(Quantum) Min-Entropy Resources

Christopher Portmann*[1,2]

[1]Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland.
[2]Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.

May 30, 2017

Abstract

We model (interactive) resources that provide Alice with a string X and a guarantee that any Eve interacting with her interface of the resource obtains a (quantum) system E such that the conditional (smooth) min-entropy of X given E is lower bounded by some k, $H_{\min}^{\delta}(X|E) \geq k$. This (abstract) resource specification encompasses any setting that results in the honest players holding such a string (or aborting). For example, it could be constructed from, e.g., noisy channels, quantum key distribution (QKD), or a violation of Bell inequalities, which all may be used to derive bounds on the min-entropy of X.

As a first application, we use this min-entropy resource to modularize key distribution (KD) schemes by dividing them in two parts, which may be analyzed separately. In the first part, a KD protocol constructs a min-entropy resource given the (physical) resources available in the specific setting considered. In the second, it distills secret key from the min-entropy resource — i.e., it constructs a secret key resource. We prove security for a generic key distillation protocol that may use any min-entropy resource. Since the notion of resource construction is composable — security of a composed protocol follows from the security of its parts — this reduces proving security of a KD protocol (e.g., QKD) to proving that it constructs a min-entropy resource.

As a second application, we provide a composable security proof for the recent Fehr-Salvail protocol [EUROCRYPT 2017] that authenticates classical messages with a quantum message authentication code (Q-MAC), and recycles all the key upon successfully verifying the authenticity of the message. This protocol uses (and recycles) a non-uniform key, which we model as consuming and constructing a min-entropy resource.

*chportma@ethz.ch

1 Introduction

When formalizing information processing systems, one models the information that matters, e.g., the input and output values of the system. A concrete implementation is much more complex, e.g., values are output at certain times, encoded in some physical form. If the exact physical encoding or timing information is not considered relevant, this is generally not modeled as part of the abstract representation of the information processing system. Such a model can be described as a *specification* of a system, since it specifies certain behaviors that the system must have, but leaves many (irrelevant) parameters unspecified.

The level of specification of information processing systems found in the literature is often fixed, e.g., the Universal Composability (UC) framework [1, 2] provides a concrete model of systems in terms of interactive Turing machines, and all objects in the framework must be specified in the given language (or something equivalent) with the given level of specificity. Using such a framework, one can neither model more specific objects (e.g., a protocol run at a specific location in time and space), nor less specific objects (e.g., a non-deterministic behavior), and even less compose such objects with each other.

The Abstract Cryptography (AC) framework [3] uses a top-down approach to model cryptographic security, which does not have this limitation. The more traditional bottom-up approach starts with a concrete model of information processing systems, then defines how these systems communicate, how scheduling is performed, how parties are corrupted, etc. Instead of this, AC starts on the most abstract level. It models abstract objects satisfying certain axioms that are needed to make cryptographic statements. These objects can then be instantiated with, e.g., different models of computation, communication, scheduling, etc. In particular, as done in [4], AC can be instantiated with a model of *resource specifications*, where two resources satisfy a relation $\mathcal{R} \subset \mathcal{S}$, if $\mathcal{R}$ is more specific than $\mathcal{S}$, i.e., any concrete system satisfying the specifications of $\mathcal{R}$ also satisfies those of $\mathcal{S}$. Such resource specifications can be composed and a security statements about the composed system may be derived from the framework.

1.1 Contributions

Our main contribution is to use the concept of resource specifications [3–6] to model min-entropy resources, i.e., systems that provide honest player(s) with a random string X and an adversary with a (possibly quantum) system E such that the joint state ρ_{XE} has bounded conditional (smooth) min-entropy,[1] $H_{\min}^{\delta}(X|E)_{\rho} \geq k$. The same techniques could be used for other entropy measures. The reason we choose the smooth min-entropy, is that it

[1] A formal definition of smooth min-entropy is provided in Appendix A.3.

has many applications in cryptography, e.g., it caracterizes the maximum amount of secret key that can be extracted from a source [7].

Specifications are essential in modeling min-entropy resources, since we generally do not know (and do not care) how the joint state ρ_{XE} was generated — whether the adversary can influence it or not, whether this is done with one round or multiple rounds of interaction. Any system which interacts arbitrarily with the adversary, but provides a random string X to the honest player(s) with a guaranteed lower bound on its conditional min-entropy satisfies the specification, and can be used by protocols requiring such a bound.

We then present two applications in which these min-entropy specifications are needed to model the security of cryptographic schemes. In the first, we show how to distill secret key from any min-entropy resource shared between two players. The protocol is standard, it uses error correction and privacy amplification to construct a secret key resource. But the proof is not restricted to a certain context or specific source of randomness, it is valid for any min-entropy resource, e.g., whether it is constructed by noisy classical channels [8–10], standard quantum key distribution (QKD) [7, 11–14] or even untrusted (but non-communicating) devices [15–18]. We discuss this application further in Section 1.2.

Our second application is to provide a composable security proof for a recent authentication protocol by Fehr and Salvail [19, 20], that encodes classical messages in quantum states. Due to the quantum properties of these states, all of the secret key used in the protocol can be recycled once the recipient has confirmed the authenticity of the message. But a small loss of entropy occurs in the key, so it cannot be modeled as a standard (uniform) key resource [21]. Instead, we model the shared key as a min-entropy specification, and prove that a slightly modified version [20] of the original Fehr-Salvail protocol [19] uses a min-entropy resource and an insecure channel to construct an authentic channel and a new min-entropy resource (the recycled key). This result is discussed further in Section 1.3.

1.2 Distilling Secret Key

Secret key distillation from a joint probability distribution P_{XYE} between three players, Alice, Bob, and Eve, was proposed independently by Maurer [8] and by Ahlswede and Csiszár [9]. This problem has since been generalized to many different contexts, e.g., in a finite setting [10], when E is quantum and the tripartite state ρ_{XYE} has been obtained from a QKD protocol [7, 12–14], or in a device-independent setting, where the devices generating ρ_{XYE} are untrusted [17, 18]. The protocols always follow the same pattern: if needed, one performs some *advantage distillation* to increase the correlations between the honest players, then one performs *error correction* so that they share the same strings, and finally *privacy amplification* to extract a secret key. The

different security proofs found in the literature that one can obtain secret key given a bound on the correlations of the state ρ_{XYE} are very similar, with (small) variations to account for the changes in context.

This overlap between different works can be avoided by employing a modular (composable) approach: a task is divided in different parts, and the security of each part is proven separately. Thus, if one part is changed, only that piece requires a new security proof; the new piece can then be seamlessly plugged into the other parts. The AC framework [3, 4] formalizes this as a resource theory: a cryptographic protocol uses some resource specification $\mathcal{R}$ to construct some other resource specification $\mathcal{S}$. Different protocols may be used to construct $\mathcal{S}$ in different ways. The next part of a cryptosystem may use $\mathcal{S}$ to construct $\mathcal{T}$, and is oblivious to how $\mathcal{S}$ was constructed. The piece constructing $\mathcal{S}$ may be changed at will, without affecting anything else.

More concretely, we prove in this work that a min-entropy resource may be used to construct a secret key resource — using the aforementioned steps of error correction and privacy amplification. As a consequence, information-theoretic key distribution protocols (e.g., QKD) do not need to show that they produce secret key (and needlessly repeat many of the steps), it is sufficient to prove that they construct a min-entropy resource, i.e., that they generate a raw key with a bound on its min-entropy. Bounds on the security of the final key then follow generically from the composability of the AC framework by plugging this into our work.

This also provides clear conditions on the min-entropy of the raw key that are sufficient for the error correction and privacy amplification to go through (namely, that the constructed resource corresponds to a min-entropy specification, which we define in Section 3).

1.3 Quantum Authentication of Classical Messages

As far back as 1982, Bennett, Brassard, and Breidbart [22] discussed how one could authenticate a classical message in a quantum state, so that after confirming reception of the original message, the secret key used by the protocol can be reused. A recent breakthrough result by Fehr and Salvail [19, 20] showed how to do this with a *prepare-and-measure* protocol, i.e., one which involves only preparing and measuring single qubit states, and which could already be implemented with today's technology [23]. This has many interesting applications, e.g., it could be used as a subroutine for authenticating messages in QKD.[2] One would then not need to sacrifice any key bits for authentication.

Fehr and Salvail use a trace-distance-type security criterion that is tailored for substitution attacks — Eve changes the message being sent. They then show that this criterion is sufficient to prove that their protocol can be

[2] Whether this application is practical depends on the noise tolerance of the Fehr-Salvail protocol, which was has not been worked out [19].

composed sequentially with itself. Different contexts, such as sequential composition with other protocols,[3] parallel composition,[3] or impersonation attacks — Eve sends a forged cipher to Bob without knowledge of a valid message-cipher pair — were not explicitly considered in [19].[4] When key recycling is involved, impersonation attacks are particularly powerful, because they allow Eve to obtain part of the recycled key after Bob receives the forged cipher (e.g., he uses it in a protocol which leaks it, like a one-time pad), which she can use to generate a message correlated to the key and provide it to Alice for authentication. The resulting cipher could then potentially leak more information about the remaining secret key than a cipher prepared by Alice under a substitution attack, where the message and key are independent. Note that even if the protocol is only composed in a restricted setting in which the recycled key is not leaked, the accept/reject bit of the receiver is generally correlated to the recycled key and cannot be hidden, which leads to the same type of attacks.

This raises the question of whether there are other attacks or vulnerabilities that have not been considered, and what security criteria must be satisfied for the protocol to be usable, e.g., as a subroutine in QKD. This is answered in a generic way by composable frameworks. In the AC language, a QKD protocol uses an authentic channel resource specification $\mathcal{A}$ for the players to communicate [21]. A standard authentication scheme that appends a message authentication code (MAC) to the message constructs such an authentic channel $\mathcal{A}$ [24]. And hence, by the composition theorem of the framework, the two may be composed, and the total error is the sum of the errors of the individual protocols.

In this work we perform such a composable analysis for a slightly modified version [20] of the original Fehr-Salvail protocol [19]. We show that this protocol uses a min-entropy resource $\mathcal{H}^k_{\min}$, a uniform key resource $\mathcal{K}$, and an insecure channel $\mathcal{Q}$ to construct a new min-entropy resource $\mathcal{H}^k_{\min}$, a new uniform key $\mathcal{K}$, and an authentic channel $\mathcal{A}$. The constructed channel $\mathcal{A}$ may then be used by any protocol requiring such a resource, while the constructed key resources $\mathcal{H}^k_{\min}$ and $\mathcal{K}$ (the recycled keys) may be plugged into the next round of authentication — or any other protocol requiring such keys.

[3] Ad hoc security definitions for individual protocols — e.g., trace-distance-type criteria — do not necessarily guarantee that a composed protocol is secure. When using such definitions, one needs to additionally prove (for every different context) that the protocol can be safely used, and work out the corresponding error. For example, Fehr and Salvail do this for sequential composition of their protocol with itself [19]. This can be avoided by using composable security definitions — e.g., the notion of resource construction from AC — which guarantee security in any environment. The error of the composed protocol is then the sum of the erros of the individual components.

[4] Following an initial draft of the current work pointing out the issue with impersonation attacks and proposing a solution that recycles less key in the case of a reject, an extended version of the Fehr-Salvail paper was made available [20], which sketches how the protocol can be modified to resist impersonation attacks without any extra loss of key.

1.4 Structure of the paper

We start by introducing the AC framework in Section 2, where we instantiate the systems with resource specifications. In Section 3 we then define the min-entropy specifications that are used throughout this work. In Section 4 we show how to distill secret key from such a min-entropy resource. And in Section 5 we provide a composable security proof for the Fehr-Salvail authentication protocol, in which the non-uniform keys are modeled as min-entropy resources.

2 Constructive Cryptography

The AC framework [3, 4] models cryptography as a resource theory, e.g., a QKD protocol constructs a secret key resource from an authentic channel and an insecure quantum channel. More generally, a security statement is a constructive statement of the form "γ constructs $\mathcal{S}$ from $\mathcal{R}$ with error ε," which we denote

$$\mathcal{R} \xrightarrow{\gamma,\varepsilon} \mathcal{S}. \tag{1}$$

For this reason the framework is also called *constructive cryptography* in the literature [4, 25].

In (1), $\mathcal{R}$ and $\mathcal{S}$ are resource specifications denoting the resources that are used by the construction and the ones that are achieved by the construction γ, respectively. Naturally, if γ constructs $\mathcal{S}$ from $\mathcal{R}$ and π constructs $\mathcal{T}$ from $\mathcal{S}$, then one expects that applying both constructions in sequence constructs $\mathcal{T}$ from $\mathcal{R}$ with an error which is the sum of the individual errors, i.e.,

$$\mathcal{R} \xrightarrow{\gamma,\varepsilon} \mathcal{S} \quad \text{and} \quad \mathcal{S} \xrightarrow{\pi,\delta} \mathcal{T} \implies \mathcal{R} \xrightarrow{\pi\circ\gamma,\varepsilon+\delta} \mathcal{T}. \tag{2}$$

Similarly, if γ_1 constructs $\mathcal{S}_1$ from $\mathcal{R}_1$ and γ_2 constructs $\mathcal{S}_2$ from $\mathcal{R}_2$, then one expects that if resources $\mathcal{R}_1$ and $\mathcal{R}_2$ are both available simultaneously, and one applies both constructions, this should result in the resources $\mathcal{S}_1$ and $\mathcal{S}_2$ both being constructed, i.e.,

$$\mathcal{R}_1 \xrightarrow{\gamma_1,\varepsilon_1} \mathcal{S}_1 \quad \text{and} \quad \mathcal{R}_2 \xrightarrow{\gamma_2,\varepsilon_2} \mathcal{S}_2 \implies \mathcal{R}_1\|\mathcal{R}_2 \xrightarrow{\gamma_1|\gamma_2,\varepsilon_1+\varepsilon_2} \mathcal{S}_1\|\mathcal{S}_2. \tag{3}$$

In the rest of this section we formalize the notions of resource specifications and construction, which allows us to define constructive security statement such as Eq. (1) and prove that Eqs. (2) and (3) hold with this notion of construction. We do this following the AC top-down approach, i.e., we only define the properties of the objects that are needed, allowing them to be instantiated with any concrete model that satisfies these properties.

(a) A noiseless channel.

(b) Any depolarizing channel given by $\mathcal{E}_\lambda(\rho) = (1-\lambda)\rho + \frac{\lambda}{d}I$, where $\lambda \leq p$.

Figure 1 – Two examples of resource specifications. (a) is a specification that contains one channel, the identity. (b) is a specification for any depolarization channel with $\lambda \leq p$.

2.1 Specifications

As mentioned in Section 1, a specification can be thought of as a (partial) description of an object to the accuracy needed for the task at hand. This concept is much more general than modeling cryptographic systems, and has been used to model resource theories in physics [5, 6]. For example, let $\mathcal{S}$ denote a chair. A chair with wheels $\mathcal{R}$ is more specific than a chair. We thus have $\mathcal{R} \subset \mathcal{S}$, where $\subset$ is a transitive relation meaning "more specific than". A piece of furniture $\mathcal{T}$ is less specific, hence $\mathcal{T} \supset \mathcal{S}$. As another example, consider instructions for building a model car, which state that a piece should be painted. Let $\mathcal{R}$ denote the pair of the piece from the model car and some paint, and let γ denote the action of painting the piece. Then given $\mathcal{R}$, γ constructs a painted piece $\mathcal{S}$. When actually building the model car, the paint chosen will have a certain color, e.g., red. Let $\mathcal{R}'$ denote the pair of the piece from the model car and red paint. We then have $\mathcal{R}' \subset \mathcal{R}$, because $\mathcal{R}'$ is more specific than $\mathcal{R}$. And applying γ to $\mathcal{R}'$ we obtain $\mathcal{S}' \subset \mathcal{S}$, where $\mathcal{S}'$ is the piece of the car painted red. The instructions apply to anything that satisfies the specifications, in particular, to objects that are more specific.

We define specifications as in [4]: a specification is a subset of a universe Φ of objects, namely those that satisfy the specification. The relation $\mathcal{R} \subset \mathcal{S}$ for $\mathcal{R}, \mathcal{S} \in \mathcal{P}(\Phi)$ is then simply the subset relation, where $\mathcal{P}(\Phi)$ denotes the power set of Φ.[5] We call the elements $\mathsf{R} \in \Phi$ *atomic resources*, and the specifications $\mathcal{R} \in \mathcal{P}(\Phi)$ are *resource specifications*.

As two examples, we have illustrated in Figure 1 specifications for noiseless and noisy channels. Here the atomic resources correspond to individual channels defined by their input and output behavior, and the specification denotes any set of channels satisfying the specification, e.g., depolarizing channels with noise $\lambda \leq p$ as in Figure 1b.

[5] Specifications are more general than this, and may be instantiated in other ways than with sets.

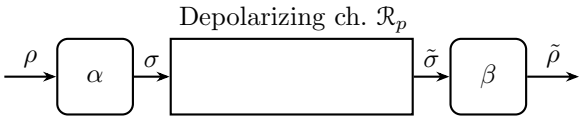


Figure 2 – Error correction converters α and β are applied to Alice and Bob's interfaces of the channel specification $\mathcal{R}_p$.

2.2 Converters

To model cryptographic protocols, we consider resources that have *interfaces*, where each interface can be accessed by one user. For example, the channel specifications from Figure 1 have an input interface and an output interface, with which the sender (Alice) and receiver (Bob) may interact — to send and receive messages, respectively. We usually label interfaces so as to make explicit who controls the interface, e.g., A, B, E, for Alice, Bob, and Eve.

A local operation performed at one interface is called a *converter*. For example, Alice may encode her message with a converter α and Bob may decode it with a converter β, as drawn in Figure 2. Formally, we consider a set of objects Σ, called converters, which are functions mapping a resource specification to another specification, i.e., $\alpha : \mathcal{P}(\Phi) \to \mathcal{P}(\Phi)$ for $\alpha \in \Sigma$. For example, the resource constructed in Figure 2 is given by $\beta(\alpha(\mathcal{R}_p))$ — or, equivalently, $\alpha(\beta(\mathcal{R}_p))$ — which we simply write $\beta\alpha\mathcal{R}_p$ (or $\alpha\beta\mathcal{R}_p$). We usually draw converters with rounded corners.

We often use subscripts to denote the interface to which a converter applies, e.g., $\beta_B\alpha_A\mathcal{R}_p$. Converters applied at different interfaces must commute (as in Figure 2), i.e.,

$$\beta_B\alpha_A\mathcal{R} = \alpha_A\beta_B\mathcal{R}.$$

Composition of converters, $\beta \circ \alpha$, is defined by

$$(\beta \circ \alpha)\mathcal{R} \coloneqq \beta(\alpha\mathcal{R}).$$

Converters must conserve the specificity relation, i.e.,

$$\mathcal{R} \subset \mathcal{S} \implies \alpha\mathcal{R} \subset \alpha\mathcal{S}.$$

The set Σ must also be closed under composition and contain an identity element $\mathrm{id} \in \Sigma$ satisfying

$$\mathrm{id} \circ \alpha = \alpha \circ \mathrm{id} = \alpha.$$

In this work we usually write converters for honest players on the left of the resources, and converters for dishonest players on the right, i.e., we write $\alpha_A\mathcal{R}\sigma_E$ instead of $\sigma_E\alpha_A\mathcal{R}$, where E denotes Eve's interface.

Note that a set of converters Σ that are maps $\alpha : \Phi \to \Phi$ on the set of atomic resources satisfying the properties above immediately induces a set of converters on resource specifications with

$$\alpha\mathcal{R} \coloneqq \{\alpha\mathsf{R} : \mathsf{R} \in \mathcal{R}\}.$$

2.3 Approximations

After constructing the resource $\beta\alpha\mathcal{R}_p$ illustrated in Figure 2, one typically wants to state that it approximately corresponds to a noiseless channel $\mathcal{S}_{\mathrm{id}}$, i.e., $\beta\alpha\mathcal{R}_p \subset \mathcal{S}^{\varepsilon}_{\mathrm{id}}$, where $\mathcal{S}^{\varepsilon}_{\mathrm{id}}$ is an ε-ball around $\mathcal{S}_{\mathrm{id}}$ containing any channel that is ε-close to $\mathcal{S}_{\mathrm{id}}$. Such an ε-ball is defined with respect to a pseudo-metric on atomic resources, $d : \Phi \times \Phi \to \mathbb{R}^+$,

$$\mathcal{R}^{\varepsilon} \coloneqq \{\mathsf{S} \in \Phi : \exists \mathsf{R} \in \mathcal{R}, d(\mathsf{R}, \mathsf{S}) \leq \varepsilon\}.$$

It follows from the triangle inequality of the pseudo-metric that

$$(\mathcal{R}^{\varepsilon})^{\delta} \subset \mathcal{R}^{\varepsilon+\delta}.$$

Furthermore, if the pseudo-metric is contractive, i.e., for any $\alpha \in \Sigma$ and any $\mathsf{R}, \mathsf{S} \in \Phi$, $d(\alpha\mathsf{R}, \alpha\mathsf{S}) \leq d(\mathsf{R}, \mathsf{S})$, then

$$\alpha\mathcal{R}^{\varepsilon} \subset (\alpha\mathcal{R})^{\varepsilon}.$$

2.4 Resource Composition

If two resources $\mathcal{R}$ and $\mathcal{S}$ are simultaneously accessible to the players, we wish to write this as one resource corresponding to the *(parallel) composition* of both, i.e., they are merged into one resource such that the interfaces of each resource are simultaneously available to each player. To do this, we define a parallel composition operation on resource specifications $\| : \mathcal{P}(\Phi) \times \mathcal{P}(\Phi) \to \mathcal{P}(\Phi)$ and write $\mathcal{R}\|\mathcal{S}$ for the resulting specification. For example, a quantum key distribution (QKD) protocol usually requires two resources to be available to the players: an insecure quantum channel $\mathcal{Q}$ and a (multiple use, two-way) authentic classical channel $\mathcal{A}^c$.[6] As drawn in Figure 3, the channel $\mathcal{Q}$ just delivers the (quantum) message to Eve and allows her to replace it with an arbitrary message that is sent to Bob. The channel $\mathcal{A}^c$ faithfully delivers (classical) messages between Alice and Bob, but provides Eve with copies.[7] The players thus have access to the resource $\mathcal{A}^c\|\mathcal{Q}$ and run their protocol corresponding to a pair of converters $(\pi_A^{\mathrm{qkd}}, \pi_B^{\mathrm{qkd}})$.[8] The constructed system is given by the specification $\pi_B^{\mathrm{qkd}}\pi_A^{\mathrm{qkd}}(\mathcal{A}^c\|\mathcal{Q})$.

[6] The superscript c in $\mathcal{A}^c$ represents the number of uses of the channel, which we usually denote by an unspecified constant c.

[7] In order to satisfy the requirement of sequential scheduling for the specific instantiation of atomic resources with quantum combs (see Appendix B.1, in particular, Remark B.1), $\mathcal{A}^c$ does not immediately output two messages at Eve's and the receiver's interfaces. $\mathcal{A}^c$ outputs a single message at the receiver's interace. Upon a request from Eve at her interface, it then gives her a copy of the messages that were sent. To simplify Figure 3, we do not draw the extra "request arrows", but only the information that is output by the systems. These requests are not needed for an instantiation of systems such as causal boxes that supports more complex scheduling (see Appendix B.2).

[8] Similarly to the authentic channel $\mathcal{A}^c$, π_A^{qkd} and π_B^{qkd} do not spontaneously output the key generated, they wait for a request to output it. Furthermore, the protocol starts with π_A^{qkd} being activated at its outer interface, which is not drawn in Figure 3 either.

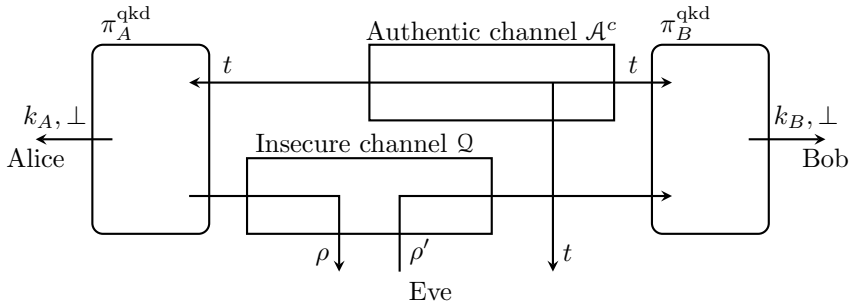


Figure 3 – The real QKD setting, with Alice on the left, Bob on the right and Eve below. Resources $\mathcal{A}^c$ and $\mathcal{Q}$ are available to the honest players, who run their protocol $(\pi_A^{\text{qkd}}, \pi_B^{\text{qkd}})$. At the end of this they either hold keys (k_A, k_B) or produce an error $\perp$.

This notion of parallel composition of resources induces a notion of parallel composition of converters $\alpha|\beta$, defined as

$$(\alpha|\beta)(\mathcal{R}\|\mathcal{S}) \coloneqq (\alpha\mathcal{R})\|(\beta\mathcal{S}).$$

We require $\|$ to be associative, and when multiple resources are in parallel, we add subscripts to the resources and converters to clarify how they connect, e.g, $(\alpha_1|\beta_{23})(\mathcal{R}_1\|\mathcal{S}_2\|\mathcal{T}_3)$ — or $(\alpha_{A_1}|\beta_{B_{23}})(\mathcal{R}_1\|\mathcal{S}_2\|\mathcal{T}_3)$ when we additionally need to denote the interface to which the converters connect. Naturally, we also require that the specificity relation be conserved, i.e.,

$$\mathcal{R} \subset \mathcal{S} \implies \mathcal{R}\|\mathcal{T} \subset \mathcal{S}\|\mathcal{T} \quad \text{and} \quad \mathcal{T}\|\mathcal{R} \subset \mathcal{T}\|\mathcal{S}.$$

As for converters, if an operation $\|$ with the same properties is defined on atomic resources, then this yields a parallel composition operation on specifications, defined as

$$\mathcal{R}\|\mathcal{S} \coloneqq \{\mathsf{R}\|\mathsf{S} : \mathsf{R} \in \mathcal{R}, \mathsf{S} \in \mathcal{S}\}.$$

And if the pseudo-metric is context-insensitive, i.e., for any atomic resources $\mathsf{R}, \mathsf{S}, \mathsf{T} \in \Phi$, $d(\mathsf{R}\|\mathsf{T}, \mathsf{S}\|\mathsf{T}) \leq d(\mathsf{R}, \mathsf{S})$ and $d(\mathsf{T}\|\mathsf{R}, \mathsf{T}\|\mathsf{S}) \leq d(\mathsf{R}, \mathsf{S})$, then

$$\mathcal{R}^\varepsilon\|\mathcal{S} \subset (\mathcal{R}\|\mathcal{S})^\varepsilon \quad \text{and} \quad \mathcal{R}\|\mathcal{S}^\varepsilon \subset (\mathcal{R}\|\mathcal{S})^\varepsilon.$$

2.5 Cryptographic Security

In a context where some players are dishonest, one typically does not have an exact description of how they may influence a protocol outcome, but one has an upper bound on what they can do. For example, in the case of QKD, one would ideally construct a secret key resource $\mathcal{K}$ that at most allows the

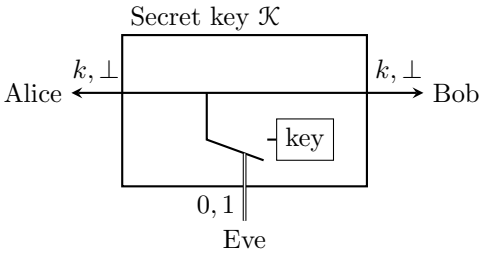


Figure 4 – A secret key resource that allows Eve to decide if Alice and Bob get a uniform key or an error message.[10]

adversary, Eve, to decide if the players get a key or not,[9] but not get any information about the value of the key, as drawn in Figure 4.[10]

In reality, Eve might have less power than this, e.g., she decides that the players should get the key, but the protocol aborts nonetheless. This, of course, is also an acceptable resource to construct, since it is stronger than $\mathcal{K}$ — it is stronger (for the honest players), because Eve has less influence over the outputs. More precisely, any resource $\mathcal{K}\sigma_E$ is an acceptable ideal resource for QKD, since anything achieved by it can be achieved by $\mathcal{K}$ if Eve decides to run σ_E at her interface. A specification of an ideal key resource that (at most) allows Eve to provoke an abort is thus given by

$$\mathcal{K}^* := \{\mathcal{K}\sigma_E : \sigma \in \Sigma\}.$$

We are now ready to define the notion of construction in the special case of three party protocols with honest Alice and Bob and dishonest Eve.

Definition 2.1 (Cryptographic security [3, 4])**.** We say that a protocol $\pi = (\pi_A, \pi_B)$ constructs a resource specification $\mathcal{S}$ from the specification $\mathcal{R}$ with error ε, which we denote

$$\mathcal{R} \xrightarrow{\pi,\varepsilon} \mathcal{S},$$

if

$$\pi_B \pi_A \mathcal{R} \subset (\mathcal{S}^*)^\varepsilon. \tag{4}$$

One will often want to make several statements about a protocol, e.g., $\mathcal{R} \xrightarrow{\pi,\varepsilon} \mathcal{S}$ and $\underline{\mathcal{R}} \xrightarrow{\pi,\varepsilon'} \underline{\mathcal{S}}$, where $\mathcal{R}$ and $\mathcal{S}$ might be the resources in case of

[9] Ideally one would want Eve to not even have the possibility of preventing the players from getting the key. But this cannot be achieved, since Eve can always cut the communication in the real system.

[10] To preserve a sequential execution of the systems, the key resource is defined so that upon inputing her bit, Eve receives a confirmation from $\mathcal{K}$. The players may then individually send a request to the resource, and get either their key or an error. To simplify the picture, only the actual information transmitted is drawn in Figure 4. Request and confirmation arrows have been omitted.

an active adversary (e.g., Eve can arbitrarily modify the communication between Alice and Bob), and $\underline{\mathcal{R}}$ and $\underline{\mathcal{S}}$ are resources in case no adversary is present (e.g., there is only non-malicious noise on the channels). One then typically has $\underline{\mathcal{R}} \subset \mathcal{R}^*$ and $\underline{\mathcal{S}} \subset \mathcal{S}^*$, i.e., if we can say something more specific about the resources available (e.g., specific noise model), then we can make strong statements about the constructed resource (e.g., a key is produced with probability $1 - \varepsilon$).

Note that in order to prove that Definition 2.1 is satisfied by a protocol π, it is sufficient to prove that for every $\mathsf{R} \in \mathcal{R}$ there exists an $\mathsf{S} \in \mathcal{S}$ and $\sigma \in \Sigma$ such that

$$d(\pi_B \pi_A \mathsf{R}, \mathsf{S}\sigma_E) \leq \varepsilon, \tag{5}$$

since this implies that Eq. (4) holds. The exact σ_E used in the security proof will be called *simulator*. In the following, we often write $\mathsf{R} \approx_\varepsilon \mathsf{S}$ instead of $d(\mathsf{R}, \mathsf{S}) \leq \varepsilon$, e.g., Eq. (5) becomes

$$\pi_B \pi_A \mathsf{R} \approx_\varepsilon \mathsf{S}\sigma_E.$$

We now prove that this definition of construction is composable — i.e., Eqs. (2) and (3) are satisfied — with the error of the composed construction that is the sum of the errors of the parts.

Theorem 2.2. *If the pseudo-metric $d : \Phi \times \Phi \to \mathbb{R}^+$ is contractive, then*

$$\mathcal{R} \xrightarrow{\gamma,\varepsilon} \mathcal{S} \quad \textit{and} \quad \mathcal{S} \xrightarrow{\pi,\delta} \mathcal{T} \implies \mathcal{R} \xrightarrow{\pi\circ\gamma,\varepsilon+\delta} \mathcal{T}.$$

If, additionally, d is context-insensitive, then

$$\mathcal{R}_1 \xrightarrow{\gamma_1,\varepsilon_1} \mathcal{S}_1 \quad \textit{and} \quad \mathcal{R}_2 \xrightarrow{\gamma_2,\varepsilon_2} \mathcal{S}_2 \implies \mathcal{R}_1 \| \mathcal{R}_2 \xrightarrow{\gamma_1|\gamma_2,\varepsilon_1+\varepsilon_2} \mathcal{S}_1 \| \mathcal{S}_2.$$

Proof. Using the properties of converters and ε-balls from Sections 2.2 and 2.3, one has

$$\pi\gamma\mathcal{R} \subset \pi(\mathcal{S}^*)^\varepsilon \subset (\pi\mathcal{S}^*)^\varepsilon \subset \left(\left((\mathcal{T}^*)^\delta\right)^*\right)^\varepsilon \subset \left(((\mathcal{T}^*)^*)^\delta\right)^\varepsilon \subset (\mathcal{T}^*)^{\varepsilon+\delta}.$$

Additionally using the properties of parallel composition from Section 2.4, one has

$$\begin{aligned}(\gamma_1|\gamma_2)(\mathcal{R}_1\|\mathcal{R}_2) = (\gamma_1\mathcal{R}_1)\|(\gamma_2\mathcal{R}_2) &\subset (\mathcal{S}_1^*)^{\varepsilon_1}\|(\mathcal{S}_2^*)^{\varepsilon_2} \\ &\subset (\mathcal{S}_1^*\|\mathcal{S}_2^*)^{\varepsilon_1+\varepsilon_2} \subset ((\mathcal{S}_1\|\mathcal{S}_2)^*)^{\varepsilon_1+\varepsilon_2}. \quad \square\end{aligned}$$

2.6 Atomic resources

So far we have instantiated the AC framework with specifications defined as sets of atomic resources. To model concrete systems (such as those from Figures 1, 2, 3, 4), we need to instantiate these atomic resources with a model

of interactive systems that captures quantum information-processing. Such a model has been given in [26], where the atomic resources are called *causal boxes*, and proven to satisfy the properties required by the AC framework.

The causal box framework [26] allows superpositions of causal structures to be modeled, e.g., messages can be sent in superpositions of different orders to superpositions of different players. In order for this to be possible, one has to model messages as pairs $|v, t\rangle \in \mathcal{H}_V \otimes \mathcal{H}_T$, where v denotes the value being sent and t can be understood as a time tag that controls the ordering of messages. This then allows superpositions of different values at different times (or different orders), e.g.,

$$|\psi\rangle = |v_1, t_1\rangle + |v_2, t_2\rangle.$$

Most of the results in the current paper consider simpler resources, that use (classical) sequential scheduling, i.e, they receive a message, send a message, receive another message, etc. This is the case of all the examples seen so far in this section. These can be modeled as memory channels or *quantum combs* [27–29] (see also [30–32]), i.e., systems with some internal memory M, and which upon receiving an input in some register X_i produce a single output in some register Y_i by applying a map $\mathcal{E}_i : \mathcal{L}(\mathcal{H}_{X_i M}) \to \mathcal{L}(\mathcal{H}_{M Y_i})$ which updates the internal memory and computes the output. Such systems can be seen as special cases of causal boxes, in which the (unnecessary) time tag is not written out explicitly.

These two models of quantum information-processing systems — quantum combs and causal boxes — are introduced in detail in Appendix B. In the following we model all systems as quantum combs, unless stated otherwise.

Regardless of the instantiation, the distance between two atomic resources R and S is taken to be the *distinguishing advantage*, i.e., a distinguisher D interacts with one of the two and has to guess which one it is given. The distinguishing advantage is then defined as

$$d(\mathsf{R}, \mathsf{S}) \coloneqq \sup_{\mathsf{D}} |\Pr[\mathsf{D}(\mathsf{R}) = 1] - \Pr[\mathsf{D}(\mathsf{S}) = 1]|,$$

where $\mathsf{D}(\mathsf{R})$ is the binary random variable corresponding to the distinguisher's guess when interacting with R. In the case of quantum combs the distinguishing advantage corresponds to the trace distance between the two states held in memory by the distinguisher after interacting with the corresponding systems [28, 29]. A similar result is derived for causal boxes [26].

3 Min-entropy resources

Before modeling min-entropy specifications, we first consider min-entropy atomic resources using both the quantum combs [27–29] and causal boxes [26] models, in Sections 3.1 and 3.2, respectively. We then define min-entropy

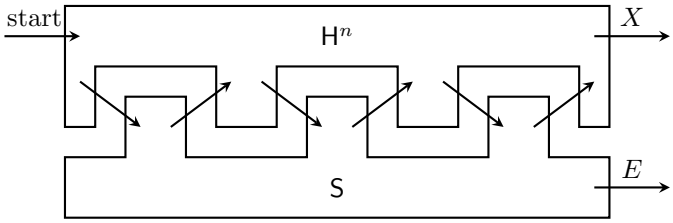


Figure 5 – H^n is a (k, δ)-min-entropy comb if for all S the state ρ_{XE} satisfies the conditions from Definition 3.1.

specifications in Section 3.3, and discuss ε-balls around min-entropy specifications in Section 3.4.

The quantum notation and concepts used in this section and the following are introduced in Appendix A. The models of quantum combs and causal boxes are explained in Appendix B.1 and Appendix B.2, respectively.

3.1 Finite dimensional systems

Quantum combs [27–29], by definition, can only interact a finite number of times with their environment, since they are modeled by (the Choi-Jamiołkowski representation of) a finite dimensional completely positive, trace-preserving (CPTP) map (see Appendix B.1). This is sufficient to model any min-entropy resource that generates the output X after a fixed number of rounds of interaction (as is the case for the applications to QKD and authentication considered in this work), or if the systems have a timeout after which they abort — since in a finite amount of time a causal system can only send a finite number of messages [26].

To model min-entropy atomic resources with combs, we consider a system H^n that is activated by receiving a fixed symbol "start". It then outputs a quantum message, receives a quantum message as input, outputs another message, etc., until a total of n messages have been exchanged with its environment. It then finally outputs a classical (random) value X from an alphabet $\mathcal{X} \cup \{\perp\}$, where $\perp$ is an error symbol denoting that the system failed to generate an output (with enough entropy). Such a system is illustrated in Figure 5, and is a called a min-entropy comb if it satisfies the following conditions.

Definition 3.1 (Min-entropy comb)**.** Let H^n be a quantum comb with a structure as described above, and let S be any comb that mirrors it: S first receives a quantum message, then outputs one, etc, for a total of n interactions, and finally outputs a quantum system E. We say that H^n is a (k, δ)-*min-entropy comb* if for all S, the final joint state ρ_{XE} is given by

$$\rho_{XE} = |\perp\rangle\langle\perp| \otimes \tau_E + \sigma_{XE} \tag{6}$$

for an arbitrary state τ_E, and a state σ_{XE} satisfying

$$H_{\min}^{\delta}(X|E)_{\sigma} \geq k, \tag{7}$$

where $H_{\min}^{\delta}(X|E)_{\sigma}$ denotes the δ-smooth conditional min-entropy of σ_{XE} and is defined in Appendix A.3, Definition A.3.

Note that the min-entropy condition in Eq. (7), is defined on the *sub-normalized* state σ_{XE}. This is because the min-entropy of the renormalized state $\sigma_{XE}/\operatorname{tr}(\sigma_{XE})$ is not meaningful when the probability of not aborting, $\operatorname{tr}(\sigma_{XE})$, is very small — one does not care what happens conditioned on an unlikely event. For a state σ_{XE} with $\operatorname{tr}(\sigma_{XE}) \leq 2^{-k} + \delta^2/2$, Eq. (7) is trivially satisfied.

3.2 Unbounded interactions

The systems defined in Section 3.1 have a fixed number of interactions (namely n) with the environment. This is necessary if one wants to keep the joint input and output Hilbert spaces finite dimensional. One can however imagine more general systems where the number of interactions is a priori unbounded and depends on the values that are input — or where the number of interactions is in a superposition of different values. We model this using causal boxes [26].

As explained in Appendix B.2, in the causal box model a message can be thought of as a pair of a value $v \in \mathcal{V}$ and a position $t \in \mathcal{T}$, where $\mathcal{T}$ is a discrete partially ordered set allowing messages to be ordered with respect to each other (e.g., $\mathcal{T} = \mathbb{Q}$). Let $\mathcal{H}_X = \mathcal{H}_{\mathcal{V}} \otimes \mathcal{H}_{\mathcal{T}}$ be the corresponding Hilbert space. An output of a causal box may consist in one message, multiple messages, no messages at all, or any superposition thereof. The corresponding message space is a Fock space given by

$$\mathcal{F}(\mathcal{H}_X) \coloneqq \bigoplus_{n=0}^{\infty} \vee^n \mathcal{H}_X \,,$$

where $\vee^n \mathcal{H}_X$ denotes the symmetric subspace of $\mathcal{H}_X^{\otimes n}$, and $\mathcal{H}_X^{\otimes 0}$ is the one dimensional space containing the vacuum state $|\Omega\rangle$.

Thus, a figure drawing a causal box does not have one arrow for every output, but instead one arrow for an output wire that many produce an unbounded number of messages. For example, in Figure 6, the two causal boxes H and S are connected by two wires, and may be repeatedly exchanging messages on these wires — these systems are not required to terminate.[11]

[11] Formally, causal boxes are modeled as sequences of maps over ever increasing intervals of $\mathcal{T}$, see Appendix B.2.

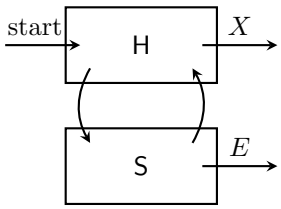


Figure 6 – In the model of causal boxes, each wire may be used an unbounded number of times to transmit messages, e.g., there is no bound on the number of rounds of communication between H and S. The system H is a (k, δ)-min-entropy causal box if for all S and all t the state $\rho_{\overline{X}E}^{\leq t}$ satisfies the conditions from Definition 3.2, where $\rho_{\overline{X}E}^{\leq t}$ is the state of the XE systems truncated at position t.

Similar to the model of min-entropy combs, we model a min-entropy causal box as being started by receiving a corresponding message,[12] after which it interacts with an environment (e.g., the system S drawn in Figure 6). At any point during this interaction, it may output a value on the wire X from the alphabet $\mathcal{X} \cup \{\perp\}$, where, as above, $\perp$ is an error symbol denoting that the system failed to generate an output (with enough entropy). But we restrict the output on X to the subspace $\mathcal{H}_X^{\otimes 0} \oplus \mathcal{H}_X^{\otimes 1}$, i.e., at most one value is output. Unlike for combs, we cannot place a requirement on the entropy of X once a value is output, since this condition might not be well-defined (e.g., for $t \in \mathbb{N}$, a value is produced in position t with probability 2^{-t}). Instead, we bound the entropy of the output up to position t for all $t \in \mathcal{T}$.

Definition 3.2 (Min-entropy causal box)**.** Let H be a causal box with a structure as described above, and let S be any causal box with an input and output wire that match the dimensions of the output and input wires of H, and with an additional output wire E, and let them be connected by these wires. Furthermore, for $VT = X$, let $\rho_{\overline{VT}E}^{\leq t}$ be the subnormalized output on XE up to position t projected on the non-vacuum subspace $\mathcal{H}_V \otimes \mathcal{H}_T \otimes \mathcal{F}(\mathcal{H}_E)$. We say that H is a (k, δ)-*min-entropy causal box* if for all S and all $t \in \mathcal{T}$, the state $\rho_{\overline{VT}E}^{\leq t}$ is given by

$$\rho_{\overline{VT}E}^{\leq t} = |\perp\rangle\langle\perp| \otimes \tau_{TE} + \sigma_{VTE}$$

for an arbitrary state τ_{TE}, and a state σ_{VTE} satisfying

$$H_{\min}^{\delta}(V|TE)_{\sigma} \geq k.$$

Note that Definition 3.2 conditions the entropy of the output on the register T as well as E, since this ordering information could be learned by an

[12] Technically this is not necessary, a causal box may spontaneously output a message. But it simplifies the scheduling with other systems to consider only causal boxes that are started by an external message.

adversary. Though if one considers only systems where timing is independent of the values of messages, then it would be sufficient to bound $H_{\min}^{\delta}(V|E)_{\sigma}$.

3.3 Min-entropy specification

For min-entropy combs and causal boxes (defined in the previous two sections) to be valid atomic resources, one still has to assign interfaces to the various inputs and outputs. In a model with two interfaces A and E — accessed by Alice and Eve, respectively — the final output X occurs at Alice's interface, and the interaction with the environment occurs at Eve's interface. The input "start" may be provided at either Alice or Eve's interface, depending on the protocol considered. A min-entropy specification is then simply the set of all min-entropy atomic resources satisfying a certain bound on the conditional min-entropy.

Definition 3.3 (Min-entropy specification)**.** A (k, δ)-min-entropy specification $\mathcal{H}_{\min}^{k,\delta}$ is the set of all (k, δ)-min-entropy atomic resources.

Definition 3.3 is typically the min-entropy specification one would construct in an adversarial setting: it provides a bound on the entropy, but not on the actual probability of terminating which such a random string, since usually Eve can force honest players to abort. If one considers a context where Eve is not active, then one generally wishes to prove something stronger, e.g., with high probability the protocol generates a random string. Such a statement can easily be achieved by restricting the set $\mathcal{H}_{\min}^{k,\delta}$ to contain only those systems such that for all S, the output $\rho_{XE} = |\perp\rangle\langle\perp| \otimes \tau_E + \sigma_{XE}$ has $\mathrm{tr}(\sigma_{XE}) \geq 1 - \varepsilon$.[13]

In the two applications considered in this work, we need min-entropy resources with three interfaces for Alice, Bob, and Eve. These are defined identically to the two interface versions described so far, except that a string Y is output at Bob's interface as well.[14] Here, the conditional min-entropy is always defined on the XE system. The allowed correlations between Y and XE will depend on the context, e.g., the min-entropy resource constructed by QKD allows Y to be an arbitrary random string, whereas the min-entropy resource used as a secret key by the Fehr-Salvail protocol requires Y to be a copy of X.

[13] In the model with causal boxes, one would require that by a certain position t_0, $\mathrm{tr}(\sigma_{XE}^{\leqslant t_0}) \geq 1 - \varepsilon$.

[14] As in the examples of systems in Section 2, to preserve sequential scheduling when the atomic resources are instantiated with quantum combs, the outputs X and Y are not produced spontaneously, but only after having received a request from Alice and Bob, respectively.

3.4 Approximate min-entropy specifications

In Section 2.3 we defined a notion of an approximate specification, directly in the AC language, by taking an ε-ball around specifications. The min-entropy resources defined in Section 3.3 have their own notion of approximation built-in, namely the smoothing parameter δ. This is useful, because (as we prove in the next lemma) δ-smoothing is a less specific condition that results in a larger set of atomic resources than ε-balls.[15] It remains open to find bounds in the other direction — i.e., whether $\mathcal{H}_{\min}^{k,\delta+\varepsilon} \subset \left(\mathcal{H}_{\min}^{k,\delta}\right)^{\varepsilon'}$ for some reasonable ε' — or examples showing that such bounds do not exist.

Lemma 3.4. *For min-entropy specifications one has*

$$\left(\mathcal{H}_{\min}^{k,\delta}\right)^{\varepsilon} \subset \mathcal{H}_{\min}^{k,\delta+\sqrt{2\varepsilon}}.$$

Proof. By contradiction, let us suppose there exists an H such that

$$\mathsf{H} \notin \mathcal{H}_{\min}^{k,\delta+\sqrt{2\varepsilon}}, \tag{8}$$

but

$$\mathsf{H} \in \left(\mathcal{H}_{\min}^{k,\delta}\right)^{\varepsilon}. \tag{9}$$

From Eq. (8) we find that there must exist an S such that the state $\rho_{XE} = |\bot\rangle\langle\bot| \otimes \tau_E + \sigma_{XE}$ resulting from S and H interacting has

$$H_{\min}^{\delta+\sqrt{2\varepsilon}}(X|E)_{\sigma} < k. \tag{10}$$

From Eq. (9) there must exist an $\mathsf{H}' \approx_{\varepsilon} \mathsf{H}$ such that when interacting with the same S, the resulting state $\rho'_{XE} = |\bot\rangle\langle\bot| \otimes \tau'_{XE} + \sigma'_{XE}$ has

$$H_{\min}^{\delta}(X|E)_{\sigma'} \geq k. \tag{11}$$

Since $\mathsf{H}' \approx_{\varepsilon} \mathsf{H}$, it follows that $D(\rho'_{XE}, \rho_{XE}) \leq \varepsilon$, where $D(\cdot,\cdot)$ is the trace distance. One then obtains

$$\begin{aligned} D(\rho'_{XE}, \rho_{XE}) &= \frac{1}{2}\left\|\sigma'_{XE} - \sigma_{XE}\right\|_{\mathrm{tr}} + \frac{1}{2}\left\|\tau'_E - \tau_E\right\|_{\mathrm{tr}} \\ &\geq \frac{1}{2}\left\|\sigma'_{XE} - \sigma_{XE}\right\|_{\mathrm{tr}} + \frac{1}{2}\left|\operatorname{tr}\tau'_E - \operatorname{tr}\tau_E\right| \\ &= \bar{D}(\sigma'_{XE}, \sigma_{XE}) \\ &\geq P(\sigma'_{XE}, \sigma_{XE})^2/2, \end{aligned}$$

where $\bar{D}(\cdot,\cdot)$ is the generalized trace distance and $P(\cdot,\cdot)$ is the purified distance (see Appendix A.2 and [33]).

Putting this together with Eq. (11) and the triangle inequality, there must exist a $\tilde{\sigma}_{XE}$ such that $H_{\min}(X|E)_{\tilde{\sigma}} \geq k$ and $P(\tilde{\sigma}_{XE}, \sigma_{XE}) \leq \delta + \sqrt{2\varepsilon}$, which contradicts Eq. (10). □

[15] It is currently unknown if it is possible to prove that a QKD protocol constructs the smaller set of resources without the smoothing parameter.

4 Distilling Secret Key

In this section we show how to extract secret key from a tripartite min-entropy resource, where Alice and Bob obtain strings X and Y, and Eve gets side information. In Section 4.1 we show how error correction and verification construct a min-entropy resource which provides Alice and Bob with identical strings $X' = Y'$, given a resource that has no guarantee on the correlations between X and Y. Then in Section 4.2 the players use privacy amplification to construct a secret key resource (see Figure 4 for an illustration of a secret key resource). The two steps are composed in Section 4.3.

These steps of error correction and privacy amplification are performed in a generic way for any resource that satisfies the min-entropy specification. We show in Appendix C that QKD is a special case of this, which constructs a (more specific) min-entropy resource.

4.1 Error Correction

In this section we analyze a generic class of error correction schemes, which are now standard in QKD (see, e.g., [12, 14]). The error correction procedure has two steps. In the first, Alice applies a function $Z = \mathrm{synd}(X)$ which computes a syndrome for X. She then sends this on an authentic channel to Bob, who applies the second function $\hat{X} = \mathrm{corr}(Y, Z)$ to get an estimate $\hat{X}$ of Alice's string X. Such pairs of functions $(\mathrm{synd}, \mathrm{corr})$ are parametrized by two values: by a subset $\mathcal{S} \subset \mathcal{X} \times \mathcal{X}$ of strings that they can correct, i.e, for all $(x, y) \in \mathcal{S}$, $\mathrm{corr}(y, \mathrm{synd}(x)) = x$, and by the length of the string $|Z| = r$, which bounds how much information is leaked to the adversary about X. Let π^{corr} denote the first part of the procedure.

In the second step, the players verify whether the error correction was successful. They do this by first choosing a function f uniformly at random from a family of almost universal hash functions, i.e., a set $\mathcal{F} = \{f : \mathcal{X} \to \mathcal{Y}\}$ such that for all $x, x' \in \mathcal{X}$, $x \neq x'$,

$$\Pr_{f \in \mathcal{F}}\left[f(x) = f(x')\right] \leq \varepsilon_{\mathrm{verif}}. \tag{12}$$

Alice sends $(f, f(X))$ to Bob, who verifies that $f(X) = f(\hat{X})$, and tells Alice whether this is successful or whether they should abort. Let the length of the hash be $|f(x)| = t$, i.e., $|\mathcal{Y}| = 2^t$. Let π^{verif} denote the second part of this procedure. The complete error correction scheme is then $\pi^{\mathrm{ec}} = \pi^{\mathrm{verif}} \circ \pi^{\mathrm{corr}}$.

There are now two cases to consider. The first is when the players have absolutely no guarantee about the correlations between X and Y — in QKD, this is the case if an adversary is eavesdropping on the channel and can arbitrarily change the quantum messages. In this case, we wish to bound the information Eve has as well as bound the probability that the honest players end up with different strings. The second case is when some bounds

on the correlations between X and Y are known (e.g., the number of bit flips between the two) — in QKD, this is the case if only natural noise is present on the channel. If such a more specific resource is present, we then wish to prove that a more specific (stronger) resource is constructed, namely, we additionally want a bound on the probability that the players abort — which is known as the *robustness* (to this noise model) of a protocol.

4.1.1 Security

We start with the first case, when Alice and Bob share a resource $\overline{\mathcal{H}}_{\min}^{k,\delta}$, where Bob's string Y may be arbitrary (but is always $\perp$ if Alice's is $\perp$). Furthermore, they share an authentic channel $\mathcal{A}^c$.[16] It is straightforward that without any further information about Y one has no hope of guaranteeing that π^{corr} will work. Instead, we just bound the information leaked to the adversary by this procedure.

Lemma 4.1. *π^{corr} leaks at most r bits of information about Alice's string X to Eve, i.e.,*

$$\overline{\mathcal{H}}_{\min}^{k,\delta} \| \mathcal{A}^c \xrightarrow{\pi^{corr},0} \overline{\mathcal{H}}_{\min}^{k-r,\delta}.$$

Proof. Immediate from Lemma D.1. □

In this case, the crucial part of the error correction procedure is the error verification, which constructs a min-entropy resource that provides Bob with a perfect copy of Alice's string (or aborts).

Theorem 4.2. *Let $\overline{\mathcal{H}}_{\min}^{k,\delta}$ denote a (k,δ)-min-entropy resource, where Bob's string Y is arbitrary (but is always $\perp$ if Alice's is $\perp$), and $\mathcal{H}_{\min}^{k,\delta}$ denote a (k,δ)-min-entropy resource in which Bob has an exact copy of Alice's string. Then*

$$\overline{\mathcal{H}}_{\min}^{k,\delta} \| \mathcal{A}^c \xrightarrow{\pi^{verif},\varepsilon_{verif}} \mathcal{H}_{\min}^{k-t,\delta}.$$

Note that one has $\mathcal{H}_{\min}^{k,\delta} \subset \overline{\mathcal{H}}_{\min}^{k,\delta}$. What π^{verif} does is check if the resource shared by Alice and Bob belongs to $\mathcal{H}_{\min}^{k,\delta}$, and aborts if not. It leaks t bits in the process and fails with probability $\varepsilon_{\text{verif}}$.

Proof. Let $\mathsf{H} \in \overline{\mathcal{H}}_{\min}^{k,\delta}$ and define H' to work as follows. H' internally runs H. If it obtains $X = \perp$, it simply outputs $\perp$ at both Alice and Bob's interfaces when requested. If $X \neq \perp$, it prepares $(f, f(X))$ for a uniformly chosen f to be output at Eve's interface as information sent on the authentic channel if requested. It checks whether $f(X) = f(Y)$, and prepares the corresponding bit of backwards information to be output at Eve's interface if requested. If

[16] See the description of the multiple use authentic channel $\mathcal{A}^c$ in Section 2.4 and Footnote 7 (though in this case, a single use channel is sufficient).

these strings are equal, H' now outputs $X' = Y' = X$ at Alice's and Bob's interfaces when requested. If they are different, it outputs $X' = Y' = \perp$.

To prove that this theorem holds, we will show that

$$\pi^{\text{verif}}\overline{\mathcal{H}}^{k,\delta}_{\min} \subset \left(\mathcal{H}^{k-t,\delta}_{\min}\right)^{\varepsilon_{\text{verif}}}.$$

This statement follows if we can show that $\mathsf{H}' \in \mathcal{H}^{k-t,\delta}_{\min}$ and that $\pi^{\text{verif}}\mathsf{H} \approx_{\varepsilon_{\text{verif}}} \mathsf{H}'$. Note that $\pi^{\text{verif}}\mathsf{H}$ and H' behave identically, except for the string Y' output at Bob's interface, which, in the case of H' is always $Y' = X'$, whereas in the real setting one might have $Y' \neq X'$. A bound on the probability that $Y' \neq X'$ is thus a bound on the distinguishability between the two systems; and it follows from the almost universal hashing property (Eq. (12)) that $\Pr[Y' \neq X'] \leq \varepsilon_{\text{verif}}$.

To prove that $\mathsf{H}' \in \mathcal{H}^{k-t,\delta}_{\min}$ we need to show that for all S interacting with H', the resulting state is of the from $\rho_{X'Y'E'} = |\perp,\perp\rangle\langle\perp,\perp| \otimes \tau_{E'} + \sigma_{X'Y'E'}$ with $X' = Y'$ and $H^{\delta}_{\min}(X'|E')_{\sigma} \geq k - t$. By construction we always have $X' = Y'$, so the only condition to verify is the min-entropy bound. The last messages output by H' at Eve's interface are f, $f(X)$, and the decision bit $f(X) = f(Y)$. We denote these registers by F, Z, and Ω. It is sufficient to consider a system S that interacts with H, and together with the output in register E also outputs $FZ\Omega$, hence $E' = EFZ\Omega$. By definition of H, the state $\rho_{XYEFZ\Omega}$ resulting from S interacting with H and adding the transcript $FZ\Omega$ that is produced at Eve's interface has the form $\rho_{XYEFZ\Omega} = |\perp,\perp\rangle\langle\perp,\perp| \otimes \tau_{EFZ\Omega} + \gamma_{XYEFZ\Omega}$ with $H^{\delta}_{\min}(X|E)_{\gamma} \geq k$. From Lemma D.1 one has $H^{\delta}_{\min}(X|EFZ)_{\gamma} \geq k - t$. Furthermore, $\gamma_{XYEFZ\Omega} = \gamma^0_{XYEFZ} \otimes |0\rangle\langle 0| + \gamma^1_{XYEFZ} \otimes |1\rangle\langle 1|$, and $\sigma_{X'Y'E'} = \gamma^1_{XYEFZ} \otimes |1\rangle\langle 1|$. It then follows from Lemma D.2 that $H^{\delta}_{\min}(X'|E')_{\sigma} \geq k - t$. □

Corollary 4.3. *$\pi^{ec} = \pi^{verif} \circ \pi^{corr}$ constructs $\mathcal{H}^{k-r-t,\delta}_{\min}$ from $\overline{\mathcal{H}}^{k,\delta}_{\min}$ and $\mathcal{A}^c$ with error ε_{verif},*

$$\overline{\mathcal{H}}^{k,\delta}_{\min} \| \mathcal{A}^c \xrightarrow{\pi^{ec},\varepsilon_{verif}} \mathcal{H}^{k-r-t,\delta}_{\min},$$

where $\mathcal{A}^c = \mathcal{A}^{c_1} \| \mathcal{A}^{c_2}$, and $\mathcal{A}^{c_1}$ and $\mathcal{A}^{c_2}$ are used by π^{corr} and π^{verif}, respectively.

Proof. Follows from Lemma 4.1, Theorem 4.2, and Theorem 2.2. □

4.1.2 Robustness

We now consider the case where correlations between X and Y are known. The procedure π^{corr} must be chosen to deal specifically with these errors. Let $\overline{\mathcal{R}}^{k,\delta,p}_{\min} \subset \overline{\mathcal{H}}^{k,\delta}_{\min}$ be a min-entropy specification that is restricted to resources that only abort with probability at most p and furthermore, that do not allow arbitrary outputs Y, but only strings such that $(X, Y) \subset \mathcal{S}$, where $\mathcal{S}$ is the

set of pairs that can be corrected. And let $\mathcal{R}_{\min}^{k,\delta,p} \subset \mathcal{H}_{\min}^{k,\delta}$ be a specification of resources that also abort with probability at most p and produce identical strings at Alice's and Bob's interfaces. It is straightforward that in this case the procedure π^{ec} constructs $\mathcal{R}_{\min}^{k,\delta,p}$ from $\overline{\mathcal{R}}_{\min}^{k-r-t,\delta,p}$, i.e., one can make statements about the probability that the protocol aborts.

Lemma 4.4. *Let π^{ec}, $\overline{\mathcal{R}}_{\min}^{k,\delta,p}$, and $\mathcal{R}_{\min}^{k,\delta,p}$ be as described above. Then*

$$\overline{\mathcal{R}}_{\min}^{k,\delta,p} \| \mathcal{A}^c \xrightarrow{\pi^{ec},0} \mathcal{R}_{\min}^{k-r-t,\delta,p}.$$

Proof. Immediate from Lemma D.1, and the properties of the error correction code chosen. □

Note that if $(X, Y) \subset \mathcal{S}$ only holds with probability $1 - \varepsilon$, then one does not have the resource $\overline{\mathcal{R}}_{\min}^{k,\delta,p}$, but a less specific resource $\left(\overline{\mathcal{R}}_{\min}^{k,\delta,p}\right)^{\varepsilon}$, and using the fact that for any $\mathcal{S}$, $\mathcal{S}^{\varepsilon} \xrightarrow{\text{id},\varepsilon} \mathcal{S}$, and Theorem 2.2, one has

$$\left(\overline{\mathcal{R}}_{\min}^{k,\delta,p}\right)^{\varepsilon} \| \mathcal{A}^c \xrightarrow{\pi^{\text{ec}},\varepsilon} \mathcal{R}_{\min}^{k-r-t,\delta,p}.$$

4.2 Privacy Amplification

After the error correction scheme, the players share a string that is partially known to the adversary. To obtain a secret string, Alice picks a string Z uniformly at random, a *seed*, and sends it to Bob on an authentic channel. They then each compute the strings $K = \text{Ext}(X, Z)$ and $K' = \text{Ext}(Y, Z)$ for some predefined function Ext, known as an *extractor*. This procedure is called privacy amplification [34, 35], and we denote the corresponding pair of converters as π^{pa}. The function Ext has to satisfy the following property.

Definition 4.5. A function $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *quantum-proof (k, ε)-strong extractor for subnormalized states* if for any subnormalized state ρ_{XE} classical on X, with $H_{\min}(X|E)_\rho \geq k$, and a uniform Z, we have

$$\frac{1}{2} \left\| \rho_{\text{Ext}(X,Z)ZE} - \tau_K \otimes \tau_Z \otimes \rho_E \right\|_{\text{tr}} \leq \varepsilon,$$

where τ_K is the fully mixed state.

The more standard definition for quantum-proof extractors only requires them to be defined for normalized states. But as shown in Lemma D.3, any extractor for normalized states is also an extractor for subnormalized states with slightly weaker parameters. Efficient constructions of extractors are given in, e.g., [35–39]. Note that some of these, e.g., the universal hashing extractors [35, 37, 38], directly satisfy Definition 4.5.

We are now ready to state the main theorem for this section.

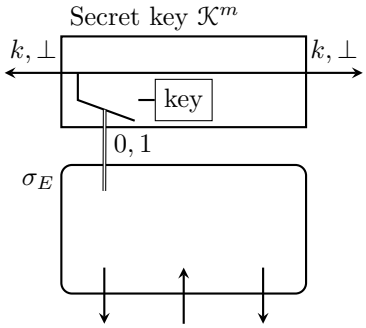


Figure 7 – An m-bit secret key resource $\mathcal{K}^m$ connected to a simulator σ_E at Eve's interface. As in Section 2.5, $\mathcal{K}^m$ does not spontaneously output the keys at the players' interfaces, but only after having received a request, which is omitted from the drawing.

Theorem 4.6. *Let π^{pa} be a privacy amplification protocol as described above, which uses a quantum-proof (k, ε_{pa})-strong extractor for subnormalized states. Given a (k, δ)-min-entropy resource $\mathcal{H}_{\min}^{k,\delta}$ which provides Alice and Bob with identical strings $X = Y$, and an authentic channel $\mathcal{A}^c$, π^{pa} constructs am m-bit secret key resource $\mathcal{K}^m$ (see Figure 7) with error $\varepsilon_{pa} + 2\delta$,*

$$\mathcal{H}_{\min}^{k,\delta} \| \mathcal{A}^c \xrightarrow{\pi^{pa}, \varepsilon_{pa}+2\delta} \mathcal{K}^m.$$

Unlike previous proofs, the current one requires a simulator, σ_E, which we draw in Figure 7. Note that the number of messages exchanged at the outer interface of σ_E (i.e., the number of arrows in Figure 7) will depend on the atomic resource $\mathsf{R} \in \pi^{\mathrm{pa}}(\mathcal{H}_{\min}^{k,\delta} \| \mathcal{A}^c)$ from the real system. For example, in the case of a min-entropy resource constructed using a QKD protocol, this would be three messages as drawn in Figure 7: the quantum states generated by Alice are output at Eve's interface, the modified states are then input by Eve, and finally a transcript of the classical communication is given to Eve as well (upon request).

Proof. To prove that $\pi^{\mathrm{pa}}(\mathcal{H}_{\min}^{k,\delta} \| \mathcal{A}^c) \subset ((\mathcal{K}^m)^*)^{\varepsilon_{\mathrm{pa}}}$, for every atomic resource $\pi^{\mathrm{pa}}(\mathsf{H} \| \mathsf{A}) \in \pi^{\mathrm{pa}}(\mathcal{H}_{\min}^{k,\delta} \| \mathcal{A}^c)$ we will find a K and σ_E such that $\pi^{\mathrm{pa}}(\mathsf{H} \| \mathsf{A}) \approx_{\varepsilon_{\mathrm{pa}}} \mathsf{K}\sigma_E$. Since $\mathcal{A}^c$ and $\mathcal{K}^m$ both have cardinality 1, we only need to find a simulator σ_E for every H. We construct σ_E as follows. σ_E runs H internally and generates all the communication at the outer interface. If H outputs $\perp$, σ_E notifies the key resource K to output an error $\perp$ as well. If H outputs a string $X \neq \perp$, then it picks a random seed Z, which is made available to be output at its outer interface as the transcript on the authentic channel. It notifies K to generate a uniform key k, which is output at Alice's and Bob's interfaces when requested.

Let a distinguisher interact with the real system. After interacting with H it gets a system E, then obtains Z and finally an output K from Alice's and Bob's interface. We take $Z = \perp$ in case H generated a string $X = \perp$. The distinguisher then holds the state

$$\rho_{KZE} = |\perp,\perp\rangle\langle\perp,\perp| \otimes \rho_E^{\perp} + \rho^{\top}_{\mathrm{Ext}(X,Z)ZE}.$$

In the case where the distinguisher is interacting with $\mathsf{K}\sigma_E$, it is going to get the state

$$\tilde{\rho}_{KZE} = |\perp,\perp\rangle\langle\perp,\perp| \otimes \rho_E^{\perp} + \tau_K \otimes \tau_Z \otimes \rho_E^{\top}.$$

The distinguishability between the two systems is bounded by the trace distance between ρ_{KZE} and $\tilde{\rho}_{KZE}$, namely

$$\frac{1}{2}\|\rho_{KZE} - \tilde{\rho}_{KZE}\|_{\mathrm{tr}} = \frac{1}{2}\left\|\rho^{\top}_{\mathrm{Ext}(X,Z)ZE} - \tau_K \otimes \tau_Z \otimes \rho_E^{\top}\right\|_{\mathrm{tr}} \leq \varepsilon_{\mathrm{pa}} + 2\delta,$$

where the last inequality uses the fact that $H^{\delta}_{\min}(X|E)_{\rho^{\top}} \geq k$, that Ext is a quantum-proof $(k, \varepsilon_{\mathrm{pa}})$-strong extractor for subnormalized states and Lemma D.4, which shows that a (k,ε)-extractor has error $\varepsilon + 2\delta$ if used on states with a bound on their smooth min-entropy instead of their min-entropy. □

4.3 Composed statement

By composing Corollary 4.3, Lemma 4.4 and Theorem 4.6, we get the following.

Corollary 4.7. *Let $\overline{\mathcal{H}}^{k,\delta}_{\min}$ be a (k,δ)-min-entropy resource that produces an arbitrary output at Bob's interface, let $\overline{\mathcal{R}}^{k,\delta}_{\min} \subset \overline{\mathcal{H}}^{k,\delta}_{\min}$ be a (k,δ)-min-entropy resource that never aborts and furthermore, produces strings $(X,Y) \subset \mathcal{S}$ that are always corrected by the functions $(\mathrm{synd}, \mathrm{corr})$. Let $\underline{\mathcal{K}}^m$ be a secret key resource that always provides the players with a uniform key of length m and let $\mathcal{K}^m$ be a secret key resource that only provides a key if the adversary allows it. Finally, let $\pi = \pi^{pa} \circ \pi^{ec}$ be the construction described in this section. Then*

$$\overline{\mathcal{R}}^{k,\delta}_{\min}\|\mathcal{A}^c \xrightarrow{\pi,\varepsilon_{pa}+2\delta} \underline{\mathcal{K}}^m$$

and

$$\overline{\mathcal{H}}^{k,\delta}_{\min}\|\mathcal{A}^c \xrightarrow{\pi,\varepsilon_{verif}+\varepsilon_{pa}+2\delta} \mathcal{K}^m,$$

where $\mathcal{A}^c = \mathcal{A}^{c_1}\|\mathcal{A}^{c_2}$, and $\mathcal{A}^{c_i}$ are the authentic channels used by the different parts of the protocol.

5 Quantum Authentication of Classical Messages

Fehr and Salvail [19, 20] propose a prepare-and-measure protocol that authenticates a classical message by encoding it into a quantum cipher. The main feature of their protocol is that it recycles all the key if the message is accepted by the receiver. In this section we provide a composable security analysis of a slightly modified version of their protocol, which is adapted from [20]. We first provide a high level view of what the protocol achieves in the AC framework in Section 5.1. Then in Section 5.2 we give the details of the protocol. The security proof is provided in Section 5.3. And finally, in Section 5.4 we prove bounds on the security if the compromised key is replaced instead of being discarded.

5.1 The Construction

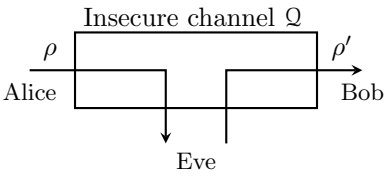
In this section we model the Fehr-Salvail protocol as a pair of converters $\pi = (\pi_A, \pi_B)$ that construct some resource $\mathcal{S}$ given some other resource $\mathcal{R}$. As in Section 4, there are two statements we wish to make. The first is when an adversary is present and the players share an insecure quantum channel $\mathcal{Q}$ as drawn in Figure 8a, i.e., the adversary can change the message being sent and insert a message of her own. We model the real and ideal systems for this case in Section 5.1.1 and Section 5.1.2, respectively. The second setting is when no adversary is present, but the channel shared has some natural noise, as in Figure 8b. This case is discussed in Section 5.1.3.

5.1.1 Real System

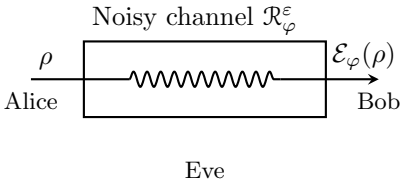
The protocol $\pi = (\pi_A, \pi_B)$ has a very simple structure. First π_A encodes a classical message in a quantum cipher and sends it to Bob on the insecure channel $\mathcal{Q}$. π_B decodes, and either accepts or rejects the message. It also recycles some key depending on the decision. π_B then sends one bit of information back to Alice, to notify her of whether the message was accepted or rejected, after which π_A recycles Alice's keys.

To send this bit of information to Alice, we assume that the players share a backward authentic channel $\underline{\mathcal{A}}^1$. As in Section 4, this is defined as a channel that always transmits the message, but provides a copy to Eve if she requests it. This is illustrated in Figure 8c (but to simplify the drawing, we do not draw the request that Eve must make to get the transcript of the authentic channel).

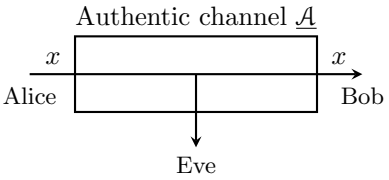
The final resources the players are going to need are the key resources. The protocol uses three keys, $(\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}}, \theta)$. ℓ_{ss} and ℓ_{mac} need to be uniform, so we provide Alice and Bob with a shared uniform key resource $\mathcal{K}$, as depicted in Figure 4, which generates these keys. Note that if Eve does not allow the players to get a key, they cannot run the protocol, and it is trivially secure.



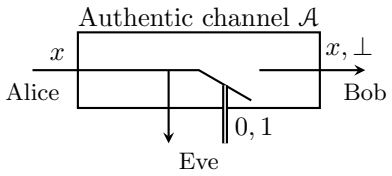
(a) An insecure channel from Alice (on the left) to Bob (on the right) allows Eve (below) to intercept the message and insert a message of her own.



(b) When no adversary is present, Alice's message is delivered to Bob, but some natural noise is inserted.



(c) An idealized authentic channel from Alice to Bob allows Eve to receive a copy of the message, but guarantees that Bob always gets it.



(d) A realistic authentic channel from Alice to Bob allows Eve to receive a copy of the message and choose whether Bob receives it or an error symbol.

Figure 8 – Some resources needed in the Fehr-Salvail construction.

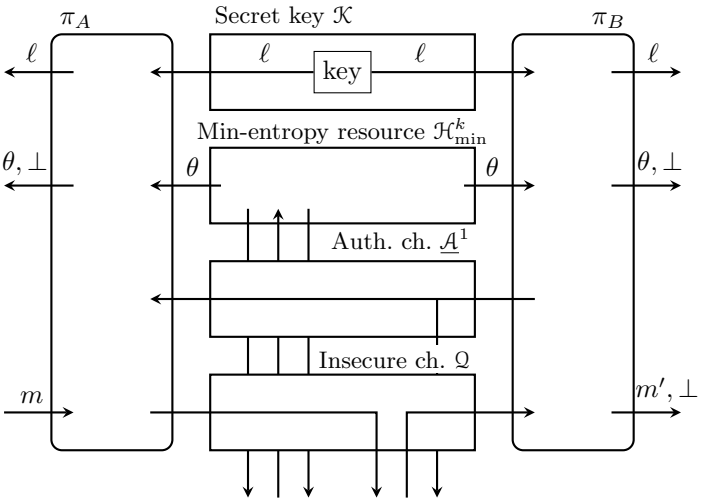
Thus, in the following, we assume the switch is set by Eve to provide the players with a key.

The key θ does not need to be uniform, it is sufficient if it has bounded min-entropy. So we provide the players with a $(k, 0)$-min-entropy resource $\mathcal{H}^{k,0}_{\min}$ as defined in Section 3.3. Since we always take the smoothing parameter to be 0 in this section, we denote this resource by $\mathcal{H}^{k}_{\min}$. Note that to satisfy sequential scheduling, both the key resources $\mathcal{K}$ and $\mathcal{H}^{k}_{\min}$ only provide the keys (or error messages) to the players when they request them (see Remark B.1, and the discussion of these resources in Sections 2.5 and 3.3).

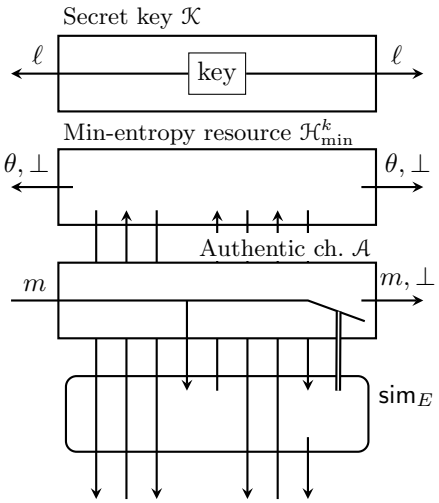
Putting this together, we get the real system drawn in Figure 9a. (The switch on $\mathcal{K}$ as well as the requests to get keys and messages have been omitted from the picture.)

5.1.2 Ideal system

The goal of the protocol is to construct an authentic channel. But the channel $\underline{\mathcal{A}}$ depicted in Figure 8c always delivers the message, and this cannot be achieved, since Eve can jumble the communication if desired. What is achieved is a slightly weaker resource $\mathcal{A}$, which allows Eve to choose if Bob gets the message or not — here too, the receiver must request the message



(a) The real system consists of the resources consumed and the honest players converters (π_A, π_B) that run the protocol.



(b) The ideal system consists of the constructed resources and the simulator sim_E.

Figure 9 – The real and ideal systems of the modified FS protocol in the case where Eve is present.

for it to be output, it is not spontaneously output when Eve allows it. This is illustrated in Figure 8d without the request arrow for the message to be delivered.

The protocol also recycles keys, which is modeled as key resources in the ideal system. All the uniform key $(\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}})$ is recycled, so the ideal system must have a resource $\mathcal{K}$ as well, which provides the players with fresh uniform keys (independent of the messages and ciphers obtained by Eve).

As we show in Theorem 5.4 in Section 5.3, the subnormalized key with distribution $P_{\Theta'}(\theta) \coloneqq \Pr[\Theta = \theta \text{ and "accept"}]$ that is output by players the if the message is accepted has the same min-entropy as the original normalized key Θ. So the recycled key in the ideal system is captured by a specification $\mathcal{H}^k_{\min}$ with the same entropy bound k. Note that the renormalized key with distribution $P_{\Theta'}(\theta) \coloneqq \Pr[\Theta = \theta | \text{"accept"}]$ may have much less entropy, so there is effectively an entropy loss during the protocol. But the relevant measure of entropy for future uses of the key is that of the subnormalized state — since the resource consumed, $\mathcal{H}^k_{\min}$, measures the entropy of the subnormalized state.

Putting this together along with a simulator sim_E that is needed for the security proof, we get the ideal system drawn in Figure 9b.

The corresponding constructive statement formulated in the AC framework is that π constructs $\mathcal{K}\|\mathcal{H}^k_{\min}\|\mathcal{A}$ from $\mathcal{K}\|\mathcal{H}^k_{\min}\|\underline{\mathcal{A}}^1\|\mathcal{Q}$ (with some error ε_{adv}),

$$\mathcal{K}\|\mathcal{H}^k_{\min}\|\underline{\mathcal{A}}^1\|\mathcal{Q} \xrightarrow{\pi,\varepsilon_{\text{adv}}} \mathcal{K}\|\mathcal{H}^k_{\min}\|\mathcal{A}. \tag{13}$$

The key resources $\mathcal{K}$ and $\mathcal{H}^k_{\min}$ may be seen as catalysts, since they appear both in the real and ideal systems.

5.1.3 Natural Noise

In the case where Eve is not present, the players share a channel that has natural noise instead of the insecure channel $\mathcal{Q}$. More specifically, the protocol is designed to correct φ errors, so we assume a channel specification that is ε-close to having φ errors when the states sent are encoded as in the protocol.[17] We denote this channel specification by $\mathcal{R}^{\varepsilon}_{\varphi}$, and illustrate this in Figure 8b.

Furthermore, in this case we wish to make a stronger statement, namely that the message is delivered for sure, i.e., a channel of the type $\underline{\mathcal{A}}$ from Figure 8c is constructed. But to achieve this, it is not sufficient that the communication is not jumble by Eve, we also need to be sure that the players

[17] We model the channel as only adding noise to the quantum states sent, but assume that the classical part of the cipher is transmitted without errors. One can easily compose a noisy classical channel with converters that perform error correction if this is not the case (see Figure 2), i.e., construct a noiseless channel from a noisy one. We do not want to do this for a quantum channel, because quantum error correcting codes are not prepare-and-measure.

always get keys. We denote by $\underline{\mathcal{K}}$ and $\underline{\mathcal{H}}^k_{\min}$ resources which always provide keys to the players. In this case, the recycled keys are of the same type.

The corresponding constructive statement is that π constructs $\underline{\mathcal{K}}\|\underline{\mathcal{H}}^k_{\min}\|\underline{\mathcal{A}}$ from $\underline{\mathcal{K}}\|\underline{\mathcal{H}}^k_{\min}\|\underline{\mathcal{A}}^1\|\mathcal{R}^\varepsilon_\varphi$ (with some error $\varepsilon_{\text{noise}}$),

$$\underline{\mathcal{K}}\|\underline{\mathcal{H}}^k_{\min}\|\underline{\mathcal{A}}^1\|\mathcal{R}^\varepsilon_\varphi \xrightarrow{\pi,\varepsilon_{\text{noise}}} \underline{\mathcal{K}}\|\underline{\mathcal{H}}^k_{\min}\|\underline{\mathcal{A}}. \tag{14}$$

5.2 Protocol

The Fehr-Salvail [19] protocol requires two different (keyed) hash functions, which we denote $\mathsf{ss} : \{0,1\}^{n_{\mathsf{ss}}} \times \{0,1\}^{r_{\mathsf{ss}}} \to \{0,1\}^{m_{\mathsf{ss}}}$ and $\mathsf{mac} : \{0,1\}^{n_{\mathsf{mac}}} \times \{0,1\}^{r_{\mathsf{mac}}} \to \{0,1\}^{m_{\mathsf{mac}}}$. Both of these functions are constructed from extractors[18] $\mathrm{Ext}_h : \{0,1\}^{n_h} \times \{0,1\}^{r_h - m_h} \to \{0,1\}^{m_h}$, for $h \in \{\mathsf{ss}, \mathsf{mac}\}$. The hash functions are defined as $h(x, \ell_1\|\ell_2) := \mathrm{Ext}_h(x, \ell_1) \oplus \ell_2$.

Note that not any extractor will do. They have to be quantum-proof (k, ε)-strong extractors for subnormalized states for any value k and an error $\varepsilon = \frac{\nu_h}{2}\sqrt{2^{-k+m_h}}$, where ν_h are parameters specific to each extractor. Universal hashing [35], almost universal hashing [37], dual universal hashing [38], as well as δ-biased masking [36] all satisfy this requirement (for parameters ν_h which depend on the specific constructions). To obtain composable security, we additionally require that these extractors be linear functions in the first input [20], which is satisfied by all the constructions cited above.

The reason for this specific form of extractor is that the security proof requires the following property.

Definition 5.1 (ν-key-privacy [19])**.** A function $h : \mathcal{X} \times \mathcal{L} \to \mathcal{T}$ offers ν-key-privacy if for any subnormalized state $\rho_{LXTE} \in \mathcal{S}_{\leq}(\mathcal{H}_{LXTE})$ with the properties $\rho_{LX} = \tau_L \otimes \rho_X$, $T = h(X, L)$, and $L \leftrightarrow XT \leftrightarrow E$ forms a Markov chain, it holds that

$$\|\rho_{LTE} - \tau_L \otimes \rho_{TE}\|_{\mathrm{tr}} \leq \nu\sqrt{2^{-H_{\min}(X|TE)+m}},$$

where τ_L is the fully mixed state and $\mathcal{T} = \{0,1\}^m$.

Fehr and Salvail [19] prove that if Ext_h is an extractor of the type given above, then the corresponding function h provides ν_h-key-privacy (see Lemma D.6).

Note that a function like h obtained by XORing a uniform key always produces a uniform output.

Definition 5.2 (Uniformity [19])**.** We say that a function $h : \mathcal{X} \times \mathcal{L} \to \mathcal{T}$ is *uniform* if for a uniform L and any $x \in \mathcal{X}$, $T = h(x, L)$ is uniformly random on $\mathcal{T}$.

[18] The definition of an extractor is given in Definition 4.5.

The first keyed hash function, (a *secure sketch*) ss, is used for error correction. Apart from the underlying extractor having the required properties, we additionally need that for a uniformly chosen $\ell \in \{0,1\}^{r_{\mathsf{ss}}}$ and any $x, x' \in \{0,1\}^{n_{\mathsf{ss}}}$ with Hamming distance $w(x,x') \leq \varphi n_{\mathsf{ss}}$ for some fixed φ, x may be recovered from $(x', \mathsf{ss}(x,\ell), \ell)$ except with probability $\varepsilon_{\mathsf{ss}}$. This can be implemented using universal hashing [7], but the recovery operation is not known to be efficient. Fehr and Salvail propose another construction based in δ-biased masking [36], which has an efficient recovery operation, but has less noise tolerance φ (see [19] for more details).

The second keyed hash function, mac, is used to detect if the adversary tampered with the message. The additional requirement is that $\{\mathsf{mac}(\cdot,\ell)\}_\ell$ must be a family of $\varepsilon_{\mathsf{mac}}$-*strongly universal* hash functions [40, 41], i.e., for any $x_1, x_2 \in \{0,1\}^{n_{\mathsf{mac}}}$ and $t_1, t_2 \in \{0,1\}^{m_{\mathsf{mac}}}$ with $x_1 \neq x_2$,

$$\Pr_\ell[\mathsf{mac}(x_1,\ell) = t_1 \text{ and } \mathsf{mac}(x_2,\ell) = t_2] \leq \frac{\varepsilon_{\mathsf{mac}}}{2^{m_{\mathsf{mac}}}}.$$

Constructions for such hash functions are given in [40, 41], e.g., $\mathsf{mac}(x, y\|b) = \phi(x * y) + b$ where ϕ is any linear surjective function and $*$ and $+$ are multiplication and addition in the corresponding finite fields. In this example, $\mathrm{Ext}_{\mathsf{mac}}(x,y) = \phi(x*y)$ is a universal hash function, so mac has the required extractor properties. We denote by ν_{mac} the corresponding extractor parameter. The probability that tampering is not detected when this function is used as a standard message authentication code (MAC) — i.e., when a tag $t = \mathsf{mac}(x,\ell)$ is appended to a message x, and upon receiving (x', t'), the receiver checks if $t' = \mathsf{mac}(x',\ell)$ [40, 41] — is $\varepsilon_{\mathsf{mac}}$. In the case of the example given, $\nu_{\mathsf{mac}} = 1$ and $\varepsilon_{\mathsf{mac}} = \frac{1}{2^{m_{\mathsf{mac}}}}$.

In the following we denote the length of the message to be authenticated by m and the length of the first input to ss by $n = n_{\mathsf{ss}}$. The function mac is always used with $n_{\mathsf{mac}} = n + m + m_{\mathsf{ss}}$.

The final ingredient needed is a code $\mathcal{C} \subset \{0,1\}^n$ with minimum distance d between any two code words.

The modified Fehr-Salvail protocol works as follows (see Remark 5.3 here below for a description of the differences with the original protocol).

Encryption. The players, Alice and Bob, share keys $\ell_{\mathsf{ss}} \in \{0,1\}^{r_{\mathsf{ss}}}$, $\ell_{\mathsf{mac}} \in \{0,1\}^{r_{\mathsf{mac}}}$, and $\theta \in \mathcal{C}$. ℓ_{ss} and ℓ_{mac} have to be uniform. θ has bounded min-entropy, i.e., it should be generated by a min-entropy resource with parameter k. To authenticate a message $y \in \{0,1\}^m$, Alice picks a string $x \in \{0,1\}^n$ uniformly at random, and generates the n qubit quantum state $H^\theta|x\rangle$, where $H^\theta = \bigotimes_i H^{\theta_i}$ and H is the Hadamard matrix. She then computes the values $s = \mathsf{ss}(x, \ell_{\mathsf{ss}})$ and $t = \mathsf{mac}(x\|y\|s, \ell_{\mathsf{mac}})$. Finally, she sends the cipher consisting of $y\|s\|t$ and $\rho = H^\theta|x\rangle\langle x|H^\theta$ to Bob.

Note that it follows from Lemma D.7 that the function $\chi_y : \{0,1\}^n \times \{0,1\}^{r_{\mathsf{ss}}+r_{\mathsf{mac}}} \to \{0,1\}^{m_{\mathsf{ss}}+m_{\mathsf{mac}}}$ with $\chi_y(x, \ell_g \| \ell_h) := s \| t$ provides $(\nu_g + \nu_h)$-key-privacy and uniformity.

Decryption. Upon receiving $y' \| s' \| t'$ and ρ' from Alice, Bob first computes $H^\theta \rho' H^\theta$ and measures in the computational basis, obtaining $\tilde{x}$. He then uses the recovery procedure to get x' from $(\tilde{x}, s', \ell_{\mathsf{ss}})$. He checks if $w(x', \tilde{x}) \leq \varphi n$ and if $t' = h(x' \| y' \| s', \ell_{\mathsf{mac}})$. If one of these conditions does not hold, he rejects the message. Otherwise, he accepts y' as the message that Alice sent.

Key recycling. If the message was rejected, Bob recycles ℓ_{ss} and ℓ_{mac}. If the message was accepted, he recycles ℓ_{ss} and ℓ_{mac}, as well as θ. He sends one bit of information on a backward authentic channel to Alice to tell her if he accepted or rejected, and she recycles the same keys.

Remark 5.3. The protocol described here differs in two ways from the original Fehr-Salvail protocol [19]. Firstly, the extractors have to be linear in their first input, which was introduced in the extended version [20] following an initial draft of the current work pointing out the issue with impersonation attacks. Secondly, we do not require the players to have fresh key to replace the discarded θ in case of a reject, our analysis goes through without this. Hence, in this version of the protocol, the players can run the authentication scheme even if they only have the keys $(\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}}, \theta)$, but no access to a key refreshing function as in [19, 20] that generates a new θ'.

5.3 Analysis

Our task now is to prove that Eqs. (13) and (14) hold and to bound the corresponding errors. We get similar errors to the original, non-composable proof [19, 20], but with minor improvements in the constants. This is stated in the following theorem.

Theorem 5.4. *Let $\mathcal{K}$, $\underline{\mathcal{K}}$, $\mathcal{H}^k_{\min}$, $\underline{\mathcal{H}}^k_{\min}$, $\underline{\mathcal{A}}^1$, $\mathcal{Q}$, $\mathcal{R}^\varepsilon_\varphi$, $\mathcal{A}$, and $\underline{\mathcal{A}}$, be resource specification as described above and let $\pi = (\pi_A, \pi_B)$ be the converters running the modified Fehr-Salvail protocol from Section 5.2. Then*

$$\underline{\mathcal{K}} \| \underline{\mathcal{H}}^k_{\min} \| \underline{\mathcal{A}}^1 \| \mathcal{R}^\varepsilon_\varphi \xrightarrow{\pi, \varepsilon_{noise}} \underline{\mathcal{K}} \| \underline{\mathcal{H}}^k_{\min} \| \underline{\mathcal{A}}$$

and

$$\mathcal{K} \| \mathcal{H}^k_{\min} \| \underline{\mathcal{A}}^1 \| \mathcal{Q} \xrightarrow{\pi, \varepsilon_{adv}} \mathcal{K} \| \mathcal{H}^k_{\min} \| \mathcal{A},$$

with $\varepsilon_{noise} = \varepsilon + \varepsilon_{\mathsf{ss}}$ and

$$\varepsilon_{adv} = \varepsilon_{\mathsf{mac}} + (\nu_{\mathsf{ss}} + \nu_{\mathsf{mac}}) \sqrt{\left(2 + \frac{|\mathcal{C}|}{2^{d/2}} + \frac{|\mathcal{C}| 2^{h(\varphi)n}}{2^d}\right) 2^{m_{\mathsf{ss}} + m_{\mathsf{mac}} - k}}. \tag{15}$$

Proof. The formal statements we will prove are that for any $\mathsf{K} \in \underline{\mathcal{K}}$, $\mathsf{H} \in \underline{\mathcal{H}^k_{\min}}$, $\mathsf{A}^1 \in \underline{\mathcal{A}}^1$, and $\mathsf{R} \in \mathcal{R}^{\varepsilon}_{\varphi}$, there exists a $\mathsf{K}' \in \mathcal{K}$, $\mathsf{H}' \in \underline{\mathcal{H}^k_{\min}}$, $\mathsf{A} \in \underline{\mathcal{A}}$, and a simulator sim_E such that

$$\pi_B \pi_A \big(\mathsf{K} \| \mathsf{H} \| \mathsf{A}^1 \| \mathsf{R}\big) \approx_{\varepsilon_{\text{noise}}} \big(\mathsf{K}' \| \mathsf{H}' \| \mathsf{A}\big) \mathsf{sim}_E; \tag{16}$$

and that for any $\mathsf{K} \in \mathcal{K}$, $\mathsf{H} \in \mathcal{H}^k_{\min}$, $\mathsf{A}^1 \in \underline{\mathcal{A}}^1$, and $\mathsf{Q} \in \mathcal{Q}$, there exists a $\mathsf{K}' \in \mathcal{K}$, $\mathsf{H}' \in \mathcal{H}^k_{\min}$, $\mathsf{A} \in \mathcal{A}$, and a simulator sim_E such that

$$\pi_B \pi_A \big(\mathsf{K} \| \mathsf{H} \| \mathsf{A}^1 \| \mathsf{Q}\big) \approx_{\varepsilon_{\text{adv}}} \big(\mathsf{K}' \| \mathsf{H}' \| \mathsf{A}\big) \mathsf{sim}_E. \tag{17}$$

We start with the case of Eq. (16). Since for any resource $\mathcal{R}$, $\mathcal{R}^{\varepsilon} \xrightarrow{\text{id},\varepsilon} \mathcal{R}$, it follows from Theorem 2.2 that it is sufficient to consider a noisy channel specification $\mathcal{R}_{\varphi}$ and add an error ε to the final statement.

The distinguisher could either first provide Alice with a message y to be encrypted, or first interact with the key resources so that they generate keys ℓ, θ. The second case is a more powerful distinguisher, since it can choose a message correlated to θ, due to the side information it has about θ. So w.l.o.g. we consider only this second case, i.e., the distinguisher first interacts with $\underline{\mathcal{H}^k_{\min}}$ so that θ is generated, and notifies $\underline{\mathcal{K}}$ to generate the key $\ell = (\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}})$. It then provides a message y to Alice, who prepares the cipher, and sends it on the noisy channel $\mathcal{R}_{\varphi}$. Due to the error correction properties of the function ss, Bob can reconstruct the correct x except with probability $\varepsilon_{\mathsf{ss}}$. If he reconstructs the correct x, then Alice's message is always accepted and θ is recycled.

For every $\mathsf{H} \in \underline{\mathcal{H}^k_{\min}}$ we construct a H' that behaves identically to H, except that once θ has been generated, H' does not accept to output it at the players' interface if requested, but waits to get a notification at Eve's interface that it can be output. The simulator sim_E allows the distinguisher to interact directly with H', except for the last message. It also blocks the notification to K' to generate the key. Once θ has been generated (but not output), the activation of K' received from the distinguisher (but not delivered), and the simulator has received the notification that the message has been received and delivered by A, it generates the one bit message for the transcript of the backwards authentic channel and notifies H' and K' that their keys can now be output if requested.

These real and ideal systems behave identically, except if Bob fails to correctly reconstruct x in the real system. So the final error is $\varepsilon_{\text{noise}} = \varepsilon + \varepsilon_{\mathsf{ss}}$.

In the case of Eq. (17), we may also assume w.l.o.g. that the distinguisher first interacts with $\mathcal{H}^k_{\min}$ and notifies $\mathcal{K}$ to generate the keys. But it then has two options. It first provides Alice with a message y, intercepts and possibly changes the cipher, and finally obtains Bob's outcome as well as the keys — a substitution attack. Or, the distinguisher may first input a cipher on the insecure channel $\mathcal{Q}$, obtain Bob's output as well as the recycled keys, then

choose a message y that it inputs at Alice's interface, and finally gets her cipher — an impersonation attack.

We start analyzing the substitution attack. This case follows closely the security proof from [19]. Let $\rho_{\Theta E}$ be the subnormalized state of the key θ and Eve's side information after interacting with H when a key θ is successfully generated. Eve will now measure the E system to choose her message y, resulting in a new state $\sigma_{Y\Theta E} = \sum_y p_y |y,\theta\rangle\langle y,\theta| \otimes \sigma_E^{y,\theta}$, where we have normalized the states so that $\operatorname{tr} \sigma^y_{\Theta E} = \operatorname{tr} \rho_{\Theta E}$. By definition we have $H_{\min}(\Theta|EY)_\sigma \geq k$. Note that one also has

$$2^{-H_{\min}(\Theta|EY)_\sigma} = p_{\text{guess}}(\Theta|EY)_\sigma = \sum_y p_y p_{\text{guess}}(\Theta|E)_{\sigma^y} = \sum_y p_y 2^{-H_{\min}(\Theta|E)_{\sigma^y}}. \quad (18)$$

From now one, we take y to be fixed and $\sigma^y_{\Theta E}$ to be the shared state. At the end of the proof we average over the different y weighted by p_y.

Alice runs her authentication protocol, after which the shared state between Alice and the distinguisher is given by $\sigma^y_{L\Theta XZQE}$, where Z contains the classical part of the cipher, Q contains the quantum part, X is the uniform string that Alice generated and encoded in Q, and L contains the uniform keys $\ell_{\mathsf{ss}} \| \ell_{\mathsf{mac}}$. The ZQ systems are intercepted by the distinguisher, who applies a map $\mathcal{E} : \mathcal{L}(\mathcal{H}_{ZQE}) \to \mathcal{L}(\mathcal{H}_{ZZ'QE})$ which leaves Z unmodified and generates a new Z'. Let $\mu^y_{L\Theta XZZ'QE}$ be the resulting state. $Z'Q$ is now sent to Bob, who measures Q to get $\tilde{X}$, decodes it with (S', ℓ_{ss}) to get X', and checks whether $w(X', \tilde{X}) \leq \varphi n$ and $T' = h(Y' \| S' \| X', \ell_{\mathsf{mac}})$, where $Z' = Y' \| S' \| T'$. He finally sends a bit D to Alice containing his decision. If $D = 1$ he outputs the received message Y' when requested, and outputs the keys L and Θ when requested. If $D = 0$, he outputs an error $\perp$ and only recycles L. Let the final state be $\rho^y_{DL\Theta XX'\tilde{X}ZZ'E}$.

In the ideal case, we define H' and sim_E to work as follows. H' first runs H, so that exactly the same key Θ and side information E are generated while interacting with the distinguisher — the simulator sim_E lets all these messages between H' and the distinguisher go through. Once the distinguisher has input the message y in the ideal authentic channel, the simulator gets a copy, which it forwards to H'. H' then picks its own keys $(\ell'_{\mathsf{ss}}, \ell'_{\mathsf{mac}})$ uniformly at random and a uniform X, and generates a cipher ZQ. It then outputs ZQ at Eve's interface, which the simulator sim_E passes on to the distinguisher. Let the state shared between the different systems at this point be $\tilde{\sigma}^y_{L\Theta XZQE}$, where L represents the new keys that are to be output by $\mathcal{K}$ (not those generated internally by H'). The distinguisher performs the same map, $\mathcal{E}$, as when interacting with the real system, resulting in a state $\tilde{\mu}^y_{L\Theta XZZ'QE}$, and gives $Z'Q$ to the simulator sim_E who forwards them to H'. H' now measures Q just as Bob would do, gets $\tilde{X}$. It then reconstructs X', checks that $X' = X$, that $w(X', \tilde{X}) \leq \varphi n$ and that $Z = Z'$. If one of these three

conditions is not satisfied, it outputs a bit $D = 0$, otherwise $D = 1$, which the simulator intercepts. If $D = 0$, sim_E tells the authentic channel to output an error symbol at Bob's interface when requested, if $D = 1$ the message y is output instead. Regardless of the value of D, sim_E outputs D as the bit on the backward authentic channel if requested, and also notifies $\mathcal{K}$ to output a random key $\ell = \ell_{\mathsf{ss}} \| \ell_{\mathsf{mac}}$ when requested. And if $D = 0$, it tells H' to output $\perp$ when requested, otherwise θ. Let the final state be $\tilde{\rho}^y_{DL\Theta XX'\tilde{X}ZZ'E}$.

We now need to prove two things. Firstly, that $\mathsf{H}' \in \mathcal{H}^k_{\min}$, and secondly that the real and ideal systems are indistinguishable except with advantage ε_{adv}, i.e.,

$$\frac{1}{2}\left\|\rho^{y,1}_{L\Theta ZZ'E} - \tilde{\rho}^{y,1}_{L\Theta ZZ'E}\right\|_{\text{tr}} \leq \varepsilon^{y,1}_{\text{adv}} \quad \text{and} \quad \frac{1}{2}\left\|\rho^{y,0}_{LZZ'E} - \tilde{\rho}^{y,0}_{LZZ'E}\right\|_{\text{tr}} \leq \varepsilon^{y,0}_{\text{adv}}, \tag{19}$$

where $\rho^y_{L\Theta XX'\tilde{X}ZZ'ED} = \rho^{y,0}_{L\Theta XX'\tilde{X}ZZ'E} \otimes |0\rangle\langle 0| + \rho^{y,1}_{L\Theta XX'\tilde{X}ZZ'E} \otimes |1\rangle\langle 1|$ and $\sum_y p_y(\varepsilon^{y,0}_{\text{adv}} + \varepsilon^{y,1}_{\text{adv}}) = \varepsilon_{\text{adv}}$.

We start with $\mathsf{H}' \in \mathcal{H}^k_{\min}$. For this, it is sufficient to show that

$$H_{\min}\left(\Theta|ZZ'E\right)_{\tilde{\rho}^{y,1}} \geq H_{\min}(\Theta|E)_{\sigma^y},$$

where $\sigma^y_{\Theta E}$ is the state output by H (after the measurement to choose y), since it them follows from Eq. (18) that Θ has enough min-entropy. From Lemma D.2 we have

$$H_{\min}\left(\Theta|ZZ'E\right)_{\tilde{\rho}^{y,1}} \geq H_{\min}\left(\Theta|ZZ'E\right)_{\tilde{\rho}^{y}} = H_{\min}\left(\Theta|ZZ'E\right)_{\tilde{\mu}^{y}}.$$

Applying a map to the side information can only increase the entropy, hence

$$H_{\min}\left(\Theta|ZZ'E\right)_{\tilde{\mu}^{y}} \geq H_{\min}(\Theta|ZQE)_{\tilde{\sigma}^{y}}.$$

Because $Z = y\|S\|T$ and the function which computes $S\|T$ is uniform (see Definition 5.2), Z is independent from the other systems, hence

$$H_{\min}(\Theta|ZQE)_{\tilde{\sigma}^{y}} = H_{\min}(\Theta|QE)_{\tilde{\sigma}^{y}}.$$

Finally, Q was generated by applying a unitary H^θ to a fully mixed state $\frac{1}{2^n}\sum_x |x\rangle\langle x|$, so Q is also fully mixed and independent of the other systems (which contain no information about x), hence

$$H_{\min}(\Theta|QE)_{\tilde{\sigma}^{y}} = H_{\min}(\Theta|E)_{\tilde{\sigma}^{y}}.$$

We now return to Eq. (19). From the properties of mac, it follows that if $D = 1$, then $Z' = Z$ and $X' = X$ except with probability $\varepsilon_{\mathsf{mac}}$, i.e., the state $\bar{\rho}^y_{L\Theta XX'\tilde{X}Y'ZZ'ED}$ obtained by flipping the value of D from 1 to 0 if either $Z' \neq Z$ or $X' \neq X$ must be $\varepsilon_{\mathsf{mac}}$-close to $\rho^y_{L\Theta XX'\tilde{X}ZZ'ED}$. It now suffices to bound the distance between $\tilde{\rho}^y$ and $\bar{\rho}^y$. To simplify notation, we introduce

a new register Θ' such that if $D = 0$, $\Theta' = \perp$, and if $D = 1$, then $\Theta' = \Theta$. Thus, we are now trying to prove that

$$\frac{1}{2}\left\|\bar{\rho}^y_{L\Theta' ZZ'ED} - \tilde{\rho}^y_{L\Theta' ZZ'ED}\right\|_{\mathrm{tr}} \leq \varepsilon^y_{\mathrm{adv}} - \varepsilon_{\mathsf{mac}}. \tag{20}$$

In the ideal case we have $\tilde{\rho}^y_{L\Theta' ZZ'ED} = \tau_L \otimes \bar{\rho}^y_{\Theta' ZZ'ED}$, where τ_L is the fully mixed state, because by construction L is uniform and independent of the rest, and $\tilde{\rho}^y_{\Theta' ZZ'ED} = \bar{\rho}^y_{\Theta' ZZ'ED}$ — H' runs the real protocol, the only difference is the reject condition, but by the flip of D that generated $\bar{\rho}^y$ from ρ^y makes them now abort under the same conditions. Plugging this in Eq. (20), it remains to show that

$$\frac{1}{2}\left\|\bar{\rho}^y_{L\Theta' ZZ'ED} - \tau_L \otimes \bar{\rho}^y_{\Theta' ZZ'ED}\right\|_{\mathrm{tr}} \leq \varepsilon^y_{\mathrm{adv}} - \varepsilon_{\mathsf{mac}}.$$

From Lemma D.7 it follows that the function

$$\chi_y : \{0,1\}^n \times \{0,1\}^{r_{\mathsf{ss}}+r_{\mathsf{mac}}} \to \{0,1\}^{m_{\mathsf{ss}}+m_{\mathsf{mac}}}$$

with $\chi_y(x, \ell_{\mathsf{ss}} \| \ell_{\mathsf{mac}}) \coloneqq s \| t$, $s = \mathsf{ss}(x, \ell_{\mathsf{ss}})$, and $t = \mathsf{mac}(x \| y \| s, \ell_{\mathsf{mac}})$ provides $(\nu_{\mathsf{ss}} + \nu_{\mathsf{mac}})$-key-privacy. Furthermore, the state $\bar{\rho}^y_{LX\Theta' ZZ'ED}$ satisfies the assumptions of Definition 5.1 (with $T = Z$). Hence we have

$$\frac{1}{2}\left\|\bar{\rho}^y_{L\Theta' ZZ'ED} - \tau_L \otimes \bar{\rho}^y_{\Theta' ZZ'ED}\right\|_{\mathrm{tr}} \leq \frac{\nu_{\mathsf{ss}} + \nu_{\mathsf{mac}}}{2} \sqrt{2^{-H_{\min}(X|\Theta' ZZ'ED)_{\bar{\rho}^y} + m_{\mathsf{ss}} + m_{\mathsf{mac}}}}.$$

It now remains to upper bound

$$2^{-H_{\min}(X|\Theta' ZZ'ED)_{\bar{\rho}^y}} = p_{\mathrm{guess}}\left(X|\Theta' ZZ'ED\right)_{\bar{\rho}^y} = p_{\mathrm{guess}}\left(X|\Theta' ZZ'E\right)_{\bar{\rho}^y},$$

where we have removed D because this register is redundant, it can be inferred from Θ' (since $\Theta' = \perp \iff D = 0$).

Let us define a new register Ω which takes the value 1 if $w(X, \tilde{X}) \leq \varphi n$ and $\Omega = 0$ otherwise. Let $\bar{\rho}^y_{X\Theta' ZZ'E\Omega} = \bar{\rho}^{y,0}_{X\Theta' ZZ'E} \otimes |0\rangle\langle 0| + \bar{\rho}^{y,1}_{X\Theta' ZZ'E} \otimes |1\rangle\langle 1|$. We have

$$\begin{aligned} p_{\mathrm{guess}}\left(X|\Theta' ZZ'E\right)_{\bar{\rho}^y} &\leq p_{\mathrm{guess}}\left(X|\Theta' ZZ'E\Omega\right)_{\bar{\rho}^y} \\ &= p_{\mathrm{guess}}\left(X|\Theta' ZZ'E\right)_{\bar{\rho}^{y,0}} + p_{\mathrm{guess}}\left(X|\Theta' ZZ'E\right)_{\bar{\rho}^{y,1}} \\ &\leq p_{\mathrm{guess}}\left(X|ZZ'E\right)_{\bar{\rho}^{y,0}} + p_{\mathrm{guess}}\left(X|\Theta ZZ'E\right)_{\bar{\rho}^{y,1}}. \end{aligned}$$

The third line follows because adding Θ to the side information when $\Theta' = \perp$ can only increase the probability of guessing X.

We now bound these two terms separately.

$$\begin{aligned} p_{\text{guess}}\big(X|ZZ'E\big)_{\bar{\rho}^{y,0}} &\leq p_{\text{guess}}\big(X|ZZ'E\big)_{\bar{\rho}^{y}} \\ &= p_{\text{guess}}\big(X|ZZ'E\big)_{\rho^{y}} \\ &= p_{\text{guess}}\big(X|ZZ'E\big)_{\mu^{y}} \\ &\leq p_{\text{guess}}(X|ZQE)_{\sigma^{y}} \\ &= p_{\text{guess}}(X|QE)_{\sigma^{y}}. \end{aligned}$$

The first line follows from Lemma D.2. The fourth line follows because applying a map to the side information can only decrease the probability of guessing X. The fifth line follows because χ_y is uniform so Z is independent. Finally, by noting that $\sigma^{y}_{\Theta XQE} = \mathcal{M}^{\text{BB84}}_{\Theta A,X}\left(\sigma^{y}_{\Theta XE} \otimes \Phi^{+}_{AQ}\right)$, where Φ^{+}_{AQ} are EPR pairs and $\mathcal{M}^{\text{BB84}}_{\Theta A,X}$ measures A according to the basis in Θ and writes the result in X (see Appendix D.4 for a formal definition of $\mathcal{M}^{\text{BB84}}_{\Theta A,X}$), we can apply Lemma D.8 with $B = QE$, from which we get

$$p_{\text{guess}}(X|QE)_{\sigma^{y}} \leq p_{\text{guess}}(\Theta|E)_{\sigma^{y}}\left(1 + \frac{|\mathcal{C}|}{2^{d/2}}\right).$$

To bound $p_{\text{guess}}(X|\Theta ZZ'E)_{\bar{\rho}^{y,1}}$ we will use Lemma D.9. Let P^{Ω} be an operator which projects the state on the event $\Omega = 1$, namely $w(X, \tilde{X}) \leq \varphi n$. Let $\mathcal{M}^{\text{BB84}}_{\Theta Q,\tilde{X}}$ be Bob's measurement of the cipher Q that yields the string $\tilde{X}$. Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_{ZQE}) \to \mathcal{L}(\mathcal{H}_{ZZ'QE})$ be the map performed by the distinguisher on the cipher. We thus have $\bar{\rho}^{y,1}_{X\Theta ZZ'E} = \text{tr}_{\tilde{X}} \circ P^{\Omega} \circ \mathcal{M}^{\text{BB84}}_{\Theta Q,\tilde{X}} \circ \mathcal{E}(\sigma^{Y}_{X\Theta ZQE})$. Note furthermore that by the uniformity of χ_y, $Z = y\|S\|T$ where $S\|T$ is uniform and independent from the other registers, and XQ may be generated by measuring halves of EPR pairs Φ^{+}_{AQ} according to Θ (which commutes with $\mathcal{E}$). Hence we have

$$\bar{\rho}^{y,1}_{X\Theta ZZ'E} = \text{tr}_{\tilde{X}} \circ P^{\Omega} \circ \mathcal{M}^{\text{BB84}}_{\Theta Q,\tilde{X}} \circ \mathcal{M}^{\text{BB84}}_{\Theta A,X} \circ \mathcal{E}(\sigma^{y}_{\Theta E} \otimes \Phi^{+}_{AQ} \otimes \tau_Z).$$

This puts us in a position to apply Lemma D.9 with $B = Q$ and $C = ZZ'E$, from which we get

$$p_{\text{guess}}\big(X|\Theta ZZ'E\big)_{\bar{\rho}^{y,1}} \leq p_{\text{guess}}(\Theta|E)_{\sigma^{y}}\left(1 + \frac{|\mathcal{C}|2^{h(\varphi)n}}{2^{d}}\right).$$

Finally, taking the average over p_y along with Jensen's inequality, we get the bound from Eq. (15).

The final case to consider is that of impersonation attacks. In the real system, the distinguisher sends a forged cipher to Bob, who performs the decoding. He then either accepts and recycles both $\ell = (\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}})$ and θ, or rejects and recycles only $\ell = (\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}})$. Let $\sigma_{L\Theta ED}$ denote the joint state at

this point, where, as previously, D is Bob's decision to accept or reject the message, L contains the uniform keys $(\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}})$, Θ is the non-uniform key (which may have been given to the distinguisher if $D = 1$).

The distinguisher can then choose a message Y to input at Alice's interface for encryption. Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_{L\Theta ED}) \to \mathcal{L}(\mathcal{H}_{L\Theta Y ED})$ be the operator applied by the distinguisher to generate Y, which we define so as to leave the classical registers $L\Theta D$ unmodified, and furthermore, $\mathcal{E}$ is only allowed to use information from Θ if $D = 1$. We denote the resulting state by $\rho_{L\Theta Y ED} = \mathcal{E}(\sigma_{L\Theta ED})$. Finally, Alice's protocol generates a cipher, resulting in the joint shared state $\rho_{L\Theta UYQED}$, where UY denotes the classical part of the cipher with $U = S\|T$ (jointly written $Z = Y\|S\|T$ in the proof against substitution attacks), and Q is the quantum part of the cipher.

In the ideal case, if the simulator sim_E receives a forged cipher at its outer interface from the distinguisher before it receives the message y from the authentic channel, it knows that we are dealing with an impersonation attack. It then tells the authentic channel to output an error when requested, the key resource K' to output some fresh uniform key $\ell = (\ell_{\mathsf{ss}}, \ell_{\mathsf{mac}})$ when requested, and the min-entropy resource H' to output an error $\perp$ when requested. Let $\tilde{\sigma}_{L\Theta ED}$ denote the joint state at this point. As in the real case, the distinguisher applies the map $\mathcal{E}$ to generate a message Y, inputs this to the authentic channel, which gives it to the simulator. sim_E now picks its own key ℓ' and asks H' to give it the key θ that it generated while running H internally. sim_E then follows the protocol and generates a cipher YUQ, which it outputs at its outer interface. Let the final state shared by the different parties be $\tilde{\rho}_{L\Theta UYQED}$.

As in the case of impersonation attacks, we need to prove two things. Firstly, that $\mathsf{H}' \in \mathcal{H}^k_{\min}$, and secondly, that

$$\frac{1}{2}\|\rho_{LUYQED} - \tilde{\rho}_{LUYQED}\|_{\mathrm{tr}} \leq \varepsilon_{\mathrm{adv}}. \tag{21}$$

Note that Eq. (21) does not contain Θ. This is because it is only ever recycled in the real case (the ideal system cannot get fooled by an impersonation attack), but the bit $D = 1$ is already enough to perfectly distinguisher real from ideal in this case, one does not need Θ.

Since H' always outputs $\perp$, it trivially satisfies the definition of a $(k, 0)$-min-entropy resource. For bounding Eq. (21), note that by the definition of mac, the probability of accepting the forged cipher is at most $\varepsilon_{\mathsf{mac}}$. Let $\bar{\sigma}_{L\Theta ED}$ be the state obtained by flipping D from 1 to 0 on $\sigma_{L\Theta ED}$ and define $\bar{\rho}_{L\Theta UYQED}$ as the state obtained after the distinguisher applies $\mathcal{E}$ to $\bar{\sigma}_{L\Theta ED}$ and Alice generates the cipher. Then

$$\frac{1}{2}\|\rho_{LUYQED} - \bar{\rho}_{LUYQED}\|_{\mathrm{tr}} \leq \varepsilon_{\mathsf{mac}}.$$

Furthemore, in the ideal system one has $\tilde{\rho}_{LUYQED} = \tau_L \otimes \tau_U \otimes \bar{\rho}_{YQED}$, where τ_L and τ_U are fully mixed states. This follows, because L is uniform by

definition, U is uniform because it is generated by the uniform function χ_y, and $\tilde{\rho}_{YQED} = \bar{\rho}_{YQED}$ because the simulator uses the same θ and performs the same operation to generate Q. Since we always have $D = 0$, this register can be removed, and it remains to show that,

$$\frac{1}{2}\|\bar{\rho}_{LUYQE} - \tau_L \otimes \tau_U \otimes \bar{\rho}_{YQE}\|_{\mathrm{tr}} \leq \varepsilon_{\mathrm{adv}} - \varepsilon_{\mathsf{mac}}.$$

We now look more closely at how the protocol generates U. Since the extractors used are linear, we have $u = s\|t$ with $s = A_{\ell_{\mathsf{ss}}}x + b_{\ell_{\mathsf{ss}}}$ and $t = A_{\ell_{\mathsf{mac}}}(x\|y\|s) + b_{\ell_{\mathsf{mac}}}$, where $A_{\ell_{\mathsf{ss}}}$ and $A_{\ell_{\mathsf{mac}}}$ are matrices, and $b_{\ell_{\mathsf{ss}}}$ and $b_{\ell_{\mathsf{mac}}}$ are strings, which depend on ℓ_{ss} and ℓ_{mac}. One can alternatively write this as $u = \big(A_{\ell_{\mathsf{ss}}}x\|A^1_{\ell_{\mathsf{mac}}}x\big) + \big(0\|A^3_{\ell_{\mathsf{mac}}}A_{\ell_{\mathsf{ss}}}x\big) + B_{\ell_{\mathsf{ss}},\ell_{\mathsf{mac}}}y + c_{\ell_{\mathsf{ss}},\ell_{\mathsf{mac}}}$, where $A^1_{\ell_{\mathsf{mac}}}$ and $A^3_{\ell_{\mathsf{mac}}}$ are the first n columns and last m_{ss} columns of $A_{\ell_{\mathsf{mac}}} = A^1_{\ell_{\mathsf{mac}}}\|A^2_{\ell_{\mathsf{mac}}}\|A^3_{\ell_{\mathsf{mac}}}$, respectively, and $B_{\ell_{\mathsf{ss}},\ell_{\mathsf{mac}}}$ and $c_{\ell_{\mathsf{ss}},\ell_{\mathsf{mac}}}$ are a matrix and string which depend on ℓ_{ss} and ℓ_{mac}.

Since $\mathrm{Ext}_{\mathsf{mac}}(x\|y\|s, \ell_{\mathsf{mac}}) = A_{\ell_{\mathsf{mac}}}(x\|y\|s)$ is a (k,ε)-strong extractor, then so is $\mathrm{Ext}'_{\mathsf{mac}}(x, \ell_{\mathsf{mac}}) \coloneqq A^1_{\ell_{\mathsf{mac}}}x$. And from Lemma D.5 and the bounds on the errors of $\mathrm{Ext}_{\mathsf{ss}}$ and $\mathrm{Ext}_{\mathsf{mac}}$, we find that $\mathrm{Ext}(x, \ell_{\mathsf{ss}}\|\ell_{\mathsf{mac}}) \coloneqq A_{\ell_{\mathsf{ss}}}x\|A^1_{\ell_{\mathsf{mac}}}x$ is a (k,ε)-strong extractor for any k and $\varepsilon = \frac{\nu_{\mathsf{ss}}+\nu_{\mathsf{mac}}}{2}\sqrt{2^{-k+m_{\mathsf{ss}}+m_{\mathsf{mac}}}}$. The state $\bar{\rho}_{LUYQE}$ may thus be written as $\bar{\rho}_{LUYQE} = \mathcal{G} \circ \mathcal{F}\big(\bar{\rho}_{L\mathrm{Ext}(X,L)YQE}\big)$, where $\mathcal{F} : \mathcal{L}(\mathcal{H}_{LU}) \to \mathcal{L}(\mathcal{H}_{LU})$ with $U = ST$ reads L and S and XORs $A^3_{\ell_{\mathsf{mac}}}s$ to the T register, and $\mathcal{G} : \mathcal{L}(\mathcal{H}_{LUY}) \to \mathcal{L}(\mathcal{H}_{LUY})$ reads L and Y and XORs $B_{\ell_{\mathsf{ss}},\ell_{\mathsf{mac}}}y$ and $c_{\ell_{\mathsf{ss}},\ell_{\mathsf{mac}}}$ to U. Since L is uniform and independent from $\bar{\rho}_{YQE}$, it follows from the definition of an extractor that

$$\frac{1}{2}\big\|\mathcal{G} \circ \mathcal{F}\big(\bar{\rho}_{L\mathrm{Ext}(X,L)YQE}\big) - \mathcal{G} \circ \mathcal{F}(\tau_L \otimes \tau_U \otimes \bar{\rho}_{YQE})\big\|_{\mathrm{tr}} \leq \frac{\nu_{\mathsf{ss}} + \nu_{\mathsf{mac}}}{2}\sqrt{2^{-H_{\min}(X|YQE)_{\bar{\rho}}+m_{\mathsf{ss}}+m_{\mathsf{mac}}}}.$$

To finish the proof we need that $\mathcal{F}$ and $\mathcal{G}$ XOR a value to a uniform string, which results in a uniform string, hence

$$\mathcal{G} \circ \mathcal{F}(\tau_L \otimes \tau_U \otimes \bar{\rho}_{YQE}) = \tau_L \otimes \tau_U \otimes \bar{\rho}_{YQE},$$

and we need to upper bound $2^{-H_{\min}(X|YQE)_{\bar{\rho}}} = p_{\mathrm{guess}}(X|YQE)_{\bar{\rho}}$. This latter bound is obtained from Lemma D.8 following the same steps as the bound on $p_{\mathrm{guess}}(X|QE)_{\sigma^y}$ in the case of substitution attacks, from which we get

$$p_{\mathrm{guess}}(X|YQE)_{\bar{\rho}} \leq p_{\mathrm{guess}}(\Theta|E)_{\sigma}\left(1 + \frac{|\mathcal{C}|}{2^{d/2}}\right) \leq 2^k\left(1 + \frac{|\mathcal{C}|}{2^{d/2}}\right). \qquad \square$$

5.4 Continuing after a reject

Since the construction from Theorem 5.4 generates the same resources $\mathcal{K}$ and $\mathcal{H}^k_{\min}$ that it uses, it is trivial to recursively apply the protocol to authenticate

multiple messages using the same keys. By Theorem 2.2, the error of n runs of the protocol, $\pi \circ \cdots \circ \pi$, is $n\varepsilon_{\text{adv}}$. But note that the protocol does not perform anything if it gets an error from the resource $\mathcal{H}^k_{\min}$ instead of a key. This way of composing the protocol with itself aborts all future rounds as soon as tampering is detected and the key θ is not recycled.

One can imagine a different scenario, in which the players have spare secret key, which they use to replace θ, if it cannot be recycled. Let $\underline{\mathcal{K}}$ denote such an extra key resource, and let $\mathcal{H}^k_{\min}$ denote a min-entropy resource, which might produce an error $\perp$. Given these two resources, we wish to construct a new resource $\underline{\mathcal{H}}^{k'}_{\min}$ which always outputs a key, by "giving" the key from $\underline{\mathcal{K}}$ to $\mathcal{H}^k_{\min}$. We are then left with a resource $\mathcal{K}$ which might still output a key if it was not given to $\mathcal{H}^k_{\min}$. $\mathcal{K}$ can be defined as in Figure 4, with a switch that decides if it produces a key or not.

Lemma 5.5. *Let $\pi^{new} = (\pi_A^{new}, \pi_B^{new})$ be a protocol where both π_A^{new} and π_B^{new} get keys (k, θ) from $\underline{\mathcal{K}}$ and $\mathcal{H}^k_{\min}$. If $\theta \neq \perp$, they output (k, θ) at their outer interfaces when requested. If $\theta = \perp$, they output $(\perp, k)$ at their outer interfaces instead. Then*

$$\underline{\mathcal{K}} \| \mathcal{H}^k_{\min} \xrightarrow{\pi^{new}, 0} \mathcal{K} \| \underline{\mathcal{H}}^{k'}_{\min}$$

with $k' = -\log\left(2^{-n} + 2^{-k}\right)$.

Proof. Let $\mathsf{H} \in \mathcal{H}^k_{\min}$, and after interacting with this, let the shared state of the key and the distinguisher be $\rho_{\Theta E} = |\perp\rangle\langle\perp| \otimes \mu_E + \sigma_{\Theta E}$ with $H_{\min}(\Theta|E)_\sigma \geq k$.

We define H' to run H, and if it gets $\perp$, it generates a fresh uniform key τ_Θ, which it outputs when requested. The shared state is then $\rho'_{\Theta E} = \tau_\Theta \otimes \mu_E + \sigma_{XE}$. One has

$$p_{\text{guess}}(\Theta|E)_{\rho'} \leq p_{\text{guess}}(\Theta|E)_{\tau \otimes \mu} + p_{\text{guess}}(\Theta|E)_\sigma \leq 2^{-n} + 2^{-k}.$$

Hence

$$H_{\min}(\Theta|E)_{\rho'} = -\log p_{\text{guess}}(\Theta|E)_{\rho'} \geq -\log\left(2^{-n} + 2^{-k}\right).$$

This shows that $\mathsf{H}' \in \underline{\mathcal{H}}^k_{\min}$. We additionally need H' to output at Eve's interface whether H generated $\perp$ or not, and for a simulator to activate the corresponding switch on $\mathcal{K}$. □

If one has enough spare key $\underline{\mathcal{K}}$, recursively composing π^{new} with the modified Fehr-Salvail protocol π — i.e., running $\pi \circ \pi^{\text{new}} \circ \pi \circ \cdots \circ \pi^{\text{new}} \circ \pi$ — allows one to encrypt multiple messages by using keys from $\underline{\mathcal{K}}$ to replace lost θ. Note that since the entropy of the key decreases slightly when this is done, the error ε_{adv} will increase slightly with each run (if one does not change the parameters to compensate).

Appendices

A Notation and basic concepts

We assume the reader is familiar with basic quantum information theory, e.g., textbooks such as [42, 43]. In this appendix we explain the notation, and introduce the distance and entropy measures that we use in this work.

A.1 Quantum states, maps, and norms

We use standard notation for quantum information theory. $\mathcal{H}$ denotes a Hilbert space. In all sections except Section 3.2 and Appendix B.2, where causal boxes are used, Hilbert spaces are finite dimensional. In finite dimensions, $\mathcal{L}(\mathcal{H})$ denotes the set of linear operators on $\mathcal{H}$, $\mathcal{S}(\mathcal{H})$ is the set of normalized positive operators — density operators — and $\mathcal{S}_{\leq}(\mathcal{H})$ is the set of subnormalized positive operators, i.e., if $\rho \in \mathcal{S}_{\leq}(\mathcal{H})$, then $0 \leq \operatorname{tr}\rho \leq 1$. In infinite dimensions, $\mathfrak{T}(\mathcal{H})$ denotes the set of trace class operators.[19]

We write $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ for a bipartite quantum system and $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ for a bipartite (subnormalized) quantum state. $\rho_A = \operatorname{tr}_B(\rho_{AB})$ and $\rho_B = \operatorname{tr}_A(\rho_{AB})$ denote the corresponding reduced density operators. Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a completely positive, trace-preserving (CPTP) map.[20] When it is applied to a state $\rho \in \mathcal{S}_{\leq}(\mathcal{H}_{AC})$, we write $\mathcal{E}(\rho)$ as shorthand for $(\mathcal{E} \otimes \mathrm{id}_C)(\rho)$, where id_C is the identity on system C.

The only norm we need in this work is the trace norm (or Schatten 1-norm), defined as $\|A\|_{\mathrm{tr}} \coloneqq \operatorname{tr}\sqrt{A^\dagger A}$.

A.2 Distance measures

The trace distance between two states ρ and σ is given by

$$D(\rho, \sigma) \coloneqq \frac{1}{2}\|\rho - \sigma\|_{\mathrm{tr}}.$$

This corresponds to the maximum advantage one has in distinguishing between the two states, i.e., if given ρ or σ chosen uniformly at random one has to guess which one we hold, then the probability of guessing correctly is [43]

$$p = \frac{1}{2} + \frac{1}{2}D(\rho, \sigma).$$

Another widely used measure is the fidelity, defined as

$$F(\rho, \sigma) \coloneqq \operatorname{tr}\left(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right).$$

[19] $V \in \mathfrak{T}(\mathcal{H})$ if $\|V\|_{\mathrm{tr}} = \sum_i \langle i|\sqrt{V^\dagger V}|i\rangle < \infty$, where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}$. A density operator is a non-negative self-adjoint operator $\rho \in \mathfrak{T}(\mathcal{H})$ with $\operatorname{tr}\rho = 1$.

[20] In the case of infinite dimensional systems, a CPTP map acts on trace class operators, $\mathcal{E} : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$.

When dealing with subnormalized states, we need to generalize these measures to retain their properties. The following distance notions are treated in detail in [33], and we refer to that work for more information.

For any two subnormalized states $\rho, \sigma \in \mathcal{S}_{\leq}(\mathcal{H})$, we define the generalized trace distance as

$$\bar{D}(\rho, \sigma) \coloneqq D(\rho, \sigma) + \frac{1}{2}|\operatorname{tr}\rho - \operatorname{tr}\sigma|,$$

and the generalized fidelity as

$$\bar{F}(\rho, \sigma) \coloneqq F(\rho, \sigma) + \sqrt{(1 - \operatorname{tr}\rho)(1 - \operatorname{tr}\sigma)}.$$

The (generalized) fidelity has a useful property, known as Uhlmann's theorem (see [33, 42]), which states that for any two states ρ and σ, there exist purifications of these states which have the same fidelity. The *purified distance* is defined based on the fidelity, so as to have the same property [33]:

$$P(\rho, \sigma) \coloneqq \sqrt{1 - \bar{F}^2(\rho, \sigma)}.$$

This metric coincides with the generalized distance for pure states, and is larger otherwise.

Lemma A.1 ([33, Lemma 6])**.** *Let $\rho, \sigma \in \mathcal{S}_{\leq}(\mathcal{H})$. Then*

$$\bar{D}(\rho, \sigma) \leq P(\rho, \sigma) \leq \sqrt{2\bar{D}(\rho, \sigma)}.$$

The purified distance is used to define smooth min-entropy in the following section.

A.3 Min-entropy

The *smooth conditional min-entropy* that we use throughout this work to define the randomness of a quantum system was first proposed by Renner [7]. It represents the optimal measure for randomness extraction in the sense that it is always possible to extract that amount of almost uniform randomness from a source, but never more. Before defining this notion, we first state a *non-smooth* version.

Definition A.2 (conditional min-entropy [7])**.** Let $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$. The *min-entropy* of A conditioned on B is defined as

$$H_{\min}(A|B)_\rho \coloneqq \max\{\lambda \in \mathbb{R} : \exists \sigma_B \in \mathcal{S}(\mathcal{H}_B) \text{ s.t. } 2^{-\lambda}\mathbb{1}_A \otimes \sigma_B \geq \rho_{AB}\},$$

where $\mathbb{1}_A$ denotes the identity operator and $A \geq B$ if and only if $A - B$ is positive semi-definite ($A - B \geq 0$).

We will often drop the subscript ρ when there is no doubt about what underlying state is meant.

This definition has a simple operational interpretation when the first system is classical, which is the case we consider. König et al. [44] showed that for a state $\rho_{XB} = \sum_{x\in\mathcal{X}} p_x |x\rangle\langle x| \otimes \rho_B^x$ classical on X,

$$H_{\min}(X|B)_\rho = -\log p_{\text{guess}}(X|B)_\rho, \tag{22}$$

where $p_{\text{guess}}(X|B)$ is the maximum probability of guessing X given B, namely

$$p_{\text{guess}}(X|B)_\rho \coloneqq \max_{\{\Gamma_x\}_{x\in\mathcal{X}}} \left(\sum_{x\in\mathcal{X}} p_x \operatorname{tr}(\Gamma_x \rho_B^x) \right),$$

where the maximum is taken over all positive-operator valued measures (POVMs) $\{\Gamma_x\}_{x\in\mathcal{X}}$ on B (i.e., Γ_x is positive and $\sum_x \Gamma_x = I$). If the system B is empty, then the min-entropy of X reduces to the Rényi entropy of order infinity, $H_{\min}(X) = -\log \max_{x\in\mathcal{X}} p_x$ (often written $H_\infty(X)$). In this case the connection to the guessing probability is particularly obvious: when no side information is available, the best guess we can make is simply the value $x \in \mathcal{X}$ with highest probability.

The *smooth* min-entropy then consists in maximizing the min-entropy over all subnormalized states δ-close in the purified distance to the actual state ρ_{XB} of the system considered. Thus by introducing an extra error δ, we have a state with potentially much more entropy.

Definition A.3 (smooth min-entropy [7, 33])**.** Let $\delta \geq 0$ and $\rho_{AB} \in \mathcal{S}_\leq(\mathcal{H}_{AB})$, then the *$\delta$-smooth min-entropy* of A conditioned on B is defined as

$$H_{\min}^\delta(A|B)_\rho \coloneqq \max_{\sigma_{AB}: P(\sigma,\rho)\leq\delta} H_{\min}(A|B)_\sigma.$$

B Formalizing Information-Processing Systems

B.1 Quantum Combs

A *quantum comb* [27–29] (see also [30–32]) models an interactive quantum information-processing system that receives an input, sends an output, receives an input, sends an output, etc, and terminates after a fixed number of steps. Such a system is drawn in Figure 10. One trivial way to model such systems is to explicitly denote their internal memory, e.g., let $\mathcal{H}_M$ be the space of the internal memory, then a system is given by a sequence of CPTP maps:

$$\mathcal{E}_i : \mathcal{L}(\mathcal{H}_{X_i M}) \to \mathcal{L}(\mathcal{H}_{M Y_i}).$$

Let the internal memory start in some initial state $|0\rangle_M$. Upon receiving an input $\rho_{X_1} \in \mathcal{L}(\mathcal{H}_{X_1})$ one can evaluate the output and new memory state

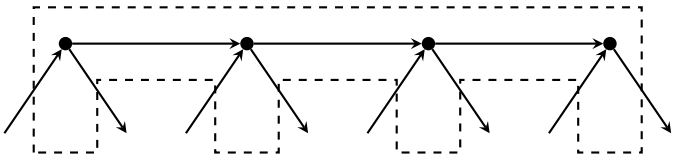


Figure 10 – A single information-processing system modeled as a comb. The nodes represent an operation and the arrows capture a quantum state. Each tooth of the comb corresponds to a pair of an input and an output message.

as $\sigma_{MY_1} = \mathcal{E}_1(\rho_{X_1} \otimes |0\rangle\langle 0|_M)$. Upon receiving the next input σ_{X_2}, the new memory state and output are $\tau_{MY_2} = \mathcal{E}_2(\sigma_{X_2 M})$, etc.

A more compact representation of a comb which omits the internal memory is given by a single CPTP map

$$\mathcal{E} : \mathcal{L}(\mathcal{H}_{X_1 \cdots X_n}) \to \mathcal{L}(\mathcal{H}_{Y_1 \cdots Y_n}),$$

which, for all $i \in [n]$ and all $\rho_{X_1 \cdots X_n}, \sigma_{X_1 \cdots X_n} \in \mathcal{L}(\mathcal{H}_{X_1 \cdots X_n})$ such that $\rho_{X_1 \cdots X_i} = \sigma_{X_1 \cdots X_i}$ satisfies the relation

$$\mathrm{tr}_{Y_{i+1} \cdots Y_n}[\mathcal{E}(\rho_{X_1 \cdots X_n})] = \mathrm{tr}_{Y_{i+1} \cdots Y_n}[\mathcal{E}(\sigma_{X_1 \cdots X_n})],$$

i.e., if the inputs are identical up to position i, then the outputs must be identical up to position i as well. This can be seen as a causality condition, namely that an input after i cannot influence an output before i.

A very convenient representation of combs is given by the Choi-Jamiołkowski representation [43] of the map $\mathcal{E}$, namely the operator $\mathsf{R}_{Y_1 \cdots Y_n X_1 \cdots X_n} \in \mathcal{L}(\mathcal{H}_{Y_1 \cdots Y_n X_1 \cdots X_n})$ given by

$$\mathsf{R}_{Y_1 \cdots Y_n X_1 \cdots X_n} \coloneqq \sum_{i,j} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j|.$$

The causality condition then becomes

$$\mathrm{tr}_{Y_{i+1} \cdots Y_n}(\mathsf{R}_{Y_1 \cdots Y_n X_1 \cdots X_n}) = \mathsf{R}_{Y_1 \cdots Y_i X_1 \cdots X_i} \otimes I_{X_{i+1} \cdots X_n}.$$

Remark B.1 (Sequential scheduling). If the output value in register Y_i corresponds to one message being sent to one (random) party — where the name of the party might be a *classical* part of the message — then the composition of combs obtained by routing messages to the correct parties is alway a new well-defined comb.[21] The systems used in this work in all sections except Section 3.2 follow this rule, and are thus modeled as quantum combs. In Appendix B.2 we discuss some settings that do not use sequential scheduling, and thus need a more complex model of systems to be captured.

[21] This follows because in such a network of systems, there is always ever only one active party, the one that has just received a message. Thus, the next message to be output and the next active party is always uniquely defined.

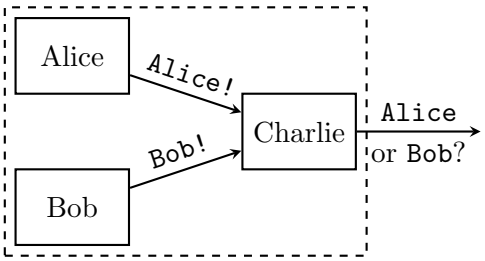


Figure 11 – Alice and Bob both send messages to Charlie, who outputs the first message he receives. Although each system can be described by a comb, the composition of the three, depicted as the dashed box, is undefined.

B.2 Causal Boxes

The quantum combs introduced in Appendix B.1 are well-suited for modeling finite systems with sequential scheduling, which is the case for all the concrete protocols analyzed in this work. There are however situations which require a more developed model of systems. Consider the example drawn in Figure 11: two players, Alice and Bob, each send a message to a third player, Charlie, who outputs the first message he receives and ignores the second. Each of the systems is a well-defined comb. Alice and Bob just output a single message. When Charlie receives the first message, $m = (v, p)$ — value v from player p — he outputs v and ignores all further inputs. But the composition of all three systems (depicted as a dashed box in Figure 11) is not defined: it is a system with no input and one output, but this output is undetermined.

The composition of these three systems is undefined, because Charlie's output depends on the order of the messages he receives, but this is not specified by the individual systems of Alice and Bob. The *causal box* framework [26] was developed to model such systems. It achieves this by assigning a tag $t \in \mathcal{T}$ to values $v \in \mathcal{V}$ that are output (and input) by quantum information-processing systems. $\mathcal{T}$ is a partially ordered set (e.g., $\mathcal{T} = \mathbb{Q}$), and $t \in \mathcal{T}$, which can be thought of as a time, denotes the order of v with respect to other messages. This also allows superpositions of causal structures to be modeled by allowing a message to be in a superposition of different positions, e.g., $|t_1\rangle + |t_2\rangle$. Additionally, when the cardinality of $\mathcal{T}$ is infinite, the resulting causal boxes can process an unbounded number of messages, e.g., a beacon which outputs a qubit every second is valid causal box, but cannot be modeled as a quantum comb.

More precisely, a quantum message that is either input to or output from a causal box is an element of a Hilbert space with an orthonormal basis given by $\{|v, t\rangle\}_{v\in\mathcal{V}, t\in\mathcal{T}}$. For a finite $\mathcal{V}$ and infinite $\mathcal{T}$, this Hilbert space corresponds to

$$\mathbb{C}^{|\mathcal{V}|} \otimes \ell^2(\mathcal{T}), \tag{23}$$

where $\ell^2(\mathcal{T}) = \{(x_t)_{t\in\mathcal{T}} : x_t \in \mathbb{C}, \|x\| < \infty\}$ is the sequence space with

bounded 2-norm with $\|x\| = \sqrt{\langle x|x\rangle}$ and $\langle x|y\rangle = \sum_{t\in\mathcal{T}} \overline{x_t} y_t$.

An arrow used in figures such as Figure 6 captures an unbounded number of messages being output or input. We refer to such an object as a wire (which may connect two systems), and its Hilbert space is given by a Fock space,

$$\mathcal{F}(\mathcal{H}) \coloneqq \bigoplus_{n=0}^{\infty} \vee^n \mathcal{H}\,, \tag{24}$$

where $\vee^n\mathcal{H}$ denotes the symmetric subspace of $\mathcal{H}^{\otimes n}$, and $\mathcal{H}^{\otimes 0}$ is the one dimensional space containing the vacuum state $|\Omega\rangle$. Plugging Eq. (23) into Eq. (24) for a d dimensional value ($|\mathcal{V}| = d$), we find that the message space of a wire is

$$\mathcal{F}\Big(\mathbb{C}^d \otimes \ell^2(\mathcal{T})\Big) = \bigoplus_{n=0}^{\infty} \vee^n \Big(\mathbb{C}^d \otimes \ell^2(\mathcal{T})\Big)\,. \tag{25}$$

The orthogonal subspaces $\vee^n\big(\mathbb{C}^d \otimes \ell^2(\mathcal{T})\big)$ for $n \in \mathbb{N}_0$ capture n messages being sent on a wire. The restriction to the symmetric space guarantees that there is no order amongst the messages other than what might be defined from their state, e.g., their position in $\mathcal{T}$.

Let A denote a wire that carries d_A-dimensional messages. Abusing language, we will refer to this as a d_A-dimensional wire.[22] We write $\mathcal{F}_A^{\mathcal{T}}$ for the corresponding state space, namely

$$\mathcal{F}_A^{\mathcal{T}} \coloneqq \mathcal{F}\Big(\mathbb{C}^{d_A} \otimes \ell^2(\mathcal{T})\Big)\,.$$

Note that for any Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$,

$$\mathcal{F}(\mathcal{H}_A) \otimes \mathcal{F}(\mathcal{H}_B) \cong \mathcal{F}(\mathcal{H}_A \oplus \mathcal{H}_B)\,, \tag{26}$$

where the isomorphism preserves the meaning associated with the bases of the Fock spaces, i.e., a tensor product of two vacuum states on the left in Eq. (26) is mapped to a vacuum state on the right, a tensor product of a vacuum state and one message on the left is mapped to a single message with the same value and position on the right, etc. (see [26] for the exact isomorphism). This allows the tensor product of two wires with dimensions d_A and d_B to be written as one wire with dimension $d_A + d_B$,

$$\mathcal{F}_A^{\mathcal{T}} \otimes \mathcal{F}_B^{\mathcal{T}} \cong \mathcal{F}_{AB}^{\mathcal{T}}.$$

Similarly, for any $\mathcal{P} \subset \mathcal{T}$, a wire may be split in two parts corresponding to messages in $\mathcal{P}$ and $\tilde{\mathcal{P}} \coloneqq \mathcal{T} \setminus \mathcal{P}$, respectively:

$$\mathcal{F}_A^{\mathcal{T}} \cong \mathcal{F}_A^{\mathcal{P}} \otimes \mathcal{F}_A^{\tilde{\mathcal{P}}}.$$

[22] The Hilbert space of the wire is in fact infinite dimensional.

We use this in particular to trace out messages that are not before some position $t \in \mathcal{T}$ by taking $\mathcal{P} = \{p \in \mathcal{T} : p \leq t\}$, e.g.,

$$\rho_A^{\leq t} = \mathrm{tr}_{\not\leq t}(\rho_A).$$

Let $\mathcal{F}_X^{\mathcal{T}}$ and $\mathcal{F}_Y^{\mathcal{T}}$ denote the Hilbert spaces of an input wire X and output wire Y. And let $\mathfrak{T}(\mathcal{F}_X^{\mathcal{T}})$ and $\mathfrak{T}(\mathcal{F}_Y^{\mathcal{T}})$ be the corresponding sets of trace class operators. For the specical case of a totally ordered set $\mathcal{T}$,[23] a causal box is defined as a set of mutually consistent CPTP maps

$$\mathsf{R} = \left\{\mathcal{E}^{\leq t} : \mathfrak{T}\left(\mathcal{F}_X^{\mathcal{T}}\right) \to \mathfrak{T}\left(\mathcal{F}_Y^{\leq t}\right)\right\}_{t\in\mathcal{T}},$$

i.e., for $t \leq u$,

$$\mathcal{E}^{\leq t} = \mathrm{tr}_{>t} \circ \mathcal{E}^{\leq u}.$$

In some cases the map $\mathcal{E} = \lim_{t\to\infty} \mathcal{E}^{\leq t}$ is well-defined, in which case a causal box can be defined by this limit instead of by the sequence.

As for quantum combs, causal boxes must satisfy a notion of causality, so that an input before position t cannot influence an output after position t. The exact definition is not needed in this work, so we omit it, and refer the interested reader to [26]. Similarly, causal boxes can be represented using the Choi-Jamiołkowski isomorphism, which we omit here as well.

Causal boxes may be connected in arbitrary ways, i.e., any output wire of one box can be "plugged into" an input wire of the same dimension from a different box, or may be looped back and connected to one if its own inputs. This always results in a new well-defined causal box, even if loops are present. It does not create any causality conflicts since messages are ordered and an output can only depend on inputs that arrived before.

Remark B.2 (From combs to causal boxes). Quantum combs may be seen as special cases of causal boxes, which do not specify the positions $t \in \mathcal{T}$ of the outputs, only the (local) order with respect to the other outputs it generates. One can easily "upgrade" a quantum comb to a causal box by assigning some (fixed) processing time δ_i to produce the output Y_i after receiving the input X_i, in which case it inherits all the properties (e.g., closure under composition) of causal boxes. Alternatively, a comb can be modeled as a specification of causal boxes, namely those that produce the same outputs in the same order, but at undetermined times.

C Quantum Key Distribution

A QKD protocol typically has three phases.[24] In the first, the players exchange some quantum states — either one player (Alice) generates them

[23] The case for a partial order on $\mathcal{T}$ can be found in [26].

[24] A detailed review of QKD can be found in [23].

and sends them to the other (Bob), or an untrusted third party (Eve) prepares states that are sent to both players. We assume for simplicity that the players measure the quantum states upon reception, but the same analysis holds for protocols that require quantum memory as well. In Figure 3 we illustrated the case where the players have access to an (insecure) quantum channel that they use to send quantum states from Alice to Bob. In the second phase of the protocol, the players compare some of the measurement results to estimate the amount of noise on the channel. At the end of this phase, they obtain a bound on the entropy of the remaining undisclosed bit strings conditioned on the adversary's information. In the final phase, the players run some (classical) post-processing protocols on the strings they hold to extract a secret key. More precisely, they first need to correct errors between the strings held by Alice and Bob. Then they run a privacy amplification step to extract a secret key from their strings.

In Section 4 we used these error correction and privacy amplification procedures to get a secret key from any min-entropy resource. Here, we show that a standard QKD security proof, but with the post-processing omitted, constructs such a min-entropy resource. More precisely, let $\pi_{AB}^{\text{dis}} = (\pi_A^{\text{dis}}, \pi_B^{\text{dis}})$ be a protocol that distributes quantum states using an insecure channel $\mathcal{Q}$, then uses an authentic channel $\mathcal{A}^c$ to compare the measurement results, and either aborts or produces two (random) strings X and Y. Let Eve have access to the quantum channel and apply any operation allowed by quantum mechanics to the states being sent, and let her obtain a transcript of the messages sent on the classical authentic channel. We prove below that if we can bound the information Eve has about X, then π_{AB}^{dis} constructs a min-entropy resource.

Proving that we can bound the information Eve has about X is the difficult part of QKD security proofs. Here we only show that if this can be done, then the protocol can be written as a constructive statement in the AC framework. An overview of how one can actually bound Eve's information can be found in [23], and detailed security proofs for BB84 and BBM92 that compute these bounds are given in [14].

Lemma C.1. *Let $\pi_{AB}^{dis} = (\pi_A^{dis}, \pi_B^{dis})$ be a protocol as described above. Suppose that one can prove that the subnormalized state σ_{XYE} resulting from Alice and Bob not aborting is such that $H_{\min}^{\delta}(X|E)_\sigma \geq k$. And let $\overline{\mathcal{H}}_{\min}^{k,\delta}$ be a (k,δ)-min-entropy resource where the output Y at Bob's interface is arbitrary (but is always $\perp$ if Alice's is $\perp$). Then π_{AB}^{dis} (perfectly) constructs $\overline{\mathcal{H}}_{\min}^{k,\delta}$ from $\mathcal{Q}\|\mathcal{A}^c$,*

$$\mathcal{Q}\|\mathcal{A}^c \xrightarrow{\pi_{AB}^{dis},0} \overline{\mathcal{H}}_{\min}^{k,\delta}.$$

Proof. We will show that $\pi_{AB}^{\text{dis}}(\mathcal{Q}\|\mathcal{A}^c) \subset \overline{\mathcal{H}}_{\min}^{k,\delta}$. By contradiction, suppose there exists $\mathsf{H} \in \pi_{AB}^{\text{dis}}(\mathcal{Q}\|\mathcal{A}^c)$ such that $\mathsf{H} \notin \overline{\mathcal{H}}_{\min}^{k,\delta}$. This means there must

exist an S such that the output $\rho_{XE} = |\perp\rangle\langle\perp| \otimes \tau_E + \sigma_{XE}$ after interacting with H has $H^{\delta}_{\min}(X|E)_{\sigma} < k$. By running such a system S, Eve would thus obtain more information about the string X than allowed. □

If no adversary is eavesdropping on the quantum channel $\mathcal{Q}$, but instead it is only subject to natural noise, then one can make stronger statements than Lemma C.1 in which Y is not arbitrary, but a bound on the number of errors between X and Y is known, and the probability of aborting is also bounded. Such statements are necessary for proving the robustness of the protocols, i.e., the probability that they terminate with a shared secret key when only natural noise is present (see [14, 21] for a formal treatment of robustness in QKD.)

For example, instead of an insecure channel $\mathcal{Q}$, let the players share a noisy channel specification $\mathcal{C}$ such as the depolarizing channels depicted in Figure 1b. Then one can often prove statements such as

$$\mathcal{C}\|\mathcal{A}^c \xrightarrow{\pi^{\text{dis}}_{AB},\varepsilon_{\text{noise}}} \overline{\mathcal{R}}^{k,\delta}_{\min}, \tag{27}$$

where $\overline{\mathcal{R}}^{k,\delta}_{\min} \subset \overline{\mathcal{H}}^{k,\delta}_{\min}$ is a specification of min-entropy resources that never aborts and outputs strings X and Y with specific correlations (e.g., no more than t bit flips).

Composing Corollary 4.7, Lemma C.1, and Eq. (27), we recover the standard QKD security statement [21].

Corollary C.2. *Let $\pi^{qkd} = \pi^{pa} \circ \pi^{ec} \circ \pi^{dis}$ consist of the composition of the protocols described here and Section 4, then*

$$\mathcal{C}\|\mathcal{A}^c \xrightarrow{\pi^{qkd},\varepsilon_{noise}+\varepsilon_{pa}+2\delta} \underline{\mathcal{K}}^m,$$

and

$$\mathcal{Q}\|\mathcal{A}^c \xrightarrow{\pi^{qkd},\varepsilon_{verif}+\varepsilon_{pa}+2\delta} \mathcal{K}^m,$$

where $\mathcal{A}^c = \mathcal{A}^{c_1}\|\mathcal{A}^{c_2}\|\mathcal{A}^{c_3}$, and $\mathcal{A}^{c_i}$ are the authentic channels used by the different parts of the protocol.

D Technical Lemmas

D.1 Min-entropy inequalities

The following inequality shows that if an additional r bit string Z is given to the adversary, then she gets r bits of information.

Lemma D.1 ([45, Lemma 11])**.** *Let $\rho \in \mathcal{S}_{\leq}(\mathcal{H}_{ABZ})$ be any subnormalized state where Z is a classical system over the alphabet $\mathcal{Z}$. Then*

$$H^{\delta}_{\min}(A|BZ)_{\rho} \geq H^{\delta}_{\min}(A|B)_{\rho} - \log|\mathcal{Z}|.$$

The next inequality shows that the min-entropy of a state conditioned on an event is bounded by the min-entropy before this conditioning.

Lemma D.2. *Let $\rho \in \mathcal{S}_{\leq}(\mathcal{H}_{ABZ})$ be any subnormalized state with a binary classical register Z. This state may be written as*

$$\rho_{ABZ} = \rho^0_{AB} \otimes |0\rangle\langle 0| + \rho^1_{AB} \otimes |1\rangle\langle 1|.$$

Then

$$H^{\delta}_{\min}(A|B)_{\rho^0} \geq H^{\delta}_{\min}(A|B)_{\rho} \ .$$

Proof. Follows from [14, Lemma 10] by taking X to be empty, $Y = Z$ and $\Omega : \mathcal{Y} \to \{0,1\}$ is the identity. We also remove the condition $\delta \in [0, \sqrt{\operatorname{tr} \rho})$ by defining $H_{\min}(A|B)_\rho = +\infty$ if $\operatorname{tr} \rho = 0$. □

D.2 Extractors

Extractors are usually defined on normalized states. We show here than any extractor for normalized states is also an extractor for subnormalized states. This proof follows the steps of an equivalent proof for multi-source extractors in the Markov model from [46, Lemma 37], but is adapted to seeded extractors.

Lemma D.3. *If* Ext *is a quantum-proof (k, ε)-strong extractor for normalized states, then it is a quantum-proof $(k+1, 2\varepsilon)$-strong extractor for subnormalized states.*

Proof. Let $\rho_{XE} \in \mathcal{S}_{\leq}(\mathcal{H}_{XE})$ be a subnormalized state with $H_{\min}(X|E)_\rho \geq k+1$, and let $p = \operatorname{tr}(\rho_{XE})$. We define $\tilde{\rho}_E \coloneqq \frac{1-p}{p}\rho_E$ and the normalized state

$$\sigma_{XEP} \coloneqq \rho_{XE} \otimes |0\rangle\langle 0|_P + \tau_X \otimes \tilde{\rho}_E \otimes |1\rangle\langle 1|_P, \tag{28}$$

where τ_X is the fully mixed state.

This state satisfies a slightly modified min-entropy condition:

$$\begin{aligned} p_{\text{guess}}(X|EP)_\sigma &= p_{\text{guess}}(X|E)_\rho + p_{\text{guess}}(X|E)_{\tau\otimes\tilde{\rho}} \\ &\leq 2^{-k-1} + (1-p)2^{-n} \leq 2^{-k}, \end{aligned}$$

where n is the length of the string X. Hence $H_{\min}(X|EP)_\sigma \geq k$. And because Ext is an extractor for normalized states it follows that

$$\frac{1}{2}\left\|\sigma_{\text{Ext}(X,Z)ZEP} - \tau_K \otimes \tau_Z \otimes \sigma_{EP}\right\|_{\text{tr}} \leq \varepsilon.$$

Plugging in Eq. (28) and tracing out P, we get

$$\frac{1}{2}\left\|\rho_{\text{Ext}(X,Z)ZE} - \tau_{\text{Ext}(X,Z)Z} \otimes \tilde{\rho}_E - \tau_K \otimes \tau_Z \otimes \rho_E + \tau_K \otimes \tau_Z \otimes \tilde{\rho}_E\right\|_{\text{tr}} \leq \varepsilon.$$

Thus starting from the expression $\|\rho_{\mathrm{Ext}(X,Z)ZE} - \tau_K \otimes \tau_Z \otimes \rho_E\|_{\mathrm{tr}}$ and then adding and subtracting the term $\tau_{\mathrm{Ext}(X,Z)Z} \otimes \tilde{\rho}_E - \tau_K \otimes \tau_Z \otimes \tilde{\rho}_E$ as well as applying the triangle inequality leaves us with

$$\begin{aligned}\frac{1}{2}\left\|\rho_{\mathrm{Ext}(X,Z)ZE} - \tau_K \otimes \tau_Z \otimes \rho_E\right\|_{\mathrm{tr}} \\ &\leq \varepsilon + \frac{1}{2}\left\|\tau_{\mathrm{Ext}(X,Z)Z} \otimes \tilde{\rho}_E - \tau_K \otimes \tau_Z \otimes \tilde{\rho}_E\right\|_{\mathrm{tr}} \\ &\leq \varepsilon + \frac{1}{2}\operatorname{tr}(\tilde{\rho}_E)\left\|\tau_{\mathrm{Ext}(X,Z)Z} - \tau_K \otimes \tau_Z\right\|_{\mathrm{tr}} \leq 2\varepsilon. \qquad \square\end{aligned}$$

The following lemma shows that any extractor defined for subnormalized states can be used to extract from states with a bound on the smooth min-entropy instead of on the min-entropy with a small adjustment to the error parameter. Note that the original lemma from [39, Lemma 3.5] omitted to specify that the extractor has to be defined for subnormalized states for the proof to go through.

Lemma D.4 ([39, Lemma 3.5])**.** *If* Ext *is a quantum-proof* (k,ε)*-strong extractor for subnormalized states, then for any subnormalized* $\rho_{XE} \in \mathcal{S}_{\leq}(\mathcal{H}_{XE})$ *with classical* X *and* $H^{\delta}_{\min}(X|E)_\rho \geq k$*, and a uniform* Z*,*

$$\frac{1}{2}\left\|\rho_{\mathrm{Ext}(X,Z)ZE} - \tau_K \otimes \tau_Z \otimes \rho_E\right\|_{\mathrm{tr}} \leq \varepsilon + 2\delta,$$

where τ_K *is the fully mixed state.*

The final extractor lemma that we need states that the composition of two extractors is also an extractor, and is also taken from [39].

Lemma D.5 ([39, Lemma A.4])**.** *Let* $\mathrm{Ext}_1 : \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^{m_1}$ *and* $\mathrm{Ext}_2 : \{0,1\}^n \times \{0,1\}^{d_2} \to \{0,1\}^{m_2}$ *be quantum-proof* (k,ε_1)*- and* $(k-m_1,\varepsilon_2)$*-strong extractors for subnormalized states. Then the composition of the two, namely*

$$\begin{aligned}\mathrm{Ext}_3 :&\{0,1\}^n \times \{0,1\}^{d_1+d_2} \to \{0,1\}^{m_1+m_2} \\ &(x, y_1\|y_2) \mapsto \mathrm{Ext}_1(x,y_1)\|\,\mathrm{Ext}_2(x,y_2),\end{aligned}$$

is a quantum-proof $(k,\varepsilon_1+\varepsilon_2)$*-strong extractor for subnormalized states.*

D.3 Key-Privacy and uniformity

The lemmas in this section are all from [19]. The first states that a specific kind of extractor can provides ν-key-privacy (Definition 5.1) and uniformity (Definition 5.2).

Lemma D.6 ([19, Proposition 2])**.** *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^{r-m} \to \{0,1\}^m$ *be a quantum-proof* (k,ε)*-strong extractors for subnormalized states for any* k *and* $\varepsilon = \frac{\nu}{2}\sqrt{2^{-k+m}}$*. And let* $h : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^m$ *be defined as* $h(x,\ell_1\|\ell_2) \coloneqq \mathrm{Ext}(x,\ell_1) \oplus \ell_2$*. Then* h *provides* ν*-key-privacy.*

The next lemma shows that the composition of two functions that provide key-privacy results in a new function also providing key-privacy. The same holds for uniformity.

Lemma D.7 ([19, Proposition 4]). *Let $h_1 : \mathcal{X} \times \mathcal{L}_1 \to \mathcal{T}_1$ and $h_2 : (\mathcal{X} \times \mathcal{T}_1) \times \mathcal{L}_2 \to \mathcal{T}_2$ be two functions. We define $h : \mathcal{X} \times (\mathcal{L}_1 \times \mathcal{L}_2) \to (\mathcal{T}_1 \times \mathcal{T}_2)$ with $h(x, \ell_1 \| \ell_2) \coloneqq t \| h_2(x \| t, \ell_2)$ where $t \coloneqq h_1(x, \ell_1)$. If h_1 and h_2 provide ν_1 and ν_2-key-privacy, respectively, then h provides $\nu_1 + \nu_2$-key-privacy. And if h_1 and h_2 are both uniform, then h is uniform.*

D.4 Guessing Games

The lemmas in this section are also from [19]. They are concerned with a setting in which different players sharing a quantum state are trying to guess the outcome of a measurement performed by one of them.

In the following we denote n EPR pairs by Φ^+_{AB}, and $P^\theta_x = H^\theta |x\rangle\langle x| H^\theta$ denotes a projector, which we use to measure qubits in either the computational or diagonal basis. Note that by measuring half of EPR pairs with these projectors, the other half results in the state $H^\theta |x\rangle\langle x| H^\theta$, i.e.,

$$\mathrm{tr}_A \Big[\Big(P^\theta_x \otimes I_B \Big) \Phi^+_{AB} \Big(P^\theta_x \otimes I_B \Big) \Big] = \frac{1}{2^n} H^\theta |x\rangle\langle x| H^\theta .$$

Given two registers Θ and A, where Θ is classical and A is quantum, we denote the map which performs this measurement on A according to Θ and writes the result in a register X as $\mathcal{M}^{\mathrm{BB84}}_{\Theta A, X}$, i.e.,

$$\mathcal{M}^{\mathrm{BB84}}_{\Theta A, X}(\rho_{\Theta A}) = \sum_{\theta, x} \mathrm{tr}_A \, |x\rangle\langle x| \otimes \Big[\Big(|\theta\rangle\langle\theta| \otimes P^\theta_x \Big) \rho_{\Theta A B} \Big(|\theta\rangle\langle\theta| \otimes P^\theta_x \Big) \Big].$$

The first lemma considers a two player setting, where one player obtains the measurement outcome X and the second player wants to guess it.

Lemma D.8 ([19, Corollary 2]). *Let $\rho_{\Theta E}$ be any cq-state, where the strings $\theta \in \mathcal{C} \subset \{0,1\}^n$ are taken from a code $\mathcal{C}$ with minimal distance d, let $\mathcal{E} : \mathcal{L}(\mathcal{H}_E) \to \mathcal{L}(\mathcal{H}_{AB})$ be any CPTP map where $\mathcal{L}(\mathcal{H}_A)$ is an n qubit Hilbert space, and let $\sigma_{X\Theta B} \coloneqq \mathcal{M}^{BB84}_{\Theta A, X} \circ \mathcal{E}(\rho_{\Theta E})$. Then*

$$p_{\mathrm{guess}}(X|B)_\sigma \leq p_{\mathrm{guess}}(\Theta|E)_\rho \left(1 + \frac{|\mathcal{C}|}{2^{d/2}} \right).$$

The second lemma considers a three player setting. The first player obtains the measurement outcome X, the second one has to get an outcome X' that is close to X and the third one wants to guess X. Note that in this setting, the all players have access to Θ.

Lemma D.9 ([19, Corollary 3, Remark 6]). *Let $\rho_{\Theta E}$ be any cq-state, where the strings $\theta \in \mathcal{C} \subset \{0,1\}^n$ are taken from a code $\mathcal{C}$ with minimal distance d. Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_E) \to \mathcal{L}(\mathcal{H}_{ABC})$ be any CPTP map where $\mathcal{L}(\mathcal{H}_A)$ and $\mathcal{L}(\mathcal{H}_B)$ are an n qubit Hilbert spaces. Let $\sigma_{XX'\Theta C} \coloneqq \mathcal{M}^{BB84}_{\Theta A,X} \circ \mathcal{M}^{BB84}_{\Theta B,X'} \circ \mathcal{E}(\rho_{\Theta E})$, i.e., both A and B are measured according to Θ and the results are written in X and X', respectively. Finally, let $\sigma^1_{XX'\Theta C}$ be the projection of $\sigma_{XX'\Theta C}$ on the space with $w(X,X') \leq \varphi n$. Then*

$$p_{\text{guess}}(X|\Theta C)_{\sigma^1} \leq p_{\text{guess}}(\Theta|E)_\rho \left(1 + \frac{|\mathcal{C}|2^{h(\varphi)n}}{2^d}\right).$$

Acknowledgments

CP if grateful to Serge Fehr for lively conversations on composable security, and for a lot of help understanding his paper. He would also like to thank Ueli Maurer for discussions on Constructive Cryptography, and Renato Renner for commenting on an initial draft of this work and proposing many of the ideas used in this paper.

CP is partially supported by the US Air Force Office of Scientific Research (AFOSR) via grant FA9550-16-1-0245, the Swiss National Science Foundation (via the National Centre of Competence in Research 'Quantum Science and Technology'), and the Zurich Information Security and Privacy Center.

References

[1] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of the 42nd Symposium on Foundations of Computer Science, FOCS '01*, pages 136–145. IEEE, 2001. [doi:10.1109/SFCS.2001.959888].

[2] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2013. Updated version of [1]. [IACR e-print: 2000/067].

[3] Ueli Maurer and Renato Renner. Abstract cryptography. In *Proceedings of Innovations in Computer Science, ICS 2011*, pages 1–21. Tsinghua University Press, 2011.

[4] Ueli Maurer and Renato Renner. From indifferentiability to constructive cryptography (and back). In *Theory of Cryptography, Proceedings of TCC 2016-B, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 3–24. Springer, 2016. [doi:10.1007/978-3-662-53641-4_1, IACR e-print: 2016/903].

[5] Lídia del Rio. *Resource theories of knowledge*. PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2015. [doi:10.3929/ethz-a-010553983].

[6] Lídia del Rio, Lea Kraemer, and Renato Renner. Resource theories of knowledge. Eprint, 2015. [arXiv:1511.08818].

[7] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, September 2005. [arXiv:quant-ph/0512258].

[8] Ueli Maurer. Secret key agreement by public discussion. *IEEE Transaction on Information Theory*, 39(3):733–742, May 1993. A preliminary version appeared at CRYPTO '92. [doi:10.1109/18.256484].

[9] Rudolph Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography—Part I: Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, July 1993. [doi:10.1109/18.243431].

[10] Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *Advances in Cryptology – ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 199–216. Springer, 2005. [doi:10.1007/11593447_11].

[11] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[12] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, 2012. [doi:10.1038/ncomms1631, arXiv:1103.4130].

[13] Masahito Hayashi and Toyohiro Tsurumaru. Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, 14(9):093014, 2012. [doi:10.1088/1367-2630/14/9/093014, arXiv:1107.0589].

[14] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. Eprint, 2015. [arXiv:1506.08458].

[15] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95:010503, June 2005. [doi:10.1103/PhysRevLett.95.010503, arXiv:quant-ph/0405101].

[16] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009. [doi:10.1088/1367-2630/11/4/045021, arXiv:0903.4460].

[17] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113:140501, September 2014. [doi:10.1103/PhysRevLett.113.140501, arXiv:1210.1810].

[18] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. Eprint, 2016. [arXiv:1607.01797].

[19] Serge Fehr and Louis Salvail. Quantum authentication and encryption with key recycling. In *Advances in Cryptology – EUROCRYPT 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 311–338. Springer, 2017. [doi:10.1007/978-3-319-56617-7_11, IACR e-print: 2017/102].

[20] Serge Fehr and Louis Salvail. Quantum authentication and encryption with key recycling. Eprint, 2017. Extended version of [19]. [arXiv:1610.05614].

[21] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. Eprint, 2014. [arXiv:1409.3525].

[22] Charles H. Bennett, Gilles Brassard, and Seth Breidbart. Quantum cryptography II: How to re-use a one-time pad safely even if P=NP. Original unpublished manuscript uploaded to arXiv in 2014, 1982. [arXiv:1407.0451].

[23] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, September 2009. [doi:10.1103/RevModPhys.81.1301, arXiv:0802.4155].

[24] Christopher Portmann. Key recycling in authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, July 2014. [doi:10.1109/TIT.2014.2317312, arXiv:1202.1229].

[25] Ueli Maurer. Constructive cryptography—a new paradigm for security definitions and proofs. In *Proceedings of Theory of Security and Applications, TOSCA 2011*, volume 6993 of *Lecture Notes in Computer Science*, pages 33–56. Springer, 2012. [doi:10.1007/978-3-642-27375-9_3].

[26] Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner, and Björn Tackmann. Causal boxes: Quantum information-processing systems closed under composition. *IEEE Transactions on Information Theory*, 63(5):3277–3305, May 2017. [doi:10.1109/TIT.2017.2676805, arXiv:1512.02240].

[27] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th Symposium on Theory of Computing, STOC '07*, pages 565–574. ACM, 2007. [doi:10.1145/1250790.1250873, arXiv:quant-ph/0611234].

[28] Gus Gutoski. On a measure of distance for quantum strategies. *Journal of Mathematical Physics*, 53(3):032202, 2012. [doi:10.1063/1.3693621, arXiv:1008.4636].

[29] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80:022339, August 2009. [doi:10.1103/PhysRevA.80.022339, arXiv:0904.4483].

[30] Lucien Hardy. Reformulating and reconstructing quantum theory. Eprint, 2011. [arXiv:1104.2066].

[31] Lucien Hardy. The operator tensor formulation of quantum theory. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 370(1971):3385–3417, 2012. [doi:10.1098/rsta.2011.0326, arXiv:1201.4390].

[32] Lucien Hardy. Quantum theory with bold operator tensors. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 373(2047), 2015. [doi:10.1098/rsta.2014.0239].

[33] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56(9):4674–4681, 2010. [doi:10.1109/TIT.2010.2054130, arXiv:0907.5238].

[34] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 41(6):1915–1923, November 1995. [doi:10.1109/18.476316].

[35] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography, Proceedings of TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005. [doi:10.1007/978-3-540-30576-7_22, arXiv:quant-ph/0403133].

[36] Serge Fehr and Christian Schaffner. Randomness extraction via δ-biased masking in the presence of a quantum attacker. In *Theory of Cryptography, Proceedings of TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 465–481. Springer, 2008. [doi:10.1007/978-3-540-78524-8_26, arXiv:0706.2606].

[37] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, August 2011. A preliminary version appeared at ISIT 2010. [doi:10.1109/TIT.2011.2158473, arXiv:1002.2436].

[38] Masahito Hayashi and Toyohiro Tsurumaru. More efficient privacy amplification with less random seeds via dual universal hash function. *IEEE Transactions on Information Theory*, 62(4):2213–2232, April 2016. [doi:10.1109/TIT.2016.2526018, arXiv:1311.5322].

[39] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, 2012. [doi:10.1137/100813683, arXiv:0912.5514].

[40] Mark N. Wegman and Larry Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[41] Douglas R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4(3):369–380, 1994. A preliminary version appeared at CRYPTO '91. [doi:10.1007/BF01388651].

[42] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[43] John Watrous. Theory of quantum information, 2016. Book draft, `https://cs.uwaterloo.ca/~watrous/TQI/`.

[44] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, 2009. [arXiv:0807.1338].

[45] Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner. Impossibility of growing quantum bit commitments. *Physical Review Letters*, 107:090502, August 2011. [doi:10.1103/PhysRevLett.107.090502, arXiv:1105.1165].

[46] Rotem Arnon-Friedman, Christopher Portmann, and Volkher B. Scholz. Quantum-proof multi-source randomness extractors in the Markov

model. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:34. Schloss Dagstuhl, 2016. [doi:10.4230/LIPIcs.TQC.2016.2, arXiv:1510.06743].