Composable and Finite Computational Security of Quantum Message Transmission

Fabio Banfi[0000−0001−9788−4700], Ueli Maurer, Christopher Portmann[0000−0003−2679−1202], and Jiamin Zhu[0000−0002−9722−9404]

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 [15, 17]. 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., [8] and [24] 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 [11], QCCA1 in [1], and QCCA2 as well as notions of quantum unforgeability and quantum authenticated encryption in [2]. These are just some of the security games one can imagine — in the classical, symmetric-key setting, [24] 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 [32] 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 [28, 30, 31], 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 [1, 2, 11] 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 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

[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 Sect. 1.6.

sometimes finds that the definitions used are inappropriate but the protocols are actually secure like for quantum key distribution [10,25,39], that the definitions are still secure (up to a loss of security parameter) like for delegated quantum computation [18], or that not only the definitions but also the protocols are insecure like in relativistic and bounded storage bit commitment and (biased) coin tossing [44].[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* [7], 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 Sect. 1.3 below we explain the intuition behind this security paradigm.

We then show that (slightly modified) protocols from the literature [1, 2] satisfy these definitions. These protocols use the quantum one-time pad and quantum information-theoretic authentication as subroutine [6,36], 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 Sect. 1.4.

[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.

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 Sect. 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 $\mathbb{S} = \{\mathsf{S}_k\}_{k\in\mathbb{N}}$, 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 $\mathbb{S}$.

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 Sect. 1.1, we use the Abstract and Constructive Cryptography (AC) framework of Maurer and Renner [28, 30, 31] 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 [2] 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 [1] 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 [2].

We first note that encryption schemes are defined to be stateless in [1, 2, 11] 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 [2]. In particular, its classical analogue is easily shown to be equivalent to a standard IND-CCA2 notion, whereas the notion put forth in [2], 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 [15] 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 [17].

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

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

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

[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 [9, 26, 33].

[4] $I_{\mathrm{acc}}(K;E) \coloneqq \max_{\Gamma} I(K;\Gamma(E))$, 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.

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 [25,38]. A scheme satisfying the latter notion — the trace distance criterion — constructs a secure key even when the quantum channel used is completely insecure [10,38,39]. 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 [10,38], the trace distance criterion has become a reference for what a quantum key distribution scheme must satisfy [40,42].

Previous work on computational security of quantum message transmission [1, 2, 11] 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 Sect. 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 [3, 4, 34, 35] and Canetti [12–14], who each defined their own framework, dubbed *reactive simulatability* and *universal composability* (UC), respectively. Unruh adapted UC to the quantum setting [43], whereas Maurer and Renner's AC applies to any model of computation, classical or quantum [30]. 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 $\{\mathcal{E}^{(k)}\}_k$, where $k \in \mathbb{N}$ is a security parameter, and distinguishability between networks of machines is then defined asymptotically in k.[6]

Concrete security [7] 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

[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.

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* [27, 29]. Generalizations to the quantum case have been proposed by Gutoski and Watrous [19, 20] — and called *quantum strategies* — by Chiribella, D'Ariano and Perinotti [16] — called *quantum combs* — and by Hardy [21–23] — *operator tensors*. A model for discrete quantum systems that can additionally model time and superpositions of causal structures is the *causal boxes* framework [37].

None of the previous works on computational security of quantum message transmission satisfy any of the three criteria outlined in Sect. 1.1. These criteria are however standard by now for quantum key distribution [38, 42]. In the classical case, they have also been used for computational security, e.g., [17, 32].

1.8 Structure of this Paper

In Sect. 2 we introduce the elements needed from AC [28,30,31], and from the discrete system model with which we instantiate AC, namely quantum combs [16]. This allows us to define the notion of a finite construction of a resource (e.g., a secure channel) from another resource (e.g., an insecure channel and a key). In Sect. 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 Sect. 1.4. Finally, in Sect. 4 we compare our security definitions to some game-based ones from the literature [2] and prove the results described in Sect. 1.5.

2 Abstract & Constructive Cryptography

In this section we give a brief overview of the Abstract and Constructive Cryptography (AC) framework, which is sufficient to understand the main claims of this work. A more extended introduction to AC is provided in the full version [5], which is needed to understand the proofs. We refer to [28, 30, 31, 38] for further reading.

The AC framework views cryptography as a resource theory in which a protocol is a transformation between resources. Players may share certain resources — e.g., secret key, an authentic channel, a public-key infrastructure, common reference strings, etc. — and use these to construct other resources — e.g., an authentic channel, a secure channel, secret key, a bit commitment resource, an idealization of a multipartite function, etc. More abstractly, a protocol π uses some resource R (the *assumed* resource) 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 provided in the full version [5].

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.,

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

In this work, resources R, S or T are instantiated with a model of quantum interactive systems called *quantum strategies* [19, 20] or *quantum combs* [16] in the literature. We use the term *interface* to denote the inputs and outputs accessible to a specific player, e.g., most resources considered in this work have 3 interfaces for Alice, Bob and Eve. In the following we often provide pseudo-code describing a resource. However, this always corresponds to a specific quantum strategy/comb. When multiple resources $\mathsf{R}_1, \ldots, \mathsf{R}_n$ are accessible to players, we write $[\mathsf{R}_1, \ldots, \mathsf{R}_n]$ for the new resource resulting from combining the individual R_i in parallel. The mathematical meaning of this expression is explained in the full version [5].

We often write a protocol $\pi = (\pi_A, \pi_B)$ as a tuple, where each element π_A corresponds to the operations of a specific player (e.g., A for Alice), and only interacts at the corresponding interface of the shared resources. Formally, these are functions mapping a resource to another resource. Running several protocols then corresponds to the composition of the functions as in Eq. (4).

Finally, the error of a construction ε that appears in Eq. (3) is a function mapping distinguishers to real numbers. In information-theoretic security, one has that $\varepsilon(\mathsf{D})$ is small for all distinguishers D. In computational security this might not be the case, since security does not hold against all adversaries, only efficient ones. More precisely, let $\mathsf{D}[\mathsf{R}]$ be the random variable corresponding to the distinguisher's output when interacting with R. Then the functions

$$\Delta^{\mathsf{D}}(\mathsf{R},\mathsf{S}) := |\Pr[\mathsf{D}[\mathsf{R}] = 0] - \Pr[\mathsf{D}[\mathsf{S}] = 0]| \quad \text{and} \quad d^{\mathcal{D}}(\mathsf{R},\mathsf{S}) := \sup_{\mathsf{D}\in\mathcal{D}} \Delta^{\mathsf{D}}(\mathsf{R},\mathsf{S})$$

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 measured resources.[7] Thus, for any distinguisher D, we define the class

$$\mathcal{B}(\mathsf{D}) := \{\mathsf{D}' | \exists \alpha \text{ such that } \mathsf{D}\alpha = \mathsf{D}' \text{ or } \mathsf{D}'\alpha = \mathsf{D}\}, \tag{5}$$

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. (5).

[7] For more details on this, we refer to the full version [5].

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 [30]). *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. The details may be found in the full version [5].

3 Constructing Quantum Cryptographic Channels

In Sect. 3.1 we introduce the notations for Pauli operators and Bell basis. In Sect. 3.2 and Sect. 3.3 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 Sect. 3.4 and (2) the Pauli-malleable confidential quantum channel PMCC in Sect. 3.5. A construction of the ordered secure quantum channel OSC from one which is secure but not ordered (SC) is also presented in the full version [5].

3.1 Quantum Operators and States

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.

$$P_k = P_{x,z} = \bigotimes_{i=1}^{m} P_{x_i z_i}, \qquad \text{where} \quad P_{ab} = \begin{cases} I & a = 0, b = 0, \\ X & a = 1, b = 0, \\ Z & a = 0, b = 1, \\ XZ & a = 1, b = 1. \end{cases}$$

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, $|\phi_0\rangle \coloneqq \left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)^{\otimes m}$, and $|\phi_k\rangle \coloneqq I^{\otimes m} \otimes P_k |\phi_0\rangle$ as the result of applying P_k to half of the qubits. Then $\{|\phi_k\rangle\}_{k\in\{0,1\}^{2m}}$ forms the Bell basis for $2m$ qubits.

3.2 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 $\mathsf{seed}(s)$, set variable seed to s.*
  - *On input $\mathsf{input}(x)$, 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 $\mathsf{input}(x)$, output $f(x)$ at interface A.*
- **Interface B:** *On input $\mathsf{input}(x)$, 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 Sect. 2. In terms of AC construction, this means that

$$[\mathsf{KEY}^r, \mathsf{PRF}_A^{r,\nu,\mu}, \mathsf{PRF}_B^{r,\nu,\mu}] \xrightarrow{\pi^{\mathsf{PRF}},\epsilon^{\mathsf{PRF}}} \mathsf{URF}^{\nu,\mu}. \tag{6}$$

Concrete constructions of PRFs proven secure in the presence of quantum adversaries may be found in [45].

3.3 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. 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 [6]. 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.

3.4 Constructing an Ordered Secure Quantum Channel

As shown in [36], 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 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 the full version [5] 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 $\mathsf{dec}^{\text{q-auth}} : \mathcal{K} \times \mathcal{L}(\mathcal{H}_{\tilde{C}}) \to \mathcal{L}(\mathcal{H}_B \oplus |\perp\rangle\langle\perp|)$. We also denote by $\mathcal{E}$ the CPTP map that always discards the state and replaces it with error state $|\perp\rangle\langle\perp|$. In this section, we build on top of these encoding and decoding maps to construct a multi-message ordered secure quantum channel

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 $\perp$ to Bob.
6. π_B: Bob outputs the decrypted message $\tilde{\rho}^B$.

Fig. 1. 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.

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 Fig. 2 and the components are described in Fig. 1.

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 Fig. 1, corresponding to Alice and Bob both applying the following CPTP maps with increasing index* i*:*

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

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

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 advantage of the one time secure quantum channel construction. Then,*

$$\Big[\mathsf{IC}^{\ell,n+\log\ell}, \mathsf{URF}^{\log\ell,\mu}, \mathsf{QC}_A^{\ell,m,n+log\ell}, \mathsf{QC}_B^{\ell,m,n+log\ell}\Big] \xrightarrow{\pi_{AB},\ell\epsilon^{\text{q-auth}}} \Big[\mathsf{OSC}^{\ell,m}, \mathsf{QC}_E^{2\ell,m,n+\log\ell}\Big].$$

Proof. The proof of Theorem 1 appears in the full version [5].

Remark 1. 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.

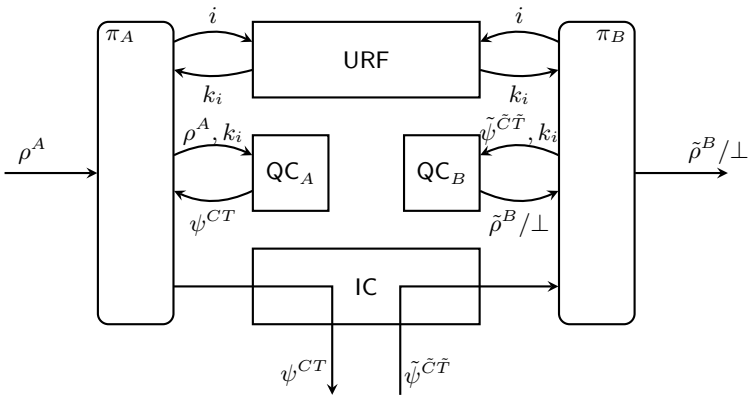

Fig. 2. The real system consisting of the shared resources $\mathsf{IC}^{\ell,n+\log\ell}$ and $\mathsf{URF}^{\log\ell,\mu}$, Alice and Bob's computing resources $\mathsf{QC}_A^{\ell,m,n+\log\ell}\mathsf{QC}_B^{\ell,m,n+\log\ell}$, and the protocol converters π_A and π_B.

Suppose now that one has a PRF resource and a bound ϵ^{PRF} satisfying Eq. (6), that is, indistinguishable from URF within ϵ^{PRF}, the following corollary follows trivially from the composition theorem.

Corollary 1.

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

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* $\pi_{AB}, \mathsf{IC}^{\ell,n+\log\ell}, \mathsf{QC}_A^{\ell,m,n+log\ell}, \mathsf{QC}_B^{\ell,m,n+log\ell}$.

3.5 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 Fig. 3. 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

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. 3. 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 $2m$.

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 Fig. 4.

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 Fig. 3, 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.,

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

Proof. The proof of Theorem 2 appears in the full version [5].

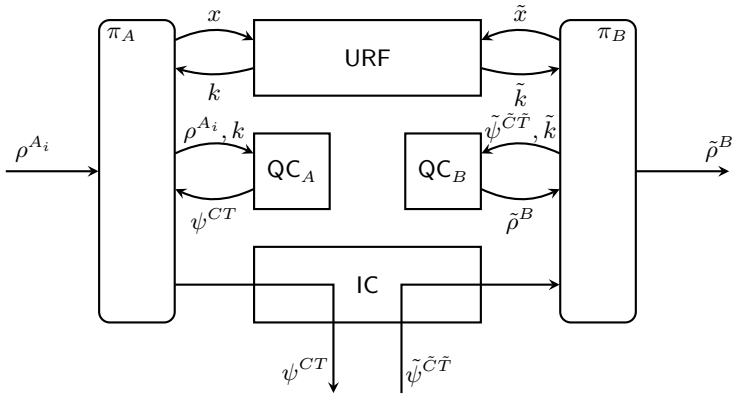

Fig. 4. The real system consisting of shared resources $\mathsf{IC}^{\ell,m+\nu}$ and $\mathsf{URF}^{\nu,2m}$, Alice and Bob's computing resources $\mathsf{QC}_A^{\ell,m,m+\nu}$ and $\mathsf{QC}_B^{\ell,m,m+\nu}$, and the protocol converters π_A and π_B.

Remark 2. 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. (6), that is, indistinguishable from URF within ϵ^{PRF}, the following corollary follows trivially from the composition theorem.

Corollary 2.

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

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 [2]. 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 [2] 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 both 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 [6], 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 [2], for key-generation function $\mathtt{Gen}$ (inducing a probability distribution over some key-space $\mathcal{K}$), encryption function $\mathtt{Enc}$, and decryption function $\mathtt{Dec}$, we can characterize a SQES $\mathfrak{S} \coloneqq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ as follows.

Lemma 1 ([2, Corollary 1]). *Let $\mathfrak{S} = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ 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 $\Pi^T_{k,r} \coloneqq |\psi_{k,r}\rangle\langle\psi_{k,r}|^T$, such that:*

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

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

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

For a SQES $\mathfrak{S}$, we define a security notion XXX in terms of the advantage $\mathbf{Adv}^{\mathrm{xxx}}_{\mathfrak{S},\mathsf{D}}$ 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 $\mathbf{Adv}^{\mathsf{xxx}}_{\mathfrak{S},\mathsf{D}}$ 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 $\mathbf{Adv}^{\mathsf{yyy}}_{\mathfrak{S},\mathsf{D}} \leq c \cdot \mathbf{Adv}^{\mathsf{xxx}}_{\mathfrak{S},\mathsf{DC}}$, 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[8] 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 that for distinction problems we always make the game system output the bit output by the distinguisher. In this case we use the expression $\mathsf{D}[\mathsf{G}]$ 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 $\mathsf{AGM\text{-}QCCA2}$ definition, which is *not* a distinction problem), we use the expression $\mathsf{G}[\mathsf{D}]$. 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 $x \leftarrow \mathsf{D}^{\mathbf{O}_1(\cdot),\mathbf{O}_2(\cdot)}$, 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.

4.2 Relating QAE and CC-QSEC

In this section we first present the quantum authenticated encryption security definition introduced in [2], and then show that it directly implies our constructive security notion $\mathsf{CC\text{-}QSEC}$ of constructing a secure channel from an insecure one and a shared secret key.

QAE Security Definition ([2]). We begin by restating what it means for a SQES $\mathfrak{S}$ to be secure in the QAE sense according to [2]. 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

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

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 [2], when phrased classically is equivalent to the canonical notion of authenticated encryption (dubbed IND-CCA3 by Shrimpton in [41]). 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 ciphertexts 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 [2] 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 submitted 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 original plaintext can thus be easily retrieved. We now restate the definition from [2] (Definition 10 therein), adapted to our notation, and in the concrete setting (as opposed to the asymptotic one).

Definition 10 (QAE Security [2]). *For SQES* $\mathfrak{S} \coloneqq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ *(implicit in all defined systems) we define the* QAE-advantage *of* $\mathfrak{S}$ *for distinguisher* D *as*

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

where the interactions of D *with game systems* $\mathsf{G}^{\text{qae-real}}$ *and* $\mathsf{G}^{\text{qae-ideal}}$ *are defined in Fig. 5.*

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

Theorem 3. *Let* $\mathfrak{S} \coloneqq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ *be a SQES (implicit in all defined systems). Then with protocol* $\pi^{\text{q-enc}}_{AB} = (\pi^{\text{q-enc}}_{A}, \pi^{\text{q-enc}}_{B})$ *making use of quantum computers* QC^{ℓ}_{A} *and* QC^{ℓ}_{B} *as defined in Fig. 6, simulator* $\mathsf{sim}^{\text{qae}}_{E}$ *making use of quantum computer* QC^{ℓ}_{E} *as defined in Fig. 7 (until the dashed line), and (trivial) reduction system* C *as specified in the proof, for any distinguisher* D *we have*

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

Proof. The proof of Theorem 3 appears in the full version [5].

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

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

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

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

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

Fig. 5. QAE security games $\mathsf{G}^{\text{qae-real}}$ (**left**) and $\mathsf{G}^{\text{qae-ideal}}$ (**right**).

Corollary 3. *With* $\varepsilon(\mathsf{D}) := \sup_{\mathsf{D}' \in \mathcal{B}(\mathsf{D})} \mathbf{Adv}^{\text{qae},\ell}_{\mathfrak{S},\mathsf{D}'}$*, we have*

$$\left[\mathsf{KEY}, \mathsf{IC}^\ell, \mathsf{QC}^\ell_A, \mathsf{QC}^\ell_B\right] \xrightarrow{\pi^{\text{q-enc}}_{AB},\varepsilon} \left[\mathsf{SC}^\ell, \mathsf{QC}^\ell_E\right],$$

where the class $\mathcal{B}(\mathsf{D})$ *is defined in Eq. (5).*

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

$\pi^{\text{q-enc}}_A\ \mathsf{QC}^\ell_A$

1. QC^ℓ_A 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^ℓ_A samples randomness $r \xleftarrow{p_k} \mathcal{R}$, computes the ciphertext $\sigma^C \leftarrow V_k(\varrho^M \otimes \Pi^T_{k,r})V_k^\dagger$, and outputs σ^C at the inside interface to IC^ℓ.

$\pi^{\text{q-enc}}_B\ \mathsf{QC}^\ell_B$

1. QC^ℓ_B 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^ℓ_B computes $MT \leftarrow V_k\sigma^C V_k^\dagger$, and if $\{P^T_{\omega_k}, \mathbb{1} - P^T_{\omega_k}\}(\omega^T) \Rightarrow 0$, outputs the plaintext message ϱ^M at the outside interface.

Fig. 6. Encryption and decryption protocols.

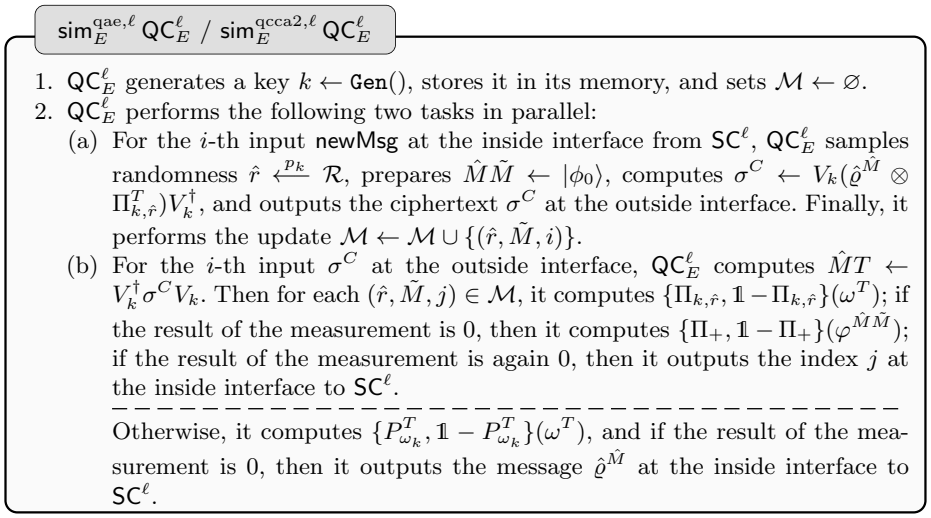

Fig. 7. QAE (until the dashed line) and QCCA2 (until the end) simulators.

SQESs that satisfy CC-QSEC, but not QAE. Following [15], 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 $\mathsf{sim}_E^{\mathrm{qae},\ell}\mathsf{QC}_E^\ell$ from Fig. 7, 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. 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 [2], 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.

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

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

$k \leftarrow \mathtt{Gen}()$
$\bar{\varrho}^{\bar{M}} \leftarrow \mathsf{D}^{\mathtt{Enc}_k(\cdot),\mathtt{Dec}_k(\cdot)}$ ▷ *Keep* $\bar{\varrho}^{\bar{M}}$
$\hat{r} \xleftarrow{p_k} \mathcal{R}$ ▷ *Keep* $\hat{r}$
$\hat{M}\tilde{M} \leftarrow |\phi_0\rangle$
$\hat{\sigma}^{\hat{C}} \leftarrow V_k(\hat{\varrho}^{\hat{M}} \otimes \Pi^T_{k,\hat{r}})V_k^\dagger$ ▷ *Ignore* $\bar{\varrho}^M$
$b' \leftarrow \mathsf{D}^{\mathtt{Enc}_k(\cdot),\mathbf{Dec}(\cdot)}(\hat{\sigma}^{\hat{C}})$
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 $\bar{\varrho}^{\bar{M}}$ ▷ *Original challenge*
  else
    return $\hat{D}_k(\rho^{MT})$ ▷ *Invalid ciphertext*
  return ϱ^M

Fig. 8. RRC-QCCA2 games $\mathsf{G}^{\text{rrc-qcca2-real}}$ (**left**) and $\mathsf{G}^{\text{rrc-qcca2-ideal}}$ (**right**).

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, 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 the fake setting of AGM-QCCA2, 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* $\mathfrak{S} \coloneqq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ *(implicit in all defined systems) we define the* RRC-QCCA2-advantage *of* $\mathfrak{S}$ *for distinguisher* D *as*

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

where the interactions of D *with game systems* $\mathsf{G}^{\text{rrc-qcca2-real}}$ *and* $\mathsf{G}^{\text{rrc-qcca2-ideal}}$ *are defined in Fig. 8.*

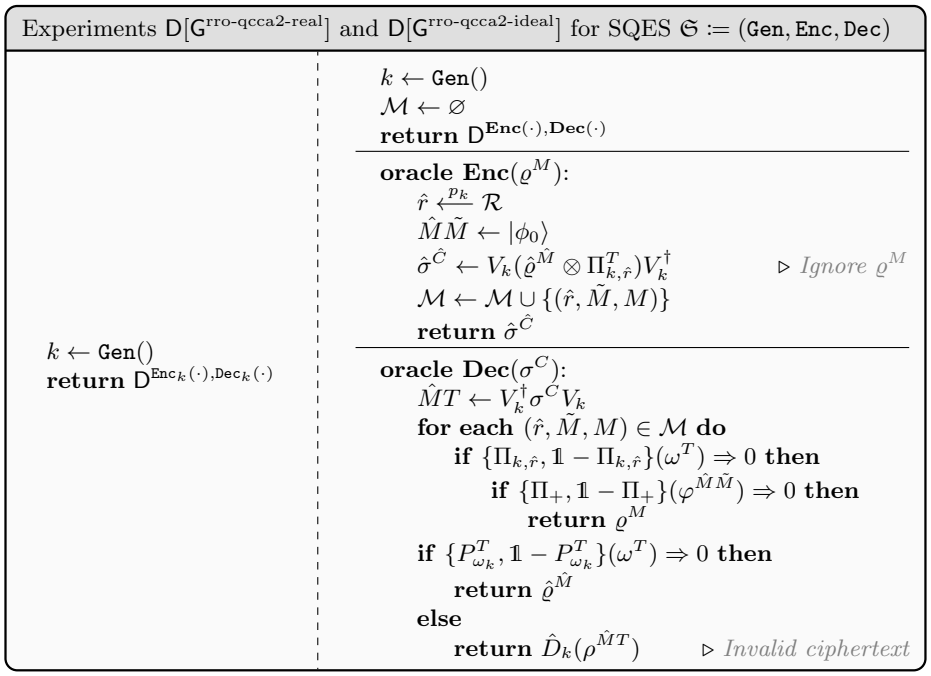

Fig. 9. RRO-QCCA2 games $\mathsf{G}^{\text{rro-qcca2-real}}$ (**left**) and $\mathsf{G}^{\text{rro-qcca2-ideal}}$ (**right**).

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.

Definition 12 (RRO-QCCA2 Security). *For SQES* $\mathfrak{S} := (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ *(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 Fig. 9.*

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 [2] 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 [2] for QAE, whose classical restriction was shown to be equivalent to the common classical notion of authenticated encryption IND-CCA3 from [41], 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 [2], 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 2. 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 $\hat{c}$.

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 [2].

Lemma 3. *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*

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

Proof. The proof of Lemma 3 appears in the full version [5].

It is easy to show that the other direction of Lemma 3 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 $\mathbf{Adv}^{\text{rrc-qcca2},\ell}_{\mathfrak{S},\mathsf{D}} \leq 2 \cdot \mathbf{Adv}^{\text{rro-qcca2},\ell-1}_{\mathfrak{S},\mathsf{DC}}$, and therefore the two notions are asymptotically equivalent, as we formalize in the following lemma.

Lemma 4. *For SQES satisfying Condition 1,* RRC-QCCA2 *and* RRO-QCCA2 *are asymptotically equivalent.*

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 4. 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 3, 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 $\pi^{\text{q-enc}}_{AB} = (\pi^{\text{q-enc}}_{A}, \pi^{\text{q-enc}}_{B})$ making use of quantum computers QC^{ℓ}_{A} and QC^{ℓ}_{B} (already defined in Fig. 6 for Theorem 3), simulator $\mathsf{sim}^{\text{qcca2}}_{E}$ making use of quantum computer QC^{ℓ}_{E} as defined in Fig. 7 (until the end), and (trivial) reduction system C as specified in the proof, for any distinguisher D we have*

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

Proof. The proof of Theorem 4 appears in the full version [5].

Corollary 5. *With $\varepsilon(\mathsf{D}) := \sup_{\mathsf{D}' \in \mathcal{B}(\mathsf{D})} \mathbf{Adv}^{\text{rro-qcca2},\ell}_{\mathfrak{S},\mathsf{D}'}$, we have*

$$\left[\mathsf{KEY}, \mathsf{IC}^{\ell}, \mathsf{QC}^{\ell}_{A}, \mathsf{QC}^{\ell}_{B}\right] \xrightarrow{\pi^{\text{q-enc}}_{AB}, \varepsilon} \left[\mathsf{NMCC}^{\ell}, \mathsf{QC}^{\text{qcca2},\ell}_{E}\right],$$

where the class $\mathcal{B}(\mathsf{D})$ is defined in Eq. (5).

Using Lemma 3, we finally obtain the following corollary.

Corollary 6. *With $\varepsilon(\mathsf{D}) := \sup_{\mathsf{D}' \in \mathcal{B}(\mathsf{D})} \mathbf{Adv}^{\text{rrc-qcca2},\ell}_{\mathfrak{S},\mathsf{D}'}$, we have*

$$\left[\mathsf{KEY}, \mathsf{IC}^{\ell}, \mathsf{QC}^{\ell}_{A}, \mathsf{QC}^{\ell}_{B}\right] \xrightarrow{\pi^{\text{q-enc}}_{AB}, (\ell+1)\cdot\varepsilon} \left[\mathsf{NMCC}^{\ell}, \mathsf{QC}^{\text{qcca2},\ell}_{E}\right],$$

where the class $\mathcal{B}(\mathsf{D})$ is defined in Eq. (5).

RRO-QCCA2 is Stronger than CC-QCNF. We remark that even though 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

CP acknowledges support from the Zurich Information Security and Privacy Center.

References

1. Alagic, G., Broadbent, A., Fefferman, B., Gagliardoni, T., Schaffner, C., Jules, M.S.: Computational security of quantum encryption. In: International Conference on Information Theoretic Security. pp. 47–71. Springer (2016)
2. Alagic, G., Gagliardoni, T., Majenz, C.: Unforgeable quantum encryption. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018, Proceedings, Part III. Lecture Notes in Computer Science, vol. 10822, pp. 489–519. Springer (2018)
3. Backes, M., Pfitzmann, B., Waidner, M.: A general composition theorem for secure reactive systems. In: Theory of Cryptography, Proceedings of TCC 2004. Lecture Notes in Computer Science, vol. 2951, pp. 336–354. Springer (2004)
4. Backes, M., Pfitzmann, B., Waidner, M.: The reactive simulatability (RSIM) framework for asynchronous systems. Information and Computation **205**(12), 1685–1720 (2007), extended version of [35]
5. Banfi, F., Maurer, U., Portmann, C., Zhu, J.: Composable and finite computational security of quantum message transmission. IACR Cryptology ePrint Archive **2019**, 914 (2019)
6. Barnum, H., Crépeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. In: Proceedings of the 43rd Symposium on Foundations of Computer Science, FOCS '02. pp. 449–458. IEEE (2002)
7. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: Proceedings of the 38th Annual Symposium on Foundations of Computer Science. pp. 394–403. FOCS '97, IEEE Computer Society (1997)
8. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Advances in Cryptology – CRYPTO '98. pp. 26–45. Springer (1998)
9. Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In: Advances in Cryptology – ASIACRYPT 2000. Lecture Notes in Computer Science, vol. 1976, pp. 531–545. Springer (2000)
10. Ben-Or, M., Horodecki, M., Leung, D., Mayers, D., Oppenheim, J.: The universal composable security of quantum key distribution. In: Theory of Cryptography, Proceedings of TCC 2005. Lecture Notes in Computer Science, vol. 3378, pp. 386–406. Springer (2005)

11. Broadbent, A., Jeffery, S.: Quantum homomorphic encryption for circuits of low t-gate complexity. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015. pp. 609–629. Springer (2015)
12. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: Proceedings of the 42nd Symposium on Foundations of Computer Science, FOCS '01. pp. 136–145. IEEE (2001)
13. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067 (2013), http://eprint.iacr.org/2000/067, updated version of [12]
14. Canetti, R., Dodis, Y., Pass, R., Walfish, S.: Universally composable security with global setup. In: Theory of Cryptography, Proceedings of TCC 2007. Lecture Notes in Computer Science, vol. 4392, pp. 61–85. Springer (2007)
15. Canetti, R., Krawczyk, H., Nielsen, J.B.: Relaxing chosen-ciphertext security. In: Boneh, D. (ed.) Advances in Cryptology – CRYPTO 2003. pp. 565–582. Springer (2003)
16. Chiribella, G., D'Ariano, G.M., Perinotti, P.: Theoretical framework for quantum networks. Physical Review A **80**, 022339 (Aug 2009)
17. Coretti, S., Maurer, U., Tackmann, B.: Constructing confidential channels from authenticated channels—public-key encryption revisited. In: Sako, K., Sarkar, P. (eds.) Advances in Cryptology – ASIACRYPT 2013. pp. 134–153. Springer (2013)
18. Dunjko, V., Fitzsimons, J.F., Portmann, C., Renner, R.: Composable security of delegated quantum computation. In: Advances in Cryptology – ASIACRYPT 2014, Proceedings, Part II. Lecture Notes in Computer Science, vol. 8874, pp. 406–425. Springer (2014)
19. Gutoski, G.: On a measure of distance for quantum strategies. Journal of Mathematical Physics **53**(3), 032202 (2012)
20. Gutoski, G., Watrous, J.: Toward a general theory of quantum games. In: Proceedings of the 39th Symposium on Theory of Computing, STOC '07. pp. 565–574. ACM (2007)
21. Hardy, L.: Reformulating and reconstructing quantum theory (2011), http://www.arxiv.org/abs/1104.2066, eprint
22. Hardy, L.: 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)
23. Hardy, L.: Quantum theory with bold operator tensors. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **373**(2047) (2015)
24. Katz, J., Yung, M.: Characterization of security notions for probabilistic private-key encryption. Journal of Cryptology **19**(1), 67–95 (Jan 2006)
25. König, R., Renner, R., Bariska, A., Maurer, U.: Small accessible quantum information does not imply security. Physical Review Letters **98**, 140502 (Apr 2007)
26. Krawczyk, H.: The order of encryption and authentication for protecting communications (or: How secure is SSL?). In: Advances in Cryptology – CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 310–331. Springer (2001). https://doi.org/10.1007/3-540-44647-8_19
27. Maurer, U.: Indistinguishability of random systems. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 110–132. Springer (2002)
28. Maurer, U.: Constructive cryptography—a new paradigm for security definitions and proofs. In: Proceedings of Theory of Security and Applications, TOSCA 2011. Lecture Notes in Computer Science, vol. 6993, pp. 33–56. Springer (2012)

29. Maurer, U., Pietrzak, K., Renner, R.: Indistinguishability amplification. In: Annual International Cryptology Conference. pp. 130–149. Springer (2007)
30. Maurer, U., Renner, R.: Abstract cryptography. In: Proceedings of Innovations in Computer Science, ICS 2011. pp. 1–21. Tsinghua University Press (2011)
31. Maurer, U., Renner, R.: From indifferentiability to constructive cryptography (and back). In: Theory of Cryptography, Proceedings of TCC 2016-B, Part I. Lecture Notes in Computer Science, vol. 9985, pp. 3–24. Springer (2016)
32. Maurer, U., Rüedlinger, A., Tackmann, B.: Confidentiality and integrity: A constructive perspective. In: Cramer, R. (ed.) Theory of Cryptography. pp. 209–229. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
33. Maurer, U., Tackmann, B.: 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. pp. 505–515. ACM (2010)
34. Pfitzmann, B., Waidner, M.: Composition and integrity preservation of secure reactive systems. In: Proceedings of the 7th ACM Conference on Computer and Communications Security, CSS '00. pp. 245–254. ACM (2000)
35. Pfitzmann, B., Waidner, M.: A model for asynchronous reactive systems and its application to secure message transmission. In: IEEE Symposium on Security and Privacy. pp. 184–200. IEEE (2001)
36. Portmann, C.: Quantum authentication with key recycling. In: Advances in Cryptology – EUROCRYPT 2017, Proceedings, Part III. Lecture Notes in Computer Science, vol. 10212, pp. 339–368. Springer (2017)
37. Portmann, C., Matt, C., Maurer, U., Renner, R., Tackmann, B.: Causal boxes: Quantum information-processing systems closed under composition. IEEE Transactions on Information Theory **63**(5), 3277–3305 (May 2017)
38. Portmann, C., Renner, R.: Cryptographic security of quantum key distribution (2014), http://www.arxiv.org/abs/1409.3525, eprint
39. Renner, R.: Security of Quantum Key Distribution. Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich (Sep 2005)
40. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Reviews of Modern Physics **81**, 1301–1350 (Sep 2009)
41. Shrimpton, T.: A characterization of authenticated-encryption as a form of chosen-ciphertext security. IACR Cryptology ePrint Archive **2004**, 272 (2004)
42. Tomamichel, M., Leverrier, A.: A largely self-contained and complete security proof for quantum key distribution. Quantum **1**, 14 (Jul 2017)
43. Unruh, D.: Universally composable quantum multi-party computation. In: Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 486–505. Springer (2010)
44. Vilasini, V., Portmann, C., del Rio, L.: Composable security in relativistic quantum cryptography (2017), eprint
45. Zhandry, M.: How to construct quantum random functions. In: Proceedings of the 43rd Symposium on Foundations of Computer Science, FOCS '12. pp. 679–687. IEEE (2012)