Quantum Information and Computation, Vol. 21, No. 11&12 (2021) 0901–0930
© Rinton Press

QUBIT-BASED UNCLONABLE ENCRYPTION WITH KEY RECYCLING

DAAN LEERMAKERS
Department of Mathematics and Computer Science, Eindhoven University of Technology
5600MB Eindhoven, The Netherlands

BORIS ŠKORIĆ
Department of Mathematics and Computer Science, Eindhoven University of Technology
5600MB Eindhoven, The Netherlands

Received March 31, 2021
Revised June 27, 2021

We re-visit Unclonable Encryption as introduced by Gottesman in 2003 [1]. We look at the combination of Unclonable Encryption and Key Recycling, while aiming for low communication complexity and high rate. We introduce a qubit-based prepare-and-measure Unclonable Encryption scheme with re-usable keys. Our scheme consists of a single transmission by Alice and a single classical feedback from Bob. The transmission from Alice to Bob consists entirely of qubits. The rate, defined as the message length divided by the number of qubits, is higher than what can be achieved using Gottesman's scheme [1]. We provide a security proof based on the diamond norm distance, taking noise into account.

Keywords: unclonable encryption; Quantum Key Recycling; quantum cryptogtraphy
Communicated by: S Braunstein & H Zbinden

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) [2, 3, 4] schemes provide a way of re-using encryption keys. (ii) Unclonable Encryption (UE) [1] guarantees that a message remains secure even if the keys leak at some time in the future.

In this paper we introduce a sheme that achieve both the key recycling and UE properties, and we explicitly prove that this can be achieved with low communication complexity. Our scheme acts 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 [5], 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 theoretically 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. [6, 7, 8, 9, 10, 11, 12, 13, 14, 15]. Much less known is that the concept of QKR was proposed two years before QKD [2]. QKR encrypts a classical message into a quantum 'cipherstate' using basis choices that are a shared secret between Alice and Bob, and allows for the re-use of this secret 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 [16] 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. [7, 9, 11, 15]), while a security proof for qubit-based QKR has been provided fairly recently [3]. A cipher with near optimal rate using high-dimensional qudits was introduced in 2005 [17]. 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 [18]. 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 passes. 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 [19]; a further reduction of the total amount of communicated data.

1.3 Unclonable Encryption

In 2003, D. Gottesman introduced a scheme called *Unclonable Encryption*[a] (UE) [1] 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.) It is important to remark here that the 'standard' way of using QKD (building a pool of key material for later use as one-time pad) is *not* unclonable encryption: the ciphertext is classical and can be copied for later decryption.

[a] This is slightly different from the unclonability notion of Broadbent and Lord [20] which considers two collaborating parties who both wish to recover the plaintext.

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 UE without key expenditure.

Since QKR sends a message directly instead of establishing a key for later use, QKR protocols are natural candidates to have the UE property. In the case of noiseless quantum channels, the high-dimensional encryption scheme [17] and the qubit-based schemes [3, 4] seem to have UE; for noisy channels [4] with modified parameters also seems to have UE. However, none of these conjectures have been explicitly stated or proven, which is a shame since resilience against key leakage is an interesting security feature. The QKR protocol where Alice sends only qubits [19] is clearly not unclonable, due to the fact that single-use keys are stored at the end of each round.

2 Contributions

We construct an Unclonable Encryption scheme with recyclable keys, while aiming for low communication complexity and high rate. We consider the following setting. Alice and Bob have a reservoir of shared key material. Alice sends data to Bob in N chunks. Each chunk individually is tested by Bob for consistency (sufficiently low noise and valid MAC). In case of `reject` they have to access new key material from the reservoir. In case of `accept`, Alice and Bob re-use their key material; this may be done either by keeping keys unchanged or by re-computing keys without accessing the reservoir. If the N'th round was an `accept`, all keys of round N are assumed to become public.

- We define the Key Recycling (KR) and Unclonable Encryption (UE) properties in terms of statistical indistinguishability. For these definitions we show a relation between KR and UE: If a KR scheme re-uses all its long-term secrets in unchanged form upon `accept`, then it also has the UE property.
- We introduce KRUE, a qubit-based prepare-and-measure scheme that satisfies KR and UE. Alice sends a single transmission, which consists entirely of qubits. Bob responds with an authenticated classical feedback bit. We provide a security proof 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 [11]. In the case of a noiseless channel this reduction is almost immediate, without involving any inequalities.
- KRUE by itself is not a fully functional scheme. It relies on an external mechanism to securely transport some key material for the key update. We propose to employ the 'Quantum Alice and Silent Bob' QKR scheme [19], which is highly efficient, as the external mechanism. The advantage of using QKR is that it can be combined efficiently with KRUE to yield a two-pass protocol, i.e. its advantage is low round complexity. We derive the asymptotic rate of the combined KRUE+QKR scheme for BB84 encoding and 6-state encoding. In the case of BB84 encoding the asymptotic rate of KRUE+QKR is $\frac{[1-2h(\beta)]^2}{1-h(\beta)}$, Here h is the binary entropy function, and β is the tolerated bit error rate in the quantum channel.[b]

[b] For comparison, the key generation rate of BB84 QKD is $1-2h(\beta)$.

We present a rate comparison between various constructions that achieve UE and KR simultaneously. KRUE+QKR has the highest rate.

The outline of the paper is as follows. After introducing notation and preliminaries in Section 3, we introduce the attacker model and security definitions in Section 4. We then introduce the KRUE protocol (Section 5) and its EPR version (Section 6), We present the security proof and the rate analysis in Section 7. In Section 8 we compare KRUE+QKR to existing qubit-based alternatives and alternative external mechanisms for KRUE. In Section 9 we summarise and suggest topics for future work.

3 Preliminaries

3.1 Notation and terminology

Classical Random Variables are denoted with capital letters, and their realisations with lower-case 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 Hamming weight of a string s is denoted as $|s|$. The complement of a Boolean variable $x \in \{0,1\}$ is written as $\bar{x} = 1-x$. 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 $\sum_{i=1}^{k} p_i \log\frac{1}{p_i}$. 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 with classical bit x encoded in basis b is written as $|\psi_x^b\rangle$. The set of bases is $\mathcal{B}$. In case of BB84 states we have $\mathcal{B} = \{x,z\}$; in case of 6-state encoding $\mathcal{B} = \{x,y,z\}$. A mixed state (also called density matrix) in Hilbert space $\mathcal{H}$ is a positive semidefinite operator on $\mathcal{H}$ with unit trace. We write 'tr' for trace. We write $\mathcal{S}(\mathcal{H})$ to denote the space of (not necessarily normalised) positive semi-definite operators acting on $\mathcal{H}$. Consider a density matrix $\rho \in \mathcal{S}(\mathcal{H})$ with eigenvalues $\{\lambda_i\}$. The 1-norm of ρ is written as $\|\rho\|_1 = \mathrm{tr}\,|\rho| = \mathrm{tr}\,\sqrt{\rho^\dagger\rho} = \sum_i |\lambda_i|$. The trace norm is $\|\rho\|_{\mathrm{tr}} = \frac{1}{2}\|\rho\|_1$. The trace distance $D(\rho,\sigma)$ between two density matrices ρ and σ is defined as $D(\rho,\sigma) = \frac{1}{2}\mathrm{tr}\,|\rho-\sigma|$. It is the generalisation of the statistical distance between classical random variables, and it is a measure for the distinguishability of ρ and σ.

We use capitalised superscripts to label subsystems of a Hilbert space. Non-italic labels 'A', 'B' and 'E' indicate the subsystem of Alice/Bob/Eve. Consider classical variables X, Y and a quantum system in Eve's possession 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. $\rho^{Y\mathrm{E}} = \mathrm{tr}_X \rho^{XY\mathrm{E}} = \mathbb{E}_y|y\rangle\langle y| \otimes \rho^{\mathrm{E}}_y$, with $\rho^{\mathrm{E}}_y = \mathbb{E}_{x|y}\rho^{\mathrm{E}}_{xy}$. The fully mixed state on $\mathcal{H}_A$ is denoted as χ^A. We also use the notation $\mu^X = \mathbb{E}_x|x\rangle\langle x|$ for a classical variable X that is not necessarily uniform. The distance from uniformity of X's distribution given Eve's subsystem is given by $D(\rho^{X\mathrm{E}}, \chi^X \otimes \rho^{\mathrm{E}})$. This is a measure of Eve's ability to distinguish X from uniform, given quantum side information. Similarly, for nonuniform X, the distance $D(\rho^{X\mathrm{E}}, \rho^{X} \otimes \rho^{\mathrm{E}})$ expresses how different the 'posterior' $X|E$ is from the prior distribution of X.

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 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 $\frac{1}{2} + \frac{1}{4}\|\mathcal{E} - \mathcal{E}'\|_\diamond$. In quantum cryptography, a popular proof technique is to consider Alice and Bob performing actions on noisy EPR pairs. These actions are described by a CPTP map $\mathcal{E}$ acting on the input EPR states and outputting classical outputs for Alice and Bob, and correlated quantum side information for Eve. The security of such a protocol is quantified by the diamond norm between the actual map $\mathcal{E}$ and an idealised map $\mathcal{F}$ which produces perfectly behaving outputs (e.g. perfectly secret QKD keys). 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 [15].

A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{T}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [21] 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 $h \in H$.

An information-theoretically secure MAC function can be constructed using pairwise independent hash functions and a shared key [21]. The probability of forging the authentication tag that an information-theoretically secure MAC outputs is equal to the probability of randomly guessing the key or the tag. When the smallest size of the key and tag is λ this is $2^{-\lambda}$.

3.2 Pairwise independent hashing with easy inversion

We will need a privacy amplification function that is easily computable in two directions. Unfortunately the code-based construction due to Gottesman [1] does not work with the proof technique of [11], which requires a family of universal hash functions. We will be using a family of pairwise independent hash functions $F : \{0,1\}^k \to \{0,1\}^k$ that are easy to invert. An easy way to construct such a family is to use an affine function in $GF(2^k)$ [22]. Let $u = (u_1, u_2)$ with $u_1, u_2 \in GF(2^k)$ randomly chosen. Define $F_u(x) = u_1 \cdot x + u_2$, where the operations are in $GF(2^k)$. Likewise $F_u^{\mathrm{inv}}(z) = u_1^{-1} \cdot (z + u_2)$. A pairwise independent family of hash functions Φ from $\{0,1\}^k$ to $\{0,1\}^\ell$, with $\ell < k$, can be obtained by taking the ℓ most significant bits of $F_u(x)$.[c] We denote this as

$$\Phi_u(x) \overset{\mathrm{def}}{=} F_u(x)[:\ell]. \tag{1}$$

The inverse operation is as follows. Given $c \in \{0,1\}^\ell$, generate random $r \in \{0,1\}^{k-\ell}$ and output $F_u^{\mathrm{inv}}(c\|r)$. It obviously holds that $\Phi_u(F_u^{\mathrm{inv}}(c\|r)) = c$. Computing an inverse in

[c] The proof is straightforward. Write $F_u(x) = c\|r$, with $c \in \{0,1\}^\ell$. Let $x' \neq x$. Then $\Pr_u[\Phi_u(x) = c \wedge \Phi_u(x') = c'] = \sum_{r,r' \in \{0,1\}^{k-\ell}} \Pr_u[F_u(x) = c\|r \ \wedge \ F_u(x') = c'\|r']$. By the pairwise independence of F this gives $\sum_{r,r' \in \{0,1\}^{k-\ell}} 2^{-2k} = 2^{-2\ell}$.

$GF(2^k)$ costs $O(k \log^2 k)$ operations [23].

3.3 Post-selection

For protocols that are invariant under permutation of their inputs it has been shown [24] that security against collective attacks (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 $\mathcal{F}$ be the perfect functionality of that protocol. If for all input permutations π 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, which is negligible compared to n. We use the term 'privacy amplification' for the act of hashing to a smaller message size in order to obtain a better security parameter.

3.4 Noise symmetrisation with random Pauli operators

In [11] 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 half of the EPR pair, with $\alpha_j \in \{0,1,2,3\}$ random and public; then they forget α. The upshot is that Eve's state (the purification of the Alice+Bob system) is simplified to the 4×4 diagonal matrix ${\rm Diag}(1 - \frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2})$. 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 definitions

4.1 Attacker model

We work in same setting as Gottesman [1], as discussed in Section 1.3. We distinguish between on the one hand long-term secrets and on the other hand short-term secrets. A variable is considered short-term only if it is created[d] and immediately operated upon locally (without waiting for incoming communication), and then deleted. All other variables are long-term. (An example of a short-term variable is a nonce that is generated, immediately used a function evaluation and then deleted. On the other hand, all keys that are stored between protocol rounds are long-term.)

We consider two world views.

- **World1**. All secrets can be kept confidential indefinitely or destroyed.
- **World2**. Long-term secrets 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.

[d] Performing a measurement on a quantum state is also considered to 'create' a classical variable.

QKR protocols are typically designed to be secure in world1. In this paper we prove 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'.[e] 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.

4.2 Security definitions

We briefly introduce the formalism for describing quantum encryptions of classical messages, and key recycling schemes.

Definition 1 *A quantum encryption scheme* QE *with message space $\mathcal{M}$, key space $\mathcal{K}$, and Hilbert space $\mathcal{H}$ consists of the following components:*

1. *A key generation function* $\mathsf{QE.Gen}$: $1^\lambda \to \mathcal{K}$*, where λ is the security parameter.*
2. *A CPTP map* $\mathsf{QE.Encr}$: $\mathcal{M}\times\mathcal{K}\times\mathcal{S}(\mathcal{H})\to\mathcal{M}\times\mathcal{K}\times\mathcal{S}(\mathcal{H})$ *that takes as input a message $m\in\mathcal{M}$ and a key $k\in\mathcal{K}$, acts on an initial quantum state $\pi^0\in\mathcal{S}(\mathcal{H})$, and outputs a cipherstate $\pi_{mk}\in\mathcal{S}(\mathcal{H})$ which may or may not contain a classical part. (The m and k are not modified.) We write* $\mathsf{QE.Encr}\Big(|m\rangle\langle m|\otimes|k\rangle\langle k|\otimes\pi^0\Big)=|m\rangle\langle m|\otimes|k\rangle\langle k|\otimes\pi_{mk}$.
3. *A measurement* $\mathsf{QE.Decr}$: $\mathcal{K}\times\mathcal{S}(\mathcal{H})\to\mathcal{K}\times\mathcal{M}'\times\{0,1\}$ *that takes as input a key $k\in\mathcal{K}$ and a cipherstate, and outputs a message $m'\in\mathcal{M}'$ and a flag $\omega\in\{0,1\}$. Here we have defined $\mathcal{M}'=\mathcal{M}\cup\{\perp\}$. (The k is not modified.) The flag is set as $\omega=0$ if $m'=\perp$ and $\omega=1$ otherwise. The POVM operators at given k are written as $\{D^k_{m'}\}_{m'\in\mathcal{M}'}$, with $\forall_k \sum_{m'\in\mathcal{M}'}D^k_{m'}=\mathbb{1}$.*

The measurement has a fully classical outcome. Without loss of generality we write $\pi^0=|0\rangle\langle 0|$. The actions of Alice, Eve and Bob are described as follows. Alice and Bob generate a shared key $k=\mathsf{QE.Gen}()$. Alice draws a plaintext message m from a distribution that is not necessarily uniform, and not necessarily known to Alice. The non-uniformity takes into account that Eve may have prior knowledge about the likelihood of messages, or even know part of the plaintext. Alice applies $\mathsf{QE.Encr}$, yielding cipherstate π_{mk} which she sends to Bob.

Eve intercepts π_{mk}. Eve entangles a quantum state of her own with π_{mk}, resulting in a state $\rho^{\rm BF}_{mk}=U(\pi_{mk}\otimes|e\rangle\langle e|)$, where $|e\rangle$ is the initial state of Eve's quantum system and U is a unitary operation. The label 'B' stands for the subsystem forwarded to Bob. The 'F' part

[e] One data transmission will be called a *pass*. A round consists of multiple passes.

is the subsystem kept by Eve.[f] The above procedure, with postponed measurement on the F system, is the most general action possible for Eve, and comprises options like e.g. copying classical information, or completely keeping π_{mk}. Eve's overall action can be written as a CPTP map $\mathcal{A}$ which acts as $(\mathcal{A}\circ\mathsf{QE.Encr})\Big(|mk0e\rangle\langle mk0e|\Big) = |mk\rangle\langle mk|\otimes\rho^{\rm BF}_{mk}$.[g] Bob acts on the 'B' part of $\rho^{\rm BF}_{mk}$ with $\mathsf{QE.Decr}$. He makes the value of ω public.

This whole sequence of events results in a final state that we refer to as the *output* of the scheme, $(\mathsf{QE.Decr}\circ\mathcal{A}\circ\mathsf{QE.Encr})\Big(|mk0e\rangle\langle mk0e|\Big) = |mk\rangle\langle mk|\otimes\sum_{m'\in\mathcal{M}'}|m'\rangle\langle m'|\otimes{\rm tr}_{\,\rm B}D^k_{m'}\rho^{\rm BF}_{mk}$ $\overset{\rm def}{=}|mk\rangle\langle mk|\otimes\sum_{m'\in\mathcal{M}'}|m'\rangle\langle m'|({\rm tr}\,D^k_{m'}\rho^{\rm BF}_{mk})\otimes\rho^{\rm F}_{mkm'}$.

Writing the classical variables m, k, m', ω as subsystems of a large quantum-classical state, we express the output state as

$$\rho^{MKM'\Omega{\rm F}} = \sum_{m\in\mathcal{M}}\Pr[M=m]\sum_{k\in\mathcal{K}}\frac{1}{|\mathcal{K}|}\sum_{m'\in\mathcal{M}'}({\rm tr}\,D^k_{m'}\rho^{\rm BF}_{mk})|mkm'\omega(m')\rangle\langle mkm'\omega(m')|\otimes\rho^{\rm F}_{mkm'}. \tag{3}$$

Correctness. We say that a quantum encryption scheme QE is ε-correct if $\Pr[\Omega=1\wedge M'\neq M]\leq\varepsilon$ for any adversarial action $\mathcal{A}$ and any distribution of M. This definition adheres to the correctness definition in the QKD literature (see e.g. [25, 15]). (In classical cryptography the correctness requirement would be that $\Pr[\Omega=1\wedge M'=M]\geq 1-\varepsilon$ if Eve does not interfere. We will see that our scheme satisfies both correctness notions.)

Security. A quantum encryption scheme is considered secure if the cipherstate does not give Eve more information about the message than she already had. This can be expressed in terms of the statistical distance (trace distance) between Eve's a priori distribution of M and Eve's a posteriori distribution of M given Ω and the 'F' subsystem, where F may be obtained via any adversarial action $\mathcal{A}$ as described above, and in particular can comprise the entire cipherstate. We define the *Encryption* property (**ENC**) as follows.

Definition 2 *Let* QE *be a quantum encryption according to Def. 1 with output state* $\rho^{MKM'\Omega{\rm F}} = (\mathsf{QE.Decr}\circ\mathcal{A}\circ\mathsf{QE.Encr})(\sum_{mk}\frac{\Pr[M=m]}{|\mathcal{K}|}|mk0e\rangle\langle mk0e|)$ *as described above. We say that* QE *is* **ε-encrypting (ε-ENC)** *if the output satisfies*

$$\|\rho^{M\Omega{\rm F}}-\rho^{M}\otimes\rho^{\Omega{\rm F}}\|_1\leq\varepsilon \tag{4}$$

for all adversarial actions $\mathcal{A}$ *and all distributions of* M.

(The ε is referred to as the *error*). Note that in (4) M' has been traced out. In the case $\omega=1$ it is obvious that we are allowed to trace out M', as Eve gains no knowledge about M'. But in the case $\omega=0$ Eve learns that $m'=\perp$, so strictly speaking M' is not entirely hidden from Eve. However, Eve already has access to Ω; given $\omega=0$, learning that $m'=\perp$ conveys no additional information.[h]

Our Def. 2 differs from the more conventional "statistical privacy" property as defined in e.g. [17], primarily in that we include the flag Ω. Our motivation for including Ω is that we

[f] Here we do not use the label 'E' because later in the paper that will be reserved exclusively for Eve's *quantum* side information, while F may contain classical variables as well.

[g] We use combined notation $|mk0e\rangle$ for $|m\rangle\otimes|k\rangle\otimes|0\rangle\otimes|e\rangle$.

[h] Alternatively, in Def. 1 we could have assigned a random value to m' in case of decryption failure. Then Eve would have no access whatsoever to M'.

later want to express that a QKR scheme, which by default has the flag Ω, is ε-encrypting.

$$\varepsilon\text{-statistical privacy :} \quad \forall_{m_0,m_1\in\mathcal{M}} \quad \|\mathbb{E}_k \pi_{m_0 k} - \mathbb{E}_k \pi_{m_1 k}\|_{\rm tr} \leq \varepsilon. \tag{5}$$

Lemma 1 *ε-ENC (Def. 2) implies ε-statistical privacy.*

Proof: Consider the special case where M is deterministic, $M = m_0$. Furthermore we take the special case that Eve keeps the entire cipherstate. Then $\rho^{MF} = |m_0\rangle\langle m_0| \otimes \mathbb{E}_k \pi_{m_0 k}$ and $\rho^M \otimes \rho^F = |m_0\rangle\langle m_0| \otimes \mathbb{E}_{mk}\pi_{mk}$ We get

$$\begin{aligned} \|\mathbb{E}_k \pi_{m_0 k} - \mathbb{E}_{mk}\pi_{mk}\|_1 &= \||m_0\rangle\langle m_0| \otimes \mathbb{E}_k \pi_{m_0 k} - |m_0\rangle\langle m_0| \otimes \mathbb{E}_{mk}\pi_{mk}\|_1 \\ &= \|\rho^{MF} - \rho^M \otimes \rho^F\|_1 \leq \|\rho^{M\Omega F} - \rho^M \otimes \rho^{\Omega F}\|_1 \leq \varepsilon. \end{aligned} \tag{6}$$

Similarly, for deterministic $M = m_1$ we get $\|\mathbb{E}_k \pi_{m_1 k} - \mathbb{E}_{mk}\pi_{mk}\|_1 \leq \varepsilon$. Together this yields $\|\mathbb{E}_k \pi_{m_0 k} - \mathbb{E}_k \pi_{m_1 k}\|_1 \leq 2\varepsilon$. □

Alice and Bob share a 'reservoir' of key material. The aim of Quantum Key Recycling (QKR) is to use up this reservoir as slowly as possible, while having low round complexity and high rate. We define a QKR scheme as a Quantum Encryption scheme with the additional property that (most of) the key material can be re-used when Alice and Bob detect no disturbance. This definition differs slightly from others used in the literature in two respects, (i) In [3] an *authentication* scheme with key re-use is also referred to as QKR. However, as mentioned in [3], message encryption is trivially added; (ii) We do not demand re-use of the exact same key in unmodified form, but allow a small amount of fresh randomness to be hashed into the old key.

Definition 3 *A Quantum Key Recycling scheme* QKR *with message space $\mathcal{M}$, key space $\mathcal{K}$ and Hilbert space $\mathcal{H}$ consists of the following components:*

1. *A key generation function* QKR.Gen: $1^\lambda \to \mathcal{K}$*, where λ is the security parameter.*
2. *A CPTP map* QKR.Encr: $\mathcal{M}\times\mathcal{K}\times\mathcal{S}(\mathcal{H}) \to \mathcal{M}\times\mathcal{K}\times\mathcal{S}(\mathcal{H})$ *that takes as input a message $m \in \mathcal{M}$ and a key $k \in \mathcal{K}$, acts on an initial state $\pi^0 \in \mathcal{S}(\mathcal{H})$, and outputs a cipherstate $\pi_{mk} \in \mathcal{S}(\mathcal{H})$ which may or may not contain a classical part. (The m and k are not modified.) We write* $\mathsf{QKR.Encr}\Big(|mk\rangle\langle mk| \otimes \pi^0\Big) = |mk\rangle\langle mk| \otimes \pi_{mk}$.
3. *A measurement* QKR.Decr: $\mathcal{K}\times\mathcal{S}(\mathcal{H}) \to \mathcal{K}\times\mathcal{S}(\mathcal{M}')\times\{0,1\}$ *that takes as input a key $k \in \mathcal{K}$ and a cipherstate, and outputs (i) a message $m' \in \mathcal{M}$ or the error message $\perp$; (ii) a flag ω which is set to $\omega = 0$ (*`reject`*) if $m' = \perp$ and to $\omega = 1$ (*`accept`*) if $m' \in \mathcal{M}$. (The k is not modified.)*
4. *A function* QKR.Refresh: $\mathcal{K}\times\{0,1\} \to \mathcal{K}\times\{0,1\}$ *that takes as input a key $k \in \mathcal{K}$ and the flag ω, and outputs a new key $\tilde{k} \in \mathcal{K}$. (The ω is not modified.) The* Refresh *function may use randomness from the reservoir.*

The part of a QKR protocol that differs from mere quantum encryption is that the flag ω gets communicated from Bob to Alice, and then both parties do a key refresh. For the `reject` case it has been shown [17] that Refresh needs at least $\log|\mathcal{M}|$ bits of fresh randomness from the reservoir. In some schemes, e.g. [3], the key remains unchanged ($\tilde{k} = k$) in case of `accept`, whereas in others [19] the $\tilde{k}$ is computed by hashing some randomness from the protocol into k (without accessing the reservoir).

Definition 4 (Rate) *Let* QKR *be a quantum key recycling scheme according to Def. 3, with message space* $\mathcal{M}$ *and a cipherstate that comprises* n *qubits. Let* $\mathsf{QKR.Refresh}$ *use* κ *bits from the reservoir upon* `accept`*. The rate of* QKR *is defined as*

$$\text{rate} = \frac{\log|\mathcal{M}| - \kappa}{n}. \tag{7}$$

Def. 4 is a natural definition given the fact that qubits are the most expensive resource. For $\kappa = 0$ the rate (7) measures how many actual message bits are received by Bob per expended qubit. For $\kappa > 0$ (key material is spent from the reservoir) it is straightforward to define a fair comparison w.r.t. schemes that do *not* tap into the reservoir: simply imagine sending κ random bits inside the message instead of using the reservoir; this effectively reduces the message length as in (7).[i]

The output state of a QKR protocol is $\rho^{MKM'\tilde{K}\Omega\mathrm{F}} = (\mathsf{QKR.Refresh} \circ \mathsf{QKR.Decr} \circ \mathcal{A} \circ \mathsf{QKR.Encr})\,(\sum_{mk} \frac{\Pr[M=m]}{|\mathcal{K}|}|mk0e\rangle\langle mk0e|)$. We introduce notation $\rho^{MKM'\tilde{K}\mathrm{F}}_{\mathtt{accept}} = \rho^{MKM'\tilde{K},\Omega=1,\mathrm{F}}$ and
$\rho^{MKM'\tilde{K}\mathrm{F}}_{\mathtt{reject}} = \rho^{MKM'\tilde{K},\Omega=0,\mathrm{F}}$, with $\rho^{MKM'\tilde{K}\mathrm{F}}_{\mathtt{accept}} + \rho^{MKM'\tilde{K}\mathrm{F}}_{\mathtt{reject}} = \rho^{MKM'\tilde{K}\Omega\mathrm{F}}$. The `accept` and `reject` part of the state are sub-normalised. We write $\tilde{k}_{\mathtt{acccept}} = \mathsf{QKR.Refresh}(k, 1)$.

Definition 5 *A quantum key recycling scheme with output state* $\rho^{MKM'\tilde{K}\Omega\mathrm{F}}$ *is called* **ε-recycling (ε-KR)** *if (i) the reservoir is not accessed for creating the updated key* $\tilde{k}_{\mathtt{accept}}$ *and (ii) the output state satisfies*

$$\|\rho^{M\tilde{K}\Omega\mathrm{F}} - \rho^{\tilde{K}} \otimes \rho^{M\Omega\mathrm{F}}\|_1 \leq \varepsilon. \tag{8}$$

Intuitively, Def. 5 says that even in the case of known plaintext Eve's posterior distribution of $\tilde{K}$ is hardly distinguishable from the prior distribution. (For `reject` this is the case because the key gets refreshed from the reservoir; for `accept` it is the case because Eve cannot learn much when she causes little disturbance.) Upon `accept` it is then safe to re-use key material, in the form of $\tilde{k}$, without accessing the reservoir. The indistinguishability formulation (8) is the same as in [17] and is also used for part of the key material in [3].

As mentioned in Section 4.1, looking at the KR property makes sense only before the end of round N. It is assumed in the attacker model that the 'old' keys do not leak during this period. Hence it is possible to write (8) in a form that has K traced out.

Definition 6 *A scheme with output state* $\rho^{MKM'\tilde{K}\Omega\mathrm{F}}$ *is called* ε**-unclonable (ε-UE)** *if it satisfies*

$$\|\rho^{MK\tilde{K}\mathrm{F}}_{\mathtt{accept}} - \rho^{M} \otimes \rho^{K\tilde{K}\mathrm{F}}_{\mathtt{accept}}\|_1 \leq \varepsilon. \tag{9}$$

Intuitively, Def. 6 states that either the `accept` probability is low due to Eve's interference, or else Eve's posterior distribution of M, given that k and $\tilde{k}$ leak after completion of an `accept`ing protocol run, is hardly distinguishable from the prior distribution. This UE definition specifies no requirement for the `reject` case, since the ENC property already exists to keep M safe in case of `reject` (even if Eve keeps the whole cipherstate).

Note that other definitions exist than the ones given above. For instance, Fehr and Salvail [3] have a definition of recycling that allows Alice and Bob to re-use their keys in unmodified

[i] Note that Def. 4 is consistent with the notion of key generation rate in QKD. QKD followed by transfer of a one-time-padded message $\mu \in \mathcal{M}$ can be seen as a special case of Def. 3, where $\mathsf{QKR.Decr}$ involves a lot of communication, and $\mathcal{K}$ is the key space of the MACs.

form even if Eve obtains some information about part of the key (the measurement basis B), as long as the min-entropy of B remains high enough. Such leakage may occur e.g. when Eve observes the feedback bit ω after slightly manipulating the cipherstate. In our definition of recycling, on the other hand, Eve is not allowed to know even a single bit about the updated key $\tilde{K}$.

Furthermore, Def. 6 differs from Gottesman's definition of unclonable encryption [1],

$$\begin{aligned} &\forall_{m_0,m_1\in\mathcal{M}:m_1\neq m_0} \text{ and for a fraction } \geq 1-\varepsilon \text{ of keys } k\in\mathcal{K}: \\ &\quad \|\rho^{\mathrm{F}}_{\mathrm{accept}}(m_0,k)-\rho^{\mathrm{F}}_{\mathrm{accept}}(m_1,k)\|_1 \leq \varepsilon. \end{aligned} \tag{10}$$

The main difference is that we have to keep track of $\tilde{K}$ as well as K since we are in the QKR setting. Apart from this detail, Def. 6 and (10) are very similar. In fact, if the K in (10) is read as $K,\tilde{K}$ together, then Def. 6 implies (10). This can be seen as follows. (i) Going from the register M to specific values m_0, m_1 follows the same step as in the proof of Lemma 1. (ii) Def. 6 works with an average over k, and hence the desired $\|\cdots\|_1 \leq \varepsilon$ property may fail to hold for a fraction ε of all values $k\in\mathcal{K}$. Hence in a fraction $1-\varepsilon$ of k-values the property does hold, which is the same fraction as in (10).

Our preference for our KR and UE definitions stems from (i) the fact that they allow for a unified treatment of all the components[j] of k; (ii) compatibility with the proof technique of [11, 24], which makes it possible to prove security of high-rate schemes; (iii) having the same type of definition for UE and KR. Furthermore our KR definition is compatible with [17].

Note that our KR and UE do not automatically imply ENC. The ENC property has to be considered as a separate requirement. For the combination of ENC and KR we have the following two lemmas.

Lemma 2

$$\|\rho^{M\tilde{K}\Omega\mathrm{F}}-\rho^M\otimes\rho^{\tilde{K}}\otimes\rho^{\Omega\mathrm{F}}\|_1\leq\varepsilon \quad\Longrightarrow\quad \varepsilon\textit{-ENC} \;\wedge\; 2\varepsilon\textit{-KR}. \tag{11}$$

Proof. Taking the lhs of (11) and tracing over $\tilde{K}$ yields ε-ENC. Furthermore, using the triangle inequality we write $\|\rho^{M\tilde{K}\Omega\mathrm{F}}-\rho^{\tilde{K}}\otimes\rho^{M\Omega\mathrm{F}}\|_1 \leq \|\rho^{M\tilde{K}\Omega\mathrm{F}}-\rho^M\otimes\rho^{\tilde{K}}\otimes\rho^{\Omega\mathrm{F}}\|_1 + \|\rho^M\otimes\rho^{\tilde{K}}\otimes\rho^{\Omega\mathrm{F}}-\rho^{\tilde{K}}\otimes\rho^{M\Omega\mathrm{F}}\|_1$. Both terms individually are bounded by ε by the lhs of (11); the first term directly, the second term after taking the $\tilde{K}$-trace. This proves 2ε-KR. □

Lemma 3

$$(\tilde{K}_{\mathtt{accept}}=K) \;\wedge\; \varepsilon_1\textit{-ENC} \;\wedge\; \varepsilon_2\textit{-KR} \quad\Longrightarrow\quad (\varepsilon_1+\varepsilon_2)\textit{-UE}. \tag{12}$$

Proof. With $\tilde{K}_{\mathrm{accept}}=K$ we have $\|\rho^{MK\tilde{K}\mathrm{F}}_{\mathtt{accept}}-\rho^M\otimes\rho^{K\tilde{K}\mathrm{F}}_{\mathtt{accept}}\|_1 \leq \|\rho^{MK\mathrm{F}}_{\mathtt{accept}}-\rho^M\otimes\rho^K\otimes\rho^{\mathrm{F}}_{\mathrm{accept}}\|_1 + \|\rho^M\otimes\rho^K\otimes\rho^{\mathrm{F}}_{\mathrm{accept}}-\rho^M\otimes\rho^{K\mathrm{F}}_{\mathtt{accept}}\|_1$. The first term is bounded by taking the trace over K and using ε_1-ENC. For the second we take the trace over M, yielding $\|\rho^{K\mathrm{F}}_{\mathtt{accept}}-\rho^K\otimes\rho^{\mathrm{F}}_{\mathrm{accept}}\|_1$. This expression is bounded by ε_2, which is seen by taking the M-trace of (8). □

Lemma 2 allows us to prove both ENC and KR by upperbounding a single quantity. Lemma 3 is an important statement: any ENC scheme that upon `accept` re-uses its keys *in unmodified form* and satisfies KR is automatically a UE scheme. It is interesting to note

[j] e.g. measurement basis, MAC key, and seeds for hash functions.

that [3] has $\tilde{K}_{\tt accept} = K$ but does not satisfy our KR definition, whereas [4, 19] satisfies our KR definition but does not have $\tilde{K}_{\tt accept} = K$. By Theorem 4 in [17] and Lemma 3, the *high-dimensional* scheme of Damgård et al. [17] has the UE property.

4.3 CPTP maps in the EPR formulation

EPR version of preparing and sending a state.

In order to make contact with the proof technique of Section 3.3 we re-formulate the statements of Section 4.2 in terms of CPTP maps that act on noisy EPR pairs. In the EPR version of a protocol in general, Alice's act of sending an n-qubit state (which then gets entangled with Eve's state) to Bob is replaced by the following sequence. (i) Eve creates an arbitrary pure state; (ii) Eve then sends n-qubit subsystems to Alice and Bob while keeping her own subsystem which is entangled with the other two; (iii) Alice performs a measurement in the same basis as the one in which she was originally preparing; (iv) Alice sends a classical message to Bob which depends on her (random) measurement outcome and the state that she wanted to send.[k] The security equivalence between Alice preparing & sending a state and the EPR version has been shown in the context of QKD [26, 27] and has been the basis for the proof framework of Renner et al. [28, 11].

CPTP maps for the EPR formulation of QKR.

Eve prepares a high-dimensional state $\rho^{\rm ABE}$, gives subsystem A to Alice and B to Bob, and keeps E herself. Alice's subsystem is an n-qubit space, and Bob's subsystem likewise. The AB system can be seen as n noisy EPR pairs, with the purification held by Eve. Alice and Bob first execute an initialisation procedure $\mathcal{I}$ which prepares the message and the key in the 'MK' quantum subsystem. Then Alice acts on the MKA system with a measurement that acts like $\mathsf{QKR.Encr}$ (Def. 3) and results in a random outcome. She sends some classical data to Bob, which depends on m, k, and the random outcome; effectively this turns the B system into the cipherstate as specified by $\mathsf{QKR.Encr}$. E is Eve's quantum side information. The $\mathsf{QKR.Decr}$ acts on the KB system. One detail remains to complete the translation from the original prepare-send-measure description to the EPR version. If the cipherstate in Def. 3 comprises a classical part T ('transcript') then (i) Alice sends t to Bob over a classical channel; (ii) the 'F' system in Section 4.2 consists of T and E.

In what follows, the notation $\mathcal{E}(\rho^{\rm ABE})$ stands for the CPTP map $\mathsf{QKR.Refresh} \circ \mathsf{QKR.Decr} \circ \mathsf{QKR.Encr} \circ \mathcal{I}$ acting on the AB part of $\rho^{\rm ABE}$. The output is $\mathcal{E}(\rho^{\rm ABE}) = \rho^{MKM'\tilde{K}T\Omega{\rm E}}$. The different nature of the KR and UE property forces us to introduce additional notations. On the one hand, we write $\mathcal{E}_{\rm UE} = {\rm tr}_{M'} \circ \mathcal{E}$, so that $\mathcal{E}_{\rm UE}(\rho^{\rm ABE}) = \rho^{MK\tilde{K}T\Omega{\rm E}}$. On the other hand we write $\mathcal{E}_{\rm KR} = {\rm tr}_{KM'} \circ \mathcal{E}$, with $\mathcal{E}_{\rm KR}(\rho^{\rm ABE}) = \rho^{M\tilde{K}T\Omega{\rm E}}$. Furthermore we introduce the notation $\mathcal{E}_{\rm UE}^{\tt accept}$ for $\mathcal{E}_{\rm UE}$ followed by selecting the $\Omega = 1$ part of the state, and similarly $\mathcal{E}_{\rm UE}^{\tt reject}$[l].

The 'ideal' version of $\mathcal{E}$ is denoted as $\mathcal{F}$, with notations $\mathcal{F}_{\rm UE}$, $\mathcal{F}_{\rm UE}^{\tt accept}$ and $\mathcal{F}_{\rm KR}$ defined as for $\mathcal{E}$. The $\mathcal{F}$ is 0-ENC, 0-KR and 0-UE. The $\mathcal{F}$ satisfies $\mathcal{F}_{\rm KR}(\rho^{\rm ABE}) = \sum_{m\in\mathcal{M}} \Pr[M = m] \sum_{\tilde{k}\in\mathcal{K}} \frac{1}{|\mathcal{K}|} |m\tilde{k}\rangle\langle m\tilde{k}| \otimes {\rm tr}_{M\tilde{K}} \mathcal{E}_{\rm KR}(\rho^{\rm ABE})$, $\mathcal{F}_{\rm UE}^{\tt reject} = \mathcal{E}_{\rm UE}^{\tt reject}$, and $\mathcal{F}_{\rm UE}^{\tt accept}(\rho^{\rm ABE})$

[k] Consider Alice who in the original prepare-and-send formulation wants to send a bit x encoded as $|\psi_x^b\rangle$ in some basis b. In the EPR setting, Alice measures her own part of the EPR pair in basis b. Alice gets a random result $s \in \{0, 1\}$; she sends $x \oplus s$, which informs Bob whether his state is a 'flipped' version of the one that Alice wants to send.

[l] $\mathcal{E}_{\rm UE}^{\rm accept}$ and $\mathcal{E}_{\rm UE}^{\tt reject}$ are not trace-preserving.

$= \sum_{m\in\mathcal{M}} \Pr[M=m]|m\rangle\langle m| \otimes \mathrm{tr}_M \mathcal{E}_{\rm UE}^{\tt accept}(\rho^{\rm ABE})$. [m]

We consider again the sequence of N chunks. The KR property must hold in the first $N-1$ rounds. The ENC and UE property must hold in all rounds. The following condition implies that the 0-KR and 0-UE properties hold except with probability ε,

$$\forall_{j\in\{1,\ldots,N\}} \quad \left\| \mathcal{E}_{\rm UE}^{(j)} \circ \mathcal{E}_{\rm KR}^{(j-1)} \circ \cdots \circ \mathcal{E}_{\rm KR}^{(1)} \;-\; \mathcal{F}_{\rm UE}^{(j)} \circ \mathcal{F}_{\rm KR}^{(j-1)} \circ \cdots \circ \mathcal{F}_{\rm KR}^{(1)} \right\|_\diamond \leq \varepsilon, \tag{13}$$

where the superscript is the round index. We can arrive at a simplified statement using the following lemma.

Lemma 4 *For any CPTP maps $\mathcal{A},\mathcal{A}',\mathcal{B},\mathcal{B}'$, it holds that*

$$\|\mathcal{A}\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}'\|_\diamond \quad\leq\quad \|\mathcal{A}-\mathcal{A}'\|_\diamond + \|\mathcal{B}-\mathcal{B}'\|_\diamond. \tag{14}$$

Proof:

$$\begin{aligned} \|\mathcal{A}\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}'\|_\diamond &= \|\mathcal{A}\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}' + \mathcal{A}'\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}\|_\diamond & (15)\\ &\leq \|(\mathcal{A}-\mathcal{A}')\circ\mathcal{B}\|_\diamond + \|\mathcal{A}'\circ(\mathcal{B}-\mathcal{B}')\|_\diamond & (16)\\ &\leq \|\mathcal{A}-\mathcal{A}'\|_\diamond + \|\mathcal{B}-\mathcal{B}'\|_\diamond & (17) \end{aligned}$$

where the last inequality holds because a CPTP map can never increase the trace distance. □

Using Lemma 4 it is easily seen that the following condition implies (13),

$$(N-1)\|\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR}\|_\diamond + \|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond \leq \varepsilon. \tag{18}$$

It is therefore sufficient to upper bound the single-round quantities $\|\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR}\|_\diamond$ and $\|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond$,

$$\begin{aligned} \|\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR}\|_\diamond &= \frac{1}{2}\sup_{\rho^{\rm ABE}} \left\| \mathcal{E}_{\rm KR}(\rho^{\rm ABE}) - \mathbb{E}_{m\tilde{k}} |m\tilde{k}\rangle\langle m\tilde{k}| \otimes \mathrm{tr}_{\,M\tilde{K}}\, \mathcal{E}_{\rm KR}(\rho^{\rm ABE}) \right\|_1 & (19)\\ \|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond &= \frac{1}{2}\sup_{\rho^{\rm ABE}} \left\| \mathcal{E}_{\rm UE}^{\tt accept}(\rho^{\rm ABE}) - \mathbb{E}_m |m\rangle\langle m| \otimes \mathrm{tr}_{\,M}\, \mathcal{E}_{\rm UE}^{\tt accept}(\rho^{\rm ABE}) \right\|_1. & (20) \end{aligned}$$

5 The proposed scheme

5.1 Structure

We propose a qubit-based prepare-and-measure scheme for Unclonable Encryption with Key Recycling. It consists of two components: (i) a core part that we call KRUE, which protects the message, and (ii) a quantum key recycling scheme QKR for refreshing some of the keys.

KRUE involves two passes: one from Alice to Bob, followed by a short feedback message from Bob to Alice. We do not specify QKR, but only demand that it is likewise a two-pass scheme.

We denote the composition of KRUE and QKR as “KRUE+QKR”. This composition is a two-pass protocol, defined as follows.

1. Alice sends the first pass of KRUE and the first pass of QKR together.

[m] 0-ENC and 0-KR follow from Lemma 2. Given 0-ENC the behaviour of $\mathcal{E}_{\rm UE}$ in case of `reject` is already ideal.

2. Bob sends the second pass of KRUE and the second pass of QKR together.
3. Alice and Bob both execute QKR.Refresh and then KRUE.Refresh.

If KRUE has `accept` but QKR has `reject` then QKR is re-run again on its own until it succeeds. This is safe since QKR serves only to transport random keys for the next round.

Note that it is possible, without loss of security, to run QKR 'in the background' to transport key material. Our motivation for the parallel structure is to reduce the total number of communication rounds.

5.2 KRUE *building blocks*

KRUE consists of publicly known algorithms Gen, Encr, Decr and Refresh. It works with bit-lengths λ, ℓ, k, and n which are publicly known. KRUE needs the following ingredients, which Alice and Bob have agreed on beforehand.

- A set $\mathcal{B}$ of measurement bases. In particular the BB84 set consisting of the standard basis and the Hadamard basis, or the 6-state set consisting of the bases in the $\pm x$, $\pm y$, $\pm z$ direction.
- An information-theoretically secure MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^{\ell-\lambda} \to \{0,1\}^\lambda$, outputting a tag τ of length λ, where λ is the security parameter. For an adversary who does not know the key, the probability of forgery is $2^{-\lambda}$.
- The pairwise independent hash families $\{F_u\} : \{0,1\}^k \to \{0,1\}^k$ and $\{\Phi_u\} : \{0,1\}^k \to \{0,1\}^\ell$ as discussed in Section 3.2. We use the $\{\Phi_u\}$ for privacy amplification in the 'standard' way, except that Alice is now able to choose the outcome of the hashing.
- A binary linear error correcting code which has encoding function $\text{Enc} : \{0,1\}^k \to \{0,1\}^n$ in systematic form and decoding function $\text{Dec} : \{0,1\}^n \to \{0,1\}^k$. The code is built to correct bit error rate β with certainty. (The distance of the code is $2\beta n$.) Asymptotically the codeword length n as a function of k and β is given by $n \to \frac{k}{1-h(\beta)}$.

5.3 KRUE *protocol steps*

In round j, Alice wants to send a message $\mu_j \in \{0,1\}^{\ell-\lambda}$. We will often drop the index j for notational brevity. The protocol steps are described below. Section 5.4 lists some of the considerations that lie at the basis of this protocol design.

KRUE.Gen:

The KRUE.Gen generates the shared key material between Alice and Bob. This consists of a mask $z \in \{0,1\}^\ell$, a MAC key $k_{\text{MAC}} \in \{0,1\}^\lambda$, a basis sequence $b \in \mathcal{B}^n$, keys $\varphi_0, \varphi_1 \in \{0,1\}^\lambda$ for authenticating the feedback bit, a key $u \in \{0,1\}^{2k}$ for universal hashing and a key $e \in \{0,1\}^{n-k}$ to mask the redundancy bits. Alice and Bob furthermore have a reservoir of spare key material (k_{rej}) from which to refresh key material in case of `reject`.

The protocol steps are listed below and depicted in Fig. 1.

KRUE.Encr:

Alice generates a random string $r \in \{0,1\}^{k-\ell}$. She computes the authentication tag $\tau = \Gamma(k_{\text{MAC}}, \mu)$, the augmented message $m = \mu \| \tau$, the ciphertext $c = z \oplus m$, the reversed privacy amplification $p = F_u^{\text{inv}}(c\|r) \in \{0,1\}^k$ and the qubit payload $x = \text{Enc}(p) \oplus (\vec{0}^k \| e) \in \{0,1\}^n$. She prepares $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{x_i}^{b_i}\rangle$ and sends it to Bob.

KRUE.Decr:

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 $\hat{\mu} \| \hat{\tau} = \hat{c} \oplus z$. He sets $\omega = 1$ (`accept`) if $\Gamma(k_{\mathrm{MAC}}, \hat{\mu}) == \hat{\tau}$ and the ECC decoding did not abort, otherwise $\omega = 0$ (`reject`). He sends φ_ω to Alice; Alice deduces ω from Bob's feedback, or aborts if she does not receive either φ_0 or φ_1.

<u>KRUE.Refresh</u>:
Alice and Bob perform the following actions (a tilde denotes the key for the next round):
— Re-use $b, u, k_{\mathrm{MAC}}, \varphi_{\overline{\omega}}$.
— Refresh φ_ω, e to entirely new $\tilde{\varphi}_\omega, \tilde{e}$ using an external mechanism.
— In case of `accept` re-use z. In case of `reject` take fresh $\tilde{z}$ from k_{rej}.

After round N, according to the attacker model, all keys from all rounds leak[n] except for masks z associated with `reject` events. I.e. what leaks is: b, u, k_{MAC}, $\{\varphi_0^{(j)}, \varphi_1^{(j)}, e^{(j)}\}_{j=1}^N$, and if round N was `accept` also $z^{(N)}$.

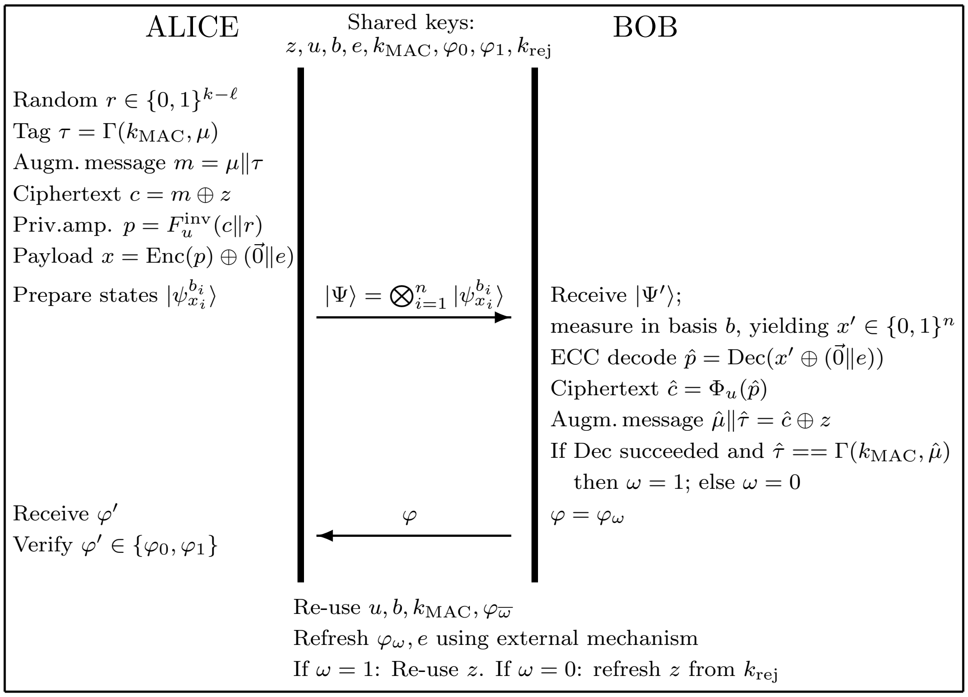
ALICE
Shared keys:
$z, u, b, e, k_{\mathrm{MAC}}, \varphi_0, \varphi_1, k_{\mathrm{rej}}$
BOB
Random $r \in \{0,1\}^{k-\ell}$
Tag $\tau = \Gamma(k_{\mathrm{MAC}}, \mu)$
Augm. message $m = \mu \| \tau$
Ciphertext $c = m \oplus z$
Priv.amp. $p = F_u^{\mathrm{inv}}(c \| r)$
Payload $x = \mathrm{Enc}(p) \oplus (\vec{0} \| e)$
Prepare states $|\psi_{x_i}^{b_i}\rangle$
$|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{x_i}^{b_i}\rangle$
Receive $|\Psi'\rangle$;
measure in basis b, yielding $x' \in \{0,1\}^n$
ECC decode $\hat{p} = \mathrm{Dec}(x' \oplus (\vec{0} \| e))$
Ciphertext $\hat{c} = \Phi_u(\hat{p})$
Augm. message $\hat{\mu} \| \hat{\tau} = \hat{c} \oplus z$
If Dec succeeded and $\hat{\tau} == \Gamma(k_{\mathrm{MAC}}, \hat{\mu})$
then $\omega = 1$; else $\omega = 0$
Receive φ'
Verify $\varphi' \in \{\varphi_0, \varphi_1\}$
φ
$\varphi = \varphi_\omega$
Re-use $u, b, k_{\mathrm{MAC}}, \varphi_{\overline{\omega}}$
Refresh φ_ω, e using external mechanism
If $\omega = 1$: Re-use z. If $\omega = 0$: refresh z from k_{rej}

Fig. 1. *A single round of* KRUE.

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

5.4 Design rationale

The rationale behind the various design choices in our scheme is as follows.

- The payload $x \in \{0,1\}^n$ needs to be uniform (as seen by Eve), otherwise Eve can get information about the basis b from the qubit states $|\psi^{b_i}_{x_i}\rangle$. Uniformity is most difficult to achieve in the case of known plaintext μ. We make x uniform in three steps. The z masks the ℓ bits of $m \in \{0,1\}^\ell$; then appending r increases that to k bits; finally the e masks the $n-k$ redundancy bits. Here we need that the error-correcting code is in systematic form.
- The tag τ allows Bob to verify if the received string m has been manipulated.
- The UE property holds for the following reason. After the keys have been revealed, Eve extracts partial information about x from her quantum system. If x itself was a ciphertext, she would be able to perform decryption and thus obtain some non-negligible amount of information about the plaintext. However, the actual ciphertext c is obtained from x by a privacy amplification step (similar to QKD), and hence Eve knows almost nothing about the ciphertext.
- The usual steps of information reconciliation (error correction Enc,Dec) and privacy amplification (Φ_u) are performed. What is special here is that we do not want the outcome of the hash Φ_u to be random, but equal to some target value c. For this reason we are applying the construction of Section 3.2 with the truncation of the invertible F_u.
- We want to re-use the basis b in unmodified form. Our definition of the KR property (Def. 5) demands that Eve learns next to nothing about b, with a formulation in terms of a trace distance, until we let b leak after round N. This requirement is impossible to satisfy if Eve has access to the feedback bit ω. She may make a guess for b in a small number of qubit positions, just small enough to be on the edge of the ECC's error-correction capability, measure those qubits in the guessed bases and forward the resulting state to Bob. Observing ω then yields non-negligible information about b. In order to avoid this problem we encrypt ω temporarily. Bob's feedback φ_ω simultaneously encrypts and authenticates ω. (Note that all ω's are revealed after round N, because all keys leak eventually.) The keys φ_0, φ_1 essentially form a single-use random codebook.
- It is always safe to re-use the key $k_{\rm MAC}$ and the seed u. Intuitively this is clear from the fact that z, e, r together entirely mask the relation between the payload x and the augmented message m. Since the tag is part of m, the $k_{\rm MAC}$ can safely be re-used when m is secure.
- The reason for doing the refreshment of φ_ω, e via an *external* mechanism is that it would be inefficient to send them via Unclonable Encryption. These keys are revealed after round N, so they do not need the extra level of protection. In Section 7.6 we study the case where $\tilde{\varphi}_\omega, \tilde{e}$ are sent as part of μ; it turns out that this causes a severe penalty on the rate.

Remark. It is possible to send the *current*-round e via QKR instead of the next-round key $\tilde{e}$. This would make e into a short-term variable instead of a long-term key, and would make it possible to elegantly use Lemma 3 in the security proof of KRUE. However, it would also complicate the security analysis of the *combined* scheme. We will not pursue this possibility.

5.5 Correctness

It is straightforward to see that KRUE satisfies $2^{-\lambda}$-correctness as defined in Section 4.2. Bob only `accepts` (sets $\omega = 1$) if the reconstructed tag successfully authenticates the reconstructed plaintext $\hat{\tau} == \Gamma(k_{\rm MAC}, \hat{\mu})$. The information-theoretically secure MAC and Eve's ignorance of $k_{\rm MAC}$ then guarantee that $\Pr[\Omega = 1 \wedge M' \neq M] \leq 2^{-\lambda}$. Furthermore, if Eve's interference on the quantum channel results in fewer than $n\beta$ bit flips then the error correction takes care of the noise, resulting in $\Pr[\Omega = 1 \wedge M' = M] = 1$.

6 EPR version of KRUE

The security proof (Section 7) will be based on the EPR variant of the scheme. Here we first present the EPR version of KRUE (see Fig. 2) and its description in terms of CPTP maps.

6.1 Protocol steps in the EPR version

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. Then Alice measures her qubits in the basis $b \in \mathcal{B}^n$, resulting in a string $s \in \{0,1\}^n$. Bob too measures his qubits in basis b, which yields $t \in \{0,1\}^n$.[o] Alice computes x as specified in Section 5.3, 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 5.3. KRUE.Refresh is performed as before.

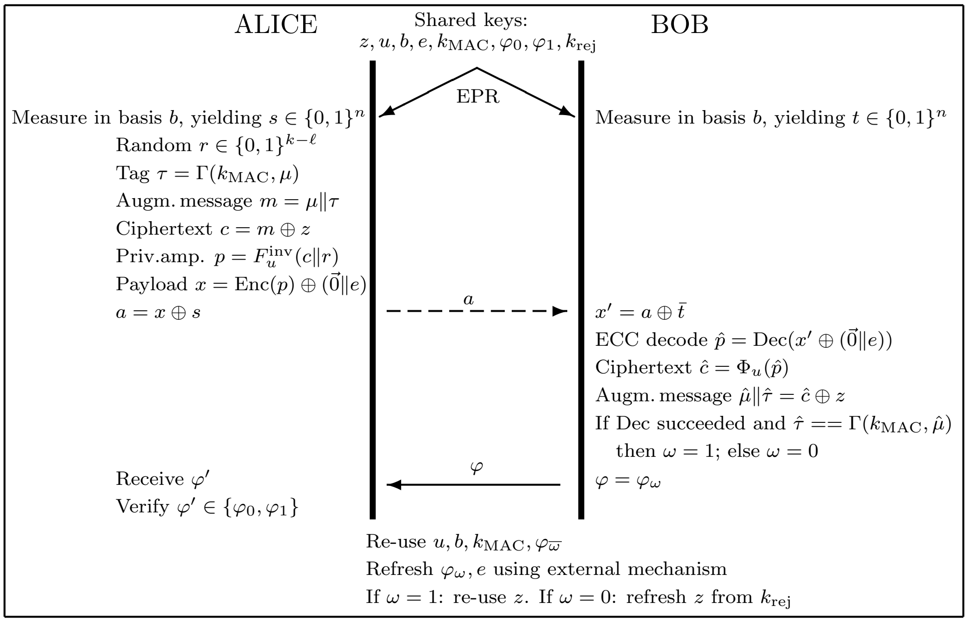
ALICE
Shared keys:
$z, u, b, e, k_{\rm MAC}, \varphi_0, \varphi_1, k_{\rm rej}$
BOB
EPR
Measure in basis b, yielding $s \in \{0,1\}^n$
Random $r \in \{0,1\}^{k-\ell}$
Tag $\tau = \Gamma(k_{\rm MAC}, \mu)$
Augm. message $m = \mu \| \tau$
Ciphertext $c = m \oplus z$
Priv.amp. $p = F_u^{\rm inv}(c\|r)$
Payload $x = {\rm Enc}(p) \oplus (\vec{0}\|e)$
$a = x \oplus s$
a
Measure in basis b, yielding $t \in \{0,1\}^n$
$x' = a \oplus \bar{t}$
ECC decode $\hat{p} = {\rm Dec}(x' \oplus (\vec{0}\|e))$
Ciphertext $\hat{c} = \Phi_u(\hat{p})$
Augm. message $\hat{\mu}\|\hat{\tau} = \hat{c} \oplus z$
If Dec succeeded and $\hat{\tau} == \Gamma(k_{\rm MAC}, \hat{\mu})$
then $\omega = 1$; else $\omega = 0$
φ
$\varphi = \varphi_\omega$
Receive φ'
Verify $\varphi' \in \{\varphi_0, \varphi_1\}$
Re-use $u, b, k_{\rm MAC}, \varphi_{\overline{\omega}}$
Refresh φ_ω, e using external mechanism
If $\omega = 1$: re-use z. If $\omega = 0$: refresh z from $k_{\rm rej}$

Fig. 2. *EPR version of* KRUE. *The dashed line is a communication that is public but cannot be altered by Eve.*

[o] If the EPR pairs are noiseless then $t = \bar{s}$; the inversion occurs because we work with singlet states.

Notation	*Meaning*
$a \in \{0,1\}^n$	bitmap from random s (EPR) to payload x
$b \in \mathcal{B}^n$	measurement basis
$\mathcal{B}$	set of qubit bases
β	ECC correctable error rate
$c \in \{0,1\}^\ell$	ciphertext; $c = m \oplus z$
$e \in \{0,1\}^{n-k}$	mask for the ECC redundancy bits
F	pairwise independent hash
Φ	truncated version of F
$\varphi_0, \varphi_1 \in \{0,1\}^\lambda$	authentication tags for the feedback bit ω
$\gamma \in [0, \frac{1}{2}]$	bit error prob. caused by Eve
Γ	MAC function
h	entropy function
k	ECC message length
$k_{\text{MAC}} \in \{0,1\}^\lambda$	MAC key for Alice's message tag
ℓ	length of message + tag
λ	tag length; security parameter
$m \in \{0,1\}^\ell$	augmented message $\mu \Vert \tau$
$\mu \in \{0,1\}^{\ell-\lambda}$	Alice's message
n	number of qubits; ECC codeword length
N	number of rounds
$\omega \in \{0,1\}$	reject/accept feedback bit
$p \in \{0,1\}^k$	temporary variable; ECC message
$r \in \{0,1\}^{k-\ell}$	randomness for privacy amplification
$s \in \{0,1\}^n$	Alice's measurement outcome (EPR)
$t \in \{0,1\}^n$	Bob's measurement outcome (EPR)
$\tau \in \{0,1\}^\lambda$	tag
$u \in \{0,1\}^{2k}$	hash seed
$x \in \{0,1\}^n$	'payload'; data encoded in the qubits
$z \in \{0,1\}^\ell$	One Time Pad for the augmented message

6.2 CPTP maps for the EPR version of KRUE

We specify the CPTP maps which represent the actions of Alice and Bob executed on the noisy EPR pairs. We follow Section 4.3 and fill in the specific variables that make up the abstract 'K' and 'T'. We start with $\mathcal{E}_{\text{UE}}$ and write $\mathcal{E}_{\text{KR}} = \mathcal{T}_{\text{KR}} \circ \mathcal{E}_{\text{UE}}$, where $\mathcal{T}_{\text{KR}}$ is a partial trace operation. The $\mathcal{E}_{\text{UE}}$ can be viewed as four consecutive maps: an initialization step $\mathcal{I}$ that prepares the input variables; a measurement step $\mathcal{M}$; a post-processing step $\mathcal{P}$ representing all further computations; and a partial trace step $\mathcal{T}_{\text{UE}}$ where all variables that are not part of the output are traced away,

$$\mathcal{E}_{\text{UE}} = \mathcal{T}_{\text{UE}} \circ \mathcal{P} \circ \mathcal{M} \circ \mathcal{I}. \tag{21}$$

The initialization merely appends the input variables,

$$\mathcal{I}(\rho^{\text{ABE}}) = \mathbb{E}_{mbzue} |mbzue\rangle\langle mbzue| \otimes \rho^{\text{ABE}}. \tag{22}$$

Here b, z, u, e are uniform, but m not necessarily. The measurement acts on the classical b-register and on 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,

$$\mathcal{M}(|b\rangle\langle b| \otimes \rho^{\text{ABE}}) = \mathbb{E}_{st|b} |bst\rangle\langle bst| \otimes \rho^{\text{E}}_{bst}. \tag{23}$$

Here the distribution of s and t is governed by the precise details of the ρ^{ABE} created by Eve. Anticipating the post-selection and random-Paulis technique applied in Section 7.1 we write the effect of Eve's actions as i.i.d. noise with noise parameter γ. The marginals of s and t are uniform, while for all $j \in \{1, \dots, n\}$ it holds that $\Pr[s_j = t_j] = \gamma$.

Anticipating another simplification introduced in Section 7.1, in the formulas below we ignore the fact that the two authentication tags (τ and φ_ω) can each be forged by Eve with probability $2^{-\lambda}$; the price for this omission is paid elsewhere, namely a term $2 \cdot 2^{-\lambda}$ in the overall error of the scheme.

The flag ω is computed as a function of s and t, which we will denote as $\omega = \theta_{st}$. Then

$$\theta_{st} = \begin{cases} 1 \text{ if } |\bar{s} \oplus t| \leq n\beta \\ 0 \text{ if } |\bar{s} \oplus t| > n\beta \end{cases}. \tag{24}$$

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

$$P_{\rm corr}(n, \beta, \gamma) \stackrel{\rm def}{=} \mathbb{E}_{st}\theta_{st} = \sum_{c=0}^{\lfloor n\beta \rfloor} \binom{n}{c} \gamma^c (1-\gamma)^{n-c}. \tag{25}$$

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

$$\begin{aligned}(\mathcal{P} \circ \mathcal{M} \circ \mathcal{I})(\rho^{\rm ABE}) \ &= \mathbb{E}_{mbzuest}|mbzuest\rangle\langle mbzuest| \otimes \rho^{\rm E}_{bst} \otimes \\ &\sum_{capxx'\omega\tilde{z}} \mathbb{E}_r|capxx'\omega\tilde{z}r\rangle\langle capxx'\omega\tilde{z}r|\delta_{a,s\oplus x}\delta_{c,m\oplus z} \\ &\delta_{p,F_u^{\rm inv}(c\|r)}\delta_{x,p\|[{\rm Red}(p)\oplus e]}\delta_{x',\bar{t}\oplus a}\delta_{\omega,\theta_{st}}\big[\omega\delta_{\tilde{z}z} + \frac{\overline{\omega}}{2^\ell}\big].\end{aligned} \tag{26}$$

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 $\mathcal{T}_{\rm UE}$ 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 initially in encrypted form, but the keys φ_0, φ_1 are 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[p]

$$\begin{aligned}\mathcal{E}_{\rm UE}(\rho^{\rm ABE}) \quad &= \quad \mathbb{E}_{mbzue}\sum_{a\tilde{z}\omega}|mbzuea\tilde{z}\omega\rangle\langle mbzuea\tilde{z}\omega| \otimes \mathbb{E}_{st}\rho^{\rm E}_{bst}\sum_p 2^\ell \delta_{\Phi_u(p),m\oplus z} \\ &2^{-k}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}\delta_{\omega,\theta_{st}}\Big[\omega\delta_{\tilde{z}z} + \overline{\omega}2^{-\ell}\Big].\end{aligned} \tag{27}$$

As discussed in Section 4.2, only the `accept` part (the $\omega = 1$ part) of the idealized $\mathcal{F}_{\rm UE}$ is relevant. This is obtained as $\mathcal{F}_{\rm UE}^{\tt accept}(\rho^{\rm ABE}) = \mathbb{E}_m|m\rangle\langle m| \otimes {\rm tr}_M\mathcal{E}_{\rm UE}^{\rm accept}(\rho^{\rm ABE})$. We get

$$\begin{aligned}\mathcal{F}_{\rm UE}^{\tt accept}(\rho^{\rm ABE}) \quad &= \ \mathbb{E}_{mbzue}\sum_{a\tilde{z}}|mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z} \\ &\otimes\mathbb{E}_{st}\rho^{\rm E}_{bst}\theta_{st}\sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}\ \mathbb{E}_{m'}\delta_{\Phi_u(p),m'\oplus z}.\end{aligned} \tag{28}$$

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

$$\begin{aligned}(\mathcal{E}_{\rm UE}^{\rm accept} - \mathcal{F}_{\rm UE}^{\rm accept})(\rho^{\rm ABE}) &= \mathbb{E}_{mbzue}\sum_{a\tilde{z}}|mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z} \\ \otimes\mathbb{E}_{st}\rho^{\rm E}_{bst}\theta_{st}\sum_p 2^{\ell-k}&\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}[\delta_{\Phi_u(p),m\oplus z} - \mathbb{E}_{m'}\delta_{\Phi_u(p),m'\oplus z}].\end{aligned} \tag{29}$$

[p] Note that tracing out u or $z\tilde{z}$ in (27) 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 $z\tilde{z}$.

For the description of $\mathcal{E}_{\rm KR}$ we have to take (27) and trace out z, e, ω.

$$\mathcal{E}_{\rm KR}(\rho^{\rm ABE}) = \mathbb{E}_{mbu} 2^{-n} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathbb{E}_{st}\rho^{\rm E}_{bst}\Big[\theta_{st}\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde{z}} + 2^{-\ell}\overline{\theta_{st}}\Big]. \quad (30)$$

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

$$\mathcal{F}_{\rm KR}(\rho^{\rm ABE}) = \mathbb{E}_{mbu}2^{-n-\ell}\sum_{a\tilde{z}}|mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathbb{E}_{st}\mathbb{E}_{b'}\rho^{\rm E}_{b'st}. \quad (31)$$

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

Lemma 5 *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 5 allows us to write

$$(\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR})(\rho^{\rm ABE}) = \mathbb{E}_{mbu}2^{-n-\ell}\sum_{a\tilde{z}}|mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathbb{E}_{st}\rho^{\rm E}_{bst}\theta_{st}[2^{\ell}\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde{z}} - 1]. \quad (32)$$

7 Security proof

7.1 Proof technique

We work in the proof framework developed by Renner et al. [11, 28]. We give a security proof for the EPR version of the protocol, making use of Post-selection (Section 3.3) and the random-Pauli noise symmetrisation technique (Section 3.4). Security of the EPR version implies security of the prepare-and-measure protocol of Section 5.3.

We are allowed to use Post-selection because KRUE is invariant under permutation of the EPR pairs. The permutation invariance follows from the following two observations. (i) The initialisation procedure $\mathcal{I}$ which creates the shared keys and the message (variables that could potentially break permutation symmetry), occurs *after* Eve has sent out the 'A' and 'B' subsystems. Hence, Eve has to perform her entanglement at a moment when none of the protocol variables yet exist. (ii) A permutation re-arranges the noise in the observed strings s and t over the bit positions $\{1, \ldots, n\}$, which could potentially break the symmetry; 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, i.e. the probability distributions of all the random variables remain the same. 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.[q]

[q] In 8-state encoding [29], applying a Pauli matrix modifies the basis b in a way known to Alice and Bob. Again, this does not affect the probability distribution of b.

In our analysis we will use λ as the security parameter, i.e. we will strive to make all diamond distances smaller than $2^{-\lambda}$. In the asymptotics this will not always be explicitly visible, as λ drops out of the expressions for asymptotic rate.

7.2 Intermezzo: QKD asymptotics

In Appendix 1, we consider a version of QKD where privacy amplification is implemented as in Section 5.3, and the syndrome is sent to Bob in OTP'ed form; we show that this leads to a bound of the form

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond \leq \tfrac{1}{2}\mathbb{E}_{mbu}\frac{1}{2^{n+\ell}}\sum_{ac}\left\|\mathbb{E}_{st}\rho^{\rm E}_{bst}\theta_{st}2^{\ell}[\delta_{c,m\oplus\Phi_u(a\oplus s)}-\mathbb{E}_{m'}\delta_{c,m'\oplus\Phi_u(a\oplus s)}]\right\|_1, \quad (33)$$

which after some algebra gives rise to

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond \leq \min\Big(P_{\rm corr}, \frac{1}{2}\mathbb{E}_b {\rm tr}\sqrt{2^{\ell}\mathbb{E}_{ss'}\delta_{ss'}\rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}}\Big), \quad (34)$$

and that from (34) the well known asymptotic QKD rate is obtained: $1-2h(\beta)$ for BB84 [15] and $1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})$ for 6-state QKD [11]. If the syndrome ($\sigma = \texttt{Syn}\,x$) is sent in the clear, the right hand side of (33) 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 (34) is an extra factor 2^{n-k} under the square root; while this alteration reduces ℓ by an amount $n-k$, it has no effect on the rate since spending key material to OTP the syndrome would incur a penalty of exactly the same size.

7.3 Security of KRUE*; qubit expenditure*

We are now ready to prove the security of KRUE. We first show that when the fraction ℓ/n approaches the asymptotic key generation rate of QKD with one-way postprocessing[r], KRUE satisfies ENC, KR and UE. In Section 7.4 we analyse the reduction of the rate due to the use of QKR as the external mechanism. Both KRUE and the composition KRUE+QKR have $\kappa = 0$ in Definition 4. The rate directly follows from the number of qubits used.

Since our analysis focuses on the asymptotics, it is not necessary to specify security parameters in detail. It suffices to state that KRUE has to satisfy the ENC, KR, and UE properties with some arbitrary 'epsilon' error values that are small but constant, i.e. do not increase when ℓ is sent to infinity. Similarly, for the composition with QKR we only have to show that the error of the combined scheme is still constant. That being said, our results allow for a non-asymptotic analysis as well, but we leave this for future work since it would require too much space.

In KRUE there are two authentication tags. Each of these has forgery probability $2^{-\lambda}$. In the diamond norm formalism we can say that we are at trace distance $2\cdot 2^{-\lambda}$ away from ideality. Thus we can pretend that the two tags cannot be forged and simply add a constant penalty $2\cdot 2^{-\lambda}$ to the error. The penalty term does not affect the asymptotics. This procedure allows us to write the CPTP maps for the protocol in a simplified form as in Section 6.2, i.e. not needing various case distinctions due to accidentally successful forgeries.

Theorem 1 *Asymptotically, the* KRUE *protocol can satisfy the ENC, KR and UE properties as defined in Section 4.2 with any fixed security parameter while achieving the following*

[r] As opposed to QKD protocols with more passes that allow Alice and Bob to perform advantage distillation, which yields a higher rate.

ratio $r = \ell/n$,

$$r^{\mathsf{KRUE}}_{\rm 4state} = r^{\rm QKD}_{\rm 4state} = 1 - 2h(\beta) \quad ; \quad r^{\mathsf{KRUE}}_{\rm 6state} = r^{\rm QKD}_{\rm 6state} = 1 - h(1 - \tfrac{3\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}). \tag{35}$$

Proof of Theorem 1: We denote the maximally achievable value of ℓ, at given n and security parameter, as $\ell_{\rm max}$. We need to determine $\ell_{\rm max}$ for both the UE and the KR property individually and take the smaller of the two. From (19) and (20) in Section 4.3 we know the ENC, KR and UE properties follow from the upper bounds on the diamond distances $\|\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR}\|_\diamond$ and $\|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond$. We bound UE-distance starting from (29) (part 1) and the KR-distance starting from (32) (part 2).

Part 1. First we note that (29) is the difference of two sub-normalised states that both have trace equal to $P_{\rm corr}$. This immediately yields the bound $\|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond \leq P_{\rm corr}$. Furthermore, from (29) we get, by using the orthogonality of the eigenspaces of the classical subsystems,

$$\begin{aligned}&\|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond = \\ &\mathbb{E}_{mbzue} \tfrac{1}{2^n} \sum_a \left\| \mathbb{E}_{st} \rho^{\rm E}_{bst} \theta_{st} \sum_p 2^{\ell+n-k} \delta_{s\oplus a, p\|[{\rm Red}(p)\oplus e]} [\delta_{\Phi_u(p), m\oplus z} - \mathbb{E}_{m'} \delta_{\Phi_u(p), m'\oplus z}] \right\|_1\end{aligned} \tag{36}$$

which resembles (33). 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 1, upon doubling as in (A.5), applying the $\mathbb{E}_u$ then yields instead of $\delta_{ss'}$ the following expression,

$$(2^{n-k})^2 \sum_{pp'} \delta_{pp'} \delta_{s\oplus a, p\|(e\oplus {\rm Red} p)} \delta_{s'\oplus a, p'\|(e\oplus {\rm Red} p')} = (2^{n-k})^2 \delta_{ss'} \delta_{e, (s\oplus a)[k+1:n] \oplus {\rm Red}((s\oplus a)[:k])}. \tag{37}$$

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 (34). Asymptotically this yields $\ell^{\rm UE,4state}_{\rm max} = n - 2nh(\beta)$ and $\ell^{\rm UE,6state}_{\rm max} = n - nh(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$.

Part 2. First we note that (32) 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 (32) we find

$$\|\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR}\|_\diamond = \tfrac{1}{2} \mathbb{E}_{mbu} \frac{1}{2^{n+\ell}} \sum_{a\tilde{z}} \left\| \mathbb{E}_{st} \rho^{\rm E}_{bst} \theta_{st} [2^\ell \delta_{\Phi_u((s\oplus a)[:k]), m\oplus \tilde{z}} - 1] \right\|_1. \tag{38}$$

This expression very closely resembles (33), 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 (A.5) and further in Appendix 1 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 $\ell^{\rm UE}_{\rm max} \leq \ell^{\rm KR}_{\rm max}$. 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 $\ell^{\rm KR}_{\rm max}/\ell^{\rm UE}_{\rm max} = \frac{(1-h)^2}{1-2h} \geq 1$. For 6-state we see $\ell^{\rm KR}_{\rm max}/\ell^{\rm UE}_{\rm max} = \frac{(1-h)(1+h-H)}{1-H} = \frac{1-H+h(H-h)}{1-H} \geq 1$. □

Remark: In the zero-noise case ($\beta = 0$) there is no mask e. Then we have, without inequalities, $\|\mathcal{E}_{\rm UE} - \mathcal{F}_{\rm UE}\|_\diamond = \|\mathcal{E}_{\rm KR} - \mathcal{F}_{\rm KR}\|_\diamond = \|\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD}\|_\diamond = \mathbb{E}_{mubza} \| \mathbb{E}_{st} \theta_{st} \rho^{\rm E}_{bst} \big[2^\ell \delta_{\Phi_u(s\oplus a), m\oplus z} - 1\big] \|_1$, i.e. the KR and UE properties reduce to QKD security.

Also note that for $\beta = 0$ we could invoke Lemma 3 to prove UE, by slightly cheating and viewing the constant-length keys φ_0, φ_1 as 'external' to the proof.

For $\beta > 0$ we are not allowed to invoke Lemma 3, since not all the key material is carried to the next round in unmodified form: upon `accept` the e is updated. The e plays an integral role in the bounding of the diamond norm (36) and cannot be moved outside that part of the proof.

7.4 Security and rate of the composition KRUE+QKR

We consider the composition of KRUE with the 'Quantum Alice and Silent Bob' QKR scheme [19], which is a two-pass protocol with the following properties: (i) its asymptotic rate equals the QKD rate; (ii) Alice's pass comprises only qubits and no classical communication.

First we show that security-wise the effect of the composition is that the errors simply add up or remain unchanged. Hence, the composition does not complicate the asymptotic analysis.

Theorem 2 *Let* QKR *be a ε_1-KR scheme in which Alice makes one pass. Let P be a ε_2-KR, ε_3-UE scheme in which Alice makes one pass. Let Q be the composition of* QKR *and P such that Alice sends her messages in parallel, and the message of* QKR *is used as key material in P. Then Q is $(\varepsilon_1 + \varepsilon_2)$-KR, and it is ε_3-UE with respect to the message of P.*

Proof: See Appendix B. □

Next, we determine the asymptotic rate of KRUE+QKR. Due to the additional qubits spent in QKR, the rate is lower than the $\frac{\ell}{n}$ fraction of KRUE (and therefore lower than the QKD rate).

Theorem 3 *The asymptotic rate of the composed scheme* KRUE+QKR *in the case of 4-state and 6-state encoding is given by*

$$r^{\mathsf{KRUE+QKR}}_{\rm 4state} = \frac{[1-2h(\beta)]^2}{1-h(\beta)} \quad ; \quad r^{\mathsf{KRUE+QKR}}_{\rm 6state} = \frac{[1-h(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})]^2}{1-h(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}) + h(\beta)}. \tag{39}$$

Proof: Let $\mu \in \{0,1\}^L$. Sending μ via KRUE needs $n = L/r^{\mathsf{KRUE}}$ qubits. Asymptotically, the size of $\tilde{k}_{\rm OTP}$ and $\tilde{k}_{\rm fb}$ is negligible compared to $\tilde{e}$. The size of $\tilde{e}$ is $nh(\beta)$. Sending $\tilde{e}$ via QKR takes $nh(\beta)/r^{\mathsf{QKR}} = Lh(\beta)/(r^{\mathsf{QKR}} r^{\mathsf{KRUE}})$ qubits. The total number of qubits spent is $q = L/r^{\mathsf{KRUE}} + Lh(\beta)/(r^{\mathsf{QKR}} r^{\mathsf{KRUE}})$. Using $r^{\mathsf{KRUE}} = r^{\rm QKD}$ and $r^{\mathsf{QKR}} = r^{\rm QKD}$ this can be written as $q = L(r^{\rm QKD} + h(\beta))/(r^{\rm QKD})^2$. Finally the overall rate is $\frac{L}{q} = \frac{(r^{\rm QKD})^2}{r^{\rm QKD} + h(\beta)}$, with $r^{\rm QKD}$ as given in (35). □

Interestingly, the rate $r^{\mathsf{KRUE+QKR}}_{\rm 4state}$ that we achieve here is twice the rate of the composition {QKD followed by Gottesman's Unclonable Encryption scheme [1]}.[s]

[s] The rate for that combination is obtained as follows. The UE step needs $n_{\rm UE} = L/[1-2h(\beta)]$ 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 $L/(n_{\rm UE} + n_{\rm QKD}) = \frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$.

7.5 Combining KRUE *with QKD*

We briefly comment on the option of combining KRUE with a QKD scheme instead of a QKR scheme as the external mechanism. QKD spends as many qubits as QKR; hence KRUE combined with QKD achieves the rate given in Theorem 3. However, the drawback of QKD is that it is not a two-pass protocol.

7.6 KRUE**: sending key updates via* KRUE *itself*

In order to get a more 'self-contained' scheme, we study the option of *not* using an external mechanism to transport the next-round keys $\tilde{\varphi}_\omega, \tilde{e}$. Instead we reserve space in the message μ for this purpose. We refer to the resulting scheme as KRUE*. The security of KRUE* is the same as for KRUE. The rate, however, is seriously reduced, since the effective message size is now smaller by an amount $\lambda + n - k$, which asymptotically goes to $nh(\beta)$. This causes an reduction of the rate by an amount $h(\beta)$, i.e. $r^{\mathsf{KRUE}^*} = r^{\mathsf{KRUE}} - h(\beta)$.

8 Comparison to other schemes

We briefly comment on the round complexity and the asymptotic rate of the protocols proposed in this paper as compared to other schemes. The word 'round complexity' here is not to be confused with the N rounds in our protocol. For a given message chunk μ_j we count *the number of times Alice has to send something*, and refer to this number as Alice's number of *passes*.

We compare against other information-theoretically secure schemes which also do not use up[t] key material,

- **QKD+OTP**. Key establishment using Quantum Key Distribution, followed by One Time Pad classical encryption. We consider efficient QKD with negligible waste of qubits [10] 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 [4, 19]. Only a single pass by Alice is needed, since Alice and Bob already share key material.
- **QKD+[1]**. Key establishment using QKD, followed by Gottesman's Unclonable Encryption [1]. At least two passes by Alice are needed.
- **QKR+[1]**. Key establishment using QKR, followed by Gottesman's Unclonable Encryption. Only a single pass by Alice is needed when the two are performed in parallel.[u]

The scheme properties are summarised in Table 1, and the rates 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 over a noisy channel do not have the Unclonable Encryption property.

To our knowledge, the only existing scheme with an explicit proof of the UE property before our work was Gottesman's construction [1]. (And thus "QKD/QKR + [1]" was the only known way to have UE without net expenditure of key material.) Our best performing

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

[u] We don't give a proof for this combination as [1] uses a different proof technique.

	Alice	Asymptotic	
Protocol	#passes	rate (4-state)	Unclonability
QKD + OTP	2	$1-2h(\beta)$	no
QKR [4, 19]	1	$1-2h(\beta)$	no
QKD + [1]	2	$\frac{1}{2}\cdot\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
QKR + [1]	1	$\frac{1}{2}\cdot\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
KRUE*	1	$1-3h(\beta)$	yes
KRUE+QKD	2	$\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
KRUE+QKR	1	$\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes

Table 1. *Comparison of schemes that have no net expenditure of key material upon* `accept`*.*

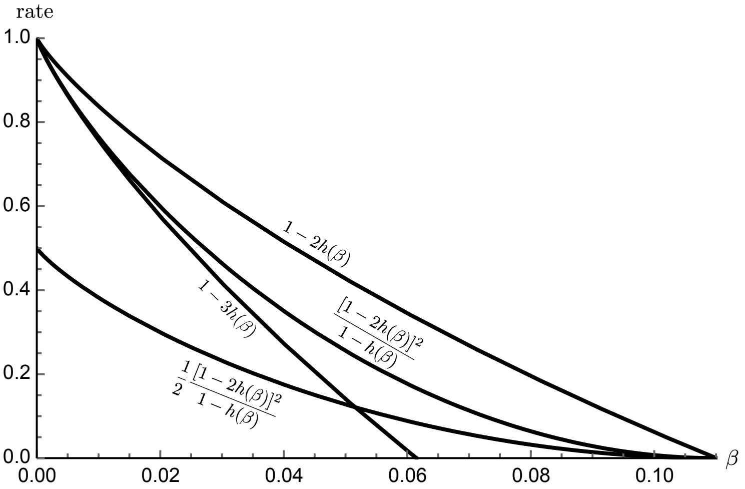

Fig. 3. *Asymptotic communication rates (4-state) as a function of the noise parameter β.*

scheme is KRUE+QKR, with one pass from Alice and double the rate of QKR + [1]. Our sub-optimal scheme KRUE* has a better rate than QKD/QKR + [1] at noise levels below $\beta \approx 0.052$.

The above comparison does not contain the key recycling schemes [17, 3], because [17] is defined only for the noiseless case $\beta = 0$, while [3] has low rate ($\leq \frac{1}{3}$) and limited noise tolerance. Note that [17] has the UE property by Lemma 3, and we suspect that [3] satisfies a version of unclonability with a somewhat modified definition that allows for a reduction of the min-entropy of some of the keys. We believe that the QKR scheme [4] can be tweaked to have the UE property by doing more privacy amplification; this would probably lead to the same rate as KRUE*.

We briefly comment on the key sizes as a function of the message length L. The keys in KRUE are the OTP $z \in \{0,1\}^\ell$, the hash seed $u \in \{0,1\}^{2k}$, the basis choice $B \in \mathcal{B}^n$, the redundancy mask $e \in \{0,1\}^{n-k}$, the authentication key $k_{\rm MAC} \in \{0,1\}^\lambda$ and the random codebook $(\varphi_0, \varphi_1) \in \{0,1\}^{2\lambda}$. Counting only contributions proportional to n, the total size in bits is $\ell + k + n + n\log\mathcal{B} + \mathcal{O}(1)$. With $L \approx \ell$, $\ell \approx r^{\rm QKD}n$, $k \approx n[1-h(\beta)]$, the key size of KRUE (in the case of 4-state encoding) is approximately $L\frac{4-3h(\beta)}{1-2h(\beta)} \geq 4L$.

Furthermore, sending $nh(\beta)$ bits via the QKR scheme [19] takes a further $4\frac{nh(\beta)}{1-2h(\beta)}$ key bits. This adds up to $L\frac{4-7h(\beta)+6[h(\beta)]^2}{[1-2h(\beta)]^2}$ as the total key size for KRUE+QKR.

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 L.

Gottesman's scheme has somewhat shorter keys, total length $L\frac{2-h(\beta)}{1-2h(\beta)}+\mathcal{O}(1)$, but it needs to refresh $\approx L/[1-2h(\beta)]$ bits every round.

9 Discussion

We have proven, in the proof framework developed by Renner et al., that quantum encryption over noisy channels can have Unclonability (as defined by Gottesman) as well as Key Recycling. The rate of KRUE, when disregarding the external mechanism, equals the QKD rate. The rate of KRUE+QKR is lower ($\frac{[1-2h(\beta)]^2}{1-h(\beta)}$ in the case of 4-state encoding), but (i) positive on the same β-interval as QKD and (ii) better than alternative schemes that achieve both UE and KR. It is an open question whether the low rate of UE schemes compared to QKD is unavoidable. The error-correction redundancy data has to be somehow protected; this requirement does not exist in QKD. Yet, the UE requirement makes it difficult to protect the redundancy, as long-term keys will leak eventually. Perhaps an error-correcting scheme like [30], which was used in [3], can help here.

Our scheme was designed by starting from QKR and making the privacy amplification a step in the computation of the qubit payload. Gottesman's construction [1] does something very similar, and hence one might try to construct a variant of KRUE that is closer to [1]. This would have the advantage that there is no longer a seed u that needs to be stored as part of the keys, as [1] 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.

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 [4], or (ii) find a way to cope with a reduced entropy of b as in [3]. 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 ω's. For a *small* accumulation (e.g. size N) we expect that it *is* realistic to hide the feedbacks temporarily.

It is of course possible to tweak KRUE in various ways to make it more efficient. It may be possible to improve on the length of the hash seed, or the length of the MAC key, or the entropy of b. We did not pursue such optimisations as our focus was on the rate.

The downside associated with encoding a message directly into qubits is the vulnerability to erasures (particle loss) on the quantum channel. Whereas QKD can just ignore erasures, in QKR they have to be compensated by the error-correcting code, which incurs a serious rate penalty. A protocol like the one proposed in section 6.2 of [4], where Alice sends qubits but Bob sends the message, could solve this problem.

Acknowledgements

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

References

1. D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581602, 2003.
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*, 13:453458, 2014. Original manuscript 1982.
3. S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Eurocrypt*, pages 311338, 2017.
4. D. Leermakers and B. Skoric. Security proof for Quantum Key Recycling with noise. *Quantum Information and Computation*, 19, 2019.
5. C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175179, 1984.
6. A.K. Ekert. Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.*, 67:661 663, 1991.
7. D. Bru. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):30183021, 1998.
8. D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.
9. P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. Phys.Rev.Lett., 85:441, 2000
10. H.-K. Lo, H.F. Chau, and M. Ardehali. Efficient Quantum Key Distribution scheme and proof of its unconditional security. *Journal of Cryptology*, 18:133165, 2005.
11. R. Renner. Security of quantum key distribution. PhD thesis, ETH Zurich, 2005.
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.*, 95:080501, 2005.
13. M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography*, volume 3378 of LNCS, pages 386406, 2005.
14. T. Sasaki, Y. Yamamoto, and M. Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509:475478, 2014.
15. M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 07 2017.
16. W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. it Nature, 299:802803, 1982.
17. I.B. Damgard, T.B. Pedersen, and L. Salvail. A Quantum Cipher with Near Optimal Key-Recycling. *CRYPTO*, 2005.
18. C. Portmann. Quantum authentication with key recycling. In Jean-Sebastien Coron and Jesper Buus Nielsen, editors, Advances in Cryptology *Eurocrypt*, 2017, pages 339368, Cham, 2017. Springer International Publishing.
19. D. Leermakers and B. Skoric. Quantum Alice and silent Bob: Qubit-based Quantum Key Recycling with almost no classical communication. *Quantum Information and Computation*, 21(1+2):118, 2021.
20. A. Broadbent and S. Lord. Uncloneable quantum encryption via random oracles. 2019. https://eprint.iacr.org/2019/257.
21. M.N. Wegman and J.W. Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22:265279, 1981.
22. M. Luby and A. Wigderson. Pairwise independence and derandomization. *Foundations and Trends in Theoretical Computer Science*, 1, 1999.
23. R.T. Moenck. Fast Computation of GCDs. In *Proceedings of the fifth annual ACM Symposium on Theory of Computing*, STOC 73, pages 142151, New York, NY, USA, 1973. ACM.
24. M. Christandl, R. Konig, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.
25. C. Portmann and R. Renner. Cryptographic security of quantum key distribution. 2014. https://arxiv.org/abs/1409.3525.
26. A.K. Ekert. Quantum cryptography based on Bells theorem. Phys.Rev.Lett., 67(6):661663, 1991.

27. C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bells theorem. *Phys. Rev. Lett.*, 68:557, 1992.
28. R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev. A*, 72:012332, 2005.
29. B. Skorič 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.
30. Y. Dodis and A. Smith. Correcting errors without leaking partial information. In ACM STOC, pages 654663, 2005.

Appendix 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 $\sigma = \texttt{Syn}(x) \in \{0,1\}^{n-k}$, 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

$$\mathcal{E}_{\rm QKD}(\rho^{\rm ABE}) = \mathbb{E}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle mbuac\omega| \otimes \mathbb{E}_{st} \rho^{\rm E}_{bst} \delta_{\omega,\theta_{st}} [\omega \delta_{c,m\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \quad \text{(A.1)}$$

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

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

The difference is given by

$$\begin{aligned} (\mathcal{E}_{\rm QKD} - \mathcal{F}_{\rm QKD})(\rho^{\rm ABE}) \quad &= \quad \mathbb{E}_{mbu} 2^{-n} \sum_{ac} |mbuac, \omega=1\rangle\langle mbuac, \omega=1| \\ &\quad \otimes \mathbb{E}_{st} \rho^{\rm E}_{bst} \theta_{st} [\delta_{c,m\oplus\Phi_u(a\oplus s)} - \mathbb{E}_{m'} \delta_{c,m'\oplus\Phi_u(a\oplus s)}]. \qquad \text{(A.3)} \end{aligned}$$

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 (A.3) it follows that

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond \leq \tfrac{1}{2}\mathbb{E}_{mbu}2^{-n-\ell}\sum_{ac}\left\|\mathbb{E}_{st}\rho^{\rm E}_{bst}\theta_{st}2^{\ell}[\delta_{c,m\oplus\Phi_u(a\oplus s)}-\mathbb{E}_{m'}\delta_{c,m'\oplus\Phi_u(a\oplus s)}]\right\|_1. \tag{A.4}$$

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

$$\tfrac{1}{2}\mathbb{E}_{mbu}2^{-n-\ell}\sum_{ac}\operatorname{tr}\Big(\mathbb{E}_{ss'tt'}\theta_{st}\theta_{s't'}\rho^{\rm E}_{bst}\rho^{\rm E}_{bs't'}2^{2\ell} \tag{A.5}$$

$$\cdot[\delta_{\Phi_u(a\oplus s),m\oplus c}-\mathbb{E}_{m'}\delta_{\Phi_u(a\oplus s),m'\oplus c}][\delta_{\Phi_u(a\oplus s'),m\oplus c}-\mathbb{E}_{m''}\delta_{\Phi_u(a\oplus s'),m''\oplus c}]\Big)^{1/2}.$$

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

$$\begin{aligned}&2^{2\ell}\mathbb{E}_{mu}[\delta_{\Phi_u(a\oplus s),m\oplus c}-\mathbb{E}_{m'}\delta_{\Phi_u(a\oplus s),m'\oplus c}][\delta_{\Phi_u(a\oplus s'),m\oplus c}-\mathbb{E}_{m''}\delta_{\Phi_u(a\oplus s'),m''\oplus c}]\\&=2^{\ell}\delta_{ss'}(1-\mathbb{E}_{mm'}\delta_{mm'})<2^{\ell}\delta_{ss'}\end{aligned} \tag{A.6}$$

which leads to

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond < \tfrac{1}{2}\mathbb{E}_b\operatorname{tr}\sqrt{2^{\ell}\mathbb{E}_{ss'tt'}\theta_{st}\theta_{s't'}\rho^{\rm E}_{bst}\rho^{\rm E}_{bs't'}\delta_{ss'}}. \tag{A.7}$$

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

$$\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond \leq \min\Big(P_{\rm corr}, \tfrac{1}{2}\mathbb{E}_b\operatorname{tr}\sqrt{2^{\ell}\mathbb{E}_{ss'}\rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}\delta_{ss'}}\Big). \tag{A.8}$$

Using Post-selection, random Paulis and smooth Rényi entropy techniques, it has been shown [11, 4] that the right hand side of (A.8) 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 $\texttt{Syn}(x)$, 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. (A.1) gains an extra part due to the syndrome σ and becomes

$$\begin{aligned}\mathcal{E}^{\rm plain}_{\rm QKD}(\rho^{\rm ABE}) \quad = \quad & \mathbb{E}_{mbu}2^{-n}\sum_{ac\sigma\omega}|mbuac\sigma\omega\rangle\langle mbuac\sigma\omega|\\ & \otimes\mathbb{E}_{st}\rho^{\rm E}_{bst}\delta_{\omega,\theta_{st}}\delta_{\sigma,\texttt{Syn}(a\oplus s)}[\omega\delta_{c,m\oplus\Phi_u(a\oplus s)}+\overline{\omega}\delta_{c\perp}].\end{aligned} \tag{A.9}$$

The factor $\delta_{\sigma,\mathtt{Syn}(a\oplus s)}$ is carried along untouched in the whole computation up to (A.5), 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 (A.6) 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}.

$$\|\mathcal{E}^{\rm plain}_{\rm QKD}-\mathcal{F}^{\rm plain}_{\rm QKD}\|_\diamond \leq \min\Big(P_{\rm corr},\, \tfrac{1}{2}\mathbb{E}_b{\rm tr}\sqrt{2^\ell 2^{n-k}\mathbb{E}_{ss'}\rho^{\rm E}_{bs}\rho^{\rm E}_{bs'}\delta_{ss'}}\Big). \tag{A.10}$$

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.

Appendix B: Proof of Theorem 2

We consider the EPR version of Q. Eve creates a state that can be written as $\rho^{\rm A_1B_1A_2B_2E}$, where the labels '1' and '2' refer to the EPR pairs intended for QKR and P respectively, and A,B refers to the EPR parts going to Alice and Bob. As in Section 4.3 we introduce different notation for the same CPTP map depending on the property that we are looking at (KR or UE). Thus we have CPTP maps $\mathcal{Q}_{\rm 1KR}$, $\mathcal{Q}_{\rm 1UE}$, $\mathcal{Q}_{\rm 2KR}$, $\mathcal{Q}_{\rm 2UE}$, with

$$(\mathcal{Q}_{\rm 2KR}\circ\mathcal{Q}_{\rm 1KR})(\rho^{\rm A_1B_1A_2B_2E}) = \mathcal{Q}_{\rm 2KR}(\rho^{M_1\tilde K_1T_1{\rm A_2B_2E}}) = \rho^{\tilde K_1T_1M_2\tilde K_2T_2{\rm E}} \tag{B.1}$$

$$(\mathcal{Q}^{\mathsf{acc}}_{\rm 2UE}\circ\mathcal{Q}_{\rm 1UE})(\rho^{\rm A_1B_1A_2B_2E}) = \mathcal{Q}^{\mathsf{acc}}_{\rm 2UE}(\rho^{M_1K_1\tilde K_1T_1{\rm A_2B_2E}}) = \rho^{M_1K_1\tilde K_1T_1M_2K_2\tilde K_2T_2{\rm E}}_{[\Omega=1]}. \tag{B.2}$$

With respect to the KR property, the ideal functionality is $\mathcal{Q}^{\rm ideal}_{\rm 2KR}\circ\mathcal{Q}^{\rm ideal}_{\rm 1KR}$. With respect to UE the ideal functionality is as follows. In case of `reject` there are no requirements. In case of `accept` the M_2 is protected by $\mathcal{Q}^{\mathsf{acc},{\rm ideal}}_{\rm 2UE}$ even if $\mathcal{Q}_{\rm 1UE}$ does not behave ideally; hence the ideal functionality is described by the mapping $\mathcal{Q}^{\mathsf{acc},{\rm ideal}}_{\rm 2UE}\circ\mathcal{Q}_{\rm 1UE}$. We have

$$\begin{aligned}(\mathcal{Q}^{\rm ideal}_{\rm 2KR}\circ\mathcal{Q}^{\rm ideal}_{\rm 1KR})(\rho^{\rm A_1B_1A_2B_2E}) &= \mathcal{Q}^{\rm ideal}_{\rm 2KR}(\rho^{M_1\tilde K_1}\otimes\rho^{T_1{\rm A_2B_2E}})\\ &= \rho^{\tilde K_1M_2\tilde K_2}\otimes\rho^{T_1T_2{\rm E}} \qquad\qquad (B.3)\\ (\mathcal{Q}^{\mathsf{acc},{\rm ideal}}_{\rm 2UE}\circ\mathcal{Q}_{\rm 1UE})(\rho^{\rm A_1B_1A_2B_2E}) &= \mathcal{Q}^{\mathsf{acc},{\rm ideal}}_{\rm 2UE}(\rho^{M_1K_1\tilde K_1T_1{\rm A_2B_2E}})\\ &= \rho^{M_2}\otimes\rho^{M_1K_1\tilde K_1T_1K_2\tilde K_2T_2{\rm E}}_{[\Omega=1]}. \qquad\qquad (B.4)\end{aligned}$$

It is given that $\|\mathcal{Q}_{\rm 1KR}-\mathcal{Q}^{\rm ideal}_{\rm 1KR}\|_\diamond\leq\varepsilon_1$, and $\|\mathcal{Q}_{\rm 2KR}-\mathcal{Q}^{\rm ideal}_{\rm 2KR}\|_\diamond\leq\varepsilon_2$, and $\|\mathcal{Q}_{\rm 2UE}-\mathcal{Q}^{\rm ideal}_{\rm 2UE}\|_\diamond\leq\varepsilon_3$. The KR property of Q follows trivially from

$$\Big\|\mathcal{Q}_{\rm 2KR}\circ\mathcal{Q}_{\rm 1KR}-\mathcal{Q}^{\rm ideal}_{\rm 2KR}\circ\mathcal{Q}^{\rm ideal}_{\rm 1KR}\Big\|_\diamond \leq \Big\|\mathcal{Q}_{\rm 1KR}-\mathcal{Q}^{\rm ideal}_{\rm 1KR}\Big\|_\diamond + \Big\|\mathcal{Q}_{\rm 2KR}-\mathcal{Q}^{\rm ideal}_{\rm 2KR}\Big\|_\diamond \leq \varepsilon_1+\varepsilon_2. \tag{B.5}$$

Finally, the UE property with regard to M_2 follows from

$$\Big\|\mathcal{Q}_{\rm 2UE}\circ\mathcal{Q}_{\rm 1UE}-\mathcal{Q}^{\rm ideal}_{\rm 2UE}\circ\mathcal{Q}_{\rm 1UE}\Big\|_\diamond \leq \Big\|\mathcal{Q}_{\rm 2UE}-\mathcal{Q}^{\rm ideal}_{\rm 2UE}\Big\|_\diamond \leq \varepsilon_3. \tag{B.6}$$