Quantum Alice and Silent Bob

Qubit-based Quantum Key Recycling with almost no classical communication

Daan Leermakers and Boris Škorić

Abstract

We introduce a Quantum Key Recycling (QKR) protocol that needs no classical communication from Alice to Bob. Alice sends only a cipherstate, which consists of qubits that are individually measured by Bob. Bob merely has to respond with an authenticated one-bit accept/reject classical message.[1]

Compared to Quantum Key Distribution (QKD), QKR has reduced round complexity. Compared to other qubit-wise QKR protocols, our scheme has far less classical communication.

We provide a security proof proof similar to [1] and find that the communication rate is asymptotically the same as for QKD with one-way postprocessing.

1 Introduction

1.1 Quantum Key Recycling

QKR achieves information-theoretically secure communication in such a way that no existing key material is used up as long as the quantum channel is undisturbed. The main advantage of QKR over QKD is reduced round complexity: QKR needs only one message from Alice to Bob, and one from Bob to Alice. A prepare-and-measure QKR scheme based on qubits was proposed already in 1982 [2]. However, QKR received little attention for a long time. A security proof[2] for qubit-based[3] QKR was given only in 2017 by Fehr and Salvail [5]. In [1] it was shown (for a scheme similar to [5]) that the communication rate in case of a noisy quantum channel is asymptotically the same as for QKD with one-way postprocessing.

1.2 Putting the message in the quantum states

All currently existing qubit-wise QKR schemes encode random bits into the quantum state, and then extract a classical One-Time Pad (OTP) from these random bits. Alice sends a classical ciphertext (the message xor'ed with the OTP) along with the quantum states.

In 2003 Gottesman [6] proposed a scheme called 'Unclonable Encryption' which encodes a message directly into qubit states. However, it allows only for partial re-use of keys. The high-dimensional QKR of Damgård, Pedersen and Salvail [3, 4] has full recycling of keys, but requires quantum computation for encryption and decryption.

1.3 Contributions

We construct a qubit-based Quantum Key Recycling protocol that reduces the need for classical communication to a minimum.

- Our protocol is a modification of [1]. All classical communication from Alice to Bob is stripped away by encoding it directly into the qubits. The only remaining classical communication is a single authenticated `Accept/Reject` feedback bit from Bob to Alice indicating whether the message was correctly received.

[1]The title refers to the movie character Silent Bob, who hardly ever speaks.

[2]For a scheme slightly different from [2].

[3]as opposed to schemes that work with higher-dimensional spaces, e.g. using mutually unbiased bases [3, 4].

- In case of `Reject`, Alice and Bob have to tap into fresh key material. We implement this key update by hashing fresh key material into the old keys. This reduces the `Reject`-case key expenditure with respect to [5] and [1]. In the absemce of noise the `Reject`-case key expenditure asymptotically equals the length of the message, which is optimal [3].
- We prove the security of our protocol against general attacks. We use a universally composable measure of security, namely the diamond norm between the actual protocol and an idealized protocol in which the secrets are replaced by random strings after protocol execution. The proof follows the same steps as [1], and at an early stage the `Accept`-case part of the proof reduces exactly to the derivation in [1].
- We find the same asymptotic communication rate as [1], i.e. the rate of QKD with one-way postprocessing. The finite-size effects are the same as [1], but with an additional small term due to the new key refresh procedure in the `Reject` case.

1.4 Outline

In Section 2 we introduce notation and briefly review post-selection and the results of [1]. We state our motivation in Section 3, and we list the steps of the proposed protocol in Section 4. Section 5 presents a stepwise re-formulation of the protocol which is equivalent in terms of security but better suited to the proof technique that we use. In Section 6 we derive the output state of the protocol, and in Section 7 we present the security proof. We conclude with a discussion and suggestions for future work.

2 Preliminaries

2.1 Notation and terminology

Classical Random Variables (RVs) are denoted with capital letters, and their realisations with lowercase letters. The probability that a RV X takes value x is written as $\Pr[X = x]$. The expectation with respect to RV X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X = x]f(x)$. Sets are denoted in calligraphic font. The notation 'log' stands for the logarithm with base 2. The notation h stands for the binary entropy function $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. Sometimes we write $h(\{p_1,\ldots,p_k\})$ meaning $\sum_i p_i \log\frac{1}{p_i}$. Bitwise XOR of binary strings is written as '$\oplus$'. The Kronecker delta is denoted as δ_{ab}. The complement 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 $\bar{g}$.

We write $\mathbb{1}$ for the identity matrix. A linear error-correcting code with a $\ell \times n$ generator matrix G can always be written in systematic form, $G = (\mathbb{1}_\ell|\Gamma)$, where the $\ell \times (n-\ell)$ matrix Γ contains the checksum relations. For message $p \in \{0,1\}^\ell$, the codeword $c_p = p \cdot G$ then has p as its first ℓ bits, followed by $n-\ell$ redundancy bits.

For quantum states we use Dirac notation. A qubit state with classical bit x encoded in basis b is written as $|\psi^b_x\rangle$. We will always assume that we are working with 6-state encoding (known from 6-state QKD, with three possible bases) or 8-state encoding [7, 8]. Occasionally we will comment if a result is different for BB84-encoding.

The notation 'tr' stands for trace. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \operatorname{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. The trace distance between matrices ρ and σ is denoted as $\delta(\rho;\sigma) = \frac{1}{2}||\rho-\sigma||_1$. It is a generalisation of the statistical distance and represents the maximum possible advantage one can have in distinguishing ρ from σ.

Quantum states with non-italic label 'A', 'B' and 'E' indicate the subsystem of Alice/Bob/Eve. Since Eve is assumed to have full control over the environment, we also refer to the 'E' system as the environment. Consider uniform classical variables X, Y and a quantum system under Eve's control that depends on X and Y. The combined classical-quantum state is $\rho^{XY\mathrm{E}} = \mathbb{E}_{xy}|xy\rangle\langle xy| \otimes \rho^{\mathrm{E}}_{xy}$. The state of a sub-system is obtained by tracing out all the other subspaces, e.g. $\rho^{Y\mathrm{E}} = \operatorname{tr}_X \rho^{XY\mathrm{E}} =$

$\mathbb{E}_y|y\rangle\langle y|\otimes\rho_y^{\rm E}$, with $\rho_y^{\rm E}=\mathbb{E}_x\rho_{xy}^{\rm E}$. The fully mixed state on Hilbert space $\mathcal{H}_A$ is denoted as χ^A. The security of the variable X, given that Eve holds the 'E' subsystem, can be expressed in terms of a trace distance as follows [9],

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

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

We write $\mathcal{S}(\mathcal{H}_{\rm A})$ to denote the space of density matrices on Hilbert space $\mathcal{H}_{\rm A}$, i.e. positive semi-definite operators acting on $\mathcal{H}_{\rm A}$. Any quantum channel can be described by a completely positive trace-preserving (CPTP) map $\mathcal{E}:\mathcal{S}(\mathcal{H}_{\rm A})\to\mathcal{S}(\mathcal{H}_{\rm B})$ that transforms a mixed state $\rho^{\rm A}$ to $\rho^{\rm B}$: $\mathcal{E}(\rho^{\rm A})=\rho^{\rm B}$. For a map $\mathcal{E}:S(\mathcal{H}_{\rm A})\to S(\mathcal{H}_{\rm B})$, the notation $\mathcal{E}(\rho^{\rm AC})$ stands for $(\mathcal{E}\otimes\mathbb{1}_C)(\rho^{\rm AC})$, i.e. $\mathcal{E}$ acts only on the A subsystem. The diamond norm of $\mathcal{E}$ is defined as $\|\mathcal{E}\|_\diamond=\frac12\sup_{\rho^{\rm AC}\in\mathcal{S}(\mathcal{H}_{\rm AC})}\|\mathcal{E}(\rho^{\rm AC})\|_1$ with $\mathcal{H}_{\rm C}$ an auxiliary system that can be considered to be of the same dimension as $\mathcal{H}_{\rm A}$. The diamond norm $\|\mathcal{E}-\mathcal{E}'\|_\diamond$ can be used to upper bound the probability of distinguishing two CPTP maps $\mathcal{E}$ and $\mathcal{E}'$ given that the process is observed once. The maximum probability of a correct guess is $\frac12+\frac14\|\mathcal{E}-\mathcal{E}'\|_\diamond$. The security of a protocol is quantified by the diamond norm between the real protocol $\mathcal{E}$ and an protocol with ideal functionality $\mathcal{F}$. When $\|\mathcal{E}-\mathcal{F}\|_\diamond\leq\varepsilon$ we can consider $\mathcal{E}$ to behave ideally except with probability ε; this security metric is composable with other (sub-)protocols.

A family of hash functions $H=\{h:\mathcal{X}\to\mathcal{T}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [10] 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 $|H|=|\mathcal{X}|$. We define the rate of a quantum communication protocol as the number of message bits communicated per sent qubit.

2.2 Post-selection

For protocols that are invariant under permutation of their inputs it has been shown [11] that security against collective attacks (the same attack applied to each qubit individually) implies security against general attacks, at the cost of extra privacy amplification. Let $\mathcal{E}$ be a protocol that acts on $S(\mathcal{H}_{\rm AB}^{\otimes n})$ and let $\mathcal{F}$ describe the perfect functionality of that protocol. If for all permutations π on the input there exists a map $\mathcal{K}_\pi$ on the output such that $\mathcal{E}\circ\pi=\mathcal{K}_\pi\circ\mathcal{E}$ then,

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

where d is the dimension of the $\mathcal{H}_{\rm AB}$ space. ($d=4$ for qubits). The product form $\sigma^{\otimes n}$ greatly simplifies the security analysis: now it suffices to prove security against 'collective' attacks, and to pay a price $2(d^2-1)\log(n+1)$ in the amount of privacy amplification.

2.3 Brief summary of results from [1]

It was shown that the asymptotic communication rate of QKR is the same as the rate of QKD with one-way postprocessing. Alice encodes random bits into the qubits; over a classical channel she sends a ciphertext, OTP'ed information for error-correction, and an authentication tag. Let the CPTP map $\mathcal{E}$ be the protocol of [1], and $\mathcal{F}$ its idealized version where the message and the next round's keys are completely unknown to Eve. It was shown that

$$\|\mathcal{E}-\mathcal{F}\|_\diamond\leq 2^{-\lambda+1}+(n+1)^{15}\ \min\big(\varepsilon+\frac12{\rm tr}_E\sqrt{|\mathcal{B}|^n2^\ell{\rm tr}_{BS}\big(\bar\rho^{BS{\rm E}}\big)^2},P_{\rm corr}\big), \tag{3}$$

where λ is the length of the authentication tags, ε the amount of state 'smoothing' [9], n the number of qubits, $\mathcal{B}$ the alphabet of the qubit basis choice, ℓ the message length, B the basis sequence, S the random data encoded in the qubits, and $P_{\rm corr}$ the noise-dependent probability of successful error correction. The $\bar\rho^{BS{\rm E}}$ is the state $\mathcal{E}(\sigma^{\otimes n})$ (see Section 2.2) smoothened by an amount ε, with everything traced out except the B, S and E subsystems. If 6-state encoding[4] of bits is used then the 4×4 matrix σ is completely determined [12] by a single parameter: the bit error probability γ on the quantum channel. Asymptotically for large n, the bound (3) reduces to

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq 2^{-\lambda+1} + n^{15} \min\left(\sqrt{2^{\ell-n+nh(\{1-\frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\})-nh(\gamma)}}, P_{\rm corr}\right), \tag{4}$$

which yields exactly the same rate[5] $1-h(\{1-\frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\})$ as 6-state QKD with one-way postprocessing.[6] The security of N QKR rounds follows from $\|\mathcal{E}_N \circ \cdots \circ \mathcal{E}_1 - \mathcal{F}_N \circ \cdots \circ \mathcal{F}_1\|_\diamond \leq N\|\mathcal{E} - \mathcal{F}\|_\diamond$.

3 Motivation

As mentioned in Section 1, current QKR schemes all have some drawback. Either they require a quantum computer for their implementation or they have classical ciphertext. In this work we aim for a QKR protocol that has all the desiderata one would expect:

- All actions on quantum states should be simple single-qubit actions like state preparation and measurement.
- Alice should send only qubits, so that no bandwidth is wasted.
- Bob should send only an authenticated `Accept`/`Reject` bit.
- No key material should be consumed in case of `Accept`, and the bare minimum[7] should be consumed in case of `Reject`.
- The communication rate should equal that of QKD.

4 Our Quantum Key Recycling protocol

4.1 Protocol design considerations

Our protocol is very similar the the protocol in [1]. There are two main differences:

1. There is no classical communication from Alice to Bob.
2. In case of `Reject` the keys are not thrown away. Instead, fresh key material is hashed into the old keys to obtain the keys for the next round.

In the transformation from [1] to a protocol without classical ciphertext, there are several proof-technical issues. Most importantly, the qubit payload $X \in \{0,1\}^n$ needs to be uniformly random (see Section 5.3). This has to be reconciled with the fact that (i) the message is typically not uniform; (ii) the error-correction encoding step introduces redundancy. Our solution to these issues is shown in Fig. 1, which depicts most of the variables in the protocol. Alice first OTPs the message with a mask z. Then she does the error correction encoding, but randomized by OTP-ing the redundancy bits with a mask e. The last step is made easy by writing the error-correcting code in *systematic form* (Section 2.1).

4.2 Setup and protocol steps

Alice and Bob have agreed on a linear error-correcting code with encoding and decoding functions $\text{Enc} : \{0,1\}^\ell \to \{0,1\}^n$ and $\text{Dec} : \{0,1\}^n \to \{0,1\}^\ell$. The value of ℓ depends on the number of errors that must be corrected and on the choice of code. We will use notation $\texttt{Enc}_e(c) \stackrel{\text{def}}{=}$

[4]For 4-state (BB84) 'conjugate' coding Eve has two degrees of freedom, i.e. a more powerful attack.

[5]The term $nh(\gamma)$ gets cancelled because Alice and Bob expend $nh(\gamma)$ bits of key material to OTP the redundancy bits.

[6]For 4-state encoding the result is different from (4) and yields the BB84 rate.

[7]For the noiseless case, the optimum is the length of the plaintext minus one [3].

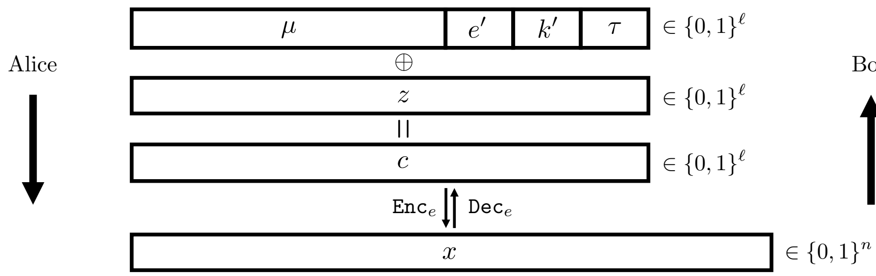

Figure 1: *Classical processing performed by Alice, and in reverse by Bob.*

$\mathrm{Enc}(c) \oplus (0_\ell \| e)$, i.e. $\mathtt{Enc}_e(c)$ is the encoding of c with mask e applied to the redundancy bits. Similarly $\mathtt{Dec}_e(x) \stackrel{\text{def}}{=} \mathrm{Dec}(x \oplus (0_\ell \| e))$.
Furthermore Alice and Bob have agreed on a MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^* \to \{0,1\}^\lambda$, and two pairwise independent hash functions $F_u : \mathcal{B}^n \times \{0,1\}^n \to \{0,1\}^\ell \times \mathcal{B}^n$ $(u \in \mathcal{U})$ and $G_v : \mathcal{B}^n \times \mathcal{Q} \to \{0,1\}^\ell \times \mathcal{B}^n$ $(v \in \mathcal{V})$.[8]
Alice's message is $\mu \in \{0,1\}^\nu$, with $\nu = \ell - 2\lambda - (n - \ell)$. The key material shared between Alice and Bob consists of a mask $z \in \{0,1\}^\ell$, a MAC key $\xi \in \{0,1\}^\lambda$ for Alice's message, a basis sequence $B \in \mathcal{B}^n$, a mask $e \in \{0,1\}^{n-\ell}$ for the redundancy bits, a MAC key $k \in \{0,1\}^\lambda$ for Bob's feedback bit, and seeds $u \in \mathcal{U}$, $v \in \mathcal{V}$ for pairwise independent hashing.[9] Furthermore Alice and Bob have a 'reservoir' of additional spare key material.

One round of the protocol consists of the following steps (see Fig. 2):
Encryption:
Alice generates random strings $e' \in \{0,1\}^{n-\ell}$, $k' \in \{0,1\}^\lambda$. She computes the authentication tag $\tau = \Gamma(\xi, \mu \| e' \| k')$, the 'augmented message' $m = \mu \| e' \| k' \| \tau$ (with $m \in \{0,1\}^\ell$), the ciphertext $c = z \oplus m$, and the qubit payload $x = \mathtt{Enc}_e(c) \in \{0,1\}^n$. She prepares $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{x_i}^{b_i}\rangle$ and sends it to Bob.
Decryption:
Bob receives $|\Psi'\rangle$. He measures $|\Psi'\rangle$ in the basis b. The result is $x' \in \{0,1\}^n$. He tries to recover $\hat{c} = \mathtt{Dec}_e(x')$. He computes $\hat{m} = \hat{c} \oplus z$, which he parses as $\hat{m} = \hat{\mu} \| \hat{e}' \| \hat{k}' \| \hat{\tau}$.
Feedback:
Bob checks if $\Gamma(\xi, \hat{\mu} \| \hat{e}' \| \hat{k}') == \hat{\tau}$. He sets $\omega = 1$ ('`Accept`') if the error correction did not produce an error and the MAC $\hat{\tau}$ is correct; $\omega = 0$ ('`Reject`') otherwise. He computes $\tau_{\text{fb}} = \Gamma(k, \omega)$ and sends ω, τ_{fb} to Alice. Alice checks the MAC on the feedback.
Key Update:
The keys/seeds ξ, u, v are always re-used. The updated version of the z, b, e, k in the next round is denoted as $\tilde{z}, \tilde{b}, \tilde{e}, \tilde{k}$.

- In case of `Accept`:
  Alice sets $\tilde{e} = e', \tilde{k} = k'$ and $\tilde{z} || \tilde{b} = F_u(b || x)$.
  Bob sets $\tilde{e} = \hat{e}', \tilde{k} = \hat{k}'$ and $\tilde{z} || \tilde{b} = F_u(b || \hat{x})$, with $\hat{x} = \mathtt{Enc}_e(\hat{c})$.
- In case of `Reject`:
  Alice and Bob take new $\tilde{e}, \tilde{k}$ from their reservoir.
  They take $q \in \mathcal{Q}$ from the reservoir and set $\tilde{z} \| \tilde{b} = G_v(b \| q)$.

[8] The set $\mathcal{B}$ is the alphabet of qubit basis choices. In BB84 encoding we have $\mathcal{B} = \{+, \times\}$; in 6-state encoding $\mathcal{B} = \{x, y, z\}$.
[9] The strings u and v are never both used in the same round. We describe them independently since they have a different length, but the shorter (v) may as well be a substring of the longer (u).

Alice	Shared secret keys: z, b, e, k, ξ, u, v	Bob
Take random $e' \in \{0,1\}^{n-\ell}$, $k' \in \{0,1\}^{\lambda}$		
Tag: $\tau = \Gamma(\xi, \mu \| e' \| k')$ Plaintext: $m = \mu \| e' \| k' \| \tau$ Ciphertext: $c = z \oplus m$ Encoding: $x = \mathtt{Enc}_e(c)$		
Prepare n quantum states: $\lvert\psi_{x_i}^{b_i}\rangle$	$\bigotimes_{i=1}^{n} \lvert\psi_{x_i}^{b_i}\rangle$ $\longrightarrow$	
		Measure $\lvert{\psi_{x_i}^{b_i}}'\rangle$ in the b_i basis yielding x' Decoding: $\hat{c} = \mathtt{Dec}_e(x')$ Plaintext: $\hat{m} = z \oplus \hat{c} = \hat{\mu} \| \hat{e}' \| \hat{k}' \| \hat{\tau}$
		Only if $\hat{\tau} == \Gamma(\xi, \hat{\mu} \| \hat{e}' \| \hat{k}')$ and `Dec` succeeds: $\omega = 1$, $\omega = 0$ otherwise $\tau_{\text{fb}} = \Gamma(k, \omega)$
Verify $\tau'_{\text{fb}} == \Gamma(k, \omega')$	$\longleftarrow$ ω, τ_{fb}	
Always re-use ξ, u, v Next round key in Accept case: $\tilde{z} \| \tilde{b} = F_u(b \| x)$, $\tilde{e} = e'$, $\tilde{k} = k'$		Always re-use ξ, u, v Next round key in Accept case: $\tilde{z} \| \tilde{b} = F_u(\hat{b} \| \hat{x})$, $\hat{e}'$, $\hat{k}'$
Reject: $\tilde{e}$, $\tilde{k}$ and q from reservoir $\tilde{z} \| \tilde{b} = G_v(b \| q)$		Reject: $\tilde{e}$, $\tilde{k}$ and q from reservoir $\tilde{z} \| \tilde{b} = G_v(\hat{b} \| q)$

Figure 2: *One round of the QKR protocol without classical communication from Alice to Bob.*

5 Protocol reformulation for the security proof

We introduce a sequence of small modifications to the protocol of Section 4. While the original protocol $\mathcal{E}_{\rm orig}$ in Section 4 is the one that Alice and Bob actually execute, we will write down the security proof for the modified protocol $\mathcal{E}_{\rm mod}$. Due to their almost-equivalence, security of $\mathcal{E}_{\rm mod}$ implies security of $\mathcal{E}_{\rm orig}$ up to a constant $2^{-\lambda+1}$.

- We go to an EPR version in order to apply standard proof methods.
- We add random permutation of the qubits so that post-selection can be used.
- We add random Pauli transforms in order to simplify the purified state.
- We pretend that the two authentication tags cannot be forged.

5.1 Masking the qubit payload with public randomness

Alice picks a random string $a \in \{0,1\}^n$ and publishes it over an authenticated channel.[10] Alice computes $s = x \oplus a$. Instead of qubit states $|\psi^{b_i}_{x_i}\rangle$ she prepares $|\psi^{b_i}_{s_i}\rangle$. We denote Bob's measurement result as $t \in \{0,1\}^n$. Bob computes $x' = t \oplus a$.
Since a is public and independently random, this roundabout way of getting x' to Bob is equivalent to the original protocol as far as security is concerned.

5.2 EPR version of the protocol

Instead of having Alice prepare a qubit state and Bob measuring it, now Eve prepares a noisy two-qubit EPR state (singlet state) and gives the two subsystems 'A' and 'B' to Alice and Bob respectively. Alice and Bob measure their i'th qubit in basis b_i; this yields s_i for Alice and t_i for Bob, where t_i equals $\overline{s_i}$ plus noise. The s_i (or t_i) is random.
Alice computes $a = s \oplus x$ and publishes a in an authenticated way. Bob computes $y = t \oplus a$. The rest of the classical processing is the same as in the original protocol, with $x' = \bar{y}$.
Note that the statistics of the variables s, t, a, x, x' is the same as in Section 5.1, although the origin of the variables is now different. The equivalence between prepare-and-measure on the one hand and the EPR mechanism on the other hand has been exploited in many works.

5.3 Adding a random permutation

After Eve has handed out all n EPR pairs, Alice and Bob publicly agree on a random permutation $\pi \in S_n$. (Here S_n is the set of n-element permutations.) Before performing any measurement they both apply π to their own set of n qubits. Then they forget π. The remainder of the protocol is as in Section 5.2.
For Alice and Bob the effect of the permutation is that the noise is distributed differently over the qubits. The error-correction step is insensitive to the location of bit errors; only the number of bit errors matters. Hence all the classical variables that are processed/computed after the error correction step are unaffected by π. The only *output* variable of the protocol that is affected is a. However, a was a uniform[11] random variable and has now become a different uniform variable; as far as security is concerned, the new protocol is equivalent to the one in Section 5.2.
Let $\mathcal{E}_{\rm perm}$ denote the protocol containing the random permutation step. In the language of Section 2.2 we can write $\mathcal{E}_{\rm perm} \circ \pi = \mathcal{E}_{\rm perm}$. (After all, a permutation followed by a random permutation is a random permutation.) We conclude that the post-selection criterion holds and we can apply (2).
Note that $\mathcal{E}_{\rm perm}$ needs quantum memory. This has no practical significance, since Alice and Bob actually execute $\mathcal{E}_{\rm orig}$, while $\mathcal{E}_{\rm perm}$ is a proof-technical fiction.

[10] This is a tamper-proof channel with perfect authentication. Eve is allowed to know a.

[11] From Eve's point of view, a gets randomized by x, which is uniform because it is built from z and e, which are unknown to Eve.

5.4 Adding random Pauli transforms

This is the trick introduced by [12]. For each individual EPR pair, Alice and Bob publicly agree on a random $\alpha \in \{0, 1, 2, 3\}$. They both apply the Pauli transform σ_α to their own qubit state, and then forget α. This happens before they do their measurement. The rest of the protocol is as in section 5.3.
The mapping in a single qubit position can be written as

$$\rho^{\mathrm{AB}} \mapsto \tilde{\rho}^{\mathrm{AB}} = \tfrac{1}{4} \sum_\alpha (\sigma_\alpha \otimes \sigma_\alpha) \rho^{\mathrm{AB}} (\sigma_\alpha \otimes \sigma_\alpha). \tag{5}$$

The net effect of the Pauli transforms is that the measurement sequence b gets randomized[12] with public randomness; but b was already random, so security-wise nothing has changed.
The random-Paulis trick yields a major simplification: For six-state encoding (and higher), only one degree of freedom is left in the description of Eve's state, namely the bit error probability. This was an important ingredient of the security proof in [1].

5.5 Pretending that the authentication tags are unforgeable

We pretend that Eve is unable to forge the authentication tags τ and τ_{fb}, which is true except with probability $\leq 2 \cdot 2^{-\lambda}$. This has two benefits: (i) We get rid of complicated case-by-case analyses that would allow events where the error correction yields a wrong $\hat{c}$ without warning, while $\hat{\tau}$ looks correct; (ii) In the `Accept` case Bob's reconstructed variables $\hat{c}, \hat{m}$ equal Alice's c, m, thus reducing the number of variables.

5.6 Effect of the modifications

Fig. 3 depicts the protocol $\mathcal{E}_{\mathrm{mod}}$. Due to the unforgeability of the tags we can write

$$\|\mathcal{E}_{\mathrm{orig}} - \mathcal{F}_{\mathrm{orig}}\|_\diamond \leq 2^{-\lambda+1} + \|\mathcal{E}_{\mathrm{mod}} - \mathcal{F}_{\mathrm{mod}}\|_\diamond. \tag{6}$$

Furthermore, due to the permutation invariance of $\mathcal{E}_{\mathrm{mod}}$ we can apply the post-selection proof technique and use (2). Finally, thanks to the random Paulis, the state σ in (2) will have the very simple form that makes it possible to arrive at an expression like (4).

6 The output state

The Completely Positive Trace Preserving (CPTP) map $\mathcal{E}_{\mathrm{mod}}$ acts on the 'AB' subsystem (the $2n$ qubits controlled by Alice and Bob) without affecting the 'E' subsystem. We write

$$\mathcal{E}_{\mathrm{mod}} = \mathcal{T} \circ \mathcal{P} \circ \mathcal{M} \circ \mathcal{I}. \tag{7}$$

The map $\mathcal{I}$ fetches the classical input variables, $\mathcal{M}$ is the measurement, $\mathcal{P}$ is the classical processing, and $\mathcal{T}$ traces away all variables that are not outputs. The input variables are $mzbekuv$. We have $\mathcal{I}(\rho^{\mathrm{ABE}}) = \mathbb{E}_{mzbekuv} |mzbekuv\rangle\langle mzbekuv| \otimes \rho^{\mathrm{ABE}}$.[13] Note that all input variables except m are uniform.
The measurement $\mathcal{M}$ introduces coupling between the classical b register and the quantum state. Furthermore, it destroys the AB subsystem and creates new classical registers $s, t \in \{0,1\}^n$.

$$\mathcal{M}\big(|b\rangle\langle b| \otimes \rho^{\mathrm{ABE}}\big) = \mathbb{E}_{st} |bst\rangle\langle bst| \otimes \rho^{\mathrm{E}}_{bst}. \tag{8}$$

[12]Let Alice and Bob both perform a projective measurement on their own part of $\tilde{\rho}^{\mathrm{AB}}$ in basis $|\psi^b_x\rangle, |\psi^b_{\bar{x}}\rangle$. This can be rewritten as projective measurements on ρ^{AB} in basis $\sigma_\alpha|\psi^b_x\rangle, \sigma_\alpha|\psi^b_{\bar{x}}\rangle$.

[13]One can also start from a protocol description $\mathcal{E}'_{\mathrm{mod}}$ that acts on a state $|\mathrm{inputs}\rangle\langle\mathrm{inputs}| \otimes \rho^{\mathrm{AB}}$, i.e. $\mathcal{E}'_{\mathrm{mod}}$ describes how the protocol acts on the quantum state ρ^{AB} given some value of the classical inputs. The quantity of interest is then $\mathcal{E}'_{\mathrm{mod}}$ acting on a linear combination of input values; this exactly matches the above mapping $\mathcal{I}$.

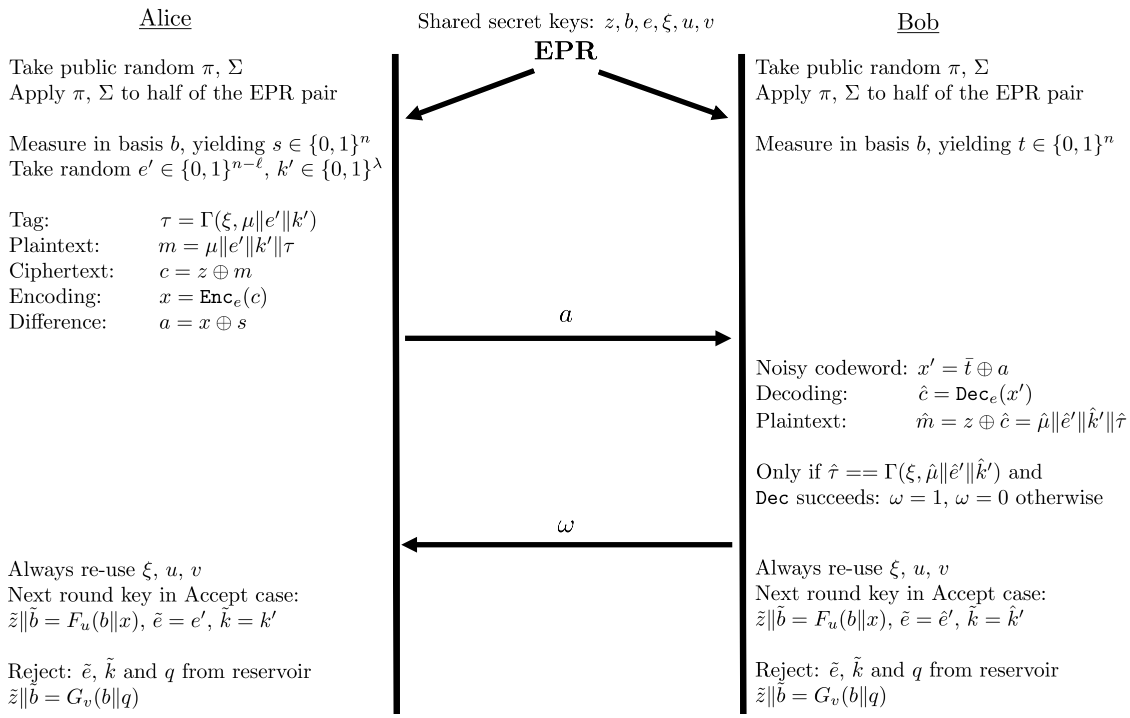

Figure 3: *The modified protocol with EPR states, random permutation, random Pauli transformations and perfect authentication. The notation π stands for a permutation and Σ for a vector of n Pauli matrices.*

For the factorised form of ρ^{ABE} it holds that $\mathbb{E}_{st}(\cdots) = \sum_{st} 2^{-n} P_{t|s}(\cdots)$, with $P_{t|s} \stackrel{\text{def}}{=} \gamma^{|s\oplus\bar{t}|}(1-\gamma)^{|s\oplus t|}$, where γ is the bit error probability caused by Eve.
The processing $\mathcal{P}$ introduces the new variables[14] $cxay\omega\tilde{z}\tilde{b}$ created by Alice and Bob's computations, and fetches q from the reservoir. Let $n\beta$ be the number of bit errors that the error-correcting code can correct. We define the indicator function θ_{st} such that $\theta_{st} = 1$ when $|\bar{s} \oplus t| \leq n\beta$ and $\theta_{st} = 0$ otherwise.

$$\begin{aligned}(\mathcal{P} \circ \mathcal{M} \circ \mathcal{I})(\rho^{\mathrm{ABE}}) \quad = \quad & \mathbb{E}_{mzbekuvq} |mzbekuvq\rangle\langle mzbekuvq| \otimes \\ & \sum_{cxay\omega\tilde{z}\tilde{b}} |cxay\omega\tilde{z}\tilde{b}\rangle\langle cxay\omega\tilde{z}\tilde{b}| \otimes \mathbb{E}_{st} |st\rangle\langle st| \otimes \rho^{\mathrm{E}}_{bst} \\ & \delta_{c,m\oplus z}\delta_{x,\mathtt{Enc}_e(c)}\delta_{a,x\oplus s}\delta_{y,t\oplus a}\delta_{\omega,\theta_{st}}\left[\theta_{st}\delta_{\tilde{z}\|\tilde{b},F_u(b\|x)} + \overline{\theta_{st}}\delta_{\tilde{z}\|\tilde{b},G_v(b\|q)}\right]. \end{aligned} \tag{9}$$

The protocol output consists of the classical variables $a\omega m\tilde{z}\tilde{b}uv$. The map $\mathcal{T}$ traces out all the non-output registers. Applying this trace to (9) yields

$$\mathcal{E}_{\mathrm{mod}}(\rho^{\mathrm{ABE}}) \quad = \quad \rho^{UV\tilde{Z}\tilde{B}MA\Omega\mathrm{E}}$$

$$= \quad \mathbb{E}_{uvm\tilde{z}\tilde{b}a} \sum_{\omega} |uv\tilde{z}\tilde{b}ma\omega\rangle\langle uv\tilde{z}\tilde{b}ma\omega| \otimes [\omega\rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} + \overline{\omega}\rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}\tilde{z}a}] \tag{10}$$

$$\rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} \quad = \quad \mathbb{E}_{bst}\rho^{\mathrm{E}}_{bst}\theta_{st}2^{\ell}|\mathcal{B}|^n\delta_{\tilde{z}\|\tilde{b},F_u(b\|a\oplus s)} \tag{11}$$

$$\rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}\tilde{z}a} \quad = \quad \mathbb{E}_{bst}\rho^{\mathrm{E}}_{bst}\overline{\theta_{st}}2^{\ell}|\mathcal{B}|^n\mathbb{E}_q\delta_{\tilde{z}\|\tilde{b},G_v(b\|q)}. \tag{12}$$

[14]Here we do not keep track of the updates $\tilde{e}$ and $\tilde{k}$. Their security is trivial: they are updated either from m, which is confidential, or from the reservoir.

Here we used $\sum_{ce} \delta_{x,\mathtt{Enc_e(c)}} = 1$. In slight abuse of notation we have written $2^{-n}\sum_a = \mathbb{E}_a$, $2^{-\ell}\sum_{\tilde z} = \mathbb{E}_{\tilde z}$, $|\mathcal{B}|^{-n}\sum_{\tilde b} = \mathbb{E}_{\tilde b}$. In (10,11,12) we should have formally written $\rho^{\mathrm{E}[\omega=1]}_{uv\tilde b\tilde z ma}$ and $\rho^{\mathrm{E}[\omega=0]}_{uv\tilde b\tilde z ma}$, but in the subscript we have kept only the variables on which the state actually has dependence. The idealized version $\mathcal{F}_{\mathrm{mod}}$ of the protocol is obtained by first executing $\mathcal{E}_{\mathrm{mod}}$, then tracing away the message m and the keys $uv\tilde z\tilde b$, and finally replacing them with completely random values.[15]

$$\mathcal{F}_{\mathrm{mod}}(\rho^{\mathrm{ABE}}) = \chi^{UV\tilde Z\tilde BA} \otimes \mathbb{E}_m |m\rangle\langle m| \otimes \sum_\omega |\omega\rangle\langle\omega| \otimes \Big(\omega\rho^{\mathrm{E}[\omega=1]} + \overline{\omega}\rho^{\mathrm{E}[\omega=0]}\Big) \tag{13}$$

$$\rho^{\mathrm{E}[\omega=1]} = \mathbb{E}_{bst}\rho^{\mathrm{E}}_{bst}\theta_{st} \tag{14}$$

$$\rho^{\mathrm{E}[\omega=0]} = \mathbb{E}_{bst}\rho^{\mathrm{E}}_{bst}\overline{\theta_{st}}. \tag{15}$$

The states with label '$[\omega=1]$' are sub-normalised; we have $\mathrm{tr}\,\rho^{\mathrm{E}[\omega=1]} = P_{\mathrm{corr}}$ and $\mathbb{E}_u \mathrm{tr}\,\rho^{\mathrm{E}[\omega=1]}_{u\tilde b\tilde z a} = P_{\mathrm{corr}}$, where we define P_{corr} as the probability that the number of errors can be corrected. In the factorised form of ρ it holds that

$$P_{\mathrm{corr}}(n,\beta,\gamma) = \mathbb{E}_{st}\theta_{st} = \sum_{c=0}^{\lfloor n\beta\rfloor}\binom{n}{c}\gamma^c(1-\gamma)^{n-c}. \tag{16}$$

Similarly $\mathrm{tr}\,\rho^{\mathrm{E}[\omega=0]} = 1 - P_{\mathrm{corr}}$ and $\mathbb{E}_v \mathrm{tr}\,\rho^{\mathrm{E}[\omega=0]}_{v\tilde b\tilde z a} = 1 - P_{\mathrm{corr}}$.
Note that the trace distance of the actual versus the ideal output state has an intuitive meaning as the distance of the keys/seeds from uniformity given Eve's side information,

$$\Big\|(\mathcal{E}_{\mathrm{mod}} - \mathcal{F}_{\mathrm{mod}})(\rho^{\mathrm{ABE}})\Big\|_1 = \Big\|\rho^{UV\tilde Z\tilde BMA\Omega\mathrm{E}} - \chi^{UV\tilde Z\tilde B}\rho^{MA\Omega\mathrm{E}}\Big\|_1 = 2d(UV\tilde Z\tilde B|MA\Omega\mathrm{E}). \tag{17}$$

7 Security Proof

7.1 Attacker Model

The attacker model is the standard one in quantum cryptography. No information leaks from the labs of Alice or Bob, i.e. there are no side-channels. Eve fully controls the environment outside Alice and Bob's labs. Eve has unbounded quantum memory and unbounded (quantum-)computational resources. Eve's measurements are noiseless.

7.2 Forward secrecy

Equations (10) and (13) serve as the starting point for the security proof. Note that the expression (13) is also obtained if M is *not* traced away; consequently the analysis of known-plaintext and unknown-plaintext attacks turns out to be identical, just as was the case in [1]. An even stronger result holds: In (10) the M is entirely decoupled from Eve's (classical and quantum) side information and from the next-round variables $UV\tilde Z\tilde B$. Hence our protocol has forward secrecy: a compromise of the updated keys has no impact on the secrecy of the message μ.

7.3 Main result: upper bound on the diamond norm

Theorem 1 *Let ρ^{ABE} have the factorised form $(\sigma^{\mathrm{ABE}})^{\otimes n}$, with σ^{ABE} symmetrised by the random Pauli transform. Let ε be a smoothing parameter, and let $\bar\rho$ denote a smoothed state. Then*

$$\Big\|\mathcal{E}_{\mathrm{orig}} - \mathcal{F}_{\mathrm{orig}}\Big\|_\diamond < 2^{-\lambda+1} + (n+1)^{15}\left[\sqrt{\frac{2^{\ell-2}}{|\mathcal{Q}|}} + \min\left\{P_{\mathrm{corr}}, \varepsilon + \frac{1}{2}\mathrm{tr}_{\mathrm{E}}\sqrt{2^\ell|\mathcal{B}|^n \mathrm{tr}_{BS}(\bar\rho^{BSE})^2}\right\}\right]. \tag{18}$$

[15] The distribution of m does not have to be uniform.

The $\min\{\cdots\}$ term is the same as in (3), which implies that the asymptotic rate of our QKR scheme is as mentioned in Section 2.3. The term $\sqrt{2^{\ell-2}/|\mathcal{Q}|}$ dictates that, in order to have α bits of security, we have to set $\log|\mathcal{Q}| > \ell - 2 + 2\alpha + 30\log(n+1)$. Hence in case of `Reject` the amount of expended key material is $n - 1 + 30\log(n+1) + \lambda + 2\alpha$. Asymptotically this is $n[1 + \mathcal{O}(\frac{\log n}{n})]$.

Proof of Theorem 1: The term $2^{-\lambda+1}$ comes from the transition from $\mathcal{E}_{\rm orig}$ to $\mathcal{E}_{\rm mod}$. The factor $(n+1)^{15}$ comes from applying the postselection theorem (2). For bounding the trace norm $\|(\mathcal{E}_{\rm mod} - \mathcal{F}_{\rm mod})(\rho^{\rm ABE})\|_1$, we start from (10),(13) and use the fact that the eigenvalue problem reduces to an individual eigenvalue problem for each value of the classical variables, orthogonal to the other values. We get

$$\begin{aligned}
\|(\mathcal{E}_{\rm mod} - \mathcal{F}_{\rm mod})(\rho^{\rm ABE})\|_1 &= D_{\tt acc} + D_{\tt rej} &(19)\\
D_{\tt acc} &= \mathbb{E}_{um\tilde{z}\tilde{b}a}\left\|\rho^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \rho^{{\rm E}[\omega=1]}\right\|_1 &(20)\\
D_{\tt rej} &= \mathbb{E}_{vm\tilde{z}\tilde{b}a}\left\|\rho^{{\rm E}[\omega=0]}_{v\tilde{b}\tilde{z}a} - \rho^{{\rm E}[\omega=0]}\right\|_1. &(21)
\end{aligned}$$

First we provide two upper bounds on $D_{\tt acc}$. The first one simply follows from the triangle inequality,

$$\mathbb{E}_u\left\|\rho^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \rho^{{\rm E}[\omega=1]}\right\|_1 \leq \mathbb{E}_u\|\rho^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a}\|_1 + \mathbb{E}_u\|\rho^{{\rm E}[\omega=1]}\|_1 = \mathbb{E}_u{\rm tr}\,\rho^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} + {\rm tr}\,\rho^{{\rm E}[\omega=1]} = 2P_{\rm corr}. \quad (22)$$

The second bound on $D_{\tt acc}$ takes some more work. We introduce smoothing of ρ as in [12, 9, 13], allowing states $\bar{\rho}$ that are ε-close to ρ in the sense of trace distance. We have $D_{\tt acc} \leq 2\varepsilon + \overline{D}_{\tt acc}$, with $\overline{D}_{\tt acc} = \mathbb{E}_{uvm\tilde{z}\tilde{b}a}\|\bar{\rho}^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \bar{\rho}^{{\rm E}[\omega=1]}\|_1$. We write

$$\begin{aligned}
\overline{D}_{\tt acc} &= \mathbb{E}_{mu\tilde{z}\tilde{b}a}{\rm tr}\sqrt{(\bar{\rho}^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \bar{\rho}^{{\rm E}[\omega=1]})^2} &(23)\\
&\stackrel{\rm Jensen}{\leq} \mathbb{E}_{m\tilde{z}\tilde{b}a}{\rm tr}\sqrt{\mathbb{E}_u(\bar{\rho}^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \bar{\rho}^{{\rm E}[\omega=1]})^2} &(24)\\
&= \mathbb{E}_{m\tilde{z}\tilde{b}a}{\rm tr}\sqrt{\mathbb{E}_u(\bar{\rho}^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a})^2 - (\bar{\rho}^{{\rm E}[\omega=1]})^2}. &(25)
\end{aligned}$$

In (24) we used Jensen's inequality for concave operators. In (25) we used $\mathbb{E}_u\bar{\rho}^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a} = \bar{\rho}^{{\rm E}[\omega=1]}$. Next we evaluate the expression under the square root, making use of the properties of the pairwise independent hash function F. Squaring (11) yields

$$\begin{aligned}
&\mathbb{E}_u(\bar{\rho}^{{\rm E}[\omega=1]}_{u\tilde{b}\tilde{z}a})^2 - (\bar{\rho}^{{\rm E}[\omega=1]})^2\\
&\quad= \mathbb{E}_{bb'ss'tt'}\bar{\rho}^{\rm E}_{bst}\bar{\rho}^{\rm E}_{b's't'}\theta_{st}\theta_{s't'}2^{2\ell}|\mathcal{B}|^{2n}\mathbb{E}_u\delta_{\tilde{z}\|\tilde{b},F_u(b\|a\oplus s)}\delta_{\tilde{z}\|\tilde{b},F_u(b'\|a\oplus s')} - (\bar{\rho}^{{\rm E}[\omega=1]})^2 &(26)\\
&\quad= \mathbb{E}_{bb'ss'tt'}\bar{\rho}^{\rm E}_{bst}\bar{\rho}^{\rm E}_{b's't'}\theta_{st}\theta_{s't'}\left\{1 + (2^\ell|\mathcal{B}|^n - 1)\delta_{bb'}\delta_{ss'}\right\} - (\bar{\rho}^{{\rm E}[\omega=1]})^2 &(27)\\
&\quad= (2^\ell|\mathcal{B}|^n - 1)\mathbb{E}_{bb'ss'tt'}\delta_{bb'}\delta_{ss'}\bar{\rho}^{\rm E}_{bst}\bar{\rho}^{\rm E}_{b's't'}\theta_{st}\theta_{s't'} &(28)\\
&\quad< 2^\ell|\mathcal{B}|^n\mathbb{E}_{bb'ss'tt'}\delta_{bb'}\delta_{ss'}\bar{\rho}^{\rm E}_{bst}\bar{\rho}^{\rm E}_{b's't'} &(29)\\
&\quad= 2^\ell|\mathcal{B}|^n\mathbb{E}_{bb'ss'}\delta_{bb'}\delta_{ss'}\bar{\rho}^{\rm E}_{bs}\bar{\rho}^{\rm E}_{b's'} = 2^\ell|\mathcal{B}|^n{\rm tr}_{BS}(\bar{\rho}^{BSE})^2. &(30)
\end{aligned}$$

In (29) we used $\theta_{st} \leq 1$. We have obtained the bound $\overline{D}_{\tt acc} < {\rm tr}_{\rm E}\sqrt{2^\ell|\mathcal{B}|^n{\rm tr}_{BS}(\bar{\rho}^{BSE})^2}$. We derive a bound on $D_{\tt rej}$ using similar steps, but without the smoothing. Squaring (12) and taking the expectation $\mathbb{E}_v$ we get

$$
\begin{aligned}
& \mathbb{E}_v(\rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}\tilde{z}a})^2 - (\rho^{\mathrm{E}[\omega=0]})^2 \\
& \quad = \mathbb{E}_{bb'ss'tt'}\rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'}\overline{\theta_{st}}\,\overline{\theta_{s't'}}\mathbb{E}_{qq'}2^{2\ell}|\mathcal{B}|^{2n}\mathbb{E}_v\delta_{\tilde{z}\|\tilde{b},G_v(b\|q)}\delta_{\tilde{z}\|\tilde{b},G_v(b'\|q')} - (\rho^{\mathrm{E}[\omega=0]})^2 && (31) \\
& \quad = \mathbb{E}_{bb'ss'tt'}\rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'}\overline{\theta_{st}}\,\overline{\theta_{s't'}}\mathbb{E}_{qq'}\{1+(2^{\ell}|\mathcal{B}|^n-1)\delta_{bb'}\delta_{qq'}\} - (\rho^{\mathrm{E}[\omega=0]})^2 && (32) \\
& \quad = \frac{2^{\ell}|\mathcal{B}|^n-1}{|\mathcal{Q}|}\mathbb{E}_{bb'ss'tt'}\delta_{bb'}\rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'}\overline{\theta_{st}}\,\overline{\theta_{s't'}} && (33) \\
& \quad < \frac{2^{\ell}|\mathcal{B}|^n}{|\mathcal{Q}|}\mathbb{E}_{bb'ss'tt'}\delta_{bb'}\rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'} = \frac{2^{\ell}|\mathcal{B}|^n}{|\mathcal{Q}|}\mathbb{E}_{bb'}\delta_{bb'}\rho^{\mathrm{E}}_{b}\rho^{\mathrm{E}}_{b'} && (34) \\
& \quad = \frac{2^{\ell}}{|\mathcal{Q}|}(\rho^{\mathrm{E}})^2. && (35)
\end{aligned}
$$

In the last step we used the special property that ρ^{E}_b does not actually depend on b and thus equals ρ^{E} [1]. (This property holds for the factorised and Pauli-symmetrised form of ρ^{ABE}.) We have obtained a bound $D_{\mathtt{rej}} < \sqrt{2^{\ell}/|\mathcal{Q}|}$. □

In the proof above the updated $\tilde{e}$ and $\tilde{k}$ do not appear explicitly. The security of $\tilde{e}\tilde{k}$ is guaranteed because (i) in the `Accept` case the update resides inside m, which is secure; (ii) in the `Reject` case the update is done from the reservoir.

Similarly, in the proof the MAC key ξ does not appear explicitly. The fact that m is secure implies that the tag τ remains confidential (τ is a part of m), and hence there is no leakage about the MAC key ξ that was used to create the tag.

8 Discussion

We have shown that the protocol in [1] can be modified in a way that eliminates all classical communication from Alice to Bob. Essentially we have moved the classical OTP of [1] to the next QKR round, where it gets used as a mask on the message before the encoding step. Furthermore the error correction and authentication are happening 'inside' the quantum state. The asymptotic communication rate is not affected and is equal to the rate of QKD with one-way postprocessing. Our protocol has forward secrecy.

The size of the keys shared by Alice and Bob is $n + n\log|\mathcal{B}| + \log|\mathcal{U}| + 2\lambda$, (namely $z \in \{0,1\}^{\ell}$, $e \in \{0,1\}^{n-\ell}$, $b \in \mathcal{B}^n$, $u \in \mathcal{U}$, $\xi \in \{0,1\}^{\lambda}$, $k \in \{0,1\}^{\lambda}$), with $\log|\mathcal{U}| = n + n\log|\mathcal{B}|$. The size of $\mathcal{U}$ can be reduced to $|\mathcal{U}| \approx 2^{n-k}$ by using *almost-pairwise independent* hashes.

It is possible to make the seed u public randomness that is drawn in every QKR round. This would not affect the security, and it would reduce the amount of shared key material. However, it would require either (a) a source of public randomness that is not known by Eve beforehand, e.g. a broadcast; or (b) communication of u from Alice to Bob or the other way round. The former involves nontrivial logistics, while the latter violates the aims of this paper.

In the `Accept` case the size of the reservoir is unaffected. In the `Reject` case the number of bits expended from the reservoir is $n+\mathcal{O}(\log n)$. Asymptotically, in the noiseless case, this expenditure is close to the optimum value ℓ [3]. It is not possible to protect an ℓ-bit message information-theoretically with less key expenditure.

We have not done anything about the classical communication from Bob to Alice. It cannot be removed, because Alice needs to know if Bob correctly received her message. On the other hand, one can consider a scenario where Alice and Bob are both senders, in an alternating way. Then the feedback bit can be placed inside the next message, resulting in a fully quantum conversation.

There is one drawback to the protocol described in this paper. It is bad at dealing with erasures. As the actual message (as opposed to a random string) is encoded in the quantum state, absorption of qubits in the quantum channel has to be compensated in the error-correcting code. The effect of erasures on the rate is severe. A solution as proposed in [1] would imply that the message is no longer encoded directly in the qubits; instead Alice sends a random string to Bob, part of which

survives the channel and gets used to derive an OTP. Such a solution does not satisfy the aims of the this paper.
As a topic for future work we mention finite-size analysis, e.g. smoothing without taking the limit $n \to \infty$.

Acknowledgements

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

References

[1] D. Leermakers and B. Škorić. Security proof for Quantum Key Recycling with noise. `https://eprint.iacr.org/2018/264`.

[2] 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.

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

[4] 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.

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

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

[7] 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.

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

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

[10] 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.

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

[12] R. Renner. *Security of quantum key distribution*. PhD thesis, ETH Zürich, 2005.

[13] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.