SECURITY PROOF FOR QUANTUM KEY RECYCLING WITH NOISE

Daan Leermakers and Boris Škorić

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]. We 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.

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.

- We introduce a number of modifications in the QKR protocol of Škorić and de Vries [2]. (i) 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. (ii) 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 technical reasons we combine the privacy amplification and the key refreshment into a single hashing operation. This simplifies the security proof. (iii) The message contains keys for the next round. Consequently our scheme does not consume key material.
- We provide a security proof. Our proof technique differs from [1]. We treat all keys on the same footing. Our approach is as follows. We work with an EPR formulation of the protocol. The permutation invariance of the protocol allows us to invoke Post-selection [10]. In order to prove security against general attacks we only need to demonstrate security against 'collective' attacks, i.e. attacks where Eve collects quantum side information from individual EPR pairs, in exactly the same way for each EPR pair. We apply symmetrisation of the individual noisy EPR pairs as introduced in [11, 12]. The only remaining degree of freedom in the attack is a single scalar, the bit error probability. We provide an upper bound on the diamond distance between the real protocol and an idealised version in which the keys are completely decoupled from Eve's side information. We do this for one QKR round. The security of multiple rounds follows inductively by universal composability.

  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 divided by n. 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 $\{1, \dots, n\}$. 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 $h(\{p_1, \dots, p_k\})$ 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 $\|A\|_1 = \operatorname{tr} \sqrt{A^\dagger A} = \sum_i |\lambda_i|$. 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. $\rho^{\mathrm{YE}} = \operatorname{tr}_X \rho^{\mathrm{XYE}} = \mathbb{E}_y |y\rangle\langle y| \otimes \rho^E_y$, 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],

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

i.e. the distance between the true classical-quantum state and a state in which X is completely unknown to Eve.

We write $\mathcal{S}(\mathcal{H}_A)$ to denote the space of density matrices on Hilbert space $\mathcal{H}_A$, i.e. positive semi-definite operators acting on $\mathcal{H}_A$. Any quantum channel can be described by a Completely Positive Trace-Preserving (CPTP) map $\mathcal{E}$: $\mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ that transforms a mixed state $\rho^{\mathrm{A}} \in \mathcal{S}(\mathcal{H}_A)$ to another mixed state $\rho^{\mathrm{B}} \in \mathcal{S}(\mathcal{H}_B)$. We write $\mathcal{E}(\rho^{\mathrm{A}}) = \rho^{\mathrm{B}}$. The diamond norm of a map is defined as $\|\mathcal{E}\|_\diamond \stackrel{\text{def}}{=} \frac{1}{2} \sup_{\rho^{\mathrm{AC}} \in \mathcal{S}(\mathcal{H}_{AC})} \|\mathcal{E}(\rho^{\mathrm{AC}})\|_1$ with $\mathcal{H}_C$ an auxiliary system that can be considered to be of the same dimension as $\mathcal{H}_A$. For a map $\mathcal{E}\colon\ \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$, the notation $\mathcal{E}(\rho^{\rm AC})$ means $(\mathcal{E}\otimes \mathbb{1}_{\rm C})(\rho^{\rm AC})$, i.e. $\mathcal{E}$ acts only on the 'A' subsystem. A natural distance measure between two CPTP maps $\mathcal{E}_1$ and $\mathcal{E}_2$ is given by $\|\mathcal{E}_1-\mathcal{E}_2\|_\diamond$; this is the maximum possible advantage that one can have in distinguishing between the two maps given one observation of their action.

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 $S(\rho)=-{\rm tr}\,\rho\log\rho$. The ε-smooth Rényi entropy of order α is defined as [13]

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

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 asymptotically approaches the von Neumann entropy.

Lemma 1 *Let σ be a density matrix. It holds that*

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

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

This lemma follows from [11] (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*

We use the universal composability framework [11][16]. Let $\mathcal{E}$ be the CPTP map that describes one round of the QKR protocol. Let $\mathcal{F}$ denote an 'ideal', perfectly secure version of $\mathcal{E}$. We say that one round of the QKR protocol is ε-secure when $\|\mathcal{E}-\mathcal{F}\|_\diamond\leq\varepsilon$. Since the diamond norm is a composable security measure, the key material that is to be re-used can be considered uniform in the second round except with probability ε. By an induction argument the scheme is then $N\varepsilon$-secure after N rounds. This can be seen as follows. The security of two rounds is

$$\begin{aligned}\|\mathcal{E}\circ\mathcal{E}-\mathcal{F}\circ\mathcal{F}\|_\diamond &= \|\mathcal{E}\circ\mathcal{E}-\mathcal{E}\circ\mathcal{F}+\mathcal{E}\circ\mathcal{F}-\mathcal{F}\circ\mathcal{F}\|_\diamond = \|\mathcal{E}\circ(\mathcal{E}-\mathcal{F})+(\mathcal{E}-\mathcal{F})\circ\mathcal{F}\|_\diamond\\ &\leq \|\mathcal{E}\circ(\mathcal{E}-\mathcal{F})\|_\diamond+\|(\mathcal{E}-\mathcal{F})\circ\mathcal{F}\|_\diamond \qquad \text{(triangle ineq.)}\\ &\leq \|\mathcal{E}-\mathcal{F}\|_\diamond+\|\mathcal{E}-\mathcal{F}\|_\diamond\leq 2\varepsilon. \end{aligned} \tag{5}$$

The inequality (5) follows from (i) the fact that a CPTP map cannot increase distance, yielding $\|\mathcal{E}\circ(\mathcal{E}-\mathcal{F})\|_\diamond\leq\|\mathcal{E}-\mathcal{F}\|_\diamond$; (ii) maximising over states $\mathcal{F}(\rho)$ is a subset of maximising over ρ, yielding $\|(\mathcal{E}-\mathcal{F})\circ\mathcal{F}\|_\diamond\leq\|\mathcal{E}-\mathcal{F}\|_\diamond$.

A QKR protocol has to satisfy two requirements:

- The encrypted message must be secure.
- If Alice and Bob don't detect disturbance on the quantum channel, it must be safe to re-use keys, even if Eve knows the plaintext.

A QKR security proof needs to demonstrate $\|\mathcal{E}-\mathcal{F}\|_\diamond \leq \varepsilon$ for two different definitions of "ideal $\mathcal{F}$". In the case where Eve does not know the plaintext, the ideal mapping $\mathcal{F}$ is constructed to mimic $\mathcal{E}$ except that the message and the next-round keys are replaced by completely random variables. In the case of known plaintext, this replacement is done only for the next-round keys.

Some technical complications may arise in the security proof due to the imperfection of the MAC function used by Alice and Bob. An elegant way to avoid computational complications is to describe the classical channel as a channel that is perfectly authenticated (Eve only listens) except with probability η, where η is the failure probability of the MAC. If the protocol has security ε in case of a perfectly authenticated classical channel, then the real-life security is $\varepsilon+\eta$. For QKD this method was written out in detail in Appendix D of [16].

2.4 *Post-selection*

Attacks where Eve acts on individual qubits identically in all positions are called *collective attacks*. For protocols that are invariant under permutation of the input states, a post-selection argument [10] can be used to show that ε-security against collective attacks implies ε'-security against general attacks, with $\varepsilon' = \varepsilon(n+1)^{d^2-1}$. Here d is the dimension of the combined Alice-Bob subsystem ($d=4$ for qubits).

A mapping $\mathcal{E}$ is called permutation-symmetric if for all permutations π there exists a mapping $\mathcal{K}_\pi$ such that $\mathcal{E}\circ\pi = \mathcal{K}_\pi \circ \mathcal{E}$. (Any protocol that starts with a random permutation p and afterwards applies no operation that depends on p is obviously permutation-symmetric. It has $\mathcal{K}_\pi = \mathbb{1}$.) In [10] the following result was proven[a]for any permutation-symmetric protocol $\mathcal{E}$ acting on $\mathcal{S}(\mathcal{H}_{AB}^{\otimes n})$,

$$\|\mathcal{E}-\mathcal{F}\|_\diamond \quad \leq \quad (n+1)^{d^2-1} \max_{\sigma\in\mathcal{S}(\mathcal{H}_{ABE})} \Big\|(\mathcal{E}-\mathcal{F})(\sigma^{\otimes n})\Big\|_1. \tag{6}$$

Practically this means it is possible to upgrade from security against collective attacks to security against general attacks by paying a modest price in terms of privacy amplification, namely changing the usual privacy amplification term $2\log\frac{1}{\varepsilon}$ to $2\log\frac{1}{\varepsilon}+2(d^2-1)\log(n+1)$.

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 [17] 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

[a] This follows from applying Theorem 1 in [10] to $\mathcal{E}-\mathcal{F}$ and then using eq.(5) in [10].

corner points of a cube on the Bloch sphere. We write $b = 2u + w$, with $u, w \in \{0, 1\}$. The states are

$$|\psi_{uwg}\rangle = (-1)^{gu}\left[(-\sqrt{i})^{g}\cos\tfrac{\alpha}{2}|g \oplus w\rangle + (-1)^{u}(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|\overline{g \oplus w}\rangle\right]. \tag{7}$$

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 [18, 19, 20] 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 auxiliary state

Consider Eve preparing noisy EPR pairs for Alice and Bob. Let one noisy singlet state be denoted as σ^{AB}. Eve holds the purifying 'auxiliary' state $\sigma^{\mathrm{E}} = \mathrm{tr}_{\,\mathrm{AB}}|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}|$. One of the results of [9] was an expression for Eve's auxiliary state after the symmetrisation technique of [11] is applied to σ^{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 $\Psi^{\pm}, \Phi^{\pm}$ are the Bell basis states in the AB subsystem, and $|m_i\rangle$ is an orthonormal basis in Eve's four-dimensional ancilla space. The single remaining degree of freedom γ is the bit error probability caused by Eve.[b] Let $\boldsymbol{v} = (v_1, v_2, v_3)$ be a 3-component vector on the Bloch sphere. Let $|\boldsymbol{v} \cdot \boldsymbol{m}\rangle$ be shorthand notation for $v_1|m_1\rangle + v_2|m_2\rangle + v_3|m_3\rangle$. Alice and Bob do a measurement in the $\boldsymbol{v}$-basis, such that $|\boldsymbol{v}\rangle$ stands for '0' and $|-\boldsymbol{v}\rangle$ for '1'. Let $x \in \{0, 1\}$ be the bit value that Alice measures, and $y \in \{0, 1\}$ Bob's bit value. (In the noiseless case we have $y = \bar{x}$ because of the anti-correlation in the singlet state.) After these measurements have taken place, Eve's auxiliary system is in state $\sigma^{\boldsymbol{v}}_{xy}$, given by

$$\sigma^{\boldsymbol{v}}_{xy} \stackrel{\mathrm{def}}{=} |E^{\boldsymbol{v}}_{xy}\rangle\langle E^{\boldsymbol{v}}_{xy}|, \tag{8}$$

$$\begin{aligned}
|E^{\boldsymbol{v}}_{01}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1 - \tfrac{3}{2}\gamma}|m_0\rangle + \sqrt{\tfrac{\gamma}{2}}|\boldsymbol{v} \cdot \boldsymbol{m}\rangle\right] \\
|E^{\boldsymbol{v}}_{10}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1 - \tfrac{3}{2}\gamma}|m_0\rangle - \sqrt{\tfrac{\gamma}{2}}|\boldsymbol{v} \cdot \boldsymbol{m}\rangle\right] \\
|E^{\boldsymbol{v}}_{00}\rangle &= \frac{1}{\sqrt{2(1-v_3^2)}}\left[(-v_1 v_3 - i v_2)|m_1\rangle + (-v_2 v_3 + i v_1)|m_2\rangle + (1 - v_3^2)|m_3\rangle\right] \\
|E^{\boldsymbol{v}}_{11}\rangle &= \frac{1}{\sqrt{2(1-v_3^2)}}\left[(-v_1 v_3 + i v_2)|m_1\rangle + (-v_2 v_3 - i v_1)|m_2\rangle + (1 - v_3^2)|m_3\rangle\right].
\end{aligned} \tag{9}$$

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 $|\frac{-v_1 v_3 - i v_2}{\sqrt{1-v_3^2}}|^2 = 1 - v_1^2$ and $|\frac{-v_2 v_3 + i v_1}{\sqrt{1-v_3^2}}|^2 = 1 - v_2^2$. 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 $|E^{\boldsymbol{v}}_{00}\rangle\langle E^{\boldsymbol{v}}_{00}| = \frac{1}{2}\sum_{j=1}^{3}|m_j\rangle\langle m_j| - \frac{1}{2}|\boldsymbol{v} \cdot \boldsymbol{m}\rangle\langle \boldsymbol{v} \cdot \boldsymbol{m}| + \frac{i}{2}\sum_{jkp=1}^{3}\varepsilon_{jkp} v_j |m_k\rangle\langle m_p|$, 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

[b] In the case of 4-state encoding 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. Otherwise Eve has more degrees of freedom [12].

defined by the pair $(\mathcal{B}, b)$. The following useful identity holds,

$$\mathbb{E}_{xy}\sigma^b_{xy} \quad = \quad (1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma}{2}\sum_{j=1}^{3}|m_j\rangle\langle m_j|. \tag{10}$$

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 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 [21]. 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 $\mu = \frac{1}{|\mathcal{B}|} + \frac{|\mathcal{B}|-1}{|\mathcal{B}|}\sqrt{\max_{bb'\in\mathcal{B}:b'\neq b}\max_{xx'}\|F^b_x F^{b'}_{x'}\|_\infty}$. Here F^b_x 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.[c]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 Protocol

4.1 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 several changes:

- Some key refreshment of the basis key occurs even in case of an Accept.
- We derive the one time pad not only from the qubits' payload but also from the basis key. It turns out that with this construction it becomes evident that rate 1 (at zero noise) can be achieved not only using 8-state encoding but also using 6-state encoding.
- For technical reasons we combine the privacy amplification and the key refreshment into a single hashing operation. This simplifies the security proof.
- Part of the message is used to communicate keys for the next round. Consequently the scheme does not consume existing key material.

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

The key material shared between Alice and Bob consists of several parts: a basis sequence $b \in \mathcal{B}^n$, two MAC keys $k^1_{\rm MAC}, k^2_{\rm MAC} \in \{0,1\}^\lambda$, an extractor key[d] $u \in \mathcal{U}$, and a classical OTP $k_{\rm syn} \in \{0,1\}^a$ for protecting the syndrome. The plaintext is $m_{\rm bare} \in \{0,1\}^{\ell'}$, with $\ell' \overset{\rm def}{=} \ell - 2\lambda - a$.

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.[e]

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 $x \in \{0,1\}^n, k \in \{0,1\}^{2\lambda+a}$. Concatenate $m = m_{\rm bare}||k$ to form augmented message $m \in \{0,1\}^\ell$. 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.

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 $\hat{x} = x' \oplus \texttt{SynDec}(k_{\rm syn} \oplus s' \oplus \texttt{Syn}\, x')$. Compute $\hat{z}||\hat{b}' = \texttt{Ext}(u, \hat{x}||b)$ and $\hat{m} = c' \oplus \hat{z}$. Accept only if $\tau' = \Gamma(k_{\rm MAC}, \hat{x}||c'||s')$ holds and the syndrome decoding was successful. Communicate Accept/Reject to Alice (publicly but with authentication using $k^2_{\rm MAC}$). In case of Accept parse $\hat{m}$ as $\hat{m}_{\rm bare}||\hat{k}$.

Key update

Alice and Bob perform the following updates for the next round.

- In case of Reject: Take completely new keys $k^1_{\rm MAC}, k^2_{\rm MAC}, k_{\rm syn}, b, u$.
- In case of Accept: Set $b \leftarrow b'$, $(k^1_{\rm MAC}||k^2_{\rm MAC}||k_{\rm syn}) \leftarrow k$. The key u is re-used.

The protocol uses up $2\lambda+a$ bits of key material (the two MAC keys and $k_{\rm syn}$) but also delivers the same amount in the augmented message m; hence the net effect in case of Accept is that Alice and Bob expend no key material. The value of the parameter a (size of the syndrome) depends on the noise level and on the choice of error-correcting code. See Section 5.5 for a discussion of the balance between message length and syndrome length.

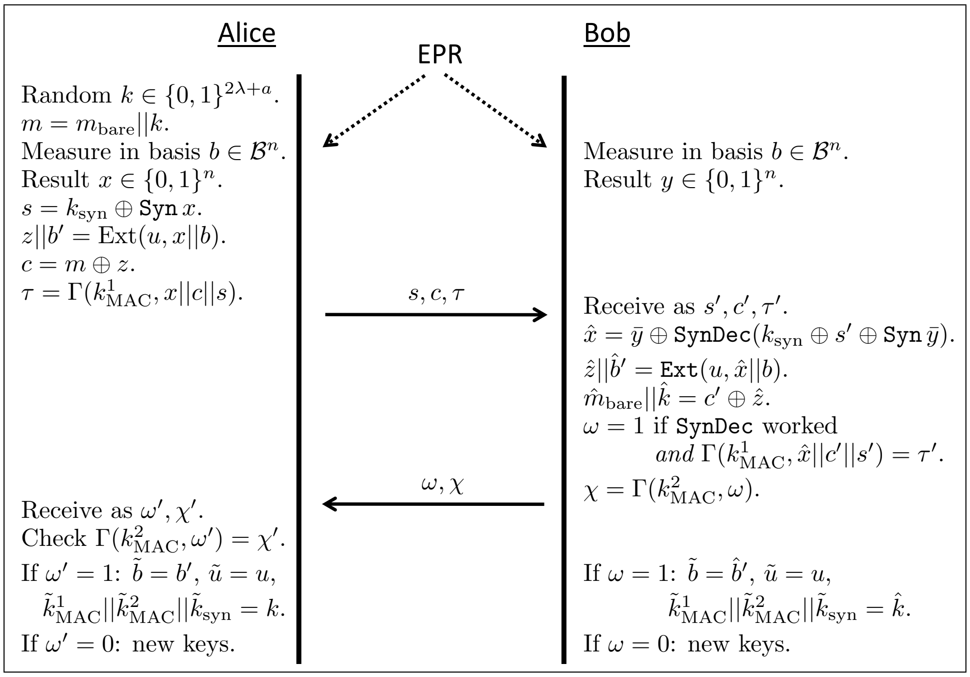
4.2 EPR version of the protocol

We work with the EPR version of the protocol (Fig. 1). The protocol steps are practically the same as in Section 4.1. The only difference is that Alice does not prepare the state $|\Psi\rangle$; instead Alice performs a measurement in the b-basis on one half of an EPR pair, resulting in a state $|\Psi\rangle$ with random payload x. This EPR pair does not have to be produced by Alice herself but can come from an outside source. Most generally this is described by an attacker Eve creating an 8-dimensional quantum state $\rho^{\rm ABE}$ and sending 2-dimensional subspaces to

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

[e] 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.

both Alice and Bob. If Eve is to have any hope of being undetected the ρ^{AB} subsystem should be close to an EPR state.



Alice:

Random $k \in \{0,1\}^{2\lambda+a}$.
$m = m_{\mathrm{bare}}||k$.
Measure in basis $b \in \mathcal{B}^n$.
Result $x \in \{0,1\}^n$.
$s = k_{\mathrm{syn}} \oplus \mathtt{Syn}\, x$.
$z||b' = \mathrm{Ext}(u, x||b)$.
$c = m \oplus z$.
$\tau = \Gamma(k^1_{\mathrm{MAC}}, x||c||s)$.
Receive as ω', χ'.
Check $\Gamma(k^2_{\mathrm{MAC}}, \omega') = \chi'$.
If $\omega' = 1$: $\tilde{b} = b'$, $\tilde{u} = u$,
$\tilde{k}^1_{\mathrm{MAC}}||\tilde{k}^2_{\mathrm{MAC}}||\tilde{k}_{\mathrm{syn}} = k$.
If $\omega' = 0$: new keys.

Bob:

Measure in basis $b \in \mathcal{B}^n$.
Result $y \in \{0,1\}^n$.
Receive as s', c', τ'.
$\hat{x} = \bar{y} \oplus \mathtt{SynDec}(k_{\mathrm{syn}} \oplus s' \oplus \mathtt{Syn}\, \bar{y})$.
$\hat{z}||\hat{b}' = \mathtt{Ext}(u, \hat{x}||b)$.
$\hat{m}_{\mathrm{bare}}||\hat{k} = c' \oplus \hat{z}$.
$\omega = 1$ if $\mathtt{SynDec}$ worked
and $\Gamma(k^1_{\mathrm{MAC}}, \hat{x}||c'||s') = \tau'$.
$\chi = \Gamma(k^2_{\mathrm{MAC}}, \omega)$.
If $\omega = 1$: $\tilde{b} = \hat{b}'$, $\tilde{u} = u$,
$\tilde{k}^1_{\mathrm{MAC}}||\tilde{k}^2_{\mathrm{MAC}}||\tilde{k}_{\mathrm{syn}} = \hat{k}$.
If $\omega = 0$: new keys.

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

4.3 Invariances

We argue that our QKR protocol is statistically equivalent to a protocol that additionally does a random permutation[f]of the input EPR particles. The argument is as follows. In the original prepare-and-measure protocol of Section 4.1 the basis sequence B and the payload X are uniform; therefore it does not matter if Alice performs a random permutation $b \mapsto \pi(b), x \mapsto \pi(x)$ (and Bob the corresponding permutation). The effect is still a uniform payload encoded in a uniform basis. The above action is identical to keeping b, x untouched but permuting the qubits: Alice applies π, and Bob π^{-1}. In the EPR version Alice and Bob both apply the same permutation, i.e. the EPR pairs get permuted.

In a similar fashion, we argue that the EPR protocol is statistically equivalent to a protocol where Alice and Bob first apply the random-Pauli transform as introduced by [11] in every qubit position. The argument is analogous to the one in [11]. Before measuring their i'th qubit in basis b_i Alice and Bob both apply the same random Pauli operation $A_i \overset{\$}{\leftarrow} \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ and then forget A_i. The effect on each mixed EPR state is $\rho^{\mathrm{AB}} \mapsto \frac{1}{4}\sum_\alpha (\sigma_\alpha \otimes \sigma_\alpha)\rho^{\mathrm{AB}}(\sigma_\alpha \otimes \sigma_\alpha)$, which gives a huge simplification and allows one to use a single-parameter description of noisy EPR states as in Section 2.6. Applying a uniformly chosen Pauli operation on a qubit state and then measuring in basis b_i has exactly the same effect as keeping the qubit unmodified and measuring in a uniformly transformed basis. But as b was completely random, this is

[f] Here the randomness is public but cannot be affected by Eve.

statistically equivalent to doing no transform at all.
By this line of reasoning we have a sequence of equivalences $\mathcal{E} \equiv \mathcal{E}^{\rm EPR} \equiv \mathcal{E}_\pi^{\rm EPR} \equiv \mathcal{E}_{\pi\Sigma}^{\rm EPR}$ showing that the original prepare-and-measure protocol $\mathcal{E}$ behaves statistically the same as the EPR version with random permutation ('π') and noise symmetrisation (random Pauli transformations, 'Σ'). We will give a security proof for $\mathcal{E}_{\pi\Sigma}^{\rm EPR}$. Security of $\mathcal{E}_{\pi\Sigma}^{\rm EPR}$ implies security of $\mathcal{E}$.

5 Security proof

5.1 Attacker model and proof steps

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.
The security proof consists of the following steps. We specify the CPTP map $\mathcal{E}_{\pi\Sigma}^{\rm EPR}$ and the idealised version $\mathcal{F}$, both for the known plaintext and unknown plaintext case. Then we invoke Post-selection and noise symmetrisation. This means we can start from (6), and for the single-position noisy EPR states σ use the symmetrised states as described in Section 2.6, i.e. parametrised only by the bit error probability γ. We derive an upper bound on the trace norm appearing in (6). We do this for the limit $n \to \infty$ (Theorem 1) as well as non-asymptotically (Theorem 2). For the asymptotic result 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 average over the hashing key u is pulled into the square root using Jensen's inequality; then the properties of pairwise independent hashes are used to evaluate the average over u; then the trace is pulled into the square root as well; 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.
The proof of the non-asymptotic result follows similar steps up to and including the average over u, but does not make use of smoothing. The operator square root is evaluated explicitly, which is feasible because of the diagonal form of the operator. No use is made of entropies.
We always model Eve's ability to interfere on the classical channel as a failure probability $2^{-\lambda}$ on a channel without any interference.

5.2 The CPTP maps

The action of one QKR round on the n noisy EPR states is denoted as $\mathcal{E}_{\pi\Sigma}^{\rm EPR}$. The output consists of Eve's auxiliary states as well as all the classical variables shown in Fig. 1, some of which are observed by Eve. The $\mathcal{E}_{\pi\Sigma}^{\rm EPR}$ comprises initialisation $\mathcal{I}$, measurement $\mathcal{M}$ and post-processing $\mathcal{P}$,

$$\mathcal{E}_{\pi\Sigma}^{\rm EPR} = \mathcal{P} \circ \mathcal{M} \circ \mathcal{I} \circ \Sigma \circ \pi. \tag{11}$$

In the initialisation step the message and all the keys are fetched and put in working memory. Mathematically this action can be written as tensoring the ABE state $\sigma^{\otimes n}$ with a fully mixed state of the form $\mathbb{E}_{\rm keys}|{\rm keys}\rangle\langle{\rm keys}|$.
The measurement $\mathcal{M}$ reads out the state of the basis key register b and then performs a measurement in this basis, resulting in values x, y held by Alice and Bob respectively. Let

$\sigma \in \mathcal{S}(\mathcal{H}_{\rm ABE})$ (for a single position $i \in \{1, \ldots, n\}$) be of the form $|\Psi^{\rm ABE}\rangle\langle\Psi^{\rm ABE}|$ as specified in Section 2.6. Then the action of $\mathcal{M}$ is

$$\begin{aligned} \mathcal{M}\Big(\mathbb{E}_b |b\rangle\langle b| \otimes \sigma^{\otimes n}\Big) &= \mathbb{E}_b \mathbb{E}_{xy} |bxy\rangle\langle bxy| \otimes \rho^E_{bxy}, \\ \rho^E_{bxy} &\overset{\rm def}{=} \bigotimes_{i=1}^{n} \sigma^{b_i}_{x_i y_i}, \end{aligned} \tag{12}$$

where Eve's auxiliary states $\sigma^{b_i}_{x_i y_i}$ are as defined by (8) with $\boldsymbol{v}$ equal to the appropriate basis vector corresponding to b_i. The notation $\mathbb{E}_{xy}(\cdot)$ stands for $\sum_x 2^{-n} \sum_y p_{y|x}(\cdot)$, with $p_{y|x} = \gamma^{|x\oplus\bar{y}|}(1-\gamma)^{|x\oplus y|}$.

The post-processing $\mathcal{P}$ generates all the remaining classical variables occurring in Fig. 1. We distinguish between *output variables* and *internal variables.* The list of output variables comprises the keys for the next round $(\tilde{u}, \tilde{b}, k)$ and the transcript s, c, τ, ω, χ visible to Eve. We also include $m_{\rm bare}$ in the output list. The internal variables are traced over in the computation of the output.

We will ignore the authentication tags τ and χ since we handle the possibility of each MAC failure by adding $2^{-\lambda}$ to the trace distance. We set $s' = s$, $c' = c$, $\omega' = \omega$ for the same reason. We introduce an indicator variable $\theta_{xy} \in \{0, 1\}$ which indicates whether error correction succeeds,

$$\theta_{xy} \overset{\rm def}{=} \begin{cases} 1 & \text{if Hamm}(x \oplus \bar{y}) \leq t \\ 0 & \text{otherwise} \end{cases}, \tag{13}$$

and automatically set the value of the Accept/Reject bit to $\omega = \theta_{xy}$. When $\omega = 1$ each 'hatted' variable equals the variable without hat.

Formally, the above tweaks define a CPTP map $\mathcal{E}^{\rm EPR}_{\pi\Sigma{\rm Auth}}$ that uses a perfectly authenticated classical channel. This map is close to $\mathcal{E}^{\rm EPR}_{\pi\Sigma}$,

$$\|\mathcal{E}^{\rm EPR}_{\pi\Sigma{\rm Auth}} - \mathcal{E}^{\rm EPR}_{\pi\Sigma}\|_\diamond \leq 2 \cdot 2^{-\lambda}. \tag{14}$$

By the triangle inequality we have

$$\|\mathcal{E}^{\rm EPR}_{\pi\Sigma} - \mathcal{F}\|_\diamond \leq 2 \cdot 2^{-\lambda} + \|\mathcal{E}^{\rm EPR}_{\pi\Sigma{\rm Auth}} - \mathcal{F}\|_\diamond. \tag{15}$$

For didactic purposes we write down the intermediate state including internal variables and then trace them out. We have

$$\begin{aligned} &\rho^{\overbrace{XYUBZB'K_{\rm syn}}^{\rm internal}\overbrace{\tilde{B}\tilde{U}MSC\Omega E}^{\rm output}} \\ &= \mathbb{E}_{xyubk_{\rm syn}} \sum_{zb's} |xyubzb'k_{\rm syn}\rangle\langle xyubzb'k_{\rm syn}| \otimes \mathbb{E}_m \sum_{\tilde{b}\tilde{u}c\omega} |\tilde{b}\tilde{u}msc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \otimes \rho^E_{bxy} \\ &\qquad \delta_{s,k_{\rm syn}\oplus\mathtt{Syn}\,x}\ \delta_{z||b',{\rm Ext}(u,x||b)}\ \delta_{c,m\oplus z}\ \left\{\omega\theta_{xy}\delta_{\tilde{u}u}\delta_{\tilde{b}b'} + \bar{\omega}\overline{\theta_{xy}}\frac{1}{|B||U|}\right\}. \end{aligned} \tag{16}$$

Here the expectations over $u, b, k_{\rm syn}$ are uniform. The $\mathbb{E}_m$ is not necessarily uniform because m contains the plaintext message $m_{\rm bare}$. The protocol output is given by

$\mathcal{E}^{\rm EPR}_{\pi\Sigma{\rm Auth}}(\sigma^{\otimes n}) = {\rm tr}\,_{XYUBZB'K_{\rm syn}}\rho^{XYUBZB'K_{\rm syn}\tilde{B}\tilde{U}MSC\Omega E} = \rho^{\tilde{B}\tilde{U}MSC\Omega E}$.

$$\rho^{\tilde{B}\tilde{U}MSC\Omega E} = \mathbb{E}_{\tilde{b}\tilde{u}ms}\sum_{c\omega} 2^{-\ell}|\tilde{b}\tilde{u}msc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \otimes [\omega\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]} + \bar{\omega}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=0]}] \quad (17)$$

$$\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]} = \mathbb{E}_{xy}\theta_{xy}2^{\ell}\sum_b \delta_{(m\oplus c)||\tilde{b},{\rm Ext}(\tilde{u},x||b)}\rho^E_{bxy} \quad (18)$$

$$\rho^E_{\tilde{b}\tilde{u}mc,[\omega=0]} = \mathbb{E}_{xy}\overline{\theta_{xy}}\mathbb{E}_b\rho^E_{bxy}. \quad (19)$$

Note that S is completely decoupled from the rest, since it is a one-time-pad encryption.
Next we describe the action of the ideal protocol $\mathcal{F}'$ in the case of unknown plaintext. We write $\mathcal{F}' = \mathcal{R}' \circ \mathcal{E}^{\rm EPR}_{\pi\Sigma}$, where $\mathcal{R}'$ replaces $\tilde{b}\tilde{u}m$ with random[g]values that have no coupling to Eve's state,

$$\mathcal{F}'(\sigma^{\otimes n}) = \mathcal{R}'(\rho^{\tilde{B}\tilde{U}MSC\Omega E}) = \mathbb{E}_{\tilde{b}\tilde{u}m}|\tilde{b}\tilde{u}m\rangle\langle\tilde{b}\tilde{u}m| \otimes \rho^{SC\Omega E}. \quad (20)$$

In the case of known plaintext we write $\mathcal{F} = \mathcal{R} \circ \mathcal{E}^{\rm EPR}_{\pi\Sigma}$. We have to split up $m = m_{\rm bare}||k$. The $\mathcal{R}$ replaces $\tilde{b}\tilde{u}k$ with random values that have no coupling to Eve's state,

$$\mathcal{F}(\sigma^{\otimes n}) = \mathcal{R}(\rho^{\tilde{B}\tilde{U}MSC\Omega E}) = \mathbb{E}_{\tilde{b}\tilde{u}k}|\tilde{b}\tilde{u}k\rangle\langle\tilde{b}\tilde{u}k| \otimes \rho^{M_{\rm bare}SC\Omega E}. \quad (21)$$

We note that $\mathcal{F}'(\sigma^{\otimes n}) = \mathcal{F}(\sigma^{\otimes n})$. This is seen as follows. Taking the partial trace ${\rm tr}_{\tilde{U}}$ of (17) leads to an expectation $\mathbb{E}_{\tilde{u}}\delta_{(m\oplus c)||\tilde{b},{\rm Ext}(\tilde{u},x||b)}$ which evaluates to the constant $\frac{1}{2^{\ell}|B|}$ due to the properties of the pairwise independent hash function `Ext`. This entirely decouples M from Eve's auxiliary state.
Consequently we do not have to provide two security proofs but only one. We will derive an upper bound on $\|(\mathcal{E}^{\rm EPR}_{\pi\Sigma{\rm Auth}} - \mathcal{F})(\sigma^{\otimes n})\|_1$. By taking a partial trace of (17) we find $\rho^{M_{\rm bare}SC\Omega E}$,

$$\rho^{M_{\rm bare}SC\Omega E} = \mathbb{E}_{m_{\rm bare}}|m_{\rm bare}\rangle\langle m_{\rm bare}| \otimes \mu^{SC} \otimes \sum_{\omega}|\omega\rangle\langle\omega| \otimes [\omega\rho^E_{[\omega=1]} + \bar{\omega}\rho^E_{[\omega=0]}], \quad (22)$$

$$\rho^E_{[\omega=1]} = \mathbb{E}_{xy}\theta_{xy}\mathbb{E}_b\rho^E_{bxy} \quad (23)$$

$$\rho^E_{[\omega=0]} = \mathbb{E}_{xy}\overline{\theta_{xy}}\mathbb{E}_b\rho^E_{bxy}. \quad (24)$$

The states with subscript $[\omega = 1]$ are sub-normalised and their trace is $P_{\rm corr}$, the probability that error correction succeeds,

$$P_{\rm corr}(t,\gamma) = \mathbb{E}_{xy}\theta_{xy} = \sum_{a=0}^{t}\binom{n}{a}\gamma^a(1-\gamma)^{n-a}. \quad (25)$$

The states with subscript $[\omega = 0]$ have trace $1 - P_{\rm corr}$. The quantity that we now have to bound is

$$\|(\mathcal{E}^{\rm EPR}_{\pi\Sigma{\rm Auth}} - \mathcal{F})(\sigma^{\otimes n})\|_1 = \|\rho^{\tilde{B}\tilde{U}KM_{\rm bare}C\Omega E} - \mu^{\tilde{B}\tilde{U}K} \otimes \rho^{M_{\rm bare}C\Omega E}\|_1 = 2d(\tilde{B}\tilde{U}K|M_{\rm bare}C\Omega E). \quad (26)$$

The S has dropped out of this expression since S is completely decoupled. The expression (26) makes sense of course; we are interested in the security of all the next-round keys given the data and auxiliaries in the hands of Eve.

[g] Again, m is not necessarily uniform because it contains $m_{\rm bare}$.

Note that the maximisation $\max_\sigma$ in (6) has become maximisation over γ. We will first derive bounds as a function of γ and then study the implications at a given bit error rate $\beta = t/n$ tolerated by the error-correcting code. Asymptotically the optimal value of γ equals β.

It is important to remark that the two 'Reject' case expressions (19) and (24) are identical. In the difference $\rho^{\tilde B\tilde U K M_{\rm bare} C\Omega E} - \mu^{\tilde B\tilde U K} \otimes \rho^{M_{\rm bare} C\Omega E}$ we see that the $\omega = 0$ part vanishes.

5.3 Asymptotic result

Theorem 1 *Consider one round of the QKR protocol (Section 4.1) 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*

$$d(\tilde B\tilde U K|M_{\rm bare}C\Omega E) \leq \min\Big(P_{\rm corr}(t,\gamma),\ \ \sqrt{2^{\ell-2-n+nh(\{1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}\})-nh(\gamma)}}\Big) \qquad (27)$$

with $P_{\rm corr}$ as defined in (25).

Let $\beta \overset{\rm def}{=} t/n$. For $\gamma > \beta$ the probability $P_{\rm corr}$ 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 $\frac{\ell' - \mathcal{O}(\log n)}{n}$ goes to

$$\text{asymptotic rate} = 1 - h(\{1 - \tfrac{3}{2}\beta, \tfrac{\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}\}), \qquad (28)$$

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

Proof of Theorem 1: We write $D \overset{\rm def}{=} \|\rho^{\tilde B\tilde U K M_{\rm bare} C\Omega E} - \mu^{\tilde B\tilde U K} \otimes \rho^{M_{\rm bare} C\Omega E}\|_1$. We introduce smoothing as in [13, 11, 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 $\bar D \overset{\rm def}{=} \|\bar\rho^{\tilde B\tilde U K M_{\rm bare} C\Omega E} - \mu^{\tilde B\tilde U K} \otimes \bar\rho^{M_{\rm bare} C\Omega E}\|_1$. Substituting (17,22) into this expression gives

$$\bar D \;\;=\;\; \mathbb{E}_{\tilde b\tilde u mc}\|\bar\rho^E_{\tilde b\tilde u mc,[\omega=1]} - \bar\rho^E_{[\omega=1]}\|_1. \qquad (29)$$

In slight abuse of notation we have written $\mathbb{E}_c(\cdots) \overset{\rm def}{=} \sum_c 2^{-\ell}(\cdots)$. The $\bar\rho^E_{\tilde b\tilde u mc,[\omega=1]}$ and $\bar\rho^E_{[\omega=1]}$ are both sub-normalised states with trace $P_{\rm corr}(t,\gamma)$. Hence it holds that $\bar D \leq 2P_{\rm corr}(t,\gamma)$. This corresponds to the first expression in the 'min' in (27). We derive the second expression as follows.

$$\begin{aligned}
\bar D \;\;&=\;\; \mathbb{E}_{\tilde b\tilde u mc}{\rm tr}\sqrt{(\bar\rho^E_{\tilde b\tilde u mc,[\omega=1]} - \bar\rho^E_{[\omega=1]})^2} && (30)\\
&\overset{\rm Jensen}{\leq}\;\; \mathbb{E}_{\tilde b mc}{\rm tr}\sqrt{\mathbb{E}_{\tilde u}(\bar\rho^E_{\tilde b\tilde u mc,[\omega=1]} - \bar\rho^E_{[\omega=1]})^2} && (31)\\
&=\;\; \mathbb{E}_{\tilde b mc}{\rm tr}\sqrt{\mathbb{E}_{\tilde u}(\bar\rho^E_{\tilde b\tilde u mc,[\omega=1]})^2 - (\bar\rho^E_{[\omega=1]})^2}. && (32)
\end{aligned}$$

From the properties of two-universal hash functions we get

$$
\begin{aligned}
&\mathbb{E}_{\tilde{u}}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]})^2 - (\bar{\rho}^E_{[\omega=1]})^2 \\
&= \mathbb{E}_{xx'} \sum_{bb'} [2^{2\ell} \mathbb{E}_{\tilde{u}} \delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x||b)} \delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x'||b')}] \bar{\rho}^E_{bx,[\omega=1]} \bar{\rho}^E_{b'x',[\omega=1]} - (\bar{\rho}^E_{[\omega=1]})^2 && (33) \\
&= \mathbb{E}_{xx'} \sum_{bb'} [|\mathcal{B}|^{-2n} + \delta_{bb'}\delta_{xx'}(2^\ell |\mathcal{B}|^{-n} - |\mathcal{B}|^{-2n})] \bar{\rho}^E_{bx,[\omega=1]} \bar{\rho}^E_{b'x',[\omega=1]} - (\bar{\rho}^E_{[\omega=1]})^2 && (34) \\
&= (2^\ell |\mathcal{B}|^n - 1) \mathbb{E}_{xx'} \mathbb{E}_{bb'} \delta_{bb'} \delta_{xx'} \bar{\rho}^E_{bx,[\omega=1]} \bar{\rho}^E_{b'x',[\omega=1]} && (35) \\
&\leq (2^\ell |\mathcal{B}|^n - 1) \mathbb{E}_{xx'} \mathbb{E}_{bb'} \delta_{bb'} \delta_{xx'} \bar{\rho}^E_{bx} \bar{\rho}^E_{b'x'} && (36) \\
&= (2^\ell |\mathcal{B}|^n - 1) \mathbb{E}_{bx} \mathbb{E}_{b'x'} \mathrm{tr}_{BX} |bx\rangle\langle bx||b'x'\rangle\langle b'x'| \otimes \bar{\rho}^E_{bx} \bar{\rho}^E_{b'x'} && (37) \\
&= (2^\ell |\mathcal{B}|^n - 1) \mathrm{tr}_{BX} (\bar{\rho}^{BXE})^2. && (38)
\end{aligned}
$$

Line (36) should be read as an operator inequality for a sum of positive semidefinite matrices; we used $\theta_{xy} \leq 1$. Substituting (38) into (32) gives

$$
\begin{aligned}
\bar{D} \quad &< \quad \sqrt{2^\ell |\mathcal{B}|^n}\ \mathrm{tr}_E \sqrt{\mathrm{tr}_{BX} (\bar{\rho}^{BXE})^2} && (39) \\
&\overset{\text{Jensen}}{\leq} \quad \sqrt{2^\ell |\mathcal{B}|^n} \sqrt{\mathrm{rank}(\mathrm{tr}_{BX} (\bar{\rho}^{BXE})^2)} \sqrt{\mathrm{tr}_{BXE} (\bar{\rho}^{BXE})^2} && (40) \\
&= \quad \sqrt{2^\ell |\mathcal{B}|^n \mathrm{rank}(\bar{\rho}^E) \mathrm{tr}\, (\bar{\rho}^{BXE})^2}. && (41) \\
&= \quad \sqrt{2^\ell |\mathcal{B}|^n 2^{S_0(\bar{\rho}^E) - S_2(\bar{\rho}^{BXE})}} = \sqrt{2^\ell |\mathcal{B}|^n 2^{S_0^\varepsilon(\rho^E) - S_2^\varepsilon(\rho^{BXE})}} && (42) \\
&= \quad \sqrt{2^\ell |\mathcal{B}|^n 2^{S_0^\varepsilon([\mathbb{E}_{bxy}\sigma^b_{xy}]^{\otimes n}) - S_2^\varepsilon([\mathbb{E}_{bxy}|bx\rangle\langle bx| \otimes \sigma^b_{xy}]^{\otimes n})}} && (43) \\
&\overset{\text{Lemma 1}}{\to} \quad \sqrt{2^\ell |\mathcal{B}|^n 2^{nS(\mathbb{E}_{bxy}\sigma^b_{xy}) - nS(\mathbb{E}_{bxy}|bx\rangle\langle bx| \otimes \sigma^b_{xy})}}. && (44)
\end{aligned}
$$

(In the last two lines we have $x, y \in \{0, 1\}$ and $b \in \mathcal{B}$ in contrast to the previous lines.) In line (40) we used a rank equality that is further detailed in Appendix A. From (10) 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

$$
\begin{aligned}
S(\mathbb{E}_{bxy}|bx\rangle\langle bx| \otimes \sigma^b_{xy}) \quad &= \quad S(BX) + \mathbb{E}_{bx} S(\mathbb{E}_y \sigma^b_{xy}) && (45) \\
&= \quad \log |\mathcal{B}| + 1 + \mathbb{E}_{bx} S([1-\gamma]\sigma^b_{x\bar{x}} + \gamma\sigma^b_{xx}) && (46) \\
&= \quad \log |\mathcal{B}| + 1 + h(\gamma). && (47)
\end{aligned}
$$

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 (28). If only the xz-plane of the Bloch sphere is involved in the protocol, then (44) still holds, but with different σ^b_{xy} matrices, yielding a QKR rate equal to the BB84 QKD rate.

5.4 Non-asymptotic result without smoothing

We want to have a security proof also for finite n. One approach would be to start from (43) 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 4.1). 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*

$$f(\gamma) \stackrel{\rm def}{=} \sqrt{(1-\tfrac{3}{2}\gamma)(1-\gamma)} + \sqrt{\tfrac{3}{2}\gamma(1+\gamma)}. \tag{48}$$

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

$$d(\tilde{B}\tilde{U}K|M_{\rm bare}C\Omega E) \leq \min\Big\{P_{\rm corr}(t,\gamma),\ \tfrac{1}{2}\sqrt{2^{\ell-n+2n\log f(\gamma)}}\Big\}. \tag{49}$$

For large γ the probability $P_{\rm corr}(t,\gamma)$ 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 $\ell<n-n\cdot 2\log f(\gamma)$, so that the $\sqrt{\cdots}$ in (49) becomes exponentially small in n.

Proof of Theorem 2: We follow the proof of Theorem 1 up to (39) but without smoothing ($\varepsilon=0$).

$$D \quad < \quad \sqrt{2^{\ell-n}}{\rm tr}\sqrt{\mathbb{E}_{bx}(\rho^E_{bx})^2}. \tag{50}$$

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

$$\begin{aligned}
\mathbb{E}_{bx}(\rho^E_{bx})^2 &= \bigotimes_{i=1}^n\Big\{(1-\gamma)^2\mathbb{E}_{b_i}\frac{\sigma^{b_i}_{01}+\sigma^{b_i}_{10}}{2}+\gamma^2\mathbb{E}_{b_i}\frac{\sigma^{b_i}_{00}+\sigma^{b_i}_{11}}{2}\Big\} && (51)\\
&= \Big\{(1-\gamma)\Big[(1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0|+\tfrac{\gamma}{6}\sum_{j=1}^3|m_j\rangle\langle m_j|\Big]+\tfrac{\gamma^2}{3}\sum_{j=1}^3|m_j\rangle\langle m_j|\Big\}^{\otimes n} && (52)\\
&= \Big\{(1-\gamma)(1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0|+\tfrac{\gamma(1+\gamma)}{6}\sum_{j=1}^3|m_j\rangle\langle m_j|\Big\}^{\otimes n} && (53)
\end{aligned}$$

from which it follows that

$${\rm tr}\sqrt{\mathbb{E}_{bx}(\rho^E_{bx})^2}=\Big\{\sqrt{(1-\gamma)(1-\tfrac{3}{2}\gamma)}+\sqrt{\tfrac{3}{2}\gamma(1+\gamma)}\Big\}^n. \tag{54}$$

□

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

$$\begin{aligned}
\ell &\leq n-2n\log f(\beta)-2\xi\sqrt{\nu n}-2\nu-1 && (55)\\
\xi &\stackrel{\rm def}{=} \min\left\{\frac{f'(\beta)}{f(\beta)}\left[\sqrt{\frac{2\beta}{\ln 2}+\frac{\nu}{n}}+\sqrt{\frac{\nu}{n}}\right],\quad\frac{\sqrt{3}}{\ln 2}\right\}. && (56)
\end{aligned}$$

Then

$$d(\tilde{B}\tilde{U}K|M_{\rm bare}C\Omega E)\leq 2^{-\nu}. \tag{57}$$

Proof: See Appendix B.
If according to (55) the length ℓ becomes smaller than $2\lambda + a$ (negative size of the message $m_{\rm bare}$) then this means that the desired security level ν cannot be achieved.
A typical choice for the tag length would be $\lambda = \nu$, yielding security $\|(\mathcal{E}^{\rm EPR}_{\pi\Sigma} - \mathcal{F})(\sigma^{\otimes n})\|_1 \leq 2 \cdot 2^{-\lambda} + 2 \cdot 2^{-\nu} = 2^{-\nu+2}$. Several things are worth noting.

- The ξ is of order 1. Hence the term $\xi\sqrt{\nu n}$ scales as $\sqrt{n}$.
- 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 (49) changes by a factor $(n+1)^{15}$, which can be compensated by shrinking ℓ from (55) to

$$\ell \leq n - 2n \log f(\beta) - 2\xi\sqrt{\nu n} - 2\nu - 1 - 30 \log(n+1). \tag{58}$$

5.5 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 $\eta = 2 \cdot 2^{-\lambda} + 2 \cdot 2^{-\nu}$ 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. After $N = \lfloor \theta/\eta \rfloor$ rounds they have to refresh *all* their key material. We define the amortised QKR rate as

$$A \stackrel{\rm def}{=} \frac{\text{total message data sent in } N \text{ rounds} - \text{expended key material}}{N \cdot n} \tag{59}$$

$$= \frac{\ell'}{n} - \frac{\log |\mathcal{U} \times \mathcal{B}^n|}{N \cdot n}, \tag{60}$$

namely the usual definition of rate ($\frac{\ell'}{n}$) minus the amortised cost of completely replacing u and b after N rounds. The A is an operational quantity that measures how much useful classical payload is sent per qubit. The subtraction can be understood as the cost of putting enough key material into all the $m_{\rm bare}$ to compensate for the eventual replacement of u, b.
The total message size is $N\ell' = N(\ell - 2\lambda - a)$, with ℓ specified in (58). The total key expenditure consists of $\log |\mathcal{B}^n|$ bits of basis key b, and $\log |\mathcal{U}| = \log |\{0,1\}^n \times \mathcal{B}^n|$ bits of extractor key u. This gives

$$A = 1 - \frac{a}{n} - 2 \log f(\beta) - \frac{2\xi\sqrt{\nu}}{\sqrt{n}} - \frac{30 \log(n+1)}{n} - \frac{2\lambda + 2\nu}{n} - \frac{1 + 2 \log |\mathcal{B}|}{N}. \tag{61}$$

Note that η can be made exponentially small (N exponentially large) by increasing λ and ν. For large n and N the rate (61) tends to $1 - h(\beta) - 2 \log f(\beta)$, which is lower than the asymptotic result of Section 5.3. The discrepancy is of course caused by the fact that we did not use smoothing for Theorem 2. Fig. 2 shows the asymptotic (QKR=QKD) rate (28) as

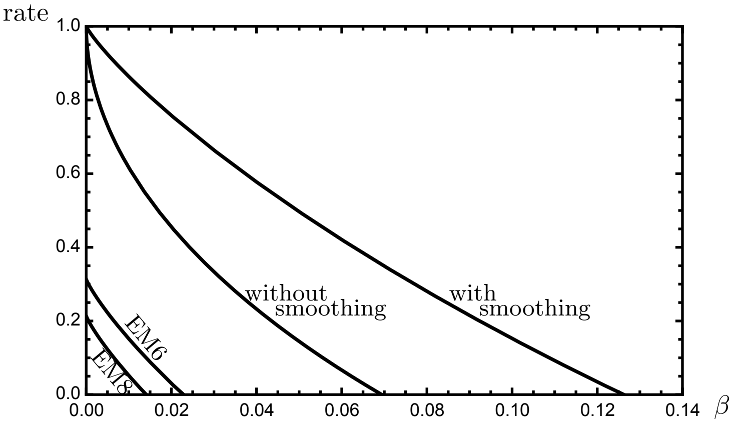


Fig. 2. *Asymptotic QKR rates. The 'with smoothing' curve is the result (28). The 'without smoothing' curve is the result $1 - h(\beta) - 2\log f(\beta)$ obtained without smoothing. The 'EM6' and 'EM8' curves correspond to the bound $1 - \log(2\mu) - 2h(\beta)$ based on Entanglement Monogamy, with constants $\mu = \mu_6$ and $\mu = \mu_8$ respectively (see Section 3).*

well as the $\varepsilon = 0$ rate (61) 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.

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 $n + n\log|\mathcal{B}|$ to approximately $n - \ell + 2\log\frac{1}{\delta}$.

Typically θ is fixed. Then it remains to tune N (which via $\eta = \theta/N$ fixes ν) 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.

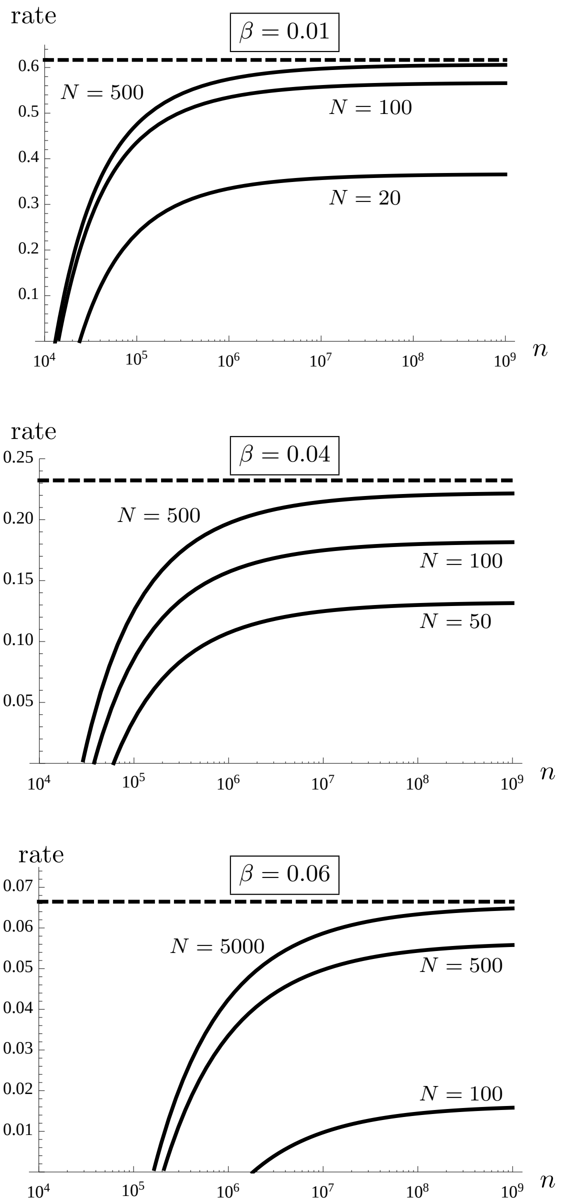


Fig. 3. *Non-asymptotic bound on the amortised QKR rate as a function of the number of qubits (n), for various values of the design parameter N and tolerated noise β. The dashed lines indicate the $\varepsilon = 0$ limit $1 - h(\beta) - 2\log f(\beta)$. $\lambda = \nu$; $\theta = 2^{-256}$; the syndrome 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. [22]), where Φ is defined as $\Phi(z) \overset{\mathrm{def}}{=} \int_z^\infty (2\pi)^{-1/2}\exp[-x^2/2]\mathrm{d}x$.*

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 shortening ℓ'. An 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 (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.

Upon Accept, our protocol does not *reduce* the stack of shared key material that Alice and Bob have. A difference with respect to [1] is that the 'top' keys on the stack are *modified* upon Accept. We do not see this as a significant drawback; the key modification is just some additional data processing.

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 4.1 employing such an error-correcting code. On the one hand, the parameter a 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 is often larger than 90%. Under such circumstances the QKR scheme of Section 4.1 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 $s' = k_{\rm syn} \oplus S(y')$, $z'||b' = \texttt{Ext}(u, y'||b)$, $c' = m \oplus z'$, $t' = \Gamma(k^1_{\rm MAC}, \mathcal{J}'||y'||c'||s')$. 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 $\tau = \Gamma(k^1_{\rm MAC}, \mathcal{J}||y||c||s)$. 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.

6.3 Future work

It is possible to evaluate or bound the $S_0^\varepsilon(\rho^E)$ and $S_2^\varepsilon(\rho^{BXE})$ in (42) 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 4.1 can be improved and embellished in various ways. For instance, the λ-bit space in m reserved for the new $k^1_{\rm MAC}$ may not be necessary. Alice's 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]).

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 reduce the cost of refreshing b from $2n$ bits to n bits.

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, Niek Bouman, Benne de Weger and Aart Blokhuis 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).

Appendix A: Rank equality

Here we show that $\mathrm{rank}(\mathrm{tr}_{BX}(\bar{\rho}^{BXE})^2) = \mathrm{rank}(\bar{\rho}^E)$. We write $\bar{\rho}^{BXE}$ in its spectral decomposition, $\bar{\rho}^{BXE} = \sum_j r_j |v_j\rangle\langle v_j|$, where the v_j are the eigenvectors in the BXE space, and $r_j > 0$. We have $\bar{\rho}^E = \mathrm{tr}_{BX}\bar{\rho}^{BXE} = \sum_j r_j V_j$, with $V_j \overset{\rm def}{=} \mathrm{tr}_{BX}|v_j\rangle\langle v_j|$. Similarly we write

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

$\mathrm{tr}_{BX}(\bar{\rho}^{BXE})^2 = \sum_j r_j^2 V_j$. Since $V_j > 0$ we can write $V_j = A_j^\dagger A_j$. We construct a matrix $A = [\sqrt{r_1}A_1; \sqrt{r_2}A_2; \sqrt{r_3}A_3; \cdots]$ by concatenating the matrices A_j under each other. It holds that $\sum_j r_j V_j = A^\dagger A$. Similarly we construct $Q = [r_1 A_1; r_2 A_2; r_3 A_3; \cdots]$, so that $\sum_j r_j^2 V_j = Q^\dagger Q$. We use the fact that $\mathrm{rank}(A^\dagger A) = \mathrm{rank}(A)$ and $\mathrm{rank}(Q^\dagger Q) = \mathrm{rank}(Q)$. By the construction of A and Q, the rows of A span the same space as the rows of Q.

Appendix B: Proof of Theorem 3

We (implicitly) define a function $\gamma_{\max}(t,\nu)$ as $P_{\mathrm{corr}}(t,\gamma_{\max}) = 2^{-\nu}$. For $\gamma \geq \gamma_{\max}$ eq. (57) clearly holds. Next we need to bound the expression $\log f(\gamma)$ for $\gamma \leq \gamma_{\max}$. Taking the Chernoff bound $P_{\mathrm{corr}}(t,\gamma) \leq \exp[-\frac{n}{2\gamma}(\gamma - \frac{t}{n})^2]$ and solving for γ we get

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

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

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

- 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

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

From (B.2) and (B.3) we conclude $n \log f(\gamma_{\max}(t,\nu)) \leq n \log f(\beta) + \xi\sqrt{\nu n}$ with ξ as defined in (56). With ℓ chosen according to (55), the expression $\sqrt{2^{\ell - n + 2n\log f(\gamma_{\max})}}$ in (49) is upper bounded by $2^{-\nu}/\sqrt{2}$. Hence the second expression in the $\min\{\cdot,\cdot\}$ (49) is upper bounded by $\frac{2^{-\nu}}{2\sqrt{2}} + \frac{2^{-\nu}}{2} + \frac{2^{-2\nu}}{2\sqrt{2}} < 2^{-\nu}$. □

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. M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.
11. R. Renner. *Security of quantum key distribution.* PhD thesis, ETH Zürich, 2005.
12. R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.
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. Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. 2014.
17. D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.
18. 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.
19. D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.
20. P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.
21. 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.
22. 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.