt{\mathrm{tr}\,(\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E)^2} && (22)\\
&\leq \sqrt{2\mathrm{rank}(\bar{\rho}^E)}\mathbb{E}_{\tilde{b}\tilde{u}mc}\sqrt{\mathrm{tr}\,(\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E)^2} && (23)\\
&\overset{\text{Jensen}}{\leq} \sqrt{2\mathrm{rank}(\bar{\rho}^E)}\sqrt{\mathrm{tr}\,\mathbb{E}_{\tilde{b}\tilde{u}mc}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E)^2} && (24)\\
&= \sqrt{2\mathrm{rank}(\bar{\rho}^E)}\sqrt{\mathrm{tr}\,\mathbb{E}_{\tilde{b}\tilde{u}mc}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc})^2 - \mathrm{tr}\,(\bar{\rho}^E)^2}. && (25)
\end{aligned}$$

In (23) we used that $\mathrm{rank}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc} - \bar{\rho}^E) \leq \mathrm{rank}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc}) + \mathrm{rank}(\bar{\rho}^E)$ and[g] $\mathrm{rank}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc}) \leq \mathrm{rank}(\bar{\rho}^E)$. From the properties of two-universal hash functions we get

$$\begin{aligned}
\mathrm{tr}\,\mathbb{E}_{\tilde{u}}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc})^2 &= \mathrm{tr}\,\mathbb{E}_{xx'}\sum_{bb'}[2^{2\ell}\mathbb{E}_{\tilde{u}}\delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x||b)}\delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x'||b')}]\bar{\rho}^E_{bx}\bar{\rho}^E_{b'x'} && (26)\\
&= \mathrm{tr}\,\mathbb{E}_{xx'}\sum_{bb'}[|\mathcal{B}|^{-2n} + \delta_{bb'}\delta_{xx'}(2^\ell|\mathcal{B}|^{-n} - |\mathcal{B}|^{-2n})]\bar{\rho}^E_{bx}\bar{\rho}^E_{b'x'} && (27)\\
&= \mathrm{tr}\,(\bar{\rho}^E)^2 + (2^\ell|\mathcal{B}|^n - 1)\mathrm{tr}\,\mathbb{E}_{bx}\mathbb{E}_{b'x'}|bx\rangle\langle bx||b'x'\rangle\langle b'x'| \otimes \bar{\rho}^E_{bx}\bar{\rho}^E_{b'x'} && (28)\\
&= \mathrm{tr}\,(\bar{\rho}^E)^2 + (2^\ell|\mathcal{B}|^n - 1)\mathrm{tr}\,(\bar{\rho}^{BXE})^2. && (29)
\end{aligned}$$

Substitution into (25) gives

$$\begin{aligned}
\bar{D} &< \sqrt{2^{\ell+1}|\mathcal{B}|^n\mathrm{rank}(\bar{\rho}^E)\mathrm{tr}\,(\bar{\rho}^{BXE})^2} && (30)\\
&= \sqrt{2^{\ell+1}|\mathcal{B}|^n 2^{S_0(\bar{\rho}^E) - S_2(\bar{\rho}^{BXE})}} = \sqrt{2^{\ell+1}|\mathcal{B}|^n 2^{S_0^\varepsilon(\rho^E) - S_2^\varepsilon(\rho^{BXE})}} && (31)\\
&= \sqrt{2^{\ell+1}|\mathcal{B}|^n 2^{S_0^\varepsilon([\mathbb{E}_{bxy}\sigma^b_{xy}]^{\otimes n}) - S_2^\varepsilon([\mathbb{E}_{bxy}|bx\rangle\langle bx|\otimes\sigma^b_{xy}]^{\otimes n})}} && (32)\\
&\overset{\text{Lemma 1}}{\to} \sqrt{2^{\ell+1}|\mathcal{B}|^n 2^{nS(\mathbb{E}_{bxy}\sigma^b_{xy}) - nS(\mathbb{E}_{bxy}|bx\rangle\langle bx|\otimes\sigma^b_{xy})}}. && (33)
\end{aligned}$$

(In the last two lines we have $x, y \in \{0,1\}$ and $b \in \mathcal{B}$ in contrast to the previous lines.) From (8) we have $S(\mathbb{E}_{bxy}\sigma^b_{xy}) = h(\{1 - \frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\}) = -(1 - \frac{3}{2}\gamma)\log(1 - \frac{3}{2}\gamma) - 3\frac{\gamma}{2}\log\frac{\gamma}{2}$ and

$$\begin{aligned}
S(\mathbb{E}_{bxy}|bx\rangle\langle bx| \otimes \sigma^b_{xy}) &= S(BX) + \mathbb{E}_{bx}S(\mathbb{E}_y\sigma^b_{xy}) && (34)\\
&= \log|\mathcal{B}| + 1 + \mathbb{E}_{bx}S([1-\gamma]\sigma^b_{x\bar{x}} + \gamma\sigma^b_{xx}) && (35)\\
&= \log|\mathcal{B}| + 1 + h(\gamma). && (36)
\end{aligned}$$

In the last line we used that the projectors $\sigma^b_{x\bar{x}}$ and σ^b_{xx} are orthogonal to each other. □

Note that the description of Eve's ancilla state in Section 2.6 is valid for 4-state (BB84) encoding under the condition that test states are used which probe the whole Bloch sphere; then the QKR rate is given by (19). If only the xz-plane of the Bloch sphere is involved in the protocol, then (33) still holds, but with different σ^b_{xy} matrices, yielding a QKR rate equal to the BB84 QKD rate.

[g] This holds because $\bar{\rho}^E$ is a sum of many terms $\bar{\rho}^E_{\tilde{b}\tilde{u}mc}$.

5.5 Non-asymptotic result without smoothing

We want to have a bound on $d(\tilde{B}\tilde{U}|MC\Omega E)$ also for finite n. One approach would be to start from (32) and analyse the smooth entropies S_0^ε and S_2^ε for finite n and ε, and minimise over ε. However, that is a cumbersome procedure. Below we present a less tight but easier to derive bound, obtained by setting ε to zero.

Theorem 2 *Consider one round of the QKR protocol (Section 4). Let Eve cause noise described by parameter γ as discussed in Section 2.6. Let t be the number of errors that can be corrected by the error-correcting code. Let the function f be defined as*

$$f(\gamma) \stackrel{\text{def}}{=} \sqrt{(1-\tfrac{3}{2}\gamma)(1-\gamma)} + \sqrt{\tfrac{3}{2}\gamma(1+\gamma)}. \tag{37}$$

The trace distance between the real state and the ideal state can be bounded as

$$d(\tilde{B}\tilde{U}|MC\Omega E) \leq 2^{1-\lambda} + \min\left\{P_{\text{corr}}(t,\gamma),\ \tfrac{1}{2}\sqrt{2^{\ell-n+2n\log f(\gamma)}}\right\}. \tag{38}$$

For large γ the probability $P_{\text{corr}}(t,\gamma)$ is exponentially small in n. Note that $2\log f(\gamma) \in [0,1)$ for $\gamma \in [0,\frac{1}{2})$. For any $\gamma < \frac{1}{2}$ it is possible to choose ℓ such that the $\sqrt{\cdots}$ in (38) becomes exponentially small in n. However, this is only half of the story, because the QKR rate is obtained by subtracting the key expenditure from ℓ.

Proof of Theorem 2: We follow the proof of Theorem 1 up to (21) but without smoothing ($\varepsilon = 0$). Using Jensen's inequality for concave operators we write

$$\mathbb{E}_{\tilde{u}}\sqrt{(\rho^E_{b\tilde{u}mc} - \rho^E)^2} \quad\leq\quad \sqrt{\mathbb{E}_{\tilde{u}}(\rho^E_{b\tilde{u}mc} - \rho^E)^2} = \sqrt{\mathbb{E}_{\tilde{u}}(\rho^E_{b\tilde{u}mc})^2 - (\rho^E)^2}. \tag{39}$$

The last equality holds because $\mathbb{E}_{\tilde{u}}\rho^E_{b\tilde{u}mc} = \rho^E$. Next we use (27), but without the trace. This gives

$$D \quad\leq\quad \sqrt{2^{\ell-n}}\,\text{tr}\,\sqrt{\mathbb{E}_{bx}(\rho^E_{bx})^2}. \tag{40}$$

Next we show that the expression under the square root is diagonal. Using $\rho^E_{bx} = \bigotimes_i\{(1-\gamma)\sigma^{b_i}_{x_i\overline{x_i}} + \gamma\sigma^{b_i}_{x_ix_i}\}$ and the orthogonality $\sigma^b_{x\bar{x}}\sigma^b_{xx} = 0$ we get

$$\begin{aligned}
\mathbb{E}_{bx}(\rho^E_{bx})^2 &= \bigotimes_{i=1}^n\left\{(1-\gamma)^2\mathbb{E}_{b_i}\frac{\sigma^{b_i}_{01}+\sigma^{b_i}_{10}}{2} + \gamma^2\mathbb{E}_{b_i}\frac{\sigma^{b_i}_{00}+\sigma^{b_i}_{11}}{2}\right\} &(41)\\
&= \left\{(1-\gamma)\Big[(1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma}{6}\sum_{j=1}^3|m_j\rangle\langle m_j|\Big] + \tfrac{\gamma^2}{3}\sum_{j=1}^3|m_j\rangle\langle m_j|\right\}^{\otimes n} &(42)\\
&= \left\{(1-\gamma)(1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma(1+\gamma)}{6}\sum_{j=1}^3|m_j\rangle\langle m_j|\right\}^{\otimes n} &(43)
\end{aligned}$$

from which it follows that

$$\text{tr}\,\sqrt{\mathbb{E}_{bx}(\rho^E_{bx})^2} = \left\{\sqrt{(1-\gamma)(1-\tfrac{3}{2}\gamma)} + \sqrt{\tfrac{3}{2}\gamma(1+\gamma)}\right\}^n. \tag{44}$$

□

Theorem 3 *Consider the context of Theorem 2. Let $\beta = t/n$. Let σ be a security parameter. Let ℓ be chosen as*

$$\ell \leq n - 2n\log f(\beta) - 2\xi\sqrt{\sigma n} - 2\sigma - 1 \tag{45}$$

$$\xi \stackrel{\text{def}}{=} \min\left\{\frac{f'(\beta)}{f(\beta)}\left[\sqrt{\frac{2\beta}{\ln 2}+\frac{\sigma}{n}}+\sqrt{\frac{\sigma}{n}}\right], \quad \frac{\sqrt{3}}{\ln 2}\right\}. \tag{46}$$

Then

$$d(\tilde{B}\tilde{U}|MC\Omega E) \leq 2\cdot 2^{-\lambda} + 2^{-\sigma}. \tag{47}$$

Proof: See Appendix 1.

If according to (45) the length ℓ becomes negative then this means that the desired security level σ cannot be achieved.

A typical choice for the tag length would be $\lambda = \sigma + 1$, yielding $2/2^{\sigma}$ in the right hand side of (47). Several things are worth noting.

- The ξ is of order 1. Hence the term $\xi\sqrt{\sigma n}$ scales as $\sqrt{n}$.
- The function f is concave. There is no advantage for Eve in choosing a position-dependent noise level γ_i instead of the same noise level γ for all $i \in [n]$.
- Analysis of QKD instead of QKR using the same technique yields a result similar to Theorem 2, but with a slightly more favourable function instead of $f(\gamma)$, namely $\sqrt{(1-\gamma)(1-\frac{3}{2}\gamma)}+\sqrt{\frac{1}{2}\gamma(1-\gamma)}+\gamma\sqrt{2}$. (We mention this without showing the proof.) Nevertheless, the asymptotics of QKD and QKR are the same.

As explained in Section 2.4, by invoking post-selection we can 'buy' security against general attacks by reducing the message length ℓ a bit. The bound (38) changes by a factor $(n+1)^{15}$, which can be compensated by shrinking ℓ from (45) to

$$\ell \leq n - 2n\log f(\beta) - 2\xi\sqrt{\sigma n} - 2\sigma - 1 - 30\log(n+1). \tag{48}$$

5.6 Non-asymptotic QKR rate; Choosing the parameter values

We want to characterize the non-asymptotic performance of our QKR scheme under ideal circumstances. Consider a sequence of QKR rounds with a large number of consecutive Accepts. Let $\eta = 2\cdot 2^{-\lambda} + 2^{-\sigma}$ be the 'imperfection' induced by one round of QKR. Let θ be the maximum distance that Alice and Bob are willing to tolerate between reality and the ideal state $\rho^{(0)}$. After $N = \lfloor\theta/\eta\rfloor$ rounds they have to refresh *all* their key material. The QKR rate is

$$\text{rate} = \frac{\text{total message data sent in } N \text{ rounds} - \text{expended key material}}{N\cdot n}. \tag{49}$$

The total message size is $N\ell$, with ℓ specified in (48). The total key expenditure consists of N times two λ-bit authentication tags, N a-bit OTPs that protect the syndromes (asymptotically $a \approx nh(\beta)$), $n\log|\mathcal{B}|$ bits of basis key b, and n bits of extractor key u. This gives

$$\text{rate} = 1 - \frac{a}{n} - 2\log f(\beta) - \frac{2\xi\sqrt{\sigma}}{\sqrt{n}} - \frac{30\log(n+1)}{n} - \frac{2\lambda+2\sigma}{n} - \frac{1+\log|\mathcal{B}|}{N}. \tag{50}$$

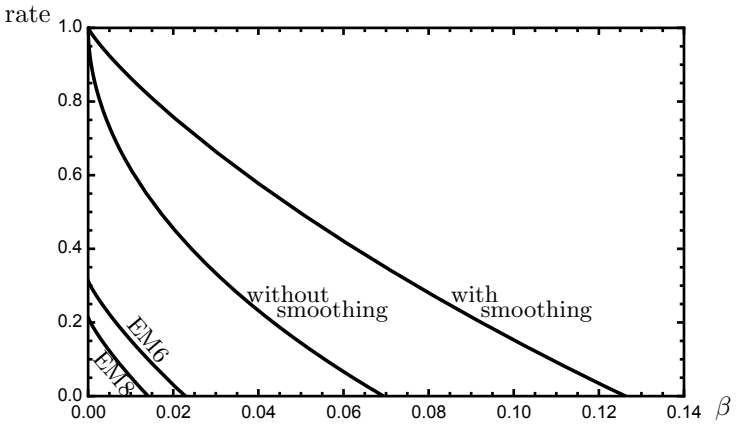

Fig. 2. *Asymptotic QKR rates. The 'with smoothing' curve is the result (19). The 'without smoothing' curve is the result* $1 - h(\beta) - 2\log f(\beta)$ *obtained without smoothing. The 'EM6' and 'EM8' curves correspond to the bound* $1 - \log(2\mu) - 2h(\beta)$ *based on Entanglement Monogamy, with constants* $\mu = \mu_6$ *and* $\mu = \mu_8$ *respectively (see Section 3).*

Note that η can be made exponentially small (N exponentially large) by increasing λ and σ.

For large n and N the rate (50) tends to $1 - h(\beta) - 2\log f(\beta)$, which is lower than the asymptotic result of Section 5.4. The discrepancy is of course caused by the fact that we did not use smoothing in Theorem 2. Fig. 2 shows the asymptotic (QKR=QKD) rate (19) as well as the $\varepsilon = 0$ rate (50) in the limit $n \to \infty, N \to \infty$ and the rates obtained from the Entanglement Monogamy approach (Section 3). Obviously smoothing improves the tightness of the provable bounds significantly. Furthermore it is also clear that the Entanglement Monogamy bounds are very far from tight.

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 (50).

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

Furthermore, it is possible to send keys *for the next round* ($k_{\rm syn}$ and the two MAC-padding OTPs) as part of the payload *in the current round*. This trick completely nullifies the key expenditure in case of Accept, but reduces the message size by $a + 2\lambda$. The rate is unaffected.

Typically θ is fixed. Then it remains to tune N (which via $\eta = \theta/N$ fixes σ) and n for fixed (θ, β) so as to optimise the rate. In Fig. 3 the non-asymptotic rate is plotted for $\theta = 2^{-256}$ and various values of β, N and n. We see that the asymptotic rate can be approached well for realistic values of N and n.

6 Discussion

6.1 Comparison to existing results

The proof technique of [1] requires a special 'key privacy' property of the MAC function, and has to keep track of the security of the MAC key. We avoid this requirement at the cost of spending λ additional bits of key. An interesting difference with respect to [1] is that we

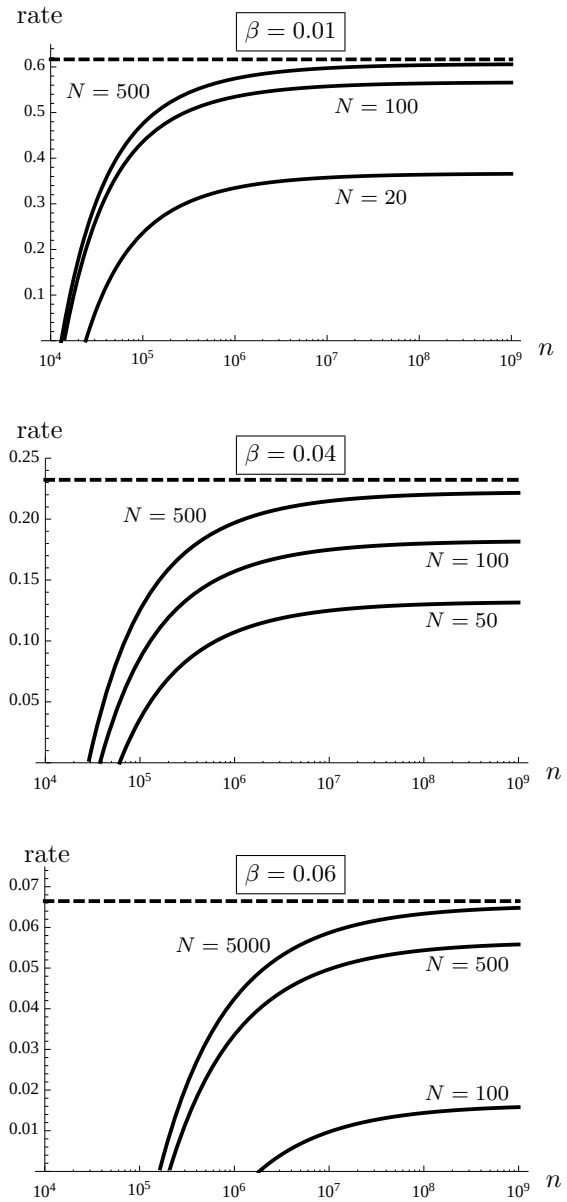

Fig. 3. *Non-asymptotic bound on the QKR rate as a function of the number of qubits (n), for various values of the design parameter N and tolerated noise β. The dashed lines indicate the $\varepsilon = 0$ limit $1 - h(\beta) - 2\log f(\beta)$. $\lambda = \sigma + 1$; $\theta = 2^{-256}$; the syndrome length a is set to $nh(\beta) + \sqrt{n}\Phi^{\mathrm{inv}}(10^{-6})\sqrt{\beta(1-\beta)}\log\frac{1-\beta}{\beta}$ (see e.g. [21]), where Φ is defined as $\Phi(z) \stackrel{\mathrm{def}}{=} \int_z^\infty (2\pi)^{-1/2}\exp[-x^2/2]\mathrm{d}x$.*

capture the security of the basis key B and the extractor key U in a single quantity (a single trace distance), whereas [1] uses a min-entropy result for B and a trace distance for U.

We compare our result to the min-entropy analysis of attacks in [9]. 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 more than our leakage result $2\log f(\beta)$. We conclude that non-smooth min-entropy is too pessimistic as a measure of security in this context.

It was pointed out in [2, 9] that with 8-state encoding there is no leakage about the qubit payload X, whereas 6-state and BB84 encoding allow Eve to learn a lot about X in case of a Reject. One may conclude that more privacy amplification is needed for 6-state and BB84 encoding than for 8-state. However, it turns out that the situation is the same for all encoding schemes: the privacy amplification key U adequately masks X and gets replaced upon Reject.

6.2 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 4 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 $n\cdot 2\log f(\beta)$ 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 4 simply does not work. (Note that continuous-variable schemes do not have erasures but instead have large β.)

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 $x\in\{0,1\}^q$ encoded in q qubits, with $q(1-\eta)>n$.
2. Bob receives qubits in positions $i\in\mathcal{I}$, $\mathcal{I}\subseteq[q]$ 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 $s'=k_{\rm syn}\oplus S(y')$, $z'||b'=\texttt{Ext}(u,y'||b)$, $c'=m\oplus z'$, $t'=\Gamma(k_{\rm MAC},\mathcal{J}'||y'||c'||s')$. He sends $\mathcal{J}',s',c',t'$.
3. Alice receives this data as $\mathcal{J},s,c,t$. She computes y by doing error correction on $x_{\mathcal{J}}$ aided by the syndrome $k_{\rm syn}\oplus s$. Then she computes $z||b''=\texttt{Ext}(u,y||b)$, $\hat{m}=z\oplus c$ and $\tau=\Gamma(k_{\rm MAC},\mathcal{J}||y||c||s)$. Alice Accepts the message $\hat{m}$ if $\tau=t$ and Rejects otherwise.[h] Key refreshment is as in the original protocol.

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.

[h] Alice may send the (authenticated) Accept/Reject bit along with the next batch of qubits; then the protocol has only two rounds.

6.3 Future work

It is possible to evaluate or bound the $S_0^\varepsilon(\rho^E)$ and $S_2^\varepsilon(\rho^{BXE})$ in (31) for finite n and ε 'by hand', i.e. specifically for $\rho^E_{bxy} = \otimes_{i=1}^n \sigma^{b_i}_{x_i y_i}$. That would yield a non-asymptotic result for ℓ that is more favorable than Theorem 3.

It is interesting to note that QKR protocols which derive an OTP z from the qubit payload and then use z for 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 4 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 5.6, 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 it 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 slightly improve the rate (50) by reducing the amortised cost of refreshing b from $\frac{2}{N}$ to approximately $\frac{1}{N}$.

Finally, various tricks known from QKD may be applied to improve the noise tolerance of QKR, e.g. artificial noise added by Alice.

Acknowledgements

We thank Serge Fehr and Niek Bouman for helpful discussions. We thank the anonymous reviewers of Asiacrypt for pointing out a flaw in a previous version. 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). *Int. J. of Quantum Information*, 2017.
3. C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE Int. Conf. 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. *Security of quantum key distribution.* PhD thesis, ETH Zürich, 2005.

11. R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.
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. R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.
14. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.
15. 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.
16. D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.
17. 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.
18. D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.
19. P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.
20. M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. One-sided device-independent QKD and position-based cryptography from monogamy games. In *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 609–625, 2013.
21. D. Baron, M.A. Khojastepour, and R.G. Baraniuk. How quickly can we approach channel capacity? In *Asilomar Conf. on Signals, Systems and Computers*, pages 1096–1100. IEEE, 2004.

Appendix A: Proof of Theorem 3

We (implicitly) define a function $\gamma_{\max}(t,\sigma)$ as $P_{\rm corr}(t,\gamma_{\max}) = 2^{-\sigma}$. For $\gamma \geq \gamma_{\max}$ eq. (47) clearly holds. Next we need to bound the expression $\log f(\gamma)$ for $\gamma \leq \gamma_{\max}$. Taking the Chernoff bound $P_{\rm corr}(t,\gamma) \leq \exp[-\frac{n}{2\gamma}(\gamma - \frac{t}{n})^2]$ and solving for γ we get

$$\gamma_{\max}(t,\sigma) \leq \gamma_0(t,\sigma) \stackrel{\rm def}{=} \frac{t}{n} + \frac{\sigma \ln 2}{n} + \sqrt{2\frac{t}{n}\frac{\sigma \ln 2}{n} + (\frac{\sigma \ln 2}{n})^2}. \tag{A.1}$$

We will bound the expression $\log f(\gamma_0)$ in two different ways: for 'large' β and for 'small' β.

- As f is a concave function we have $f(\gamma_0) \leq f(\beta) + (\gamma_0 - \beta)f'(\beta)$. This yields

$$\begin{aligned} \log f(\gamma_0) &\leq \log f(\beta) + \log[1 + \frac{f'(\beta)}{f(\beta)}(\gamma_0 - \beta)] \leq \log f(\beta) + \frac{f'(\beta)}{f(\beta)}\frac{\gamma_0 - \beta}{\ln 2} \\ &= \log f(\beta) + \frac{\sigma}{n} + \sqrt{2\beta\frac{\sigma}{n\ln 2} + (\frac{\sigma}{n})^2}. \end{aligned} \tag{A.2}$$

- We write $\log f(\gamma_0) = \log f(\beta) + \log \frac{f(\gamma_0)}{f(\beta)} \leq \log f(\beta) + \log \frac{f(\gamma_0)}{f(\beta)}\Big|_{\beta=0}$. The inequality follows from the fact that $f(\gamma_0)/f(\beta)$ is a decreasing function of β. This yields

$$\log f(\gamma_0) \leq \log f(\beta) + \log f(\frac{2\sigma}{n}) \leq \log f(\beta) + \log[1 + \sqrt{\tfrac{3}{2}(\tfrac{2\sigma}{n})}] \leq \log f(\beta) + \tfrac{1}{\ln 2}\sqrt{\tfrac{3\sigma}{n}}. \tag{A.3}$$

From (A.2) and (A.3) we conclude $n \log f(\gamma_{\max}(t,\sigma)) \leq n \log f(\beta) + \xi\sqrt{\sigma n}$ with ξ as defined in (46). With ℓ chosen according to (45), the expression $\sqrt{2^{\ell - n + 2n\log f(\gamma_{\max})}}$ in (38) is upper bounded by $2^{-\sigma}/\sqrt{2}$. Hence the second expression in the $\min\{\cdot,\cdot\}$ (38) is upper bounded by $\frac{2^{-\sigma}}{2\sqrt{2}} + \frac{2^{-\sigma}}{2} + \frac{2^{-2\sigma}}{2\sqrt{2}} < 2^{-\sigma}$. □