Qubit-based Unclonable Encryption with Key Recycling

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

Abstract

We re-visit Unclonable Encryption as introduced by Gottesman in 2003. We introduce two qubit-based prepare-and-measure Unclonable Encryption schemes with re-usable keys. In our first scheme there is no classical communication from Alice to Bob. Over a noisy channel its communication rate is lower than in Quantum Key Recycling schemes that lack unclonability. Our second scheme needs more rounds but has the advantage that it achieves the same rate as Quantum Key Distribution.
We provide security proofs for both our schemes, based on the diamond norm distance, taking noise into account.

1 Introduction

1.1 Doing better than One-Time Pad encryption

Classically, the best confidentiality guarantee is provided by One-Time Pad (OTP) encryption. If Alice and Bob share a uniform n-bit secret key, they can exchange an n-bit message with information-theoretic security. In the classical setting Eve is able to save a copy of the ciphertext. For the message to remain secure in the future, two conditions must be met:

1. The key is used only once.
2. The key is never revealed.

If a quantum channel is available, these conditions can both be relaxed. (i) Quantum Key Recycling (QKR) [5, 11, 14] schemes provide a way of re-using encryption keys. (ii) Unclonable Encryption (UE) [9] guarantees that a message remains secure even if the keys leak at some time in the future. In this paper we introduce schemes that achieve both the QKR and UE properties while acting only on individual qubits with simple prepare-and-measure operations.

1.2 Quantum Key Recycling

The most famous use of a quantum channel in the context of cryptography is Quantum Key Distribution (QKD). First proposed in 1984 [4], QKD allows Alice and Bob to extend a small key, used for authentication, to a longer key in an information-theoretically secure way. Combined with classical OTP encryption this lets Alice and Bob exchange messages with unconditional security. The QKD field has received a large amount of attention, resulting in QKD schemes that discard fewer qubits, various advanced proof techniques, improved noise tolerance, improved rates, use of EPR pairs, higher-dimensional quantum systems etc. [1, 2, 8, 10, 12, 15, 18–21].
Much less known is that the concept of QKR was proposed two years before QKD [5]. QKR allows for the re-use of the secret encoding key when no disturbance is detected. QKD and QKR have a lot in common. (i) They both encode classical data in quantum states, in a basis that is not a priori known to Eve. (ii) They rely on the no-cloning theorem [24] to guarantee that without disturbing the quantum state, Eve can not gain information about the classical payload or about the basis.
The security of QKD has been well understood for a long time [e.g. 8, 18–20], while a security proof for qubit-based QKR has been provided fairly recently [11]. A cipher with near optimal rate

using high-dimensional qudits was introduced in 2005 [7]. Unfortunately, their method requires a quantum computer to perform encryption and decryption. In 2017, a way of doing authentication (and encryption) of quantum states with Key Recycling was proposed [17]. However this work did not lead to a prepare-and-measure variant.

The main advantage of QKR over QKD+OTP is reduced round complexity: QKR needs only two rounds. After the communication from Alice to Bob, only a single bit of authenticated information needs to be sent back from Bob to Alice. Recently, it was shown that QKR over a noisy quantum channel can achieve the same communication rate as QKD (in terms of message bits per qubit) even if Alice sends only qubits [13]; a further reduction of the total amount of communicated data.

1.3 Unclonable Encryption

In 2003, D. Gottesman introduced a scheme called *Unclonable Encryption*[1] (UE) [9] where the message remains secure even if the encryption keys leak at a later time (provided that no disturbance is detected). His work was motivated by the fact that on the one hand many protocols require keys to be deleted, but on the other hand permanent deletion of data from nonvolatile memory is a nontrivial task. In this light it is prudent to assume that all key material which is not *immediately* discarded is in danger of becoming public in the future; hence the UE security notion demands that the message stays safe even if all this key material is made public after Alice and Bob decide that they detected no disturbance. (In case disturbance is detected, the keys have to remain secret forever or permanently destroyed.)

Gottesman remarked on the close relationship between UE and QKD, and in fact constructed a QKD variant from UE. The revealing of the basis choices in QKD is equivalent to revealing keys in UE.

It is interesting to note that Gottesman's UE construction allows partial re-use of keys. However, it still expends one bit of key material per qubit sent. In the current paper we introduce qubit-based[2] UE without key expenditure.

2 Contributions

We propose two prepare-and-measure Unclonable Encryption schemes with full key recycling. (These can also be viewed as two variants of the same basic idea.) Alice sends data to Bob in N chunks. Each chunk has a length of ℓ bits and is encoded into n qubits. Each chunk individually is tested by Bob for consistency (sufficiently low noise and valid MAC). In case of `accept`, Alice and Bob re-use their keys; in case of `reject` they have to access new key material. After the N rounds all key material is assumed to become public.

Our two protocol variants differ as follows:

- Variant 1. ('Embedded'). All communication from Alice to Bob is encoded directly into the qubits. A round consists of the qubits sent by Alice, and a one-bit feedback message returned by Bob. Over a noisy channel the rate is lower than the QKD rate.
- Variant 2. ('Interactive'). A round consists of four passes. After Bob has confirmed receipt of Alice's qubits, Alice sends a syndrome. Finally Bob sends a feedback bit. The rate equals the QKD rate.

We provide a security proof for each variant by upper bounding the diamond distance between the protocol and its idealized functionality. In particular, we use a reduction to the diamond distance that is associated with the security of QKD [18]. In the case of a noiseless channel this reduction is almost immediate, without involving any inequalities.

The *Embedded* variant has the advantage of low round complexity, but has a low rate; the *Interactive* variant achieves the QKD rate but its communication complexity (number of passes) is high.

[1] This is slightly different from the unclonability notion of Broadbent and Lord [3] which considers two collaborating parties who both wish to recover the plaintext.

[2] Although this is not mentioned in the literature, we suspect that the high-dimenional QKR scheme of Damgård et al. [7] has the UE property.

The rate reduction in the *Embedded* variant is given by $\frac{n-k}{n}$, where n is the number of qubits and k the message length of the error-correcting code.
The outline of the paper is as follows. After introducing notation and preliminaries in Section 3, we introduce the security definition in Section 4. We then discuss the details of the *Embedded* protocol (Section 5) and its security (Section 6). Next, we introduce and analyze the *Interactive* protocol (Section 7). Finally, in Section 8 we compare our schemes to existing qubit-based alternatives.

3 Preliminaries

3.1 Notation and terminology

Classical Random Variables are denoted with capital letters, and their realisations with lowercase letters. The expectation with respect to X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X = x]f(x)$. For the ℓ most significant bits of the string s we write $s[{:}\ell]$. 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 $h(p_1,\dots,p_k)$ meaning $\sum_{i=1}^{k} p_i \log\frac{1}{p_i}$. Bitwise XOR of binary strings is written as '$\oplus$'. The Kronecker delta is denoted as δ_{ab}. We will speak about 'the bit error rate β of a quantum channel'. This is defined as the probability that a classical bit x, sent by Alice embedded in a qubit, arrives at Bob's side as the flipped value $\bar{x}$. 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 $|\psi_x^b\rangle$. The set of bases is denoted as $\mathcal{B}$. In the case of BB84 states we have $\mathcal{B} = \{x,z\}$; in case of 6-state encoding $\mathcal{B} = \{x,y,z\}$. The notation 'tr' stands for trace. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. Quantum states with non-italic label 'A', 'B' and 'E' indicate the subsystem of Alice/Bob/Eve.
Consider 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 subsystem is obtained by tracing out all the other subspaces, e.g. $\rho^{Y\mathrm{E}} = \mathrm{tr}_X \rho^{XY\mathrm{E}} = \mathbb{E}_y |y\rangle\langle y| \otimes \rho^{\mathrm{E}}_y$, with $\rho^{\mathrm{E}}_y = \mathbb{E}_x \rho^{\mathrm{E}}_{xy}$. The fully mixed state on Hilbert space $\mathcal{H}_A$ is denoted as χ^A. We also use the notation $\mu^X = \mathbb{E}_x |x\rangle\langle x|$ for a classical variable X whose distribution is not necessarily uniform.
We write $\mathcal{S}(\mathcal{H})$ to denote the space of density matrices on Hilbert space $\mathcal{H}$, i.e. positive semi-definite operators acting on $\mathcal{H}$. Any quantum channel can be described by a completely positive trace-preserving (CPTP) map $\mathcal{E} : \mathcal{S}(\mathcal{H}_\mathrm{A}) \to \mathcal{S}(\mathcal{H}_\mathrm{B})$ that transforms a mixed state ρ^A to ρ^B: $\mathcal{E}(\rho^\mathrm{A}) = \rho^\mathrm{B}$. For a map $\mathcal{E} : S(\mathcal{H}_\mathrm{A}) \to S(\mathcal{H}_\mathrm{B})$, the notation $\mathcal{E}(\rho^{\mathrm{AC}})$ stands for $(\mathcal{E}\otimes\mathbb{1}_C)(\rho^{\mathrm{AC}})$, i.e. $\mathcal{E}$ acts only on the A subsystem. Applying a map $\mathcal{E}_1$ and then $\mathcal{E}_2$ is written as the combined map $\mathcal{E}_2 \circ \mathcal{E}_1$.
The diamond norm of $\mathcal{E}$ is defined as $\|\mathcal{E}\|_\diamond = \frac{1}{2}\sup_{\rho^{\mathrm{AC}}\in\mathcal{S}(\mathcal{H}_{\mathrm{AC}})} \|\mathcal{E}(\rho^{\mathrm{AC}})\|_1$ with $\mathcal{H}_\mathrm{C}$ an auxiliary system that can be considered to be of the same dimension as $\mathcal{H}_\mathrm{A}$. 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 $\frac{1}{2} + \frac{1}{4}\|\mathcal{E}-\mathcal{E}'\|_\diamond$. The security of a protocol is quantified by the diamond norm between the actual protocol $\mathcal{E}$ and a protocol with ideal functionality $\mathcal{F}$. When $\|\mathcal{E}-\mathcal{F}\|_\diamond \le \varepsilon$ we can consider $\mathcal{E}$ to behave ideally except with probability ε; this security metric is composable with other (sub-)protocols [20].
A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{T}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [23] 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 $h \in H$. We define the rate of a quantum communication protocol as the number of message bits communicated per sent qubit.

3.2 Post-selection

For protocols that are invariant under permutation of their inputs it has been shown [6] 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

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

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, which is negligible compared to n.

3.3 Noise symmetrisation with random Pauli operators

In [18] it was shown that for n-EPR states in factorised form, as obtained from e.g. Post-selection, a further simplification is possible. For each individual qubit j, Alice and Bob apply the Pauli operation σ_{α_j} to their respective half of the EPR pair, with $\alpha_j\in\{0,1,2,3\}$ random and public; then they forget α. The end result is that Eve's state (the purification of the Alice+Bob system) is simplified to the 4×4 diagonal matrix $\text{Diag}(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2})$. Only one parameter is left over, the bit error probability γ caused by Eve.

This symmetrisation trick is allowed when the *statistics* of the variables in the protocol is invariant under the Pauli operations.

4 Attacker model and security definition

<u>Attacker model</u>. We work in same setting as Gottesman [9], as discussed in Section 1.3. We distinguish between on the one hand long-term secrets (basis choices, encryption keys, authentication keys) and on the other hand short-term secrets. We consider two world views.

- **World1**. All secrets can be kept confidential indefinitely or destroyed.
- **World2**. Long-term keys are in danger of leaking at some point in time.

There are several motivations for entertaining the second world view. (a) It is difficult to permanently erase data from nonvolatile memory. (b) Whereas everyone understands the necessity of keeping message content confidential, it is not easy to guarantee that protocol implementations (and users) handle the keys with the same care as the messages.

QKR protocols are typically designed to be secure in world1. In this paper we provide some security guarantees that additionally hold in world2. One way of phrasing this is to say that we add 'user-proofness' to QKR.

Alice sends data to Bob in N chunks. We refer to the sending of one chunk as a 'round'. In each round Bob tells Alice if he noticed a disturbance ("`reject`") or not ("`accept`"). In case of `reject` they are *alarmed* and they know that they must take special care to protect the keys of this round indefinitely (i.e. a fallback to *World1* security). Crucially, *we assume that a key theft occurring before the end of round N is immediately noticed by Alice and/or Bob.* Without this assumption it would be impossible to do Key Recycling in a meaningful way. We allow all keys to become public after round N.

The rest of the attacker model consists of the standard assumptions: no information, other than specified above, leaks from the labs of Alice and Bob; there are no side-channel attacks; Eve has unlimited (quantum) resources; all noise on the quantum channel is considered to be caused by Eve.

Security definition. We aim for two security properties:[3]

1. *Key Recycling.* In case of `accept` the keys can be safely re-used without endangering messages. In case of `reject` the messages are safe provided that the keys are refreshed. We demand that the Key Recycling property holds in the first $N-1$ rounds.
2. *Unclonable Encryption.* We use Gottesman's definition [9]. In case of `accept`, the message remains secret even if all keys leak. In the `reject` case, the message is secure as long as the keys are kept secret. We demand that the Unclonable Encryption property holds in all rounds.

The different nature of the above two properties forces us to introduce two different notations for the CPTP map that is executed by Alice and Bob. On the one hand, we write $\mathcal{E}_{\rm KR}$ for one round of the protocol, where at the end of the round the old keys (from the beginning of the round) are traced away. On the other hand, we write $\mathcal{E}_{\rm uncl}$ for one round without such a tracing operation. The following condition implies that the above given security properties hold except with probability ε,

$$\forall_{j\in\{1,\ldots,N\}} \quad \left\| \mathcal{E}^{(j)}_{\rm uncl}\circ\mathcal{E}^{(j-1)}_{\rm KR}\circ\cdots\circ\mathcal{E}^{(1)}_{\rm KR} - \mathcal{F}^{(j)}_{\rm uncl}\circ\mathcal{F}^{(j-1)}_{\rm KR}\circ\cdots\circ\mathcal{F}^{(1)}_{\rm KR}\right\|_\diamond \leq \varepsilon, \tag{2}$$

where the superscript is the round index, and $\mathcal{F}$ stands for the idealized version of the protocol. We can arrive at a simplified statement using the following lemma.

Lemma 1 *For any CPTP maps $\mathcal{A},\mathcal{A}',\mathcal{B},\mathcal{B}'$, it holds that*

$$\|\mathcal{A}\circ\mathcal{B}-\mathcal{A}'\circ\mathcal{B}'\|_\diamond \quad\leq\quad \|\mathcal{A}-\mathcal{A}'\|_\diamond+\|\mathcal{B}-\mathcal{B}'\|_\diamond. \tag{3}$$

Proof:

$$\begin{aligned}
\|\mathcal{A}\circ\mathcal{B}-\mathcal{A}'\circ\mathcal{B}'\|_\diamond &= \|\mathcal{A}\circ\mathcal{B}-\mathcal{A}'\circ\mathcal{B}'+\mathcal{A}'\circ\mathcal{B}-\mathcal{A}'\circ\mathcal{B}\|_\diamond & (4)\\
&\leq \|(\mathcal{A}-\mathcal{A}')\circ\mathcal{B}\|_\diamond+\|\mathcal{A}'\circ(\mathcal{B}-\mathcal{B}')\|_\diamond & (5)\\
&\leq \|\mathcal{A}-\mathcal{A}'\|_\diamond+\|\mathcal{B}-\mathcal{B}'\|_\diamond & (6)
\end{aligned}$$

where the last inequality holds because a CPTP map can never increase the trace distance. □
Using Lemma 1 it is easily seen that the following condition implies (2),

$$(N-1)\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond+\|\mathcal{E}_{\rm uncl}-\mathcal{F}_{\rm uncl}\|_\diamond\leq\varepsilon. \tag{7}$$

It is therefore sufficient to upper bound the single-round quantities $\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond$ and $\|\mathcal{E}_{\rm uncl}-\mathcal{F}_{\rm uncl}\|_\diamond$. The ideal mapping $\mathcal{F}$ is obtained from $\mathcal{E}$ as follows. From $\mathcal{E}(\rho^{\rm ABE})$ one traces out those classical variables that are supposed to remain unknown to Eve, and takes a tensor product with an isolated mixed state of these variables. In the case of $\mathcal{E}_{\rm KR}$ the relevant variables are the message m and the next-round keys, which we denote here as $\tilde{k}$. In the case of $\mathcal{E}_{\rm uncl}$ it is only the message, and only the `accept` part of the mapping is relevant. (Upon `reject` the functionality of $\mathcal{E}_{\rm uncl}$ is ideal by definition.) Hence we have

$$\begin{aligned}
\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond &= \frac{1}{2}\sup_{\rho^{\rm ABE}}\left\|\mathcal{E}_{\rm KR}(\rho^{\rm ABE})-\mathop{\mathbb{E}}_{m\tilde{k}}|m\tilde{k}\rangle\langle m\tilde{k}|\otimes{\rm tr}_{M\tilde{K}}\,\mathcal{E}_{\rm KR}(\rho^{\rm ABE})\right\|_1 & (8)\\
\|\mathcal{E}_{\rm uncl}-\mathcal{F}_{\rm uncl}\|_\diamond &= \frac{1}{2}\sup_{\rho^{\rm ABE}}\left\|\mathcal{E}^{\tt accept}_{\rm uncl}(\rho^{\rm ABE})-\mathop{\mathbb{E}}_{m}|m\rangle\langle m|\otimes{\rm tr}_{M}\,\mathcal{E}^{\tt accept}_{\rm uncl}(\rho^{\rm ABE})\right\|_1. & (9)
\end{aligned}$$

[3]Note that each property implies that the encryption scheme has unconditional security, i.e. if Eve has access only to the ciphertext/cipherstate she learns nothing about the message.

5 Description of the 'Embedded' protocol variant

5.1 Pairwise independent hashing with easy inversion

We will need the privacy amplification step to be easily computable in two directions. Unfortunately the code-based construction due to Gottesman [9] does not work with the proof technique of [18], which requires a family of universal hash functions. We will be using a family of invertible functions $F : \{0,1\}^\nu \to \{0,1\}^\nu$ that has the collision properties of a pairwise independent hash function. An easy way to construct such a family is to use multiplication in $GF(2^\nu)$. Let $u \in GF(2^\nu)$ be randomly chosen. Define $F_u(x) = u \cdot x$, where the multiplication is in $GF(2^\nu)$. A pairwise independent family of hash functions Φ from $\{0,1\}^\nu$ to $\{0,1\}^\ell$, with $\ell \le \nu$, is implemented by taking the ℓ most significant bits of $F_u(x)$. We denote this as

$$\Phi_u(x) = F_u(x)[:\ell]. \tag{10}$$

The inverse operation is as follows. Given $c \in \{0,1\}^\ell$, generate random $r \in \{0,1\}^{\nu-\ell}$ and output $F_u^{\rm inv}(c\|r)$. It obviously holds that $\Phi_u(F_u^{\rm inv}(c\|r)) = c$. Computing an inverse in $GF(2^\nu)$ costs $O(\nu \log^2 \nu)$ operations [16].

5.2 Protocol steps of the 'Embedded' variant

Alice and Bob have agreed on a MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^{\ell-\lambda} \to \{0,1\}^\lambda$, the function families F and Φ as discussed in Section 5.1, with $\nu = k$, and a linear error correcting code which has encoding function $\mathrm{Enc} : \{0,1\}^k \to \{0,1\}^n$ in systematic form and decoding $\mathrm{Dec} : \{0,1\}^n \to \{0,1\}^k$.
In round j, Alice wants to send a message $\mu_j \in \{0,1\}^{\ell-(n-k)-2\lambda-1}$. We will often drop the index j for notational brevity.
The key material shared between Alice and Bob consists of a mask $z \in \{0,1\}^\ell$, a MAC key $k_{\rm MAC} \in \{0,1\}^\lambda$, a basis sequence $b \in \mathcal{B}^n$, a MAC key $k_{\rm fb} \in \{0,1\}^\lambda$ for the feedback bit, a one-time pad $k_{\rm OTP} \in \{0,1\}$ for the feedback bit, a key $u \in \{0,1\}^k$ for universal hashing and a key $e \in \{0,1\}^{n-k}$ to mask the redundancy bits. They have a reservoir of spare key material ($k_{\rm rej}$) from which to refresh their keys in case of `reject`.
In each round Alice and Bob perform the following steps (see Fig. 1):
Encryption:
Alice generates random strings $\kappa \in \{0,1\}^{\lambda+1+n-k}$ and $r \in \{0,1\}^{k-\ell}$. She computes the authentication tag $\tau = \Gamma(k_{\rm MAC}, \mu\|\kappa)$, the augmented message $m = \mu\|\kappa\|\tau$, the ciphertext $c = z \oplus m$, the reversed privacy amplification $p = F_u^{\rm inv}(c\|r) \in \{0,1\}^k$ and the qubit payload $x = \mathrm{Enc}(p) \oplus (\vec{0}^k\|e) \in \{0,1\}^n$. 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 decodes $\hat{p} = \mathrm{Dec}(x' \oplus (\vec{0}_k\|e))$. He computes $\hat{c} = \Phi_u(\hat{p})$ and $\hat{\mu}\|\hat{\kappa}\|\hat{\tau} = \hat{c} \oplus z$. He sets $\omega = 1$ (`accept`) if $\Gamma(k_{\rm MAC}, \hat{\mu}\|\hat{\kappa}) == \hat{\tau}$, otherwise $\omega = 0$ (`reject`). He computes $\tau_{\rm fb} = \Gamma(k_{\rm fb}, \omega \oplus k_{\rm OTP})$ and sends $\omega \oplus k_{\rm OTP}$ and $\tau_{\rm fb}$ to Alice.
Key Update:
Alice and Bob perform the following actions (a tilde denotes the key for the next round):
In case of `accept`: Re-use $b, u, k_{\rm MAC}, z$. Set next round keys: $(\tilde{k}_{\rm fb}, \tilde{k}_{\rm OTP}, \tilde{e}) = \kappa$.
In case of `reject`: Re-use $b, u, k_{\rm MAC}$. Take fresh $\tilde{z}$, $\tilde{k}_{\rm fb}$, $\tilde{k}_{\rm OTP}$, $\tilde{e}$ from $k_{\rm rej}$.

After round N, according to the attacker model, all keys from all rounds leak[4] except for masks z associated with `reject` events. I.e. what leaks is: $b, u, k_{\rm MAC}$, $\{k_{\rm fb}^{(j)}, k_{\rm OTP}^{(j)}, e^{(j)}\}_{j=1}^N$, and if round N was `accept` also $z^{(N)}$.

[4]Optionally this leakage can be made part of the protocol, i.e. Alice and Bob publish the keys.

Remarks:

- The augmented message m contains the three keys $\tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}$ for the next round. This means that qubits are 'spent' in order to send something other than μ, which reduces the communication rate. Here the mask $e \in \{0,1\}^{n-k}$ for the redundancy bits is the dominant part; its size is asymptotically $nh(\beta)$ bits, giving rise to a rate penalty term $h(\beta)$ familiar from QKD.
- The `accept`/`reject` feedback bit is encrypted, which temporarily prevents Eve from gaining information from 'oracle' access to the feedback. This allows us to re-use b in unmodified form after `accept`.
- Even in the case of known plaintext, from Eve's point of view the 'payload' $x \in \{0,1\}^n$ in the state $\bigotimes_{i=1}^{n} |\psi_{x_i}^{b_i}\rangle$ is uniformly distributed. The z masks ℓ bits; then appending r increases that to k bits; finally the e masks the $n-k$ redundancy bits.

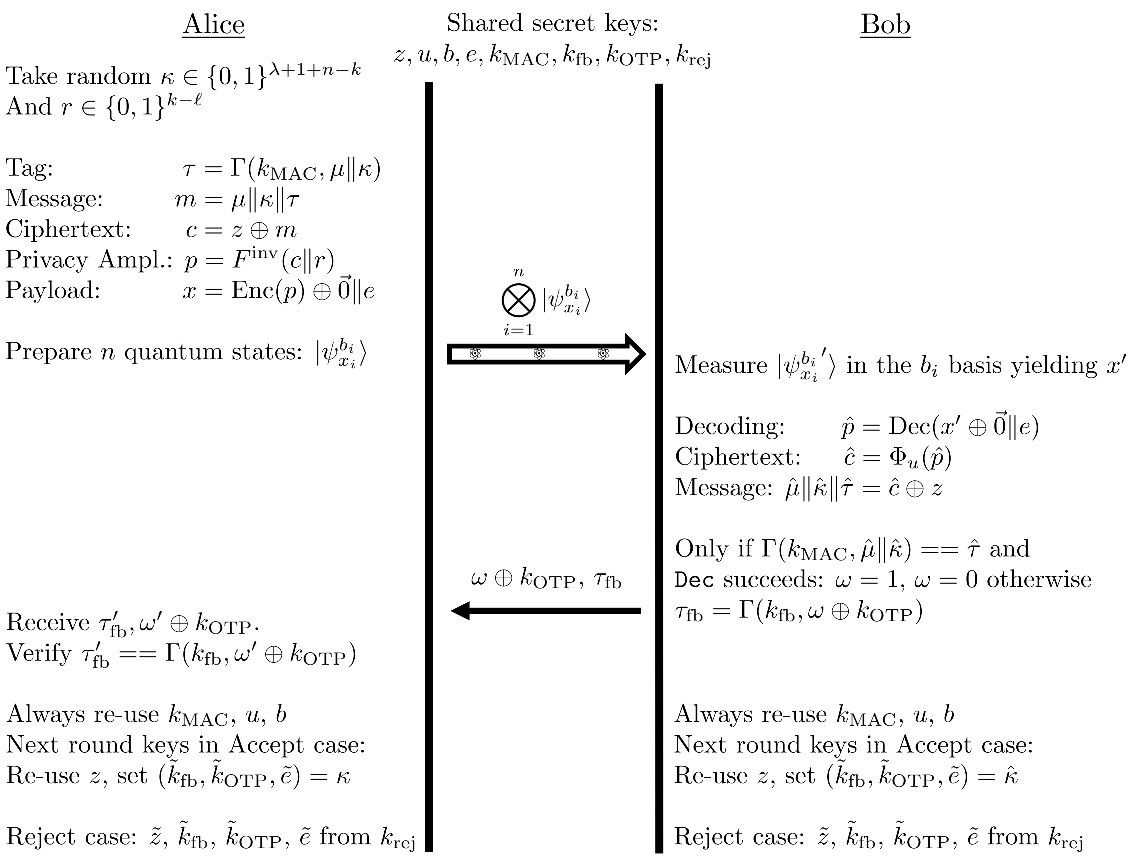

Figure 1: *Protocol steps of the 'Embedded' variant.*

5.3 EPR version of the 'Embedded' protocol

We will base the security proof on the EPR version of the protocol, making use of Post-selection (Section 3.2) and the random-Pauli noise symmetrisation technique (Section 3.3).
n noisy singlet states are produced by an untrusted source, e.g. Eve. One half of each EPR pair is sent to Alice, the other half to Bob. Alice and Bob apply the random Pauli operations as described in Section 3.3. Then Alice measures her qubits in the bases $b \in \mathcal{B}^n$ resulting in a string $s \in \{0,1\}^n$. Bob too measures his qubits in basis b, which yields $t \in \{0,1\}^n$. Alice computes x as specified in Section 5.2, then computes $a = x \oplus s$ and sends a to Bob over an authenticated classical channel. Bob receives a, computes $x' = \bar{t} \oplus a$ and performs the decryption steps specified in Section 5.2.

We are allowed to use Post-selection because our protocol is invariant under permutation of the EPR pairs. A permutation re-arranges the noise in the observed strings s and t over the bit positions $\{1, \ldots, n\}$; however, the error correction step is insensitive to such a change.
The use of the noise symmetrisation technique is allowed because the statistics is invariant under the Pauli operations. In the case of BB84 encoding and 6-state encoding, the Paulis cause bit flips in the string $x \in \{0,1\}^n$ in positions known to Alice and Bob, which does not change the protocol in any essential way.[5]
Security of the EPR version implies security of the prepare-and-measure protocol of Section 5.2.

6 Security proof for the EPR 'Embedded' protocol

6.1 CPTP maps

We now specify the exact form of the CPTP map which represents one round. We start with $\mathcal{E}_{\text{uncl}}$ and write $\mathcal{E}_{\text{KR}} = \mathcal{T}_{\text{KR}} \circ \mathcal{E}_{\text{uncl}}$, where $\mathcal{T}_{\text{KR}}$ is a partial trace operation. The $\mathcal{E}_{\text{uncl}}$ can be viewed as four consecutive maps: an initialization step $\mathcal{I}$ where the input variables are prepared; a measurement step $\mathcal{M}$; a post-processing step $\mathcal{P}$ representing all further computations; a partial trace step $\mathcal{T}_{\text{uncl}}$ where all variables that are not part of the output or the transcript are traced away,

$$\mathcal{E}_{\text{uncl}} = \mathcal{T}_{\text{uncl}} \circ \mathcal{P} \circ \mathcal{M} \circ \mathcal{I}. \tag{11}$$

The initialization merely appends the input variables,

$$\mathcal{I}(\rho^{\text{ABE}}) = \mathop{\mathbb{E}}_{mbzue} |mbzue\rangle\langle mbzue| \otimes \rho^{\text{ABE}}. \tag{12}$$

Here b, z, u, e are uniform, but m not necessarily. The measurement acts on the b-space and ρ^{ABE}, outputting the strings s, t and Eve's state ρ^{E}_{bst}, which is correlated to the measurement basis b and the outcomes s, t,

$$\mathcal{M}(|b\rangle\langle b| \otimes \rho^{\text{ABE}}) = \mathop{\mathbb{E}}_{st} |bst\rangle\langle bst| \otimes \rho^{\text{E}}_{bst}. \tag{13}$$

Here the distribution of s and t is governed by the i.i.d. noise with noise parameter γ. The marginals of s and t are uniform, while for all $j \in \{1, \ldots, n\}$ it holds that $\Pr[s_j = t_j] = \gamma$. In the post-processing the flag ω is computed as a function of s and t which we will denote as θ_{st}. Let $n\beta$ be the number of errors that can be corrected by the error-correcting code. Then

$$\theta_{st} = \begin{cases} 1 \text{ if } |\bar{s} \oplus t| \le n\beta \\ 0 \text{ if } |\bar{s} \oplus t| > n\beta \end{cases}. \tag{14}$$

We will use the notation $P_{\text{corr}}(n, \beta, \gamma)$ for the probability of the event $\theta_{st} = 1$.

$$P_{\text{corr}}(n, \beta, \gamma) \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{st} \theta_{st} = \sum_{c=0}^{\lfloor n\beta \rfloor} \binom{n}{c} \gamma^c (1-\gamma)^{n-c}. \tag{15}$$

[5] In 8-state encoding [22], applying a Pauli changes the basis b in a way known to Alice and Bob. Again, this does not affect the security.

The result of applying $\mathcal{I}, \mathcal{M}, \mathcal{P}$ is given by

$$(\mathcal{P}\circ\mathcal{M}\circ\mathcal{I})(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbzuest} |mbzuest\rangle\langle mbzuest| \otimes \rho^{\rm E}_{bst} \otimes \sum_{capxx'\omega\tilde{z}} \mathop{\mathbb{E}}_{r} |capxx'\omega\tilde{z}r\rangle\langle capxx'\omega\tilde{z}r|$$

$$\delta_{a,s\oplus x}\delta_{c,m\oplus z}\delta_{p,F_u^{\rm inv}(c\|r)}\delta_{x,p\|[{\rm Red}(p)\oplus e]}\delta_{x',\bar{t}\oplus a}\delta_{\omega,\theta_{st}}\big[\omega\delta_{\tilde{z}z}+\frac{\overline{\omega}}{2^\ell}\big]. \tag{16}$$

Here r is uniform and 'Red(p)' stands for the redundancy bits appended to p in the systematic-form ECC encoding Enc(p).
In the final step $\mathcal{T}_{\rm uncl}$ we trace away all variables that are not part of the transcript or the output: s, t, c, p, x, x', r. These variables exist only temporarily and can be quickly discarded by Alice and Bob; they are never stored in nonvolatile memory. The a and ω are observed by Eve as part of the communication. (The ω in encrypted form, but the key is assumed to leak in the future.) The b, z, u, e are assumed to leak in the future and thus they have to be kept as part of the state. We obtain[6]

$$\mathcal{E}_{\rm uncl}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}\omega} |mbzuea\tilde{z}\omega\rangle\langle mbzuea\tilde{z}\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst} \sum_p 2^\ell \delta_{\Phi_u(p),m\oplus z}$$

$$2^{-k}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}\delta_{\omega,\theta_{st}}\Big[\omega\delta_{\tilde{z}z}+\overline{\omega}2^{-\ell}\Big]. \tag{17}$$

As discussed in Section 4, only the $\texttt{accept}$ part (the $\omega = 1$ part) of the idealized $\mathcal{F}_{\rm uncl}$ is relevant. This is obtained as $\mathcal{F}^{\texttt{accept}}_{\rm uncl}(\rho^{\rm ABE}) = \mathbb{E}_m |m\rangle\langle m| \otimes {\rm tr}_M \mathcal{E}^{\rm accept}_{\rm uncl}(\rho^{\rm ABE})$. We get

$$\mathcal{F}^{\texttt{accept}}_{\rm uncl}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}} |mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z} \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst}\theta_{st} \sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]} \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(p),m'\oplus z}. \tag{18}$$

Note that this expression is sub-normalized; its trace equals $P_{\rm corr}$. We write

$$(\mathcal{E}^{\rm accept}_{\rm uncl} - \mathcal{F}^{\rm accept}_{\rm uncl})(\rho^{\rm ABE}) = \tag{19}$$

$$\mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}} |mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z} \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst}\theta_{st} \sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}[\delta_{\Phi_u(p),m\oplus z} - \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(p),m'\oplus z}].$$

For the description of $\mathcal{E}_{\rm KR}$ we have to take (17) and trace out z, e, ω.

$$\mathcal{E}_{\rm KR}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst} \Big[\theta_{st}\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde{z}} + 2^{-\ell}\overline{\theta_{st}}\Big]. \tag{20}$$

The ideal functionality $\mathcal{F}_{\rm KR}$ has $m, b, u, \tilde{z}$ decoupled from the rest of the system. We have $\mathcal{F}_{\rm KR}(\rho^{\rm ABE}) = \mathbb{E}_{mbu} 2^{-\ell} \sum_{\tilde{z}} |mbu\tilde{z}\rangle\langle mbu\tilde{z}| \otimes {\rm tr}_{MBU\tilde{Z}} \mathcal{E}_{\rm KR}(\rho^{\rm ABE})$, which yields

$$\mathcal{F}_{\rm KR}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathop{\mathbb{E}}_{st}\mathop{\mathbb{E}}_{b'} \rho^{\rm E}_{b'st}. \tag{21}$$

Note that $\mathbb{E}_{st}\,\mathbb{E}_{b'}\,\rho^{\rm E}_{b'st} = \rho^{\rm E}$.

Lemma 2 *Let $\rho^{\rm ABE}$ denote the purification of a 4^n-dimensional state $\rho^{\rm AB}$. Let $b \in \mathcal{B}^n$ be a qubit-wise orthonormal basis. It holds that $\rho^{\rm E}_b = \rho^{\rm E}$.*

Proof: Let $P^{\rm A}_{bs}$ denote a projection operator on subsystem 'A' corresponding to a measurement in basis b with outcome $s \in \{0,1\}^n$. We have $\rho^{\rm E}_b \stackrel{\rm def}{=} \mathbb{E}_{st}\,\rho^{\rm E}_{bst} = \sum_{st} {\rm tr}_{\rm AB}(P^{\rm A}_{bs} \otimes P^{\rm B}_{bt} \otimes \mathbb{1})\rho^{\rm ABE}$ $= {\rm tr}_{\rm AB}([\sum_s P^{\rm A}_{bs}] \otimes [\sum_t P^{\rm B}_{bt}] \otimes \mathbb{1})\rho^{\rm ABE} = \rho^{\rm E}$. We use the fact that $\sum_s P^{\rm A}_{bs} = \mathbb{1}$ and $\sum_t P^{\rm B}_{bt} = \mathbb{1}$ for any b. □

Lemma 2 allows us to write

$$(\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR})(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst}\theta_{st}[2^\ell\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde{z}} - 1]. \tag{22}$$

[6]Note that tracing out u or $z\tilde{z}$ in (17) yields a state in which the m-subspace is completely decoupled from the rest of the Hilbert space. This shows that the scheme, when merely viewed as an encryption scheme, protects m unconditionally as soon as the adversary does not know u or $z\tilde{z}$.

6.2 Intermezzo: QKD asymptotics

In Appendix A, we consider a version of QKD where privacy amplification is implemented as in Section 5.2, and the syndrome is sent to Bob in OTP'ed form; we show that this leads to a bound of the form

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond \leq \tfrac{1}{2}\mathop{\mathbb{E}}_{mbu}\frac{1}{2^{n+\ell}}\sum_{ac}\left\|\mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\theta_{st}2^\ell[\delta_{c,m\oplus\Phi_u(a\oplus s)}-\mathop{\mathbb{E}}_{m'}\delta_{c,m'\oplus\Phi_u(a\oplus s)}]\right\|_1, \tag{23}$$

which after some algebra gives rise to

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond \leq \min\Big(P_{\rm corr}, \frac{1}{2}\mathop{\mathbb{E}}_b{\rm tr}\sqrt{2^\ell\mathop{\mathbb{E}}_{ss'}\delta_{ss'}\rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}}\Big), \tag{24}$$

and that from (24) the well known asymptotic QKD rates can be obtained: $1-2h(\beta)$ for BB84 and $1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})$ for 6-state QKD. If the syndrome (denoted as $\sigma=\texttt{Syn}\,x$) is sent in the clear, the right hand side of (23) acquires an extra $\sum_\sigma$ outside the trace norm and a factor $\delta_{\sigma,\texttt{Syn}(s\oplus a)}$ inside the trace norm; the effect on (24) is an extra factor 2^{n-k} under the square root; while this alteration reduces the threshold value $\ell_{\rm max}$ by an amount $n-k$, it has no effect on the rate since OTP'ing the syndrome would incur a penalty of exactly the same size.

6.3 Achievable rate of the Embedded variant

In the analysis we do not explicitly write down contributions from the authentication failure probability. It is implicitly understood that each MAC adds a term $2^{-\lambda}$ to the overall security parameter.

Theorem 1 *The Embedded protocol variant satisfies the Key Recycling and Unclonable Encryption properties as defined in Section 4 while achieving the following asymptotic rate,*

$$r^{\rm embedded}_{\rm 4state}=1-3h(\beta)\quad;\quad r^{\rm embedded}_{\rm 6state}=1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})-h(\beta). \tag{25}$$

In other words, the achievable rate is worse than the QKD rate by a term $h(\beta)$.

Proof of Theorem 1: Because of the inclusion of $n-k+\lambda+1$ extra bits in the augmented message m, the asymptotic rate of the protocol is $r^{\rm embedded}=\ell_{\rm max}/n-h(\beta)$. We need to determine the value of $\ell_{\rm max}$ for both the 'uncl' and 'KR' property separately and take the smaller of the two.

Part 1. First we note that (19) is the difference of two sub-normalised states that both have trace equal to $P_{\rm corr}$. This immediately yields the bound $\|\mathcal{E}_{\rm uncl}-\mathcal{F}_{\rm uncl}\|_\diamond\leq P_{\rm corr}$. Furthermore, from (19) we get

$$\|\mathcal{E}_{\rm uncl}-\mathcal{F}_{\rm uncl}\|_\diamond = \mathop{\mathbb{E}}_{mbzue}\tfrac{1}{2^n}\sum_a\left\|\mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\theta_{st}\sum_p 2^{\ell+n-k}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}[\delta_{\Phi_u(p),m\oplus z}-\mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(p),m'\oplus z}]\right\|_1 \tag{26}$$

which resembles (23). The main difference is the $2^{n-k}\sum_p\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}$. In the derivation as shown in Appendix A, upon doubling as in (38) applying the $\mathbb{E}_u$ then yields instead of $\delta_{ss'}$ the following expression,

$$(2^{n-k})^2\sum_{pp'}\delta_{pp'}\delta_{s\oplus a,p||(e\oplus{\rm Red}p)}\delta_{s'\oplus a,p'||(e\oplus{\rm Red}p')}=(2^{n-k})^2\delta_{ss'}\delta_{e,(s\oplus a)[k+1:n]\oplus{\rm Red}((s\oplus a)[:k])}. \tag{27}$$

The factor $(2^{n-k})^2\delta_{e,\ldots}$, together with the $\mathbb{E}_e$ outside the trace norm, together have the same effect as having the plaintext syndrome in the QKD derivation: a factor 2^{n-k} under the square root in (24). Asymptotically this yields $\ell^{\rm uncl,4state}_{\rm max}=n-2nh(\beta)$ and $\ell^{\rm uncl,6state}_{\rm max}=n-nh(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})$.

Part 2. First we note that (22) is the difference of two sub-normalised states that both have trace equal to $P_{\rm corr}$. This immediately yields the bound $\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond\leq P_{\rm corr}$. Furthermore, from (22) we find

$$\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond=\tfrac{1}{2}\mathop{\mathbb{E}}_{mbu}\frac{1}{2^{n+\ell}}\sum_{a\tilde z}\left\|\mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\theta_{st}[2^\ell\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde z}-1]\right\|_1. \tag{28}$$

This expression very closely resembles (23), with $\tilde{z}$ precisely playing the role of c, and the term $\mathbb{E}_{m'}\, \delta_{c,m'\oplus\Phi_u(a\oplus s)}$ replaced by the constant '1'. Carrying the '1' through steps (38) and further in Appendix A yields the same result as the QKD derivation, except for one important difference: the $(s+a)[:k]$ restriction to the first k bits yields a modification of $\delta_{ss'}$ to the first k bits only. In the end result the parameter n is entirely replaced by k. Hence we obtain asymptotically $\ell^{\rm KR,4state}_{\rm max} = k - kh(\beta) = n(1-h(\beta))^2$ and $\ell^{\rm KR,6state}_{\rm max} = k + kh(\beta) - kh(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$
$= n[1-h(\beta)][1+h(\beta) - h(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})]$.
It is easily seen that $\ell^{\rm uncl}_{\rm max} \leq \ell^{\rm KR}_{\rm max}$. For brevity we use shorthand notation $h = h(\beta)$ and $H = h(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$, noting that $H > h$ and $H < 2h$. For BB84 encoding we see $\ell^{\rm KR}_{\rm max}/\ell^{\rm uncl}_{\rm max} = \frac{(1-h)^2}{1-2h} \geq 1$. For 6-state we see $\ell^{\rm KR}_{\rm max}/\ell^{\rm uncl}_{\rm max} = \frac{(1-h)(1+h-H)}{1-H} = \frac{1-H+h(H-h)}{1-H} \geq 1$. $\square$

7 The 'Interactive' protocol

7.1 Protocol steps of the 'Interactive' variant

If we don't restrict ourselves to a single communication from Alice to Bob, and allow Alice to send classical data as well, we can handle the syndrome more efficiently than in the *Embedded* variant. Alice sends the syndrome in plaintext, but only after getting from Bob a confirmation that he has received the qubits.

The protocol steps are written out in Appendix B. A single round is depicted in Fig. 2.

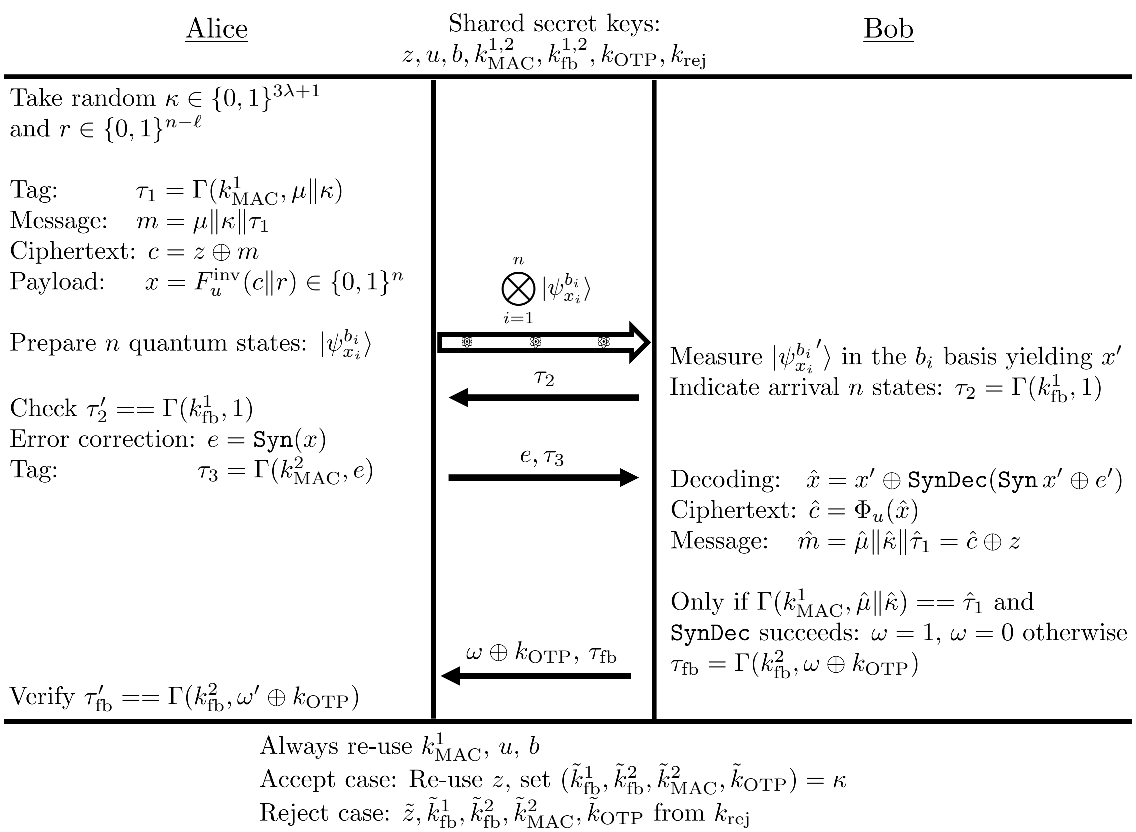

Figure 2: *Protocol steps of the 'Interactive' variant.*

Remark:

- In the case of a noiseless quantum channel, there is no need to send the syndrome, and the two protocol variants become identical. Furthermore, the diamond norm reduces exactly to the expression for QKD.
- Alice has to wait for the feedback τ_2, otherwise Eve's attack on the quantum state would depend on $\mathtt{Syn}\, x$, something that the proof technique cannot handle.

7.2 Achievable rate of the 'Interactive' variant

Theorem 2 *The* Interactive *protocol variant satisfies the Key Recycling and Unclonable Encryption properties as defined in Section 4 while achieving the same asymptotic rate as QKD-with-one-way-postprocessing.*

Proof: We work with the EPR version, i.e. there are additional variables $s,t,a\in\{0,1\}^n$ just as in Section 5.3. We write $\mathcal{G},\mathcal{J}$ instead of $\mathcal{E},\mathcal{F}$ to distinguish from the *Embedded* case. Using the same methods as in Section 6.1 (maps for initialisation, measurement, postprocessing and tracing) we first derive the map $\mathcal{G}_{\rm uncl}$ that corresponds to one round of the protocol. We have[7]

$$\begin{aligned}\mathcal{G}_{\rm uncl}(\rho^{\rm ABE}) &= \mathop{\mathbb{E}}_{mbzu} \frac{1}{2^n}\sum_{ea\omega\tilde z} |mbzuea\tilde z\omega\rangle\langle mbzuea\tilde z\omega| \otimes \\ &\quad \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst}\delta_{\omega,\theta_{st}} 2^\ell \delta_{\Phi_u(s\oplus a),m\oplus z}\delta_{e,\mathtt{Syn}(a\oplus s)}[\omega\delta_{\tilde z z}+\overline{\omega}2^{-\ell}] \qquad (29)\end{aligned}$$

from which we obtain

$$\begin{aligned}\mathcal{G}^{\tt accept}_{\rm uncl}(\rho^{\rm ABE})-\mathcal{J}^{\tt accept}_{\rm uncl}(\rho^{\rm ABE}) &= \mathop{\mathbb{E}}_{mbzu}\frac{1}{2^n}\frac{1}{2^{n-k}}\sum_{ea}|mbzuea,\tilde z{=}z,\omega{=}1\rangle\langle mbzuea,\tilde z{=}z,\omega{=}1| \\ &\otimes \mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\theta_{st}2^{n-k}\delta_{e,\mathtt{Syn}(a\oplus s)}2^\ell[\delta_{\Phi_u(s\oplus a),m\oplus z}-\mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(s\oplus a),m'\oplus z}]. \qquad (30)\end{aligned}$$

Again we have the difference of two sub-normalised terms and conclude $\|\mathcal{G}_{\rm uncl}-\mathcal{J}_{\rm uncl}\|_\diamond\leq P_{\rm corr}$. Next we note that (30) is practically identical to the QKD expression (36) with an extra constraint $\delta_{e,\mathtt{Syn}(a\oplus s)}$ thrown in. The effect of this constraint is exactly as in the derivation for QKD with syndrome-in-the-clear. We get asymptotically $\ell^{\rm uncl}_{\rm max}=nr^{\rm QKD}$.
The $\mathcal{G}_{\rm KR}$ is obtained by tracing out z,ω from (29), which yields

$$\mathcal{G}_{\rm KR}(\rho^{\rm ABE})=\mathop{\mathbb{E}}_{mbu}\frac{1}{2^n}\sum_{ea\tilde z}|mbuea\tilde z\rangle\langle mbuea\tilde z|\otimes\mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\delta_{e,\mathtt{Syn}(a\oplus s)}[\theta_{st}2^\ell\delta_{\Phi_u(s\oplus a),m\oplus\tilde z}+\overline{\theta_{st}}]. \qquad (31)$$

The ideal functionality $\mathcal{J}_{\rm KR}$ has $m,b,u,\tilde z$ decoupled from the rest of the system. Following the recipe for obtaining $\mathcal{J}$ from $\mathcal{G}$ as in Section 6.1 we get

$$(\mathcal{G}_{\rm KR}-\mathcal{J}_{\rm KR})(\rho^{\rm ABE})=\mathop{\mathbb{E}}_{mbu}\frac{1}{2^{n+\ell}}\sum_{ea\tilde z}|mbuea\tilde z\rangle\langle mbuea\tilde z|\otimes\mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\theta_{st}\delta_{e,\mathtt{Syn}(a\oplus s)}[2^\ell\delta_{\Phi_u(s\oplus a),m\oplus\tilde z}-1]. \qquad (32)$$

Again we have the difference of two norm-$P_{\rm corr}$ terms and conclude $\|\mathcal{G}_{\rm KR}-\mathcal{J}_{\rm KR}\|_\diamond\leq P_{\rm corr}$. Furthermore (32) gives

$$\|\mathcal{G}_{\rm KR}-\mathcal{J}_{\rm KR}\|_\diamond=\mathop{\mathbb{E}}_{mbu}\frac{1}{2^{n+\ell}}\sum_{ea\tilde z}\Big\|\mathop{\mathbb{E}}_{st}\rho^{\rm E}_{bst}\theta_{st}\delta_{e,\mathtt{Syn}(a\oplus s)}[2^\ell\delta_{\Phi_u(s\oplus a),m\oplus\tilde z}-1]\Big\|_1. \qquad (33)$$

This is almost identical to the corresponding expression for QKD with syndrome-in-the-clear, except for the constant '1' which does not affect the final result. □

[7] As for the *Embedded* case, tracing out u or $z\tilde z$ from (29) completely decouples m from the rest of the state; this demonstrates that the *Interactive* variant too, when viewed merely as an encryption, unconditionally protects m as soon as u or $z\tilde z$ is hidden from Eve.

8 Communication rate and complexity

We briefly comment on the communication complexity (round complexity) and the asymptotic rate of our protocols as compared to other schemes. The word 'round complexity' here is not to be confused with the N rounds in our protocol. We count *the number of times Alice has to send something* per message μ and refer to this number as Alice's number of passes. The rate is defined as $|\mu|/n$, the size of the message divided by the number of qubits. We compare against the following methods for sending a message with information-theoretic security without using up[8] key material,

- **QKD+OTP**. Key establishment using Quantum Key Distribution, combined with One Time Pad classical encryption. We consider efficient QKD with negligible waste of qubits [15] and the smallest possible number of communication rounds: only 2 passes by Alice.
- **QKR**. Qubit-wise prepare-and-measure Quantum Key Recycling as described in [13,14]. Only a single pass by Alice is needed, since Alice and Bob already share key material.
- **QKD+Uncl.** Key establishment using Quantum Key Distribution, followed by Gottesman's Unclonable Encryption [9]. At least two passes by Alice are needed.

Protocol	Alice #passes	Asymptotic rate (4-state)	Unclonability
QKD + OTP	2	$1-2h(\beta)$	no
QKR	1	$1-2h(\beta)$	no
QKD + Uncl.	2	$\frac{1}{2}\cdot\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
Embedded	1	$1-3h(\beta)$	yes
Interactive	2	$1-2h(\beta)$	yes

Table 1: *Comparison of schemes.*

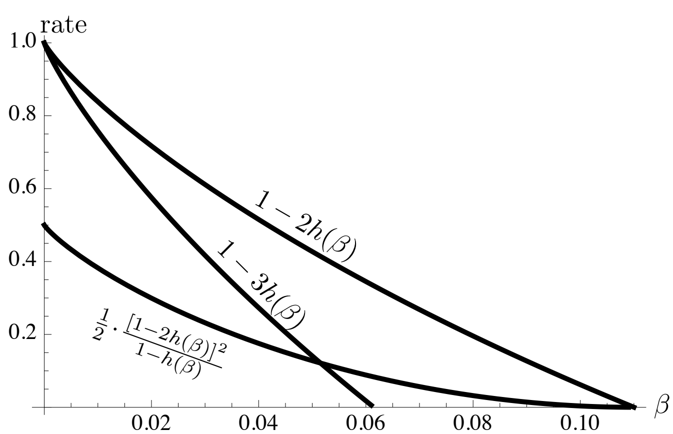

Figure 3: *Asymptotic communication rates (4-state) as a function of the noise parameter β.*

The scheme properties are summarised in Table 1, and the rates[9] are plotted in Fig. 3. (We only show 4-state encoding. The comparison holds qualitatively for 6-state encoding as well, but with slightly higher rates.) QKR is an improvement over QKD in terms of round complexity, while achieving the same rate. However, QKD and QKR do not have the Unclonable Encryption property. The only known UE option until now was 'QKD+Uncl'. Our *Interactive* scheme has

[8]Our schemes use up key material, but this is amortised over N rounds. We neglect this expenditure for the purpose of the comparison.

[9]The rate for QKD+Uncl is obtained as follows. The UE step needs $n_{\rm UE} = |\mu|/[1-2h(\beta)]$ qubits. Then $n_{\rm UE}$ bits of key need to be refreshed using QKD; this takes $n_{\rm QKD} = n_{\rm UE}/[1-2h(\beta)]$ qubits. The rate is $|\mu|/(n_{\rm UE}+n_{\rm QKD})$.

the same round complexity as QKD+Uncl but a significantly higher rate. Our *Embedded* scheme has a better round complexity than QKD+Uncl; furthermore it has a better rate at noise levels below $\beta \approx 0.052$.
We also briefly comment on the key sizes. The key material used in the *Embedded* variant consists of the OTP $z \in \{0,1\}^\ell$, the hash seed $u \in \{0,1\}^k$, the basis choice $B \in \mathcal{B}^n$, the redundancy mask $e \in \{0,1\}^{n-k}$, the authentication keys $k_{\rm MAC} \in \{0,1\}^\lambda$, $k_{\rm fb} \in \{0,1\}^\lambda$ and the OTP $k_{\rm OTP} \in \{0,1\}$. Counting only contributions proportional to n, the total size in bits is $\ell + n + n \log \mathcal{B} + \mathcal{O}(1)$. With $\ell \approx |\mu| + nh(\beta)$ and $n \approx |\mu|/[1-3h(\beta)]$ we can write the total size as $|\mu| \frac{2+\log|\mathcal{B}|-2h(\beta)}{1-3h(\beta)} + \mathcal{O}(1)$.
In the *Interactive* variant, the large keys are $z \in \{0,1\}^\ell$, $u \in \{0,1\}^n$ and $b \in \mathcal{B}^n$. With $\ell \approx |\mu|$ and $n \approx |\mu|/[1-2h(\beta)]$ we can express the total key size as $|\mu| \frac{2+\log|\mathcal{B}|-2h(\beta)}{1-2h(\beta)} + \mathcal{O}(1)$.
The keys are expended over a block of N rounds (or $\leq N$ in case of `reject`). If there are no `reject`s, the 'amortised' key expenditure per round equals the above key size divided by N, which can be made much smaller than $|\mu|$.
Gottesman's scheme has somewhat shorter keys, total length $|\mu| \frac{2-h(\beta)}{1-2h(\beta)} + \mathcal{O}(1)$, but it needs to refresh $\approx |\mu|/[1-2h(\beta)]$ bits every round.

9 Discussion

We have shown that quantum encryption can have Unclonability as well as Key Recycling. Essentially, this is achieved by starting from QKR and making the privacy amplification a step in computing the qubit payload. Gottesman's construction [9] does something very similar, and hence one may try to construct a variant of the *Embedded* and *Interactive* protocols that is closer to [9]. This would have the advantage that there is no longer a seed u that needs to be stored as part of the keys, as [9] employs ECC-based privacy amplification. However, the proof technique that we use, with its reliance on hash families, does not work for ECC-based privacy amplification.

We suspect that the rate decrease from $1-2h(\beta)$ to $1-3h(\beta)$ which occurs when we 'embed' everything in the quantum state is unavoidable. While the *Interactive* variant does not need to protect the syndrome/redundancy, the *Embedded* variant *does*, but at the same time *cannot* because the keys get revealed. The price paid is to reserve space $nh(\beta)$ in the message to refresh the redundancy encryption key.
Our protocols (temporarily) hide the `accept/reject` feedback bit ω. This is a technicality that allows us to re-use b in un-altered form. The alternative would be to send ω in the clear and then either (i) partially refresh b as in [14], or (ii) find a way to cope with a reduced entropy of b as in [11]. Note that it is not realistic to hide a *large* accumulation of ω-feedbacks from Eve. Alice and Bob would have to act for a long time in a way that, to an external observer, does not depend on the ωs. However, Eve may be able to observe e.g. how often Alice and Bob have to engage in QKD to refill their key 'reservoir', which reveals the total number of `reject`s. For a *small* accumulation (e.g. size N) we expect that it *is* realistic to hide the feedbacks temporarily.
The downside associated with encoding a message directly into qubits is the vulnerability to erasures (particle loss) on the quantum channel. While QKD can just ignore erasures, in QKR they have to be compensated by the error-correcting code, which incurs a serious rate penalty.

Acknowledgements

Part of this research was funded by NWO (CHIST-ERA project 651.002.003, ID_IOT).

A QKD asymptotics

We consider a QKD version that looks as much as possible like our protocol, and apply Renner's proof technique to quickly derive bounds on the diamond norm. For brevity we ignore message authentication tags and their failure probability, since they do not affect the asymptotics. We do not consider two-way postprocessing tricks like advantage distillation. We refer to the resulting rates in this Appendix as the asymptotic rate of QKD-with-one-way-postprocessing.

QKD Protocol.

Eve sends EPR pairs, in the singlet state. Alice and Bob randomly choose measurement bases from the set $\mathcal{B}$, perform their measurements, and then publicly announce their basis choices. They disregard all events where they chose different bases, and are left with n bits. Alice has measurement outcome $s \in \{0,1\}^n$, Bob has $t \in \{0,1\}^n$. Alice generates random $x \in \{0,1\}^n$, $u \in \{0,1\}^n$. She computes a mask $a = s \oplus x$ and OTP $z = \Phi_u(x)$. She sends a to Bob over an authenticated channel. She also sends the syndrome $\sigma = \mathtt{Syn}(x) \in \{0,1\}^{n-k}$, either in the clear or OTP'ed. (We will analyze both options.)

Bob computes $x' = t \oplus \bar{a}$ and tries to reconstruct x from x' and σ. If he finds a $\hat{x}$ satisfying $|\hat{x} \oplus x'| \leq n\beta$ he sets $\omega = 1$, otherwise $\omega = 0$. He sends ω to Alice.

In case $\omega = 0$ Alice sets $c = \perp$. In case $\omega = 1$ she sets $c = m \oplus z$. Alice sends c, u. If $\omega = 1$ Bob reconstructs $\hat{z} = \Phi_u(\hat{x})$ and $\hat{m} = c \oplus \hat{z}$.

Analysis in case of OTP'ed syndrome.

Eve observes b, u, a, c, ω and holds a quantum state $\rho^{\rm E}_{bst}$ correlated to b, s, t. The message m must be secure given Eve's information. The output state of the QKD protocol is given by

$$\mathcal{E}_{\rm QKD}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle mbuac\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst} \delta_{\omega,\theta_{st}} [\omega \delta_{c, m\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \tag{34}$$

The idealized output state is obtained as $\mathbb{E}_m |m\rangle\langle m| \otimes {\rm tr}_M \mathcal{E}_{\rm QKD}(\rho^{\rm ABE})$, which yields

$$\mathcal{F}_{\rm QKD}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle mbuac\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst} \delta_{\omega,\theta_{st}} [\omega \mathop{\mathbb{E}}_{m'} \delta_{c, m'\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \tag{35}$$

The difference is given by

$$\begin{aligned}(\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD})(\rho^{\rm ABE}) \quad = \quad & \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac} |mbuac, \omega = 1\rangle\langle mbuac, \omega = 1| \\ & \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst} \theta_{st} [\delta_{c, m\oplus\Phi_u(a\oplus s)} - \mathop{\mathbb{E}}_{m'} \delta_{c, m'\oplus\Phi_u(a\oplus s)}].\end{aligned} \tag{36}$$

This expression can be seen as the difference between two sub-normalized states which both have norm $P_{\rm corr}$. Hence an upper bound $\|\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD}\|_\diamond \leq P_{\rm corr}$ immediately follows. Furthermore, from (36) it follows that

$$\|\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD}\|_\diamond \leq \tfrac{1}{2} \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{ac} \left\| \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst} \theta_{st} 2^\ell [\delta_{c, m\oplus\Phi_u(a\oplus s)} - \mathop{\mathbb{E}}_{m'} \delta_{c, m'\oplus\Phi_u(a\oplus s)}] \right\|_1. \tag{37}$$

Expanding the trace norm as $\|A\|_1 = {\rm tr}\sqrt{A^\dagger A}$ we write the right hand side as

$$\tfrac{1}{2} \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{ac} \tag{38}$$

$${\rm tr} \sqrt{\mathop{\mathbb{E}}_{ss'tt'} \theta_{st}\theta_{s't'} \rho^{\rm E}_{bst} \rho^{\rm E}_{bs't'} 2^{2\ell} [\delta_{\Phi_u(a\oplus s), m\oplus c} - \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(a\oplus s), m'\oplus c}][\delta_{\Phi_u(a\oplus s'), m\oplus c} - \mathop{\mathbb{E}}_{m''} \delta_{\Phi_u(a\oplus s'), m''\oplus c}]}.$$

Using Jensen's inequality for operators we 'pull' $\mathbb{E}_u$ and $\mathbb{E}_m$ under the square root and then make use of the pairwise-independent properties of Φ_u when acted upon with $\mathbb{E}_u$. This yields

$$\begin{aligned}2^{2\ell} \mathop{\mathbb{E}}_{mu} [\delta_{\Phi_u(a\oplus s), m\oplus c} - \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(a\oplus s), m'\oplus c}][\delta_{\Phi_u(a\oplus s'), m\oplus c} - \mathop{\mathbb{E}}_{m''} \delta_{\Phi_u(a\oplus s'), m''\oplus c}] &= 2^\ell \delta_{ss'} (1 - \mathop{\mathbb{E}}_{mm'} \delta_{mm'}) \\ &< \quad 2^\ell \delta_{ss'}\end{aligned} \tag{39}$$

which leads to

$$\|\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD}\|_\diamond < \tfrac{1}{2} \mathop{\mathbb{E}}_b {\rm tr} \sqrt{2^\ell \mathop{\mathbb{E}}_{ss'tt'} \theta_{st}\theta_{s't'} \rho^{\rm E}_{bst} \rho^{\rm E}_{bs't'} \delta_{ss'}}. \tag{40}$$

Next we use $\theta_{st} \leq 1$ and $\mathbb{E}_t\, \rho^{\rm E}_{bst} = \rho^{\rm E}_{bs}$, yielding $\|\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD}\|_\diamond < \frac{1}{2}\mathbb{E}_b \operatorname{tr}\sqrt{2^\ell\, \mathbb{E}_{ss'}\, \rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}\delta_{ss'}}$. Combining the two obtained bounds gives

$$\|\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD}\|_\diamond \leq \min\Big(P_{\rm corr}, \tfrac{1}{2}\mathop{\mathbb{E}}_b \operatorname{tr}\sqrt{2^\ell \mathop{\mathbb{E}}_{ss'} \rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}\delta_{ss'}}\Big). \tag{41}$$

Using Post-selection, random Paulis and smooth Rényi entropy techniques, it has been shown [14, 18] that the right hand side of (41) can be upper bounded as $\propto \sqrt{2^{\ell-n+nh(\beta)}}$ for BB84 bases, and as $\propto \sqrt{2^{\ell-n-nh(\beta)+nh(1-\frac{3}{2}\beta,\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})}}$ for 6-state QKD.
When n is increased then either $P_{\rm corr}$ becomes exponentially small (if Eve's noise γ exceeds β) or (when $\gamma \leq \beta$) the expression under the square root becomes exponentially small, provided ℓ is set smaller than some threshold value $\ell_{\rm max}$. This threshold is given by $\ell^{\rm BB84}_{\rm max} = n - nh(\beta)$ and $\ell^{\rm 6state}_{\rm max} = n + nh(\beta) - nh(1 - \frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$. Taking into account the key expenditure for masking the syndrome $\mathtt{Syn}(x)$, the asymptotic rate is $r = \ell_{\rm max}/n - h(\beta)$, i.e. $r^{\rm BB84} = 1 - 2h(\beta)$; $r^{\rm 6state} = 1 - h(1 - \frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$.

Analysis in case of plaintext syndrome

We indicate the differences w.r.t. the analysis above. Eq. (34) gains an extra part due to the syndrome σ and becomes

$$\mathcal{E}^{\rm plain}_{\rm QKD}(\rho^{\rm ABE}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\sigma\omega} |mbuac\sigma\omega\rangle\langle mbuac\sigma\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\rm E}_{bst}\delta_{\omega,\theta_{st}}\delta_{\sigma,\mathtt{Syn}(a\oplus s)}[\omega\delta_{c,m\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \tag{42}$$

The factor $\delta_{\sigma,\mathtt{Syn}(a\oplus s)}$ is carried along untouched in the whole computation up to (38), where it gets doubled to $\delta_{\sigma,\mathtt{Syn}(a\oplus s)}\delta_{\sigma,\mathtt{Syn}(a\oplus s')}$. However, the $\delta_{ss'}$ produced in (39) undoes the doubling. One extra step is needed. The sum $\sum_e$ is rewritten as $2^{n-k} \cdot \frac{1}{2^{n-k}}\sum_\sigma$, and Jensen's inequality is used, 'pulling' the averaging operation $\frac{1}{2^{n-k}}\sum_\sigma$ into the square root, where it acts on $\delta_{\sigma,\mathtt{Syn}(a\oplus s)}$, giving rise to a constant 2^{k-n}.

$$\|\mathcal{E}^{\rm plain}_{\rm QKD} - \mathcal{F}^{\rm plain}_{\rm QKD}\|_\diamond \leq \min\Big(P_{\rm corr}, \tfrac{1}{2}\mathop{\mathbb{E}}_b \operatorname{tr}\sqrt{2^\ell 2^{n-k} \mathop{\mathbb{E}}_{ss'} \rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}\delta_{ss'}}\Big). \tag{43}$$

The $\ell_{\rm max}$ is decreased by an amount $n - k$, but the rate is exactly the same as before, since this time there is no key expenditure of $n - k$ bits for encrypting the syndrome.

B Protocol steps of the 'Interactive' variant

Alice and Bob have agreed on a MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^{\ell-\lambda} \to \{0,1\}^\lambda$, an invertible mapping $F_u : \{0,1\}^n \to \{0,1\}^n$ and $\Phi_u(x) = F_u(x)[:\ell]$ as discussed in Section 5.1. The keys are a mask $z \in \{0,1\}^\ell$, two MAC keys $k^{1,2}_{\rm MAC} \in \{0,1\}^\lambda$, a basis sequence $b \in \mathcal{B}^n$, two MAC keys $k^{1,2}_{\rm fb} \in \{0,1\}^\lambda$, a one-time pad $k_{\rm OTP}$ for the feedback bit, and a seed $u \in \{0,1\}^n$ for universal hashing. They have a reservoir $k_{\rm rej}$ of spare key material to refresh their keys from.
In each round Alice and Bob perform the following steps.
Alice: Random strings $\kappa \in \{0,1\}^{3\lambda+1}$, $r \in \{0,1\}^{n-\ell}$. Compute the authentication tag $\tau_1 = \Gamma(k^1_{\rm MAC}, \mu\|\kappa)$, augmented message $m = \mu\|\kappa\|\tau_1$, ciphertext $c = z \oplus m$ and qubit payload $x = F^{\rm inv}_u(c\|r) \in \{0,1\}^n$. Prepare and send $|\Psi\rangle = \bigotimes_{i=1}^n |\psi^{b_i}_{x_i}\rangle$.
Bob: Receive $|\Psi\rangle'$. Measure in the basis b, yielding $x' \in \{0,1\}^n$. Send confirmation of receipt $\tau_2 = \Gamma(k^1_{\rm fb}, 1)$; in case of non-receipt send $\tau_2 = \Gamma(k^1_{\rm fb}, 0)$.
Alice: Receive τ_2'. If τ_2' checks out send $e = \mathtt{Syn}(x)$, $\tau_3 = \Gamma(k^2_{\rm MAC}, e)$. Otherwise abort.
Bob: Receive e', τ_3'. If τ_3' does not check out abort. Otherwise recover $\hat{x} = x' \oplus \mathtt{SynDec}(e' \oplus \mathtt{Syn}\, x')$; compute $\hat{c} = \Phi_u(\hat{x})$ and $\hat{m} = \hat{c} \oplus z$; parse $\hat{m}$ as $\hat{\mu}\|\hat{\kappa}\|\hat{\tau}_1$. Set $\omega = 1$ if $\Gamma(k_{\rm MAC}, \hat{\mu}\|\hat{\kappa}) == \hat{\tau}_1$, otherwise $\omega = 0$. Compute $\tau_{\rm fb} = \Gamma(k^2_{\rm fb}, \omega \oplus k_{\rm OTP})$. Send $\omega \oplus k_{\rm OTP}$, $\tau_{\rm fb}$.
Key Update:
In case of `accept`: Re-use $z, b, u, k_{\rm MAC}$. Set next round keys $(\tilde{k}^1_{\rm fb}, \tilde{k}^2_{\rm fb}, \tilde{k}^2_{\rm MAC}, \tilde{k}_{\rm OTP}) = \kappa$.
In case of `reject`: Re-use $b, u, k_{\rm MAC}$. Take fresh $\tilde{z}, \tilde{k}^1_{\rm fb}, \tilde{k}^2_{\rm fb}, \tilde{k}^2_{\rm MAC}, \tilde{k}_{\rm OTP}$ from $k_{\rm rej}$.

References

[1] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (1991), 661 –663.

[2] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, and J. Oppenheim, *The universal composable security of quantum key distribution*, Theory of cryptography, 2005, pp. 386–406.

[3] A. Broadbent and S. Lord, *Uncloneable quantum encryption via random oracles* (2019). `https://eprint.iacr.org/2019/257`.

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

[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** (2014), 453–458. Original manuscript 1982.

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

[7] I.B. Damgård, T.B. Pedersen, and L. Salvail, *A Quantum Cipher with Near Optimal Key-Recycling*, CRYPTO (2005).

[8] D. Bruß, *Optimal eavesdropping in quantum cryptography with six states*, Phys. Rev. Lett. **81** (1998), no. 14, 3018–3021.

[9] D. Gottesman, *Uncloneable encryption*, Quantum Information and Computation **3** (2003), no. 6, 581–602.

[10] D. Gottesman and J. Preskill, *Secure quantum key distribution using squeezed states*, Phys. Rev. A **63** (2001), 022309.

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

[12] B. Kraus, N. Gisin, and R. Renner, *Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication*, Phys.Rev.Lett. **95** (2005), 080501.

[13] D. Leermakers and B. Škorić, *Quantum Alice and Silent Bob*. `https://eprint.iacr.org/2019/875`.

[14] ———, *Security proof for Quantum Key Recycling with noise*, Quantum Information Processing **19** (2019).

[15] H.-K. Lo, H.F. Chau, and M. Ardehali, *Efficient Quantum Key Distribution scheme and proof of its unconditional security*, Journal of Cryptology **18** (2005), 133–165.

[16] R. T. Moenck, *Fast Computation of GCDs*, Proceedings of the fifth annual acm symposium on theory of computing, 1973, pp. 142–151.

[17] C. Portmann, *Quantum authentication with key recycling*, Advances in Cryptology – Eurocrypt 2017, 2017, pp. 339–368.

[18] R. Renner, *Security of quantum key distribution*, Ph.D. Thesis, 2005.

[19] P. Shor and J. Preskill, *Simple proof of security of the BB84 quantum key distribution protocol*, Phys.Rev.Lett. **85** (2000), 441.

[20] M. Tomamichel and A. Leverrier, *A largely self-contained and complete security proof for quantum key distribution*, Quantum **1** (201707), 14.

[21] T. Sasaki, Y. Yamamoto, and M. Koashi, *Practical quantum key distribution protocol without monitoring signal disturbance*, Nature **509** (2014May), 475–478.

[22] 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).

[23] 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** (1981), 265–279.

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