Security proof for Quantum Key Recycling with noise

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

Abstract

Quantum Key Recycling aims to re-use the keys employed in quantum encryption and quantum authentication schemes. We consider QKR protocols where classical information is embedded in qubit states. A partial security analysis for such protocols was done in [1]. In the current paper we introduce a number of small protocol modifications and provide a security proof. Our proof is based on a computation of the statistical distance between the real quantum state of the system and a state in which the keys are completely secure. This is a non-asymptotic result. It also determines how much privacy amplification is needed as a function of the bit error rate. It turns out that less privacy amplification is needed than suggested by the min-entropy analysis in [1].

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 [2]. QKD establishes a random secret key known only to Alice and Bob, and uses the no-cloning theorem for unknown quantum states [3] 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 [4]. Let Alice and Bob encrypt classical data as quantum states, using a classical key to determine the basis in which the data is encoded. If they do not detect any manipulation of the quantum states, then Eve has learned almost nothing about the encryption key, and hence it is safe for Alice and Bob to re-use the key. After the discovery of QKD, interest in QKR was practically nonexistent for a long time, despite the benefits that QKR can offer for communication efficiency. It received some attention again in 2003 when Gottesman [5] 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 [6, 7]. Though elegant, their scheme unfortunately needs a quantum computer for encryption and decryption. In 2017 Fehr and Salvail [8] introduced a qubit-based QKR scheme (similar to [4]) 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 [9] proposed a variant with 8-state encoding, which drastically reduces the need for privacy amplification. It is meant to operate at the same noise levels as QKD, but the security was not proven. In [1] we studied attacks on the qubit-based QKR schemes of [8, 9], but that did not produce a full 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 number of small modifications in the QKR protocol of Škorić and de Vries [9]. In particular, our extractor function is a $2N$-wise independent hash function, and we refresh keys after at most $N+1$ rounds.
- We give a security proof for the new scheme. Our main result is an upper bound on the amount of coupling between the keys and Eve's (quantum and classical) side information. This result is formulated in terms of trace distance between quantum states, and hence is Universally Composable. We use our bound in a round-by-round argument to prove the security of the plaintext as well as the keys.
- The required amount of privacy amplification depends on the bit error rate β. When n qubits are sent, the privacy leakage in the case of 8-state encoding is $2n \log[\sqrt{(1-\beta)(1-\frac{3}{2}\beta)}+\sqrt{\frac{1}{2}\beta(1-\beta)}+\beta\sqrt{2}]$ bits. This number is more favourable than the min-entropy analysis in [1].

The outline of the paper is as follows. In the preliminaries section we introduce notation, we briefly review 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 introduce the modified QKR protocol. Section 4 explains our approach and states the main theorem, i.e. the distance bound. The proof of this theorem is given in Section 7. In Section 5 we use the distance bound to prove the security of the QKR protocol. Section 6 contains a discussion of parameter choices, rates, comparison to the literature, handling of erasures, and suggestions for future work.

2 Preliminaries

2.1 Notation and terminology

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

Hermitian conjugate of an operator A is written as $A^\dagger$. The complex conjugate of z is denoted as z^*. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. The trace distance between matrices ρ and σ is denoted as $\delta(\rho;\sigma) = \frac{1}{2}||\rho - \sigma||_1$. It is a generalisation of the statistical distance and represents the maximum possible advantage one can have in distinguishing ρ from σ.
Consider a uniform classical variable X and a mixed state ρ_X that depends on X. The combined classical-quantum state is $\mathbb{E}_x|x\rangle\langle x| \otimes \rho_x$. The statistical distance between X and a uniform variable given ρ_X (for unknown X) is a measure of the security of X given ρ. This distance is defined as [10]

$$d(X|\rho_X) \stackrel{\text{def}}{=} \delta\Big(\mathbb{E}_x|x\rangle\langle x| \otimes \rho_x \;;\; \mathbb{E}_x|x\rangle\langle x| \otimes \mathbb{E}_{x'}\rho_{x'}\Big) \tag{1}$$

i.e. the distance between the true classical-quantum state and a state in which the quantum state is decoupled from X. X is said to be ε-secure with respect to ρ if $d(X|\rho) \leq \varepsilon$. When this is the case, it can be considered that X is 'ideal' except with probability ε. Such a statement is very useful for Universally Composable security.
A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{T}\}$ is called k-independent [11] (or k-wise independent) if it holds for all distinct k-tuples $x_1, \ldots, x_k \in \mathcal{X}$ and all k-tuples $y_1, \ldots, y_k \in \mathcal{T}$ that $\Pr_{h\in H}[h(x_1) = y_1 \wedge \cdots \wedge h(x_k) = y_k] = |\mathcal{T}|^{-k}$. Here the probability is over random $h \in H$. k-independence can be achieved with a hash family of size $\log|H| = \mathcal{O}(k \log\log|\mathcal{X}|)$ [12] or $\log|H| = \mathcal{O}(k \log k)$ [13].

2.2 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 [14] the vectors are $\pm x$, $\pm y$, $\pm z$ on the Bloch sphere. We have $\mathcal{B} = \{0,1,2\}$ and

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

For 8-state encoding [9] we have $\mathcal{B} = \{0,1,2,3\}$ and the eight states are the corner points of a cube on the Bloch sphere. We write $b = 2u + w$, with $u, w \in \{0,1\}$. The states are

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

The angle α is defined as $\cos\alpha = 1/\sqrt{3}$. For given g, the four states $|\psi_{uwg}\rangle$ are the Quantum One-Time Pad (QOTP) encryptions [15, 16, 17] 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.

2.3 Eve's ancilla state

Attacks on QKR were studied in some detail in [1]. They formulated an EPR version of qubit-based QKR protocol. Instead of creating $|\psi_{b_i x_i}\rangle$ and sending it to Bob, Alice performs

a measurement on one half an EPR singlet state (using basis b_i) while the other half goes to Bob. Eve may manipulate the EPR state. Any manipulation turns the pure EPR state into a mixed state. The noise symmetrisation technique of [18] was applied to simplify the state. If Eve's actions induce bit error probability β (defined as a bit mismatch in x_i between Alice and Bob), then this corresponds to a state of the AB subsystem of the form $\tilde{\rho}^{\mathrm{AB}} = (1-\frac{3}{2}\beta)|\Psi^-\rangle\langle\Psi^-| + \frac{\beta}{2}\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+|\right)$, where $|\Psi^\pm\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$ and $|\Phi^\pm\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$ denote the Bell basis states.[1] Eve's state is obtained by purifying $\tilde{\rho}^{\mathrm{AB}}$. The pure state is $|\Psi^{\mathrm{ABE}}\rangle = \sqrt{1-\frac{3}{2}\beta}|\Psi^-\rangle\otimes|m_0\rangle + \sqrt{\frac{\beta}{2}}\left(-|\Phi^-\rangle\otimes|m_1\rangle + i|\Psi^+\rangle\otimes|m_2\rangle + |\Phi^+\rangle\otimes|m_3\rangle\right)$, where $|m_i\rangle$ is some orthonormal basis in Eve's four-dimensional ancilla space. Let $\boldsymbol{v}$ be a 3-component vector on the Bloch sphere describing the '0' bit value in a certain basis. Let x be the bit value that Alice measures, and y Bob's bit value. (In the noiseless case we have $y = \bar{x}$ because of the anti-correlation in the singlet state.) One of the results of [1] was an expression for Eve's mixed ancilla state when $\boldsymbol{v}, x, y$ are fixed,

$$\sigma^{\boldsymbol{v}}_{xy} \stackrel{\mathrm{def}}{=} |E^{\boldsymbol{v}}_{xy}\rangle\langle E^{\boldsymbol{v}}_{xy}|. \tag{4}$$

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

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

$$\omega^b_x(\beta) \stackrel{\mathrm{def}}{=} (1-\beta)\sigma^{\boldsymbol{v}(b)}_{x\bar{x}} + \beta\sigma^{\boldsymbol{v}(b)}_{xx} = (1-\beta)|E^{\boldsymbol{v}(b)}_{x\bar{x}}\rangle\langle E^{\boldsymbol{v}(b)}_{x\bar{x}}| + \beta|E^{\boldsymbol{v}(b)}_{xx}\rangle\langle E^{\boldsymbol{v}(b)}_{xx}|. \tag{6}$$

3 The QKR protocol

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

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

1. We introduce an additional one-time-pad that protects the message authentication tag. This change induces a penalty in the amount of key material that is spent by Alice and Bob. However, the size of the tag is constant, so the penalty is of little consequence.
2. We demand that the extractor function is $2N$-wise independent, for some integer N. After $N+1$ rounds most of the key material is refreshed.

The key material shared between Alice and Bob consists of five parts: a basis sequence $b \in \mathcal{B}^n$, a MAC key $k_{\text{MAC}} \in \mathcal{K}$, an extractor key[2] $u \in \mathcal{U}$, a classical OTP $k_{\text{SS}} \in \{0,1\}^a$ for protecting the secure sketch, and a classical OTP $k_{\text{tag}} \in \{0,1\}^\lambda$ for protecting the message authentication tag. The plaintext is $\mu \in \{0,1\}^\ell$.
Alice and Bob have agreed on a $2N$-wise independent extractor function $\texttt{Ext} : \mathcal{U} \times \{0,1\}^n \to \{0,1\}^\ell$, a MAC function $M : \mathcal{K} \times \{0,1\}^{n+\ell+a} \to \{0,1\}^\lambda$, a linear error-correcting code with syndrome function $S : \{0,1\}^n \to \{0,1\}^a$, and a Secure Sketch that uses this error-correcting code. The basis set $\mathcal{B}$, the functions $\texttt{Ext}, M, S$, and the Secure Sketch algorithm are publicly known.
Encryption
Alice performs the following steps. Generate random $x \in \{0,1\}^n$. Compute $s = k_{\text{SS}} \oplus S(x)$ and $z = \texttt{Ext}(u, x)$. Compute the ciphertext $c = \mu \oplus z$ and encrypted authentication tag $t = k_{\text{tag}} \oplus M(k_{\text{MAC}}, x||c||s)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{b_i x_i}\rangle$ according to section 2.2. Send $|\Psi\rangle$, s, c, t to Bob.
Decryption
Bob receives $|\Psi'\rangle$, s', c', t'. He performs the following steps. Measure $|\Psi'\rangle$ in the b-basis. This yields $x' \in \{0,1\}^n$. Recover $\hat{x}$ from x' and $k_{\text{SS}} \oplus s'$ (by the reconstruction procedure of the Secure Sketch). Compute $\hat{z} = \texttt{Ext}(u, \hat{x})$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if the Secure Sketch reconstruction succeeded and $k_{\text{tag}} \oplus t' = M(k_{\text{MAC}}, \hat{x}||c'||s')$. Communicate Accept/Reject to Alice.
Key update
Alice and Bob perform the following actions. If Bob Accepts, replace k_{SS} and k_{tag}. If Bob Rejects, replace $k_{\text{SS}}, k_{\text{tag}}, b, u$. After $N+1$ 'Accept' rounds Alice and Bob refresh b and u.

See Section 6.1 for a discussion of the balance between message length and key expenditure.

4 Main result

4.1 Our approach: N rounds

In QKR two things have to be protected: the messages and the re-used keys. In the protocol of Section 3 that means protecting the message μ in every round, as well as protecting the keys U and B until they are refreshed, i.e. until a Reject occurs or $N+1$ consecutive Accepts. (Note that k_{MAC} is already perfectly protected by the k_{tag} at the cost of sacrificing λ bits of key material in every round.)
The worst case scenario is as follows. During a number of successive rounds Bob Accepts, while Eve knows the plaintext in these rounds; then in the next round Eve does not know the plaintext and attacks the message μ, which typically causes a Reject. In the first rounds Eve has an opportunity to obtain information about B and U, which are constantly being re-used; in the final round she may use that information to learn something about the data content of the qubits and hence about the OTP z in the final round. The amount of privacy

[2]The extractor key was not mentioned explicitly in [9].

amplification in the protocol must be sufficient to reduce Eve's useful knowledge to practically zero.

We take the following approach to prove the security of the QKR protocol of Section 3. Consider the parameter N in the $2N$-wise independent hash function `Ext`. We look at a succession of N rounds in which Bob Accepts and Eve knows the plaintext. We show that after these N rounds, the keys U and B are close to 'perfect', in the sense of statistical distance from uniformity, given all the classical and quantum side information available to Eve. For the quantum side information we have a per-round argument that precisely determines the optimal ancilla states that Eve can obtain: after every round the situation is 'perfect' except with some small probability. In the perfect case Eve has no better option than to couple an ancilla to the AB system exactly as described in Section 2.3. This carries us to the next round, etc., and in this way the non-perfection probability grows linearly with the number of rounds.

Finally, the amount of Privacy Amplification needed to protect the message is obtained from [1], in particular the min-entropy expressions.[3] For 8-state encoding no such PA is needed.

At every stage of the proof we are helped by the fact that we express security in terms of trace distance, which allows us to compose pieces and to simply add up non-perfection probabilities.

In round $N+1$ the attack on the plaintext is just as if Eve is fresh in round 1.

We do not aim for full key recycling. We are already happy if the number of key bits spent is much smaller than the message size.

4.2 The result

Alice and Bob's shared key material consists of $k_{\rm SS}$, $k_{\rm tag}$, $k_{\rm MAC}$, b and u. The only keys open to attack are b and u, since $k_{\rm MAC}$ is protected by $k_{\rm tag}$, and $k_{\rm SS}$ and $k_{\rm tag}$ get discarded after each round. Eve's classical side information consists of s (OTP'ed syndrome), t (OTP'ed authentication tag), and the ciphertext $c = z \oplus \mu$. The s and t carry no information about b and u. We assume that Eve knows the plaintext μ in rounds $1 \dots N$; this implies that she knows z. We use the notation $x^r \in \{0,1\}^n$, $z^r \in \{0,1\}^\ell$ for the strings in round $r \in \{1, \dots, N+1\}$, and we introduce shorthand notation $x = (x^1, \dots, x^N)$, $z = (z^1, \dots, z^N)$.

Eve's quantum side information from the first N rounds consists of her ancilla particles which have interacted with the EPR pairs. We denote the mixed state of all these particles collectively as ρ. This state depends on x and b. Since $z^r = \texttt{Ext}(u, x^r)$ and we are interested only in the coupling between the state and the keys u, b, we will consider the mixed quantum-classical state $\mathbb{E}_{ub} |ub\rangle\langle ub| \otimes \rho(zub)$, where the states $|ub\rangle$ form an orthonormal basis for the classical variables u, b. Our main result puts an upper bound on the nonuniformity of U, B given Z and $\rho(ZUB)$.

Theorem 4.1 *Let $f(\beta) = \sqrt{(1-\beta)(1-\frac{3}{2}\beta)} + \sqrt{\frac{1}{2}\beta(1-\beta)} + \beta\sqrt{2}$. Let Eve create ancilla states for each EPR pair individually, as specified in Section 2.3, under the constraint that the average bit error rate in every round remains below a parameter $\beta \in [0, \frac{1}{2})$. Then it holds that*

$$d\Big(UB|Z\rho(ZUB)\Big) \leq \frac{3}{2^{\ell+1}} \binom{N}{2} + \frac{1}{2}\Big(1 + \sqrt{2^{\ell - n + 2n \log f(\beta)}}\Big)^N - \frac{1}{2}. \tag{7}$$

This result tells us that the statistical distance can be made exponentially small by setting ℓ smaller than approximately $n[1 - 2\log f(\beta)]$. Asymptotically (for $N \gg 1$ and $n \gg \log N$) this

[3] The min-entropy loss gives a conservative (and possibly too pessimistic) bound which holds even if some bits of the plaintext are known.

yields a balance of {message length minus key expenditure} that scales as $n[1 - 2\log f(\beta) - h(\beta)]$. See Section 6.1. This balance is positive up to $\beta \approx 0.09$, i.e. up to this noise level it makes sense to use the QKR protocol.
The proof of Theorem 4.1 is given in Section 7. The full security proof for the protocol is given in Section 5.

5 Security of the protocol

From Theorem 4.1 we construct a security proof for the QKR protocol. We define

$$\alpha_{n\ell\beta} \stackrel{\text{def}}{=} \sqrt{2^{\ell - n + 2n\log f(\beta)}} \quad ; \quad \varepsilon_r^{n\ell\beta} \stackrel{\text{def}}{=} \frac{3}{2^{\ell+1}}\binom{r}{2} + \frac{(1+\alpha_{n\ell\beta})^r - 1}{2} \tag{8}$$

and

$$1 - \Omega_N^{n\ell\beta} \stackrel{\text{def}}{=} \prod_{r=1}^{N}(1 - \varepsilon_r^{n\ell\beta} - 2^{-\lambda}). \tag{9}$$

Consider the worst case scenario: Eve knows the plaintext in rounds $1 \dots N$ and wants to learn the plaintext in round $N+1$.

- In round 1, Eve starts without (quantum or classical) side information from previous rounds. Since she already knows the plaintext in this round, the best she can do is extract information into ancilla states without causing a Reject. As she has no side information yet, the only way to create her ancilla states is according to Section 2.3, possibly with i-dependent bit error probability.
- At the beginning of round 2, the security of the keys U, B is perfect except with probability less than $\varepsilon_1^{n\ell\beta} + 2^{-\lambda}$. The $\varepsilon_1^{n\ell\beta}$ follows from Theorem 4.1 and represents the probability that Eve can learn something from the ancillas. The $2^{-\lambda}$ is the probability that the MAC verification accidentally fails to notice a problem. With probability higher than $1 - \varepsilon_1^{n\ell\beta} - 2^{-\lambda}$, Eve is in a situation where she has no side information that could help her to mount a better ancilla strategy than the one of Section 2.3.
- At the beginning of round 3, the security of the keys U, B is perfect with probability larger than $(1 - \varepsilon_1^{n\ell\beta} - 2^{-\lambda})(1 - \varepsilon_2^{n\ell\beta} - 2^{-\lambda})$. Etcetera.
- After round N, the keys U, B are perfectly secure with probability larger than $\prod_{r=1}^{N}(1 - \varepsilon_r^{n\ell\beta} - 2^{-\lambda}) = 1 - \Omega_N^{n\ell\beta}$.

For 8-state encoding the analysis ends here. With probability larger than $1 - \Omega_N^{n\ell\beta}$ Eve has no way to attack the plaintext, since the plaintext x^{N+1} is random and the 8-state encoding is essentially Quantum-One-Time-Padding with a perfectly random key. Hence x^{N+1} is $\Omega_N^{n\ell\beta}$-secure.
For 4-state and 6-state encoding Eve has a second attack method. In any of the rounds (say round r) she may steal all the qubits (causing a Reject) and extract partial information about x^r from the stolen qubits. This is called the 'M1 attack' in [1]. This attack has to be countered by applying a proper amount of Privacy Amplification, i.e. choosing the correct value for the message length ℓ. Expressed in terms of min-entropy loss, 4-state encoding leaks $1 - \log(\cos\frac{\pi}{8})^{-2} \approx 0.77$ bits per qubit; 6-state encoding leaks $1 - \log(\cos\frac{\alpha}{2})^{-2} \approx 0.66$ bits per qubit, with α as defined in Section 2.2. This leakage does not depend on β. It exists already at $\beta = 0$. The length parameter ℓ must satisfy two requirements: (i) the amount of

privacy amplification $(n-\ell)$ must be sufficiently large to compensate for the above-mentioned leakage; (ii) the $\Omega_N^{n\ell\beta}$ must be small.

Let $\alpha_{n\ell\beta} < \frac{1}{N}$. Then we can bound $\Omega_N^{n\ell\beta}$ as

$$\Omega_N^{n\ell\beta} < \frac{N}{2^\lambda} + \sum_{r=1}^{N} \varepsilon_r^{n\ell\beta} = \frac{N}{2^\lambda} + \frac{3}{2^{\ell+1}}\binom{N+1}{3} + \frac{(1+\alpha_{n\ell\beta})^{N+1} - 1 - (N+1)\alpha_{n\ell\beta}}{2\alpha_{n\ell\beta}} \quad (10)$$

$$\leq \frac{N}{2^\lambda} + \frac{3}{2^{\ell+1}}\binom{N+1}{3} + \frac{3}{4}\binom{N+1}{2}\alpha_{n\ell\beta}. \quad (11)$$

6 Discussion

6.1 Choosing the parameter values

Consider 8-state encoding, and the case that Bob Accepts $N+1$ consecutive rounds. The total message size is $(N+1)\ell$. The total key expenditure consists of $N+1$ λ-bit OTPs that protect the authentication tags, $N+1$ a-bit OTPs that protect the syndromes (asymptotically $a \approx nh(\beta)$), $2n$ bits of basis key b, and $\mathcal{O}(N \log N)$ bits of extractor key. We look at the QKR 'rate', which we express as the message length minus the key expenditure, per round and per qubit. For the message length we set $\ell = n - 2n \log f(\beta) - 2 \log \frac{3N^2}{8\Omega}$ in order to obtain $\Omega_N^{n\ell\beta} \approx \Omega$ for some small constant Ω.

$$\frac{|\text{total msg}| - |\text{total key}|}{(N+1)n} = 1 - \frac{a}{n} - 2\log f(\beta) - \frac{\lambda}{n} - \frac{2}{N+1} - \frac{\mathcal{O}(\log N)}{n} - \frac{2\log\frac{3N^2}{8\Omega}}{n}. \quad (12)$$

Note that λ is a constant w.r.t. n but has to grow as $\log N$. We see that the highest rate is obtained by setting $N \gg 1$, $n \gg \log N$. The asymptotic rate is $1 - h(\beta) - 2\log f(\beta)$. See Fig. 1. The asymptotic rate is positive up to $\beta \approx 0.09$. Up to this noise level using QKR makes sense.

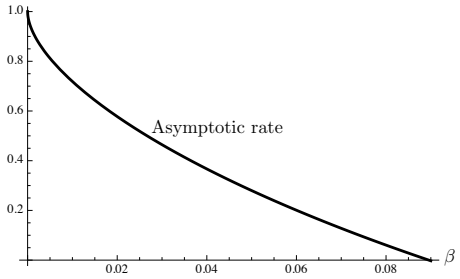

Figure 1: *The asymptotic rate* $1 - h(\beta) - 2\log f(\beta)$.

It is possible to reduce the key expenditure. "Scheme #3" in [9] 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 (12).

6.2 Comparison to existing results

The proof technique of Fehr and Salvail [8] requires a special property ('key privacy') of the MAC function, and they have to keep track of the security of the MAC key. We avoid

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

The min-entropy analysis of attacks in [1] has turned out to be too pessimistic in certain respects. For the 'K2 attack' (a known-plaintext attack on b) a min-entropy loss of $\log(\sqrt{6\beta(1-\frac{3}{2}\beta)}+1)$ bits per qubit was found for 8-state encoding; that is considerably more than our leakage result $2\log f(\beta)$ in Theorem 4.1. Clearly min-entropy is too pessimistic as a measure of security in this context. Note that in [8] all security bounds are expressed in terms of min-entropy.

6.3 Dealing with erasures

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

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

The security is not negatively affected by the existence of erasures. Assume that Eve holds all the qubits that have not reached Bob. Since the data in the qubits is random, and does

not contribute to the computation of z', it holds that (i) it is not important if Eve learns the content of these bits, (ii) known plaintext does not translate to partial knowledge of the data content of these qubits, which would endanger the basis key b and the extractor key u.

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

6.4 Future work

It is interesting to note that QKR protocols which first send a random string z and then use z for OTP encryption look a lot like Quantum Key Distribution, but with reduced communication complexity. This changes when the message is put directly into the qubits, e.g. as is done in Gottesman's Unclonable Encryption [5]. It remains a topic for future work to prove security of such a QKR scheme.

The QKR scheme of Section 3 can be improved and embellished in various ways. For instance, the λ-bit key expenditure for protecting the MAC-key may not be necessary if the MAC function is properly chosen. 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 [8]).

Furthermore, as mentioned in Section 6.1, one may use 'scheme #3' of [9] which protects the syndrome by sending it through the quantum channel instead of classically OTP-ing it. This reduces the key expenditure but does not affect the rate.

Another interesting option is to deploy the Quantum One Time Pad with approximately half the key length, which still yields information-theoretic security. This would improve the rate (12) by reducing the term $\frac{2}{N+1}$ to approximately $\frac{1}{N+1}$.

Instead of $2N$-wise independent hashing one may use 'almost $2N$-wise independence' [12]. A small security penalty is incurred, but the size of the extractor key u is reduced.

We suspect that the inequality in (7) is not tight. Given the similarities between QKR and QKD we would intuitively expect that the required amount of privacy amplification is the same as for QKD. A known result for QKD, based on von Neumann entropy, is $-(1-\frac{3}{2}\beta)\log(1-\frac{3}{2}\beta)-\frac{3}{2}\beta\log\frac{\beta}{2}-h(\beta)$, which is less than the $2n\log f(\beta)$ of (7) for all β. Perhaps an improved proof technique can get closer to the QKD result.

7 Proof of Theorem 4.1

7.1 Rewriting the statistical distance

We allow Eve to cause different bit error probabilities $\beta_i^r \in [0,\frac{1}{2})$ in each round r and qubit position i individually. The combined quantum-classical state of all Eve's ancillas, together with the classical variables of interest, is given by $\mathbb{E}_{ub}|ub\rangle\langle ub|\otimes\rho(zub)$, with

$$\begin{aligned}\rho(zub) &= \bigotimes_{r=1}^{N}\mathbb{E}_{x^r:z^r=\mathtt{Ext}(u,x^r)}\bigotimes_{i=1}^{n}\omega_{x_i^r}^{b_i}(\beta_i^r)\\ &= \bigotimes_{r=1}^{N}2^{\ell}\sum_{x^r\in\{0,1\}^n}\delta_{z^r,\mathtt{Ext}(u,x^r)}\bigotimes_{i=1}^{n}\tfrac{1}{2}\omega_{x_i^r}^{b_i}(\beta_i^r),\end{aligned}\tag{13}$$

where $\omega_{x_i^r}^{b_i}$ is defined as in (6). For notational convenience we introduce two averaged quantities, $\chi_z \stackrel{\text{def}}{=} \mathbb{E}_{ub}\rho(zub)$ and $\rho_{\text{av}} \stackrel{\text{def}}{=} \mathbb{E}_z\rho(zub)$. The ρ_{av} is easy to compute by summing over the Kronecker deltas in (13),

$$\rho_{\text{av}} = \bigotimes_{r=1}^{N}\bigotimes_{i=1}^{n}\frac{\omega_0^{b_i}(\beta_i^r)+\omega_1^{b_i}(\beta_i^r)}{2}. \tag{14}$$

Note that ρ_{av} does not actually depend on b, since from (6) it follows that

$$\frac{\omega_0^b(\beta)+\omega_1^b(\beta)}{2} = (1-\tfrac{3}{2}\beta)|m_0\rangle\langle m_0| + \tfrac{\beta}{2}(\mathbb{1}-|m_0\rangle\langle m_0|). \tag{15}$$

We define $D \stackrel{\text{def}}{=} d(UB|Z\rho(ZUB))$. We have

$$\begin{aligned} D &= \mathbb{E}_z d(UB|\rho(zUB)) \\ &= \mathbb{E}_z\delta\Big(\mathbb{E}_{ub}|ub\rangle\langle ub|\otimes\rho(zub);\ \mathbb{E}_{ub}|ub\rangle\langle ub|\otimes\mathbb{E}_{u'b'}\rho(zu'b')\Big) \\ &= \tfrac{1}{2}\mathbb{E}_{zub}\big\|\rho(zub)-\chi_z\big\|_1. \end{aligned} \tag{16}$$

In the last line we have used the block structure of $\mathbb{E}_{ub}|ub\rangle\langle ub|\otimes(\cdots)$ to move the $\mathbb{E}_{ub}$ out of the trace norm. Next we apply the triangle inequality.

$$\begin{aligned} D &\leq \tfrac{1}{2}\mathbb{E}_{zub}\|\rho(zub)-\rho_{\text{av}}\|_1 + \tfrac{1}{2}\mathbb{E}_{zub}\|\rho_{\text{av}}-\chi_z\|_1 \\ &= \tfrac{1}{2}\mathbb{E}_{zub}\|\rho(zub)-\rho_{\text{av}}\|_1 + \tfrac{1}{2}\mathbb{E}_{z}\|\rho_{\text{av}}-\chi_z\|_1 \\ &\stackrel{\text{def}}{=} D_1 + D_2. \end{aligned} \tag{17}$$

In the next two subsections we upper bound D_1 and D_2.

7.2 Bounding the D_2 term

Case 1: the $z^1\cdots z^N$ are mutually distinct.
By the defining property of N-wise independent hashing, taking the expectation $\mathbb{E}_u$ over the product $\prod_{r=1}^N \delta_{z^r,\texttt{Ext}(u,x^r)}$ simply yields a factor $2^{-\ell N}$ and generates the constraint that the strings $x^1,\ldots,x^N$ are mutually distinct. Thus we get

$$\chi_z = \mathbb{E}_b\, 2^{-nN}\sum_{x\,\text{distinct}}\bigotimes_{r=1}^{N}\bigotimes_{i=1}^{n}\omega_{x_i^r}^{b_i}(\beta_i^r). \tag{18}$$

On the other hand, ρ_{av} can be expressed in a similar way but without the constraint, namely $\rho_{\text{av}} = \mathbb{E}_b 2^{-nN}\sum_x\bigotimes_{r=1}^N\bigotimes_{i=1}^n\omega_{x_i^r}^{b_i}(\beta_i^r)$. Taking the difference yields

$$\|\rho_{\text{av}}-\chi_z\|_1 = \Big\|2^{-nN}\,\mathbb{E}_b\sum_{\substack{x^1\cdots x^N\\ \text{not distinct}}}\bigotimes_{r=1}^{N}\bigotimes_{i=1}^{n}\omega_{x_i^r}^{b_i}(\beta_i^r)\Big\|_1. \tag{19}$$

This expression can be bounded by counting terms in the x-summation.

$$\begin{aligned}
\|\rho_{\rm av}-\chi_z\|_1 &= 2^{-nN}\#\{\text{not distinct } x\}\Big\|\mathbb{E}_b\mathbb{E}_{\substack{x^1\cdots x^N\\ \text{not distinct}}}\bigotimes_{r=1}^{N}\bigotimes_{i=1}^{n}\omega_{x_i^r}^{b_i}(\beta_i^r)\Big\|_1\\
&= 2^{-nN}\#\{\text{not distinct } x\}\|\text{normalised mixed state}\|_1\\
&= 2^{-nN}\#\{\text{not distinct } x\}\\
&= 2^{-nN}\Big[2^{nN}-\prod_{a=0}^{N-1}(2^n-a)\Big]=1-\prod_{a=0}^{N-1}(1-\frac{a}{2^n})\\
&\leq \sum_{a=0}^{N-1}\frac{a}{2^n}=\frac{1}{2^n}\binom{N}{2}. \qquad (20)
\end{aligned}$$

Case 2: more than 0 collisions exist in $z^1\cdots z^N$. In this case we use $\|\rho_{\rm av}-\chi_z\|_1\leq 2$. Combining the two cases, we derive a bound on D_2 as follows,

$$\begin{aligned}
D_2 &= \tfrac{1}{2}\mathbb{E}_z\|\rho_{\rm av}-\chi_z\|_1=\frac{1}{2\#z}\sum_{z\,\text{dist}}\|\rho_{\rm av}-\chi_z\|_1+\frac{1}{2\#z}\sum_{z\,\text{not dist}}\|\rho_{\rm av}-\chi_z\|_1\\
&\leq \frac{1}{2}\frac{\#\{\text{distinct } z\}}{\#z}2^{-n}\binom{N}{2}+\frac{\#\{\text{not distinct } z\}}{\#z}\\
&< \tfrac{1}{2}\cdot 2^{-n}\binom{N}{2}+2^{-\ell}\binom{N}{2}<\tfrac{3}{2}\cdot 2^{-\ell}\binom{N}{2}. \qquad (21)
\end{aligned}$$

7.3 Bounding the D_1 term

We start from $D_1\stackrel{\rm def}{=}\frac{1}{2}\mathbb{E}_{zub}\|\rho(zub)-\rho_{\rm av}\|_1=\frac{1}{2}\mathbb{E}_{zub}{\rm tr}\sqrt{[\rho(zub)-\rho_{\rm av}]^2}$. We apply Jensen's matrix inequality under the trace in order to move $\mathbb{E}_{zu}$ into the square root, and then use the fact that $\rho_{\rm av}=\mathbb{E}_{zu}\rho$.

$$D_1\leq\tfrac{1}{2}\mathbb{E}_b{\rm tr}\sqrt{\mathbb{E}_{zu}[\rho-\rho_{\rm av}]^2}=\tfrac{1}{2}\mathbb{E}_b{\rm tr}\sqrt{\mathbb{E}_{zu}\rho^2-\rho_{\rm av}^2}. \qquad (22)$$

Next we expand ρ twice and write

$$\begin{aligned}
\mathbb{E}_{zu}\rho^2 &= \mathbb{E}_{zu}\bigotimes_{r=1}^{N}2^{2\ell}\sum_{x^ry^r}\delta_{z^r,\mathtt{Ext}(u,x^r)}\delta_{z^r,\mathtt{Ext}(u,y^r)}\bigotimes_{i=1}^{n}\tfrac{1}{4}\omega_{x_i^r}^{b_i}(\beta_i^r)\omega_{y_i^r}^{b_i}(\beta_i^r) \qquad (23)\\
&= \mathbb{E}_u\bigotimes_{r=1}^{N}2^{\ell}\sum_{x^ry^r}\delta_{\mathtt{Ext}(u,x^r),\mathtt{Ext}(u,y^r)}\bigotimes_{i=1}^{n}\tfrac{1}{4}\omega_{x_i^r}^{b_i}(\beta_i^r)\omega_{y_i^r}^{b_i}(\beta_i^r) \qquad (24)\\
&= \sum_{xy}\Big[\mathbb{E}_u\prod_{r=1}^{N}\delta_{\mathtt{Ext}(u,x^r),\mathtt{Ext}(u,y^r)}\Big]\bigotimes_{r=1}^{N}2^{\ell}\bigotimes_{i=1}^{n}\tfrac{1}{4}\omega_{x_i^r}^{b_i}(\beta_i^r)\omega_{y_i^r}^{b_i}(\beta_i^r) \qquad (25)
\end{aligned}$$

The $\mathbb{E}_u \delta \cdots \delta$ is evaluated using the properties of $2N$-wise independent hash functions. Every occurrence $x^r \neq y^r$ gives rise to a factor $2^{-\ell}$, whereas $x^r = y^r$ yields a factor 1.

$$\begin{aligned}
\mathbb{E}_{uz}\rho^2 &= \bigotimes_{r=1}^{N} \sum_{x^r y^r} [2^\ell \delta_{x^r y^r} + (1 - \delta_{x^r y^r})] \bigotimes_{i=1}^{n} \tfrac{1}{4} \omega_{x_i^r}^{b_i}(\beta_i^r) \omega_{y_i^r}^{b_i}(\beta_i^r) && (26)\\
&= \bigotimes_{r=1}^{N} \sum_{x^r y^r} [(2^\ell - 1)\delta_{x^r y^r} + 1] \bigotimes_{i=1}^{n} \tfrac{1}{4} \omega_{x_i^r}^{b_i}(\beta_i^r) \omega_{y_i^r}^{b_i}(\beta_i^r) && (27)\\
&= \bigotimes_{r=1}^{N} \Big[(2^\ell - 1) \bigotimes_{i=1}^{n} \frac{[\omega_0^{b_i}(\beta_i^r)]^2 + [\omega_1^{b_i}(\beta_i^r)]^2}{4} + \bigotimes_{i=1}^{n} \Big(\frac{\omega_0^{b_i}(\beta_i^r) + \omega_1^{b_i}(\beta_i^r)}{2} \Big)^2 \Big]. && (28)
\end{aligned}$$

7.3.1 Diagonalisation

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

$$|E_{01}^{\boldsymbol{v}}\rangle = \sqrt{\frac{1 - \frac{3}{2}\beta}{1 - \beta}} |m_0\rangle + \sqrt{\frac{\frac{1}{2}\beta}{1 - \beta}} |\boldsymbol{v} \cdot \boldsymbol{m}\rangle. \tag{29}$$

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

$$\begin{aligned}
[\omega_x^b(\beta)]^2 &= (1-\beta)^2 \sigma_{x\bar{x}}^{\boldsymbol{v}(b)} + \beta^2 \sigma_{xx}^{\boldsymbol{v}(b)} && (30)\\
[\omega_0^b(\beta)]^2 + [\omega_1^b(\beta)]^2 &= (1-\beta)^2 [\sigma_{01}^{\boldsymbol{v}(b)} + \sigma_{10}^{\boldsymbol{v}(b)}] + \beta^2 [\sigma_{00}^{\boldsymbol{v}(b)} + \sigma_{11}^{\boldsymbol{v}(b)}]\\
&= 2(1-\beta)^2 \Big[\frac{1 - \frac{3}{2}\beta}{1-\beta} |m_0\rangle\langle m_0| + \frac{\frac{1}{2}\beta}{1-\beta} |\boldsymbol{v}(b) \cdot \boldsymbol{m}\rangle\langle \boldsymbol{v}(b) \cdot \boldsymbol{m}| \Big]\\
&\quad + \beta^2 [\sigma_{00}^{\boldsymbol{v}(b)} + \sigma_{11}^{\boldsymbol{v}(b)}]. && (31)
\end{aligned}$$

Furthermore

$$\begin{aligned}
[\omega_0^b(\beta) + \omega_1^b(\beta)]^2 &= (1-\beta)^2 [\sigma_{01}^{\boldsymbol{v}(b)} + \sigma_{10}^{\boldsymbol{v}(b)}]^2 + \beta^2 [\sigma_{00}^{\boldsymbol{v}(b)} + \sigma_{11}^{\boldsymbol{v}(b)}]\\
&= 4(1-\beta)^2 \Big[\frac{(1 - \frac{3}{2}\beta)^2}{(1-\beta)^2} |m_0\rangle\langle m_0| + \frac{(\frac{1}{2}\beta)^2}{(1-\beta)^2} |\boldsymbol{v}(b) \cdot \boldsymbol{m}\rangle\langle \boldsymbol{v}(b) \cdot \boldsymbol{m}| \Big]\\
&\quad + \beta^2 [\sigma_{00}^{\boldsymbol{v}(b)} + \sigma_{11}^{\boldsymbol{v}(b)}] && (32)
\end{aligned}$$

We see that the matrices $(\omega_0^b)^2 + (\omega_1^b)^2$ and $(\omega_0^b + \omega_1^b)^2$ are simultaneously diagonal in the basis $|m_0\rangle$, $|\boldsymbol{v} \cdot \boldsymbol{m}\rangle$, $|E_{00}^{\boldsymbol{v}}\rangle$, $|E_{11}^{\boldsymbol{v}}\rangle$. Note that $\omega_0^b + \omega_1^b$ does not actually depend on b; see (15). The eigenvalues of $(\omega_0^b)^2 + (\omega_1^b)^2$ are

$$\lambda[1] \stackrel{\text{def}}{=} 2(1-\beta)(1 - \tfrac{3}{2}\beta); \quad \lambda[2] \stackrel{\text{def}}{=} \beta(1-\beta); \quad \lambda[3] \stackrel{\text{def}}{=} \beta^2; \quad \lambda[4] \stackrel{\text{def}}{=} \beta^2. \tag{33}$$

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

$$\mu[1] \stackrel{\text{def}}{=} 4(1 - \tfrac{3}{2}\beta)^2; \quad \mu[2] \stackrel{\text{def}}{=} \beta^2; \quad \mu[3] \stackrel{\text{def}}{=} \beta^2; \quad \mu[4] \stackrel{\text{def}}{=} \beta^2. \tag{34}$$

7.3.2 Finalising the bound on D_1

We label an eigenvector by N strings: $A^r \in \{1,2,3,4\}^n$, $r \in \{1, \ldots, N\}$. The index $A_i^r \in \{1,2,3,4\}$ indicates which eigenvector is selected in round r and position i. The total eigenstate is composed by taking the tensor product of all the single-ancilla eigenstates.

We introduce the notation $v_A^r = (2^\ell - 1)\prod_i \frac{1}{4}\lambda[A_i^r]$ and $w_A^r = \prod_i \frac{1}{4}\mu[A_i^r]$. Given label A, the eigenvalue of $\mathbb{E}_{zu}\rho^2$ is $\Lambda_A = \prod_{r=1}^N (v_A^r + w_A^r)$. The corresponding eigenvalue of ρ_{av}^2 is $M_A = \prod_{r=1}^N w_A^r$. Now we can write

$$\begin{aligned}
\operatorname{tr}\sqrt{\mathbb{E}_{zu}\rho^2 - \rho_{\text{av}}^2} &= \sum_A \sqrt{\Lambda_A - M_A} = \sum_A \sqrt{\prod_{r=1}^N (v_A^r + w_A^r) - \prod_{r=1}^N w_A^r} && (35)\\
&= \sum_A \sqrt{\sum_{\mathcal{G}\subseteq[N]:\mathcal{G}\neq\emptyset} \Big(\prod_{r\in\mathcal{G}} v_A^r\Big)\Big(\prod_{a\in[N]\setminus\mathcal{G}} w_A^a\Big)} && (36)\\
&\leq \sum_A \sum_{\mathcal{G}\subseteq[N]:\mathcal{G}\neq\emptyset} \Big(\prod_{r\in\mathcal{G}} \sqrt{v_A^r}\Big)\Big(\prod_{a\in[N]\setminus\mathcal{G}} \sqrt{w_A^a}\Big) && (37)\\
&= \sum_{\mathcal{G}\subseteq[N]:\mathcal{G}\neq\emptyset} \Big(\prod_{r\in\mathcal{G}} \sqrt{2^\ell - 1}\prod_i \tfrac{1}{2}\sum_{A_i^r} \sqrt{\lambda[A_i^r]}\Big)\Big(\prod_{a\in[N]\setminus\mathcal{G}} \prod_i \tfrac{1}{2}\sum_{A_i^a} \sqrt{\mu[A_i^a]}\Big). && (38)
\end{aligned}$$

To arrive at (37) we used the inequality $\sqrt{q_1 + \cdots + q_N} \leq \sqrt{q_1} + \cdots + \sqrt{q_N}$, which holds for $q_1, \ldots, q_N \geq 0$. From the definition of the λ and μ eigenvalues (33,34) we have $\sum_{x=1}^4 \sqrt{\mu[x]} = 2$ and $\sum_{x=1}^4 \sqrt{\lambda[x]} = f(\beta)\sqrt{2}$, with $f(\beta)$ as defined in Theorem 4.1. Thus we can write

$$\begin{aligned}
\operatorname{tr}\sqrt{\mathbb{E}_{zu}\rho^2 - \rho_{\text{av}}^2} &\leq \sum_{\mathcal{G}\subseteq[N]:\mathcal{G}\neq\emptyset} \Big(\prod_{r\in\mathcal{G}} \sqrt{2^\ell - 1}\prod_{i=1}^n \frac{1}{\sqrt{2}} f(\beta_i^r)\Big)\cdot 1 && (39)\\
&< \prod_{r=1}^N \Big[1 + \sqrt{2^{\ell-n}}\prod_{i=1}^n f(\beta_i^r)\Big] - 1 && (40)\\
&= \prod_{r=1}^N \Big[1 + \sqrt{2^{\ell-n+2\sum_{i=1}^n \log f(\beta_i^r)}}\Big] - 1. && (41)
\end{aligned}$$

Eve is allowed to choose the error probability β_i^r as a function of the round r and the qubit position i. However, the average noise in every round must not exceed a fixed parameter β. Since the function $\log f$ is concave, it is optimal for Eve to set $\beta_i^r = \beta$ for all r, i. This yields

$$2D_1 < \Big[1 + \sqrt{2^{\ell-n+2n\log f(\beta)}}\Big]^N - 1. \tag{42}$$

Together with (21) this finalizes the proof of Theorem 4.1.

Acknowledgements

Part of this research was funded by NWO (CHIST-ERA project ID_IOT).

References

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

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

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

[4] 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.

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

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

[7] 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.

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

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

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

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

[12] N. Alon, O. Goldreich, and Y. Mansour. Almost k-wise independence versus k-wise independence. *Information Processing Letters*, 88(3):107–110, 2003.

[13] Y. Dodis, K. Pietrzak, and D. Wichs. Key derivation without entropy waste. In *Eurocrypt 2014*. Springer, 2014.

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

[15] 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.

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

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

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