Quantum Authentication and Encryption with Key Recycling

Or: How to Re-use a One-Time Pad Even if $P = NP$ — Safely & Feasibly

Serge Fehr[1] and Louis Salvail[2⋆]

[1] Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
[2] Université de Montréal (DIRO), Montréal, Canada

Abstract. We propose an information-theoretically secure encryption scheme for classical messages with quantum ciphertexts that offers *detection* of eavesdropping attacks, and *re-usability of the key* in case no eavesdropping took place: the entire key can be securely re-used for encrypting new messages as long as no attack is detected. This is known to be impossible for fully classical schemes, where there is no way to detect plain eavesdropping attacks.
This particular application of quantum techniques to cryptography was originally proposed by Bennett, Brassard and Breidbart in 1982, even before proposing quantum-key-distribution, and a simple candidate scheme was suggested but no rigorous security analysis was given. The idea was picked up again in 2005, when Damgård, Pedersen and Salvail suggested a new scheme for the same task, but now with a rigorous security analysis. However, their scheme is much more demanding in terms of quantum capabilities: it requires the users to have a quantum computer.
In contrast, and like the original scheme by Bennett *et al.*, our new scheme requires from the honest users merely to prepare and measure single BB84 qubits. As such, we not only show the first provably-secure scheme that is within reach of current technology, but we also confirm Bennett *et al.*'s original intuition that a scheme in the spirit of their original construction is indeed secure.

1 Introduction

Background. Classical information-theoretic encryption (like the one-time pad) and authentication (like Carter-Wegman authentication) have the serious downside that the key can be re-used only a small number of times, e.g. only *once* in case of the one-time pad for encryption or a strongly universal$_2$ hash function for authentication. This is inherent since by simply *observing* the communication, an eavesdropper Eve inevitably learns a substantial amount of information on the key. Furthermore, there is no way for the communicating parties, Alice and

⋆ Funded by Canada's NSERC discovery grant and NSERC discovery accelerator.

Bob, to *know* whether Eve is present and has observed the communication or not, so they have to assume the worst.

This situation changes radically when we move to the quantum setting and let the ciphertext (or authentication tag) be a quantum state: then, by the fundamental properties of quantum mechanics, an Eve that *observes* the communicated state inevitably *changes* it, and so it is potentially possible for the receiver Bob to detect this, and, vice versa, to conclude that the key is still secure and thus can be safely re-used in case everything looks as it is supposed to be.

This idea of key re-usability by means of a quantum ciphertext goes back to a manuscript titled "*Quantum Cryptography II: How to re-use a one-time pad safely even if $P = NP$*" by Bennett, Brassard and Breidbart written in 1982. However, their paper was originally not published, and the idea was put aside after two of the authors discovered what then became known as BB84 quantum-key-distribution [2].[1] Only much later in 2005, this idea was picked up again by Damgård, Pedersen and Salvail in [5] (and its full version in [6]), where they proposed a new such encryption scheme and gave a rigorous security proof — in contrast, Bennett *et al.*'s original reasoning was very informal and hand-wavy.

The original scheme by Bennett *et al.* is simple and natural: you one-time-pad encrypt the message, add some redundancy by encoding the ciphertext using an error correction (or detection) code, and encode the result bit-wise into what we nowadays call BB84 qubits. The scheme by Damgård *et al.* is more involved; in particular, the actual quantum encoding is not done by means of single qubits, but by means of states that form a set of mutually unbiased bases in a Hilbert space of large dimension. This in particular means that their scheme requires a *quantum computer* to produce the quantum ciphertexts and to decrypt them.

Our Results. We are interested in the question of whether one can combine the simplicity of the originally proposed encryption scheme by Bennett *et al.* with a rigorous security analysis as offered by Damgård *et al.* for their scheme; in particular, whether there is a provably secure scheme that is within reach of being implementable with current technology — and we answer the question in the affirmative.

We start with the somewhat simpler problem of finding an *authentication* scheme that allows to re-use the key in case no attack is detected, and we show a very simple solution. In order to authenticate a (classical) message msg, we encode a random bit string $x \in \{0,1\}^n$ into BB84 qubits $H^\theta|x\rangle$, where $\theta \in \{0,1\}^n$ is part of the shared secret key, and we compute a tag $t = \mathsf{MAC}(k, msg\|x)$ of the message concatenated with x, where MAC is a classical information-theoretic one-time message authentication code, and its key k is the other part of the shared secret key. The qubits $H^\theta|x\rangle$ and the classical tag t are then sent along with msg, and the receiver verifies correctness of the received message in the obvious way by measuring the qubits to obtain x and checking t.

[1] A freshly typeset version of the original manuscript was then published more than 30 years later in [3].

One-time security of the scheme is obvious, and the intuition for key-recycling is as follows. Since Eve does not know θ, she has a certain minimal amount of uncertainty in x, so that, if MAC has suitable extractor-like properties, the tag t is (almost) random and *independent* of k and θ, and thus gives away no information on k and θ. Furthermore, if Eve tries to gain information on k and θ by measuring some qubits, she disturbs these qubits and is likely to be detected. A subtle issue is that if Eve measures only *very few* qubits then she has a good chance of not being detected, while still learning a little bit on θ by the fact that she has not been detected. However, as long as her uncertainty in θ is large enough this should not help her (much), and the more information on θ she tries to collect this way the more likely it is that she gets caught.

We show that the above intuition is correct. Formally, we prove that as long as the receiver Bob accepts the authenticated message, the key-pair (k, θ) can be safely re-used, and if Bob rejects, it is good enough to simply refresh θ. Our proof is based on techniques introduced in [19] and extensions thereof.

Extending our authentication scheme to an encryption scheme is intuitively quite easy: we simply extract a one-time-pad key from x, using a strong extractor (with some additional properties) with a seed that is also part of the shared secret key. Similarly to above, we can prove that as long as the receiver Bob accepts, the key can be safely re-used, and if Bob rejects it is good enough to refresh θ.

In our scheme, the description length[2] of θ is $m+3\lambda$, where m is the length of the encrypted message *msg* and λ is the security parameter (so that the scheme fails with probability at most $2^{-\lambda}$). Thus, with respect to the number of fresh random bits that are needed for the key refreshing, i.e. for updating the key in case Bob rejects, our encryption scheme is comparable to the scheme by Damgård *et al.*[3] and optimal in terms of the dependency on the message length m.

Our schemes can be made *noise robust* in order to deal with a (slightly) noisy quantum communication; the generic solution proposed in [5, 6] of using a quantum error correction code is not an option for us as it would require a quantum computer for en- and decoding. Unfortunately, using straightforward error correction techniques, like sending along the syndrome of x with respect to a suitable error correcting code, renders our proofs invalid beyond an easy fix, though it is unclear whether the scheme actually becomes insecure. However, we can deal with the issue by means of using error correction "without leaking partial information", as introduced by Dodis and Smith [8] and extended to the quantum setting by Fehr and Schaffner [9]. Doing error correction in a more standard way, which would offer more freedom in choosing the error correction code and allow for a larger amount of noise, remains an interesting open problem.

Encryption with Key Recycling vs QKD. A possible objection against the idea of encryption with key recycling is that one might just as well use QKD

[2] In our scheme, θ is not uniformly random in $\{0,1\}^n$ but is chosen to be a code word, as such, its description length is smaller than its physical bit length, and given by the dimension of the code.

[3] Their scheme needs $m+\ell$ fresh random bits for key refreshing, where ℓ is a parameter in their construction, and their scheme fails with probability approximately $2^{-\ell/2}$.

to produce a new key, rather than re-using the old one. However, there *are* subtle advantages of using encryption with key recycling instead. For instance, encryption with key recycling is (almost) non-interactive and requires only *1 bit* of authenticated feedback: "accept" or "reject", that can be provided *offline*, i.e., after the communication of the private message, as long as it is done before the scheme is re-used. This opens the possibility to provide the feedback by means of a different channel, like by confirming over the phone. In contrast, for QKD, a *large amount* of data needs to be authenticated *online* and in *both directions*. If no physically authenticated channel is available, then the authenticated feedback can actually be done very easily: Alice appends a random token to the message she communicates to Bob in encrypted form, and Bob confirms that no attack is detected by returning the token back to Alice — in plain — and in case he detected an attack, he sends a reject message instead.[4] Furthermore, encryption with key recycling has the potential to be *more efficient* than QKD in terms of communication. Even though this is not the case for our scheme, there is certainly potential, because no sifting takes place and hence there is no need to throw out a fraction of the quantum communication. Altogether, on a stable quantum network for instance, encryption with key-recycling would be the preferred choice over QKD. Last but not least, given that the re-usability of a one-time-pad-like encryption key was one of the very first proposed applications of quantum cryptography — even before QKD — we feel that giving a satisfactory answer should be of intellectual interest.

Related Work. Besides the work of Brassard *et al.* and of Damgård *et al.*, who focus on encrypting *classical* messages, there is a line of work, like [13, 15, 11], that considers key recycling in the context of authentication and/or encryption of *quantum* messages. However, common to almost all this work is that only *part* of the key can be re-used if no attack is detected, or a new but *shorter* key can be extracted. The only exceptions we know of are the two recent works by Garg *et al.* [10] and by Portmann [16], which consider and analyze authentication schemes for quantum messages that do offer re-usability of the entire key in case no attack is detected. However, these schemes are based on techniques (like unitary designs) that require the honest users to perform quantum computations also when restricting to classical messages. Actually, [16] states it as an explicit open problem to "find a prepare-and-measure scheme to encrypt and authenticate a classical message in a quantum state, so that all of the key may be recycled if it is successfully authenticated". On the other hand, their schemes offer security against *superposition attacks*, where the adversary may trick the sender into authenticating a *superposition* of classical messages; this is something we do not consider here — as a matter of fact, it would be somewhat unnatural for us since such superposition attacks require the sender (wittingly or unwittingly) to hold a quantum computer, which is exactly what we want to avoid.

[4] Of course, when Bob sends back the token to confirm, Eve can easily replace it by the reject message and so prevent Alice and Bob from finding agreement, but this is something that Eve can always achieve by "altering the last message", also in QKD.

2 Preliminaries

2.1 Basic Concepts of Quantum Information Theory

We assume basic familiarity; we merely fix notation and terminology here.

QUANTUM STATES. The state of a quantum system with state space $\mathcal{H}$ is specified by a *state vector* $|\varphi\rangle \in \mathcal{H}$ in case of a pure state, or, more generally in case of a mixed state, by a *density matrix* ρ acting on $\mathcal{H}$. The set of density matrices acting on $\mathcal{H}$ is denoted $\mathcal{D}(\mathcal{H})$. We typically identify different quantum systems by means of labels A, B etc., and we write ρ_{A} for the state of system A and $\mathcal{H}_{\mathsf{A}}$ for its state space, etc. The joint state of a bipartite system AB is given by a density matrix ρ_{AB} in $\mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$; it is then understood that ρ_{A} and ρ_{B} are the respective *reduced* density matrices $\rho_{\mathsf{A}} = \mathrm{tr}_{\mathsf{B}}(\rho_{\mathsf{AB}})$ and $\rho_{\mathsf{B}} = \mathrm{tr}_{\mathsf{A}}(\rho_{\mathsf{AB}})$.

We also consider states that consist of a classical and a quantum part. Formally, $\rho_{X\mathsf{E}} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_{\mathsf{E}})$ is called a *cq*-state (for *c*lassical-*q*uantum), if it is of the form

$$\rho_{X\mathsf{E}} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \rho^x_{\mathsf{E}} \ ,$$

where $P_X : \mathcal{X} \to [0,1]$ is a probability distribution, $\{|x\rangle\}_{x\in\mathcal{X}}$ is a fixed orthonormal basis of $\mathcal{H}_X$, and $\rho^x_{\mathsf{E}} \in \mathcal{D}(\mathcal{H}_{\mathsf{E}})$. Throughout, we will slightly abuse notation and express this by writing $\rho_{X\mathsf{E}} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}})$.

In the context of such a cq-state $\rho_{X\mathsf{E}}$, an *event* Λ is specified by means of a decomposition $\rho_{X\mathsf{E}} = P[\Lambda] \cdot \rho_{X\mathsf{E}|\Lambda} + P[\neg\Lambda] \cdot \rho_{X\mathsf{E}|\neg\Lambda}$ with $P[\Lambda], P[\neg\Lambda] \geq 0$ and $\rho_{X\mathsf{E}|\Lambda}, \rho_{X\mathsf{E}|\neg\Lambda} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}})$. Associated to such an event Λ is the *indicator random variable* 1_Λ, i.e., the cq-state $\rho_{X1_\Lambda\mathsf{E}} \in \mathcal{D}(\mathcal{X} \otimes \{0,1\} \otimes \mathcal{H}_{\mathsf{E}})$, defined in the obvious way. Note that, for any cq-state $\rho_{X\mathsf{E}}$ and any $x \in \mathcal{X}$, the event $X{=}x$ is naturally defined and $\rho_{X\mathsf{E}|X=x} = |x\rangle\langle x| \otimes \rho^x_{\mathsf{E}}$ and $\rho_{\mathsf{E}|X=x} = \rho^x_{\mathsf{E}}$.

If a state ρ_X is purely classical, meaning that $\rho_X = \sum_x P_X(x)|x\rangle\langle x|$ and expressed as $\rho_X \in \mathcal{D}(\mathcal{X})$, we may refer to standard probability notation so that probabilities like $P[X{=}x]$ are well understood. Finally, we write $\mu_{\mathcal{X}}$ for the *fully mixed state* $\mu_{\mathcal{X}} = \frac{1}{|\mathcal{X}|}\sum_x |x\rangle\langle x| = \frac{1}{|\mathcal{X}|}\mathbb{I}_{\mathcal{X}} \in \mathcal{D}(\mathcal{X})$.

GENERAL QUANTUM OPERATIONS. Operations on quantum systems are described by *CPTP maps*. To emphasize that a CPTP map $\mathcal{Q} : \mathcal{D}(\mathcal{H}_{\mathsf{A}}) \to \mathcal{D}(\mathcal{H}_{\mathsf{A}'})$ acts on density matrices in $\mathcal{D}(\mathcal{H}_{\mathsf{A}})$, we sometimes write $\mathcal{Q}_{\mathsf{A}}$, and we say that it "acts on A". Also, we may write $\mathcal{Q}_{\mathsf{A}\to\mathsf{A}'}$ in order to be explicit about the range too. If $\mathcal{Q}$ is a CPTP map acting on A, we often abuse notation and simply write $\mathcal{Q}_{\mathsf{A}}(\rho_{\mathsf{AB}})$ or $\rho_{\mathcal{Q}(\mathsf{A})\mathsf{B}}$ for $\big(\mathcal{Q}_{\mathsf{A}} \otimes id_{\mathsf{B}}\big)(\rho_{\mathsf{AB}})$, where id_{B} is the identity map on $\mathcal{D}(\mathcal{H}_{\mathsf{B}})$.

In line with our notation for cq-states, $\mathcal{Q} : \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}}) \to \mathcal{D}(\mathcal{X}' \otimes \mathcal{H}_{\mathsf{E}'})$ is used to express that $\mathcal{Q}$ maps any cq-state $\rho_{X\mathsf{E}} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}})$ to a cq-state $\mathcal{Q}(\rho_{X'\mathsf{E}})$ in $\mathcal{D}(\mathcal{X}' \otimes \mathcal{H}_{\mathsf{E}'})$. We say that a CPTP map $\mathcal{Q} : \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}}) \to \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}'})$ is "controlled by X and acts on E" if on a cq-state $\rho_{X\mathsf{E}} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}})$ it acts as

$$\mathcal{Q}(\rho_{X\mathsf{E}}) = \sum_x P_X(x)|x\rangle\langle x| \otimes \mathcal{Q}^x(\rho^x_{\mathsf{E}})$$

with "conditional" CPTP maps $\mathcal{Q}^x : \mathcal{D}(\mathcal{H}_{\mathsf{E}}) \to \mathcal{D}(\mathcal{H}_{\mathsf{E}'})$. Note that in this case we write $\mathcal{Q}_{X\mathsf{E}\to X\mathsf{E}'}$ rather than $\mathcal{Q}_{X\mathsf{E}\to X\mathsf{E}'}$, as it is understood that $\mathcal{Q}$ keeps X alive. For concreteness, we require that such a $\mathcal{Q}$ is of the form $\mathcal{Q} = \sum_x \mathcal{P}_{|x\rangle\langle x|} \otimes \mathcal{Q}^x$ where $\mathcal{P}_{|x\rangle\langle x|}(\rho) = |x\rangle\langle x|\,\rho\,|x\rangle\langle x|$ for any $\rho \in \mathcal{D}(\mathcal{H}_X)$.[5] As such, $\mathcal{Q}$ is fully specified by means of the conditional CPTP maps $\mathcal{Q}^x$. Finally, for any function $f : \mathcal{X} \to \mathcal{Y}$, we say that $\mathcal{Q} : \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}}) \to \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_{\mathsf{E}'})$ is "controlled by $f(X)$" if it is controlled by X, but $\mathcal{Q}^x = \mathcal{Q}^{x'}$ for any $x, x' \in \mathcal{X}$ with $f(x) = f(x')$.

Markov-chain states. Let $\rho_{XY\mathsf{E}} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{H}_{\mathsf{E}})$ be a cq-state with two classical subsystems X and Y. Following [7], we define $\rho_{X\leftrightarrow Y\leftrightarrow \mathsf{E}}$ to be the "Markov-chain state"

$$\rho_{X\leftrightarrow Y\leftrightarrow \mathsf{E}} := \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_{\mathsf{E}}^y$$

with $\rho_{\mathsf{E}}^y = \sum_x P_{X|Y}(x|y)\,\rho_{\mathsf{E}}^{x,y}$. If the state $\rho_{XY\mathsf{E}}$ is clear from the context we write $X \leftrightarrow Y \leftrightarrow \mathsf{E}$ to express that $\rho_{XY\mathsf{E}} = \rho_{X\leftrightarrow Y\leftrightarrow \mathsf{E}}$. It is an easy exercise to verify that the Markov-chain condition $X \leftrightarrow Y \leftrightarrow \mathsf{E}$ holds if and only if $\rho_{XY\mathsf{E}} = \mathcal{Q}_{Y\varnothing\to\mathsf{E}}(\rho_{XY})$ for a CPTP map $\mathcal{Q}_{Y\varnothing\to\mathsf{E}} : \mathcal{D}(\mathcal{Y}) \to \mathcal{D}(\mathcal{Y} \otimes \mathcal{H}_{\mathsf{E}})$ that is controlled by Y and acts on the "empty" system $\varnothing$, i.e., the conditional maps act as $\mathcal{Q}^y_{\varnothing\to\mathsf{E}} : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_{\mathsf{E}})$.

Quantum measurements. We model a *measurement* of a quantum system A with outcome in $\mathcal{X}$ by means of a CPTP map $\mathcal{M} : \mathcal{D}(\mathcal{H}_{\mathsf{A}}) \to \mathcal{D}(\mathcal{X})$ that acts as

$$\mathcal{M}(\rho) = \sum_{x\in\mathcal{X}} \mathrm{tr}(E_x\rho)|x\rangle\langle x| \ ,$$

where $\{|x\rangle\}_{x\in\mathcal{X}}$ is a fixed basis, and $\{E_x\}_{x\in\mathcal{X}}$ forms a *POVM*, i.e., a family of positive-semidefinite operators that add up to the identity matrix $\mathbb{I}_{\mathcal{X}}$. A measurement $\mathcal{M} : \mathcal{D}(\mathcal{Z} \otimes \mathcal{H}_{\mathsf{A}}) \to \mathcal{D}(\mathcal{Z} \otimes \mathcal{X})$ is said to be a "measurement of A controlled by Z" if it is controlled by Z and acts on A as a CPTP map. It is easy to see that in this case the conditional CPTP maps $\mathcal{M}^z : \mathcal{D}(\mathcal{H}_{\mathsf{A}}) \to \mathcal{D}(\mathcal{X})$ are measurements too, referred to as "conditional measurements".

Note that whenever $\mathcal{M} : \mathcal{D}(\mathcal{H}_Z \otimes \mathcal{H}_{\mathsf{A}}) \to \mathcal{D}(\mathcal{X})$ is an *arbitrary* measurement of Z and A that is applied to a cq-state $\rho_{Z\mathsf{A}} \in \mathcal{D}(\mathcal{Z} \otimes \mathcal{H}_{\mathsf{A}})$, we may assume that $\mathcal{M}$ first "produces a copy of Z", and thus we may assume without loss of generality that $\mathcal{M} : \mathcal{D}(\mathcal{Z} \otimes \mathcal{H}_{\mathsf{A}}) \to \mathcal{D}(\mathcal{Z} \otimes \mathcal{X})$ is *controlled* by Z.

For a given $n \in \mathbb{N}$, $\mathcal{M}^{\text{BB84}}_{\Theta\mathsf{A}\to X}$ denotes the *BB84 measurement* of an n-qubit system A controlled by Θ. Formally, for every $\theta \in \{0,1\}^n$ the corresponding conditional measurement is specified by the POVM $\{H^\theta|x\rangle\langle x|H^\theta\}$ with x ranging over $\{0,1\}^n$. Here, H is the *Hadamard matrix*, and $H^\theta|x\rangle$ is a short hand for $H^{\theta_1}|x_1\rangle \otimes \cdots \otimes H^{\theta_n}|x_n\rangle \in \mathcal{H}_{\mathsf{A}} = (\mathbb{C}^2)^{\otimes n}$, where $\{|0\rangle, |1\rangle\}$ is the *computational basis* of the qubit system $\mathbb{C}^2$.

[5] This means that the system X is actually measured (in the fixed basis $\{|x\rangle\}_{x\in\mathcal{X}}$).

TRACE DISTANCE. We capture the distance between two states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ in terms of their *trace distance* $\delta(\rho,\sigma) := \frac{1}{2}\|\rho-\sigma\|_1$, where $\|K\|_1 := \mathrm{tr}\big(\sqrt{K^\dagger K}\big)$ is the *trace norm* of an arbitrary operator K. If the states ρ_{A} and $\rho_{\mathsf{A}'}$ are clear from context, we may write $\delta(\mathsf{A},\mathsf{A}')$ instead of $\delta(\rho_{\mathsf{A}},\rho_{\mathsf{A}'})$. Also, for any cq-state $\rho_{X\mathsf{E}}$ in $\mathcal{D}(\mathcal{X}\otimes\mathcal{H}_{\mathsf{E}})$, we write $\delta(X,U_{\mathcal{X}}|\mathsf{E})$ as a short hand for $\delta(\rho_{X\mathsf{E}},\mu_{\mathcal{X}}\otimes\rho_{\mathsf{E}})$. Obviously, $\delta(X,U_{\mathcal{X}}|\mathsf{E})$ captures how far away X is from uniformly random on $\mathcal{X}$ when given the quantum system E.

It is well known that the trace distance is monotone under CPTP maps, and it is easy to see that if two cq-states $\rho_{X\mathsf{E}},\sigma_{X\mathsf{E}} \in \mathcal{D}(\mathcal{X}\otimes\mathcal{H}_{\mathsf{E}})$ coincide on their classical subsystems, meaning that $\rho_X = \sigma_X$, then $\delta(\rho_{X\mathsf{E}},\sigma_{X\mathsf{E}})$ decomposes into $\delta(\rho_{X\mathsf{E}},\sigma_{X\mathsf{E}}) = \sum_x P_X(x)\,\delta(\rho^x_{\mathsf{E}},\sigma^x_{\mathsf{E}})$.

2.2 The Guessing Probability

An important concept in the technical analysis of our scheme(s) is the following notion of guessing probability, which is strongly related to the (conditional) min-entropy as introduced by Renner [17], but turns out to be more convenient to work with for our purpose. Let $\rho_{X\mathsf{E}} \in \mathcal{D}(\mathcal{X}\otimes\mathcal{H}_{\mathsf{E}})$ be a cq-state.

Definition 1. *The* guessing probability *of X given E is*

$$\mathrm{Guess}(X|\mathsf{E}) := \max_{\mathcal{M}} P[\mathcal{M}(\mathsf{E})=X] \ ,$$

where the maximum is over all measurements $\mathcal{M} : \mathcal{D}(\mathcal{H}_{\mathsf{E}}) \to \mathcal{D}(\mathcal{X})$ of E with outcome in $\mathcal{X}$.[6]

Note that if Λ is an event, then $\mathrm{Guess}(X|\mathsf{E},\Lambda)$ is naturally defined by means of applying the above to the "conditional state" $\rho_{X\mathsf{E}|\Lambda} \in \mathcal{D}(\mathcal{X}\otimes\mathcal{H}_{\mathsf{E}})$.

We will make use of the following elementary properties of the guessing probability. In all the statements, it is understood that $\rho_{X\mathsf{E}} \in \mathcal{D}(\mathcal{X}\otimes\mathcal{H}_{\mathsf{E}})$, respectively $\rho_{XZ\mathsf{E}} \in \mathcal{D}(\mathcal{X}\otimes\mathcal{Z}\otimes\mathcal{H}_{\mathsf{E}})$ in Property 2.

Property 1. $\mathrm{Guess}(X|\mathcal{Q}(\mathsf{E})) \le \mathrm{Guess}(X|\mathsf{E})$ for any CPTP map $\mathcal{Q}$ acting on E.

Property 2. $\mathrm{Guess}(X|Z\mathsf{E}) = \sum_z P_Z(z)\,\mathrm{Guess}(X|\mathsf{E},Z=z)$.

Property 3. $\mathrm{Guess}(X|\mathsf{E},\Lambda) \le \mathrm{Guess}(X|\mathsf{E})/P[\Lambda]$ for any event Λ.

Note that Property 2 implies that $\mathrm{Guess}(X|\mathsf{E},\Lambda) \le \mathrm{Guess}(X|1_\Lambda\mathsf{E})/P[\Lambda]$, but the statement of Property 3 is stronger since $\mathrm{Guess}(X|\mathsf{E}) \le \mathrm{Guess}(X|1_\Lambda\mathsf{E})$.

Proof (of Property 3). It holds that[7] $P[\Lambda]\cdot\rho_{X\mathsf{E}|\Lambda} \le \rho_{X\mathsf{E}}$, and hence that for any measurement $\mathcal{M}$ on E

$$P[\Lambda]\cdot P[\mathcal{M}(\mathsf{E})=X|\Lambda] \le P[\mathcal{M}(\mathsf{E})=X] \le \mathrm{Guess}(X|\mathsf{E}) \ ,$$

which implies the claim. □

[6] By our conventions, the probability $P[\mathcal{M}(\mathsf{E})=X]$ is to be understood as $P[X'=X]$ for the (purely classical) state $\rho_{XX'} = \rho_{X\mathcal{M}(\mathsf{E})} = (id_X\otimes\mathcal{M})(\rho_{X\mathsf{E}}) \in \mathcal{D}(\mathcal{X}\otimes\mathcal{X})$.

[7] Here and throughout, for operators K and L, the inequality $K \le L$ means that $L-K$ is positive-semidefinite.

Property 4. There exists $\sigma_E \in \mathcal{D}(\mathcal{H}_E)$ so that

$$\rho_{XE} \leq \mathrm{Guess}(X|E) \cdot \mathbb{I}_{\mathcal{X}} \otimes \sigma_E = \mathrm{Guess}(X|E) \cdot |\mathcal{X}| \cdot \mu_{\mathcal{X}} \otimes \sigma_E \ .$$

Proof. The claim follows from Renner's original definition of the conditional min-entropy as

$$H_\infty(X|E) := \max_{\sigma_E} \max_{\lambda} \{\lambda \,|\, \rho_{XE} \leq 2^{-\lambda} \cdot \mathbb{I}_{\mathcal{X}} \otimes \sigma_E\}$$

and the identity $H_\infty(X|E) = -\log \mathrm{Guess}(X|E)$, as shown in [12]. □

3 Enabling Tools

In this section, we introduce and discuss the main technical tools for the constructions and analyses of our key-recycling authentication and encryption schemes.

3.1 On Guessing the Outcome of Quantum Measurements

We consider different "guessing games", where one or two players need to guess the outcome of a quantum measurement. The bounds are derived by means of the techniques of [19].

Two-player guessing. Here, we consider a game where two parties, Bob and Charlie, need to *simultaneously* and without communication guess the outcome of BB84 measurements performed by Alice (on n qubits prepared by Bob and Charlie), when given the bases that Alice chose. This is very similar to the *monogamy game* introduced and studied in [19], but in the version we consider here, the sequence of bases is not chosen from $\{0,1\}^n$ but from a code $\mathcal{C} \subset \{0,1\}^n$ with minimal distance d. It is useful to think of d to be much larger than $\log |\mathcal{C}|$, i.e., the dimension of the code in case of a linear code. The following shows that in case of a uniformly random choice of the bases in $\mathcal{C}$, Bob and Charlie cannot do much better than to agree on a guess for the bases and to give Alice qubits in those bases.

Proposition 1. *Let $\mathcal{H}_A$ be a n-qubit system, and let $\mathcal{H}_B$ and $\mathcal{H}_C$ be arbitrary quantum systems. Consider a state $\rho_{\Theta ABC} = \mu_{\mathcal{C}} \otimes \rho_{ABC} \in \mathcal{D}(\mathcal{C} \otimes \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, and let*

$$\rho_{\Theta X X' X''} = \mathcal{N}_{\Theta C \to X''} \circ \mathcal{N}_{\Theta B \to X'} \circ \mathcal{M}^{\text{BB84}}_{\Theta A \to X}(\rho_{\Theta ABC})$$

where $\mathcal{M}^{\text{BB84}}_{\Theta A \to X}$ is the BB84-measurement of the system A (controlled by Θ), and $\mathcal{N}_{\Theta B \to X'}$ and $\mathcal{N}_{\Theta C \to X''}$ are arbitrary (possibly different) measurements of the respective systems B and C, both controlled by Θ. Then, it holds that

$$P[X' = X \wedge X'' = X] \leq \frac{1}{|\mathcal{C}|} + \frac{1}{2^{d/2}} \ .$$

Proof. The proof uses the techniques from [19]. By Naimark's theorem, we may assume without loss of generality that the conditional measurements $\mathcal{N}^{\theta}_{B\to X'}$ and $\mathcal{N}^{\theta}_{C\to X''}$ are specified by families $\{P^{\theta}_x\}_x$ and $\{Q^{\theta}_x\}_x$ of *projections*. Then, defining for every $\theta\in\mathcal{C}$ the projection $\Pi^{\theta}=\sum_x H^{\theta}|x\rangle\langle x|H^{\theta}\otimes P^{\theta}_x\otimes Q^{\theta}_x$, we see that

$$P[X'=X\wedge X''=X]\leq\frac{1}{|\mathcal{C}|}\left\|\sum_{\theta}\Pi^{\theta}\right\|\leq\frac{1}{|\mathcal{C}|}\sum_{\delta}\max_{\theta}\left\|\Pi^{\theta}\Pi^{\theta\oplus\delta}\right\|\ ,$$

where $\|\cdot\|$ refers to the standard operator norm, and the second inequality is by Lemma 2.2 in [19]. For any $\theta,\theta'\in\mathcal{C}$, bounding Π^{θ} and $\Pi^{\theta'}$ by

$$\Pi^{\theta}\leq\Gamma^{\theta}:=\sum_x H^{\theta}|x\rangle\langle x|H^{\theta}\otimes P^{\theta}_x\otimes\mathbb{I}$$

and

$$\Pi^{\theta'}\leq\Delta^{\theta'}:=\sum_x H^{\theta'}|x\rangle\langle x|H^{\theta'}\otimes\mathbb{I}\otimes Q^{\theta'}_x\ \ ,$$

it is shown in [19] (in the proof of Theorem 3.4) that

$$\left\|\Pi^{\theta}\Pi^{\theta'}\right\|\leq\left\|\Gamma^{\theta}\Delta^{\theta'}\right\|\leq\frac{1}{2^{d_H(\theta,\theta')/2}}\leq\frac{1}{2^{d/2}}$$

where the last inequality holds unless $\theta=\theta'$, from which the claim follows. □

Remark 1. If we restrict $\mathcal{H}_B$ to be a n-qubit system too, and replace the (arbitrary) measurement $\mathcal{N}_{\Theta B}$ by a BB84 measurement $\mathcal{M}^{\text{BB84}}_{\Theta B}$, i.e., "Bob measures correctly", then we get

$$P[X'=X\wedge X''=X]\leq\frac{1}{|\mathcal{C}|}+\frac{1}{2^d}\ .$$

Two-player guessing with quantum side information. Now, we consider a version of the game where Alice's choice for the bases is not uniformly random, and, additionally, Bob and Charlie may hold some quantum side information on Alice's choice at the time when they can prepare the initial state (for Alice, Bob and Charlie).

Corollary 1. *Let $\mathcal{H}_A$ be a n-qubit system, and let $\mathcal{H}_B,\mathcal{H}_C$ and $\mathcal{H}_E$ be arbitrary quantum systems. Consider a state $\rho_{\Theta E}\in\mathcal{D}(\mathcal{C}\otimes\mathcal{H}_E)$, and let*

$$\rho_{\Theta ABC}=\mathcal{Q}_{E\to ABC}\big(\rho_{\Theta E}\big)\in\mathcal{D}(\mathcal{C}\otimes\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C)$$

where $\mathcal{Q}_{E\to ABC}$ is a CPTP map acting on E (only), and let

$$\rho_{\Theta XX'X''}=\mathcal{N}_{\Theta C\to X''}\circ\mathcal{N}_{\Theta B\to X'}\circ\mathcal{M}^{\text{BB84}}_{\Theta A\to X}\big(\rho_{\Theta ABC}\big)$$

as in Proposition 1 above. Then, it holds that

$$P[X'=X\wedge X''=X]\leq\text{Guess}(\Theta|E)+\frac{\text{Guess}(\Theta|E)\cdot|\mathcal{C}|}{2^{d/2}}\ .$$

Proof. By Proposition 1, the claim holds as $P[X'=X \wedge X''=X] \leq 1/|\mathcal{C}|+1/2^{d/2}$ for the special case where $\rho_{\Theta E}$ is of the form $\rho_{\Theta E} = \mu_{\mathcal{C}} \otimes \sigma_E$. Furthermore, by Property 4 we know that an arbitrary $\rho_{\Theta E} \in \mathcal{D}(\mathcal{C} \otimes \mathcal{H}_E)$ is bounded by

$$\rho_{\Theta E} \leq \mathrm{Guess}(\Theta|E) \cdot |\mathcal{C}| \cdot \mu_{\mathcal{C}} \otimes \sigma_E \ .$$

Therefore, since the composed map

$$\mathcal{D}(\mathcal{C} \otimes \mathcal{H}_E) \to \mathcal{D}(\{0,1\}),\ \rho_{\Theta E} \mapsto \rho_{\Theta ABC} \mapsto \rho_{XX'X''} \mapsto \rho_{1_{X=X' \wedge X=X''}}$$

is still a CPTP map, it holds that for arbitrary $\rho_{\Theta E} \in \mathcal{D}(\mathcal{C} \otimes \mathcal{H}_E)$

$$P[X'=X \wedge X''=X] \leq \mathrm{Guess}(\Theta|E) \cdot |\mathcal{C}| \cdot \left(\frac{1}{|\mathcal{C}|} + \frac{1}{2^{d/2}}\right) \ ,$$

which proves the claim. □

Remark 2. Similarly to the remark above, the bound relaxes to

$$P[X'=X \wedge X''=X] \leq \mathrm{Guess}(\Theta|E) + \frac{\mathrm{Guess}(\Theta|E) \cdot |\mathcal{C}|}{2^d} \ ,$$

when "Bob measure correctly".

Single-player guessing (with quantum side information). Corollary 1 immediately gives us control also over a slightly different game, where only one party needs to guess Alice's measurement outcome, but here he is *not* given the bases. Indeed, any strategy here gives a strategy for the above simultaneous-guessing game, simply by "pre-measuring" B, and having Bob and Charlie each keep a copy of the measurement outcome.

Corollary 2. *Let $\mathcal{H}_A$ be a n-qubit system, and let $\mathcal{H}_B$ and $\mathcal{H}_E$ be arbitrary quantum systems. Consider a state $\rho_{\Theta E} \in \mathcal{D}(\mathcal{C} \otimes \mathcal{H}_E)$ and let*

$$\rho_{\Theta AB} = \mathcal{Q}_{E \to AB}\big(\rho_{\Theta E}\big) \in \mathcal{D}(\mathcal{C} \otimes \mathcal{H}_A \otimes \mathcal{H}_B)$$

where $\mathcal{Q}_{E \to AB}$ is a CPTP map acting on E, and let

$$\rho_{\Theta XX''} = \mathcal{N}_{B \to X''} \circ \mathcal{M}^{\text{BB84}}_{\Theta A \to X}\big(\rho_{\Theta AB}\big)$$

where $\mathcal{N}_{B \to X''}$ is an arbitrary measurement of B (with no access to Θ). Then, it holds that

$$P[X''=X] \leq \mathrm{Guess}(\Theta|E) + \frac{\mathrm{Guess}(\Theta|E) \cdot |\mathcal{C}|}{2^{d/2}} \ .$$

In other words, for the state $\rho_{\Theta XB} = \mathcal{M}^{\text{BB84}}_{\Theta A \to X}(\rho_{\Theta AB})$ we have that

$$\mathrm{Guess}(X|B) \leq \mathrm{Guess}(\Theta|E) + \frac{\mathrm{Guess}(\Theta|E) \cdot |\mathcal{C}|}{2^{d/2}} \ .$$

Remark 3. If we restrict the side information E to be *classical* then, using slightly different techniques, we can improve the bounds from Corollary 1 and 2 to

$$\mathrm{Guess}(\Theta|E) + \frac{1}{2^{d/2}} \ .$$

Whether this improved bound also holds in case of quantum side information is an open question.

3.2 Hash Functions with Message-Independence and Key-Privacy

The goal of key-recycling is to be able to *re-use* a cryptographic key. For this to be possible, it is necessary — actually, not necessary but sufficient — that a key *stays secure*, i.e., that the primitive that uses the key does *not* reveal anything on the key, or only very little. We introduce here a general notion that captures this, i.e., that ensures that the key stays secure *as long as* there is *enough uncertainty* in the message the primitive is applied to — in our construction(s), this uncertainty will then be derived from the quantum part.

Consider a keyed hash function $\mathsf{H} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ with key space $\mathcal{K}$, message space $\mathcal{X}$, and range $\mathcal{Y}$. We define the following properties on such a hash function.

Definition 2. *We say that* H *is* message-independent *if for a uniformly random key* K *in* $\mathcal{K}$*, the distribution of the hash value* $Y = \mathsf{H}(K, x)$ *is independent of the message* $x \in \mathcal{X}$*. And, we say that* H *is* uniform *if it is message-independent and* $Y = \mathsf{H}(K, x)$ *is uniformly random on* $\mathcal{Y}$*.*

Thus, message-independence simply ensures that if the key is uniformly random and independent of the message, then the hash of the message is independent of the message too. The key-privacy property below on the other hand ensures that for any adversary that has arbitrary but *limited* information on the message and the hash value — but no direct information on the key — has (almost) no information on the key.

Definition 3. *We say that* H *offers* ν-key-privacy *if for any state* ρ_{KXYE} *in* $\mathcal{D}(\mathcal{K} \otimes \mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{H}_E)$ *with the properties that* $\rho_{KX} = \mu_{\mathcal{K}} \otimes \rho_X$*,* $Y = \mathsf{H}(K, X)$ *and* $K \leftrightarrow XY \leftrightarrow E$*, it holds that*

$$\delta(K, U_{\mathcal{K}}|YE) \leq \frac{\nu}{2}\sqrt{\mathrm{Guess}(X|YE) \cdot |\mathcal{Y}|} \ .$$

We say that H *offers* ideal key-privacy *if it offers* 1*-key-privacy.*

Remark 4. Note that if H is message-independent then for X, Y and E as above in Definition 3, we have that $\mathrm{Guess}(X|YE) = \mathrm{Guess}(X|E)$.

Not so surprisingly, the joint notion of uniformity and key-privacy is closely related to that of a *strong extractor* [14]. Indeed, if H is uniform and offers key-privacy then it is a strong extractor: for $\rho_{KXE} = \mu_{\mathcal{K}} \otimes \rho_{XE}$ and $Y = \mathsf{H}(K, X)$, the condition on ρ_{KXYE} in Definition 3 is satisfied, and thus we have the promised bound on $\delta(\rho_{KYE}, \mu_{\mathcal{K}} \otimes \rho_{YE}) = \delta(\rho_{KYE}, \mu_{\mathcal{K}} \otimes \mu_{\mathcal{Y}} \otimes \rho_E)$, where the equality is due to uniformity. As such, [18] shows that the required bound on $\delta(K, U_{\mathcal{K}}|YE)$ is the best one can hope for. On the other hand, the following shows that from every strong extractor we can easily construct a hash function that offers uniformity and key-privacy.

Proposition 2. *Let* $\mathsf{Ext} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ *be a strong extractor, meaning that for* $\rho_{KXE} = \mu_{\mathcal{K}} \otimes \rho_{XE} \in \mathcal{D}(\mathcal{K} \otimes \mathcal{X} \otimes \mathcal{H}_E)$ *and for* Y *computed as* $Y = \mathsf{Ext}(K, X)$ *it*

holds that $\delta(\rho_{KY\mathsf{E}}, \mu_{\mathcal{K}} \otimes \rho_{Y\mathsf{E}}) \leq \frac{\nu}{2}\sqrt{\mathrm{Guess}(X|\mathsf{E}) \cdot |\mathcal{Y}|}$. *Furthermore, we assume that the range* $\mathcal{Y}$ *forms a group. Then, the keyed hash function*[8]

$$\mathsf{H} : (\mathcal{K} \times \mathcal{Y}) \times \mathcal{X} \to \mathcal{Y},\ (k\|k', x) \mapsto \mathsf{Ext}(k, x) + k'$$

with key space $\mathcal{K} \times \mathcal{Y}$ *satisfies uniformity and* ν*-key-privacy.*

Proof. Uniformity is clear. For key-privacy, consider a state $\rho_{KXY\mathsf{E}}$ with the properties as in Definition 3. We fix an arbitrary $y \in \mathcal{Y}$ and condition on $Y = y$. Conditioning on $X = x$ as well for an arbitrary $x \in \mathcal{X}$, the key (K, K') is uniformly distributed subject to $\mathsf{H}(K, x)+K' = y$. In other words, K is uniformly random in $\mathcal{K}$, and $K' = y - \mathsf{H}(K, x)$. Therefore, making use of the Markov-chain property, conditioning on $Y = y$ only, K is uniformly random in $\mathcal{K}$ and independent of X and E, and $K' = y-\mathsf{H}(K, X)$. Thus, by the extractor property, $\delta(\rho_{K'K\mathsf{E}|Y=y}, \mu_{\mathcal{Y}} \otimes \mu_{\mathcal{K}} \otimes \rho_{\mathsf{E}|Y=y}) \leq \frac{\nu}{2}\sqrt{\mathrm{Guess}(X|\mathsf{E}, Y=y) \cdot |\mathcal{Y}|}$. The claim follows by averaging over y, and applying Jensen's inequality and Property 2. □

The following technical result will be useful.

Lemma 1. *Let* $\mathsf{H} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ *be a keyed hash function that satisfies message-independence. Furthermore, let* $\rho_{KXY\mathsf{E}}$ *be a state with the properties as in Definition 3. Then*

$$\mathrm{Guess}(X|KY\mathsf{E}) \leq \mathrm{Guess}(X|Y\mathsf{E}) \cdot |\mathcal{Y}| \ .$$

Proof. Note that the Markov-chain property $K \leftrightarrow XY \leftrightarrow \mathsf{E}$ can be understood in that E is obtained by acting on XY only: $\mathsf{E} = \mathcal{Q}(XY)$. For the purpose of the argument, we extend the state $\rho_{XKY\mathsf{E}}$ to a state $\rho_{XKK'YY'\mathsf{E}\mathsf{E}'}$ as follows. We choose a uniformly random and independent K' in $\mathcal{K}$, and set $Y' = \mathsf{H}(K', X)$ and $\mathsf{E}' = \mathcal{Q}(XY')$. Note that $\rho_{XKY\mathsf{E}}$ coincides with $\rho_{XK'Y'\mathsf{E}'}$. Therefore,

$$\mathrm{Guess}(X|Y\mathsf{E}) = \mathrm{Guess}(X|Y'\mathsf{E}') = \mathrm{Guess}(X|KY'\mathsf{E}') \ ,$$

where the second equality is by the independence of K. Furthermore, by Property 3, we have that

$$\begin{aligned}\mathrm{Guess}(X|KY'\mathsf{E}') &\geq P[Y=Y']\,\mathrm{Guess}(X|KY'\mathsf{E}', Y=Y') \\ &= P[Y=Y']\,\mathrm{Guess}(X|KY\mathsf{E}, Y=Y') \ .\end{aligned}$$

Finally, by the message-independence of H, it holds that Y' is independent of $KXY\mathsf{E}$ (and with the same distribution as Y), and therefore $P[Y=Y'] \geq 1/|\mathcal{Y}|$ and $\mathrm{Guess}(X|KY\mathsf{E}, Y = Y') = \mathrm{Guess}(X|KY\mathsf{E})$. Altogether, this gives us the bound $\mathrm{Guess}(X|KY\mathsf{E}) \leq \mathrm{Guess}(X|Y\mathsf{E}) \cdot |\mathcal{Y}|$, which concludes the proof. □

Equipped with Lemma 1, we can now show the following composition results.

[8] Here, and similarly in other occasions, $k\|k'$ is simply a synonym for the element (k, k') in the Cartesian product of, here, $\mathcal{K}$ and $\mathcal{Y}$, and is mainly used to smoothen notation and avoid expressions like $\big((k, k'), x\big)$.

Proposition 3 (Parallel Composition). *Consider two keyed hash functions* $\mathsf{H}_1 : \mathcal{K}_1 \times \mathcal{X} \to \mathcal{Y}_1$ *and* $\mathsf{H}_2 : \mathcal{K}_2 \times \mathcal{X} \to \mathcal{Y}_2$ *with the same message space* $\mathcal{X}$*, and*

$$\mathsf{H} : (\mathcal{K}_1 \times \mathcal{K}_2) \times \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2,\ (k_1 \| k_2, x) \mapsto \big(\mathsf{H}_1(k_1, x), \mathsf{H}_2(k_2, x)\big)$$

with key space $\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2$ *and range* $\mathcal{Y} = \mathcal{Y}_1 \times \mathcal{Y}_2$*. If* H_1 *and* H_2 *are both message-independent (or uniform) and respectively offer* ν_1*-and* ν_2*-key privacy, then* H *is message-independent (or uniform) and offers* $(\nu_1 + \nu_2)$*-key privacy.*

Proof. That message-independence/uniformity is preserved is clear. To argue key-privacy, assume that we have $\rho_{K_1 K_2 X} = \rho_{K_1} \otimes \rho_{K_2} \otimes \rho_X$, $Y_1 = \mathsf{H}_1(K_1, X)$ and $Y_2 = \mathsf{H}(K_2, X)$, and $K_1 K_2 \leftrightarrow X Y_1 Y_2 \leftrightarrow \boldsymbol{E}$. We need to bound the distance of $K_1 K_2$ from uniform when given $Y_1 Y_1 \boldsymbol{E}$, which we can decompose into

$$\delta(K_1 K_2, U_{\mathcal{K}_1} U_{\mathcal{K}_2} | Y_1 Y_1 \boldsymbol{E}) \leq \delta(K_1, U_{\mathcal{K}_1} | Y_1 Y_2 \boldsymbol{E}) + \delta(K_2, U_{\mathcal{K}_2} | K_1 Y_1 Y_2 \boldsymbol{E}) \ .$$

The above conditions on $\rho_{K_1 K_2 X Y_1 Y_2 \boldsymbol{E}}$ imply that $K_1 \leftrightarrow X Y_1 \leftrightarrow K_2 Y_2 \boldsymbol{E}$ holds, and thus also $K_1 \leftrightarrow X Y_1 \leftrightarrow Y_2 \boldsymbol{E}$. Indeed, $K_1 K_2 \leftrightarrow X Y_1 Y_2 \leftrightarrow \boldsymbol{E}$ implies that also $K_1 \leftrightarrow X Y_1 K_2 Y_2 \leftrightarrow \boldsymbol{E}$, which together with $K_1 \leftrightarrow X Y_1 \leftrightarrow K_2 Y_2$ (which holds by choice of K_2 and Y_2) implies that $K_1 \leftrightarrow X Y_1 \leftrightarrow K_2 Y_2 \boldsymbol{E}$. Therefore, by the key-privacy property of H_1, setting $\boldsymbol{E}_1 = Y_2 \boldsymbol{E}$, we see that

$$\delta(K_1, U_{\mathcal{K}_1} | Y_1 Y_2 \boldsymbol{E}) \leq \frac{\nu_1}{2} \sqrt{\mathrm{Guess}(X | Y_1 Y_2 \boldsymbol{E}) \cdot |\mathcal{Y}_1|} \ .$$

Similarly, $K_2 \leftrightarrow X Y_2 \leftrightarrow K_1 Y_1 \boldsymbol{E}$, and so by the key-privacy property of H_2, setting $\boldsymbol{E}_2 = K_1 Y_1 \boldsymbol{E}$, we conclude that

$$\begin{aligned} \delta(K_2, U_{\mathcal{K}_2} | K_1 Y_1 Y_2 \boldsymbol{E}) &\leq \frac{\nu_2}{2} \sqrt{\mathrm{Guess}(X | Y_2 K_1 Y_1 \boldsymbol{E}) \cdot |\mathcal{Y}_2|} \\ &\leq \frac{\nu_2}{2} \sqrt{\mathrm{Guess}(X | Y_2 Y_1 \boldsymbol{E}) \cdot |\mathcal{Y}_1| \cdot |\mathcal{Y}_2|} \ , \end{aligned}$$

which proves the claim. □

Proposition 4 ("Sequarallel" Composition). *Consider two keyed hash functions* $\mathsf{H}_1 : \mathcal{K}_1 \times \mathcal{X} \to \mathcal{Y}_1$ *and* $\mathsf{H}_2 : \mathcal{K}_2 \times (\mathcal{X} \otimes \mathcal{Y}_1) \to \mathcal{Y}_2$ *with message spaces as specified, and*

$$\mathsf{H} : (\mathcal{K}_1 \times \mathcal{K}_2) \times \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2\,,\ (k_1 \| k_2, x) \mapsto \big(\mathsf{H}_1(k_1, x), \mathsf{H}_2(k_2, x \| \mathsf{H}_1(k_1, x))\big)$$

with key space $\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2$ *and range* $\mathcal{Y} = \mathcal{Y}_1 \times \mathcal{Y}_2$*. If* H_1 *and* H_2 *are both message-independent (or uniform) and respectively offer* ν_1*-and* ν_2*-key privacy, then* H *is message-independent (or uniform) and offers* $(\nu_1 + \nu_2)$*-key privacy.*

Proof. The proof goes along the same lines as the proof of Proposition 3, except that in the reasoning for the bound on $\delta(K_2, U_{\mathcal{K}_2} | K_1 Y_1 \boldsymbol{E})$, we append Y_1 to X, with the consequence that we get a bound that is in terms of $\mathrm{Guess}(X Y_1 | Y_2 Y_1 \boldsymbol{E})$, but this obviously coincides with $\mathrm{Guess}(X | Y_2 Y_1 \boldsymbol{E})$, and thus we end up with the same bound. □

4 Message Authentication with Key-Recycling

We first consider the problem of *message authentication* with key-recycling. It turns out that — at least with our approach — this is the actual challenging problem, and extending to (authenticated) encryption is then quite easy.

4.1 The Semantics

We quickly specify the semantics of a quantum authentication code (or scheme) with key-recycling.[9]

Definition 4. *A* quantum authentication code (with key recycling) QMAC *with message space* $\mathcal{MSG}$ *and key space* $\mathcal{KEY}$ *is made up of the following components: (1) A CPTP map* Auth *that is controlled by a* message $msg \in \mathcal{MSG}$ *and a* key $key \in \mathcal{KEY}$*, and that acts on an empty system and outputs a* quantum authentication tag *(with a fixed state space), (2) a measurement* Verify *that is controlled by* $msg \in \mathcal{MSG}$ *and* $key \in \mathcal{KEY}$*, and that acts on a quantum authentication tag and outputs a decision bit* $d \in \{0,1\}$*, and (3) a randomized function* $\mathsf{Refresh} : \mathcal{KEY} \to \mathcal{KEY}$.

We will often identify an authentication code, formalized as above, with the obvious *authenticated-message-transmission protocol* $\pi_{\mathsf{QMAC}}(msg)$, where Alice and Bob start with a shared key $key \in \mathcal{KEY}$, and Alice sends the message msg along with its quantum authentication tag prepared by means of Auth to Bob over a channel that is controlled by the adversary Eve, and, upon reception of the (possibly modified) message and tag, Bob verifies correctness using Verify and accordingly accepts or rejects. If he rejects, then Alice and Bob replace key by $key' := \mathsf{Refresh}(key)$.[10] Note that, for any message $msg \in \mathcal{MSG}$ and any strategy for Eve on how to interfere with the communication, the protocol $\pi_{\mathsf{QMAC}}(msg)$ induces a CPTP map $\mathcal{E}xe[\pi_{\mathsf{QMAC}}(msg)] : \mathcal{D}(\mathcal{KEY} \otimes \mathcal{H}_E) \to \mathcal{D}(\mathcal{KEY} \otimes \mathcal{H}_{E'})$ that describes the evolution of the shared key key and Eve's local system as a result of the execution of $\pi_{\mathsf{QMAC}}(msg)$.

Our goal will be to show that, for our construction given below, and for any behavior of Eve, the CPTP map $\mathcal{E}xe[\pi_{\mathsf{QMAC}}(msg)]$ maps a key about which Eve has little information into a (possibly updated) key about which Eve still has little information — what it means here to "have little information" needs to be specified, but it will in particular imply that it still allows Bob to detect a modification of the message. This then ensures re-usability of the quantum authentication code — with the same key as long as Bob accepts the incoming messages, and with the updated key in case he rejects.

[9] Our definition is tailored to our goal that the key can be re-used unchanged in case the message is accepted by the recipient, Bob, and only needs to be refreshed in case he rejects. In the literature, key-recycling sometimes comes with *two* refresh procedures, one for the case Bob rejects and one for the case he accepts.

[10] Obviously, this requires Alice and Bob to exchange fresh randomness, i.e., the randomness for executing $\mathsf{Refresh}$, in a *reliable* and *private* way; how this is done is not relevant here.

4.2 The Scheme

Let $\mathcal{MSG}$ be an arbitrary non-empty finite set. We are going to construct a quantum message authentication code QMAC with message space $\mathcal{MSG}$. To this end, let $\mathsf{MAC} : \mathcal{K} \times (\mathcal{MSG} \times \{0,1\}^n) \to \mathcal{T}$ be a classical one-time message authentication code with a message space $\mathcal{MSG} \times \{0,1\}^n$ for some $n \in \mathbb{N}$. We require MAC to be secure in the standard sense, meaning a modified message will be detected except with small probability $\varepsilon_{\mathsf{MAC}}$. Additionally, we require MAC to satisfy message-independence and ideal key-privacy, as discussed in Sect. 3.2. Actually, it is sufficient if $\mathsf{MAC}(\,\cdot\,, msg \| \cdot\,)$, i.e., the hash function $\mathcal{K} \times \{0,1\}^n \to \mathcal{T}$, $(k, x) \mapsto \mathsf{MAC}(k, msg \| x)$ obtained by fixing msg, satisfies message-independence and ideal key-privacy for any $msg \in \mathcal{MSG}$. Assuming that $\mathcal{MSG}$ consists of bit strings of fixed size so that $\mathcal{MSG} \times \{0,1\}^n = \{0,1\}^N$ for some $N \in \mathbb{N}$, the canonical message authentication codes $\mathsf{MAC} : \left(\mathbb{F}_2^{\ell \times N} \times \mathbb{F}_2^{\ell}\right) \times \mathbb{F}_2^N \to \mathbb{F}_2^{\ell}$, $(A \| b, x) \mapsto Ax + b$ and $\mathsf{MAC} : \left(\mathbb{F}_{2^N} \times \mathbb{F}_2^{\ell}\right) \times \mathbb{F}_{2^N} \to \mathbb{F}_2^{\ell}$, $(a \| b, x) \mapsto trunc(a \cdot x) + b$, where $trunc : \mathbb{F}_{2^N} \to \mathbb{F}_2^{\ell}$ is an arbitrary surjective $\mathbb{F}_2$-linear map, are suitable choices; this follows directly from Proposition 2. Finally, let $\mathcal{C} \subset \{0,1\}^n$ be a code with large minimal distance d.

Then, our quantum message authentication code QMAC has a key space $\mathcal{KEY} = \mathcal{K} \times \mathcal{C}$, where for a key $k \| \theta \in \mathcal{K} \times \mathcal{C}$ we refer to k as the "MAC key" and to θ as the "basis key", and QMAC works as described in Figure 1

$\mathsf{QMAC.Auth}(k \| \theta, msg)$: Choose a uniformly random $x \in \{0,1\}^n$ and output n qubits $\mathsf{B}_\circ$ in state $H^\theta |x\rangle$ and the classical tag $t = \mathsf{MAC}(k, msg \| x)$.

$\mathsf{QMAC.Verify}(k \| \theta, msg, t)$: Measure the qubits $\mathsf{B}_\circ$ in bases θ to obtain x' (supposed to be x), check that $t = \mathsf{MAC}(k, msg \| x')$, and output 0 or 1 accordingly.

$\mathsf{QMAC.Refresh}(k \| \theta)$: Choose a uniformly random $\theta' \in \mathcal{C}$ and output $k \| \theta'$.

Fig. 1. The quantum message authentication code MAC.

It is clear that as long as the MAC key k is "secure enough", the classical MAC takes care of an Eve that tries to modify the message msg, and it ensures that such an attack is detected by Bob, except with small probability. What is non-trivial to argue is that the MAC key (together with the basis key) indeed stays "secure enough" over multiple executions of $\pi_{\mathsf{QMAC}}(msg)$; this is what we show below.

4.3 Analysis

We consider an execution of the authenticated-message-transmission protocol $\pi_{\mathsf{QMAC}}(msg)$ for a fixed message msg. Let $\rho_{K\Theta E} \in \mathcal{D}(\mathcal{K} \otimes \mathcal{C} \otimes \mathcal{H}_E)$ be the joint state *before* the execution, consisting of the MAC key K, the basis key Θ, and Eve's local quantum system E. The joint state $\mathcal{E}xe[\pi_{\mathsf{QMAC}}(msg)](\rho_{K\Theta E})$ *after* the

execution is given by $\rho_{K\Theta' TDC} \in \mathcal{D}(\mathcal{K} \otimes \mathcal{C} \otimes \mathcal{T} \otimes \{0,1\} \otimes \mathcal{H}_C)$, where Θ' is the (possibly) updated basis key, T is the classical tag, D is Bob's decision to accept or reject, and C is Eve's new quantum system. Eve's complete information after the execution of the scheme is thus given by $E' = TDC$.

Recall that TDC is obtained as follows from $K\Theta E$. Alice prepares BB84-qubits $B_\circ$ for uniformly random bits X and with bases determined by Θ, and she computes the tag $T := \mathsf{MAC}(K, msg \| X)$. Then, Eve acts on $B_\circ E$ (in a way that may depend on T) and keeps one part, C, of the resulting state, and Bob measures the other part, B, to obtain X' and checks with the (possibly modified) tag T to decide on D.

Note that by a standard reasoning, we can think of the BB84 qubits $B_\circ$ not as being prepared by first choosing the classical bits X and then "encoding" them into qubits with the prescribed bases Θ, but by first preparing n EPR pairs $\Phi^+_{AB_\circ}$ and then measuring the qubits in A in the prescribed bases to obtain X, i.e., $\rho_{K\Theta X B_\circ E} = \mathcal{M}^{\text{BB84}}_{\Theta A \to X}\big(\Phi^+_{AB_\circ} \otimes \rho_{K\Theta E}\big)$.

The following captures the main security property of the scheme.

Theorem 1. *If the state before the execution of $\pi_{\mathsf{QMAC}}(msg)$ is of the form $\rho_{K\Theta E} = \mu_{\mathcal{K}} \otimes \rho_{\Theta E}$, then for any Eve the state $\rho_{K\Theta' E'} = \mathcal{E}xe[\pi_{\mathsf{QMAC}}(msg)](\rho_{K\Theta E})$ after the execution satisfies*

$$\mathrm{Guess}(\Theta'|E') \leq \mathrm{Guess}(\Theta|E) + \frac{1}{|\mathcal{C}|}$$

and

$$\delta(K, U_{\mathcal{K}}|\Theta' E') \leq 2\varepsilon_{\mathsf{MAC}} + \frac{\sqrt{2}}{2}\sqrt{\mathrm{Guess}(\Theta|E)\left(1 + \frac{|\mathcal{C}|}{2^{d/2}}\right)|\mathcal{T}|} \ .$$

This means that if *before* the execution of $\pi_{\mathsf{QMAC}}(msg)$, it holds that Eve's guessing probability on Θ is small and K looks perfectly random to her (even when given Θ), then *after* the execution, Eve's guessing probability on (the possibly refreshed) Θ' is still small and K still looks *almost* perfectly random to her. As such, we may then consider a *hypothetical* refreshing of K that has almost no impact, but which brings us back to the position to apply Theorem 1 again, and hence allows us to re-apply this "preservation of security" for the next execution, and so on. This in particular allows us to conclude that in an arbitrary *sequence* of executions, the MAC key K stays almost perfectly random for Eve, and thus any tampering with an authenticated message will be detected by Bob except with small probability by the security of MAC (see Sect. 4.4 for more details).

Remark 5. For simplicity, in Theorem 1 and in the remainder of this work, we assume the message *msg* to be arbitrary but *fixed*. However, it is not hard to see that we may also allow *msg* to be obtained by means of a measurement, applied to Eve's system E before the execution of $\pi_{\mathsf{QMAC}}(msg)$, i.e., Eve can choose it. The bounds of Theorem 1 then hold *on average over the measured msg*. This follows directly from Property 2 for the bound the the guessing probability,

and from a similar decomposition property for the trace distance, together with Jensen's inequality for the bound on the trace distance. We emphasize however, that we do assume *msg*, even when provided by Eve, to be *classical*, i.e., we do not consider so-called superposition attacks.

The formal proof of Theorem 1 is given below; the intuition is as follows. For the bound on the guessing probability of the (possibly updated) basis key, we have that in case Bob rejects and so the basis key is re-sampled from $\mathcal{C}$, Eve has obviously guessing probability $1/|\mathcal{C}|$. In case Bob accepts, the fact that Bob accepts may increase Eve's guessing probability. For instance, Eve may measure one qubit in, say, the computational basis, and forward the correspondingly collapsed qubit to Bob; if Bob then accepts it is more likely that this qubit had been prepared in the computational basis by Alice, giving Eve some (new) information on the basis key. However, the resulting increase in guessing probability is *inverse proportional* to the probability that Bob actually accepts, so that this advantage is "canceled out" by the possibility that Bob will not accept. For the bound on the "freshness" of K (given the basis key Θ'), by key privacy it is sufficient to argue that Eve has small guessing probability for X. In case Bob rejects, the (refreshed) basis key is useless to her for guessing X, and so the task of guessing X reduces to winning the game considered in Corollary 2. Similarly, the case where Bob accepts fits into the game in Corollary 1. In both cases, we get that the guessing probability of X essentially coincides with $\mathrm{Guess}(\Theta|\mathsf{E})$.

Proof. For the first claim, we simply observe that

$$\begin{aligned}
\mathrm{Guess}(\Theta'|T D \mathsf{C}) &= \sum_{d=0}^{1} P_D(d)\,\mathrm{Guess}(\Theta'|T\mathsf{C}, D=d) && \text{(by Property 2)}\\
&= P_D(0)\frac{1}{|\mathcal{C}|} + P_D(1)\,\mathrm{Guess}(\Theta|T\mathsf{C}, D=1)\\
&\leq P_D(0)\frac{1}{|\mathcal{C}|} + \mathrm{Guess}(\Theta|T\mathsf{C}) && \text{(by Property 3)}\\
&\leq \frac{1}{|\mathcal{C}|} + \mathrm{Guess}(\Theta|T\mathsf{B}_\circ\mathsf{E}) && \text{(by Property 1)}\\
&= \frac{1}{|\mathcal{C}|} + \mathrm{Guess}(\Theta|\mathsf{B}_\circ\mathsf{E}) && \text{(by Definition 2)}\\
&= \frac{1}{|\mathcal{C}|} + \mathrm{Guess}(\Theta|\mathsf{E}) \ .
\end{aligned}$$

where the second equality holds because Θ' is freshly chosen in case Bob rejects and $\Theta' = \Theta$ in case he accepts, and the final equality holds because of the fact that $\rho_{\mathsf{B}_\circ\Theta\mathsf{E}} = \mathrm{tr}_X \circ \mathcal{M}^{\text{BB84}}_{\Theta A\to X}\big(\Phi^+_{A\mathsf{B}_\circ}\otimes\rho_{\Theta\mathsf{E}}\big) = \mathrm{tr}_A\big(\Phi^+_{A\mathsf{B}_\circ}\big)\otimes\rho_{\Theta\mathsf{E}} = \mu_{\mathsf{B}_\circ}\otimes\rho_{\Theta\mathsf{E}}$.

For the second claim, consider $\tilde{D}$ and $\tilde{\Theta}'$ as follows. $\tilde{D}$ is 1 if $X = X'$ and Eve has not modified the tag T nor the message *msg*, and $\tilde{D}$ is 0 otherwise (i.e., $\tilde{D}$ is an "ideal version" of Bob's decision), and $\tilde{\Theta}'$ is freshly chosen if and only $\tilde{D} = 0$. The states of $K\Theta' T D \mathsf{C}$ and $K\tilde{\Theta}' T \tilde{D} \mathsf{C}$ are identical except for when $D = 1$ but

$X \neq X'$ or Eve has modified T or msg, which happens with probability at most $\varepsilon_{\mathsf{MAC}}$ by the security of MAC, and thus the two states are $\varepsilon_{\mathsf{MAC}}$-close. Therefore, $\delta(K, U_{\mathcal{K}}|\Theta' T D \mathsf{C}) \leq \delta(K, U_{\mathcal{K}}|\tilde{\Theta}' T \tilde{D} \mathsf{C}) + 2\varepsilon_{\mathsf{MAC}}$, and so it suffices to analyze the state of $K\tilde{\Theta}' T \tilde{D} \mathsf{C}$. Furthermore, we may assume that Eve's state C contains the information of whether she modified T or msg, so that $\tilde{D}$ can be computed from $1_{X=X'}$ when given C, and thus $\delta(K, U_{\mathcal{K}}|\tilde{\Theta}' \tilde{D} T \mathsf{C}) \leq \delta(K, U_{\mathcal{K}}|\tilde{\Theta}' 1_{X=X'} \tilde{D} T \mathsf{C}) = \delta(K, U_{\mathcal{K}}|\tilde{\Theta}' 1_{X=X'} T \mathsf{C})$.

Now, since K is random and independent of $X\Theta B_\circ \mathsf{E}$, T is computed as $T = \mathsf{MAC}(K, msg|X)$, and $\tilde{\Theta}\, 1_{X=X'} \mathsf{C}$ is obtained by acting on T and $X\Theta B_\circ \mathsf{E}$ only (and not on K), we see that the conditions required in Definition 3 are satisfied. Therefore, by the key-privacy of MAC, and recalling Remark 4,

$$\delta(K, U_{\mathcal{K}}|T\tilde{\Theta}' 1_{X=X'} \mathsf{C}) \leq \frac{1}{2}\sqrt{\mathrm{Guess}(X|\tilde{\Theta}' 1_{X=X'} \mathsf{C})\,|\mathcal{T}|} \ .$$

Furthermore, by Property 2, and noting that $\tilde{\Theta}'$ is freshly chosen when $X \neq X'$ and equal to Θ otherwise,

$$\begin{aligned}\mathrm{Guess}(X|\tilde{\Theta}' 1_{X=X'} \mathsf{C}) = {} & P[X \neq X']\,\mathrm{Guess}(X|\mathsf{C}, X \neq X') \\ & + P[X = X']\,\mathrm{Guess}(X|\Theta \mathsf{C}, X = X') \ .\end{aligned}$$

For the first term, we see that

$$\begin{aligned}P[X \neq X']\,\mathrm{Guess}(X|\mathsf{C}, X \neq X') &\leq \mathrm{Guess}(X|\mathsf{C}) && \text{(by Property 3)} \\ &\leq \mathrm{Guess}(X|T B_\circ \mathsf{E}) && \text{(by Property 1)} \\ &\leq \mathrm{Guess}(X|B_\circ \mathsf{E}) && \text{(by Definition 2)} \\ &\leq \mathrm{Guess}(\Theta|\mathsf{E})\big(1 + \tfrac{|\mathcal{C}|}{2^{d/2}}\big) \ , &&\end{aligned}$$

where the final inequality follows from Corollary 2 by recalling that $\rho_{\Theta X B_\circ \mathsf{E}} = \mathcal{M}^{\text{BB84}}_{\Theta A \to X}\big(\Phi^+_{AB_\circ} \otimes \rho_{\Theta \mathsf{E}}\big)$. Similarly, writing X'' for the measurement outcome when measuring C using an optimal measurement $\mathcal{N}_{\Theta \mathsf{C}}$ (controlled by Θ), we obtain

$$\begin{aligned}P[X = X']\,\mathrm{Guess}(X|\Theta \mathsf{C}, X = X') &\leq P[X = X']\,P[X = X''|X = X'] \\ &\leq P[X = X' \wedge X = X''] \\ &\leq \mathrm{Guess}(\Theta|\mathsf{E})\big(1 + \tfrac{|\mathcal{C}|}{2^{d/2}}\big) \ ,\end{aligned}$$

where the final inequality follows from Corollary 1 by observing that, using uniformity of MAC (Definition 2) in the second equality,

$$\begin{aligned}\rho_{\Theta X X X''} &= \mathcal{N}_{\Theta C \to X''} \circ \mathcal{M}^{\text{BB84}}_{\Theta B \to X'} \circ \mathcal{Q}_{T B_\circ \mathsf{E} \to B\mathsf{C}}\big(\rho_{\Theta X T B_\circ \mathsf{E}}\big) \\ &= \mathcal{N}_{\Theta C \to X''} \circ \mathcal{M}^{\text{BB84}}_{\Theta B \to X} \circ \mathcal{Q}_{T B_\circ \mathsf{E} \to B\mathsf{C}}\big(\rho_{\Theta X B_\circ \mathsf{E}} \otimes \rho_T\big) \\ &= \mathcal{N}_{\Theta C \to X''} \circ \mathcal{M}^{\text{BB84}}_{\Theta B \to X'} \circ \mathcal{Q}_{T B_\circ \mathsf{E} \to B\mathsf{C}} \circ \mathcal{M}^{\text{BB84}}_{\Theta A \to X}\big(\Phi^+_{AB_\circ} \otimes \rho_{\Theta \mathsf{E}} \otimes \rho_T\big) \\ &= \mathcal{N}_{\Theta C \to X''} \circ \mathcal{M}^{\text{BB84}}_{\Theta B \to X'} \circ \mathcal{M}^{\text{BB84}}_{\Theta A \to X} \circ \mathcal{Q}_{T B_\circ \mathsf{E} \to B\mathsf{C}}\big(\Phi^+_{AB_\circ} \otimes \rho_{\Theta \mathsf{E}} \otimes \rho_T\big) \\ &= \mathcal{N}_{\Theta C \to X''} \circ \mathcal{M}^{\text{BB84}}_{\Theta B \to X'} \circ \mathcal{M}^{\text{BB84}}_{\Theta A \to X} \circ \mathcal{Q}'_{\mathsf{E} \to ABC}\big(\rho_{\Theta \mathsf{E}}\big)\end{aligned}$$

where $\mathcal{Q}'_{\mathsf{E} \to ABC}$ is the CPTP map $\mathcal{Q}'_{\mathsf{E} \to ABC}(\sigma_{\mathsf{E}}) = \mathcal{Q}_{T B_\circ \mathsf{E} \to B\mathsf{C}}(\Phi^+_{AB_\circ} \otimes \sigma_{\mathsf{E}} \otimes \rho_T)$. Collecting the terms gives the claimed bound. □

4.4 Re-usability of QMAC

We formally argue here that Theorem 1, which analyses a *single* usage of QMAC, implies *re-usability*. The reason why this is not completely trivial is that after one execution of π_{QMAC}, the MAC key K is not perfectly secure anymore but "only" almost-perfectly secure, so that Theorem 1 cannot be directly applied anymore for a second execution. However, taking care of this is quite straightforward.

Formally, we have the following result regarding the re-usability of QMAC.

Proposition 5. *If Alice and Bob start off with a uniformly random key, then for a sequence $\pi_{\mathsf{QMAC}}(msg_1)$, $\pi_{\mathsf{QMAC}}(msg_2), \ldots$ of sequential executions of protocol π_{QMAC}, and for any strategy for Eve and any $i \in \mathbb{N}$, the probability ε_i that Eve* modifies *msg_i in the execution of $\pi_{\mathsf{QMAC}}(msg_i)$ yet Bob* accepts *is bounded by*

$$\varepsilon_i \leq (2i-1) \cdot \varepsilon_{\mathsf{MAC}} + \frac{\sqrt{2}}{2} \sum_{j<i} \sqrt{\frac{j}{|\mathcal{C}|}\left(1 + \frac{|\mathcal{C}|}{2^{d/2}}\right)|\mathcal{T}|} \ .$$

Proof. In case $i = 1$, the statement reduces to $\varepsilon_i \leq \varepsilon_{\mathsf{MAC}}$, which holds by construction of QMAC. To argue the general case, let $\rho_{K_1\Theta_1\mathsf{E}_1}, \rho_{K_2\Theta_2\mathsf{E}_2}, \ldots$ describe the evolution of the MAC key and the basis key and Eve's information on them, given that we start with a perfect key $\rho_{K_0\Theta_0\mathsf{E}_0} = \mu_{\mathcal{K}} \otimes \mu_{\mathcal{C}} \otimes \rho_{\mathsf{E}_0}$. Formally, $\rho_{K_i\Theta_i\mathsf{E}_i}$ is inductively defined as $\rho_{K_i\Theta_i\mathsf{E}_i} = \mathcal{E}xe[\pi_{\mathsf{QMAC}}(msg_i)](\rho_{K_{i-1}\Theta_{i-1}\mathsf{E}_{i-1}})$. For the sake of the argument, we also consider $\tilde{\rho}_{K_1\Theta_1\mathsf{E}_1}, \tilde{\rho}_{K_2\Theta_2\mathsf{E}_2}, \ldots$ obtained by means of setting $\tilde{\rho}_{K_0\Theta_0\mathsf{E}_0} = \rho_{K_0\Theta_0\mathsf{E}_0}$ and $\tilde{\rho}_{K_i\Theta_i\mathsf{E}_i} = \mathcal{E}xe[\pi_{\mathsf{QMAC}}(msg_i)](\mu_{\mathcal{K}} \otimes \tilde{\rho}_{\Theta_{i-1}\mathsf{E}_{i-1}})$, i.e., the evolution of the keys and Eve's information in a hypothetical setting where the MAC key is refreshed before every new execution. For these latter states $\tilde{\rho}_{K_i\Theta_i\mathsf{E}_i}$, we can inductively apply Theorem 1 and conclude that

$$\mathrm{Guess}(\Theta_i|\mathsf{E}_i) \leq \frac{i+1}{|\mathcal{C}|}$$

and

$$\delta(\tilde{\rho}_{K_i\Theta_i\mathsf{E}_i}, \mu_{\mathcal{K}} \otimes \tilde{\rho}_{\Theta_i\mathsf{E}_i}) \leq \delta_i := 2\varepsilon_{\mathsf{MAC}} + \frac{\sqrt{2}}{2}\sqrt{\frac{i}{|\mathcal{C}|}\left(1 + \frac{|\mathcal{C}|}{2^{d/2}}\right)|\mathcal{T}|}$$

for any $i \in \mathbb{N}$. But now, for the original states $\rho_{K_1\Theta_1\mathsf{E}_1}, \rho_{K_2\Theta_2\mathsf{E}_2}, \ldots$, from the triangle inequality we obtain that

$$\begin{aligned}
\delta(\rho_{K_i\Theta_i\mathsf{E}_i}, \mu_{\mathcal{K}} \otimes \tilde{\rho}_{\Theta_i\mathsf{E}_i}) &\leq \delta(\rho_{K_i\Theta_i\mathsf{E}_i}, \tilde{\rho}_{K_i\Theta_i\mathsf{E}_i}) + \delta(\tilde{\rho}_{K_i\Theta_i\mathsf{E}_i}, \mu_{\mathcal{K}} \otimes \tilde{\rho}_{\Theta_i\mathsf{E}_i}) \\
&\leq \delta(\rho_{K_{i-1}\Theta_{i-1}\mathsf{E}_{i-1}}, \mu_{\mathcal{K}} \otimes \tilde{\rho}_{\Theta_{i-1}\mathsf{E}_{i-1}}) + \delta_i \\
&\leq \sum_{j \leq i} \delta_j \ ,
\end{aligned}$$

where the last inequality is by induction (where the base case $i = 0$ is trivially satisfied). It now follows by basic properties of the trace distance that we have $\varepsilon_{i+1} \leq \varepsilon_{\mathsf{MAC}} + \sum_{j \leq i} \delta_j$. This proves the claim. □

4.5 Choosing the Parameters

Let $\lambda \in \mathbb{N}$ be the security parameter. Consider a MAC with $\varepsilon_{\mathsf{MAC}} = 2^{-\lambda}$ and $|\mathcal{T}| = 2^{\lambda}$. This can for instance be achieved with the constructions suggested in Sect. 4.2. Also, consider a code $\mathcal{C}$ with $|\mathcal{C}| = 2^{3\lambda}$ and $d = 6\lambda$, so that $|\mathcal{C}|/2^{d/2} = 1$. The description of the basis key θ thus requires 3λ bits, and, by Singleton bound, it is necessary that $n \geq 9\lambda - 1$. Then, the bound in Proposition 5 becomes

$$\varepsilon_{i+1} \leq (2i+1) \cdot 2^{-\lambda} + \sum_{j \leq i} \frac{\sqrt{2}}{2} \sqrt{\frac{j}{2^{3\lambda}} \left(1 + \frac{2^{3\lambda}}{2^{3\lambda}}\right) 2^{\lambda}} = \left(2i + 1 + \sum_{j \leq i} \sqrt{j}\right) 2^{-\lambda} \ .$$

Hence, the error probability increases at most as $\left(i\sqrt{i} + 2i + 1\right)2^{-\lambda}$ with the number i of executions.

5 Extensions and Variations

We show how to modify our scheme QMAC as to offer encryption as well, i.e., to produce an authenticated encryption of *msg*, and how to deal with noise in the quantum communication; we start with the latter since this is more cumbersome. At the end of the section, we show how to tweak our schemes so as to be able to authenticate and/or encrypt *quantum* messages as well, and we discuss some variations.

5.1 Dealing with Noise

In order to deal with noise in the quantum communication, we introduce the following primitive. We consider a keyed hash function $\mathsf{SS} : \mathcal{L} \times \{0,1\}^n \to \mathcal{S}$ that has the property that given the key ℓ, the *secure sketch* $s = \mathsf{SS}(\ell, x)$ of the message x, and a "noisy version" x' of x, i.e., such that $d_H(x, x') \leq \varphi \cdot n$ for some given noise parameter $\varphi < \frac{1}{2}$, the original message x can be recovered except with probability $\varepsilon_{\mathsf{SS}}$. Additionally, we want SS to satisfy the message-independence and ideal key-privacy properties from Definitions 2 and 3. Such constructions exist for small enough $\varphi > 0$, as discussed in Appendix B, based on techniques by Dodis and Smith [8].

Then, the key for our noise-tolerant quantum message authentication code QMAC^* consists of a (initially) uniformly random MAC key $k \in \mathcal{K}$ for MAC, an (initially) uniformly random secure-sketch key $\ell \in \mathcal{L}$ for SS, and an (initially) random and independent basis key θ, chosen from the code $\mathcal{C} \subset \{0,1\}^n$, and the scheme works as described in Figure 2.

Theorem 2. *If the state before the execution of $\pi_{\mathsf{QMAC}^*}(msg)$ is of the form $\rho_{K\Theta E} = \mu_{\mathcal{K}} \otimes \rho_{\Theta E}$, then for any Eve the state $\rho_{K\Theta' E'} = \mathcal{E}xe[\pi_{\mathsf{QMAC}^*}(msg)](\rho_{K\Theta E})$ after the execution satisfies*

$$\mathrm{Guess}(\Theta'|E') \leq \mathrm{Guess}(\Theta|E) + \frac{1}{|\mathcal{C}|}$$

and

$$\delta(KL, U_{\mathcal{K}\times\mathcal{L}}|\Theta'E') \leq 2\varepsilon_{\mathsf{MAC+SS}} + \sqrt{\mathrm{Guess}(\Theta|E)\left(2+\frac{|\mathcal{C}|}{2^{d/2}}+\frac{|\mathcal{C}|\cdot 2^{h(\varphi)n}}{2^d}\right)|\mathcal{T}||\mathcal{S}|}$$

where $\varepsilon_{\mathsf{MAC+SS}} = \varepsilon_{\mathsf{MAC}} + \varepsilon_{\mathsf{SS}}$.

$\mathsf{QMAC}^*.\mathsf{Auth}(k\|\ell\|\theta, msg)$: Choose a uniformly random $x \in \{0,1\}^n$ and output n qubits $B_\circ$ in state $H^\theta|x\rangle$ together with the secure sketch $s = \mathsf{SS}(\ell, x)$ and the tag $t = \mathsf{MAC}(k, msg\|x\|s)$.

$\mathsf{QMAC}^*.\mathsf{Verify}(k\|\ell\|\theta, msg, t)$: Measure the qubits $B_\circ$ in bases θ to obtain x', recover (what is supposed to be) x using the secure sketch s, and check the tag t. If this check fails or $d_H(x, x') > \varphi \cdot n$ then output 0, else 1.

$\mathsf{QMAC}^*.\mathsf{Refresh}(k\|\ell\|\theta)$: Choose uniformly random $\theta' \in \mathcal{C}$ and output $k\|\ell\|\theta'$.

Fig. 2. The noise-tolerant quantum message authentication code MAC^*.

Proof. The proof of the first statement, i.e., the bound on $\mathrm{Guess}(\Theta'|E')$ is exactly like in the proof of Theorem 1, with the only exception that in the one expression where the tag T appears (i.e. in the expression obtained by using Property 1), now S appears as well (along with T); but like T, it disappears again in the next step due to message-independence.

For the bound on $\delta(KL, U_{\mathcal{K}\times\mathcal{L}}|\Theta'E')$ we follow closely the proof of Theorem 1 but with the following modifications.

1. The key K is replaced by the key pair (K, L), and the tag T by the tag-secure-sketch pair (T, S), and we observe that we can understand (T, S) to be the hash of the input X under key (K, L) with respect to a hash function that satisfies message-independent and (almost) key-privacy. Indeed, this composed hash function can be understood as being obtained by means of Proposition 4. As such, whenever we argue by means of message-independence (Definition 2) or key-privacy (Definition 3) in the proof of Theorem 1, we can still do so, except that we need to adjust the bound on the uniformity of the key to the new — and now composite — hash function.
2. The auxiliary random variable $\tilde{D}$, and correspondingly $\tilde{\Theta}'$, is defined in a slightly different way: $\tilde{D}$ is 1 if $X \approx_\varphi X'$ and Eve has not modified the tag T, the secure-sketch S, nor the message *msg*. The "real" state with D and Θ' is then $(\varepsilon_{\mathsf{MAC}} + \varepsilon_{\mathsf{SS}})$-close to the modified one with $\tilde{D}$ and $\tilde{\Theta}'$ instead. Correspondingly, the decomposition of the distance to be bounded is then done with respect to the indicated random variable $1_{X\approx_\varphi X'}$ instead of $1_{X=X'}$.

3. When bounding the probability $P[X \approx_\varphi X' \wedge X = X'']$, we refer to the game analyzed in Corollary 3 in Appendix A, which applies to the situation here where some slack is given for Bob's guess.

The claimed bound is then obtained by adjusting terms according to the above changes: update the bounds obtained by applying Definition 3 to the updated bound $\sqrt{\text{Guess}(X|\cdots)\,|\mathcal{T}|\,|\mathcal{S}|}$, obtained by means of Proposition 4, and inserting the $2^{h(\varphi)n}$ blow-up when using Corollary 3 instead of Corollary 1, but making use of the observation in Remark 6. □

In essence, compared to the case with no noise, we have an additional loss due to the $|\mathcal{S}|$ term, whereas we can neglect the term with $2^{h(\varphi)n}$ for small enough φ. To compensate for this additional loss, we need to have $\varsigma = \log|\mathcal{S}|$ additional bits of entropy in Θ, i.e., we need to choose $\mathcal{C}$ with $|\mathcal{C}| = 2^{3\lambda+\varsigma}$ and $d = 6\lambda + 2\varsigma$. By Singleton bound, this requires $n \geq 9\lambda + 3\varsigma - 1$, and thus puts a bound $\varsigma < n/3$ on the size of the secure sketch, and thus limits the noise parameter φ.[11]

5.2 Adding Encryption

Adding encryption now works pretty straightforwardly. Concretely, our quantum encryption scheme with key recycling QENC^* is obtained by means of the following modifications to QMAC^*. Alice and Bob extract additional randomness from x using an extractor that offers message-independence and key-privacy, and use the extracted randomness as one-time-pad key to en-/decrypt *msg*. Finally, the resulting ciphertext c is authenticated along with x and s; this is in order to offer authenticity as well and can be omitted if privacy is the only concern.

Security can be proven along the same lines as Theorem 1, respectively Theorem 2 for the noise-tolerant version, and Proposition 5: we simply observe by means of Proposition 3 and 4 that the composition of computing the triple c, s and $t = \mathsf{MAC}(k, x\|c\|s)$ from x constitutes a keyed hash function that offers message-independence and key-privacy, and then we can argue exactly as above to show that the (possibly refreshed) key stays secure over many executions. Also, given that the key is secure before an execution, we can control the min-entropy in X as in the proof of Theorem 2 and argue almost-perfect security of the extracted one-time-pad key, implying privacy of the communicated message.

In order to accommodate for the additional entropy that is necessary to extract this one-time-pad key, which is reflected in the adjusted range of the composed keyed hash function, we now have to choose $\mathcal{C}$ with $|\mathcal{C}| = 2^{3\lambda+\varsigma+m}$ and $d = 6\lambda + 2\varsigma + 2m$, where $m = \log|\mathcal{MSG}|$; this requires $n \geq 9\lambda + 3\varsigma + 3m - 1$ by Singleton bound.

[11] We recall that, when using a δ-biased family of codes to construct the secure sketch SS, as discussed in the Appendix B, then ς does not correspond exactly to the size of the syndrome given by the code, but is determined by the parameter δ, and is actually somewhat larger than the size of the syndrome.

5.3 Optimality of the Key Recycling

Our aim was, like in [5, 6], to minimize the number of fresh random bits needed for the key refreshing. In our constructions, where the key is refreshed simply by choosing a new basis key θ, this number is obviously given by the number of bits needed to represent θ, i.e., in the above encryption scheme QENC^*, it is

$$\log |\mathcal{C}| = 3\lambda + \varsigma + m \ .$$

This is close to optimal for large messages and assuming almost no noise, so that $m \gg \lambda, \varsigma$. Indeed, assuming that Eve knows the encrypted message, i.e., we consider a known-plaintext attack, it is not hard to see that for any scheme that offers (almost) perfect privacy of the message, by simply keeping everything that is communicated from Alice to Bob, in particular by keeping all qubits that Alice communicates (which will most likely trigger Bob to reject), Eve can always learn (almost) m bits of Shannon information on the key. As such, it is obviously necessary that the key is updated with (almost) m fresh bits of randomness in case Bob rejects, since otherwise Eve will soon have accumulated too much information on the key.

Note that [5, 6] offers a rigorously proven bound (of roughly m) on the number of fresh bits necessary for key refreshing. However, their notion of key refreshing is stronger than what we require: they require that the refreshed key is close to random and independent of Eve, whereas we merely require that the refreshed key is "secure enough" as to ensure security of the primitive, i.e., authenticity in QMAC or QMAC^*, and privacy (and authenticity) in QENC^*. Indeed, in our construction we do not require that the basis key is close to random, only that it is hard to guess. However, the above informal argument shows that the bound still applies.

Similarly, one can argue that in any message authentication scheme with error probability $2^{-\lambda}$, by keeping everything Eve can obtain λ bits of information on the key. Thus, in case of almost no noise, our scheme QMAC^* is optimal up to the factor 3.

In our constructions, the number of fresh random bits needed for the key refreshing increases with larger noise. In particular in QMAC^*, ς will soon be the dominating term in case we increase the noise level. We point out that it is not clear whether such a dependency is necessary, as we briefly mention in Sect. 6.

5.4 Supporting Quantum Messages

The approach in Sect. 5.2 of extracting a (one-time pad) key also gives us the means to authenticate and/or encrypt *quantum* messages: we simply use the extracted key as quantum-one-time-pad key [1], or as key for a quantum message authentication code [4]. However, when considering arbitrary quantum messages, honest users anyway need a quantum computer, so one might just as well use the scheme by Damgård *et al.* to communicate a secret key and use this key for a quantum-one-time-pad or for quantum message authentication, or resort to [10, 16], which additionally offer security against superposition attacks.

5.5 Variations

We briefly mention a few simple variations of our schemes. The first variation is as follows. In QMAC, instead of choosing x uniformly at random and computing the tag t as $t = \mathsf{MAC}(k, msg\|x)$, we can consider a fixed tag $t_\circ \in \mathcal{T}$, and choose x uniformly at random subject to $\mathsf{MAC}(k, msg\|x) = t_\circ$. Since $t_\circ$ is fixed, it does not have to be sent along. In case the classical MAC, as a keyed hash function, is of the form as in Proposition 2, meaning that the tag is one-time-pad encrypted (which in particular holds for the canonical examples suggested in Sect. 4.2), then Theorem 1 and Proposition 5 still hold. Indeed, if MAC is of this form then the concrete choice of $t_\circ$ is irrelevant for security: if Theorem 1 would fail for one particular choice of $t_\circ$ then it would fail for any choice, and thus also for a randomly chosen tag, which would then contradict Theorem 1 for the original QMAC. Similarly, in QMAC^* and QENC^* we can fix the tag t and the secure sketch s (and ciphertext c), and choose x subject to the corresponding restrictions.

A second variation is to choose the basis key θ not as a code word, but uniformly random from $\{0,1\}^n$. As a consequence, the bounds on the games analyzed in Sect. 3.1 change — indeed, the game analyzed in Proposition 1 then becomes the monogamy-of-entanglement game considered and analyzed in [19] — and therefore we get different bounds in Theorem 1, but conceptually everything should still work out. Our goal was to minimize the number of fresh random bits needed for the key refreshing, which corresponds to the number of bits necessary to describe θ; this allows us to compare our work with [5, 6] and show that our encryption scheme performs (almost) as good as theirs in this respect. And with this goal in mind, it makes sense to choose θ as a codeword: it gives the same guessing probability for x but asks for less entropy in θ. Choosing θ uniformly random from $\{0,1\}^n$ seems to be the preferred choice for minimizing the quantum communication instead, which would be a very valid objective too.

As an interesting side remark, we observe that with the above variations, our constructions can be understood as following the design principle of the scheme originally proposed by Bennett *et al.* of encrypting and adding redundancy to the message, and encoding the result into BB84 qubits.

Finally, a last variation we mention is to use the *six-state* encoding instead of the BB84 encoding. Since the three bases of the six-state encoding have the same so-called maximal overlap, the bounds in Sect. 3.1 carry over unchanged, but we get more freedom in choosing the code $\mathcal{C}$ in $\{0,1,2\}^n$ so that fewer qubits need to be communicated for the same amount of entropy in x. Also, when choosing the bases uniformly at random in $\{0,1,2\}^n$, as in the variation above, we get a slightly larger entropy for x when using the six-state encoding.

6 Conclusion, and Open Problems

We reconsider one of the very first problems that was posed in the context of quantum cryptography, even before QKD, and we give the first solution that

offers a rigorous security proof *and* does not require any sophisticated quantum computing capabilities from the honest users. However, our solution is not the end of the story yet. An intriguing open problem is whether it is possible to do the error correction in a more straightforward way, by just sending the syndrome of x with respect to a *fixed* suitable code, rather than relying on the techniques from [8]. In return, the scheme would be simpler, it could take care of more noise — Dodis and Smith are not explicit about the amount of noise their codes can correct but it appears to be rather low — and, potentially, the number of fresh random bits needed for key refreshing might not grow with the amount of noise. Annoyingly, it *looks* like our scheme should still be secure when doing the error correction in the straightforward way, but our proof technique does not work anymore, and there seems to be no direct fix.

From a practical perspective, it would be interesting to see to what extent it is possible to optimize the quantum communication rather than the key refreshing, e.g., by using BB84 qubits with fully random and independent bases, and whether is it possible to beat QKD in terms of quantum communication.

Acknowledgments

The authors would like to thank Ivan Damgård and Christian Schaffner for interesting discussions related to this work, and Christopher Portmann for comments on an earlier version of the paper.

References

1. A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. In *41st IEEE FOCS*, pp. 547–553 (2000).
2. C.H. Bennett, and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems & Signal Processing*, pp. 175–179, 1984.
3. C.H. Bennett, G. Brassard, and S. Breidbart. Quantum cryptography II: How to re-use a one-time pad safely even if $P=NP$. In *Natural Computing*, 13(4):453–458 (2014).
4. H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *43rd IEEE FOCS*, pp. 449–458 (2002).
5. I. Damgård, T. Brochmann Pedersen, L. Salvail. A quantum cipher with near optimal key-recycling. In *CRYPTO 2005*, vol. 3621 of *LNCS*, pp. 494–510 (2005).
6. I. Damgård, T. Brochmann Pedersen, L. Salvail. How to re-use a one-time pad safely and almost optimally even if $P=NP$. In *Natural Computing*,13(4):469–486 (2014).
7. I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *CRYPTO 2007*, vol. 4622 of *LNCS*, pp. 342–359 (2007).
8. Y. Dodis and A. Smith. Correcting errors without leaking partial information. In *37th ACM STOC*, pp. 654–663 (2005).

9. S. Fehr and C. Schaffner. Randomness extraction via delta-biased masking in the presence of a quantum attacker. In *TCC 08*, vol. 4948 of *LNCS*, pp. 465–481 (2008).
10. S. Garg, H. Yuen, and M. Zhandry. New security notions and feasibility results for authentication of quantum data. Manuscript, `arXiv:1607.07759v1` (2016)
11. P. Hayden, D. Leung, and D. Mayers. Universal composable security of quantum message authentication with key recycling. Talk at *QCRYPT 2011*, Zürich (2011)
12. R. König, R. Renner and C. Schaffner. The operational meaning of min- and max-entropy. In *IEEE Transactions on Information Theory*, 55(9):4337–4347 (2009).
13. D. Leung. Quantum Vernam Cipher. In *Quantum Information & Computation*, 2(1):14–34 (2002).
14. N. Nisan and D. Zuckerman. Randomness is linear in space. In Journal of Computer and System Sciences, 52(1):43–52 (1996).
15. J. Oppenheim, and M. Horodecki. How to reuse a one-time pad and other notes on authentication, encryption and protection of quantum information. In *Physical Review A*, vol 72: 042309 (2005).
16. C. Portmann. Quantum authentication with key recycling. Manuscript, `arxiv.org/abs/1610.03422v1` (2016), also to appear in these proceedings.
17. R. Renner. Security of Quantum Key Distribution. PhD thesis, ETH Zürich, No. 16242 (2005).
18. J. Radhakrishnan, and A. Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. In *SIAM Journal on Computing*, 13(1):2–24 (2000).
19. M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. One-sided device independent QKD and position-based cryptography from monogamy games. In *EUROCRYPT 2013*, vol. 7881 of *LNCS*, pp. 609–625 (2013).

APPENDIX

A Yet Another (Version of the) Guessing Game

We consider a variant of the guessing game from Section 3.1 where Bob and Charlie need to guess Alice's measurement outcome. In the variation considered here, we give some slack to Bob in that it is good enough if his guess is close enough (in Hamming distance) to Alice's measurement outcome, and Charlie is given some (deterministic) classical side information on Alice's measurement outcome before he has to announce his guess.[12] We show that, if the minimal distance d of the code $\mathcal{C}$ is large enough, this does not help Bob and Charlie significantly. This is in line with the intuition that, for large enough d, the optimal strategy for Bob and Charlie is to pre-guess Alice's choice of bases.

Proposition 6. *Let $\mathcal{H}_A$ be a n-qubit system, and let $\mathcal{H}_B$ and $\mathcal{H}_C$ be arbitrary quantum systems. Also, let $0 \leq \varphi \leq \frac{1}{2}$ be a parameter and $f : \{0,1\}^n \to \mathcal{Y}$ a function. Consider a state $\rho_{\Theta ABC} = \mu_{\mathcal{C}} \otimes \rho_{ABC} \in \mathcal{D}(\mathcal{C} \otimes \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, and let*

$$\rho_{\Theta X X' X''} = \mathcal{N}_{\Theta f(X) C \to X''} \circ \mathcal{N}_{\Theta B \to X'} \circ \mathcal{M}^{\text{BB84}}_{\Theta A \to X}\big(\rho_{\Theta ABC}\big)$$

[12] Taking care of such side information, given to Charlie, on Alice's measurement outcome is not needed for our application, but we get it almost for free.

where $\mathcal{N}_{\Theta B\to X'}$ is an arbitrary measurement of system B controlled by Θ, and $\mathcal{N}_{\Theta f(X)C\to X''}$ is an arbitrary measurement of system C controlled by Θ and $f(X)$. Then, it holds that

$$P[X'\approx_\varepsilon X\wedge X''=X]\leq\frac{1}{|\mathcal{C}|}+\frac{2^{h(\varphi)n}\cdot|\mathcal{Y}|}{2^{d/2}}\ ,$$

where h is the binary entropy function.

Proof. Here, we can write

$$P[X'\approx_\varepsilon X\wedge X''=X]=\frac{1}{|\mathcal{C}|}\left\|\sum_\theta\tilde{\Pi}^\theta\right\|\leq\frac{1}{|\mathcal{C}|}\sum_\delta\max_\theta\left\|\tilde{\Pi}^\theta\tilde{\Pi}^{\theta\oplus\delta}\right\|$$

for projectors

$$\tilde{\Pi}^\theta=\sum_x H^\theta|x\rangle\langle x|H^\theta\otimes\left(\sum_{e\in B_\varphi^n}P^\theta_{x\oplus e}\right)\otimes Q_x^{\theta,f(x)}\ ,$$

where $B_\varphi^n\subset\{0,1\}^n$ denotes the set of stings with Hamming weight at most φn. For any $\theta\neq\theta'\in\mathcal{C}$, we can upper bound $\tilde{\Pi}^\theta$ and $\tilde{\Pi}^{\theta'}$ by

$$\tilde{\Pi}^\theta\leq\tilde{\Gamma}^\theta:=\sum_x H^\theta|x\rangle\langle x|H^\theta\otimes\left(\sum_{e\in B_\varphi^n}P^\theta_{x\oplus e}\right)\otimes\mathbb{I}=\sum_{e\in B_\varphi^n}\Gamma_e^\theta$$

and

$$\tilde{\Pi}^{\theta'}\leq\tilde{\Delta}^{\theta'}:=\sum_x H^{\theta'}|x\rangle\langle x|H^{\theta'}\otimes\mathbb{I}\otimes\left(\sum_{y\in\mathcal{Y}}Q_x^{\theta',y}\right)=\sum_{y\in\mathcal{Y}}\Delta_y^{\theta'}$$

respectively, where Γ_e^θ and $\Delta_y^{\theta'}$ are like Γ^θ and $\Delta^{\theta'}$, as defined in the proof of Proposition 1, for certain concrete choices of the POVM's $\{P_x^\theta\}_x$ and $\{Q_x^{\theta'}\}_x$ that depend on e and y, respectively. As such, we get that

$$\left\|\tilde{\Pi}^\theta\tilde{\Pi}^{\theta'}\right\|\leq\left\|\tilde{\Gamma}^\theta\tilde{\Delta}^{\theta'}\right\|\leq\sum_{e,y}\left\|\Gamma_e^\theta\Delta_y^{\theta'}\right\|\leq\frac{|B_\varphi^n|\cdot|\mathcal{Y}|}{2^{d/2}}\leq\frac{2^{h(\varphi)n}\cdot|\mathcal{Y}|}{2^{d/2}}\ .$$

Since we still have that $\left\|\tilde{\Pi}^\theta\tilde{\Pi}^\theta\right\|=\left\|\tilde{\Pi}^\theta\right\|=1$, the claim follows. □

By means of the techniques from Section 3.1, we can extend the result to the case where Bob and Charlie have a-priori quantum side information on Alice's choice of bases.

Corollary 3. *Let $\mathcal{H}_\mathsf{A}$ be a n-qubit system, and let $\mathcal{H}_\mathsf{B},\mathcal{H}_\mathsf{C}$ and $\mathcal{H}_\mathsf{E}$ be arbitrary quantum systems. Also, let $0\leq\varphi\leq\frac{1}{2}$ be a parameter and $f:\{0,1\}^n\to\mathcal{Y}$ a function. Consider a state $\rho_{\Theta\mathsf{E}}\in\mathcal{D}(\mathcal{C}\otimes\mathcal{H}_\mathsf{E})$, and let*

$$\rho_{\Theta\mathsf{ABC}}=\mathcal{Q}_{\mathsf{E}\to\mathsf{ABC}}\big(\rho_{\Theta\mathsf{E}}\big)\in\mathcal{D}(\mathcal{C}\otimes\mathcal{H}_\mathsf{A}\otimes\mathcal{H}_\mathsf{B}\otimes\mathcal{H}_\mathsf{C})$$

where $\mathcal{Q}_{E\to ABC}$ is a CPTP map acting on E, and let

$$\rho_{\Theta X X' X''} = \mathcal{N}_{\Theta f(X) C\to X''} \circ \mathcal{N}_{\Theta B\to X'} \circ \mathcal{M}^{\text{BB84}}_{\Theta A\to X}\big(\rho_{\Theta ABC}\big)$$

as in Proposition 6 above. Then, it holds that

$$P[X' \approx_\varepsilon X \wedge X'' = X] \leq \mathrm{Guess}(\Theta|E) + \frac{\mathrm{Guess}(\Theta|E)\cdot|\mathcal{C}|\cdot 2^{h(\varphi)n}\cdot|\mathcal{Y}|}{2^{d/2}} \ .$$

Remark 6. In line with the remarks in Section 3.1, if Bob "measures correctly" but is still given some slack, and, say, Charlie is given no side information on Alice's outcome, the bound relaxes to

$$P[X' \approx_\varepsilon X \wedge X'' = X] \leq \mathrm{Guess}(\Theta|E) + \frac{\mathrm{Guess}(\Theta|E)\cdot|\mathcal{C}|\cdot 2^{h(\varphi)n}}{2^{d}} \ .$$

B On the Existence of Suitable Secure Sketches

In [8, Lemma 5], Dodis and Smith show that for any constant $0 < \lambda < 1$, there exists an explicitly constructible family of binary linear codes $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ in $\{0,1\}^n$ with dimension k that efficiently correct a constant fraction of errors and have square *bias* $\delta^2 \leq 2^{-\lambda n}$. Their Lemma 4 then shows that the keyed hash function $\mathsf{Ext} : \mathcal{I}\times\{0,1\}^n \to \mathcal{SYN} = \{0,1\}^{n-k}$, $(i,x)\mapsto syn_i(x)$ is a strong extractor, where $syn_i(x)$ is the syndrome with respect to the code $\mathcal{C}_i$. More precisely, the generalization of their result to quantum side information by Fehr and Schaffner [9] shows that if $\rho_{IXE} = \mu_{\mathcal{I}}\otimes\rho_{XE} \in \mathcal{D}(\mathcal{I}\otimes\mathcal{X}\otimes\mathcal{H}_E)$ then

$$\delta(\rho_{\mathsf{Ext}(I,X)IE}, \mu_{\mathcal{SYN}}\otimes\rho_I\otimes\rho_E) \leq \frac{1}{2}\sqrt{\mathrm{Guess}(X|E)\,\delta^2\,2^n} \ .$$

It follows from Proposition 2 that the secure sketch

$$\mathsf{SS} : \mathcal{L}\times\{0,1\}^n \to \mathcal{SYN},\ (i\|b, x)\mapsto syn_i(x)+b$$

where $\mathcal{L} := \mathcal{I}\times\mathcal{SYN}$, offers uniformity and ν-key-privacy with parameter $\nu = \delta 2^{n/2}/\sqrt{|\mathcal{SYN}|} = \delta 2^k$.

Dodis and Smith are not explicit about the *size* $n-k$ of the syndrome in their construction, but looking at the details, we see that $n-k \leq \log(\delta^2\,2^n)$. As such, by artificially extending the range $\mathcal{SYN} = \{0,1\}^{n-k}$ of SS to a set $\mathcal{S} = \{0,1\}^\varsigma$ of bit strings of size $\varsigma := \log(\delta^2\,2^n)$, and re-defining SS to map $(i\|b,x)$ to $syn_i(x)+b$ *padded with sufficiently many* 0*'s*, we get that the secure sketch $\mathsf{SS} : \mathcal{L}\times\{0,1\}^n \to \mathcal{S}$ is message-independent and offers *ideal* key-privacy.[13]

[13] Alternatively, we could simply stick to $\mathsf{SS} : \mathcal{L}\times\{0,1\}^n \to \mathcal{SYN}$ but carry along the non-ideal parameter ν; however, we feel that this additional parameter would make things more cumbersome — but of course would lead to the same end result.