Composable and Finite Computational Security of Quantum Message Transmission

Fabio Banfi, Ueli Maurer, Christopher Portmann, and Jiamin Zhu

Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
{fbanfi,maurer,chportma,zhujia}@inf.ethz.ch

Abstract. Recent research in quantum cryptography has led to the development of schemes that encrypt and authenticate quantum messages with computational security. The security definitions used so far in the literature are asymptotic, game-based, and not known to be composable. We show how to define finite, composable, computational security for secure quantum message transmission. The new definitions do not involve any games or oracles, they are directly operational: a scheme is secure if it transforms an insecure channel and a shared key into an ideal secure channel from Alice to Bob, i.e., one which only allows Eve to block messages and learn their size, but not change them or read them. By modifying the ideal channel to provide Eve with more or less capabilities, one gets an array of different security notions. By design these transformations are composable, resulting in composable security.

Crucially, the new definitions are *finite*. Security does not rely on the asymptotic hardness of a computational problem. Instead, one proves a finite reduction: if an adversary can distinguish the constructed (real) channel from the ideal one (for some fixed security parameters), then she can solve a finite instance of some computational problem. Such a finite statement is needed to make security claims about concrete implementations.

We then prove that (slightly modified versions of) protocols proposed in the literature satisfy these composable definitions. And finally, we study the relations between some game-based definitions and our composable ones. In particular, we look at notions of quantum authenticated encryption and QCCA2, and show that they suffer from the same issues as their classical counterparts: they exclude certain protocols which are arguably secure.

1 Introduction

At its core, a security definition is a set of mathematical conditions, and a security proof consists in showing that these conditions hold for a given protocol. Given various security definitions, one may analyze which are stronger and weaker by proving reductions or finding separating examples. This however does not tell us which definitions one should use, since too weak definitions may have security issues and too strong definitions may exclude protocols that are arguably secure. For example, IND-CCA2 is often considered an unnecessarily strong security definition, since taking a scheme which is IND-CCA2 and appending a bit to the

ciphertext results in a new encryption scheme that is arguably as secure as the original scheme, but does not satisfy IND-CCA2 [CKN03, CMT13].

In this work we take a more critical approach to defining security. We ask what criteria a security definition needs to satisfy that are both necessary and sufficient conditions to call a protocol "secure". We then apply them to the problem of encrypting and authenticating quantum messages with computational security in the symmetric-key setting.

1.1   A Security Desideratum

Operational security. Common security definitions for encryption and authentication found in the literature are *game-based*, i.e., they require that an adversary cannot win a game such as guessing what message has been encrypted given access to certain oracles, see, e.g., [BDPR98] and [KY06] for comparisons of various such games in the public-key and private-key settings, respectively. These have been adapted for transmitting quantum messages: a definition for QCPA has been proposed in [BJ15], QCCA1 in [ABF+16], and QCCA2 as well as notions of quantum unforgeability and quantum authenticated encryption in [AGM18]. These are just some of the security games one can imagine — in the classical, symmetric-key setting, [KY06] analyzes 18 different security notions. A natural question is then to ask which of these games are the relevant ones, for which ones is it both necessary and sufficient that an adversary cannot win them. And the general answer is: we do not know.

Through such cryptographic protocols one wishes to prevent an adversary from learning some part of a message or modifying a message undetected. But it is generally unclear how such game-based security definitions relate to these operational notions — we refer to [MRT12] for a more in-depth critique of game-based security. Instead, one should directly define security *operationally*.[1] In this work we follow the constructive paradigm of [MR11, Mau12, MR16], and define a protocol to be secure if it constructs a channel with the desired properties, e.g., only leaks the message size or only allows the adversary to block the message, but not change it or insert new messages.

Composable security. A second drawback of the definitions proposed so far in the literature for computational security of quantum message transmission [BJ15, ABF+16, AGM18] is that they are not (proven to be) *composable*. A long history of work on composable security has shown that analyzing a protocol in an isolated

---

[1]Note that once a game-based definition has been proven to capture operational notions such as confidentiality or authenticity (e.g., via a reduction), then the game-based criterion may become a benchmark for designing schemes with the desired security; see the discussion in Section 1.6.

setting does not imply that it is actually secure when one considers the environment in which it is used. When performing such a composable security analysis, one sometimes finds that the definitions used are inappropriate but the protocols are actually secure like for quantum key distribution [Ren05, BHL$^+$05, KRBM07], that the definitions are still secure (up to a loss of security parameter) like for delegated quantum computation [DFPR14], or that not only the definitions but also the protocols are insecure like in relativistic and bounded storage bit commitment and (biased) coin tossing [VPdR17].[2] It is thus necessary for a protocol to be proven to satisfy a composable security definition before it may be considered (provably) secure and safely used in an arbitrary environment.

Finite security. A third problem with the aforementioned security definitions is that they are all *asymptotic*. This means that the protocols have a security parameter $k \in \mathbb{N}$ — formally, one considers a sequence of protocols $\{\Pi_k\}_{k \in \mathbb{N}}$ — and security is defined in the limit when $k \to \infty$. An implementation of a protocol will however always be finite, e.g., the honest players choose a specific parameter k_0 which they consider to be sufficient and run Π_{k_0}. A security proof for $k \to \infty$ does not tell us anything about security for any specific parameter k_0 and thus does not tell us anything about the security of Π_{k_0}, which is run by the honest players. To resolve this issue, some works consider what is called *concrete security* [BDJR97], i.e., instead of hiding parameters in O-notation, security bounds and reductions are given explicitly. This is a first step at obtaining finite security, but it still considers the security of a sequence $\{\Pi_k\}_{k \in \mathbb{N}}$ instead of security of the individual elements Π_{k_0} in this sequence. For example, one still considers adversaries that are polynomial in k, simulators that must be efficient in k, and errors that are negligible in k. But the security definition of some Π_{k_0} should not depend on any other elements in the sequence, on how the sequence is defined or whether it is defined at all. Hence notions such as poly-time, efficiency, or negligibility should not be part of a security definition for some specific Π_{k_0}. We call the security paradigm that analyzes individual elements Π_{k_0} *finite security*, and show in this work how to define it for computational security of quantum message transmission.

1.2 Overview of Results

Our contributions are threefold. We first provide definitions for encryption and authentication of quantum messages that satisfy the desideratum expressed above. In particular, we show how to define finite security in the computational case. In Section 1.3 below we explain the intuition behind this security paradigm.

---

[2]Note that a negative result in a composable framework only proves that a protocol does not construct the desired ideal functionality. This does not exclude that the protocol may construct some other ideal functionality or may be secure given some additional set-up assumptions.

We then show that (slightly modified) protocols from the literature [ABF$^+$16, AGM18] satisfy these definitions. These protocols use the quantum one-time pad and quantum information-theoretic authentication as subroutine [BCG$^+$02, Por17], but run them with keys that are only computationally secure to encrypt multiple messages. We explain the constructions and what is achieved in more detail in Section 1.4.

Now that we have security definitions that satisfy our desideratum, we revisit some game-based definitions from the literature, and compare them to our own notions of security. An overview of these results is given in Section 1.5.

1.3   Finite Computational Security

In traditional asymptotic security, a cryptographic protocol is parameterized by a single value $k \in \mathbb{N}$ — any other parameters must be expressed as a function of k — and one studies a sequence of objects $\{\Pi_k\}_{k \in \mathbb{N}}$. In composable security, one uses this to define a parameterized real world $\mathbb{R} = \{\mathsf{R}_k\}_{k \in \mathbb{N}}$ and ideal world $\$ = \{\mathsf{S}_k\}_{k \in \mathbb{N}}$, and argues that no polynomial distinguisher $\mathbb{D} = \{\mathsf{D}_k\}_{k \in \mathbb{N}}$ can distinguish one from the other with non-negligible advantage. At first glance the notions of polynomial distinguishers and negligible functions might seem essential, because an unbounded distinguisher can obviously distinguish the two, and without a notion of negligibility, how can one define what is a satisfactory bound on the distinguishability.

The latter problem is the simpler to address: instead of categorizing distinguishability as black or white (negligible or not), we give explicit bounds. The former issue is resolved by observing that we never actually prove that the real and ideal world are indistinguishable (except in the case of information-theoretic security), since in most cases that would amount to solving a problem such as $\mathsf{P} \neq \mathsf{NP}$. What one actually proves is a *reduction*, which is a finite statement, not an asymptotic one. More precisely, one proves that if D_k can distinguish R_k from S_k with advantage p_k, then some (explicit) D'_k can solve some problem W_k with probability p'_k — if one believes that W_k is asymptotically hard to solve, then this implies that $\mathbb{D}$ cannot distinguish $\mathbb{R}$ from $\$$.

A finite security statement stops after the reduction. We prove that for any k_0 and any D_{k_0},

$$d^{\mathsf{D}_{k_0}}(\mathsf{R}_{k_0}, \mathsf{S}_{k_0}) \leq f(D_{k_0}), \tag{1}$$

where $d^{\mathsf{D}_{k_0}}(\cdot, \cdot)$ denotes the advantage D_{k_0} has in distinguishing two given systems, and $f(\cdot)$ is some arbitrary function, e.g., the probability that D'_{k_0} (which is itself some function of D_{k_0}) can solve some problem W_{k_0}.

Equation 1 does not require systems to be part of a sequence with a single security parameter $k \in \mathbb{N}$. There may be no security parameter at all, or multiple parameters. Information-theoretic security corresponds to the special case where one can prove that $f(\mathsf{D}_{k_0})$ is small for all D_{k_0}.

1.4   Constructing Quantum Channels

As mentioned in Section 1.1, we use the Abstract and Constructive Cryptography (AC) framework of Maurer and Renner [MR11, Mau12, MR16] in this work. To define the security of a message transmission protocol, we need to first define the type of channel we wish to achieve — for simplicity, we always consider channels going from Alice to Bob.

The strongest channel we construct in this work is an ordered secure quantum channel, OSC, which allows Eve to decide which messages that Alice sent will be delivered to Bob and which ones get discarded. But it does not reveal any information about the messages (except their size and number) to Eve and guarantees that the delivered messages arrive in the same order in which they were sent. A somewhat weaker channel, a secure channel SC, also allows Eve to block or deliver each message, but additionally allows her to jumble their order of arrival at Bob's.

Our first result shows that a modified version of a protocol from [AGM18] constructs the strongest channel, OSC, from an insecure channel and a short key that is used to select a function from a pseudo-random family (PRF). Security holds for any distinguisher that cannot distinguish the output of the PRF from the output of a uniform function. We also show how one can construct OSC from SC by simply appending a counter to the messages.

The two channels described above are labeled "secure", because they are both confidential (Eve does not learn anything about the messages) and authentic (Eve cannot change or insert any messages). If we are willing to sacrifice authenticity, we can define weaker channels that allow Eve to modify or insert messages in specific ways. We define a non-malleable confidential channel, NMCC — which does not allow Eve to change a message sent by Alice, but does allow her to insert a message of her choice — and a Pauli-malleable channel, PMCC — which allows Eve to apply bit and phase flips to Alice's messages or insert a fully mixed state.

Our second construction modifies a protocol from [ABF+16] to construct PMCC from an insecure channel and a short key that is used to select a function from a pseudo-random family (PRF). Here too, security holds for any distinguisher that cannot distinguish the PRF from uniform.

1.5   Comparison to Game-Based Definitions

In the last part of this work, we relate existing game-based security definitions for quantum encryption with our new proposed security definitions phrased in constructive cryptography. More concretely, we focus on the notions of *quantum ciphertext indistinguishability under adaptive chosen-ciphertext attack* (QCCA2) and *quantum authenticated encryption* (QAE), both introduced in [AGM18].

We first note that encryption schemes are defined to be stateless in [BJ15, ABF+16, AGM18] and the proposed game-based definitions are tailored to such

schemes. The restricted class of encryption protocols analyzed can thus not construct ordered channels, because the players need to remember tags numbering the messages to be able to preserve this ordering. The strongest notion of encryption from these works, namely QAE, is thus closest to constructing a SC. In fact, we show that QAE is *strictly* stronger than constructing a SC: a scheme satisfying QAE constructs a SC, however there are (stateless) schemes constructing a SC that would be considered insecure by the QAE game. These schemes are obtained in the same way as the ones showing that classical IND-CCA2 is unnecessarily strong: one starts with a scheme satisfying QAE and appends a bit to the ciphertext, resulting in a new scheme that still constructs a SC, but is not QAE-secure. Our proof shows that QAE may be seen as constructing a SC with a *fixed* simulator that is hard-coded in the game. A composable security definition only requires the existence of a simulator, and the separation between the two notions is obtained by considering schemes that can be proven secure using a different simulator than the one hard-coded in the game.

For QCCA2, we first propose an alternative game-based security notion that captures the same intuition, but which we consider more natural than the one suggested in [AGM18]. In particular, its classical analogue is easily shown to be equivalent to a standard IND-CCA2 notion, whereas the notion put forth in [AGM18], when cast to a classical definition, incurs a concrete constant factor loss when compared to IND-CCA2, and requires a complicated proof of this fact. We then show that for a restricted class of protocols (which includes all the ones for which a security proof is given in previous work), our new game-based notion indeed implies that the protocol constructs a NMCC. The same separation holds here as well: QCCA2 definitions are unnecessarily strong, and exclude protocols that naturally construct a NMCC. Note that in the classical case, the IND-RCCA game [CKN03] that was developed to avoid the problems of IND-CCA2 has been shown to be exactly equivalent to constructing a classical non-malleable confidential channel in the case of large message spaces [CMT13].

1.6   Alternative Security Notions

Common security definitions often capture properties of (encryption) schemes, e.g., let M be a plaintext random variable, let C be the corresponding ciphertext, H is the entropy function, M' is the received plaintext, and accept is the event that the message is accepted by the receiver, then

$$H(M|C) = H(M) \qquad \text{and} \qquad \Pr\big[M \neq M' \text{ and accept}\big] \leq \varepsilon \qquad (2)$$

are simple notions of confidentiality and authenticity, respectively. But depending on how schemes satisfying these equations are used — e.g., encrypt-then-authen-

ticate or authenticate-then-encrypt—one gets drastically different results.[3] The equations in (2) may be regarded as crucial security properties of encryption schemes, but before schemes satisfying these may be safely used, one needs to consider the context and prove what is actually achieved by such constructs (in an operational sense).

The same applies to security definitions proposed for quantum key distribution. The accessible information[4] and the trace distance criterion[5] capture different properties of a secret key. If a scheme satisfying the former is used with an insecure quantum channel, then the resulting key could be insecure, but if the channel only allows the adversary to measure and store classical information, then the key has information-theoretic security [KRBM07, PR14]. A scheme satisfying the latter notion—the trace distance criterion—constructs a secure key even when the quantum channel used is completely insecure [Ren05, BHL+05, PR14]. Neither criterion is a satisfactory security definition on its own, they both require a further analysis to prove whether a protocol satisfying them does indeed distribute a secure key. But now that this has been done [BHL+05, PR14], the trace distance criterion has become a reference for what a quantum key distribution scheme must satisfy [SBPC+09, TL17].

Previous works on the computational security of quantum message transmission [BJ15, ABF+16, AGM18] as well as the new definition of QCCA2 proposed on this paper may be viewed in the same light. These game-based definitions capture properties of encryption schemes. But before a scheme satisfying these definitions may be safely used, one needs to analyze how the scheme is used and what is achieved by it. The constructive definitions introduced in this work and the reductions from the game-based definitions do exactly this. As a result of this, QAE or QCCA2 may be used as a benchmark for future schemes—though unlike the trace distance criterion, they are only sufficient criteria, not necessary ones.

1.7   Other Related Work

The desideratum expressed in Section 1.1 is the fruit of many different lines of research that go back to the late 90's. We give an incomplete overview of some of this work in this section.

Composable security was introduced independently by Pfitzmann and Waidner [PW00, PW01, BPW04, BPW07] and Canetti [Can01, CDPW07, Can13], who

---

[3]Encrypt-then-authenticate is always secure, but one can find examples of schemes satisfying (2) following the authenticate-then-encrypt paradigm that are insecure [BN00, Kra01, MT10].

[4]$I_{\mathrm{acc}}(K; E) := \max_\Gamma I(K; \Gamma(E))$, where ρ_{KE} is the joint state of the secret key K and the adversary's information E, and $\Gamma(E)$ is the random variable resulting from measuring the E system with a POVM Γ.

[5]$\|\rho_{KE} - \tau_K \otimes \rho_E\|$, where ρ_{KE} is the joint state of the secret key K and the adversary's information E and τ_K is a fully mixed state.

each defined their own framework, dubbed *reactive simulatability* and *universal composability* (UC), respectively. Unruh adapted UC to the quantum setting [Unr10], whereas Maurer and Renner's AC applies to any model of computation, classical or quantum [MR11]. Quantum UC may however not be used for finite security without substantial modifications, since it hard-codes asymptotic security in the framework: machines are defined by sequences of operators $\left\{\mathcal{E}^{(k)}\right\}_k$, where $k \in \mathbb{N}$ is a security parameter, and distinguishability between networks of machines is then defined asymptotically in k.[6]

Concrete security [BDJR97] addresses the issues of reductions and parameters being hidden in O-notation by requiring them to be explicit. Theses works consider distinguishing advantages (or game winning probabilities) as a function of the allowed complexity or running time of the distinguisher, and aim at proving as tight statements a possible. In such an approach, one would have to define a precise computational model. This, however, is avoided, meaning that any model in a certain class of meaningful models is considered equivalent. This unavoidably means that the security statements are asymptotic, at least with an unspecified linear or sublinear term. In contrast, the objects we consider, including distinguishers, are discrete systems and are directly composed as such, without need for considering a computational model for implementing the systems.

In the classical case, a model of discrete systems that may be used for finite security is *random systems* [Mau02,MPR07]. Generalizations to the quantum case have been proposed by Gutoski and Watrous [GW07, Gut12] — and called *quantum strategies* — by Chiribella, D'Ariano and Perinotti [CDP09] — called *quantum combs* — and by Hardy [Har11,Har12,Har15] — *operator tensors*. A model for discrete quantum systems that can additionally model time and superpositions of causal structures is the *causal boxes* framework [PMM+17].

None of the previous works on computational security of quantum message transmission satisfy any of the three criteria outlined in Section 1.1. These criteria are however standard by now for quantum key distribution [PR14, TL17]. In the classical case, they have also been used for computational security, e.g., [MRT12, CMT13].

1.8   Structure of this Paper

In Section 2 we introduce the elements needed from AC [MR11,Mau12,MR16], and from the discrete system model with which we instantiate AC, namely quantum

---

[6]The object about which ones makes a security statement is quite different in an asymptotic and a finite framework. In the former it is an infinite sequence of behaviors (e.g., a *machine* in UC), whereas in the later it is an element in such a sequence (the sequence itself is not necessarily well-defined). One thus composes different objects in the two models, and a composition theorem in one model does not immediately translate to a composition theorem in the other.

combs [CDP09]. This allows us to define the notion of a finite construction of a re-source (e.g., a secure channel) from another resource (e.g., an insecure channel and a key). In Section 3 we first define the channels and other resources needed in this work. Then we give protocols and prove that they construct various confidential and secure channels, as outlined in Section 1.4. Finally, in Section 4 we compare our security definitions to some game-based ones from the literature [AGM18] and prove the results described in Section 1.5.

2 Abstract & Constructive Cryptography

In this section we give a brief introduction to the Abstract and Constructive Cryptography (AC) framework. This framework views cryptography as a resource theory. Players may share certain resources — e.g., secret key, an authentic chan-nel, a public-key infrastructure, common reference strings, etc. — and use these to construct other resources — e.g., an authentic channel, a secure channel, se-cret key, a bit commitment resource, an idealization of a multipartite function, etc. A protocol is thus a map between resources. We give an overview of this in Section 2.1 and refer to [MR11, Mau12, PR14, MR16] for further reading.

To illustrate how this framework is used, we model known examples from the literature in Section 2.2 and Section 2.3, namely one-time authentication and en-cryption of quantum messages in the cases of both information-theoretic security and computational security, respectively. In Appendix A we define the (quantum) notation that we use throughout this paper.

The resource theory from Section 2.1 does not depend on the model of sys-tems considered — it may be instantiated with classical or quantum systems, syn-chronous or asynchronous communication, sequential or timed scheduling. In this work we consider asynchronous, sequential, quantum communication. This type of system has been studied by Gutoski and Watrous [GW07, Gut12], Chiribella, D'Ariano and Perinotti [CDP09], and Hardy [Har11, Har12, Har15], and we refer to it in the following using the term from [CDP09], namely *quantum combs*. Quan-tum combs are a generalization of *random systems* [Mau02, MPR07] to quantum information theory. In Section 2.4 we give an brief overview of quantum combs, and refer to the literature above for more details.

2.1 A Resource Theory

As mentioned at the beginning of this section, the AC framework views cryp-tography as a resource theory in which a protocol is a transformation between resources. More precisely, a protocol π uses some resource R (the *assumed* re-source) to construct some other resource S (the *constructed* resource) within ε, where ε may be thought of as the error of the construction. We denote this

$$\mathsf{R} \xrightarrow{\pi,\varepsilon} \mathsf{S}. \tag{3}$$

A formal definition of Eq. (3) is given below in Definition 1. Such a security statement is *composable*, because if π_1 constructs S from R within ε_1 and π_2 constructs T from S within ε_2, the composition of the two protocols, $\pi_2\pi_1$, constructs T from R within $\varepsilon_1 + \varepsilon_2$, i.e.,

$$\left.\begin{array}{l} \mathsf{R} \xrightarrow{\pi_1,\varepsilon_1} \mathsf{S} \\ \mathsf{S} \xrightarrow{\pi_2,\varepsilon_2} \mathsf{T} \end{array}\right\} \implies \mathsf{R} \xrightarrow{\pi_2\pi_1,\varepsilon_1+\varepsilon_2} \mathsf{T}. \tag{4}$$

Furthermore, if π constructs S from R within ε, then when some new resource U is accessible to the players, the construction still holds, albeit with a new error ε', since the computational power of U may be used by the dishonest parties to improve their attack, i.e.,

$$\mathsf{R} \xrightarrow{\pi,\varepsilon} \mathsf{S} \implies [\mathsf{R},\mathsf{U}] \xrightarrow{\pi,\varepsilon'} [\mathsf{S},\mathsf{U}]. \tag{5}$$

A proof of these two statements may be found in Appendix B.

In order to formalize Eq. (3), we need to define the different elements, namely resources R,S, a protocol π and the measure of error yielding ε. We do this briefly in the following, and refer to [MR11, Mau12, PR14, MR16] for more details.

Resources. In a setting with N parties, a *resource* is an interactive system with N interfaces — in the three party setting, the interfaces are usually denoted A, B, and E, for Alice, Bob, and Eve — allowing different parties to interact with their interface, i.e., provide inputs and receive outputs. In the following sections, resources are instantiated with quantum combs [CDP09], but the security definition is independent of the instantiation, so we defer discussing quantum combs to Section 2.4. The only property of resources that we need in this section is that many resources $\mathsf{R}_1,\ldots,\mathsf{R}_n$ taken together form a new resource, which we write $[\mathsf{R}_1,\ldots,\mathsf{R}_n]$. A party interacting at their interface of such a composed resource has simultaneous access to the corresponding interfaces of the different R_i, and may provide inputs or receive outputs at any of these.

An example of a system with multiple resources is given in Section 2.2, where we model the security of one-time authentication and encryption of quantum messages. The scheme, which is illustrated in Figure 1, involves four resources, KEY^μ, $\mathsf{IC}^{1,n}$, $\mathsf{QC}_A^{1,m,n}$, and $\mathsf{QC}_B^{1,m,n}$, drawn with square corners. In such a figure, we always put Alice on the left, Bob on the right, and Eve below. Each party has access to the inputs and outputs (illustrated by arrows) at their respective sides of the drawing (at their interfaces). The exact definition of these resources is provided in Section 3, after quantum combs have been introduced.

Converters. A *converter* may be thought of as local operations performed by some party. In Figure 1 there are two converters, $\pi_A^{\text{q-auth}}$ and $\pi_B^{\text{q-auth}}$, that correspond to Alice's and Bob's part of the encryption and authentication protocol.

Converters are always drawn with rounded corners. Each converter is associated to one interface, written as subscript, which denotes the party applying the converter. A protocol is then a tuple of converters, one for each honest party, e.g., $\pi_{AB}^{\text{q-auth}} = (\pi_A^{\text{q-auth}}, \pi_B^{\text{q-auth}})$.

Formally, a converter is defined as a function mapping a resource to another resource. Composition of converters is defined as the composition of the corresponding functions, and we usually write $\pi'\pi$ instead of $\pi' \circ \pi$. Furthermore, converters acting at different interfaces always commute, i.e., $\pi_A\pi_B = \pi_B\pi_A = \pi_{AB}$. The system drawn in Figure 1 is thus a resource given by

$$\mathsf{R} = \pi_{AB}^{\text{q-auth}}\left[\mathsf{KEY}^\mu, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\right].$$

Remark 1 (Explicit memory and computational requirements). In the spirit of making explicit statements — as opposed to hiding parameters in O-notation or poly-time statements — in the following we instantiate converters with systems that are memory-less and incapable of performing any operation on their inputs, i.e., they only forward messages between different resources and their outside interface. This forces any memory and computation capabilities of parties to be explicitly modeled as resources, e.g., the "quantum computer" resources $\mathsf{QC}_A^{1,m,n}$ and $\mathsf{QC}_B^{1,m,n}$ in Figure 1, which are required for performing the encryption and decryption operations. We note that one could equivalently "absorb" $\mathsf{QC}_A^{1,m,n}$ into $\pi_A^{\text{q-auth}}$ and $\mathsf{QC}_B^{1,m,n}$ into $\pi_B^{\text{q-auth}}$, which would result in exactly the same security statement, but not have the computational requirements spelled out.

Pseudo-metric. The final component needed before we can formalize Eq. (3) is a pseudo-metric,[7] which is used to define the error ε. We do this in the standard way by defining a *distinguisher* D to be a system that interacts with a resource, and outputs a bit. Let $\mathsf{D}[\mathsf{R}]$ be the random variable corresponding to the distinguisher's output when interacting with R. Then the functions

$$\Delta^{\mathsf{D}}(\mathsf{R}, \mathsf{S}) \coloneqq |\Pr[\mathsf{D}[\mathsf{R}] = 0] - \Pr[\mathsf{D}[\mathsf{S}] = 0]|$$

and

$$d^{\mathcal{D}}(\mathsf{R}, \mathsf{S}) \coloneqq \sup_{\mathsf{D} \in \mathcal{D}} \Delta^{\mathsf{D}}(\mathsf{R}, \mathsf{S})$$

are pseudo-metrics for any set of distinguishers $\mathcal{D}$. We define the error of a construction using one particular set $\mathcal{D}$, namely the set of distinguishers obtained from some distinguisher D by adding or removing converters between D and the

---

[7]A pseudo-metric $d(\cdot, \cdot)$ is a function which is non-negative, symmetric, satisfies the triangle inequality, and for any R, $d(\mathsf{R}, \mathsf{R}) = 0$. If additionally $d(\mathsf{R}, \mathsf{S}) = 0 \implies \mathsf{R} = \mathsf{S}$, then $d(\cdot, \cdot)$ is a metric.

measured resources. As stated in Remark 1, converters have no memory or computational power, so this results in a class of "equivalent" distinguishers. Thus, for any distinguisher D, we define the class

$$\mathcal{B}(\mathsf{D}) \coloneqq \left\{ \mathsf{D}' \middle| \exists \alpha \text{ such that } \mathsf{D}\alpha = \mathsf{D}' \text{ or } \mathsf{D}'\alpha = \mathsf{D} \right\}, \tag{6}$$

where $\Delta^{\mathsf{D}\alpha}(\mathsf{R}, \mathsf{S}) = \Delta^{\mathsf{D}}(\alpha\mathsf{R}, \alpha\mathsf{S})$. Abusing somewhat notation, we often write D instead of $\mathcal{B}(\mathsf{D})$. In the following, $d^{\mathsf{D}}(\cdot, \cdot)$ always refers to the pseudo-metric using the class of distinguishers generated from D as in Eq. (6).

Cryptographic Security. We now formalize the notion of (secure) resource construction in the three party setting, with honest Alice and Bob and dishonest Eve.

Definition 1 (Cryptographic security [MR11]). *Let ε be a function from distinguishers to real numbers. We say that a protocol $\pi_{AB} = (\pi_A, \pi_B)$ constructs a resource S from a resource R within ε if there exists a converter sim_E (called a simulator) such that for all D,*

$$d^{\mathsf{D}}(\pi_{AB}\mathsf{R}, \mathsf{sim}_E\mathsf{S}) \leq \varepsilon(\mathsf{D}).$$

If this holds, then we write

$$\mathsf{R} \xrightarrow{\pi, \varepsilon} \mathsf{S}.$$

When the resources R, S are clear from the context, we say that π is ε-secure.

$\pi_{AB}\mathsf{R}$ is often referred to as the *real* system, and $\mathsf{sim}_E\mathsf{S}$ as the *ideal* one. We emphasis that an ideal (or *constructed*) resource S will be used as the real (or *assumed*) resource in the next construction, so the terms *real* and *ideal* are relative.

Remark 2 (Efficiency & negligibility). Note that Definition 1 does not contain any notion of efficiency such as poly-time, nor does it mention that the error must be negligible. This is because concepts like efficiency and negligibility are only defined *asymptotically*. As explained in Section 1.3, we define *finite* security in this work. In this setting, *efficient* and *negligible* are ill-defined, and cannot be used — nor are they needed. Asymptotic security statements may be recovered by considering sequences of finite security statements, and taking the limit. This is further explained in Section 2.3.

2.2 Finite Information-Theoretic Security of One-Time Quantum Message Authentication and Encryption

To illustrate Definition 1 we model the security of one-time encryption and authentication of quantum messages — taken from [Por17] — which will be used as a
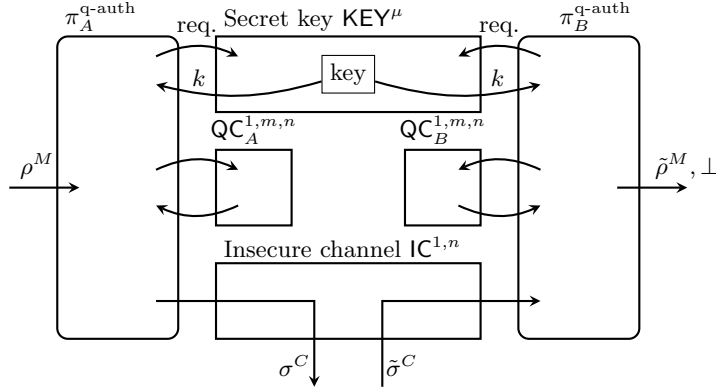
Fig. 1. The real system for quantum authentication consists of Alice's and Bob's parts of the protocol, $\pi_A^{\text{q-auth}}$ and $\pi_B^{\text{q-auth}}$, and the following four resources: a shared secret key KEY^μ, a (one-time use) insecure quantum channel $\mathsf{IC}^{1,n}$, and Alice's and Bob's local (one-time use) quantum computers $\mathsf{QC}_A^{1,m,n}$ and $\mathsf{QC}_B^{1,m,n}$. Upon receiving a message ρ^M at its outer interface, $\pi_A^{\text{q-auth}}$ stores it in $\mathsf{QC}_A^{1,m,n}$, then requests a key k from KEY^μ that is passed on to $\mathsf{QC}_A^{1,m,n}$, which performs the encryption. Finally the ciphertext σ^C received from $\mathsf{QC}_A^{1,m,n}$ is input to the channel $\mathsf{IC}^{1,n}$. Upon receiving a ciphertext $\tilde{\sigma}^C$ from the channel $\mathsf{IC}^{1,n}$, $\pi_B^{\text{q-auth}}$ stores it in $\mathsf{QC}_B^{1,m,n}$, then requests a key k from KEY^μ that is passed on to $\mathsf{QC}_B^{1,m,n}$, which performs the decryption. Finally, the result of this decryption—either the message $\tilde{\rho}^M$ or an error message $\bot$—is output at the outer interface of $\pi_B^{\text{q-auth}}$.

subroutine in Section 3. In this scheme, Alice wishes to send a quantum message to Bob in such a way that an eavesdropper, Eve, can neither read it nor change it. To do this, they share a uniform secret key, unknown to Eve, and an insecure channel, which allows Eve to intercept the message from Alice and send one of her own to Bob.[8] These two resources are denoted KEY^μ and $\mathsf{IC}^{1,n}$, and are illustrated in Figure 1. μ is the length of the secret key, the 1 as superscript of $\mathsf{IC}^{1,n}$ denotes that the channel is used (at most) once and n is the size (in qubits) of the message that can be transmitted. Formal definitions of these are provided in Section 3.2. Two more resources are needed for Alice and Bob to run their protocol, namely devices that can perform the encryption and decryption operations. These are denoted $\mathsf{QC}_A^{1,m,n}$ and $\mathsf{QC}_B^{1,m,n}$—the superscript 1 specifies that they can each perform one computation, m and n specify the size of the plaintext and ciphertext, i.e., a message of m qubits is encrypted into a ciphertext of n qubits. Alice's part of the protocol, $\pi_A^{\text{q-auth}}$, requests $\mathsf{QC}_A^{1,m,n}$ to perform the encryption and inputs the resulting ciphertext to the channel $\mathsf{IC}^{1,n}$. Bob's part of the protocol, $\pi_B^{1,m,n}$, uses $\mathsf{QC}_B^{1,m,n}$ to perform the decryption, and outputs the result. This is described in more detail in the caption of Figure 1.

---

[8] Eve does not have to wait for Alice to use the insecure channel to send her own message to Bob. She may first send him a chosen ciphertext, and only later intercept the ciphertext generated by Alice.

Fig. 2. The ideal quantum authentication system consists of a (one-time use) secure channel $\mathsf{SC}^{1,m}$, Eve's quantum computer $\mathsf{QC}_E^{2,m,n}$ (that may perform one encryption and one decryption), and the simulator $\sigma_E^{\text{q-auth}}$. Typically, upon receiving a notification from $\mathsf{SC}^{1,m}$ that Alice sent a message, $\mathsf{sim}_E^{\text{q-auth}}$ will ask $\mathsf{QC}_E^{2,m,n}$ to generate a ciphertext σ^C, which it then outputs at Eve's interface. Upon receiving a ciphertext $\tilde{\sigma}^C$ at its outer interface, it will ask $\mathsf{QC}_E^{2,m,n}$ to check its validity, and forward the result to $\mathsf{SC}^{1,m}$, which then either releases Alice's message ρ^M or outputs an error $\perp$ — if $\mathsf{sim}_E^{\text{q-auth}}$ receives a ciphertext $\tilde{\sigma}^C$ before any message ρ^M is input at Alice's interface, then the ciphertext is declared invalid and $\mathsf{SC}^{1,m}$ always outputs $\perp$.

We now need to design the ideal system. The goal of this protocol is to construct a secure channel, i.e., one which does not leak any information about the message to Eve — except the message length — and does not allow her to change the message either, nor insert one of her own. In the real world, Eve may either prevent any ciphertext from reaching Bob or jumble the ciphertext resulting in Bob receiving garbage (and outputting an error), so this must also be reflected in the ideal world. Thus, the ideal resource constructed — the secure channel $\mathsf{SC}^{1,m}$ illustrated in Figure 2 — notifies Eve when a message is input at Alice's interface (denoted by the dashed arrow),[9] and waits for a bit at Eve's interface that tells it whether to output the original message at Bob's interface or an error message $\perp$.[10] The superscript 1 specifies that this channel may be used once and m denotes the size of the message it transmits.

If such a protocol is used as a subroutine in a larger context, Eve could use the computational power of Alice and Bob to her advantage, e.g., if she needs the encryption or decryption operations to be applied to some quantum state, she can provide this state to the honest players and intercept their output. Such a construction thus provides some computation power to Eve, namely, it also con-

---

[9]Since the construction is parameterized by the message length m, there is no need to leak this information at Eve's interface. In a construction where m is unknown to Eve, a secure channel may additionally leak (an upper bound on) the message size to Eve.

[10]If Eve does not provide this bit, the channel does not output anything.

structs a resource $\mathsf{QC}_E^{2,m,n}$ which can perform one encryption and one decryption for a randomly chosen key.[11,12]

The security definition, Definition 1, requires there to exist a simulator such that the real and ideal worlds are indistinguishable. The exact simulator $\mathsf{sim}_E^{\text{q-auth}}$ will depend on the protocol analyzed, but — as described in more detail in the caption of Figure 2 — it will typically ask $\mathsf{QC}_E^{2,m,n}$ to generate a ciphertext to simulate that of Alice, then ask $\mathsf{QC}_E^{2,m,n}$ to perform a decryption to check the validity of the ciphertext received from Eve. The result of this decryption will decide whether Alice's message is released to Bob or not.

For a specific protocol $\pi_{AB}^{\text{q-auth}}$, a security proof in the information-theoretic setting consists in showing that this is secure for all distinguishers, i.e., one must find a $\mathsf{sim}_E^{\text{q-auth}}$ and some *constant function* ε such that the real and ideal systems (Figure 1 and 2) are ε-close, e.g., Lemma 1 here below.

Lemma 1. *[Por17] Let $\pi_{AB}^{\text{q-auth}}$ be any member of a family of protocols that encrypt the message using (weak) purity testing codes [BCG+02, Por17] from a set $\mathcal{C}$ of size $\log|\mathcal{C}| = \nu$ with error $\varepsilon \in \mathbb{R}$. Then there exists a $\mathsf{sim}_E^{\text{q-auth}}$ such that for any D,*

$$d^{\mathsf{D}}\left(\pi_{AB}^{\text{q-auth}}\Big[\mathsf{KEY}^{\nu+m+n}, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\Big], \mathsf{sim}_E^{\text{q-auth}}\Big[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n}\Big]\right)$$
$$\leq \max\{2^{m-n}, \varepsilon\},$$

i.e.,

$$\Big[\mathsf{KEY}^{\nu+2m+n}, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\Big] \xrightarrow{\pi_{AB}^{\text{q-auth}}, \max\{2^{m-n}, \varepsilon\}} \Big[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n}\Big].$$

Note that since we only consider constant functions ε in information-theoretic security, we write ε both for the function and the value $\varepsilon(\mathsf{D}) \in \mathbb{R}$.

Plugging in a specific instantiation of a (weak) purity testing code with $\nu = 3n$ and $\varepsilon = 2^{m-n}$ — the unitary 2-design construction [Por17] — one then obtains the following.

Corollary 1. *[Por17] Let $\pi_{AB}^{\text{q-auth}}$ be the unitary 2-design construction, then*

$$\Big[\mathsf{KEY}^{m+4n}, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\Big] \xrightarrow{\pi_{AB}^{\text{q-auth}}, 2^{m-n}} \Big[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n}\Big].$$

---

[11] For some protocols this may be providing Eve with unnecessary power, e.g., if the ciphertext looks like a full mixed state, it may be sufficient for $\mathsf{QC}_E^{2,m,n}$ to generate a purification of such a state and not need the ability to perform an encryption.

[12] In an asymptotic setting one would not care about this, since the protocol is efficient this would vanish in some poly-time statement. But in a finite setting where we keep track of all computation, one should model this explicitly. See also Remark 1.

Fig. 3. The real system for quantum authentication with a PRG. It is identical to Figure 1, except for the uniform key resource KEY^μ which has been replaced by a pseudo-random key resource $\mathsf{PRG}^{r,\mu}$ which produces a key of length μ from a uniform seed of length r. The system within the dashed line is labeled C, and is relevant in the reduction.

One may easily obtain an asymptotic security statement from Corollary 1 by taking a sequence of constructions parameterized by, e.g., $r = n - m$, and taking the limit as $r \to \infty$.

2.3   Finite Computational Security of One-Time Quantum Message Authentication and Encryption

In Section 2.2 we gave an example of a construction that has *information-the-oretic* security: the distance between the real and ideal systems is bounded for every distinguisher, i.e., ε is a constant function. If one considers *computational* security, then one is not interested in security in all contexts, but only when the distinguisher cannot solve problems considered to be "hard". A security proof is then a reduction to one of these hard problems. In the case of finite security we consider reductions to finite problems.

To illustrate this we will model a computational version of the quantum authentication and encryption protocol from Section 2.2. In fact, we will analyze exactly the same protocol, but just replace the uniform key resource KEY^μ with pseudo-random key resource $\mathsf{PRG}^{r,\mu}$, where r is the length of the (uniform) seed of the pseudo-random generator (PRG)— assumed to be hard-coded in the PRG— and μ is the length of the key it produces. The real world now looks exactly like Figure 1, except for the swap of the key for a PRG, which we have drawn in Figure 3.

The ideal world is identical to Figure 2 as our goal is still to construct the same ideal channel resource $\mathsf{SC}^{1,m}$. What changes is the error function ε which

will be small for some distinguishers and large for others. More precisely, we show that if D can distinguish the real from the ideal systems, then there exists an (explicit) distinguisher D' that can distinguish $\mathsf{PRG}^{r,\mu}$ from KEY^{μ}.

Lemma 2. *Let* $\pi_{AB}^{\text{q-auth}}$, $\mathsf{sim}_E^{\text{q-auth}}$ *and* ε *be such that for any* D,

$$d^{\mathsf{D}}\left(\pi_{AB}^{\text{q-auth}}\left[\mathsf{KEY}^{\mu}, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\right], \mathsf{sim}_E^{\text{q-auth}}\left[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n}\right]\right) \leq \varepsilon(\mathsf{D}).$$

Then for any D *we have*

$$d^{\mathsf{D}}\left(\pi_{AB}^{\text{q-auth}}\left[\mathsf{PRG}^{r,\mu}, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\right], \mathsf{sim}_E^{\text{q-auth}}\left[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n}\right]\right)$$
$$\leq d^{\mathsf{DC}}(\mathsf{PRG}^{r,\mu}, \mathsf{KEY}^{\mu}) + \varepsilon(\mathsf{D}), \quad (7)$$

where C *is the system drawn in dashed lines in* Figure 3, *and* DC *is a distinguisher obtained by composing* D *and* C *in the obvious way.*

Proof. Follows from the triangle inequality and $d^{\mathsf{D}}(\mathsf{CR}, \mathsf{CS}) \leq d^{\mathsf{DC}}(R, S)$.   □

Remark 3. The security statement in Eq. (7) is a *reduction*. It states that if it is hard to distinguish $\mathsf{PRG}^{r,\mu}$ from KEY^{μ}, then the scheme must be secure. Note that this is a *finite* reduction. We do not need to care whether $\mathsf{PRG}^{r,\mu}$ and KEY^{μ} are asymptotically indistinguishable,[13] but whether the finite instantiation for some fixed r and μ is indistinguishable — which is the relevant statement for an implementation. Unlike the asymptotic case, where one does not need to define the reduction system C or error ε precisely but just make a statement about their limit, here, the exact reduction C and parameter ε are crucial for the statement to be complete.

Suppose now that one has a bound ε' on the distinguishability of the PRG from a uniform key. Then one may plug this into Lemma 2 to get a (direct) security statement for the construction.[14]

Corollary 2. *Let* ε' *be a function such that for all* D, $d^{\mathsf{D}}(\mathsf{PRG}^{r,\mu}, \mathsf{KEY}^{\mu}) \leq \varepsilon'(\mathsf{D})$. *Then*

$$\left[\mathsf{PRG}^{r,\mu}, \mathsf{IC}^{1,n}, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n}\right] \xrightarrow{\pi_{AB}^{\text{q-auth}}, \varepsilon(\cdot) + \varepsilon'(\cdot\mathsf{C})} \left[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n}\right], \quad (8)$$

where $\varepsilon'(\cdot\mathsf{C})$ *is the function* $\mathsf{D} \mapsto \varepsilon'(\mathsf{DC})$.

---

[13]Asymptotic indistinguishability means that one sets $\mu = p(r)$ for some polynomial p and takes the limit as $r \to \infty$.

[14]Corollary 2 is a special case of the composition theorem: security of the encryption scheme with a PRG follows the security of the PRG and the security of the encryption scheme.

Asymptotic security. Eqs. (7) and (8) are finite security statements for the protocol $\pi_{AB}^{\text{q-auth}}$. Asymptotic statements may be obtained as a corollary if one takes sequences of finite statements and takes the limit. The (generic) construction presented so far has multiple parameters, namely $\varepsilon, m, n, r, \mu$. To define a sequence and take the limit, one has to simplify this. We do so by plugging in specific constructions. Suppose that we have a PRG with $\mu = p(r)$ for some polynomial p, and we take the unitary 2-design construction from Corollary 1. Then Eq. (7) becomes

$$d^{\mathsf{D}^{m,r}}\left(\pi_{AB}^{\text{q-auth}}\mathsf{R}^{m,r}, \mathsf{sim}_E^{\text{q-auth}}\mathsf{S}^{m,r}\right) \leq d^{\mathsf{D}^{m,r}\mathsf{C}^{m,r}}\left(\mathsf{PRG}^{r,p(r)}, \mathsf{KEY}^{p(r)}\right) + 2^{m-p(r)},$$

where we have set $\mathsf{R}^{m,r} := \left[\mathsf{PRG}^{r,p(r)}, \mathsf{IC}^{1,p(r)}, \mathsf{QC}_A^{1,m,p(r)}, \mathsf{QC}_B^{1,m,p(r)}\right]$ and $\mathsf{S}^{m,r} := \left[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,p(r)}\right]$, and parameterized D and C by m and r for consistency. Let us view m as fixed and take sequences with $r \in \mathbb{N}$.[15]

Since $\mathsf{C}^{m,r}$ is poly-time — $\mathsf{C}^{m,r}$ basically runs the protocol, which is efficient — the error $2^{m-p(r)}$ is negligible and we believe that $d^{\tilde{\mathsf{D}}^{m,r}}\left(\mathsf{PRG}^{r,p(r)}, \mathsf{KEY}^{p(r)}\right)$ is negligible for any poly-time $\tilde{\mathsf{D}}^{m,r}$ (in particular for $\tilde{\mathsf{D}}^{m,r} = \mathsf{D}^{m,r}\mathsf{C}^{m,r}$), then we can recover the standard asymptotic statement from Eq. (2.3). More precisely, it then follows that for any poly-time $\mathsf{D}^{m,r}$,

$$\Delta^{\mathsf{D}^{m,r}}\left(\pi_{AB}^{\text{q-auth}}\mathsf{R}^{m,r}, \mathsf{sim}_E^{\text{q-auth}}\mathsf{S}^{m,r}\right) \leq \varepsilon_{m,r} \tag{9}$$

for some negligible $\varepsilon_{m,r}$.

2.4   Instantiating AC

We consider *sequential scheduling* in this work, i.e., a system receives a message, then produces an output, receives another input, generates another output, etc. Here, the messages sent and received may be quantum, but the party to whom a message is sent is given by classical information.[16]

Quantum Combs. Let $\mathcal{H}_A$ be the input Hilbert space of a system R, $\mathcal{H}_B$ be the output Hilbert space and $\mathcal{H}_M$ be some internal memory. R is fully defined by a completely positive, trace-preserving (CPTP) map

$$\mathcal{E} : \mathcal{L}(\mathcal{H}_{AM}) \to \mathcal{L}(\mathcal{H}_{BM}), \tag{10}$$

---

[15] One may alternatively set $m = q(r)$ for some appropriate polynomial q.

[16] An alternative model of systems that allows quantum scheduling — messages can be in a superposition of sent and not sent, or a superposition of sent to player A and sent to player B — is the Causal Boxes model [PMM$^+$17], which can additionally capture relativistic causal constraints [VPdR17]. For the current work however, (classical) sequential scheduling is sufficient, so we use the simpler quantum combs [CDP09].

which specifies what output is produced and how the internal memory is updated as a function of the input and current internal memory. Each time an input $\rho \in \mathcal{L}(\mathcal{H}_A)$ is received (which may be part of a larger entangled system), the map $\mathcal{E}$ is applied, and the output $\sigma \in \mathcal{L}(\mathcal{H}_B)$ is sent to the appropriate party.

This is however a redundant description of a system, since different maps $\mathcal{E}$ may produce exactly the same output behavior. The works on quantum combs [GW07, Gut12, CDP09, Har11, Har12, Har15] define such a system for n inputs as a CPTP map

$$\Phi^n : \mathcal{L}(\mathcal{H}_A^{\otimes n}) \to \mathcal{L}(\mathcal{H}_B^{\otimes n}) \tag{11}$$

subject to a causality constraint that enforces that an output in position i can only depend on inputs in positions $\leq i$. Such a system may have various descriptions, e.g., as the (unique) Choi matrix corresponding to the map Φ^n, as a map $\mathcal{E}$ as in Eq. (10), or as pseudo-code that describes the behavior of the system.

In this work we often use pseudo-code to describe resources. Though each time it corresponds to a specific quantum comb that is uniquely defined by a map as in Eq. (11).

Resources as Combs. As stated at the beginning of Section 2.4, in our model the sender and receiver of messages are given by classical information. Formally, this means the input and output Hilbert space of a resource has the form $\mathcal{H}_A = \bigoplus_i \mathcal{H}_{A_i}$, and the first operation of a resource is a projection on the different subspaces A_i to determine this classical information. For example, the different i correspond to the different interfaces of a resource or different ports at an interface.

When two resources R and S with input (or output) spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ accessible in parallel, the resulting resource $T = [R, S]$ is a new quantum comb with input (respectively, output) space given by $\mathcal{H}_A \oplus \mathcal{H}_B$, and the initial measurement determines which sub-resource (R or S) receives and processes the input. Similarly, plugging a converter α into a resource R, results in a new resource $U = \alpha R$, whose corresponding quantum comb is computed from the comb of R and the pairs of ports connected by α.

More generally, the works on quantum combs [GW07, Gut12, CDP09, Har11, Har12, Har15] show how such objects may be composed to form networks — which are again objects of the same type, namely quantum combs — and how one defines a (distinguisher-based) pseudo-metric on combs. We refer to them for more details.

3 Constructing Quantum Cryptographic Channels

In Section 3.1 and Section 3.2 we formalize the resources used in our constructions. Then, starting from the insecure quantum channel IC, a shared secret key KEY and local pseudo random function PRF, we show how to construct (1) the ordered secure quantum channel OSC in Section 3.3 and (2) the Pauli-malleable

confidential quantum channel PMCC in Section 3.4. A construction of the ordered secure quantum channel OSC from one which is secure but not ordered (SC) is also presented in Appendix D.

3.1   Key Resources

A (shared) secret key resource corresponds to a system that provides a key k to the honest players, but nothing to the adversary.

Definition 2 (Symmetric (Classical) Key KEY). *The resource* KEY *is associated with a probability distribution P_K for (classical) key space $\mathcal{K}$. A key $k \in \mathcal{K}$ is drawn according to P_K and stored in the resource.*
 – **Interface A:** *On input* getKey, *k is output at interface A.*
 – **Interface B:** *On input* getKey, *k is output at interface B.*
 – **Interface E:** *Inactive.*

In the computational setting, instead of sharing a long key, players often share a short key which is used as seed in a local key expansion scheme. On such key expansion scheme which we use in this work is a so-called *pseudo random function*. It is essentially a family of functions which looks random.

Definition 3 (Pseudo Random Function $\mathsf{PRF}^{r,\nu,\mu}$). *The resource* $\mathsf{PRF}^{r,\nu,\mu}$ *is associated to a family of functions $\{f_k : \{0,1\}^\nu \to \{0,1\}^\mu | k \in \{0,1\}^r\}$ and has an internal variable* seed *of length r. The functions in the family have input length ν and output length μ. The resource is local to one party only. Let this party's interface be labeled X.*
 – **Interface X:**
   • *On input* seed(s), *set variable* seed *to s.*
   • *On input* input(x), *output $f_{\mathsf{seed}}(x)$ at interface X.*

The above definition of a PRF does not contain any criterion for what it means to "look random". This is defined in a second step as distinguishability from a uniform random function.

Definition 4 (Uniform Random Function $\mathsf{URF}^{\nu,\mu}$). *The resource* $\mathsf{URF}^{\nu,\mu}$ *picks a function f from all functions $\{0,1\}^\nu \to \{0,1\}^\mu$ uniformly at random.*
 – **Interface A:** *On input* input(x), *output $f(x)$ at interface A.*
 – **Interface B:** *On input* input(x), *output $f(x)$ at interface B.*
 – **Interface E:** *Inactive.*

Let π^{PRF} be the trivial protocol which uses a (short) shared key (from a KEY resource) and plugs it as seed in a PRF resource, and let $\varepsilon^{\mathsf{PRF}}(\mathsf{D})$ be the advantage the distinguisher D has in distinguishing such a construction from a URF, i.e., for all D

$$d^{\mathsf{D}}(\pi^{\mathsf{PRF}}[\mathsf{KEY}^r, \mathsf{PRF}_A^{r,\nu,\mu}, \mathsf{PRF}_B^{r,\nu,\mu}], \mathsf{URF}^{\nu,\mu}) \leq \epsilon^{\mathsf{PRF}}(\mathsf{D}),$$

where $d^{\mathsf{D}}(\cdot, \cdot)$ is the distinguisher pseudo-metric as defined in Section 2.1. In terms of AC construction, this means that

$$\left[\mathsf{KEY}^r, \mathsf{PRF}_A^{r,\nu,\mu}, \mathsf{PRF}_B^{r,\nu,\mu}\right] \xrightarrow{\pi^{\mathsf{PRF}}, \epsilon^{\mathsf{PRF}}} \mathsf{URF}^{\nu,\mu}. \tag{12}$$

Concrete constructions of PRFs proven secure in the presence of quantum adversaries may be found in [Zha12].

3.2 Channel resources

We consider three-party channels in this work: the sending party Alice has access to interface A, the receiving party Bob to interface B, and the adversary Eve to interface E. We model all our channels in the following way: upon an input at interface A, an output is generated at interface E, while upon an input at interface E, an output is generated at interface B. Moreover, we consider multi-message channels parameterized by ℓ, that is, Alice and Eve can provide at most ℓ inputs at their respective interfaces. These inputs can be entangled with each other. We model quantum channels, therefore inputs and outputs to and from the channels' interfaces are quantum systems. The channels are also parameterized by m, the size of each message in qubits.

In the following we introduce the formal description of the channels considered in this work by specifying the behavior they assume upon inputs at their A and E interfaces. First, we consider the weakest possible channel, that is, the *insecure* one, which gives full control to the adversary Eve. Eve receives all the message that Alice inputs to the channel. Bob receives all the messages that Eve inputs to the channel.

Definition 5 (Insecure Quantum Channel $\mathsf{IC}^{\ell,m}$).
  – **Interface A:** *On receiving an input system in some state ρ, perform an identity map and output the same system at interface E.*
  – **Interface E:** *On receiving an input system in some state ρ', perform an identity map and output the same system at interface B.*
Interface A and E will receive at most ℓ inputs and ignore the rest. The quantum systems input at interface A and E and output at interface B have length m in qubits.

Next, we enhance the insecure channel by providing some form of confidentiality on the states input by Alice. More precisely, we allow Eve to only get a notification that a new message has arrived in interface A, but still, Eve will retain the capability to *modify* each input ρ^{A_i} (held in register A_i).

Here, one may consider different ways in which Eve is allowed to modify the messages. The first channel we consider grants Eve the power to insert fully mixed states on the channel, as well as performing Pauli operators (bit flips and phase

flips) on Alice's message and decide when each message gets delivered. This is modeled by keeping registers A_i for each new input at interface A, and allowing Eve to input indices specifying which register should be modified and output at interface B. Along with the index, Eve also inputs a string of length $2m$, indicating on which qubits of the message to apply Pauli operators. If Eve wants a fully mixed state to be output at Bob's, she inputs $\perp$ at her interface and the channel generates the corresponding state.

Definition 6 (Pauli-Malleable Confidential Quantum Channel $\mathsf{PMCC}^{\ell,m}$).
The channel keeps registers $A_1, A_2, \ldots, A_\ell$, initially set to $\perp$.
  – **Interface A:** *Upon receiving the i-th input in some state ρ, this system is stored in register A_i, and* newMsg *is output at interface E.*
  – **Interface E:**
    • *On input $(j, k) \in [l] \times \{0, 1\}^{2m}$, output system in state $P_k \rho^{A_j} P_k$ at interface B, where ρ^{A_j} is the state of the system held in register A_j and P_k is the Pauli operator defined by the string k — see [Appendix A](#). If the tuple is invalid or ρ^{A_j} is $\perp$, the input is considered as $\perp$. After the output, the state in register A_j becomes $\perp$.*
    • *On input $\perp$, output a fully mixed stated $\frac{1}{2^m} I_{2^m}$ at interface B.*
Interface A and E will receive at most ℓ inputs and ignore the rest. The quantum systems input at interface A and output at interface B always have length m in qubits.

Another type of confidential channel we consider is obtained by removing Eve's capability to modify Alice's messages, while giving her the ability to *inject* any system (instead of only systems in the fully mixed state).

Definition 7 (Non-Malleable Confidential Quantum Channel $\mathsf{NMCC}^{\ell,m}$).
The channel keeps registers $A_1, A_2, \ldots, A_\ell$, initially set to $\perp$.
  – **Interface A:** *Upon receiving the i-th input in some state ρ, this system is stored in register A_i, and* newMsg *is output at interface E.*
  – **Interface E:**
    • *On receiving an input system in some state ρ', perform an identity map and output the same system at interface B.*
    • *On input index $j \in [\ell]$, output the system in state ρ^{A_j} held in register A_j at interface B. After the output, the state of register A_j becomes $\perp$.*
Interface A and E will receive at most ℓ inputs and ignore the rest. The quantum systems input at interface A and output at interface B always have length m in qubits.

The next property to consider is authenticity: recall that in the quantum setting, authenticity implies confidentiality, thus it does not make sense to consider a "non-confidential authentic channel", since a state cannot be cloned to be given

to both Bob and Eve. An authentic channel will automatically also be a confidential one [BCG+02]. Therefore, as a next channel we directly consider the *secure* one — by secure we mean both authentic and confidential. Eve only knows a new message has arrived but cannot read, modify, nor inject messages. Eve still has the power to block and reorder Alice's message.

Definition 8 (Secure Quantum Channel $\mathsf{SC}^{\ell,m}$). *The channel keeps registers* $A_1, A_2, \ldots, A_\ell$, *initially set to* $\perp$.
 - **Interface** A**:** *Upon receiving the i-th input in some state ρ, this system is stored in register A_i, and* newMsg *is output at interface E.*
 - **Interface** E**:** *On input index $j \in [\ell]$, output the system in state ρ^{A_j} held in register A_j at interface B. After the output, the state in register A_j becomes* $\perp$.

Interface A and E will receive at most ℓ inputs and ignore the rest. The quantum systems input at interface A and output at interface B always have length m in qubits.

Finally, we consider an even stronger version of the secure channel which preserves the *order* of the transmitted messages. In particular, the adversary now only retains the power to delete messages, but cannot change the order in which they are transmitted. This is enforced by replacing the capability to input indices by the ability of only inputting either send or skip.

Definition 9 (Ordered Secure Quantum Channel $\mathsf{OSC}^{\ell,m}$). *The channel keeps registers* $A_1, A_2, \ldots, A_\ell$, *initially set to* $\perp$.
 - **Interface** A**:** *Upon receiving the i-th input in some state ρ, this system is stored in register A_i, and* newMsg *is output at interface E.*
 - **Interface** E**:** *On i-th input* send *or* skip*: If the input is* send*, output the system in state ρ^{A_i} held in register A_i at interface B. If the input is* skip*, then output* $\perp$ *at interface B. After the output, the state in register A_i becomes* $\perp$.

Interface A and E will receive at most ℓ inputs and ignore the rest. The quantum systems input at interface A and output at interface B always have length m in qubits.

3.3   Constructing an Ordered Secure Quantum Channel

As stated in Lemma 1 from Section 2.2, there is a construction of one time secure quantum channel from one time insecure quantum channel resource and a uniform key resource within $\epsilon^{\text{q-auth}}$, i.e.

$$\left[\mathsf{IC}^{1,n}, \mathsf{KEY}^\mu, \mathsf{QC}_A^{1,m,n}, \mathsf{QC}_B^{1,m,n} \right] \xrightarrow{\pi_{AB}^{\text{q-auth}}, \epsilon^{\text{q-auth}}} \left[\mathsf{SC}^{1,m}, \mathsf{QC}_E^{2,m,n} \right].$$

Here, IC, SC and KEY are channel and key resources, as defined above. $\mathsf{QC}_{A/B/E}$ denote a resource that does quantum computation for Alice, Bob or Eve, and

---

| π_A π_B QC$_A$ QC$_B$ |

1. π_A: Alice inputs a message ρ^A and requests her computer to encrypt ρ^A.
2. QC$_A$: On the i-th input ρ^A, the computer requests (through π_A) $k_i = \mathsf{input}(i)$ from URF, computes ciphertext $\sigma^C = \mathsf{enc}_{k_i}^{\text{q-auth}}(\rho^A)$, appends index $|i\rangle\langle i|$ on the ciphertext and outputs $\psi^{CT} = \sigma^C \otimes |i\rangle\langle i|^T$ to Alice.
3. π_A: Alice sends ciphertext ψ^{CT} to Bob through insecure quantum channel IC.
4. π_B: Bob receives ciphertext $\tilde{\psi}^{\tilde{C}\tilde{T}}$ and requests his computer to decrypt $\tilde{\psi}^{\tilde{C}\tilde{T}}$.
5. QC$_B$: On the i-th input $\tilde{\psi}^{\tilde{C}\tilde{T}}$, the computer takes first n qubits as $\tilde{\sigma}^C$, measures last $\log \ell$ qubits and obtains the measurement result $\tilde{\imath}$. If $\tilde{\imath} = i$, the computer requests (through π_B) $k_i = \mathsf{input}(i)$ from resource URF, computes plaintext $\tilde{\rho} = \mathsf{dec}_{k_i}^{\text{q-auth}}(\tilde{\sigma})$. If it decrypts successfully, the computer outputs $\tilde{\rho}$ to Bob. If $\tilde{\imath} \neq i$ or it does not decrypt successfully, the computer outputs $\bot$ to Bob.
6. π_B: Bob outputs the decrypted message $\tilde{\rho}^B$.

Fig. 4. Converters and computing resources to construct $\mathsf{OSC}^{\ell,m}$ from $\mathsf{IC}^{\ell,n+\log \ell}$. $\mathsf{QC}_A^{\ell,m,n+\log \ell}$ and $\mathsf{QC}_B^{\ell,m,n+\log \ell}$ will be queried ℓ times. The plaintext has length m and the ciphertext has length $n + \log \ell$. $\mathsf{URF}^{\log \ell,\mu}$ has input length $\log \ell$ and output length μ.

allows them to perform encryption and decryption operations (we informally refer to such resources as *quantum computers* in the following). These appear in the construction statement since for finite security one makes all computational operations explicit — see Section 2 for more details.

We denote the encoding and decoding CPTP maps in this construction by $\mathsf{enc}^{\text{q-auth}} : \mathcal{K} \times \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_C)$ and $\mathsf{dec}^{\text{q-auth}} : \mathcal{K} \times \mathcal{L}(\mathcal{H}_{\tilde{C}}) \to \mathcal{L}(\mathcal{H}_B \oplus |\bot\rangle\langle\bot|)$. We also denote by $\mathcal{E}$ the CPTP map that always discards the state and replaces it with error state $|\bot\rangle\langle\bot|$. In this section, we build on top of these encoding and decoding maps to construct a multi-message ordered secure quantum channel from a multi-message insecure quantum channel, with a shared uniform random function resource $\mathsf{URF}^{\log \ell,\mu}$. The real system is drawn in Figure 5 and the components are described in Figure 4. The ideal system one wishes to build is depicted in Figure 6.

Theorem 1. *Let* $\pi_{AB} = (\pi_A, \pi_B), \mathsf{QC}_A^{\ell,m,n+\log \ell}, \mathsf{QC}_B^{\ell,m,n+\log \ell}$ *and* $\mathsf{URF}^{\log \ell,\mu}$ *denote converters and computing resources as described in Figure 4, corresponding to Alice and Bob both applying the following CPTP maps with increasing index i:*

$$\Lambda_i^{A \to CT}(\cdot) = \mathsf{enc}_{k_i}^{\text{q-auth}}(\cdot) \otimes |i\rangle\langle i|^T$$

$$\Lambda_i^{\tilde{C}\tilde{T} \to B}(\cdot) = \mathsf{dec}_{k_i}^{\text{q-auth}}\left((I^{\tilde{C}} \otimes \langle i|^{\tilde{T}})(\cdot)(I^{\tilde{C}} \otimes |i\rangle^{\tilde{T}}) \right) + \mathcal{E}\left(\bar{P}_i^{\tilde{T}}(\cdot)\bar{P}_i^{\tilde{T}} \right),$$

where $\bar{P}_i = I - |i\rangle\langle i|$, *and* k_i *is the output of* $\mathsf{URF}^{\log \ell,\mu}$ *with input i. Let* $\mathsf{QC}_E^{2\ell,m,n+\log \ell}$ *be the computing resource of Eve capable of doing ℓ encryption operations and ℓ decryption operations. Let* $\epsilon^{\text{q-auth}}$ *be the upper bound on the distinguishing advan-*

Fig. 5. The real system consisting of the shared resources $\mathsf{IC}^{\ell,n+\log\ell}$ and $\mathsf{URF}^{\log\ell,\mu}$, Alice and Bob's computing resources $\mathsf{QC}_A^{\ell,m,n+\log\ell}\mathsf{QC}_B^{\ell,m,n+\log\ell}$, and the protocol converters π_A and π_B.

Fig. 6. The ideal system consisting of $\mathsf{OSC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,n+\log\ell}$ and sim_E. $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ makes use of ℓ instances of $\mathsf{QC}^{\text{q-auth}}$ internally, while sim_E only receives and forwards messages and does no computation.

tage of the one time secure quantum channel construction. Then,

$$\left[\mathsf{IC}^{\ell,n+\log\ell}, \mathsf{URF}^{\log\ell,\mu}, \mathsf{QC}_A^{\ell,m,n+log\ell}, \mathsf{QC}_B^{\ell,m,n+log\ell}\right]$$

$$\xrightarrow{\pi_{AB},\ell\epsilon^{\text{q-auth}}} \left[\mathsf{OSC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,n+\log\ell}\right].$$

Proof. In order to prove the statement, we need to find a simulator sim_E and describe what Eve's quantum computer $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ does such that real system, as illustrated in Figure 5 and the ideal system, as illustrated in Figure 6 are indistinguishable within $\ell\epsilon^{\text{q-auth}}$, where $\epsilon^{\text{q-auth}}$ is the constant upper bound on the error of the one message authentication scheme.

The simulator sim_E works as following. On input newMsg from the ideal resource $\mathsf{OSC}^{\ell,m}$, it requests $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ to provide a quantum state ψ and outputs

ψ at interface E. On input $\tilde{\psi}$ at interface E, it requests $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ to provide send or skip signal. The signal is then forwarded to ideal channel $\mathsf{OSC}^{\ell,m}$.

Eve's computing resource $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ will use $\mathsf{QC}_E^{2,m,n}$ of the one time secure quantum channel construction as a subroutine. We refer to this subroutine computer resource as $\mathsf{QC}^{\text{q-auth}}$. $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ works as following,

- On the i-th input newMsg, the computer instantiates a new $\mathsf{QC}_i^{\text{q-auth}}$, sends newMsg to $\mathsf{QC}_i^{\text{q-auth}}$. After getting the ciphertext σ from $\mathsf{QC}_i^{\text{q-auth}}$, the computer appends index i to σ and output $\psi = \sigma \otimes |i\rangle\langle i|$ to sim_E. After output ψ, the computer updates internal counter nextIndex $= i$.
- On input $\tilde{\psi}$, the computer takes the first n qubits as ciphertext $\tilde{\sigma}$, measures the last $\log\ell$ qubits and obtains the measurement result $\tilde{i}$. If nextIndex $\neq \tilde{i}$, the computer outputs skip to sim_E. If nextIndex $= \tilde{i}$, the computer forwards ciphertext $\tilde{\sigma}$ to $\mathsf{QC}_{\tilde{i}}^{\text{q-auth}}$. If $\mathsf{QC}_{\tilde{i}}^{\text{q-auth}}$ outputs acc, the computer outputs send to sim_E. If $\mathsf{QC}_{\tilde{i}}^{\text{q-auth}}$ outputs rej, the computer outputs skip to sim_E.

We define $\mathsf{R}^\ell := \pi_{AB}\Big[\mathsf{IC}^{\ell,n+\log\ell}, \mathsf{URF}^{\log\ell,\mu}, \mathsf{QC}_A^{\ell,m,n+\log\ell}, \mathsf{QC}_B^{\ell,m,n+\log\ell}\Big]$ and $\mathsf{S}^\ell :=$ $\mathsf{sim}_E\Big[\mathsf{OSC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,n+\log\ell}\Big]$. Note that we can consider the channel of ℓ messages as ℓ different 1 message channels with an obvious converter α that directs the message according to its tag into the corresponding channel, i.e., $\mathsf{IC}^{\ell,n+\log\ell} \equiv \alpha\Big[\mathsf{IC}_1^{1,n}, \mathsf{IC}_2^{1,n}, \ldots, \mathsf{IC}_\ell^{1,n}\Big]$. Similarly $\mathsf{URF}^{\log\ell,\mu}$ can be consider as ℓ different KEY^μ resources and channel $\mathsf{OSC}^{\ell,m}$ and quantum computers $\mathsf{QC}_A^{\ell,m,n+\log\ell}$, $\mathsf{QC}_B^{\ell,m,n+\log\ell}$, $\mathsf{QC}_E^{2\ell,m,n+\log\ell}$ can all be considered as ℓ different 1 message resources with the same converter α. We further define $\mathsf{R}_i := \pi_{AB}^{\text{q-auth}}\Big[\mathsf{IC}_i^{1,n}, \mathsf{KEY}_i^\mu, \mathsf{QC}_{A_i}^{1,m,n}, \mathsf{QC}_{B_i}^{1,m,n}\Big]$ and $\mathsf{S}_i = \mathsf{sim}^{\text{q-auth}}\Big[\mathsf{OSC}_i^{1,m}, \mathsf{QC}_{E_i}^{2,m,n}\Big]$. We can see that $\mathsf{R}^\ell \equiv \alpha[\mathsf{R}_1, \mathsf{R}_2, \ldots, \mathsf{R}_\ell]$ and $\mathsf{S}^\ell \equiv \alpha[\mathsf{S}_1, \mathsf{S}_2, \ldots, \mathsf{S}_\ell]$ since for each message the protocol π_{AB} and sim_E works exactly the same as $\pi_{AB}^{\text{q-auth}}$ and $\mathsf{sim}^{\text{q-auth}}$ in the one time secure quantum channel construction. For any distinguisher D,

$$\Delta^{\mathsf{D}}\Big(\mathsf{R}^\ell, \mathsf{S}^\ell\Big) = \Delta^{\mathsf{D}\alpha}([\mathsf{R}_1, \mathsf{R}_2, \ldots, \mathsf{R}_\ell], [\mathsf{S}_1, \mathsf{S}_2, \ldots, \mathsf{S}_\ell])$$

$$\leq \sum_{i=1}^{\ell} \Delta^{\mathsf{D}\alpha}([\mathsf{S}_1, \ldots, \mathsf{S}_{i-1}, \mathsf{R}_i, \mathsf{R}_{i+1}, \ldots, \mathsf{R}_\ell],$$

$$[\mathsf{S}_1, \ldots, \mathsf{S}_{i-1}, \mathsf{S}_i, \mathsf{R}_{i+1}, \ldots, \mathsf{R}_\ell])$$

$$\leq \sum_{i=1}^{\ell} \Delta^{\mathsf{D}\alpha\mathsf{C}_i}(\mathsf{R}_i, \mathsf{S}_i)$$

$$\leq \sum_{i=1}^{\ell} \epsilon^{\text{q-auth}}(\mathsf{D}\alpha\mathsf{C}_i) \leq \ell\epsilon^{\text{q-auth}}.$$

This analysis follows from a standard hybrid argument. For a distinguisher D to distinguish in the multi-message case, the new distinguishers $\mathsf{D}\alpha\mathsf{C_i}$, attached by a converter α and $C_i = [\mathsf{S_1}, \ldots, \mathsf{S_{i-1}}, \cdot, \mathsf{R_{i+1}}, \ldots, \mathsf{R_\ell}]$, has to distinguish in one of the one message cases. The final inequality follows from the information-theoretic bound in the one message case, where we have used $\epsilon^{\text{q-auth}}$ both for the function and its upper bound. $\qquad\square$

Remark. Theorem 1 is meaningful only if the protocol is also *correct*, i.e., if the distinguisher always puts back the same ciphertext on the insecure channel in the right order, then Bob always successfully decrypts. This follows trivially from the correctness of the underlying quantum authentication protocol, so we omit a formal discussion of it.

Suppose now that one has a PRF resource and a bound ϵ^{PRF} satisfying Eq. (12), that is, indistinguishable from URF within ϵ^{PRF}, the following corollary follows trivially from the composition theorem Theorem 5 in Appendix B.

Corollary 3.

$$\left[\mathsf{IC}^{\ell, n + \log \ell}, \mathsf{KEY}^r, \mathsf{PRF}_A^{r, \log \ell, \mu}, \mathsf{PRF}_B^{r, \log \ell, \mu}, \mathsf{QC}_A^{\ell, m, n + log\ell}, \mathsf{QC}_B^{\ell, m, n + log\ell} \right]$$

$$\xrightarrow{\pi'_{AB}, \epsilon} \left[\mathsf{OSC}^{\ell, m}, \mathsf{QC}_E^{2\ell, m, n + \log \ell} \right],$$

where $\pi'_{AB} = (\pi_{AB}, \pi^{\mathsf{PRF}}), \epsilon(\mathsf{D}) = \epsilon^{\mathsf{PRF}}(\mathsf{DC}) + \ell \epsilon^{\text{q-auth}}$ *and* C *is the system including* π_{AB}, $\mathsf{IC}^{\ell, n + \log \ell}$, $\mathsf{QC}_A^{\ell, m, n + log\ell}$, $\mathsf{QC}_B^{\ell, m, n + log\ell}$.

3.4   Constructing a Pauli-Malleable Confidential Quantum Channel

In this section, we construct a Pauli-malleable confidential quantum channel $\mathsf{PMCC}^{\ell, m}$ from an insecure quantum channel $\mathsf{IC}^{\ell, m + \nu}$. In the Pauli-malleable confidential channel, the adversary can only get a notification of a new message arriving but has no access to the message. The adversary has the ability to block, reorder and modify the message via Pauli operators (bit flip and phase flip), as well as ask the channel to output a fully mixed state at Bob's interface, as defined in Definition 6.

Now we present the protocol in the multi-message case, described in Figure 7. In the protocol, Alice's computer will generate a new random string x of length ν for each message different from previous random strings and input it to $\mathsf{URF}^{\nu, 2m}$, a key k is returned by $\mathsf{URF}^{\nu, 2m}$, the Pauli-operator P_k is applied to the message and x is appended to the ciphertext. Bob's computer will do the measurement on the last ν qubits to get $\tilde{x}$, which is input to $\mathsf{URF}^{\nu, 2m}$, from which $\tilde{k}$ is obtained and finally the Pauli operator $P_{\tilde{k}}$ is applied to the ciphertext. The real system is drawn in Figure 8, and the ideal system we construct is illustrated in Figure 9.

π_A π_B QC_A QC_B

1. π_A: Alice inputs a message ρ^{A_i} and requests her computer to encrypt it.
2. QC_A: On input ρ^{A_i}, it generates a new random string x of length ν different from previously generated random strings, requests (through π_A) $k = \mathsf{input}(x)$ from URF. Then the computer applies Pauli operator P_k on the state ρ^{A_i} and gets $\sigma^C = P_k \rho^{A_i} P_k$. The computer appends $|x\rangle\langle x|^T$ to σ^C and outputs $\psi^{CT} = \sigma^C \otimes |x\rangle\langle x|^T$ to Alice.
3. π_A: Alice sends ψ^{CT} to Bob through secure quantum channel $\mathsf{IC}^{\ell,m+\nu}$.
4. π_B: Bob receives $\tilde{\psi}^{\tilde{C}\tilde{T}}$ and requests his computer to decrypt it.
5. QC_B: On input $\tilde{\psi}^{\tilde{C}\tilde{T}}$, the computer takes the first m qubits as $\tilde{\sigma}^{\tilde{C}}$. Then the computer measures the last ν qubits and get measurement result $\tilde{x}$. Then the computer requests (through π_B) $\tilde{k} = \mathsf{input}(\tilde{x})$ from URF. Then the computer applies Pauli operator $P_{\tilde{k}}$ on the state $\tilde{\sigma}^{\tilde{C}}$. Then the computer outputs $\tilde{\rho}^B = P_{\tilde{k}} \tilde{\sigma} P_{\tilde{k}}$ to Bob.
6. π_B: Bob outputs the decrypted message $\tilde{\rho}^B$.

Fig. 7. Converters and computer resources to construct $\mathsf{PMCC}^{\ell,m}$ from $\mathsf{IC}^{\ell,m+\nu}$. $\mathsf{QC}_A^{\ell,m,m+\nu}$ and $\mathsf{QC}_B^{\ell,m,m+\nu}$ will be queried ℓ times. The plaintext has length m and ciphertext has length $m + \nu$. $\mathsf{URF}^{\nu,2m}$ has input length ν and output length $2m$.

Theorem 2. *Let $\pi_{AB} = (\pi_A, \pi_B)$, $\mathsf{QC}_A^{\ell,m,m+\nu}$ and $\mathsf{QC}_B^{\ell,m,m+\nu}$ denote converters and computing resources, described in Figure 7, corresponding to Alice and Bob applying the following CPTP maps,*

$$\Lambda^{A_i \to CT}(\cdot) = \frac{1}{2^\nu} \sum_x P_{k_x}(\cdot)P_{k_x} \otimes |x\rangle\langle x|^T$$

$$\Lambda^{\tilde{C}\tilde{T} \to B}(\cdot) = \sum_x (P_{k_x} \otimes \langle x|^{\tilde{T}})(\cdot)(P_{k_x} \otimes |x\rangle^{\tilde{T}}),$$

where k_x is the output of $\mathsf{URF}^{\nu,2m}$ with input x. Let $\mathsf{QC}_E^{2\ell,m,m+\nu}$ be the computing resource of Eve capable of doing ℓ encryption operations and ℓ decryption operations. Then π_{AB} constructs a Pauli-malleable confidential quantum channel $\mathsf{PMCC}^{\ell,m}$ from an insecure quantum channel resource $\mathsf{IC}^{\ell,m+\nu}$, a shared uniform random function resource $\mathsf{URF}^{\nu,2m}$ within $\ell^2 \cdot 2^{-\nu}$, i.e.,

$$\left[\mathsf{IC}^{\ell,m+\nu}, \mathsf{URF}^{\nu,2m}, \mathsf{QC}_A^{\ell,m,m+\nu}, \mathsf{QC}_B^{\ell,m,m+\nu}\right] \xrightarrow{\pi_{AB}, \ell^2 2^{-\nu}} \left[\mathsf{PMCC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,m+\nu}\right].$$

In Appendix C we analyze the one-message case, which is then used in the following proof.

Proof. We present the simulator sim_E and $\mathsf{QC}_E^{2\ell,m,m+\nu}$ in the multi-message case and prove that R^ℓ cannot be distinguished from S^ℓ with significant advantage for any distinguisher D, where we define the real system illustrated in Figure 8 as $\mathsf{R}^\ell \coloneqq \pi_{AB}\left[\mathsf{IC}^{\ell,m+\nu}, \mathsf{URF}^{\nu,2m}, \mathsf{QC}_A^{\ell,m,m+\nu}, \mathsf{QC}_B^{\ell,m,m+\nu}\right]$, and the ideal system drawn in Figure 9 is $\mathsf{S}^\ell \coloneqq \mathsf{sim}_E\left[\mathsf{PMCC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,m+\nu}\right]$.

Fig. 8. The real system consisting of shared resources $\mathsf{IC}^{\ell,m+\nu}$ and $\mathsf{URF}^{\nu,2m}$, Alice and Bob's computing resources $\mathsf{QC}_A^{\ell,m,m+\nu}$ and $\mathsf{QC}_B^{\ell,m,m+\nu}$, and the protocol converters π_A and π_B.

Fig. 9. The ideal system consisting of $\mathsf{PMCC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,m+\nu}$ and sim_E. $\mathsf{QC}_E^{2\ell,m,m+\nu}$ makes use of ℓ instances of $\mathsf{QC}^{\text{q-otp}}$ internally while sim_E only receives and forwards messages and does no computation.

The simulator sim_E works exactly the same as the one message case analyzed in Appendix C. On input newMsg from the ideal resource $\mathsf{PMCC}^{\ell,m}$, it requests $\mathsf{QC}_E^{2\ell,m,m+\nu}$ to provide a quantum state ψ and outputs ψ at interface E. On input $\tilde{\psi}$ at interface E, it requests $\mathsf{QC}_E^{2\ell,m,m+\nu}$ to provide a tuple (i,k) (or $\perp$). The tuple (or $\perp$) is then forwarded to ideal channel $\mathsf{PMCC}^{\ell,m}$. Eve's computing resource $\mathsf{QC}_E^{2\ell,m,m+\nu}$ will use the computing resource $\mathsf{QC}^{\text{q-otp}}$ of the one message Pauli-malleable confidential quantum channel construction as a subroutine. $\mathsf{QC}_E^{2\ell,m,m+\nu}$ works as following.

- On the i-th input newMsg from sim_E, the computer instantiates a new $\mathsf{QC}_i^{\text{q-otp}}$ instance with index i and sends newMsg to $\mathsf{QC}_i^{\text{q-otp}}$. After getting the state σ from $\mathsf{QC}_i^{\text{q-otp}}$, the computer generates a random x of length ν, stores tuple (i,x) internally, appends x to state σ and outputs $\psi = \sigma \otimes |x\rangle\langle x|$ to sim_E.

– On input $\tilde{\psi}$ from interface E, the computer takes the first m qubits of $\tilde{\psi}$ as state $\tilde{\sigma}$, measures the last ν qubits of $\tilde{\psi}$ and obtains the measurement result $\tilde{x}$. If $\tilde{x}$ is not stored internally, the computer outputs $\perp$ to sim_E. If $\tilde{x}$ is store internally, the computer retrieves tuple $(\tilde{\imath}, \tilde{x})$, then it sends state $\tilde{\sigma}$ to $\mathsf{QC}_{\tilde{\imath}}^{\text{q-otp}}$. After getting output $\tilde{k}$ (or $\perp$) from $\mathsf{QC}_{\tilde{\imath}}^{\text{q-otp}}$, the computer sends tuple $(\tilde{\imath}, \tilde{k})$ (or $\perp$) to sim_E.

Let us consider $\overline{\mathsf{R}}^\ell := \pi_{AB}\left[\overline{\mathsf{IC}}^{\ell,m+\nu}, \mathsf{URF}^{\nu,2m}, \mathsf{QC}_A^{\ell,m,m+\nu}, \mathsf{QC}_B^{\ell,m,m+\nu}\right]$ and $\overline{\mathsf{S}}^\ell :=$ $\mathsf{sim}_E\left[\overline{\mathsf{PMCC}}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,m+\nu}\right]$ where the channels with overline $\overline{\mathsf{IC}}$ and $\overline{\mathsf{PMCC}}$ will reject any input from interface A if it contains the same tag x as previous input from interface E. Therefore, $\overline{\mathsf{R}}^\ell$ and R^ℓ, $\overline{\mathsf{S}}^\ell$ and S^ℓ are equivalent to any distinguisher up to the point that the distinguisher successfully guesses the string x that is randomly chosen by Alice's computer. In this case, in the real world the distinguisher inputs $\sigma \otimes |x\rangle\langle x|$ at interface E, state σ is flipped by some Pauli operator and is output at interface B. The distinguisher then forwards the output from interface B to interface A. Alice's computer happens to choose the same x for this input, thus flips the state back with the same Pauli operator and outputs same message $\sigma \otimes |x\rangle\langle x|$ at interface E. While in the ideal world, a fully mixed state with an appended tag will be output at interface E.

Let $x_1, x_2, \ldots, x_\ell$ be the random string of length ν randomly chosen by Alice, the probability that distinguisher guesses one successfully in ℓ times is

$$1 - (1 - \frac{\ell}{2^\nu})^\ell \leq \frac{\ell^2}{2^\nu}.$$

Therefore, for any distinguisher D, we have

$$d^{\mathsf{D}}\left(\mathsf{R}^\ell, \mathsf{S}^\ell\right) \leq d^{\mathsf{D}}\left(\overline{\mathsf{R}}^\ell, \overline{\mathsf{S}}^\ell\right) + \frac{\ell^2}{2^\nu}. \tag{13}$$

Following from a standard hybrid argument, if a distinguisher D can distinguish $\overline{\mathsf{R}}^\ell$ and $\overline{\mathsf{S}}^\ell$, it can be used to construct a distinguisher in the one message scenario, distinguishing $\overline{R}^1 = \pi_{AB}\left[\overline{\mathsf{IC}}^{1,m}, \mathsf{KEY}^{2m}, \mathsf{QC}_A^{1,m,m}, \mathsf{QC}_B^{1,m,m}\right]$ from $\overline{S}^1 = \mathsf{sim}^{\text{q-otp}}\left[\overline{\mathsf{PMCC}}^{1,m}, \mathsf{QC}^{\text{q-otp}}\right]$. Yet from Lemma 7 we know that $\overline{R}^1$ and $\overline{S}^1$ are equivalent. Therefore for any distinguisher D, $d^{\mathsf{D}}\left(\overline{\mathsf{R}}^\ell, \overline{\mathsf{S}}^\ell\right) = 0$.

Overall, we have proved that for any distinguisher D,

$$d^{\mathsf{D}}\left(\mathsf{R}^\ell, \mathsf{S}^\ell\right) \leq \frac{\ell^2}{2^\nu},$$

which concludes the construction proof. $\square$

Remark. The protocol given in Theorem 2 also has to satisfy correctness, i.e., when the distinguisher always puts back the same state Bob should decrypt correctly.

One can easily see that this holds, since in the real world, the state will be flipped on Alice's side and be flipped back on Bob side, thus the distinguisher will get the same state back at interface B.

Suppose now that one has a PRF resource and a bound ϵ^{PRF} satisfying Eq. (12), that is, indistinguishable from URF within ϵ^{PRF}, the following corollary follows trivially from the composition theorem Theorem 5 in Appendix B.

Corollary 4.

$$\left[\mathsf{IC}^{\ell,m+\nu}, \mathsf{KEY}^r, \mathsf{PRF}^{r,\nu,2m}, \mathsf{PRF}^{r,\nu,2m}, \mathsf{QC}_A^{\ell,m,m+\nu}, \mathsf{QC}_B^{\ell,m,m+\nu} \right]$$
$$\xrightarrow{\pi'_{AB},\epsilon} \left[\mathsf{PMCC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,m+\nu} \right].$$

where $\pi'_{AB} = (\pi_{AB}, \pi^{\mathsf{PRF}}), \epsilon(\mathsf{D}) = \epsilon^{\mathsf{PRF}}(\mathsf{DC}) + \ell^2 2^{-\nu}$ *and* C *is the system including* $\pi_{AB}, \mathsf{IC}^{\ell,m+\nu}, \mathsf{QC}_A^{\ell,m,m+\nu}, \mathsf{QC}_B^{\ell,m,m+\nu}$.

4 Relations to Game-Based Security Definitions

In this section we explore the relations between our constructive security definitions and two game based security definitions for (specific protocols making use of) symmetric quantum encryption schemes, both introduced in [AGM18]. The two notions we consider are those of *quantum ciphertexts indistinguishability under adaptive chosen-ciphertext attack* (AGM-QCCA2) and *quantum authenticated encryption* (QAE). Both definitions are inspired by classical security notions which intrinsically require the ability to copy data, which in [AGM18] were successfully translated into quantum analogue by circumventing the no-cloning theorem.

We will first show that QAE security exactly implies the constructive cryptography security notion of *constructing a secure channel from an insecure one and a shared secret key*, which we call CC-QSEC (but is actually stronger, and thus we also show a separation). Secondly, we will relate the AGM-QCCA2 security definition to the constructive cryptography security notion of *constructing a confidential channel from an insecure one and a shared secret key*, which we call CC-QCNF, but the implication will be less direct. In fact, we introduce two new (intermediate) game-based security definitions, RRC-QCCA2 and RRO-QCCA2, and show that:

1. The classical versions of AGM-QCCA2 and RRC-QCCA2 are asymptotically equivalent;
2. For a restricted class of schemes, RRC-QCCA2 implies RRO-QCCA2 (they are actually equivalent);
3. RRO-QCCA2 implies CC-QCNF (but is actually stronger).

We leave open the question whether it is possible to generalize (2.) to general schemes. Throughout this section we will assume that the plaintext and the ciphertext spaces comprise elements of the same length, an thus ignore the corresponding superscripts for channels and quantum computers.

4.1   Background and Notation

In [BCG$^+$02], a characterization of any *symmetric quantum encryption schemes* (SQES) was given, which states that encryption works by attaching some (possibly) key-dependent auxiliary state, and applying a unitary operator, and decryption undoes the unitary, and then checks whether the support of the state in the auxiliary register has changed. Thus, as pointed out in [AGM18], for key-generation function $\texttt{Gen}$ (inducing a probability distribution over some key-space $\mathcal{K}$), encryption function $\texttt{Enc}$, and decryption function $\texttt{Dec}$, we can characterize a SQES $\mathfrak{S} \coloneqq (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ as follows.

Lemma 3 ([AGM18, Corollary 1]). *Let $\mathfrak{S} = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ be a SQES. Then for every $k \in \mathcal{K}$ there exists a probability distribution $p_k : \mathcal{R} \to [0, 1]$ and a family of quantum states $\{|\psi_{k,r}\rangle^T\}_{r \in \mathcal{R}}$, with $\Pi_{k,r}^T \coloneqq |\psi_{k,r}\rangle\langle\psi_{k,r}|^T$, such that:*

- $\texttt{Enc}_k(\varrho^M) \coloneqq V_k\Big(\varrho^M \otimes \Pi_{k,r}^T\Big)V_k^\dagger$, *where r is sampled according to p_k;*
- $\texttt{Dec}_k(\sigma^C) \coloneqq \mathrm{Tr}_T\Big(P_{\omega_k}^T(V_k^\dagger \sigma^C V_k)P_{\omega_k}^T\Big) + \hat{D}_k\Big(\bar{P}_{\omega_k}^T(V_k^\dagger \sigma^C V_k)\bar{P}_{\omega_k}^T\Big);$

where $P_{\omega_k}^T$ and $\bar{P}_{\omega_k}^T$ are the orthogonal projectors onto the support of

$$\omega_k^T \coloneqq \sum_{r \in \mathcal{R}} p_k(r) \cdot \Pi_{k,r}^T = \sum_{r \in \mathcal{R}} p_k(r) \cdot |\psi_{k,r}\rangle\langle\psi_{k,r}|^T.$$

For a SQES $\mathfrak{S}$, we define a security notion XXX in terms of the advantage $\mathbf{Adv}_{\mathfrak{S},\mathsf{D}}^{\mathrm{xxx}}$ of a distinguisher D in solving some (usually distinction) problem involving $\mathfrak{S}$. In the asymptotic setting, security of $\mathfrak{S}$ according to notion XXX should be interpreted as $\mathbf{Adv}_{\mathfrak{S},\mathsf{D}}^{\mathrm{xxx}}$ being negligible for every D from some class $\mathbb{D}$ of distinguishers (usually, efficient distinguishers). Following the finite security approach, here we are just interested in relating advantages of different notions, making use of black-box reductions. Therefore, for a second notion YYY, we say that XXX *(security) implies* YYY *(security)* if and only if $\mathbf{Adv}_{\mathfrak{S},\mathsf{D}}^{\mathrm{yyy}} \leq c \cdot \mathbf{Adv}_{\mathfrak{S},\mathsf{DC}}^{\mathrm{xxx}}$, for some $c \geq 1$, where C denotes the black-box reduction that uses the distinguisher D for YYY to make a new distinguisher DC for XXX.

When describing experiments involving interaction between a distinguisher[17] D and a game system G, we use pseudo-code from G's perspective, that is, the **return** statement indicates what is output by the latter. Note that this implies

---

[17]We understand the distinguisher D as stateful, which can therefore be invoked multiple times (without making explicit the various updated states).

that for distinction problems we always make the game system output the bit output by the distinguisher. In this case we use the expression $D[G]$ to denote the bit output by D after interacting with G. On the other hand, if the output bit is decided by G (as is the case for the AGM-QCCA2 definition, restated in Appendix E, which is *not* a distinction problem), we use the expression $G[D]$. Moreover, we use both expressions not only for the returned value, but also for denoting the whole random experiments. When specifying that a distinguisher D has access to a list of oracles, e.g. $\mathbf{O}_1(\cdot)$ and $\mathbf{O}_2(\cdot)$, we write $x \leftarrow D^{\mathbf{O}_1(\cdot),\mathbf{O}_2(\cdot)}$, where the variable x holds the value output by D after the interaction with the oracles. We denote the application of a two-outcome projective measurement, e.g. $\{P^T_{\omega_k}, \mathbb{1} - P^T_{\omega_k}\}$, as $\{P^T_{\omega_k}, \mathbb{1} - P^T_{\omega_k}\} \Rightarrow b$, where $b \in \{0,1\}$ is the result of the measurement (we associate 0 to the the first outcome and 1 to the second). The state $|\phi_0\rangle$ is the EPR pair (one of the Bell state), to which we associate the two-outcome projective measurement $\{\Pi_+, \mathbb{1} - \Pi_+\}$. Furthermore, by $XY \leftarrow |\phi_0\rangle$ we mean that the EPR pair has been prepared on registers XY, and we use τ^X as a shorthand for the reduced state in register X, that is, half of a maximally-entangled state. Finally, we use sans-serif font for boolean labels, e.g. cheat, and by the expression cheat $? x : y$ we mean the value x if cheat is true (1), and the value y otherwise (false, 0).

4.2   Relating QAE and CC-QSEC

In this section we first present the quantum authenticated encryption security definition introduced in [AGM18], and then show that it directly implies our constructive security notion CC-QSEC of constructing a secure channel from an insecure one and a shared secret key.

QAE Security Definition ([AGM18]). We begin by restating what it means for a SQES $\mathfrak{S}$ to be secure in the QAE sense according to [AGM18]. On a high level, a distinguisher D must not be able to distinguish between two scenarios: in the first (the real one), it has access to regular encryption and decryption oracles, whereas in the second (the ideal one), it has access to an encryption oracle which replaces its queried plaintexts by random ones (half of a maximally-entangled state), and a decryption oracle that normally decrypts ciphertext not returned by the encryption oracle, but answers with the originally queried plaintexts otherwise (thus not really performing correct decryption). Note that this security notion, as shown in [AGM18], when phrased classically is equivalent to the canonical notion of authenticated encryption (dubbed IND-CCA3 by Shrimpton in [Shr04]). The only difference with the latter, is that the decryption oracle returns $\perp$ when queried on ciphertexts previously returned by the encryption oracle. But crucially, this detail is what would not make it possible to adapt IND-CCA3 into a quantum

definition: returning $\perp$ would require the game to *copy data* (store the cipher-
texts returned by the encryption oracle, and then compare them to each query
to the decryption oracle), which is not allowed in general in the quantum world.
Nevertheless, the formulation of QAE introduced in [AGM18] works quantumly
because, intuitively, *"it is possible to compare random states generated as half of a
maximally-entangled state"*: the trick consists of first ignoring (but storing) each
plaintext submitted by the adversary to the encryption oracle, and then, for each
plaintext, prepare an EPR pair $|\phi_0\rangle$, encrypt just half of it, and store the other
half (as well as the involved randomness) together with the original plaintext sub-
mitted by the distinguisher; then the decryption oracle normally decrypts each
ciphertext, and subsequently applies a projective measurement on the support of
$|\phi_0\rangle$ to the obtained plaintext against each stored half, and the associated orig-
inal plaintext can thus be easily retrieved. We now restate the definition from
[AGM18] (Definition 10 therein), adapted to our notation, and in the concrete
setting (as opposed to the asymptotic one).

Definition 10 (QAE Security [AGM18]). *For SQES* $\mathfrak{S} := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *(im-
plicit in all defined systems) we define the* QAE*-advantage of* $\mathfrak{S}$ *for distinguisher*
D *as*

$$\mathbf{Adv}^{\mathrm{qae}}_{\mathfrak{S},\mathsf{D}} := \Pr\Big[\mathsf{D}[\mathsf{G}^{\mathrm{qae\text{-}real}}] = 1\Big] - \Pr\Big[\mathsf{D}[\mathsf{G}^{\mathrm{qae\text{-}ideal}}] = 1\Big],$$

where the interactions of D *with game systems* $\mathsf{G}^{\mathrm{qae\text{-}real}}$ *and* $\mathsf{G}^{\mathrm{qae\text{-}ideal}}$ *are defined
in Figure 10.*

QAE Implies CC-QSEC. Here we denote by $\mathsf{G}^{\mathrm{qae\text{-}real},\ell}$ and $\mathsf{G}^{\mathrm{qae\text{-}ideal},\ell}$ the games
$\mathsf{G}^{\mathrm{qae\text{-}real}}$ and $\mathsf{G}^{\mathrm{qae\text{-}ideal}}$ where the distinguisher is allowed to make at most ℓ queries
to each oracle (and analogously for $\mathbf{Adv}^{\mathrm{qae},\ell}_{\mathfrak{S},\mathsf{D}}$).

Theorem 3. *Let* $\mathfrak{S} := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a SQES (implicit in all defined sys-
tems). Then with protocol* $\pi^{\mathrm{q\text{-}enc}}_{AB} = (\pi^{\mathrm{q\text{-}enc}}_A, \pi^{\mathrm{q\text{-}enc}}_B)$ *making use of quantum com-
puters* QC^ℓ_A *and* QC^ℓ_B *as defined in Figure 11, simulator* $\mathsf{sim}^{\mathrm{qae}}_E$ *making use of
quantum computer* QC^ℓ_E *as defined in Figure 12 (until the dashed line), and (triv-
ial) reduction system* C *as specified in the proof, for any distinguisher* D *we have*

$$\Delta^{\mathsf{D}}(\pi^{\mathrm{q\text{-}enc}}_{AB}[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}^\ell_A, \mathsf{QC}^\ell_B], \mathsf{sim}^{\mathrm{qae}}_E[\mathsf{SC}^\ell, \mathsf{QC}^\ell_E]) \leq \mathbf{Adv}^{\mathrm{qae},\ell}_{\mathfrak{S},\mathsf{DC}}.$$

Proof. Let $\mathsf{R} := \pi^{\mathrm{q\text{-}enc}}_{AB}[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}^\ell_A, \mathsf{QC}^\ell_B]$ and $\mathsf{S} := \mathsf{sim}^{\mathrm{qae}}_E[\mathsf{SC}^\ell, \mathsf{QC}^\ell_E]$. We need
to provide a reduction system C so that distinguishing between the games $\mathsf{G}^{\mathrm{qae\text{-}real},\ell}$
and $\mathsf{G}^{\mathrm{qae\text{-}ideal},\ell}$ can be reduced to distinguishing between resources R and S. Let D
be a distinguisher for R and S. Then we define an adversary $\mathsf{D}' = \mathsf{DC}$ with access
to real/ideal encryption oracle $\mathbf{Enc}(\cdot)$ and real/ideal decryption oracle $\mathbf{Dec}(\cdot)$
provided by $\mathsf{G}^{\mathrm{qae\text{-}real},\ell}/\mathsf{G}^{\mathrm{qae\text{-}ideal},\ell}$, where C behaves as follows towards D:

Experiments $\mathsf{D}[\mathsf{G}^{\text{qae-real}}]$ and $\mathsf{D}[\mathsf{G}^{\text{qae-ideal}}]$ for SQES $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$

$$k \leftarrow \mathtt{Gen}()$$
$$\mathcal{M} \leftarrow \varnothing$$
$$\mathbf{return}\ \mathsf{D}^{\mathbf{Enc}(\cdot), \mathbf{Dec}(\cdot)}$$

---

oracle Enc(ϱ^M):
$\quad \hat{r} \xleftarrow{p_k} \mathcal{R}$
$\quad \hat{M}\tilde{M} \leftarrow |\phi_0\rangle$
$\quad \hat{\sigma}^{\hat{C}} \leftarrow V_k(\hat{\varrho}^{\hat{M}} \otimes \Pi_{k,\hat{r}}^T)V_k^{\dagger} \qquad \triangleright\ \textit{Ignore } \varrho^M$
$\quad \mathcal{M} \leftarrow \mathcal{M} \cup \{(\hat{r}, \tilde{M}, M)\}$
$\quad \mathbf{return}\ \hat{\sigma}^{\hat{C}}$

$k \leftarrow \mathtt{Gen}()$
$\mathbf{return}\ \mathsf{D}^{\mathtt{Enc}_k(\cdot), \mathtt{Dec}_k(\cdot)}$

---

oracle Dec(σ^C):
$\quad \hat{M}T \leftarrow V_k^{\dagger}\sigma^C V_k$
$\quad \mathbf{for\ each}\ (\hat{r}, \tilde{M}, M) \in \mathcal{M}\ \mathbf{do}$
$\qquad \mathbf{if}\ \{\Pi_{k,\hat{r}}, \mathbb{1} - \Pi_{k,\hat{r}}\}(\omega^T) \Rightarrow 0\ \mathbf{then}$
$\qquad\quad \mathbf{if}\ \{\Pi_+, \mathbb{1} - \Pi_+\}(\varphi^{\hat{M}\tilde{M}}) \Rightarrow 0\ \mathbf{then}$
$\qquad\qquad \mathbf{return}\ \varrho^M$
$\quad \mathbf{return}\ |\bot\rangle\langle\bot|$

Fig. 10. QAE security games $\mathsf{G}^{\text{qae-real}}$ (**left**) and $\mathsf{G}^{\text{qae-ideal}}$ (**right**).

$\pi_A^{\text{q-enc}}\ \mathsf{QC}_A^{\ell}$

1. QC_A^{ℓ} request the key k from KEY and stores it in its memory.
2. For the i-th input ϱ^M at the outside interface, QC_A^{ℓ} samples randomness $r \xleftarrow{p_k} \mathcal{R}$, computes the ciphertext $\sigma^C \leftarrow V_k(\varrho^M \otimes \Pi_{k,r}^T)V_k^{\dagger}$, and outputs σ^C at the inside interface to IC^{ℓ}.

$\pi_B^{\text{q-enc}}\ \mathsf{QC}_B^{\ell}$

1. QC_B^{ℓ} request the key k from KEY and stores it in its memory.
2. For the i-th input σ^C at the inside interface from IC^{ℓ}, QC_B^{ℓ} computes $MT \leftarrow V_k\sigma^C V_k^{\dagger}$, and if $\{P_{\omega_k}^T, \mathbb{1} - P_{\omega_k}^T\}(\omega^T) \Rightarrow 0$, outputs the plaintext message ϱ^M at the outside interface.

Fig. 11. Encryption and decryption protocols.

- **Interface A:** On input message ϱ, output $\mathbf{Enc}(\varrho)$ at interface E.
- **Interface E:** On input state σ, output $\mathbf{Dec}(\sigma)$ at interface B.

Note that we trivially have that $\mathsf{CG}^{\text{qae-real},\ell} \equiv \mathsf{R}$ and $\mathsf{CG}^{\text{qae-ideal},\ell} \equiv \mathsf{S}$, hence

$$\begin{aligned}
\mathbf{Adv}_{\mathfrak{S},\mathsf{DC}}^{\text{qae},\ell} &= \Pr\left[\mathsf{DC}[\mathsf{G}^{\text{qae-real},\ell}] = 1\right] - \Pr\left[\mathsf{DC}[\mathsf{G}^{\text{qae-ideal},\ell}] = 1\right] \\
&= \Pr\left[\mathsf{D}[\mathsf{CG}^{\text{qae-real},\ell}] = 1\right] - \Pr\left[\mathsf{D}[\mathsf{CG}^{\text{qae-ideal},\ell}] = 1\right] \\
&= \Pr[\mathsf{D}[\mathsf{R}] = 1] - \Pr[\mathsf{D}[\mathsf{S}] = 1] \\
&= \Delta^{\mathsf{D}}(\mathsf{R}, \mathsf{S}).
\end{aligned}$$

This concludes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

$\mathsf{sim}_E^{\text{qae},\ell}\, \mathsf{QC}_E^\ell \; / \; \mathsf{sim}_E^{\text{qcca2},\ell}\, \mathsf{QC}_E^\ell$

1. QC_E^ℓ generates a key $k \leftarrow \text{Gen}()$, stores it in its memory, and sets $\mathcal{M} \leftarrow \varnothing$.
2. QC_E^ℓ performs the following two tasks in parallel:
   (a) For the i-th input newMsg at the inside interface from SC^ℓ, QC_E^ℓ samples randomness $\hat{r} \xleftarrow{p_k} \mathcal{R}$, prepares $\hat{M}\tilde{M} \leftarrow |\phi_0\rangle$, computes $\sigma^C \leftarrow V_k(\hat{\varrho}^{\hat{M}} \otimes \Pi_{k,\hat{r}}^T)V_k^\dagger$, and outputs the ciphertext σ^C at the outside interface. Finally, it performs the update $\mathcal{M} \leftarrow \mathcal{M} \cup \{(\hat{r}, \tilde{M}, i)\}$.
   (b) For the i-th input σ^C at the outside interface, QC_E^ℓ computes $\hat{M}T \leftarrow V_k^\dagger \sigma^C V_k$. Then for each $(\hat{r}, \tilde{M}, j) \in \mathcal{M}$, it computes $\{\Pi_{k,\hat{r}}, \mathbb{1} - \Pi_{k,\hat{r}}\}(\omega^T)$; if the result of the measurement is 0, then it computes $\{\Pi_+, \mathbb{1} - \Pi_+\}(\varphi^{\hat{M}\tilde{M}})$; if the result of the measurement is again 0, then it outputs the index j at the inside interface to SC^ℓ.
   -
   Otherwise, it computes $\{P_{\omega_k}^T, \mathbb{1} - P_{\omega_k}^T\}(\omega^T)$, and if the result of the measurement is 0, then it outputs the message $\hat{\varrho}^{\hat{M}}$ at the inside interface to SC^ℓ.

Fig. 12. QAE (until the dashed line) and QCCA2 (until the end) simulators.

Corollary 5. *With* $\varepsilon(\mathsf{D}) := \sup_{\mathsf{D}' \in \mathcal{B}(\mathsf{D})} \mathbf{Adv}_{\mathfrak{S},\mathsf{D}'}^{\text{qae},\ell}$, *we have*

$$\left[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}_A^\ell, \mathsf{QC}_B^\ell \right] \xrightarrow{\pi_{AB}^{\text{q-enc}},\varepsilon} \left[\mathsf{SC}^\ell, \mathsf{QC}_E^\ell \right],$$

where the class $\mathcal{B}(\mathsf{D})$ *is defined in Eq. (6), Section 2.1.*

QAE is Stronger than CC-QSEC. We remark that even though QAE implies CC-QSEC, the converse is not true. In particular, we find that QAE is an (unnecessarily) stronger notion than CC-QSEC. We can in fact show that there are SQESs that 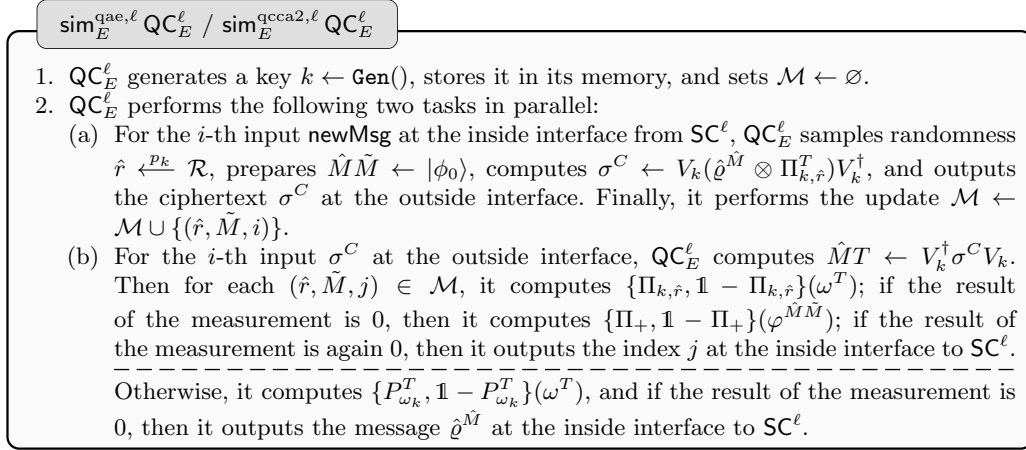satisfy CC-QSEC, but not QAE. Following [CKN03], in order to show this fact it suffices to take any SQES $\mathfrak{S}$ which is QAE secure, and slightly modify it into a new SQES $\mathfrak{S}'$ so that a classical 0-bit is appended to every encryption, which is then ignored upon decryption. Now an adversary can flip the bit of a ciphertext that it got from the encryption oracle, and then query the decryption oracle on the new ciphertext: in the real setting it will get back the original message, while in the ideal setting it will get back $|\bot\rangle\langle\bot|$, and can thus perfectly distinguish between the two, hence $\mathfrak{S}'$ cannot be QAE secure. On the other hand, $\mathfrak{S}'$ is still CC-QSEC secure because it can still be used to achieve the construction of a secure channel from an insecure one and a shared secret key. This is possible by using a simulator which works essentially as $\mathsf{sim}_E^{\text{qae},\ell}\mathsf{QC}_E^\ell$ from Figure 12, but which ignores the bit.

4.3 Relating QCCA2 and CC-QCNF

The goal of this section is to present and relate several QCCA2 security definitions. The original AGM-QCCA2 definition from [AGM18] is restated in Appendix E.

In this section we begin by introducing a new definition, RRC-QCCA2 (where RRC stands for *"real-or-random challenge"*), which is similar to AGM-QCCA2. Both notions define a challenge phase, and thus we introduce a third variant, RRO-QCCA2 (where RRO stands for *"real-or-random oracles"*), in which there is no real-or-random challenge, but rather access to real-or-random oracles. Crucially, the latter is identical to QAE as introduced by [AGM18], up to a small detail: *upon decryption, if the ciphertext was not generated by the encryption oracle, instead of returning $|\bot\rangle\langle\bot|$, return the decrypted plaintext.* Finally, we show that for a restricted class of SQESs, RRC-QCCA2 implies RRO-QCCA2, and for any SQESs, RRO-QCCA2 implies CC-QCNF.

RRC-QCCA2 Security Definition. We now introduce an alternative game-based security definition that seems more natural than AGM-QCCA2. This notion is defined in terms of a distinction problem (as opposed to AGM-QCCA2), and essentially it is analogous to the test setting of the latter, $\mathsf{G}^{\text{qcca2-test}}$, but where the decryption oracle provided to the distinguisher behaves differently: after the real-or-random challenge phase, upon querying the challenge ciphertext, it will respond with the plaintext originally submitted by the distinguisher, in both the real and ideal settings. Note that this is possible in the ideal setting, because we make use of the same trick as in $\mathsf{G}^{\text{qcca2-fake}}$, but we do not just set a flag whenever we detect that the adversary is cheating, but rather return the original message that it submitted as challenge. Since a similar behavior is implemented in the real setting, the adversary must really be able to distinguish between ciphertexts in order to win.

Definition 11 (RRC-QCCA2 Security). *For SQES $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ (implicit in all defined systems) we define the* RRC-QCCA2-*advantage of $\mathfrak{S}$ for distinguisher* D *as*

$$\mathbf{Adv}^{\text{rrc-qcca2}}_{\mathfrak{S},\mathsf{D}} := \Pr\Big[\mathsf{D}[\mathsf{G}^{\text{rrc-qcca2-real}}] = 1\Big] - \Pr\Big[\mathsf{D}[\mathsf{G}^{\text{rrc-qcca2-ideal}}] = 1\Big],$$

where the interactions of D *with game systems $\mathsf{G}^{\text{rrc-qcca2-real}}$ and $\mathsf{G}^{\text{rrc-qcca2-ideal}}$ are defined in Figure 13.*

RRO-QCCA2 Security Definition. In order to relate the latter definition with a constructive notion of confidentiality, it is helpful to have a game-based security definition which analogously to QAE defines a real and an ideal setting (by specifying real-or-random oracles, and in particular, not only a real-or-random challenge). We do this by introducing the notion RRO-QCCA2, which can be seen as a natural extension of RRC-QCCA2.

Experiments $\mathsf{G}^{\text{rrc-qcca2-real}}[\mathsf{D}]$ and $\mathsf{G}^{\text{rrc-qcca2-ideal}}[\mathsf{D}]$ for SQES $\mathfrak{S} := (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$

$k \leftarrow \texttt{Gen}()$
$\bar{\varrho}^{\bar{M}} \leftarrow \mathsf{D}^{\texttt{Enc}_k(\cdot), \texttt{Dec}_k(\cdot)}$ $\triangleright$ *Keep* $\bar{\varrho}^{\bar{M}}$
$\hat{r} \xleftarrow{p_k} \mathcal{R}$ $\triangleright$ *Keep* $\hat{r}$
$\hat{M}\tilde{M} \leftarrow |\phi_0\rangle$
$\hat{\sigma}^{\hat{C}} \leftarrow V_k(\hat{\varrho}^{\hat{M}} \otimes \Pi^T_{k,\hat{r}}) V_k^\dagger$ $\triangleright$ *Ignore* $\bar{\varrho}^{\bar{M}}$
$b' \leftarrow \mathsf{D}^{\texttt{Enc}_k(\cdot), \mathbf{Dec}(\cdot)}(\hat{\sigma}^{\hat{C}})$
return b'

$k \leftarrow \texttt{Gen}()$
$\varrho^M \leftarrow \mathsf{D}^{\texttt{Enc}_k(\cdot), \texttt{Dec}_k(\cdot)}$
$\sigma^C \leftarrow \texttt{Enc}_k(\varrho^M)$
$b' \leftarrow \mathsf{D}^{\texttt{Enc}_k(\cdot), \texttt{Dec}_k(\cdot)}(\sigma^C)$
return b'

oracle $\mathbf{Dec}(\sigma^C)$:
     $MT \leftarrow V_k^\dagger \sigma^C V_k$
     if $\{P^T_{\omega_k}, \mathbb{1} - P^T_{\omega_k}\}(\omega^T) \Rightarrow 0$ **then**
         if $\{\Pi_{k,\hat{r}}, \mathbb{1} - \Pi_{k,\hat{r}}\}(\omega^T) \Rightarrow 0$ **then**
             if $\{\Pi_+, \mathbb{1} - \Pi_+\}(\varphi^{M\tilde{M}}) \Rightarrow 0$ **then**
                 return $\bar{\varrho}^{\bar{M}}$ $\triangleright$ *Original challenge*
     else
         return $\hat{D}_k(\rho^{MT})$ $\triangleright$ *Invalid ciphertext*
     return ϱ^M

Fig. 13. RRC-QCCA2 games $\mathsf{G}^{\text{rrc-qcca2-real}}$ (**left**) and $\mathsf{G}^{\text{rrc-qcca2-ideal}}$ (**right**).

Definition 12 (RRO-QCCA2 Security). *For SQES* $\mathfrak{S} := (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ *(implicit in all defined systems) we define the* RRO-QCCA2-*advantage of* $\mathfrak{S}$ *for distinguisher* D *as*

$$\mathbf{Adv}^{\text{rro-qcca2}}_{\mathfrak{S},\mathsf{D}} := \Pr\left[\mathsf{D}[\mathsf{G}^{\text{rro-qcca2-real}}] = 1\right] - \Pr\left[\mathsf{D}[\mathsf{G}^{\text{rro-qcca2-ideal}}] = 1\right],$$

where the interactions of D *with game systems* $\mathsf{G}^{\text{rro-qcca2-real}}$ *and* $\mathsf{G}^{\text{rro-qcca2-ideal}}$ *are defined in* Figure 14.

Relating AGM-QCCA2 and RRC-QCCA2. We feel that RRC-QCCA2 is a much simpler and more natural definition than AGM-QCCA2. In fact, in [AGM18] the authors claim that AGM-QCCA2 is a "natural" security definition based on the fact that its classical analogon is shown to be equivalent to (a variation of) the standard classical IND-CCA2 security definition. We claim that our RRC-QCCA2 is more natural in the sense that it is formulated as a normal distinction problem (as opposed to AGM-QCCA2), and its classical analogon can be shown to be equivalent to standard classical IND-CCA2 security much more directly (in particular, with no concrete security loss, as opposed to AGM-QCCA2, where it is shown that the concrete reduction has a factor 2 security loss).

     Similarly as done in [AGM18] for QAE, whose classical restriction was shown to be equivalent to the common classical notion of authenticated encryption
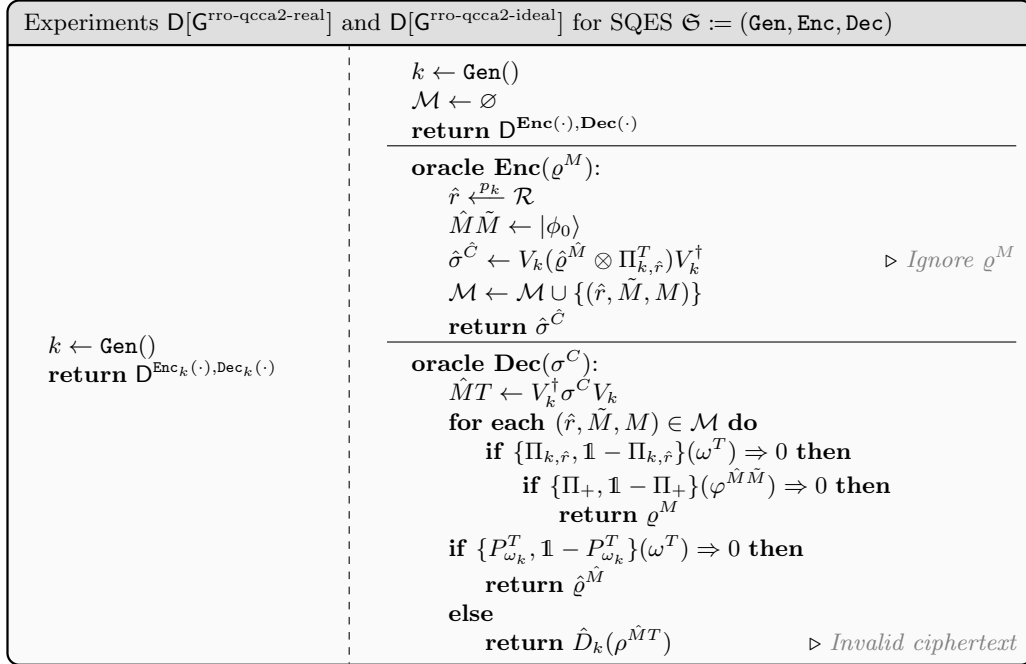

Experiments $\mathsf{D}[\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}real}}]$ and $\mathsf{D}[\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}ideal}}]$ for SQES $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$

$k \leftarrow \mathtt{Gen}()$
$\mathcal{M} \leftarrow \varnothing$
$\mathbf{return}\ \mathsf{D}^{\mathbf{Enc}(\cdot), \mathbf{Dec}(\cdot)}$

$\mathbf{oracle}\ \mathbf{Enc}(\varrho^M)$:
   $\hat{r} \xleftarrow{p_k} \mathcal{R}$
   $\hat{M}\tilde{M} \leftarrow |\phi_0\rangle$
   $\hat{\sigma}^{\hat{C}} \leftarrow V_k(\hat{\varrho}^{\hat{M}} \otimes \Pi^T_{k,\hat{r}}) V^\dagger_k$ $\triangleright$ *Ignore ϱ^M*
   $\mathcal{M} \leftarrow \mathcal{M} \cup \{(\hat{r}, \tilde{M}, M)\}$
   $\mathbf{return}\ \hat{\sigma}^{\hat{C}}$

$k \leftarrow \mathtt{Gen}()$
$\mathbf{return}\ \mathsf{D}^{\mathtt{Enc}_k(\cdot), \mathtt{Dec}_k(\cdot)}$

$\mathbf{oracle}\ \mathbf{Dec}(\sigma^C)$:
   $\hat{M}T \leftarrow V^\dagger_k \sigma^C V_k$
   $\mathbf{for\ each}\ (\hat{r}, \tilde{M}, M) \in \mathcal{M}\ \mathbf{do}$
      $\mathbf{if}\ \{\Pi_{k,\hat{r}}, \mathbb{1} - \Pi_{k,\hat{r}}\}(\omega^T) \Rightarrow 0\ \mathbf{then}$
         $\mathbf{if}\ \{\Pi_+, \mathbb{1} - \Pi_+\}(\varphi^{\hat{M}\tilde{M}}) \Rightarrow 0\ \mathbf{then}$
            $\mathbf{return}\ \varrho^M$
      $\mathbf{if}\ \{P^T_{\omega_k}, \mathbb{1} - P^T_{\omega_k}\}(\omega^T) \Rightarrow 0\ \mathbf{then}$
         $\mathbf{return}\ \hat{\varrho}^{\hat{M}}$
      $\mathbf{else}$
         $\mathbf{return}\ \hat{D}_k(\rho^{\hat{M}T})$ $\triangleright$ *Invalid ciphertext*

Fig. 14. RRO-QCCA2 games $\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}real}}$ (**left**) and $\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}ideal}}$ (**right**).

IND-CCA3 from [Shr04], we now show that our RRC-QCCA2 security notion, when casted to a classical definition, dubbed RRC-CCA2, is equivalent (in particular, with no loss factors, as opposed to AGM-QCCA2) to a common classical notion of IND-CCA2. The latter definition is the same mentioned in [AGM18], and comprises a real-or-random challenge, but the decryption oracle returns $\perp$ upon submitting the challenge ciphertext. On the other hand, RRC-CCA2 behaves exactly the same as IND-CCA2, except that it always returns the challenge plaintext as originally submitted by the adversary upon querying the challenge ciphertext, independently from the (real or ideal) setting.

Lemma 4. RRC-CCA2 *and* IND-CCA2 *are equivalent.*

Proof. To transform RRC-CCA2 into IND-CCA2, the reduction simply stores the challenge ciphertext $\hat{c}$, and returns $\perp$ whenever the decryption oracle is queried upon $\hat{c}$. To transform IND-CCA2 into RRC-CCA2, the reduction simply stores the challenge plaintext $\hat{m}$ and the challenge ciphertext $\hat{c}$, and returns $\hat{m}$ whenever the decryption oracle is queried upon $\hat{c}$. $\qquad\square$

RRC-QCCA2 Implies RRO-QCCA2. As above, here we add as superscript the parameter ℓ to games and advantages to denote that the distinguisher is allowed

to make at most ℓ queries to the oracles. Note that we relate RRC-QCCA2 and RRO-QCCA2 for only the subclass of SQESs which satisfy the following condition.

Condition 1. *SQES $\mathfrak{S}$ is such that the auxiliary state does not depend on the key (but possibly on the randomness), and it appends explicitly the randomness to the ciphertext, that is:*

$$\mathtt{Enc}_k(\varrho^M) = U_{k,r}(\varrho^M \otimes \Pi_r^T)U_{k,r}^{\dagger} \otimes |r\rangle\langle r|^R,$$

for some unitary $U_{k,r}$ depending on both the key k and the randomness r.

We remark that this restriction still captures all the explicit protocols considered in [AGM18].

Lemma 5. *Let $\mathfrak{S}$ be a SQES satisfying [Condition 1](). Then for reduction system C_I as specified in the proof, for any distinguisher D we have*

$$\mathbf{Adv}_{\mathfrak{S},\mathsf{D}}^{\mathrm{rro\text{-}qcca2},\ell} \leq \ell \cdot \mathbf{Adv}_{\mathfrak{S},\mathsf{DC}_I}^{\mathrm{rrc\text{-}qcca2},\ell-1}.$$

Proof. We need to provide a reduction system C_i, parameterized on an index $i \in \{1,\dots,\ell\}$, so that distinguishing between the two games $\mathsf{G}^{\mathrm{rrc\text{-}qcca2\text{-}real},\ell-1}$ and $\mathsf{G}^{\mathrm{rrc\text{-}qcca2\text{-}ideal},\ell-1}$ can be reduced to distinguishing between $\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}real},\ell}$ and $\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}ideal},\ell}$. Let D be a distinguisher for $\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}real},\ell}$ and $\mathsf{G}^{\mathrm{rro\text{-}qcca2\text{-}ideal},\ell}$. Then we define an adversary $\mathsf{D}' = \mathsf{DC}_I$, where I is a uniform random variable over $\{1,\dots,\ell\}$, with access to encryption oracle $\mathbf{Enc}(\cdot)$, decryption oracle $\mathbf{Dec}(\cdot)$, and challenge oracle $\mathbf{Chall}(\cdot)$, provided by $\mathsf{G}^{\mathrm{rrc\text{-}qcca2\text{-}real},\ell}/\mathsf{G}^{\mathrm{rrc\text{-}qcca2\text{-}ideal},\ell}$, where C_i internally keeps a set $\mathcal{M}$ and exports oracles $\mathbf{Enc}'(\cdot)$ and $\mathbf{Dec}'(\cdot)$ towards D which behave as follows:

- Oracle $\mathbf{Enc}'(\cdot)$: on input the j-th message ϱ^M:
    - If $j < i$:
        1. $\hat{M}\tilde{M} \leftarrow |\phi_0\rangle$.
        2. $\hat{\sigma}^{\hat{C}} \otimes |\hat{r}\rangle\langle\hat{r}|^R \leftarrow \mathbf{Enc}(\hat{\varrho}^{\hat{M}})$.
        3. $\mathcal{M} \leftarrow \mathcal{M} \cup \{(\hat{r},\tilde{M},M)\}$.
        4. Return $\hat{\sigma}^{\hat{C}} \otimes |\hat{r}\rangle\langle\hat{r}|^R$.
    - If $j = i$: return $\mathbf{Chall}(\varrho^M)$.
    - If $j > i$: return $\mathbf{Enc}(\varrho^M)$.
- Oracle $\mathbf{Dec}'(\cdot)$: on input ciphertext $\sigma^C \otimes |r\rangle\langle r|^R$:
    1. $\hat{\varrho}^{\hat{M}} \leftarrow \mathbf{Dec}(\sigma^C \otimes |r\rangle\langle r|^R)$.
    2. If $\hat{\varrho}^{\hat{M}} = |\bot\rangle\langle\bot|$, return $|\bot\rangle\langle\bot|$, otherwise proceed.
    3. For each $(\hat{r},\tilde{M},M) \in \mathcal{M}$ do the following: if $\{\Pi_{\hat{r}}, \mathbb{1} - \Pi_{\hat{r}}\}(\omega^T) \Rightarrow 0$ and $\{\Pi_+, \mathbb{1} - \Pi_+\}(\varphi^{\hat{M}\tilde{M}}) \Rightarrow 0$, return ϱ^M, otherwise proceed.
    4. Return $|\bot\rangle\langle\bot|$.

Let now define the hybrid systems H_i resulting from attaching the reduction system C_i to the real RRC-QCCA2 game, that is, define $\mathsf{H}_i \coloneqq \mathsf{C}_i\mathsf{G}^{\mathrm{rrc\text{-}qcca2\text{-}real},\ell-1}$.

Then observe that $H_{i+1} \equiv C_i G^{\text{rrc-qcca2-ideal},\ell-1}$, $H_1 \equiv G^{\text{rro-qcca2-real},\ell}$, and $H_{\ell+1} \equiv G^{\text{rro-qcca2-ideal},\ell}$. Finally, by the law of total probability, we have:

$$
\begin{aligned}
\mathbf{Adv}&_{\mathsf{G},\mathsf{DC}}^{\text{rrc-qcca2},\ell-1} \\
&= \Pr\Big[\mathsf{DC}[\mathsf{G}^{\text{rrc-qcca2-real},\ell-1}] = 1\Big] - \Pr\Big[\mathsf{DC}[\mathsf{G}^{\text{rrc-qcca2-ideal},\ell-1}] = 1\Big] \\
&= \frac{1}{\ell} \sum_{i=1}^{\ell} \Big(\Pr\Big[\mathsf{D}[\mathsf{C}_i \mathsf{G}^{\text{rrc-qcca2-real},\ell-1}] = 1\Big] - \Pr\Big[\mathsf{D}[\mathsf{C}_i \mathsf{G}^{\text{rrc-qcca2-ideal},\ell-1}] = 1\Big] \Big) \\
&= \frac{1}{\ell} \sum_{i=1}^{\ell} (\Pr[\mathsf{D}[\mathsf{H}_i] = 1] - \Pr[\mathsf{D}[\mathsf{H}_{i+1}] = 1]) \\
&= \frac{1}{\ell} \cdot (\Pr[\mathsf{D}[\mathsf{H}_1] = 1] - \Pr[\mathsf{D}[\mathsf{H}_{\ell+1}] = 1]) \\
&= \frac{1}{\ell} \cdot \Big(\Pr\Big[\mathsf{D}[\mathsf{G}^{\text{rro-qcca2-real},\ell}] = 1\Big] - \Pr\Big[\mathsf{D}[\mathsf{G}^{\text{rro-qcca2-ideal},\ell}] = 1\Big] \Big) \\
&= \frac{1}{\ell} \cdot \mathbf{Adv}_{\mathsf{G},\mathsf{D}}^{\text{rro-qcca2},\ell}.
\end{aligned}
$$

This concludes the proof. $\qquad\square$

Remark 4. It is easy to show that the other direction of Lemma 5 also holds (for the same class of SQES), that is, RRO-QCCA2 implies RRC-QCCA2. For this, the reduction C flips a bit $\tilde{B}$ and uses the RRO-QCCA2 security game to emulate the RRC-QCCA2 game, resulting in perfect emulation with probability $\frac{1}{2}$, and perfect unguessability otherwise. Thus, with DC outputting 1 if and only if D correctly guesses $\tilde{B}$, we have $\mathbf{Adv}_{\mathsf{G},\mathsf{D}}^{\text{rrc-qcca2},\ell} \leq 2 \cdot \mathbf{Adv}_{\mathsf{G},\mathsf{DC}}^{\text{rro-qcca2},\ell-1}$, and therefore the two notions are asymptotically equivalent, as we formalize in the following lemma.

Lemma 6. *For SQES satisfying Condition 1, RRC-QCCA2 and RRO-QCCA2 are asymptotically equivalent.*

Proof. This follows directly by Lemma 5 and Remark 4. $\qquad\square$

Just as we casted RRC-QCCA2 into the classical definition RRC-CCA2, we can cast RRO-QCCA2 into RRO-CCA2. Then it is possible to obtain analogous results as above for the classical notions (without restrictions on the (classical) encryption scheme).

Corollary 6. *RRC-CCA2 and RRO-CCA2 are asymptotically equivalent.*

RRO-QCCA2 Implies CC-QCNF. We can now finally relate QCCA2 game-based security definitions to the constructive cryptography notion of confidentiality, CC-QCNF. We do that by showing that RRO-QCCA2 security implies CC-QCNF, and therefore, by Lemma 5, so does RRC-QCCA2 (with concrete security loss factor ℓ).

Theorem 4. *Let $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ be a SQES (implicit in all defined systems). Then with protocol $\pi_{AB}^{\text{q-enc}} = (\pi_A^{\text{q-enc}}, \pi_B^{\text{q-enc}})$ making use of quantum computers QC_A^ℓ and QC_B^ℓ (already defined in Figure 11 for Theorem 3), simulator $\mathsf{sim}_E^{\text{qcca2}}$ making use of quantum computer QC_E^ℓ as defined in Figure 12 (until the end), and (trivial) reduction system C as specified in the proof, for any distinguisher D we have*

$$\Delta^{\mathsf{D}}(\pi_{AB}^{\text{q-enc}}[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}_A^\ell, \mathsf{QC}_B^\ell], \mathsf{sim}_E^{\text{qcca2}}[\mathsf{NMCC}^\ell, \mathsf{QC}_E^\ell]) \leq \mathbf{Adv}_{\mathfrak{S}, \mathsf{DC}}^{\text{rro-qcca2},\ell}.$$

Proof. Let $\mathsf{R} := \pi_{AB}^{\text{q-enc}}[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}_A^\ell, \mathsf{QC}_B^\ell]$ and $\mathsf{S} := \mathsf{sim}_E^{\text{qae}}[\mathsf{NMCC}^\ell, \mathsf{QC}_E^\ell]$. We need to provide a reduction system C so that distinguishing between the games $\mathsf{G}^{\text{rro-qcca2-real},\ell}$ and $\mathsf{G}^{\text{rro-qcca2-ideal},\ell}$ can be reduced to distinguishing between resources R and S. Let D be a distinguisher for R and S. Then we define an adversary $\mathsf{D}' = \mathsf{DC}$ with access to real/ideal encryption oracle $\mathbf{Enc}(\cdot)$ and real/ideal decryption oracle $\mathbf{Dec}(\cdot)$ provided by $\mathsf{G}^{\text{rro-qcca2-real},\ell}/\mathsf{G}^{\text{rro-qcca2-ideal},\ell}$, where C behaves as follows towards D:

– **Interface A:** On input message ϱ, output $\mathbf{Enc}(\varrho)$ at interface E.
– **Interface E:** On input state σ, output $\mathbf{Dec}(\sigma)$ at interface B.

Note that we trivially have that $\mathsf{CG}^{\text{rro-qcca2-real},\ell} \equiv \mathsf{R}$ and $\mathsf{CG}^{\text{rro-qcca2-ideal},\ell} \equiv \mathsf{S}$, hence

$$\begin{aligned}
\mathbf{Adv}_{\mathfrak{S},\mathsf{DC}}^{\text{rro-qcca2},\ell} &= \Pr\left[\mathsf{DC}[\mathsf{G}^{\text{rro-qcca2-real},\ell}] = 1\right] - \Pr\left[\mathsf{DC}[\mathsf{G}^{\text{rro-qcca2-ideal},\ell}] = 1\right] \\
&= \Pr\left[\mathsf{D}[\mathsf{CG}^{\text{rro-qcca2-real},\ell}] = 1\right] - \Pr\left[\mathsf{D}[\mathsf{CG}^{\text{rro-qcca2-ideal},\ell}] = 1\right] \\
&= \Pr[\mathsf{D}[\mathsf{R}] = 1] - \Pr[\mathsf{D}[\mathsf{S}] = 1] \\
&= \Delta^{\mathsf{D}}(\mathsf{R}, \mathsf{S}).
\end{aligned}$$

This concludes the proof. $\qquad\square$

Corollary 7. *With $\varepsilon(\mathsf{D}) := \sup_{\mathsf{D}' \in \mathcal{B}(\mathsf{D})} \mathbf{Adv}_{\mathfrak{S},\mathsf{D}'}^{\text{rro-qcca2},\ell}$, we have*

$$\left[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}_A^\ell, \mathsf{QC}_B^\ell\right] \xrightarrow{\pi_{AB}^{\text{q-enc}}, \varepsilon} \left[\mathsf{NMCC}^\ell, \mathsf{QC}_E^{\text{qcca2},\ell}\right],$$

where the class $\mathcal{B}(\mathsf{D})$ is defined in Eq. (6), Section 2.1.

Using Lemma 5, we finally obtain the following corollary.

Corollary 8. *With $\varepsilon(\mathsf{D}) := \sup_{\mathsf{D}' \in \mathcal{B}(\mathsf{D})} \mathbf{Adv}_{\mathfrak{S},\mathsf{D}'}^{\text{rrc-qcca2},\ell}$, we have*

$$\left[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}_A^\ell, \mathsf{QC}_B^\ell\right] \xrightarrow{\pi_{AB}^{\text{q-enc}}, (\ell+1)\cdot\varepsilon} \left[\mathsf{NMCC}^\ell, \mathsf{QC}_E^{\text{qcca2},\ell}\right],$$

where the class $\mathcal{B}(\mathsf{D})$ is defined in Eq. (6), Section 2.1.

RRO-QCCA2 is Stronger than CC-QCNF. We remark that even though the security notion RRO-QCCA2 implies CC-QCNF, the converse is not true for the same reason outlined above for QAE and CC-QSEC: it is possible to show that there are SQESs that satisfy CC-QCNF but not RRO-QCCA2 by applying the same principle of extending a RRO-QCCA2 secure scheme into one which is not anymore RRO-QCCA2, but still satisfies CC-QCNF.

Acknowledgments

References

ABF+16.   Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael St Jules. Computational security of quantum encryption. In *International Conference on Information Theoretic Security*, pages 47–71. Springer, 2016.

AGM18.   Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable quantum encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 489–519. Springer, 2018. [doi:10.1007/978-3-319-78372-7˙16, arXiv:1709.06539].

BCG+02.   Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *Proceedings of the 43rd Symposium on Foundations of Computer Science, FOCS '02*, pages 449–458. IEEE, 2002. [doi:10.1109/SFCS.2002.1181969, arXiv:quant-ph/0205128].

BDJR97.   Mihir Bellare, Anand Desai, Eron Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, FOCS '97, pages 394–403. IEEE Computer Society, 1997. [doi:10.1109/SFCS.1997.646128].

BDPR98.   Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology – CRYPTO '98*, pages 26–45. Springer, 1998. [doi:10.1007/BFb0055718].

BHL+05.   Michael Ben-Or, Michał Horodecki, Debbie Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography, Proceedings of TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406. Springer, 2005. [doi:10.1007/978-3-540-30576-7˙21, arXiv:quant-ph/0409078].

BJ15.   Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low t-gate complexity. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, pages 609–629. Springer, 2015. [doi:10.1007/978-3-662-48000-7˙30].

BN00.   Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer, 2000. [doi:10.1007/3-540-44448-3˙41].

BPW04.   Michael Backes, Birgit Pfitzmann, and Michael Waidner. A general composition theorem for secure reactive systems. In *Theory of Cryptography, Proceedings of TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2004. [doi:10.1007/978-3-540-24638-1˙19].

BPW07.   Michael Backes, Birgit Pfitzmann, and Michael Waidner. The reactive simulatability (RSIM) framework for asynchronous systems. *Information and Computation*, 205(12):1685–1720, 2007. Extended version of [PW01]. [doi:10.1016/j.ic.2007.05.002, IACR e-print: 2004/082].

Can01.   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].

Can13.   Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2013. Updated version of [Can01]. [IACR e-print: 2000/067].

CDP09.   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].

CDPW07.   Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish. Universally composable security with global setup. In *Theory of Cryptography, Proceedings of TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 61–85. Springer, 2007. [doi:10.1007/978-3-540-70936-7˙4, IACR e-print: 2006/432].

CKN03.   Ran Canetti, Hugo Krawczyk, and Jesper B. Nielsen. Relaxing chosen-ciphertext security. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, pages 565–582. Springer, 2003. [doi:10.1007/978-3-540-45146-4˙33].

CMT13.   Sandro Coretti, Ueli Maurer, and Björn Tackmann. Constructing confidential channels from authenticated channels—public-key encryption revisited. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology – ASIACRYPT 2013*, pages 134–153. Springer, 2013. [doi:10.1007/978-3-642-42033-7˙8].

DFPR14.   Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. In *Advances in Cryptology – ASIACRYPT 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 406–425. Springer, 2014. [doi:10.1007/978-3-662-45608-8˙22, arXiv:1301.3662].

Gut12.   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].

GW07.   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].

Har11.   Lucien Hardy. Reformulating and reconstructing quantum theory. Eprint, 2011. [arXiv:1104.2066].

Har12.   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].

Har15.   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].

Kra01.   Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is SSL?). In *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 310–331. Springer, 2001. [doi:10.1007/3-540-44647-8˙19].

KRBM07.   Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible
          quantum information does not imply security. *Physical Review Letters*, 98:140502,
          April 2007. [doi:10.1103/PhysRevLett.98.140502, arXiv:quant-ph/0512021].

KY06.   Jonathan Katz and Moti Yung. Characterization of security notions for proba-
          bilistic private-key encryption. *Journal of Cryptology*, 19(1):67–95, January 2006.
          [doi:10.1007/s00145-005-0310-8].

Mau02.   Ueli Maurer. Indistinguishability of random systems. In *International Conference on
          the Theory and Applications of Cryptographic Techniques*, pages 110–132. Springer,
          2002.

Mau12.   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].

MPR07.   Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability ampli-
          fication. In *Annual International Cryptology Conference*, pages 130–149. Springer,
          2007.

MR11.   Ueli Maurer and Renato Renner. Abstract cryptography. In *Proceedings of Innova-
          tions in Computer Science, ICS 2011*, pages 1–21. Tsinghua University Press, 2011.

MR16.   Ueli Maurer and Renato Renner. From indifferentiability to constructive cryptog-
          raphy (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].

MRT12.   Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann. Confidentiality and in-
          tegrity: A constructive perspective. In Ronald Cramer, editor, *Theory of Cryp-
          tography*, pages 209–229, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.
          [doi:10.1007/978-3-642-28914-9_12].

MT10.   Ueli Maurer and Björn Tackmann. On the soundness of authenticate-then-encrypt:
          Formalizing the malleability of symmetric encryption. In *Proceedings of the 17th
          ACM Conference on Computer and Communication Security*, pages 505–515. ACM,
          2010.

PMM+17.   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].

Por17.   Christopher Portmann. Quantum authentication with key recycling. In *Advances
          in Cryptology – EUROCRYPT 2017, Proceedings, Part III*, volume 10212 of *Lecture
          Notes in Computer Science*, pages 339–368. Springer, 2017. [doi:10.1007/978-3-319-
          56617-7_12, arXiv:1610.03422].

PR14.   Christopher Portmann and Renato Renner. Cryptographic security of quantum key
          distribution. Eprint, 2014. [arXiv:1409.3525].

PW00.   Birgit Pfitzmann and Michael Waidner. Composition and integrity preserva-
          tion of secure reactive systems. In *Proceedings of the 7th ACM Conference on
          Computer and Communications Security, CSS '00*, pages 245–254. ACM, 2000.
          [doi:10.1145/352600.352639].

PW01.   Birgit Pfitzmann and Michael Waidner. A model for asynchronous reactive systems
          and its application to secure message transmission. In *IEEE Symposium on Security
          and Privacy*, pages 184–200. IEEE, 2001. [doi:10.1109/SECPRI.2001.924298].

Ren05.   Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal
          Institute of Technology (ETH) Zurich, September 2005. [arXiv:quant-ph/0512258].

SBPC+09. 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].

Shr04.   Tom Shrimpton. A characterization of authenticated-encryption as a form of chosen-ciphertext security. *IACR Cryptology ePrint Archive*, 2004:272, 2004.

TL17.   Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, July 2017. [doi:10.22331/q-2017-07-14-14, arXiv:1506.08458].

Unr10.   Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 486–505. Springer, 2010. [doi:10.1007/978-3-642-13190-5˙25, arXiv:0910.2912].

VPdR17.   V. Vilasini, Christopher Portmann, and Lídia del Rio. Composable security in relativistic quantum cryptography. Eprint, 2017. [arXiv:1708.00433].

Zha12.   Mark Zhandry. How to construct quantum random functions. In *Proceedings of the 43rd Symposium on Foundations of Computer Science, FOCS '12*, pages 679–687. IEEE, 2012. [IACR e-print: 2012/182].

A   Notation

Pauli Operators. We write P_k or $P_{x,z}$ to denote a Pauli operator on m qubits, where $k = (x, z)$ are concatenation of two m-bits strings indicating in which qubit bit flips and phase flips occur.

$$P_k = P_{x,z} = \bigotimes_{i=1}^{m} P_{x_i z_i},$$

where

$$P_{ab} = \begin{cases} I & a = 0, b = 0, \\ X & a = 1, b = 0, \\ Z & a = 0, b = 1, \\ XZ & a = 1, b = 1. \end{cases}$$

Note that $P_k = P_k^\dagger$, therefore we simply write $P_k \rho P_k$ when applying a Pauli-operator P_k on state ρ. To undo Pauli-operator P_k, we simply apply P_k again, namely, $P_k P_k \rho P_k P_k = \rho$.

Bell Basis. We write $|\phi_0\rangle$ as the maximum entangled state of $2m$ qubits.

$$|\phi_0\rangle = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right)^{\otimes m}$$

and $|\phi_k\rangle$ as applying Pauli operator $I^{\otimes m} \otimes P_k$ on $|\phi_0\rangle$

$$|\phi_k\rangle = I^{\otimes m} \otimes P_k |\phi_0\rangle.$$

Then $\{|\phi_k\rangle\}_{k \in \{0,1\}^{2m}}$ forms the Bell basis for $2m$ qubits.

Symplectic Inner Product. Symplectic inner product of two string $k = (x, z)$ and $l = (x', z')$ of length $2m$ is given by

$$\mathrm{spl}(k, l) = \sum_{i=1}^{m} x_i z_i' - x_i' z_i.$$

Two Pauli operators P_k and P_l with $k = (x, z)$ and $l = (x', z')$ commute (anti-commute) if $\mathrm{spl}(k, l)$ equals to 0 (equals to 1) module 2. Hence for any P_k and P_l,

$$P_k P_l = (-1)^{\mathrm{spl}(k,l)} P_l P_k.$$

For any strings k and l we have,

$$\sum_{k \in \{0,1\}^m} (-1)^{\mathrm{spl}(k,l)} = \begin{cases} 2^n & l = 0, \\ 0 & l \neq 0, \end{cases}$$

where $l = 0$ means all bits of the string l are 0.

B   Composition

In this section we prove that Eqs. (4) and (5) hold for the construction notion from Definition 1.

Theorem 5 (Composition theorem). *Suppose that π_1 constructs S from R within ε_1 and π_2 constructs T from S within ε_2, i.e.,*

$$\mathsf{R} \xrightarrow{\pi_1, \varepsilon_1} \mathsf{S} \qquad and \qquad \mathsf{S} \xrightarrow{\pi_2, \varepsilon_2} \mathsf{T}.$$

Then it holds that

$$\mathsf{R} \xrightarrow{\pi_2 \pi_1, \varepsilon_1 + \varepsilon_2} \mathsf{T}.$$

Furthermore, for any resource U, we have

$$[\mathsf{R}, \mathsf{U}] \xrightarrow{\pi_1, \varepsilon'} [\mathsf{S}, \mathsf{U}],$$

with

$$\varepsilon'(\mathsf{D}) := \varepsilon_1(\mathsf{D}[\cdot, \mathsf{U}]).$$

Proof. Let sim and sim' be the simulators for which for all D, $d^{\mathsf{D}}(\pi_1 \mathsf{R}, \mathsf{S}\mathsf{sim}) \leq \varepsilon(\mathsf{D})$ and $d^{\mathsf{D}}(\pi_2 \mathsf{S}, \mathsf{T}\mathsf{sim}') \leq \varepsilon(\mathsf{D})$. Then from the triangle inequality we have

$$\begin{aligned} d^{\mathsf{D}}(\pi_2 \pi_1 \mathsf{R}, \mathsf{T}\mathsf{sim}'\mathsf{sim}) &\leq d^{\mathsf{D}}(\pi_2 \pi_1 \mathsf{R}, \pi_2 \mathsf{S}\mathsf{sim}) + d^{\mathsf{D}}(\pi_2 \mathsf{S}\mathsf{sim}, \mathsf{T}\mathsf{sim}'\mathsf{sim}) \\ &= d^{\mathsf{D}}(\pi_1 \mathsf{R}, \mathsf{S}\mathsf{sim}) + d^{\mathsf{D}}(\pi_2 \mathsf{S}, \mathsf{T}\mathsf{sim}') \\ &\leq \varepsilon_1(\mathsf{D}) + \varepsilon_2(\mathsf{D}). \end{aligned}$$

Furthermore

$$\begin{aligned} d^{\mathsf{D}}(\pi_1 [\mathsf{R}, \mathsf{U}], [\mathsf{S}, \mathsf{U}]\mathsf{sim}) &= d^{\mathsf{D}}([\pi_1 \mathsf{R}, \mathsf{U}], [\mathsf{S}\mathsf{sim}, \mathsf{U}]) \\ &\leq d^{\mathsf{D}[\cdot, \mathsf{U}]}(\pi_1 \mathsf{R}, \mathsf{S}\mathsf{sim}) \leq \varepsilon_1(\mathsf{D}[\cdot, \mathsf{U}]). \qquad \square \end{aligned}$$

C Quantum One-Time Pad

Here we show that the quantum one-time pad constructs a one-time Pauli-malleable confidential quantum channel $\overline{\mathsf{PMCC}}^{1,m}$ from a one-time insecure quantum channel $\overline{\mathsf{IC}}^{1,m}$ and a key resource KEY^{2m}. Note that $\overline{\mathsf{PMCC}}$ and $\overline{\mathsf{IC}}$ are a slightly modified versions of PMCC and IC. Which work as follows: after getting an input at interface E, the channels reject any input at interface A. A weaker statement has appeared in [DFPR14], where it was proven that the one-time pad constructs a confidential channel— i.e., one which allows the adversary to make arbitrary changes, but only leaks the message size— which is strictly weaker than the resource $\overline{\mathsf{PMCC}}^{1,m}$ proven to be constructed here.

The protocol is described in Figure 15. The construction also gives Eve certain computation power. We present the simulator $\mathsf{sim}^{\text{q-otp}}$ and the quantum computer of Eve $\mathsf{QC}^{\text{q-otp}}$ in Figure 16 such that the ideal channel connecting with the simulator and Eve's quantum computer can be proved equivalent to the system of Alice's and Bob's converters, quantum computers connecting with the insecure channel and the key resource.

Lemma 7. *Let* $\pi_{AB} = (\pi_A, \pi_B), \mathsf{QC}_A^{1,m,m}, \mathsf{QC}_B^{1,m,m}, \mathsf{sim}^{\text{q-otp}}, \mathsf{QC}^{\text{q-otp}}$ *denote the converters, simulator and computing resources described in Figure 15 and Figure 16. Then for any distinguisher* D, *we have*

$$d^{\mathsf{D}}\left(\pi_{AB}\left[\overline{\mathsf{IC}}^{1,m}, \mathsf{KEY}^{2m}, \mathsf{QC}_A^{1,m,m}, \mathsf{QC}_B^{1,m,m}\right], \mathsf{sim}^{\text{q-otp}}\left[\overline{\mathsf{PMCC}}^{1,m}, \mathsf{QC}^{\text{q-otp}}\right]\right) = 0.$$

Proof. We first consider the simpler case that distinguisher only inputs at interface E. In both worlds, the distinguisher prepares an arbitrary state ρ^{AE} and inputs ρ^A at interface E. In the real world, the protocol applies a Pauli operator P_k on the state and then output at interface B. The distinguisher has state

$$\Phi_{real} = \frac{1}{2^{2m}}\sum_{k\in\{0,1\}^{2m}} P_k^A \rho^{AE} P_k^A.$$

In the ideal world, since no newMsg has arrived yet, the simulator output $\perp$ to channel $\overline{\mathsf{PMCC}}^{1,m}$ and the channel outputs a fully mixed state $\frac{1}{2^m}I$ at interface B. The distinguisher has state

$$\Phi_{ideal} = \frac{1}{2^m}I \otimes \rho^E$$

It is easy to see that for any mixed state ρ^{AE},

$$\frac{1}{2^{2m}}\sum_{k\in\{0,1\}^{2m}} P_k^A \rho^{AE} P_k^A = \frac{1}{2^m}I \otimes \rho^E$$
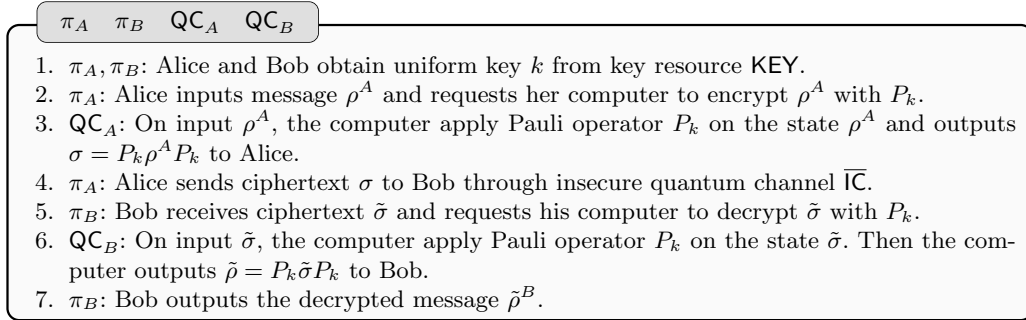

π_A π_B QC_A QC_B

1. π_A, π_B: Alice and Bob obtain uniform key k from key resource KEY.
2. π_A: Alice inputs message ρ^A and requests her computer to encrypt ρ^A with P_k.
3. QC_A: On input ρ^A, the computer apply Pauli operator P_k on the state ρ^A and outputs $\sigma = P_k \rho^A P_k$ to Alice.
4. π_A: Alice sends ciphertext σ to Bob through insecure quantum channel $\overline{\mathsf{IC}}$.
5. π_B: Bob receives ciphertext $\tilde{\sigma}$ and requests his computer to decrypt $\tilde{\sigma}$ with P_k.
6. QC_B: On input $\tilde{\sigma}$, the computer apply Pauli operator P_k on the state $\tilde{\sigma}$. Then the computer outputs $\tilde{\rho} = P_k \tilde{\sigma} P_k$ to Bob.
7. π_B: Bob outputs the decrypted message $\tilde{\rho}^B$.

Fig. 15. Converters and computer resources to construct $\overline{\mathsf{PMCC}}^{1,m}$ from $\overline{\mathsf{IC}}^{1,m}$. The quantum computer $\mathsf{QC}_A^{1,m,m}$ and $\mathsf{QC}_B^{1,m,m}$ will be requested 1 time. The plaintext and ciphertext both have length m. KEY^{2m} gives a shared key of length $2m$.
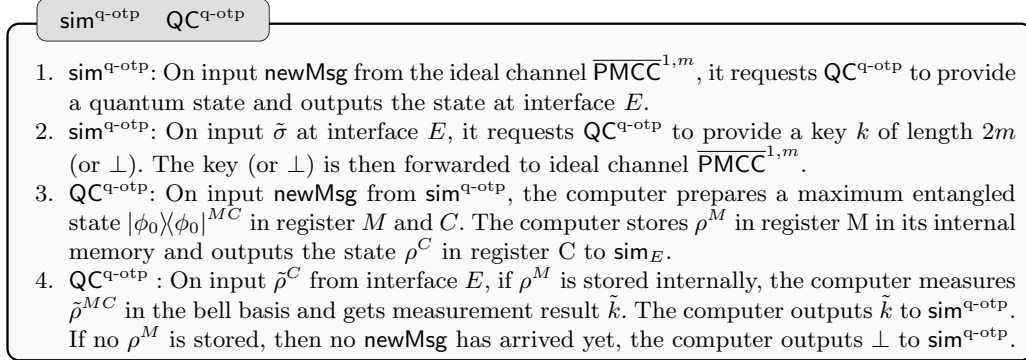

$\mathsf{sim}^{\text{q-otp}}$ $\mathsf{QC}^{\text{q-otp}}$

1. $\mathsf{sim}^{\text{q-otp}}$: On input newMsg from the ideal channel $\overline{\mathsf{PMCC}}^{1,m}$, it requests $\mathsf{QC}^{\text{q-otp}}$ to provide a quantum state and outputs the state at interface E.
2. $\mathsf{sim}^{\text{q-otp}}$: On input $\tilde{\sigma}$ at interface E, it requests $\mathsf{QC}^{\text{q-otp}}$ to provide a key k of length $2m$ (or $\perp$). The key (or $\perp$) is then forwarded to ideal channel $\overline{\mathsf{PMCC}}^{1,m}$.
3. $\mathsf{QC}^{\text{q-otp}}$: On input newMsg from $\mathsf{sim}^{\text{q-otp}}$, the computer prepares a maximum entangled state $|\phi_0\rangle\langle\phi_0|^{MC}$ in register M and C. The computer stores ρ^M in register M in its internal memory and outputs the state ρ^C in register C to sim_E.
4. $\mathsf{QC}^{\text{q-otp}}$: On input $\tilde{\rho}^C$ from interface E, if ρ^M is stored internally, the computer measures $\tilde{\rho}^{MC}$ in the bell basis and gets measurement result $\tilde{k}$. The computer outputs $\tilde{k}$ to $\mathsf{sim}^{\text{q-otp}}$. If no ρ^M is stored, then no newMsg has arrived yet, the computer outputs $\perp$ to $\mathsf{sim}^{\text{q-otp}}$.

Fig. 16. The simulator $\mathsf{sim}^{\text{q-otp}}$ and computer resource $\mathsf{QC}^{\text{q-otp}}$ connecting to the ideal resource $\overline{\mathsf{PMCC}}^{1,m}$. $\mathsf{QC}^{\text{q-otp}}$ is capable of doing 1 encryption and 1 decryption.

and therefore we have

$$\Phi_{real} = \Phi_{ideal}.$$

Now we consider the more complicated case that distinguisher first input at interface A and then at interface E. In both worlds, the distinguisher prepares an arbitrary state ρ^{AE} and a CPTP map Λ. In the real world, the distinguisher inputs ρ^A at interface A. After getting the flipped (Alice applying a Pauli operator P_k) state $P_k \rho^A P_k$ at interface E, the distinguisher applies the CPTP map Λ on register A and E. Then the distinguisher inputs the result state $\tilde{\rho}^A$ in register A into the insecure channel $\overline{\mathsf{IC}}^{1,m}$. Then the distinguisher gets the flipped (Bob applying a Pauli operator P_k) state output at interface B. The distinguisher holds state Φ_{real}

$$\Phi_{real} = \frac{1}{2^{2m}} \sum_{k \in \{0,1\}^{2m}} P_k^A \Lambda^{AE}(P_k^A \rho^{AE} P_k^A) P_k^A.$$

In the ideal world, the distinguisher inputs ρ^A at interface A. The simulator prepares a maximum entangled state $|\phi_0\rangle\langle\phi_0|^{MC}$ in register M and C and outputs the state σ^C in register C at interface E. The distinguisher applies the CPTP map Λ on register C and E. Then the distinguisher inputs the result state $\tilde{\sigma}^C$ in register C into the channel. The simulator measures the state in register M and C on bell basis, get the measurement result k and the channel applies Pauli operator P_k on the state in register A. After getting the modified state output from interface B, the distinguisher holds state Φ_{ideal}.

$$\tilde{\sigma}^{AMCE} = \Lambda^{CE}(|\phi_0\rangle\langle\phi_0|^{MC} \otimes \rho^{AE})$$

$$\Phi_{ideal} = \mathrm{Tr}_{MC} \sum_{k\in\{0,1\}^{2m}} (P_k^A \otimes |\phi_k\rangle\langle\phi_k|^{MC})\tilde{\sigma}^{AMCE}(P_k^A \otimes |\phi_k\rangle\langle\phi_k|^{MC}).$$

We prove that for any ρ^{AE} and CPTP map Λ^{XE}, where register X is A in the real world and C in the ideal world, we have $\Phi_{real} = \Phi_{ideal}$.

For any CPTP map Λ^{XE} applying on state ρ^{XE} on register X and E, we can decompose the map as

$$\begin{aligned}
\Lambda^{XE}(\rho^{XE}) &= \sum_i \Gamma_i^{XE}\rho^{XE}\Gamma_i^{XE\dagger} \\
&= \sum_i (\sum_p P_p^X \otimes \Gamma_{i,p}^E)\rho^{XE}(\sum_q P_q^X \otimes \Gamma_{i,q}^{E\dagger}) \\
&= \sum_{i,p,q} (P_p^X \otimes \Gamma_{i,p}^E)\rho^{XE}(P_q^X \otimes \Gamma_{i,q}^{E\dagger})
\end{aligned} \qquad (14)$$

Plugging Eq. (14) into $\tilde{\sigma}^{AMCE}$, we get

$$\begin{aligned}
\tilde{\sigma}^{AMCE} &= \Lambda^{CE}(|\phi_0\rangle\langle\phi_0|^{MC} \otimes \rho^{AE}) \\
&= \sum_{i,p,q} (P_p^C \otimes \Gamma_{i,p}^E)(|\phi_0\rangle\langle\phi_0|^{MC} \otimes \rho^{AE})(P_q^C \otimes \Gamma_{i,q}^{E\dagger}) \\
&= \sum_{i,p,q} P_p^C|\phi_0\rangle\langle\phi_0|^{MC}P_q^C \otimes (\Gamma_{i,p}^E\rho^{AE}\Gamma_{i,q}^{E\dagger}) \\
&= \sum_{i,p,q} |\phi_p\rangle\langle\phi_q|^{MC} \otimes (\Gamma_{i,p}^E\rho^{AE}\Gamma_{i,q}^{E\dagger}),
\end{aligned}$$

where $|\phi_p\rangle^{MC} = P_p^C |\phi_0\rangle^{MC}$, see Appendix A.

Now we can express Φ_{ideal} as

$$
\begin{aligned}
\Phi_{ideal} &= \mathrm{Tr}_{MC} \sum_{k,i,p,q} (P_k^A \otimes |\phi_k\rangle\langle\phi_k|^{MC}) \tilde{\sigma}^{AMCE} (P_k^A \otimes |\phi_k\rangle\langle\phi_k|^{MC}) \\
&= \mathrm{Tr}_{MC} \sum_{k,i,p,q} (P_k^A \otimes |\phi_k\rangle\langle\phi_k|^{MC})((\Gamma_{i,p}^E \rho^{AE} \Gamma_{i,q}^{E\dagger}) \otimes |\phi_p\rangle\langle\phi_q|^{MC})(P_k^A \otimes |\phi_k\rangle\langle\phi_k|^{MC}) \\
&= \mathrm{Tr}_{MC} \sum_{k,i,p,q} (P_k^A \otimes \Gamma_{i,p}^E \rho^{AE} P_k^A \otimes \Gamma_{i,q}^{E\dagger}) \otimes (|\phi_k\rangle\langle\phi_k|^{MC}|\phi_p\rangle\langle\phi_q|^{MC}|\phi_k\rangle\langle\phi_k|^{MC}) \\
&= \mathrm{Tr}_{MC} \sum_{k,i} (P_k^A \otimes \Gamma_{i,k}^E \rho^{AE} P_k^A \otimes \Gamma_{i,k}^{E\dagger}) \otimes |\phi_k\rangle\langle\phi_k|^{MC} \\
&= \sum_{k,i} P_k^A \otimes \Gamma_{i,k}^E \rho^{AE} P_k^A \otimes \Gamma_{i,k}^{E\dagger}
\end{aligned}
$$

Plugging Eq. (14) into Φ_{real}, we get

$$
\begin{aligned}
\Phi_{real} &= \frac{1}{2^{2m}} \sum_k P_k^A \Lambda^{AE} (P_k^A \rho^{AE} P_k^A) P_k^A \\
&= \frac{1}{2^{2m}} \sum_k P_k^A (\sum_{i,p,q} (P_p^A \otimes \Gamma_{i,p}^E) P_k^A \rho^{AE} P_k^A (P_q^A \otimes \Gamma_{i,q}^{E\dagger})) P_k^A \\
&= \frac{1}{2^{2m}} \sum_{k,i,p,q} (P_k^A P_p^A P_k^A \otimes \Gamma_{i,p}^E) \rho^{AE} (P_k^A P_q^A P_k^A \otimes \Gamma_{i,q}^{E\dagger}).
\end{aligned}
$$

Note that $P_k P_p = (-1)^{\mathrm{spl}(k,p)} P_p P_k$ (see Appendix A), so we have

$$
\begin{aligned}
\sum_{k,p,q} P_k P_p P_k(\cdot) P_k P_q P_k &= \sum_{k,p,q} (-1)^{\mathrm{spl}(k,p)} P_p P_k P_k(\cdot)(-1)^{\mathrm{spl}(k,q)} P_q P_k P_k \\
&= \sum_{k,p,q} (-1)^{\mathrm{spl}(k,p)+\mathrm{spl}(k,q)} P_p(\cdot) P_q \\
&= \sum_{p,q} P_p(\cdot) P_q \sum_k (-1)^{\mathrm{spl}(k,p \oplus q)} \\
&= \sum_{p \oplus q = 0} P_p(\cdot) P_q \cdot 2^{2m} \\
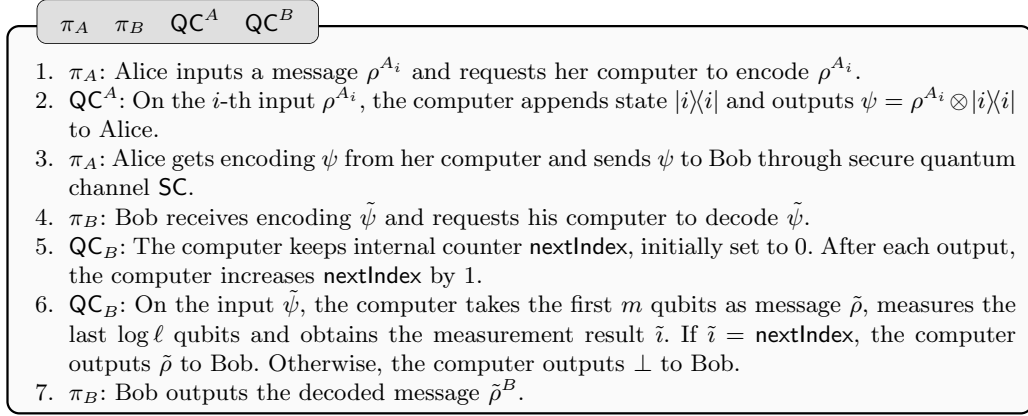&= 2^{2m} \sum_p P_p(\cdot) P_p.
\end{aligned}
$$

π_A π_B QC^A QC^B

1. π_A: Alice inputs a message ρ^{A_i} and requests her computer to encode ρ^{A_i}.
2. QC^A: On the i-th input ρ^{A_i}, the computer appends state $|i\rangle\langle i|$ and outputs $\psi = \rho^{A_i} \otimes |i\rangle\langle i|$ to Alice.
3. π_A: Alice gets encoding ψ from her computer and sends ψ to Bob through secure quantum channel SC.
4. π_B: Bob receives encoding $\tilde{\psi}$ and requests his computer to decode $\tilde{\psi}$.
5. QC_B: The computer keeps internal counter nextIndex, initially set to 0. After each output, the computer increases nextIndex by 1.
6. QC_B: On the input $\tilde{\psi}$, the computer takes the first m qubits as message $\tilde{\rho}$, measures the last $\log \ell$ qubits and obtains the measurement result $\tilde{i}$. If $\tilde{i} =$ nextIndex, the computer outputs $\tilde{\rho}$ to Bob. Otherwise, the computer outputs $\perp$ to Bob.
7. π_B: Bob outputs the decoded message $\tilde{\rho}^B$.

Fig. 17. Converters and computing resources to construct $\mathsf{OSC}^{\ell,m}$ from $\mathsf{SC}^{\ell,m+\log \ell}$. $\mathsf{QC}_A^{\ell,m,m+\log \ell}$ and $\mathsf{QC}_B^{\ell,m,m+\log \ell}$ will be requested ℓ times. The message has length m and encoding has length $m + \log \ell$.

.

Therefore we can further simplify Φ_{real}

$$\Phi_{real} = \frac{1}{2^{2m}} \sum_{k,i,p,q} (P_k^A P_p^A P_k^A \otimes \Gamma_{i,p}^E) \rho^{AE} (P_k^A P_q^A P_k^A \otimes \Gamma_{i,q}^{E\dagger})$$

$$= \frac{1}{2^{2m}} 2^{2m} \sum_{p,i} (P_p^A \otimes \Gamma_{i,p}^E) \rho^{AE} (P_p^A \otimes \Gamma_{i,p}^{E\dagger})$$

$$= \sum_{p,i} P_p^A \otimes \Gamma_{i,p}^E \rho^{AE} P_p^A \otimes \Gamma_{i,p}^{E\dagger}.$$

Therefore for any state ρ^{AE} and CPTP map Λ^{XE}, $\Phi_{real} = \Phi_{ideal}$. $\square$

D   Constructing $\mathsf{OSC}^{\ell,m}$ from $\mathsf{SC}^{\ell,m+\log \ell}$

In this section we present a construction from a secure quantum channel to an ordered secure quantum channel. In the protocol, Alice appends to each message an index. When Bob receives the message, he checks the index. He accepts the message only when the index is expected. The protocol works as following.

Theorem 6. *Let* $\pi_{AB} = (\pi_A, \pi_B)$, $\mathsf{QC}_A^{\ell,m,m+\log \ell}$ *and* $\mathsf{QC}_B^{\ell,m,m+\log \ell}$ *denote converters and computing resources corresponding to the protocol from Figure 17. Let* QC_E^ℓ *be a computing resource for Eve, capable of doing* ℓ *add operations. Then* π_{AB} *constructs an ordered secure quantum channel* $\mathsf{OSC}^{\ell,m}$ *from a secure quantum channel* $\mathsf{SC}^{\ell,m+\log \ell}$ *with* $\epsilon = 0$, *i.e.,*

$$\left[\mathsf{SC}^{\ell,m+\log \ell}, \mathsf{QC}_A^{\ell,m,m+\log \ell}, \mathsf{QC}_B^{\ell,m,m+\log \ell}\right] \xrightarrow{\pi_{AB},0} \left[\mathsf{OSC}^{\ell,m}, \mathsf{QC}_E^\ell\right].$$

Proof. In order to prove this theorem, we need to find a simulator and a program for Eve's computer such that the real system and ideal system are indistinguishable with 0 advantage.

The simulator sim_E works as following. On input newMsg from the ideal resource $\mathsf{OSC}^{\ell,m}$, sim_E outputs newMsg at interface E. On input i at interface E, sim_E inputs i to QC_E^ℓ, requests it to output a send or skip signal and forwards the signal to ideal resource OSC^ℓ.

Eve's computer QC_E^ℓ works as following. The computer keeps an internal counter $\mathsf{nextIndex}$, initially set to 0. On input i from sim_E, if $i = \mathsf{nextIndex}$, it outputs send to sim_E, otherwise, it outputs skip to sim_E. After the output, it increases $\mathsf{nextIndex}$ by 1. The computer will be requested at most ℓ times.

One can see that the real system $\pi_{AB}\left[\mathsf{SC}^{\ell,m+\log\ell}, \mathsf{QC}_A^{\ell,m,m+\log\ell}, \mathsf{QC}_B^{\ell,m,m+\log\ell}\right]$ and the ideal world $\mathsf{sim}_E\left[\mathsf{OSC}^{\ell,m}, \mathsf{QC}_E^\ell\right]$ are two equivalent systems. If the distinguisher reorders the messages, in both worlds, Bob will only receive messages with consecutive indices. Therefore, two systems are equivalent and the distinguishing advantage is 0. □

Remark. Theorem 6 is meaningful only if the protocol also provides correctness. This is trivially the case, since if the distinguisher is honest, i.e., always preserves the order of messages, then Bob will receive them all in the correct order.

E   AGM-QCCA2 Security Definition ([AGM18]).

Here we restate what it means for a SQES $\mathfrak{S}$ to be secure in the AGM-QCCA2 sense according to [AGM18]. Contrary to the QAE definition, the authors did not formulate AGM-QCCA2 in terms of a distinction problem (between a real and an ideal setting); rather, the interaction of a distinguisher D with two different games is considered:

- The first offers (true) encryption and decryption oracles, as well as a challenge phase: D is required to input a plaintext, for which it will get back either the true encryption, or the encryption of a random plaintext (τ^M, half of a maximally-entangled state). D wins the game if it guesses which of the two states was actually encrypted. After the challenge phase, D has still access to the same oracles, and could therefore in principle trivially win the game by submitting the challenge ciphertext and compare the result with the challenge plaintext;
- The second game countermeasures this by exposing towards D the same game, but where the challenge plaintext is always replaced by τ^M, and if D tries to cheat by submitting the challenge ciphertext to the decryption oracle, it instantly loses the game (and wins it with probability $\frac{1}{2}$ otherwise).

Then the advantage of D is measured as the probability of winning the first game minus the probability of cheating in the second. The rationale behind this definition is that D should not be able to have a larger probability of winning the first game than of cheating in the second. We now state our adaption of the corresponding definition from [AGM18] (Definition 9 therein).

Definition 13 (AGM-QCCA2 Security [AGM18]). *For SQES (implicit in all defined systems)* $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$, *we define the* AGM-QCCA2-*advantage of* $\mathfrak{S}$ *for distinguisher* $\mathsf{D} \in \mathbb{D}$ *as*

$$\mathbf{Adv}_{\mathfrak{S},\mathsf{D}}^{\mathrm{agm\text{-}qcca2}} := \Pr\left[\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}test}}[\mathsf{D}] = 1\right] - \Pr\left[\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}fake}}[\mathsf{D}] = 1\right],$$

where the interactions of D *with game systems* $\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}test}}$ *and* $\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}fake}}$ *are defined in Figure 18.*

Experiments $\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}test}}[\mathsf{D}]$ and $\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}fake}}[\mathsf{D}]$ for SQES $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$

$b \xleftarrow{\$} \{0,1\}$
$k \leftarrow \mathtt{Gen}()$
$\mathrm{cheat} \leftarrow 0$
$\varrho^M \leftarrow \mathsf{D}^{\mathtt{Enc}_k(\cdot),\mathtt{Dec}_k(\cdot)}$
$\hat{r} \xleftarrow{p_k} \mathcal{R}$ ▷ *Keep* $\hat{r}$
$\hat{M}\tilde{M} \leftarrow |\phi_0\rangle$

$b \xleftarrow{\$} \{0,1\}$
$k \leftarrow \mathtt{Gen}()$
$\varrho^M \leftarrow \mathsf{D}^{\mathtt{Enc}_k(\cdot),\mathtt{Dec}_k(\cdot)}$
if $b = 1$ **then**
    $\sigma^C \leftarrow \mathtt{Enc}_k(\varrho^M)$
else
    $\sigma^C \leftarrow \mathtt{Enc}_k(\tau^M)$
$b' \leftarrow \mathsf{D}^{\mathtt{Enc}_k(\cdot),\mathtt{Dec}_k(\cdot)}(\sigma^C)$
return $\mathbb{1}\{b' = b\}$

$\hat{\sigma}^{\hat{C}} \leftarrow V_k(\varrho^{\hat{M}} \otimes \Pi_{k,\hat{r}}^T)V_k^\dagger$ ▷ *Ignore* ϱ^M
$b' \leftarrow \mathsf{D}^{\mathtt{Enc}_k(\cdot),\mathbf{Dec}(\cdot)}(\hat{\sigma}^{\hat{C}})$
return cheat ? 1 : b ▷ *Ignore* b'

oracle $\mathbf{Dec}(\sigma^C)$:
    $MT \leftarrow V_k^\dagger \sigma^C V_k$
    if $\{P_{\omega_k}^T, \mathbb{1} - P_{\omega_k}^T\}(\omega^T) \Rightarrow 0$ **then**
        if $\{\Pi_{k,\hat{r}}, \mathbb{1} - \Pi_{k,\hat{r}}\}(\omega^T) \Rightarrow 0$ **then**
            if $\{\Pi_+, \mathbb{1} - \Pi_+\}(\varphi^{M\tilde{M}}) \Rightarrow 0$ **then**
                $\mathrm{cheat} \leftarrow 1$
    else
        return $\hat{D}_k(\rho^{MT})$ ▷ *Invalid ciphertext*
    return ϱ^M

Fig. 18. AGM-QCCA2 games $\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}test}}$ (**left**) and $\mathsf{G}^{\mathrm{agm\text{-}qcca2\text{-}fake}}$ (**right**).