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 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 scheme for the noisy case was proposed by Škorić and de Vries [2], based on eight-state encoding, which reduces leakage. However, a security proof was not given.
In this paper we introduce a small protocol modification to [2] and provide a security proof. Our proof is based on a bound on the trace distance between the real quantum state of the system and a state in which the keys are completely secure. We determine how much privacy amplification is needed as a function of the tolerated bit error rate. It turns out that less privacy amplification is needed than suggested by previous results.

1 Introduction

1.1 Quantum Key Recycling

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

QKR scheme (similar to [5]) that does not need a quantum computer, and they were able to prove its security in the regime of extremely low noise. Škorić and de Vries [2] proposed a variant with 8-state encoding, which drastically reduces the need for privacy amplification. It is meant to operate at 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 with 8-state encoding, taking an 'engineering' point of view: we do not aim for complete key re-use, but rather for a high ratio of message length versus expended key bits.

- We introduce a small modification in the QKR protocol of Škorić and de Vries [2]. A constant amount of key material (not proportional to the message size) is refreshed even in case of an Accept.
- We give a security proof. We use the EPR formulation of the protocol. First we consider attacks in which Eve collects quantum side information from one EPR pair at a time; then we apply the post-selection method in order to obtain security against general attacks. We derive a non-asymptotic upper bound on the amount of privacy amplification as a function of the number of qubits (n) and the tolerated bit error rate (β).
- Asymptotically (large n, and without any further tricks such as smoothening) our bound on the privacy amplification is $nh(\beta) + 2n \log[\sqrt{(1-\beta)(1-\frac{3}{2}\beta)} + \sqrt{\frac{3}{2}\beta(1+\beta)}]$ bits. This result is more favourable than the min-entropy analysis in [9] and straightforward generalisations of [1] to the noisy case. A positive rate is possible up to $\beta \approx 0.069$.

The outline of the paper is as follows. In the preliminaries section we introduce notation; we briefly review proof techniques and methods for embedding classical bits in qubits, and we summarise known results regarding Eve's optimal extraction of information from a qubit into a four-dimensional ancilla state. In Section 3 we motivate why we depart from the entanglement-monogamy based proof technique. In Section 4 we present the modified QKR protocol. Section 5 states the main theorems and discusses rates and optimal parameter choices. In Section 6 we compare to existing results, discuss erasures, and suggest topics for future work.

2 Preliminaries

2.1 Notation and terminology

Classical Random Variables (RVs) are denoted with capital letters, and their realisations with lowercase letters. The probability that a RV X takes value x is written as $\Pr[X = x]$. The expectation with respect to RV X is denoted as

$\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X=x] f(x)$. Sets are denoted in calligraphic font. We write $[n]$ for the set $\{1,\ldots,n\}$. For a string x and a set of indices $\mathcal{I}$ the notation $x_\mathcal{I}$ means the restriction of x to the indices in $\mathcal{I}$. The notation 'log' stands for the logarithm with base 2. The notation h stands for the binary entropy function $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. 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 $\sigma_x, \sigma_y, \sigma_z$, and we write $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. The standard basis is the eigenbasis of σ_z, with $|0\rangle$ in the positive z-direction. We write $\mathbb{1}$ for the identity matrix. The notation 'tr' stands for trace. The Hermitian conjugate of an operator A is written as $A^\dagger$. The complex conjugate of z is denoted as z^*. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. The trace distance between matrices ρ and σ is denoted as $\delta(\rho;\sigma) = \frac{1}{2}||\rho-\sigma||_1$. It is a generalisation of the statistical distance and represents the maximum possible advantage one can have in distinguishing ρ from σ.

Consider a uniform classical variable X and a mixed state ρ_X that depends on X. The combined classical-quantum state is $\rho^{\mathrm{XE}} = \mathbb{E}_x |x\rangle\langle x| \otimes \rho^{\mathrm{E}}_x$. The state of a sub-system is obtained by tracing out one subspace, e.g. $\rho^{\mathrm{E}} = \mathrm{tr}_X \rho^{\mathrm{XE}} = \mathbb{E}_x \rho^{\mathrm{E}}_x$. 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 [10],

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

i.e. the distance between the true classical-quantum state and a state in which X is completely unknown to Eve. X is said to be ε-secure with respect to ρ if $d(X|\rho) \le \varepsilon$. When this is the case, it can be considered that X is 'ideal' except with probability ε.

A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{T}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [11] if for all distinct pairs $x, x' \in \mathcal{X}$ and all pairs $y, y' \in \mathcal{T}$ it holds that $\Pr_{h\in H}[h(x) = y \wedge h(x') = y'] = |\mathcal{T}|^{-2}$. Here the probability is over random $h \in H$. Pairwise independence can be achieved with a hash family of size $|H| = |\mathcal{X}|$.

2.2 QKR proof structure

The protocol (see Section 4) has three basic steps. (i) Alice sends quantum states and classical data to Bob. (ii) Bob responds with a decision bit $c \in \{Accept, Reject\}$. (iii) In case of Accept, most of the key material K is re-used; in case of Reject, the key material is refreshed from K to K'.

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

2.3 Post-selection

In a *collective attack* Eve acts on individual qudits. This is not the most general attack. For protocols that obey permutation symmetry, a post-selection argument [12] can be used to show that ε-security against collective attacks implies ε'-security against general attacks, with $\varepsilon' = \varepsilon(n+1)^{d^4-1}$, where d is the dimension ($d = 2$ for qubits). Hence, by paying a modest price in terms of privacy amplification, e.g. changing the usual privacy amplification term $2 \log \frac{1}{\varepsilon}$ to $2 \log \frac{1}{\varepsilon} + 2(d^4 - 1) \log(n+1)$, one can 'buy' security against general attacks.

2.4 Encoding a classical bit in a qubit

We briefly review methods for embedding a classical bit $g \in \{0, 1\}$ into a qubit state. The standard basis is $|0\rangle, |1\rangle$ with $|0\rangle$ the positive z-direction on the Bloch sphere. The set of bases used is denoted as $\mathcal{B}$, and a basis choice as $b \in \mathcal{B}$. The encoding of bit value g in basis b is written as $|\psi_{bg}\rangle$. In BB84 encoding we write $\mathcal{B} = \{0, 1\}$, with $|\psi_{00}\rangle = |0\rangle$, $|\psi_{01}\rangle = |1\rangle$, $|\psi_{10}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|\psi_{11}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. In six-state encoding [13] the vectors are $\pm x$, $\pm y$, $\pm z$ on the Bloch sphere. For 8-state encoding [2] we have $\mathcal{B} = \{0, 1, 2, 3\}$ and the eight states are the corner points of a cube on the Bloch sphere. We write $b = 2u + w$, with $u, w \in \{0, 1\}$. The states are

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

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

2.5 Eve's ancilla state

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

$$\sigma^{\boldsymbol{v}}_{xy} \stackrel{\mathrm{def}}{=} |E^{\boldsymbol{v}}_{xy}\rangle\langle E^{\boldsymbol{v}}_{xy}|. \tag{3}$$

$$\begin{aligned}
|E^{\boldsymbol{v}}_{01}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\tfrac{3}{2}\gamma}|m_0\rangle + \sqrt{\tfrac{\gamma}{2}}\left(v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle\right)\right]\\
|E^{\boldsymbol{v}}_{10}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\tfrac{3}{2}\gamma}|m_0\rangle - \sqrt{\tfrac{\gamma}{2}}\left(v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle\right)\right]\\
|E^{\boldsymbol{v}}_{00}\rangle &= \frac{1}{\sqrt{2(1-v_z^2)}}\left[(-v_xv_z - iv_y)|m_1\rangle + (-v_yv_z + iv_x)|m_2\rangle + (1-v_z^2)|m_3\rangle\right]\\
|E^{\boldsymbol{v}}_{11}\rangle &= \frac{1}{\sqrt{2(1-v_z^2)}}\left[(-v_xv_z + iv_y)|m_1\rangle + (-v_yv_z - iv_x)|m_2\rangle + (1-v_z^2)|m_3\rangle\right].
\end{aligned} \tag{4}$$

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 $|\frac{-v_xv_z - iv_y}{\sqrt{1-v_z^2}}|^2 = 1-v_x^2$ 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 $|E^{\boldsymbol{v}}_{11}\rangle = |E^{-\boldsymbol{v}}_{00}\rangle$.

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

3 Motivation

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 [18]. It yields a trace distance $\sqrt{2^{\ell} p_{\text{win}}}$ between ideality and reality, where p_{win} is the winning probability, $p_{\text{win}} \leq \mu^n 2^{nh(\beta)}$ (asymptotically), where $\mu = \frac{1}{|\mathcal{B}|} + \frac{|\mathcal{B}|-1}{|\mathcal{B}|}\sqrt{\max_{bb' \in \mathcal{B}: b' \neq b} \max_{xx'} \|F_x^b F_{x'}^{b'}\|_{\infty}}$. Here F_x^b is the projection operator that corresponds to data bit $x \in \{0,1\}$ in the basis b. The value of μ is given by $\mu_4 = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} \approx 0.85$, $\mu_6 = \frac{1}{3} + \frac{2}{3}\sqrt{\frac{1}{2}} \approx 0.80$, $\mu_8 = \frac{1}{4} + \frac{3}{4}\sqrt{\frac{2}{3}} \approx 0.86$ for 4-state, 6-state and 8-state encoding respectively.[2] 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 superior properties [9]. Our aim is to obtain a tighter bound on the trace distance for 8-state QKR.

4 Our adapted QKR protocol

In this paper we consider the QKR scheme #2 proposed in [2], which is a slightly modified version of the QEMC* scheme of Fehr and Salvail [1]. We introduce a small change in the protocol:

- A small amount of key refreshment of the basis key occurs even in case of an Accept.

The key material shared between Alice and Bob consists of five parts: a basis sequence $b \in \mathcal{B}^n$, a MAC key $k_{\text{MAC}} \in \{0,1\}^{\lambda}$, an extractor key[3] $u \in \mathcal{U}$, an extractor key $v \in \mathcal{V}$, and a classical OTP $k_{\text{syn}} \in \{0,1\}^a$ for protecting the syndrome. The plaintext is $\mu \in \{0,1\}^{\ell}$.
Alice and Bob have agreed on a pairwise independent hash function $\texttt{Ext} : \mathcal{U} \times \{0,1\}^n \to \{0,1\}^{\ell}$, a pairwise independent hash function $\texttt{Mix} : \mathcal{V} \times \mathcal{B}^{n+q} \to \mathcal{B}^n$, a MAC function $M : \{0,1\}^{\lambda} \times \{0,1\}^{n+\ell+a} \to \{0,1\}^{\lambda}$, 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.[4]

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

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

[4] 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.

The basis set $\mathcal{B}$ and the functions $\texttt{Ext}, \texttt{Mix}, M, \texttt{Syn}, \texttt{SynDec}$ are publicly known.
Encryption
Alice performs the following steps. Generate random $x \in \{0,1\}^n$. Compute $s = k_{\text{syn}} \oplus \texttt{Syn}(x)$ and $z = \texttt{Ext}(u, x)$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $\tau = M(k_{\text{MAC}}, x||c||s)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_{b_i x_i}\rangle$ according to Section 2.4. 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 $\hat{x} = x' \oplus \texttt{SynDec}(k_{\text{syn}} \oplus s')$. Compute $\hat{z} = \texttt{Ext}(u, \hat{x})$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept only if $\tau' = M(k_{\text{MAC}}, \hat{x}||c'||s')$ holds and the syndrome decoding was successful. Communicate Accept/Reject to Alice (publicly but with authentication).
Key update
Alice and Bob perform the following actions.

- In case of Reject, they take new keys $k_{\text{syn}}, k_{\text{MAC}}, b, u, v$.
- In case of Accept, they take new keys k_{syn} and k_{MAC}. Furthermore they replace the basis key b by $b' = \texttt{Mix}(v, b||r)$, where $r \in \mathcal{B}^q$ is key material.

The key update $b \mapsto b'$ consumes existing secret key material shared between Alice and Bob. See Section 5.3 for a discussion of the balance between message length and key expenditure.

5 Main result

5.1 Attacker model and proof method

The attacker model is the one used in most works on QKD. Eve is able to manipulate the classical channel and the quantum channel between Alice and Bob in any way. Eve has no access to the private computations taking place in Alice and Bob's devices. Eve has unbounded (quantum) computation power and unbounded quantum memory.
We work with the EPR version of the protocol. First we consider attacks where Eve entangles her quantum system with individual EPR pairs. Eve is allowed to postpone measurements. For this limited class of attacks we derive a bound (Theorem 1) on the trace distance between the real state and an ideal state, as explained in Section 2.2. Finally we invoke post-selection to extend the validity of the security proof to general attacks.

5.2 The theorems

Alice and Bob's shared key material consists of $k_{\text{syn}}, k_{\text{MAC}}, b, u, v$. The only keys open to attack are b, u, v, since k_{SS} and k_{MAC} get discarded after each round. Eve's classical side information consists of s (OTP'ed syndrome), τ (authentication tag), and the ciphertext $c = z \oplus \mu$. The s and τ carry no information about b, u, v. We assume that Eve knows the plaintext μ; this implies that she knows z.

Eve's quantum side information consists of her ancilla particles which have interacted with the EPR pairs. The state of the ancillas depends on x and b. Since $z = \texttt{Ext}(u, x)$ and we are interested only in the coupling between Eve's state and the keys b, u, v, we will keep track only of z, b, u, v. We introduce the binary variable Ω, with $\Omega = 1$ indicating that Alice receives a properly authenticated Accept message from Bob. The keys after execution of one QKR round are denoted with a tilde. We have $\tilde{u} = u, \tilde{v} = v$ in case $\omega = 1$, and a completely new random $\tilde{u}, \tilde{v}$ in case $\omega = 0$. Similarly we have $\tilde{b} = \texttt{Mix}(v, b||r)$ in case $\omega = 1$ and a new random $\tilde{b}$ in case $\omega = 0$. We work with quantum-classical states; each classical variable is assigned a quantum register, indicated as a capital-letter superscript on the state ρ. Eve's ancillas are denoted as the subsystem "E". We are interested in the security of the new keys $\tilde{b}, \tilde{u}, \tilde{v}$ given z, ω and Eve's ancillas. Hence the quantity of interest is $\|\rho^{\tilde{B}\tilde{U}\tilde{V}Z\Omega\mathrm{E}} - \mu^{\tilde{B}\tilde{U}\tilde{V}} \otimes \rho^{Z\Omega\mathrm{E}}\|_1$.

Theorem 1. *Consider one round of the QKR protocol (Section 4) with 8-state encoding. Let Eve cause noise described by parameter γ as discussed in Section 2.5. Let t be the number of errors that can be corrected by the error-correcting code. Let $P_{\mathrm{corr}}(t, \gamma)$ be the probability[5] that Bob's error correction succeeds. Let the function f be defined as*

$$f(\gamma) \stackrel{\mathrm{def}}{=} \sqrt{(1 - \tfrac{3}{2}\gamma)(1 - \gamma)} + \sqrt{\tfrac{3}{2}\gamma(1 + \gamma)}. \tag{5}$$

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

$$\frac{1}{2}\left\|\rho^{\tilde{B}\tilde{U}\tilde{V}Z\Omega\mathrm{E}} - \mu^{\tilde{B}\tilde{U}\tilde{V}} \otimes \rho^{Z\Omega\mathrm{E}}\right\|_1 \leq \frac{2}{2^{\lambda}} + \min\left\{P_{\mathrm{corr}}(t, \gamma),\ \frac{\sqrt{2^{\ell - n}}}{2} + \frac{1}{2\sqrt{|\mathcal{B}|^q}} + \frac{1}{2}\sqrt{\frac{2^{\ell - n + 2n\log f(\gamma)}}{|\mathcal{B}|^q}}\right\}. \tag{6}$$

The proof is given in Appendix A.
For large γ the probability $P_{\mathrm{corr}}(t, \gamma)$ is exponentially small. For small γ the other expression in the $\min\{\cdot, \cdot\}$ is exponentially small, if ℓ is set to be sufficiently smaller than $n - 2n \log f(t/n)$.

Theorem 2. *Consider the context of Theorem 1. Let $\beta = t/n$. Let σ be a security parameter. Let the scheme parameters be chosen as*

$$q \geq \sigma \tag{7}$$

$$\ell \leq n - 2n \log f(\beta) - 2\xi\sqrt{\sigma n} - 2\sigma - 1 \tag{8}$$

$$\xi \stackrel{\mathrm{def}}{=} \min\left\{\frac{f'(\beta)}{f(\beta)}\left[\sqrt{\frac{2\beta}{\ln 2} + \frac{\sigma}{n}} + \sqrt{\frac{\sigma}{n}}\right],\quad \frac{\sqrt{3}}{\ln 2}\right\}. \tag{9}$$

Then

$$\tfrac{1}{2}\|\rho^{\tilde{B}\tilde{U}\tilde{V}Z\Omega\mathrm{E}} - \mu^{\tilde{B}\tilde{U}\tilde{V}} \otimes \rho^{Z\Omega\mathrm{E}}\|_1 \leq 2 \cdot 2^{-\lambda} + 2^{-\sigma}. \tag{10}$$

[5] We have $P_{\mathrm{corr}}(t, \gamma) = \sum_{c=0}^{t} \binom{n}{c} \gamma^c (1 - \gamma)^{n-c}$.

Proof: See Appendix C.
A typical choice for the tag length is $\lambda = \sigma + 1$, resulting in $2/2^\sigma$ in (10). Several things are worth noting.

- Theorem 2 suffices to prove the security of the protocol. The keys BUV are protected, and the Quantum One Time Pad protects the x perfectly as long as B is uniform. (See Section 2.2.)
- The ξ is of order 1. Hence the term $\xi\sqrt{\sigma n}$ scales as $\sqrt{n}$.
- The function f is concave. We could have allowed Eve to apply position-dependent noise γ_i. Due to the concavity of f the optimal attack for Eve is to set all γ_i equal.
- Analysis of QKD instead of QKR using the same technique amounts to bounding the distance $\frac{1}{2}\|\rho^{ZBU\Omega E} - \mu^Z \otimes \rho^{BU\Omega E}\|_1$. Without providing details we note that this gives a result closely resembling Theorem 1: the second argument of the $\min\{\cdot,\cdot\}$ in (6) is replaced by $\frac{1}{2}\sqrt{2^{\ell - n + 2n\log f(\gamma)}}$. This suggests that QKR's noise tolerance is not much different from QKD's.

As explained in Section 2.3, by invoking post-selection we can 'buy' security against general attacks by reducing the message length ℓ a bit. The bound (6) changes by a factor $(n+1)^{15}$, which can be compensated by shrinking ℓ from (8) to

$$\ell = n - 2n\log f(\beta) - 2\xi\sqrt{\sigma n} - 2\sigma - 1 - 30\log(n+1). \tag{11}$$

5.3 QKR rate; Choosing the parameter values

We want to characterize the performance of 8-state QKR under ideal circumstances. Consider a sequence of QKR rounds with a large number of consecutive Accepts. Let $\varepsilon = 2 \cdot 2^{-\lambda} + 2^{-\sigma}$ be the 'imperfection' induced by one round of QKR. Let θ be the maximum distance that Alice and Bob are willing to tolerate between reality and the ideal state $\rho^{(0)}$. After $N = \lfloor \theta/\varepsilon \rfloor$ rounds they have to refresh *all* their key material. One can define a 'QKR rate' as

$$\text{rate} = \frac{\text{total message data sent in } N \text{ rounds} - \text{expended key material}}{N \cdot n}. \tag{12}$$

The total message size is $N\ell$, with ℓ specified in (11). The total key expenditure consists of N times two λ-bit authentication tags, N a-bit OTPs that protect the syndromes (asymptotically $a \approx nh(\beta)$), N times $2q$ bits of fresh key mixed into b, $2n$ bits of basis key b, n bits of extractor key u and $2n + 2q$ bits of extractor key v. This gives

$$\text{rate} = 1 - \frac{a}{n} - 2\log f(\beta) - \frac{2\xi\sqrt{\sigma}}{\sqrt{n}} - \frac{30\log(n+1)}{n} - \frac{2\lambda + 2\sigma}{n} - \frac{5}{N} - \frac{2\sigma}{Nn}. \tag{13}$$

Note that ε can be made exponentially small (N exponentially large) by increasing λ and σ. The asymptotic rate is

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

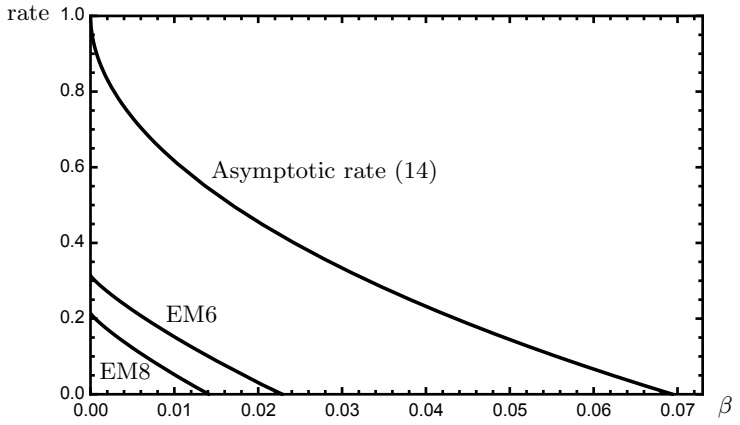

Fig. 1. *Asymptotic QKR rates. The upper curve is the bound (14) for 8-state encoding that follows from our proof technique,* $1 - h(\beta) - 2\log f(\beta)$*. The 'EM6' and 'EM8' curves correspond to the bound* $1 - \log(2\mu) - 2h(\beta)$ *based on Entanglement Monogamy, with constants* $\mu = \mu_6$ *and* $\mu = \mu_8$ *respectively (see Section 3).*

See Fig. 1. The asymptotic rate is positive up to $\beta \approx 0.069$. Up to this noise level it makes sense to use QKR. Fig. 1 also shows the bound derived using the entanglement monogamy game (see Section 3). Our bound is clearly tighter.

It is possible to reduce the key expenditure. "Scheme #3" in [2] greatly reduces the key material spent on protecting the syndrome, but it increases the number of qubits needed to convey the message. It does not modify the rate (13).
Instead of pairwise independent hashing one may use 'almost pairwise independent' hash functions. A small security penalty δ is incurred, but the length of the extractor key u is reduced from n to approximately $\min(n - \ell, \ell + 2\log\frac{1}{\delta})$.

Typically θ is fixed. Then it remains to tune N (which via $\varepsilon = \theta/N$ fixes σ) and n for fixed (θ, β) so as to optimise the rate. In Fig. 2 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.

5.4 Message bits per key bit

A figure of merit similar to the rate (12) is the number of message bits that are protected per expended key bit. In our scheme this ratio is given by

$$\frac{\text{message bits}}{\text{key bits}} = \frac{N\ell}{Na + N(4\sigma + 2) + 5n} = \frac{1 - 2\log f(\beta) - \mathcal{O}(\frac{1}{\sqrt{n}})}{h(\beta) + \mathcal{O}(\frac{\sqrt{\beta}}{\sqrt{n}} + \frac{5}{N} + \frac{1}{n})}, \qquad (15)$$

i.e. almost $N/5$ in the noiseless case (assuming $n \gg N$) and steeply decreasing as a function of β. This figure of merit can be improved in the same way as the rate: by switching to almost-pairwise independent hashes, thereby reducing the size of the extractor keys u, v (especially v).

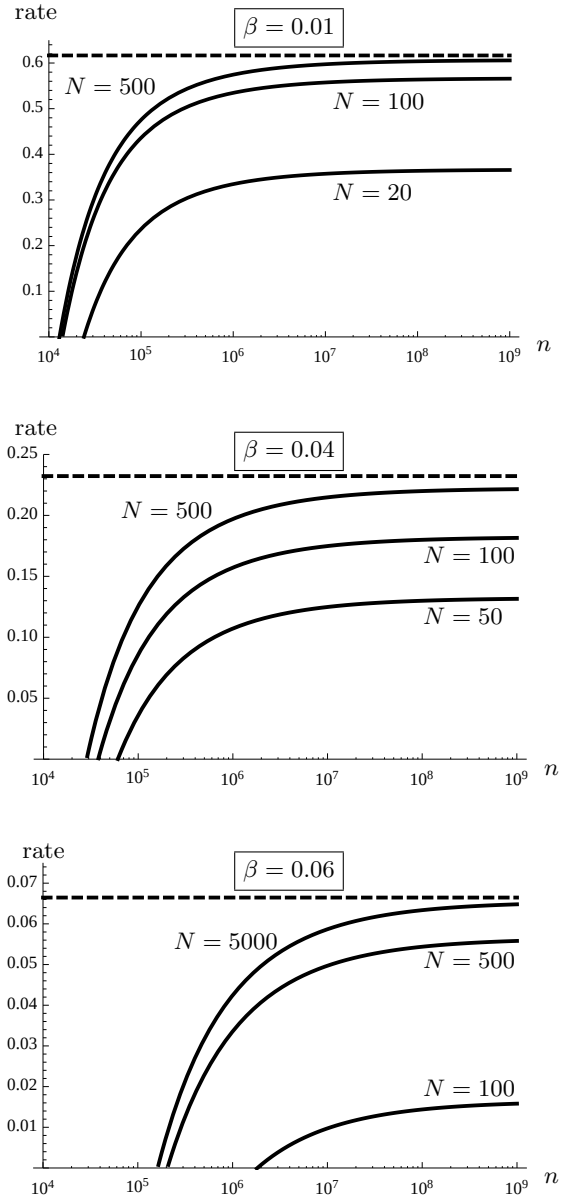

Fig. 2. *Non-asymptotic bound on the QKR rate as a function of the number of qubits (n), for various values of the design parameter N and tolerated noise β. The dashed lines indicate the asymptotic rate (14). $\lambda = \sigma + 1$; $\theta = 2^{-256}$; the syndrome length a is set to $nh(\beta) + \sqrt{n}\Phi^{\mathrm{inv}}(10^{-6})\sqrt{\beta(1-\beta)}\log\frac{1-\beta}{\beta}$ (see e.g. [19]), where Φ is defined as $\Phi(z) \stackrel{\mathrm{def}}{=} \int_z^\infty (2\pi)^{-1/2}\exp[-x^2/2]\mathrm{d}x$.*

Furthermore, it is possible to send several keys for the next round (k_{syn}, r and the two MAC protection OTPs) as part of the payload in the current round. This removes the Na and $N(4\sigma+2)$ terms from the denominator in (15) and subtracts them from the $N\ell$ in the numerator; this yields $\frac{\text{message bits}}{\text{key bits}} \to \frac{N\ell - Na - N(4\sigma+2)}{5n}$ which approximately equals $\frac{N}{5}$ times the rate (14).

6 Discussion

6.1 Comparison to existing results

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

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 the basis key and a trace distance for the extractor key.

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.

6.2 Dealing with erasures

Our analysis has not taken into account quantum channels with erasures. (Particles failing to arrive.) Consider a channel with erasure rate η and bit error rate β for the non-erased states. The Alice-to-Bob channel capacity is $(1-\eta)(1-h(\beta))$. A capacity-achieving linear error-correcting code that is able to deal with such a channel has a syndrome of size $nh(\beta) + n\eta[1-h(\beta)]$. Imagine the QKR scheme of Section 4 employing such an error-correcting code. On the one hand, the key expenditure increases from $nh(\beta)$ to $nh(\beta) + n\eta[1-h(\beta)]$. On the other hand, the leakage increases. Every qubit not arriving at Bob's side must be considered to be in Eve's possession; since an erasure can be parametrised as a qubit with $\beta = \frac{1}{2}$, the leakage is 1 bit per erased qubit. Hence the leakage term $n \cdot 2\log f(\beta)$ changes to $n(1-\eta)2\log f(\beta) + n\eta$. The combined effect of the syndrome size and the leakage increase has a serious effect on the QKR rate. The asymptotic rate becomes $1 - h(\beta) - \eta[1-h(\beta)] - (1-\eta)2\log f(\beta) - \eta$. For $\beta = 0$ this is $1-2\eta$; at zero bit error rate no more than 50% erasures can be accommodated by the scheme. In long fiber optic cables the erasure rate can be larger than 90%. Under such circumstances the QKR scheme of Section 4 simply does not work. (Note that continuous-variable schemes have much lower erasure rates.)

One can think of a number of straightforward ways to make the QKR protocol erasure-resistant. Below we sketch a protocol variant in which Alice sends qubits, and Bob returns an authenticated and encrypted message.

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

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

The above protocol looks a lot like QKD, but with reduced round complexity.

6.3 Future work

It is interesting to note that QKR protocols which first send a random string z and then use z for OTP encryption look a lot like Quantum Key Distribution, but with reduced communication complexity. This changes when the message is put directly into the qubits, e.g. as is done in Gottesman's Unclonable Encryption [6]. It remains a topic for future work to prove security of such a QKR scheme.
The QKR scheme of Section 4 can be improved and embellished in various ways. For instance, Alice's λ-bit key expenditure for one-time MACing may not be necessary. The authentication tag may simply be generated as part of the `Ext` function's output, and then the security of the MAC key can be proven just by proving the security of the extractor key u (similar to what is done in [1]).
Furthermore, as mentioned in Section 5.3, one may use 'scheme #3' of [2] which protects the syndrome by sending it through the quantum channel instead of classically OTP-ing it. This too reduces the key expenditure, and it does not affect the rate.
Another interesting option is to deploy the Quantum One Time Pad with approximately half the key length, which still yields information-theoretic security. This would slightly improve the rate (13) by reducing the amortised cost of refreshing b from $\frac{2}{N}$ to approximately $\frac{1}{N}$.
As mentioned in Section 5.2, the trace distance we have derived closely resembles the trace distance for QKD. It would be interesting to see if it is possible

to prove that the noise tolerance of QKR is the same as that of QKD, e.g. using state 'smoothening' as in Renner et al.'s work on smooth Rényi entropies. Furthermore, various tricks from QKD may apply to improve the noise tolerance of QKR, e.g. advantage distillation and artificial noise added by Alice.

Acknowledgements

We thank Serge Fehr and Niek Bouman for helpful discussions. We thank the anonymous reviewers of Asiacrypt for pointing out a flaw in a previous version. Part of this research was funded by NWO (CHIST-ERA project ID_IOT).

A Proof of Theorem 1

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

A.1 Rewriting the state

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

$$\theta_{xy} \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } \mathrm{Hamm}(x \oplus \bar{y}) \leq t \\ 0 & \text{otherwise} \end{cases}. \tag{16}$$

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

$$P_{\mathrm{corr}}(t,\gamma) = \sum_{xy} p_{xy}\theta_{xy} = \sum_{c=0}^{t} \binom{n}{c} \gamma^c (1-\gamma)^{n-c}. \tag{17}$$

Alice will re-use keys ($\Omega = 1$) if she receives an authenticated Accept bit from Bob. The probability of this event can be bounded as

$$P_{\mathrm{acc}}(t,\gamma) \leq P_{\mathrm{corr}}(t,\gamma) + 2 \cdot 2^{-\lambda}. \tag{18}$$

Here λ is the size of the authentication tag. One term $2^{-\lambda}$ comes from the possibility that Eve forges Alice's MAC. Another term $2^{-\lambda}$ comes from the possibility that Eve forges Bob's MAC on a Reject message and turns it into an Accept message.

We introduce notation $\mathbb{E}_b \stackrel{\text{def}}{=} \sum_{b\in\mathcal{B}^n} \frac{1}{|\mathcal{B}|^n}$, $\mathbb{E}_u \stackrel{\text{def}}{=} \sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|}$, $\mathbb{E}_v \stackrel{\text{def}}{=} \sum_{v\in\mathcal{V}} \frac{1}{|\mathcal{V}|}$, and in slight abuse of notation we define $\mathbb{E}_{\tilde{b}}, \mathbb{E}_{\tilde{u}}, \mathbb{E}_{\tilde{v}}$ in the same way. Furthermore we

introduce $\mathbb{E}_r \stackrel{\text{def}}{=} \sum_{r\in\mathcal{B}^q} \frac{1}{|\mathcal{B}|^q}$, $\mathbb{E}_{xy} \stackrel{\text{def}}{=} \sum_{x,y\in\{0,1\}^n} p_{xy}$. The full quantum-classical state of all the classical variables and Eve's system together is given by

$$\begin{aligned}
\rho^{B\tilde{B}U\tilde{U}V\tilde{V}RXYZ\Omega E} = & \\
& \mathbb{E}_b \sum_{\tilde{b}\in\mathcal{B}^n} \mathbb{E}_u \sum_{\tilde{u}\in\mathcal{U}} \mathbb{E}_v \sum_{\tilde{v}\in\mathcal{V}} \mathbb{E}_r \mathbb{E}_{xy} \sum_{z\in\{0,1\}^\ell} \sum_{\omega\in\{0,1\}} \\
& \delta_{z,\mathtt{Ext}(u,x)} \left[\delta_{\omega 1}(\theta_{xy} + \overline{\theta_{xy}} 2^{1-\lambda}) \delta_{\tilde{u}u} \delta_{\tilde{v}v} \delta_{\tilde{b},\mathtt{Mix}(v,b||r)} + \frac{\delta_{\omega 0}\overline{\theta_{xy}}(1-2^{1-\lambda})}{|\mathcal{B}|^n |\mathcal{U}||\mathcal{V}|} \right] \\
& |b\tilde{b}u\tilde{u}v\tilde{v}rxyz\omega\rangle\langle b\tilde{b}u\tilde{u}v\tilde{v}rxyz\omega| \otimes \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i}. \qquad (19)
\end{aligned}$$

We take the trace over the $BUVRXY$ subsystems to focus on the variables relevant to our analysis,

$$\begin{aligned}
\rho^{\tilde{B}\tilde{U}\tilde{V}Z\Omega E} = \mathbb{E}_{\tilde{b}} \mathbb{E}_{\tilde{u}} \mathbb{E}_{\tilde{v}} & \sum_{z\in\{0,1\}^\ell} \sum_{\omega\in\{0,1\}} |\tilde{b}\tilde{u}\tilde{v}z\omega\rangle\langle\tilde{b}\tilde{u}\tilde{v}z\omega| \otimes \\
& \Big[\delta_{\omega 1} \mathbb{E}_{xy} (\theta_{xy} + \overline{\theta_{xy}} 2^{1-\lambda}) \delta_{z,\mathtt{Ext}(\tilde{u},x)} \mathbb{E}_r \sum_b \delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b||r)} \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i} \\
& + \delta_{\omega 0} \mathbb{E}_{xy} \overline{\theta_{xy}} (1-2^{1-\lambda}) 2^{-\ell} \mathbb{E}_b \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i} \Big]. \qquad (20)
\end{aligned}$$

Here we have used the property $\mathbb{E}_u \delta_{z,\mathtt{Ext}(u,x)} = 2^{-\ell}$ of pairwise independent hash functions. The marginal of the part known to Eve is

$$\begin{aligned}
\rho^{Z\Omega E} = & \sum_{z\in\{0,1\}^\ell} 2^{-\ell} \sum_{\omega\in\{0,1\}} |z\omega\rangle\langle z\omega| \otimes \\
& \mathbb{E}_{xy} \Big[\delta_{\omega 1}(\theta_{xy} + \overline{\theta_{xy}} 2^{1-\lambda}) + \delta_{\omega 0} \overline{\theta_{xy}} (1-2^{1-\lambda}) \Big] \mathbb{E}_b \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i}. \qquad (21)
\end{aligned}$$

The difference between the true state and the decoupled state is

$$\begin{aligned}
\rho^{\tilde{B}\tilde{U}\tilde{V}Z\Omega E} - \mu^{\tilde{B}\tilde{U}\tilde{V}} \otimes \rho^{Z\Omega E} = & \\
& \mathbb{E}_{\tilde{b}\tilde{u}\tilde{v}} \sum_{z\in\{0,1\}^\ell} \sum_{\omega\in\{0,1\}} \delta_{\omega 1} |\tilde{b}\tilde{u}\tilde{v}z\omega\rangle\langle\tilde{b}\tilde{u}\tilde{v}z\omega| \otimes \sum_{xy} p_{xy} (\theta_{xy} + \overline{\theta_{xy}} 2^{1-\lambda}) \\
& \Big[\delta_{z,\mathtt{Ext}(\tilde{u},x)} \mathbb{E}_r \sum_b \delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b||r)} \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i} - 2^{-\ell} \mathbb{E}_b \bigotimes_{i=1}^n \sigma^{b_i}_{x_i y_i} \Big]. \qquad (22)
\end{aligned}$$

The quantity of interest is

$$D \stackrel{\text{def}}{=} \frac{1}{2} \left\| \rho^{\tilde{B}\tilde{U}\tilde{V}Z\Omega E} - \mu^{\tilde{B}\tilde{U}\tilde{V}} \otimes \rho^{Z\Omega E} \right\|_1. \qquad (23)$$

Due to the block structure of the classical part we can write

$$
\begin{aligned}
D &= \tfrac{1}{2}\mathbb{E}_{\tilde{b}\tilde{u}\tilde{v}} \sum_{z\in\{0,1\}^\ell} 2^{-\ell} \left\|(\varphi - \mathbb{E}_{\tilde{u}\tilde{v}}\varphi) + 2^{1-\lambda}(\chi - \mathbb{E}_{\tilde{u}\tilde{v}}\chi)\right\|_1 \\
\varphi &\stackrel{\text{def}}{=} \sum_{xy} p_{xy}\theta_{xy} 2^\ell \delta_{z,\mathtt{Ext}(\tilde{u},x)} \mathbb{E}_r \sum_b \delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b||r)} \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i} \\
\chi &\stackrel{\text{def}}{=} \sum_{xy} p_{xy}\overline{\theta_{xy}} 2^\ell \delta_{z,\mathtt{Ext}(\tilde{u},x)} \mathbb{E}_r \sum_b \delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b||r)} \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i}.
\end{aligned} \tag{24}
$$

Using the norm inequality $\|A+B\|_1 \le \|A\|_1 + \|B\|_1$ we get $D \le 2^{1-\lambda} + D_{\text{corr}}$,

$$
D_{\text{corr}} \stackrel{\text{def}}{=} \tfrac{1}{2}\mathbb{E}_{\tilde{b}\tilde{u}\tilde{v}} \sum_{z\in\{0,1\}^\ell} 2^{-\ell} \left\|\varphi - \mathbb{E}_{\tilde{u}\tilde{v}}\varphi\right\|_1. \tag{25}
$$

The φ is a sub-normalised mixed state, with $\operatorname{tr}\varphi = P_{\text{corr}}$.

A.2 Bound for large γ

Note that the expression $\varphi - \mathbb{E}_{\tilde{u}\tilde{v}}\varphi$ in (25) has the form $P_{\text{corr}}(t,\gamma)\cdot(\rho_1 - \rho_2)$, where ρ_1, ρ_2 are normalised. Hence we immediately have an upper bound $D_{\text{corr}} \le P_{\text{corr}}$.

A.3 Bound for small γ

The form $\varphi - \mathbb{E}_{\tilde{u}\tilde{v}}\varphi$ in (25) allows us to write $\mathbb{E}_{\tilde{u}\tilde{v}}(\varphi - \mathbb{E}_{\tilde{u}\tilde{v}}\varphi)^2 = \mathbb{E}_{\tilde{u}\tilde{v}}\varphi^2 - (\mathbb{E}_{\tilde{u}\tilde{v}}\varphi)^2$. We then have

$$
\mathbb{E}_{\tilde{u}\tilde{v}}\|\varphi - \mathbb{E}_{\tilde{u}\tilde{v}}\varphi\|_1 \le \operatorname{tr}\sqrt{\mathbb{E}_{\tilde{u}\tilde{v}}\varphi^2 - (\mathbb{E}_{\tilde{u}\tilde{v}}\varphi)^2}. \tag{26}
$$

Here we used Jensen's inequality for concave operators. Next we write

$$
\begin{aligned}
\mathbb{E}_{\tilde{u}\tilde{v}}\varphi^2 = \sum_{xx'yy'} & p_{xy}p_{x'y'}\theta_{xy}\theta_{x'y'}[2^{2\ell}\mathbb{E}_{\tilde{u}}\delta_{z,\mathtt{Ext}(\tilde{u},x)}\delta_{z,\mathtt{Ext}(\tilde{u},x')}] \\
& \mathbb{E}_{rr'}\sum_{bb'}[\mathbb{E}_{\tilde{v}}\delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b||r)}\delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b'||r')}] \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i}\sigma_{x_i' y_i'}^{b_i'}.
\end{aligned} \tag{27}
$$

Next we use $2^{2\ell}\mathbb{E}_{\tilde{u}}\delta_{z,\mathtt{Ext}(\tilde{u},x)}\delta_{z,\mathtt{Ext}(\tilde{u},x')} = \delta_{xx'}2^{-\ell} + (1-\delta_{xx'})\cdot 1 = 1 + \delta_{xx'}(2^\ell - 1)$ and

$$
\mathbb{E}_{\tilde{v}}\delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b||r)}\delta_{\tilde{b},\mathtt{Mix}(\tilde{v},b'||r')} = \frac{\delta_{bb'}\delta_{rr'}}{|\mathcal{B}|^n} + \frac{1-\delta_{bb'}\delta_{rr'}}{|\mathcal{B}|^{2n}} = \frac{1}{|\mathcal{B}|^{2n}} + \frac{\delta_{bb'}\delta_{rr'}}{|\mathcal{B}|^n}(1 - \frac{1}{|\mathcal{B}|^n}), \tag{28}
$$

which hold due to the pairwise independence of `Ext` and `Mix`. Substitution into (27) yields

$$
\mathbb{E}_{\tilde{u}\tilde{v}}\varphi^2 - (\mathbb{E}_{\tilde{u}\tilde{v}}\varphi)^2 = W_1 + W_2 + W_3, \tag{29}
$$

where we have defined

$$W_1 \stackrel{\text{def}}{=} (2^\ell - 1) \sum_{xyy'} p_{xy} p_{xy'} \theta_{xy} \theta_{xy'} \mathbb{E}_{bb'} \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i} \sigma_{x_i y_i'}^{b_i'}$$

$$= \frac{2^\ell - 1}{2^n} \mathbb{E}_x \left(\sum_y p_{y|x} \theta_{xy} \mathbb{E}_b \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i} \right)^2 \tag{30}$$

$$W_2 \stackrel{\text{def}}{=} (1 - \frac{1}{|\mathcal{B}|^n}) \frac{1}{|\mathcal{B}|^q} \sum_{xx'yy'} p_{xy} p_{x'y'} \theta_{xy} \theta_{x'y'} \mathbb{E}_b \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i} \sigma_{x_i' y_i'}^{b_i} \tag{31}$$

$$W_3 \stackrel{\text{def}}{=} (1 - \frac{1}{|\mathcal{B}|^n}) \frac{2^\ell - 1}{|\mathcal{B}|^q} \sum_{xyy'} p_{xy} p_{xy'} \theta_{xy} \theta_{xy'} \mathbb{E}_b \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i} \sigma_{x_i y_i'}^{b_i}$$

$$= (1 - \frac{1}{|\mathcal{B}|^n}) \frac{2^\ell - 1}{|\mathcal{B}|^q} \sum_{xy} p_{xy}^2 \theta_{xy} \mathbb{E}_b \bigotimes_{i=1}^n \sigma_{x_i y_i}^{b_i}. \tag{32}$$

For the trace distance we now have

$$D_{\text{corr}} \leq \tfrac{1}{2} \text{tr} \sqrt{W_1 + W_2 + W_3} \leq \tfrac{1}{2} \text{tr} \sqrt{W_1} + \tfrac{1}{2} \text{tr} \sqrt{W_2} + \tfrac{1}{2} \text{tr} \sqrt{W_3}. \tag{33}$$

We write $y = \bar{x} \oplus \Delta$ and $y' = \overline{x'} \oplus \Delta'$ and enforce the $\theta_{xy}, \theta_{x'y'}$ constraints by taking $|\Delta| \leq t$ and $|\Delta'| \leq t$. We introduce the notation $p_\Delta = \gamma^{|\Delta|}(1-\gamma)^{n-|\Delta|}$. We note that the product of σ-states has a special property,

$$\begin{aligned}
\sigma_{x_i, \overline{x_i} \oplus \Delta_i}^{b_i} \sigma_{x_i', \overline{x_i'} \oplus \Delta_i'}^{b_i} &= \delta_{\Delta_i \Delta_i'} \sigma_{x_i, \overline{x_i} \oplus \Delta_i}^{b_i} \sigma_{x_i', \overline{x_i'} \oplus \Delta_i}^{b_i} \\
&= \delta_{\Delta_i \Delta_i'} \left[\delta_{\Delta_i 0} (\delta_{x_i x_i'} \sigma_{x_i \overline{x_i}}^{b_i} + \delta_{\overline{x_i} x_i'} \sigma_{x_i \overline{x_i}}^{b_i} \sigma_{\overline{x_i} x_i}^{b_i}) + \delta_{\Delta_i 1} \delta_{x_i x_i'} \sigma_{x_i x_i}^{b_i} \right] \\
&= \delta_{\Delta_i \Delta_i'} \left[\delta_{x_i x_i'} \sigma_{x_i, \overline{x_i} \oplus \Delta_i}^{b_i} + \delta_{\overline{x_i} x_i'} \delta_{\Delta_i 0} \sigma_{x_i \overline{x_i}}^{b_i} \sigma_{\overline{x_i} x_i}^{b_i} \right].
\end{aligned} \tag{34}$$

Hence the string Δ' has to equal Δ, which allows us to simplify the operators W_1, W_2, W_3 to

$$W_1 = \frac{2^\ell - 1}{2^n} \mathbb{E}_x \left(\sum_{\Delta : |\Delta| \leq t} p_\Delta \mathbb{E}_b \bigotimes_{i=1}^n \sigma_{x_i, \overline{x_i} \oplus \Delta_i}^{b_i} \right)^2 \tag{35}$$

$$W_2 = (1 - \frac{1}{|\mathcal{B}|^n}) \frac{1}{|\mathcal{B}|^q} \sum_{\Delta : |\Delta| \leq t} p_\Delta^2 \bigotimes_{i=1}^n \tfrac{1}{4} \sum_{x_i x_i'} \mathbb{E}_{b_i} \sigma_{x_i, \overline{x_i} \oplus \Delta_i}^{b_i} \sigma_{x_i', \overline{x_i'} \oplus \Delta_i}^{b_i} \tag{36}$$

$$W_3 = (1 - \frac{1}{|\mathcal{B}|^n}) \frac{2^\ell - 1}{|\mathcal{B}|^q} \sum_x \frac{1}{2^{2n}} \sum_{\Delta : |\Delta| \leq t} p_\Delta^2 \bigotimes_{i=1}^n \mathbb{E}_{b_i} \sigma_{x_i, \overline{x_i} \oplus \Delta_i}^{b_i}. \tag{37}$$

Next we need to evaluate the expectation over b.

Lemma 1. *Let $x, x', \Delta \in \{0,1\}$ and $b \in \mathcal{B}$. For 8-state encoding it holds that*

$$\mathbb{E}_b \sigma^b_{x,\bar{x}\oplus\Delta} = |m_0\rangle\langle m_0|\delta_{\Delta 0}\frac{1-\frac{3}{2}\gamma}{1-\gamma} + \frac{\sum_{j=1}^3 |m_j\rangle\langle m_j|}{3}\left\{\delta_{\Delta 1} + \delta_{\Delta 0}\frac{\gamma/2}{1-\gamma}\right\} \quad (38)$$

$$\frac{1}{4}\sum_{xx'} \mathbb{E}_b \sigma^b_{x,\bar{x}\oplus\Delta}\sigma^b_{x',\overline{x'}\oplus\Delta} = |m_0\rangle\langle m_0|\delta_{\Delta 0}(\frac{1-\frac{3}{2}\gamma}{1-\gamma})^2 + \frac{\sum_{j=1}^3 |m_j\rangle\langle m_j|}{6}\left\{\delta_{\Delta 1} + \delta_{\Delta 0}\frac{1}{2}(\frac{\gamma}{1-\gamma})^2\right\}. \quad (39)$$

Proof: See Appendix B. □

The W_1 term

The $\mathbb{E}_b$ operation in (35) yields an expression that does not depend on x. Hence the $\mathbb{E}_x$ does nothing and W_1 is a square. We get

$$\mathrm{tr}\sqrt{W_1} = \sqrt{\frac{2^\ell - 1}{2^n}}P_{\mathrm{corr}} \le \sqrt{\frac{2^\ell - 1}{2^n}}. \quad (40)$$

The W_2 term

The eigenvectors of W_2 and W_3 are all of the same form: in k qubit systems a vector in the $|\boldsymbol{m}\rangle$-space, and in $n-k$ qubit systems the vector $|m_0\rangle$. We denote the corresponding eigenvalues as $\lambda_2(k)$ and $\lambda_3(k)$. Without loss of generality we place the $\boldsymbol{m}$-components of the eigenvectors in positions $i = 1 \ldots k$. Substitution of (39) into (36) gives

$$\begin{aligned}
\lambda_2(k) &= (1-\frac{1}{|\mathcal{B}|^n})\frac{1}{|\mathcal{B}|^q}\sum_{\substack{\Delta\in\{0,1\}^k \\ |\Delta|\le t}} p_\Delta^2(\frac{1-\frac{3}{2}\gamma}{1-\gamma})^{2n-2k}(\frac{1}{6})^k\prod_{i=1}^k\left\{\delta_{\Delta_i 1} + \delta_{\Delta_i 0}\frac{\gamma^2}{2(1-\gamma)^2}\right\} \\
&= (1-\frac{1}{|\mathcal{B}|^n})\frac{1}{|\mathcal{B}|^q}\sum_{c=0}^t\sum_{\substack{\Delta\in\{0,1\}^k \\ |\Delta|=c}}\gamma^{2c}(1-\gamma)^{2n-2c}(\frac{1-\frac{3}{2}\gamma}{1-\gamma})^{2n-2k}(\frac{1}{6})^k[\frac{\gamma^2}{2(1-\gamma)^2}]^{k-c} \\
&= (1-\frac{1}{|\mathcal{B}|^n})\frac{1}{|\mathcal{B}|^q}(\frac{\gamma^2}{12})^k(1-\tfrac{3}{2}\gamma)^{2n-2k}\sum_{c=0}^t\binom{k}{c}2^c \\
&\le (1-\frac{1}{|\mathcal{B}|^n})\frac{1}{|\mathcal{B}|^q}(\frac{\gamma^2}{12})^k(1-\tfrac{3}{2}\gamma)^{2n-2k}\cdot 3^k \\
&\le \frac{1}{|\mathcal{B}|^q}(\frac{\gamma}{2})^{2k}(1-\tfrac{3}{2}\gamma)^{2n-2k}. \quad (41)
\end{aligned}$$

In the first inequality we used that the sum over $c \le t$ is upper bounded by the full sum $c \le k$ and then we applied the binomial sum rule. We get

$$\mathrm{tr}\sqrt{W_2} = \sum_{k=0}^n\binom{n}{k}3^k\sqrt{\lambda_2(k)} \le \frac{1}{|\mathcal{B}|^{q/2}}\sum_{k=0}^n\binom{n}{k}(\tfrac{3}{2}\gamma)^k(1-\tfrac{3}{2}\gamma)^{n-k} = \frac{1}{|\mathcal{B}|^{q/2}}. \quad (42)$$

The W_3 term

$$\begin{aligned}
\lambda_3(k) &= (1-\frac{1}{|\mathcal{B}|^n})\frac{2^\ell-1}{|\mathcal{B}|^q}\frac{1}{2^n}\sum_{c=0}^{t}\sum_{\substack{\Delta\in\{0,1\}^k\\|\Delta|=c}} p_\Delta^2(\frac{1-\frac{3}{2}\gamma}{1-\gamma})^{n-k}(\frac{1}{3})^k(\frac{\gamma/2}{1-\gamma})^{k-c}\\
&\le \frac{2^{\ell-n}}{|\mathcal{B}|^q}(\frac{\gamma}{6})^k(1-\tfrac{3}{2}\gamma)^{n-k}(1-\gamma)^n\sum_{c=0}^{t}\binom{k}{c}(\frac{2\gamma}{1-\gamma})^c\\
&\le \frac{2^{\ell-n}}{|\mathcal{B}|^q}(\frac{\gamma}{6})^k(1-\tfrac{3}{2}\gamma)^{n-k}(1-\gamma)^n\cdot(\frac{1+\gamma}{1-\gamma})^k\\
&= \frac{2^{\ell-n}}{|\mathcal{B}|^q}[\frac{\gamma(1+\gamma)}{6}]^k\big[(1-\tfrac{3}{2}\gamma)(1-\gamma)\big]^{n-k}. \qquad (43)
\end{aligned}$$

In the second inequality we used that the sum over $c \le t$ is upper bounded by the full sum $c \le k$ and then we applied the binomial sum rule. We get

$$\begin{aligned}
\operatorname{tr}\sqrt{W_3} &= \sum_{k=0}^{n}\binom{n}{k}3^k\sqrt{\lambda_3(k)}\\
&\le \sqrt{\frac{2^{\ell-n}}{|\mathcal{B}|^q}}\left[\sqrt{(1-\tfrac{3}{2}\gamma)(1-\gamma)}+\sqrt{\tfrac{3}{2}\gamma(1+\gamma)}\right]^n. \qquad (44)
\end{aligned}$$

This completes the proof of Theorem 1. □

B Proof of Lemma 1

For brevity of notation we introduce $M \stackrel{\text{def}}{=} \sum_{j=1}^{3}|m_j\rangle\langle m_j|$ and write $|\boldsymbol{v}\cdot\boldsymbol{m}\rangle$ for $v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle$. From (4) we get

$$\begin{aligned}
\sigma_{01}^b &= \frac{1-\frac{3}{2}\gamma}{1-\gamma}|m_0\rangle\langle m_0| + \frac{\gamma/2}{1-\gamma}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}|\\
&\quad + \frac{\sqrt{\frac{1}{2}\gamma(1-\frac{3}{2}\gamma)}}{1-\gamma}\Big(|m_0\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}| + |\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle m_0|\Big). \qquad (45)
\end{aligned}$$

Averaging over the basis b means averaging over de basis vector $\boldsymbol{v}$, i.e. over the four values $\frac{1}{\sqrt{3}}(1,1,1)$, $\frac{1}{\sqrt{3}}(-1,-1,1)$, $\frac{1}{\sqrt{3}}(-1,1,-1)$, $\frac{1}{\sqrt{3}}(1,-1,-1)$. The cross term $|m_0\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}|$ disappears. Furthermore, terms of the form $v_iv_j|m_i\rangle\langle m_j|$ for $j \ne i$ also disappear. The average of v_j^2 is $\frac{1}{3}$ for all j. This yields $\mathbb{E}_b\sigma_{01}^b = \frac{1-\frac{3}{2}\gamma}{1-\gamma}|m_0\rangle\langle m_0| + \frac{1}{3}M\frac{\gamma/2}{1-\gamma}$, which exactly matches the $\Delta = 0$ part of (38). The analysis for σ_{10}^b is analogous, with $\boldsymbol{v} \to -\boldsymbol{v}$. For σ_{00}^b we get

$$\sigma_{00}^b = \tfrac{1}{2}M - \tfrac{1}{2}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}| + i\sum_{jkp=1}^{3}\varepsilon_{jkp}v_j|m_k\rangle\langle m_p| \qquad (46)$$

where ε_{jkp} stands for the antisymmetric Levi-Civita symbol. When we average over $\boldsymbol{v}$ the ε_{jkp} term disappears and the crossterms of the form $v_i v_j |m_i\rangle\langle m_j|$ for $j \neq i$ disappear. What is left is $\mathbb{E}_b \sigma^b_{00} = \frac{1}{2}M - \frac{1}{2}\cdot\frac{1}{3}M = \frac{1}{3}M$, which exactly matches the $\Delta = 1$ part of (38). The analysis for σ^b_{11} is analogous, with $\boldsymbol{v} \to -\boldsymbol{v}$. Next we look at the product of two σ-states (39). In the case $\Delta = 1$ we get

$$\begin{aligned}\tfrac{1}{4}\sum_{xx'} \sigma^b_{xx}\sigma^b_{x'x'} &= \tfrac{1}{4}(\sigma^b_{00}+\sigma^b_{11})^2 = \tfrac{1}{4}(M - |\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}|)^2 \\ &= \tfrac{1}{4}(M - |\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}|). \end{aligned} \tag{47}$$

Averaging over $\boldsymbol{v}$ yields $\frac{1}{4}(M - \frac{1}{3}M) = \frac{1}{6}M$. For $\Delta = 0$ we have

$$\begin{aligned}\tfrac{1}{4}\sum_{xx'} \sigma^b_{x\bar{x}}\sigma^b_{x'\overline{x'}} &= \tfrac{1}{4}(\sigma^b_{01}+\sigma^b_{10})^2 \\ &= \left(\frac{1-\frac{3}{2}\gamma}{1-\gamma}|m_0\rangle\langle m_0| + \frac{\gamma/2}{1-\gamma}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}|\right)^2 \\ &= (\frac{1-\frac{3}{2}\gamma}{1-\gamma})^2|m_0\rangle\langle m_0| + (\frac{\gamma/2}{1-\gamma})^2|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\langle\boldsymbol{v}\cdot\boldsymbol{m}|. \end{aligned} \tag{48}$$

Averaging over $\boldsymbol{v}$ yields $(\frac{1-\frac{3}{2}\gamma}{1-\gamma})^2|m_0\rangle\langle m_0| + (\frac{\gamma/2}{1-\gamma})^2\frac{1}{3}M$.

C Proof of Theorem 2

We (implicitly) define a function $\gamma_{\max}(t,\sigma)$ as $P_{\mathrm{corr}}(t,\gamma_{\max}) = 2^{-\sigma}$. For $\gamma \geq \gamma_{\max}$ eq. (10) 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

$$\gamma_{\max}(t,\sigma) \leq \gamma_0(t,\sigma) \stackrel{\mathrm{def}}{=} \frac{t}{n} + \frac{\sigma\ln 2}{n} + \sqrt{2\frac{t}{n}\frac{\sigma\ln 2}{n} + (\frac{\sigma\ln 2}{n})^2}. \tag{49}$$

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

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

$$\begin{aligned}\log f(\gamma_0) &\leq \log f(\beta) + \log[1 + \frac{f'(\beta)}{f(\beta)}(\gamma_0 - \beta)] \leq \log f(\beta) + \frac{f'(\beta)}{f(\beta)}\frac{\gamma_0 - \beta}{\ln 2} \\ &= \log f(\beta) + \frac{\sigma}{n} + \sqrt{2\beta\frac{\sigma}{n\ln 2} + (\frac{\sigma}{n})^2}. \end{aligned} \tag{50}$$

- 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

$$\begin{aligned}\log f(\gamma_0) &\leq \log f(\beta) + \log f(\frac{2\sigma}{n}) \leq \log f(\beta) + \log[1 + \sqrt{\tfrac{3}{2}(\tfrac{2\sigma}{n})}] \\ &\leq \log f(\beta) + \tfrac{1}{\ln 2}\sqrt{\tfrac{3\sigma}{n}}. \end{aligned} \tag{51}$$

From (50) and (51) we conclude $n \log f(\gamma_{\max}(t,\sigma)) \leq n \log f(\beta) + \xi\sqrt{\sigma n}$ with ξ as defined in (9). With ℓ chosen according to (8), the expression $\sqrt{2^{\ell - n + 2n \log f(\gamma_{\max})}}$ in (6) is upper bounded by $2^{-\sigma}/\sqrt{2}$. We also bound $\sqrt{2^{n-\ell}} \leq 2^{-\sigma}/\sqrt{2}$. Furthermore, setting $q = \sigma$ yields $1/\sqrt{|\mathcal{B}|^q} = 2^{-\sigma}$. Hence the second expression in the $\min\{\cdot,\cdot\}$ (6) is upper bounded by $\frac{2^{-\sigma}}{2\sqrt{2}} + \frac{2^{-\sigma}}{2} + \frac{2^{-2\sigma}}{2\sqrt{2}} < 2^{-\sigma}$. □

References

1. S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Eurocrypt*, pages 311–338, 2017.
2. B. Škorić and M. de Vries. Quantum Key Recycling with eight-state encoding. (The Quantum One Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 2017.
3. C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.
4. W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.
5. C.H. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13:453–458, 2014. Original manuscript 1982.
6. D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581–602, 2003.
7. I.B. Damgård, T.B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *CRYPTO*, pages 494–510, 2005.
8. I.B. Damgård, T.B. Pedersen, and L. Salvail. How to re-use a one-time pad safely and almost optimally even if P = NP. *Natural Computing*, 13(4):469–486, 2014.
9. D. Leermakers and B. Škorić. Optimal attacks on qubit-based Quantum Key Recycling. *Quantum Information Processing*, 2018.
10. R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.
11. M.N. Wegman and J.W. Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22:265–279, 1981.
12. M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.
13. D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.
14. A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.
15. D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.
16. P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.
17. R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.

18. 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.
19. D. Baron, M.A. Khojastepour, and R.G. Baraniuk. How quickly can we approach channel capacity? In *Asilomar Conference on Signals, Systems and Computers*, pages 1096–1100. IEEE, 2004.