Generic Composition: From Classical to Quantum Security

Nathalie Lang, Jannis Leuther and Stefan Lucks

Bauhaus-Universität Weimar, Weimar, Germany {nathalie.lang,jannis.leuther,stefan.lucks}@uni-weimar.de

Abstract. Authenticated encryption (AE) provides both authenticity and privacy. Starting with Bellare's and Namprempre's work in 2000, the Encrypt-then-MAC composition of an encryption scheme for privacy and a MAC for authenticity has become a well-studied and common approach. This work investigates the security of the Encrypt-then-MAC composition in a quantum setting which means that adversarial queries as well as the responses to those queries may be in superposition. We demonstrate that the Encrypt-then-MAC composition of a chosen-plaintext (IND-qCPA) secure symmetric encryption scheme SE and a plus-one unforgeable MAC fails to achieve chosen-ciphertext (IND-qCCA) security. On the other hand, we show that it suffices to choose a quantum pseudorandom function (qPRF) as the MAC. Namely, the Encrypt-then-MAC composition of SE and a qPRF.

Keywords: Post-Quantum, Authenticated Encryption, Generic Composition

1 Introduction

Since the year 2000, one of the main goals in the field of symmetric cryptography has been to propose and analyse efficient and secure authenticated encryption (AE) schemes. Back then, researchers focused on classical attack scenarios. In recent years, the anticipated advent of quantum computers and quantum communication channels has brought the importance of quantum security for encryption, authentication and authenticated encryption into focus. After the first proposals for quantum security definitions, the next step was to design new quantum-secure AE procedures that are consistent with the newly introduced security definitions. In the current paper, we focus on the quantum security of state-ofthe-art systems. That is, AE schemes currently in use, which were originally developed with classical security in mind. In this context, the question arises whether some of these schemes can maintain security in a setting with quantum computers and quantum communication channels. We focus on AE schemes that are constructed by combining a symmetric encryption scheme with a MAC. Special attention is paid to the Encrypt-then-MAC composition, which has become the de facto standard after the fundamental work of Bellare and Namprempre [BN00]. Authenticated encryption can be understood as the combination of privacy and authenticity. Various modelling methods have been proposed and discussed for classical adversaries [BDJR97]. Nowadays, the cryptographic research community mostly settled on the security definitions of indistinguishability (IND-CPA, IND-CCA) for privacy under chosen-plaintext and chosen-ciphertext attacks respectively, and unforgeability (EUF-CMA) for authenticity. The concept of generic composition has been introduced by Bellare and Namprempre [BN00]. The idea is to compose an IND-CCA secure authenticated encryption scheme from an IND-CPA secure symmetric encryption scheme and an EUF-CMA secure MAC. They identified three types of generic

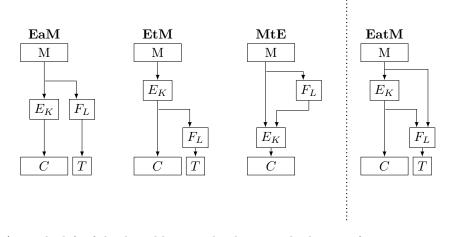


Figure 1: To the left of the dotted line are the three standard types of generic composition: Encrypt-and-MAC (EaM), Encrypt-then-MAC (EtM) and MAC-then-Encrypt (MtE). To the right of the dotted line is the generic composition, which we refer to as Encryptand+then-MAC (EatM), introduced by Chevalier et al. [CEV22a, Construction 1]. Each approach combines a MAC F under key L and an encryption algorithm E under key K to produce an authenticated encryption scheme for message M, ciphertext C and authentication tag T. Importantly, keys K and L must be chosen independently.

composition, which are illustrated in Figure 1. Importantly, in each type of composition, the MAC and encryption algorithms must use independent keys (here denoted by K and L). In the Encrypt-and-MAC (EaM) composition, the authentication tag and the ciphertext are computed separately on the input message and concatenated at the end. In MAC-then-Encrypt (MtE), the MAC first computes the authentication tag for a given message before the symmetric encryption algorithm encrypts the concatenation of the message and authentication tag to produce the ciphertext. In Encrypt-then-MAC (EtM), the ciphertext of the input message is computed first. Afterwards, a MAC computes the authentication tag for the ciphertext and both outputs are concatenated.

Bellare and Namprempre's work [BN00, BN08] shows that IND-CCA or EUF-CMA security of EaM and MtE depend on additional assumptions that need to be considered. Only EtM is *provably* IND-CCA secure, when the underlying encryption algorithm and MAC are IND-CPA secure and EUF-CMA secure respectively. This result leads to another crucial observation: the triple of security definitions IND-CPA, IND-CCA and EUF-CMA is a good choice for modelling a classical authenticated encryption scheme that preserves privacy under chosen-plaintext and chosen-ciphertext attacks as well as preserving authenticity under chosen-message attacks.

We are interested in security requirements for authenticated encryption and generic composition in the so-called Q2 model. In the Q2 attack model, an adversary can perform both offline and online computations on a quantum computer. This means, that the communication between adversary and oracle allows for quantum superposition queries and responses.

In the context of quantum security for encryption, we adapt the security terms INDqCPA and IND-qCCA introduced by Boneh and Zhandry [BZ13a] and extend them to match nonce-based authenticated encryption with associated data. These definitions are particularly relevant for existing (classical) systems: Anand et al. [ATTU16] show that these security guarantees can be achieved by current state-of-the-art encryption algorithms. For example, the counter mode (CTR) is secure if the underlying block cipher is a secure pseudorandom function (PRF), while the cipher block-chaining mode (CBC) is secure if the block cipher is a quantum pseudorandom function (qPRF).

Chevalier et al. [CEV22a] introduce stronger notions which which we adapt as qIND-qCPA and qIND-qCCA security. These definitions support challenge queries in superposition and are strictly stronger than IND-qCPA and IND-qCCA, respectively. However, qIND-qCPA and qIND-qCCA are too strong for the classical encryption algorithms mentioned above. Additionally, Chevalier et al. [CEV22a, Construction 1] introduce a fourth variant of generic composition which we refer to as Encrypt-and+then-MAC (EatM) (see also Figure 1). In this work, we will focus on the generic composition method EtM and give a proper reasoning for this decision in Section 6.3.

As of writing, the selection of quantum security definitions for plain authenticity is quite sparse. As one of the first contributions, Boneh and Zhandry introduced what we call plus-one unforgeability (PO) [BZ13b] to model the security of MACs.

As it turns out, there exists an IND-qCPA secure symmetric encryption scheme SE and a PO unforgeable MAC, such that their EtM composition is chosen-ciphertext (IND-qCCA) insecure. However, when we replace the PO unforgeable MAC by a quantum pseudorandom function (qPRF) F, the EtM composition of SE (or any other IND-qCPA secure symmetric encryption scheme) and F is chosen-ciphertext (IND-qCCA) secure.

1.1 Related Work

Classical Authenticated Encryption. The work from Bellare and Namprempre [BN00, BN08] stems from the year 2000. Today's state of the art authenticated encryption (AE) schemes are nonce-based and may also authenticate some non-confidential context information (associated data) in addition to encrypting and authenticating the message. Authenticated encryption with associated data (AEAD) had been proposed in 2002 [Rog02] while nonce-based encryption dates back to 2004 [Rog04]. In the context of this work, without loss of generality, we will refer to authenticated encryption as "AE", independent of the presence of associated data. Namprempre, Rogaway and Shrimpton reconsidered generic composition in 2014 [NRS14]. They introduced interfaces to nonce-based symmetric encryption algorithms, to nonce-based AE schemes with associated data, and to "vectorial MACs", i.e., to MACs authenticating tuples of strings rather than single strings. However, the approach from [NRS14] is less generic and less basic than the one from [BN00, BN08]: Firstly, [NRS14] assume the symmetric encryption scheme to be "tidy" in addition to being chosen-plaintext secure. This means that given a nonce N, associated data A and message M, there is exactly one ciphertext C which will decrypt to M under N, A and a given key K. Secondly, [NRS14] require the MAC to be pseudorandom, rather than just providing forgery resistance. These additional assumptions allow them to prove even MtE and EaM constructions as secure as EtM.

In [NRS14], the authors classify authenticated encryption schemes as either A-, B-, or N-schemes. Both the A- and the B-schemes employ the MAC not just for message authentication, but also to compute pseudorandom values from nonces – and thus depend on the MAC to behave like a PRF. Therefore, we will only consider the N-schemes from [NRS14] which are illustrated in Figure 2. N1 is of the EaM type, which is insecure if the MAC leaks information about the message. N3 is of the MtE type, which is insecure if the encryption function is not tidy. We will thus focus on the N2 scheme, which is the natural extension of EtM from [BN00, BN08].

Quantum-Secure Encryption. For security definitions that evaluate indistinguishability in the Q2 model, there exist various enhancements and modifications of classical definitions to fit the post-quantum needs. Carstens et al. [CETU21] create a classification system which

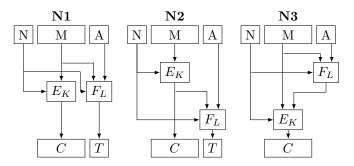


Figure 2: The three N-schemes N1, N2, and N3 from [NRS14]. An N-scheme implements a nonce-based AE scheme based on a nonce-based symmetric encryption algorithm E under a key K and a MAC F under a key L. Note that for either scheme, the MAC is vectorial, i.e., it deals with a triple of inputs.

analyses a comprehensive listing of variants of quantum indistinguishability definitions with respect to quantum chosen-plaintext security, as well as their relationships and (non-) implications towards one another. Security definitions that are polynomially equivalent are grouped into 14 *panels* with the union of panels P1 and P2 directly and indirectly implying all other panels. In [GHS16], Gagliardoni et al. define *quantum semantic security under chosen plaintext attacks* (qSEM-qCPA) as well as an equivalent security definition which is strictly stronger than Boneh and Zhandry's IND-qCPA [BZ13b]. Importantly, qSEM-qCPA and all equivalent notions from [CETU21]'s panel P1 are only applicable to permutations (*i.e.*, **un**authenticated encryption). As we will investigate the post-quantum security of authenticated encryption, we will not consider qSEM-qCPA and panel P1 in this context. Mossayebi and Schack [MS16] introduce the "Real-or-Permutation" definitions RoP-qsCPA and RoP-qsCCA. The restriction in their definition of RoP-qsCCA is that the adversary may not pose decryption queries which have been the result of a previous encryption query. We argue that this restriction of the adversary is too strong.

Quantum-Secure Authentication. Defining security notions for post-quantum authenticity has turned out to be a challenge and few definitions exist. The main issue is that in the Q2 case, no-cloning [Die82, WWZ82] prevents any challenger from recording chosen-message queries. This renders them unable to check the validity of the adversaries challenge queries. Boneh and Zhandry [BZ13a] define an authenticity notion which we refer to as "plus-one unforgeability" (PO). An adversary makes q chosen-message queries possibly in superposition and wins if they can produce q + 1 disjoint message-tag pairs that are all valid. Alagic et al. [AMRS20] point out issues related to this definition and introduce "blind unforgeability" (BU). Here, the oracle which is queried by the adversary is *blinded* on a randomly selected set of inputs. The adversary wins if they can produce a valid message-tag pair for an input on which the oracle was blinded on.

Quantum-Secure Authenticated Encryption and Generic Composition. While there have been proposals for dedicated authenticated encryption schemes secure in the Q2 model like QCB [BBC⁺21], there has not been much progress on developing suitable security definitions for authenticated encryption or generic composition. Two exceptions are Soukharev et al. [SJS16] and Chevalier et al. [CEV22a]. Below, we will have a closer look at both works and examine their relationship to the current paper.

Soukharev et al. [SJS16] study post-quantum secure generic composition. They start with Boneh's and Zhandry's security notions for chosen-plaintext security (IND-qCPA) and forgery resistance (plus-one unforgeability) [BZ13b, BZ13a]. [SJS16, Theorem 3.6] claims that the EtM composition of an IND-qCPA secure encryption scheme and a plus-one unforgeable MAC provides IND-qCCA security – a claim which we can *disprove* in section 5 of the current paper. In their attempt to prove this, they follow the classical approach from Bellare and Namprempre [BN00, BN08] very closely. We argue, however, that for two reasons, their proof of [SJS16, Theorem 3.6] skips some quantum-specific details and thus is inconclusive.

The first problem is introduced in the pseudocode from [SJS16]. They describe three games which handle decryption queries, among other things. If the decryption M of a chosen ciphertext is valid, an internal variable *bad* is set. Later, an argument is made related to the probability of *bad* being set. In the classical case, this argument is correct. In the quantum case, if one decrypts a ciphertext in superposition, its decryption M can be in superposition as well. Thus, the variable *bad* can also occur in superposition. Technically, the event of *bad* being set is not defined for this case. Of course, one could measure *bad* and consider the probability of the measurement returning true, but then, one would have to consider the impact of that measurement on other data, entangled with *bad*.

A second problem arises when [SJS16] argue that, whenever *bad* is set, the adversary wins the qCTXT game without explaining this conclusion. Their qCTXT game is similar to our definition of PO-CTXT in Definition 7, and the argument is straightforward in the classical case: there are q valid ciphertexts from q chosen-plaintext queries, and the (q + 1)th valid ciphertext is the one which decrypts to $M \neq \bot$. In total, this makes up the (q + 1) valid ciphertexts to win the game. For the quantum case, one has to consider the no-cloning theorem, which prevents a naive approach of trying to store these q ciphertexts.

Chevalier et al. [CEV22b, CEV22a] introduce new security definitions for privacy which are strictly stronger than those in [BZ13b]. In fact, security in the sense of Chevalier et al. implies security in the sense of Boneh and Zhandry, but not vice versa. For example, stream-cipher-like encryption, such as counter-mode encryption, can be secure in the context of Boneh and Zhandry, since the challenge queries are classical. On the other hand, when using the definitions from Chevalier et al., this type of cipher can never provide security. However, if one restricts the adversary to make classical challenge queries only, the definitions are equivalent. Furthermore, Chevalier et al. examine a form of generic composition which we refer to as "Encrypt-and+then-MAC" (EatM) [CEV22a, Construction 1]. They show that when instantiated with chosen-plaintext secure encryption scheme (in their stronger sense) and a qPRF, the EatM composition is chosen-ciphertext secure (also in their stronger sense) [CEV22a, Theorem 2]. Note that in EtM, the only input for the MAC is the ciphertext, while in EatM, the MAC is called with both the plaintext and the ciphertext as inputs. Figure 1 visualizes EatM next to the standard types of generic composition. We provide a formal definition of EatM in Section 2.

1.2 Unique Nonce Versus Randomness

Secure and correct encryption – authenticated or not – must be stateful or randomized. Else, the adversary could discover when two ciphertexts stem from encrypting the same message twice. In the classical setting, one typically formalizes state or randomness by an additional *nonce* input N. The adversary may choose N with the restriction of it being unique: after *i* queries with nonces N_1, \ldots, N_i , the nonce N_{i+1} for the (i + 1)st query must satisfy $N_{i+1} \notin \{N_1, \ldots, N_i\}$. An adversary maintaining this constraint is "nonce-respecting". In contrast to the classical setting, most research related to post-quantum secure encryption (from Boneh's and Zhandry's early work [BZ13b, BZ13a] to the recent paper from Chevalier et al. [CEV22a]) formalize encryption as a random process, without the option to maintain a state. That makes N is a classical random value, not chosen by the adversary.

For the current paper, we thus had to make a choice between the nonce-based approach and the randomness-based approach. Even though the post-quantum line of research is mostly based on randomness, we opted to use nonces. The reasons are as follows:

- 1. Nonce-based security is *strictly stronger* than security in the random-IV setting:
 - Security in the nonce-based setting *implies* security in the random-IV setting. I.e., with high probability an adversary choosing nonces uniformly at random is a nonce-respecting adversary (up to the birthday bound).
 - Security in the random-IV setting *does not imply* security in the nonce-based setting. E.g., CBC encryption is secure with a random IV, but not with a nonce chosen by a nonce-respecting adversary.
- 2. In Lemma 10, we show that non-repeating nonces suffice for security *without any need for randomness.* This holds for our results, as well as for a security proof in [CEV22b], which we revisit and adapt. We suspect that this also holds for most of the related work on post-quantum secure symmetric encryption.
- 3. Nonces *work well* for almost all practical applications: if not generated randomly, one can use message counters, timestamps, etc. as nonces. For this very reason, nonce-based security has long become the norm for classical authenticated encryption, see, e.g., [RBB03, BRW04, Dwo07, BDPA11, TMC⁺24].

1.3 Contribution and Outline

Contribution. Our main results are the following:

- 1. The Encrypt-then-MAC (EtM) composition of an IND-qCPA secure encryption scheme and a PO secure MAC does not suffice for IND-qCCA secure authenticated encryption.
- 2. The EtM composition of an IND-qCPA secure encryption scheme and a MAC modelled as a qPRF is an IND-qCCA secure authenticated encryption scheme.
- 3. If a composition $Comp_1 \in \{\text{EtM}, \text{EaM}, \text{EatM}\}$ of an IND-qCPA secure encryption scheme and a MAC modelled as a qPRF is IND-qCCA secure, it implies IND-qCCA security of $Comp_2 \in \{\text{EtM}, \text{EaM}, \text{EatM}\}$ as well.

Outline. This paper is organized as follows:

- **Preliminaries and Definitions** (Sections 2 to 4): We first give essential definitions and preliminaries. Section 3 and Section 4 introduce security definitions for privacy, authenticity and integrity in the Q2 model, based on previous work from [BZ13b, CEV22a, BZ13a].
- Encrypt-then-MAC with Plus-One Unforgeability (Section 5): We examine the combination of IND-qCPA, PO and IND-qCCA and show that the EtM composition of IND-qCPA secure encryption and a PO secure MAC is *not* IND-qCCA secure.
- Encrypt-then-MAC with a qPRF (Section 6): We proceed to analyse the EtM composition when using the strongest possible authenticity definition, namely the combination of an IND-qCPA secure encryption scheme and a qPRF as the MAC. We revisit and adapt the findings from [CEV22b] to show the IND-qCCA security of EtM, EaM and EatM under these conditions. As a by-product, we prove that the

IND-qCCA security of one of these compositions transfers to any of the others.

• **Conclusion** (Section 7): Finally, we present concluding remarks and discuss implications of our findings before highlighting potential future work.

2 Preliminaries

We assume the reader to be familiar with Quantum notation and standards as used in common textbooks (e.g. [Mer07]).

General Notation. By $\{0,1\}^n$, we denote the set of binary strings of length n. $\{0,1\}^*$ is the set of binary strings of arbitrary length. X || Y denotes concatenation of two bitstrings X and Y. With $|X\rangle$, we mark a state or a parameter that can be a quantum state, i.e. which can be in superposition of some kind. We will write $|X\rangle = \sum_x \alpha_x |x\rangle$ to describe all base states $x \in \{0,1\}^n$ which are present in the *n*-qubit superposition state $|X\rangle$ using the natural base. With $0 \le \alpha_x \le 1$, we denote the corresponding amplitude of the base state $|x\rangle$ in $|X\rangle$. The amplitudes in $|X\rangle$ may be distributed arbitrarily but have to be consistent with the Born rule: $\sum_{\alpha_x} |\alpha_x|^2 = 1$. If the $|\cdot\rangle$ notation is omitted, we only allow classical states or values for this parameter. Of course, a state $|X\rangle$ can also represent a base state which would thus be classical as well.

Invalid Data. Authenticated encryption needs to distinguish proper strings in $\{0, 1\}^*$ from invalid data, which we represent by \perp . If at least one of the strings X and Y is invalid, then the bit-wise XOR $X \oplus Y$ and the concatenation $X \parallel Y$ are invalid as well. If both X and Y are valid, then so are their XOR and concatenation. Within this paper, strings $|X\rangle$ will often be in a superposition of proper strings and invalid data.

For concreteness, the reader may assume an *n*-bit string X to be represented by $X = (X_{\text{str}}, X_{\perp}) \in \{0, 1\}^n \times \{0, 1\}$. If $X_{\perp} = 0$, then X is a proper *n*-bit string with the value X_{str} . If $X_{\perp} = 1$, then X is invalid and $X_{\text{str}} = 0^n$. The case $X_{\perp} = 1$ and $X_{\text{str}} \neq 0^n$ is prohibited to ensure that no invalid string holds any information beyond the fact of being invalid. A superposition of an *n*-bit string and invalid data can be written as

$$|X\rangle = \alpha_{\perp} |(0^n, 1)\rangle + \sum_{x \in \{0,1\}^n} \alpha_x |(x, 0)\rangle$$

The amplitudes α_{\perp} and the α_x are complex numbers and $|\alpha_{\perp}|^2 + \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$.

Unauthenticated Symmetric Encryption and Correctness. A symmetric encryption scheme SE is a quadruple (E, D, κ, ν) of a deterministic encryption algorithm E, a deterministic decryption algorithm D, and two integer parameters $\kappa \ge 0$ for the key size and $\nu \ge 0$ for the nonce size. A nonce (or initialisation vector) may be required for statefulness or randomization. When the integer parameters are clear from context, we may write (E, D) instead of (E, D, κ, ν) .

E takes a key $K \in \{0,1\}^{\kappa}$, nonce $N \in \{0,1\}^{\nu}$, message $M \in \{0,1\}^{*}$ and returns a ciphertext $C = E_{K}^{N}(M)$. *D* takes *K*, *N* and a ciphertext $C \in \{0,1\}^{*}$ and returns a message $M = D_{K}^{N}(C)$. *E* is *correct* if for all $K \in \{0,1\}^{\kappa}$, $N \in \{0,1\}^{\nu}$ and $M \in \{0,1\}^{*}$ it holds that $D_{K}^{N}(E_{K}^{N}(M)) = M$.

MACs. A message authentication code (MAC) algorithm is a quintuple $(F, \kappa, \tau, \nu, \mu)$ of a deterministic function F and four integer parameters $\kappa \ge 0$ for the key size, $\tau > 0$ for the tag size, $\nu \ge 0$ for the nonce size and $\mu > 0$ for the multiplicity. When all integer parameters are clear from context, we may just write F instead of $(F, \kappa, \tau, \nu, \mu)$. F takes a key $K \in \{0,1\}^{\kappa}$, a nonce $N \in \{0,1\}^{\nu}$ and a message- μ -tuple $M = (M_1, \ldots, M_{\mu}) \in (\{0,1\}^*)^{\mu}$ as its input. Then, F generates an authentication tag $T = F_K^N(M) = F_K^N(M_1, \ldots, M_{\mu}) \in \{0,1\}^{\tau}$. To check if T is a valid tag for input (N, M) under key K, compute $T^* = F_K^N(M)$ and return true if $T^* = T$, otherwise return false. Note that in the subsequent work, we may split the input and use the tuple (M, A) as the input for a MAC F to discern message and associated data. In this case, μ is the amount of blocks in both M and A combined.

Authenticated Encryption. An authenticated encryption (AE) scheme is a quintuple $(\mathbf{E}, \mathbf{D}, \kappa, \nu, \tau)$ of authenticated encryption algorithm \mathbf{E} , authenticated decryption algorithm \mathbf{D} and three integer parameters $\kappa \geq 0$ for the key size, $\nu \geq 0$ for the nonce size, and $\tau \geq 0$ for the tag size. When the integer parameters are clear from context, we may just write (\mathbf{E}, \mathbf{D}) instead of $(\mathbf{E}, \mathbf{D}, \kappa, \nu, \tau)$.

E takes a key $K \in \{0,1\}^{\kappa}$, nonce $N \in \{0,1\}^{\nu}$, associated data $A \in \{0,1\}^{*}$, message $M \in \{0,1\}^{*}$ and returns a pair $(C,T) = \mathbf{E}_{K}^{N,A}(M)$ of ciphertext $C \in \{0,1\}^{*}$ and authentication tag $T \in \{0,1\}^{\tau}$. **D** takes K, N, A and a pair $(C,T) \in \{0,1\}^{*} \times \{0,1\}^{\tau}$ and either returns a message $M = \mathbf{D}_{K}^{N,A}(C,T)$ or the failure symbol $\bot = \mathbf{D}_{K}^{N,A}(C,T)$. For all $K \in \{0,1\}^{\kappa}$, $N \in \{0,1\}^{\nu}$, $A \in \{0,1\}^{*}$ and $M \in \{0,1\}^{*}$, we require $\mathbf{D}_{K}^{N,A}(\mathbf{E}_{K}^{N,A}(M)) = M$.

In other words, authenticated encryption is an extension of symmetric encryption. Or, from another point of view, an SE is an AE scheme with three constraints: the associated data A is always the empty string, the tag size is $\tau = 0$, and the decryption algorithm never returns \perp . In Definition 1, we formalize the generic compositions EaM, EtM and EatM from Figure 1.

Definition 1 (EaM, EtM, EatM). Let N, M, C, A, T denote nonce, message, ciphertext, associated data and tag respectively as described above. Let K, L be keys chosen independently at random, $SE = (E_K, D_K)$ a symmetric encryption scheme under key K and F_L a message authentication code under key L. The authenticated encryption algorithm $AE = (\mathbf{E}_{K,L}, \mathbf{D}_{K,L})$ resulting from the EaM, EtM and EatM composition of SE and F is respectively defined as

Encrypt-and-MAC (EaM):

$$\mathbf{E}_{K,L}^{N,A}(M) = \left(E_K^N(M), F_L^N(M, A) \right),$$
$$\mathbf{D}_{K,L}^{N,A}(C,T) = \begin{cases} D_K^N(C) & \text{if } F_L^N(D_K^N(C), A) = T \\ \bot & \text{else.} \end{cases}$$

Encrypt-then-MAC (EtM):

$$\mathbf{E}_{K,L}^{N,A}(M) = \left(E_K^N(M), F_L^N(E_K^N(M), A) \right),$$
$$\mathbf{D}_{K,L}^{N,A}(C, T) = \begin{cases} D_K^N(C) & \text{if } F_L^N(C, A) = T \\ \bot & \text{else.} \end{cases}$$

Encrypt-and+then-MAC (EatM):

$$\mathbf{E}_{K,L}^{N,A}(M) = \left(E_K^N(M), F_L^N(E_K^N(M) \| M, A) \right),$$
$$\mathbf{D}_{K,L}^{N,A}(C,T) = \begin{cases} D_K^N(C) & \text{if } F_L^N(C \| D_K^N(C), A) = T \\ \bot & \text{else.} \end{cases}$$

Recall that SE is correct if $D_K^N(E_K^N(M)) = M$ holds for all messages M, nonces N, and keys K. Regardless of the composition type (EtM, EaM, or EatM), the generic composition

 $AE = (\mathbf{E}_{K,L}, \mathbf{D}_{K,L})$ of a correct SE and a function F is correct as well. In other words: if SE is correct, then $\mathbf{D}_{K,L}^{N,A}(\mathbf{E}_{K,L}^{N,A}(M))$ holds for all M, N, A, K, L.

Compressed Random Oracles. Zhandry's compressed random oracles [Zha19] provide a proof technique for simulating random oracles in a quantum setting while maintaining properties analogous to the classical setting. Due to the no-cloning theorem, directly recording the queries of a quantum adversary is non-trivial without potentially disturbing the adversary's state. The compressed random oracle model addresses this by maintaining a state vector \mathcal{D} , initially set to 0. Rather than storing explicit query results, \mathcal{D} encodes information about previous queries in a way that remains consistent with quantum superpositions. When a query $|X, Y\rangle$ is made, if \mathcal{D} does not store any information about X, the oracle updates \mathcal{D} such that $\mathcal{D} = \mathcal{D} \cup (X, H(X))$. Formally,

$$|X,Y\rangle |\mathcal{D}\rangle \mapsto |X,Y \oplus \mathcal{D}(X)\rangle |\mathcal{D} \cup (X,H(X))\rangle$$

A key property of compressed random oracles is that the oracle may remove results from previous queries stored in \mathcal{D} . This prevents the adversary from extracting information beyond what a classical random oracle would reveal. In [Zha19], Zhandry calls this the "power of forgetting". This is achieved through careful use of Fourier-space representation, ensuring that the adversary cannot distinguish the simulated oracle from a truly random function. Unlike classical databases, which store fixed values, the compressed random oracle dynamically maintains only the minimal necessary information to simulate an idealized quantum-accessible random function.

3 Quantum Security Definitions for Privacy

3.1 Nonce-Based, Classical Challenge Queries (IND-q{CPA,CCA})

In Definitions 2 and 3, we redefine the security notions IND-q{CPA,CCA} of [BZ13b] in order to make them applicable to authenticated encryption schemes including a nonce and associated data. Note that [BZ13b] show that a fully-quantum security definition is unsatisfiable and thus resort to *classical* challenge queries.

Definition 2 (IND-qCPA game with nonce and associated data). Let \mathcal{A} be a *q*-query IND-qCPA adversary and \mathcal{C} an IND-qCPA challenger with access to an authenticated encryption oracle (\mathbf{E}, \mathbf{D}) .

- 1. C generates a key K and a bit $b \in \{0, 1\}$ uniformly at random.
- 2. For each query $1 \le i \le q$, \mathcal{A} either performs an encryption query or challenge query:
 - Encryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, M_i, \Psi\rangle = \sum_{a,m,\gamma} \alpha_{a,m,\gamma} |a,m,\gamma\rangle$. N_i must not have been used in a previous encryption query. \mathcal{C} performs the authenticated encryption on each "entry" in the superposition state through the transformation

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \mathbf{E}_{K}^{N_{i},a}(m) \right\rangle$$

- Challenge query: \mathcal{A} decides on two classical triples (N_i^0, A_i^0, M_i^0) and (N_i^1, A_i^1, M_i^1) . \mathcal{C} then returns the authenticated encryption $\mathbf{E}_K^{N_i^b, A_i^b}(M_i^b)$.
- 3. \mathcal{A} outputs bit b'. \mathcal{A} wins if b' = b.

The advantage of \mathcal{A} is

$$ADV^{IND-qCPA}(\mathcal{A}) = |Pr[b' = 1 | b = 1] - Pr[b' = 1 | b = 0]|.$$

Definition 3 (IND-qCCA game with nonce and associated data). Let \mathcal{A} be a *q*-query IND-qCCA adversary and \mathcal{C} an IND-qCCA challenger with access to an authenticated encryption oracle (\mathbf{E}, \mathbf{D})

- 1. C sets $\mathfrak{D} = \{\}$ and chooses a key K and a bit $b \in \{0, 1\}$ uniformly at random.
- 2. For each query $1 \le i \le q$, \mathcal{A} either performs an encryption-, decryption- or challenge query:
 - Encryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, M_i, \Psi\rangle = \sum_{a,m,\gamma} \alpha_{a,m,\gamma} |a,m,\gamma\rangle$. N_i must not have been used in a previous encryption query. \mathcal{C} performs the authenticated decryption on each "entry" in the superposition state through the transformation

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \mathbf{E}_{K}^{N_{i},a}(m) \right\rangle$$

• Decryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, C_i, \Psi'\rangle = \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma'\rangle$. \mathcal{C} performs the authenticated encryption on each "entry" in the superposition state except those that were results or previous challenge queries through the transformation

$$\sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} \left| a,c,\gamma' \right\rangle \to \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} \left| a,c,\gamma' \oplus f_{\mathrm{dec}}(a,c) \right\rangle$$

where

$$f_{\text{dec}}(a,c) = \begin{cases} \bot & \text{if } c \in \mathfrak{D} \\ \mathbf{D}_{K}^{N_{i},a}(c) & \text{otherwise.} \end{cases}$$

- Challenge query: \mathcal{A} decides on two classical triples (N_i^0, A_i^0, M_i^0) and (N_i^1, A_i^1, M_i^1) . \mathcal{C} then returns the encryption $C^* = \mathbf{E}_{K}^{N_i^b, A_i^b}(M_i^b)$. \mathcal{C} adds C^* to \mathfrak{D} .
- 3. \mathcal{A} outputs a bit b'. \mathcal{A} wins if b' = b.

The advantage of \mathcal{A} is

$$ADV^{IND-qCCA}(\mathcal{A}) = |Pr[b' = 1 | b = 1] - Pr[b' = 1 | b = 0]|$$

Replacing Nonces with Randomization. Recall Section 1.2, where we discussed noncebased versus randomized security. The original security definitions from Boneh and Zhandry [BZ13b] assume random IVs instead of nonces. In this work, we consider a nonce-based setting, with our security games formalizing a nonce-respecting adversary. All our nonce-based security games from Definitions 2 to 5 can be modelled with randomized IVs instead by making two modifications:

- 1. For encryption queries, require N_i to be chosen uniformly at random.
- 2. By chance, a random N_i may have been used in a previous encryption query.

Beyond that, the randomized variants of the security definitions and games are identical to their nonce-based counterparts. In the remainder of this work, we will use the prefix "\$" to identify the randomized variants (e.g. \$IND-qCPA instead of IND-qCPA). These randomized variants are equivalent to the original security definitions from [BZ13b], except that the original definitions did not consider associated data as an input parameter for queries. Since the associated data is authenticated but not encrypted in AEAD schemes, it does not impact security in the sense of indistinguishability. We therefore allow ourselves to override the notation \$IND-q{CPA,CCA} to also mean the original versions (without associated data), if it is clear from context.

3.2 Nonce-Based, Quantum Challenge Queries (qIND-q{CPA,CCA})

As discussed in Section 1, Chevalier et al. [CEV22a] introduce definitions for the Q2 security of encryption schemes.¹ Both qIND-q{CPA,CCA} follow a real-or-random paradigm, where the oracle in the random world is represented by a compressed random oracle, denoted as H (see Section 2).

H is associated with a state vector \mathcal{D} stored in an additional register. Conceptually, \mathcal{D} acts as a database initialized with tuples of the form (X, \bot) for all $X \in \mathcal{X}$, where \mathcal{X} represents the adversary's query space. In this case, we denote the initialization by $\mathcal{D}(X) = \bot$. After *q* queries, the state of the oracle will be a superposition of such databases. In our setting, each *X* corresponds to a triple consisting of a nonce, associated data, and a message. As queries are made, \mathcal{D} is updated such that after ℓ different inputs X_i with $0 \le i < \ell$, \mathcal{D} contains at most ℓ tuples of the form $(X_i, (X'_i, C'_i))$, where $\mathcal{D}(X_i) = (X'_i, C'_i)$. Here, C'_i retains the same nonce and associated data as X_i , but the message is replaced with a random string M'_i . The ciphertext C'_i is obtained by calling the oracle *H* on X'_i , i.e., $H(X'_i) = C'_i$.

For clarity, we may write $\mathcal{D}(N_i, A_i, M_i)$ instead of $\mathcal{D}(X_i)$, explicitly indicating the nonce N_i , associated data A_i , and message M_i . Further, we write $\mathcal{D}^{-1}(N_i, A_i, C'_i) = M_i$ to retrieve the message M_i associated with the tuple $((N_i, A_i, M_i), ((N_i, A_i, M'_i), C'_i))$.

Similar to Section 3.1, we redefine qIND-q{CPA,CCA} in Definition 4 to include nonces and associated data which makes them applicable to nonce-based authenticated encryption schemes.

Definition 4 (qIND-qCCA game with nonce and associated data). Let \mathcal{A} be a *q*-query qIND-qCCA adversary and \mathcal{C} an qIND-qCCA challenger with access to an authenticated encryption oracle (\mathbf{E}, \mathbf{D}).

- 1. C chooses a key K and a bit $b \in \{0, 1\}$ uniformly at random.
- 2. For each query $1 \leq i \leq q$, \mathcal{A} either performs an encryption-, decryption- or challenge query:
 - Encryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, M_i, \Psi\rangle = \sum_{a,m,\gamma} \alpha_{a,m,\gamma} |a,m,\gamma\rangle$. N_i must not have been used in a previous encryption query. \mathcal{C} performs the authenticated decryption on each "entry" in the superposition state through the transformation

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \mathbf{E}_{K}^{N_{i},a}(m) \right\rangle$$

• Decryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, C_i, \Psi'\rangle = \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma'\rangle$.

If b = 1, C performs the authenticated decryption on each "entry" in the superposition state through the transformation

$$\sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} \left| a,c,\gamma' \right\rangle \to \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} \left| a,c,\gamma' \oplus \mathbf{D}_{K}^{N_{i},a}(c) \right\rangle \,.$$

Else, C calls a compressed random oracle H. \overline{D} is the updated database D.

$$\sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma'\rangle \otimes |\mathcal{D}\rangle \to \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma' \oplus \bar{\mathcal{D}}^{-1}(N_i,a,c)\rangle \otimes |\bar{\mathcal{D}}\rangle \ .$$

¹More precisely, they propose two variants: qIND-qCCA1 and qIND-qCCA2. In this work, qIND-qCCA refers specifically to qIND-qCCA2.

• Challenge query: \mathcal{A} chooses classical nonce N_i and state $|A_i, M_i, \Psi\rangle = \sum_{a,m,\gamma} \alpha_{a,m,\gamma} |a,m,\gamma\rangle$.

If b = 1, C performs the authenticated encryption on each "entry" in the superposition state through the transformation

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \mathbf{E}_{K}^{N_{i},a}(m) \right\rangle$$

Else, C calls a compressed random oracle H. \overline{D} is the updated database D.

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \otimes \left| \mathcal{D} \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \bar{\mathcal{D}}(N_i,a,m) \right\rangle \otimes \left| \bar{\mathcal{D}} \right\rangle \,.$$

3. \mathcal{A} outputs a bit b'. \mathcal{A} wins if b' = b.

The advantage of \mathcal{A} is

$$ADV^{qIND-qCCA}(\mathcal{A}) = |Pr[b' = 1 | b = 1] - Pr[b' = 1 | b = 0]|$$

By disallowing decryption queries, we obtain the qIND-qCPA game.

Replacing Nonces with Randomization. Again, we can turn the qIND-q{CPA,CCA} games from Definition 4 into a randomized variant by making the same modifications as explained at the end of Section 3.1. The subsequent, randomized variants will be denoted as \$qIND-q{CPA,CCA} and are equivalent to the original security definitions from [CEV22a], except that these original definitions did not consider any associated data input. If it is clear from context, we also write \$qIND-q{CPA,CCA} to mean the original definitions (without associated data).

3.3 Real-or-Random Nonce-Based IND-q{CPA,CCA}

In Section 6, our proof method makes use of reductions between security definitions that use different conditions to determine the success of an adversary in a challenge query. In particular, the security definitions considered in this work either employ the *left-or-right* (LoR, e.g. IND-q{CPA,CCA}) or the *real-or-random* (RoR, e.g. qIND-q{CPA,CCA}) approach for challenge queries.

In preparation to Section 6, we define the real-or-random variants of the IND-q{CPA,CCA} games in Definition 5. Afterwards, we will show that the left-or-right variants from Definitions 2 and 3 and the real-or-random variants from Definition 5 are equivalent.

Definition 5 (IND-qCCA[RoR] with nonce and associated data). Let \mathcal{A} be a q-query IND-qCCA[RoR] adversary and \mathcal{C} an IND-qCCA[RoR] challenger with access to an authenticated encryption oracle (\mathbf{E}, \mathbf{D}). Let the compressed random oracle H be defined as in Section 3.2.

1. C chooses a key K and a bit $b \in \{0, 1\}$ uniformly at random.

(

- 2. For each query $1 \le i \le q$, \mathcal{A} either performs an encryption-, decryption- or challenge query:
 - Encryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, M_i, \Psi\rangle = \sum_{a,m,\gamma} \alpha_{a,m,\gamma} |a,m,\gamma\rangle$. N_i must not have been used in a previous encryption query. \mathcal{C} performs the authenticated encryption on each "entry" in the superposition state through the transformation

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \mathbf{E}_{K}^{N_{i},a}(m) \right\rangle$$

• Decryption query: \mathcal{A} chooses classical nonce N_i and state $|A_i, C_i, \Psi'\rangle = \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma'\rangle$.

If b = 1, C performs the authenticated decryption on each "entry" in the superposition state through the transformation

$$\sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} \left| a,c,\gamma' \right\rangle \to \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} \left| a,c,\gamma' \oplus \mathbf{D}_{K}^{N_{i},a}(c) \right\rangle$$

Else, C calls a compressed random oracle H. \overline{D} is the updated database D.

$$\sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma'\rangle \otimes |\mathcal{D}\rangle \to \sum_{a,c,\gamma'} \alpha_{a,c,\gamma'} |a,c,\gamma' \oplus \bar{\mathcal{D}}^{-1}(N_i,a,c)\rangle \otimes |\bar{\mathcal{D}}\rangle$$

• Challenge query: \mathcal{A} decides on a classical triple (N_i, A_i, M_i) .

If b = 1, C then returns the encryption $C^* = \mathbf{E}_K^{N_i, A_i}(M_i)$. Else, C calls a compressed random oracle H. \overline{D} is the updated database D. C returns $C^* = \overline{D}(N_i, A_i, M_i)$.

3. \mathcal{A} outputs a bit b'. \mathcal{A} wins if b' = b.

The advantage of \mathcal{A} is

$$ADV^{IND-qCCA[RoR]}(\mathcal{A}) = |Pr[b' = 1 | b = 1] - Pr[b' = 1 | b = 0]|.$$

By disallowing decryption queries, we obtain the IND-qCPA[RoR] game.

Lemma 1. Security in the IND-qCCA[RoR] sense implies security in the IND-qCCA sense and vice versa.

Proof. [Lemma 1] Assume two adversaries: $\mathcal{A}[\text{LoR}]$ plays the IND-qCCA game with challenger $\mathcal{C}[\text{LoR}]$ and $\mathcal{A}[\text{RoR}]$ plays the IND-qCCA[RoR] game with challenger $\mathcal{C}[\text{RoR}]$.

We define two games. In the first game G_1 , $\mathcal{A}[\text{RoR}]$ tries to mimic the IND-qCCA challenger $\mathcal{C}[\text{LoR}]$. For this, $\mathcal{A}[\text{RoR}]$ chooses bit $b' \in \{0, 1\}$. When $\mathcal{A}[\text{LoR}]$ makes a challenge query $(N_i^0, A_i^0, M_i^0), (N_i^1, A_i^1, M_i^1), \mathcal{A}[\text{RoR}]$ forwards $(N_i^{b'}, A_i^{b'}, M_i^{b'})$ to $\mathcal{C}[\text{RoR}]$. When $\mathcal{A}[\text{LoR}]$ makes a guess $b'', \mathcal{A}[\text{RoR}]$ outputs 1 if b'' = b' and 0 otherwise. This is, in fact, equivalent to the scenario from the proof of [BDJR97, Theorem 1]. It holds:

$$ADV^{IND-qCCA}(\mathcal{A}[LoR]) \le 2 \cdot ADV^{IND-qCCA[RoR]}(\mathcal{A}[RoR]).$$

In the second game G_2 , $\mathcal{A}[\text{LoR}]$ tries to mimic the IND-qCCA[RoR] challenger $\mathcal{C}[\text{RoR}]$. Every encryption- and decryption query from $\mathcal{A}[\text{RoR}]$ gets forwarded to $\mathcal{C}[\text{LoR}]$ by $\mathcal{A}[\text{LoR}]$. When $\mathcal{A}[\text{RoR}]$ makes a challenge query of the form (N_i, A_i, M_i) , $\mathcal{A}[\text{LoR}]$ chooses a random triple (X_i, Y_i, Z_i) and sends (X_i, Y_i, Z_i) , (N_i, A_i, M_i) as their own challenge query to $\mathcal{C}[\text{LoR}]$. Again, the result is returned to $\mathcal{A}[\text{RoR}]$. When $\mathcal{A}[\text{RoR}]$ guesses b' = 1 (real) then $\mathcal{A}[\text{LoR}]$ also guesses b'' = 1 and 0 otherwise. This fits the setting of the proof of [BDJR97, Theorem 2]. It holds:

$$ADV^{IND-qCCA[RoR]}(\mathcal{A}[RoR]) \le ADV^{IND-qCCA}(\mathcal{A}[LoR]).$$

Lemma 2. Security in the IND-qCPA[RoR] sense implies security in the IND-qCPA sense and vice versa.

Proof. [Lemma 2] The proof is identical to that of Lemma 1, as the correctness of the result relies solely on the handling of challenge queries which are dealt with identically in IND-qCPA and IND-qCCA. $\hfill \Box$

3.4 Relevance of Notions with Classical Challenge Queries

The original \$qIND-q{CPA,CCA} notions are strictly stronger than [BZ13b]'s original \$IND-q{CPA,CCA}, respectively [CEV22b, CEV22a]. There are several reasons why we still decide to focus on the security definitions from [BZ13b] instead. Our research has been motivated to some extent by the desire to develop tools to analyse the security of existing AE schemes that may be used in practice and to understand how resistant such schemes may be to quantum attackers. As pointed out in [CEV22a], "various symmetric encryption schemes including stream cipher and some block cipher modes of operation such as CFB, OFB, CTR" are insecure in the \$qIND-qCCA sense. On the other hand, the aforementioned modes, stream ciphers and also the CBC mode are known to be secure in the \$IND-qCPA sense (when the block cipher is a PRP, or a qPRP) [ATTU16]. If we examine generic composition, but exclude stream ciphers and all common block cipher modes from the symmetric encryption component, there are hardly any schemes left. In other words, for symmetric encryption, we can't require \$qIND-qCPA security.

Beyond necessity, there is also practical relevance. From a theoretical point of view, the approach from [BZ13b] (distinguish challenge from learning queries and restrict superposition data to learning queries) seem artificial. In that sense, one can regard those notions as a step towards the notions from [CEV22a], where all queries can handle superposition data. However, the purpose of theoretical security games is to model practical attack settings. If a system communicates through quantum channels with the outside world, a matching security game *must* allow learning queries to handle superposition data. On the other hand, challenge query data represents confidential information the adversary is interested in. In most attack settings, such data will be classical, and a matching security game *can* thus restrict challenge queries to classical inputs and outputs. This renders $IND-q\{CPA,CCA\}$ from [BZ13b] relevant in their own right.

The arguments above do not only hold for \$IND-q{CPA,CCA}, from [BZ13b], but also for their nonce-based counterparts IND-q{CPA,CCA} defined by us in Definitions 2 and 3.

4 Quantum Security Definitions for Authenticity

Classical unforgeability notions like SUF-CMA cannot be modified easily to be applicable in the Q2 setting as any system in this model is subject to various properties unique to a quantum system. When we consider MACs in the Q2 setting, these MACs need to be able to handle superposition queries and are restricted by no-cloning [Die82, WWZ82] and measurement behaviour [AGM18]. As of writing, there are two security notions that are dominantly used to measure post-quantum unforgeability of MACs: plus-one unforgeability [BZ13a] and blind unforgeability [AMRS20].

Boneh and Zhandry proposed what we will call *plus-one unforgeability* (PO), whereas an adversary may query an oracle q times and must produce q + 1 valid pairs of message and authentication tag to win [BZ13a]. PO is described in Definition 6.

Definition 6 (PO Game). Let \mathcal{A} be a q-query PO adversary and \mathcal{C} a PO challenger with access to the MAC oracle F.

- 1. C generates a key K uniformly at random.
- 2. For each query $1 \le i \le q$:

- \mathcal{A} chooses *n*-qubit input-output state $|M_i, \Psi\rangle = \sum_{m,\gamma} \alpha_{m,\gamma} |m, \gamma\rangle$.
- C signs each "entry" in the superposition state through the transformation

$$\sum_{m,\gamma} \alpha_{m,\gamma} \left| m, \gamma \right\rangle \to \sum_{m,\gamma} \alpha_{m,\gamma} \left| m, \gamma \oplus F_K(m) \right\rangle$$

- When the signing oracle is stateful or randomized, an additional classical value N_i is chosen beforehand. For a stateful oracle, $N_i \notin \{N_1, \ldots, N_{i-1}\}$; for a randomized oracle, N_i is chosen uniformly at random. As it is classical, the same N_i is used for the signing in each "entry" of the superposition.
- 3. \mathcal{A} decides on q+1 classical message-tag pairs $\{(M_1^*, T_1^*), \ldots, (M_{q+1}^*, T_{q+1}^*)\}$. \mathcal{A} wins if $F_K(M_i^*) = T_i^*$ for all pairs $1 \le j \le q+1$.

Alagic et al. [AMRS20] point out a "problem with PO-unforgeability". For random $f, g, h : \{0, 1\}^n \to \{0, 1\}^n$, and $p \in \{0, 1\}^n$, the function $M_{f,g,h,p} : \{0, 1\} \times \{0, 1\}^n \to \{0, 1\}^n \times \{0, 1\}^n$ is defined by

$$M_{f,g,h,p}(b,x) = \begin{cases} g(x \mod p) & || & f(x) & \text{if } b = 1\\ 0^n & || & h(x) & \text{if } b = 0, x \neq p\\ 0^n & || & 0^n & \text{if } b = 0, x = p \end{cases}$$
(1)

Here (f, g, h, s) is the secret key. As it turns out, F is PO-unforgeable. Despite F's PO unforgeability, an attacker can recover the secret s by quantum period finding techniques, making only queries to $M_{f,g,h,p}(1, \cdot)$, and then forge $M_{f,g,h,p}(0, 0) = 0^n ||0^n$. Note that the period finding techniques imply that, after making q queries for $M_{f,g,h,p}(1, |x\rangle)$, the adversary will know $M_{f,g,h,p}(0,0) = 0^n \times 0^n$, but strictly less than q pairs $(x_i, M_{f,g,h,p}(1, x_i))$.

This can be seen as a practical vulnerability. Consider all queries starting with a prefix "From Eve". The challenger can even check if the learning queries start with "From Eve" or not. Nevertheless, the adversary presents a forged message starting with "From Bob". This issue motivated the authors to propose the concept of *blind unforgeability* (BU) [AMRS20, Definition 1]. They made two claims, which jointly would indicate blind unforgeability to be strictly stronger than PO authentictity:

- 1. a MAC exists, which is PO secure but not blindly unforgeable (see $M_{p,f,g,h}$ from Definition 10), and
- 2. every blindly unforgeable MAC is also PO secure.

While the first claim sticks, the authors subsequently withdrew the second one [AMRS18, Revision from 2023-04-20] as the proof of that claim had been found to be inconclusive. Therefore, currently it is an unproven conjecture that BU is stricly stronger than PO.

In [BN00, BN08], Bellare and Namprempre define INT-PTXT and INT-CTXT for authenticated encryption. In Definition 7, we use PO unforgeability to describe a matching security notion to INT-CTXT for the quantum case.

Definition 7 (PO-CTXT Game). Let \mathcal{A} be a *q*-query PO-CTXT adversary and \mathcal{C} a PO-CTXT challenger with access to an authenticated encryption oracle (\mathbf{E}, \mathbf{D}) .

- 1. $\mathcal C$ generates a key K uniformly at random.
- 2. For each query $1 \le i \le q$:
 - \mathcal{A} chooses a classical nonce $N_i \notin \{N_1, \ldots, N_{i-1}\}$. Furthermore, they choose a state $|A_i, M_i, \Psi_i\rangle = \sum_{a,m,\gamma} \alpha_{a,m,\gamma} |a,m,\gamma\rangle$ for associated data and message inputs (possibly in superposition) and output register $|\Psi\rangle$.
 - ${\mathcal C}$ performs the authenticated encryption on each "entry" in the superposition

state through the transformation

$$\sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \right\rangle \to \sum_{a,m,\gamma} \alpha_{a,m,\gamma} \left| a,m,\gamma \oplus \mathbf{E}_{K}^{N_{i},a}(m) \right\rangle$$

whereas $\Gamma_i = \mathbf{E}_K^{N_i,a}(m)$ encloses both the ciphertext C_i and the authentication tag T_i (e.g. through concatenation).

3. \mathcal{A} decides on q + 1 triples (N_j, A_j, Γ_j) with $\Gamma_j = (C_j, T_j)$ for ciphertext and authentication tag respectively. \mathcal{A} wins if $\mathbf{D}_K^{N_j, A_j}(\Gamma_j) \neq \bot$ for all $1 \leq j \leq q + 1$.

In [Zha21], the terminology of a quantum pseudorandom function (qPRF) is introduced, which we revisit in Definition 8. The strongest security requirement for a MAC is that it is indistinguishable from a (q)PRF. In Section 6, we achieve results about the quantum security of generic compositions for authenticated encryption by considering such MACs.

Definition 8 (Quantum Pseudorandom Function (qPRF)). Consider a function $F : \{0,1\}^{\kappa} \times \{0,1\}^n \to \{0,1\}^m$ and $k \in \{0,1\}^{\kappa}$ chosen uniformly at random. F is a pseudorandom function (PRF) if no efficient adversary can distinguish $F(k, \cdot)$ from a truly random function $\pi : \{0,1\}^n \to \{0,1\}^m$ with significant probability. F is a qPRF if no efficient quantum adversary making superposition queries can distinguish between a truly random function and $F(k, \cdot)$.

5 Encrypt-then-MAC with Plus-One Unforgeability

In the classical case, Bellare and Namprempre [BN00, BN08] show that when an IND-CPA secure symmetric encryption algorithm is combined with a SUF-CMA secure MAC using the Encrypt-then-MAC paradigm, the resulting authenticated encryption scheme is provably INT-CTXT and IND-CCA secure.

In this section, we will demonstrate that Bellare and Namprempre's result does not carry over to the quantum case when considering security definitions IND-qCPA, IND-qCCA and PO from Definitions 2, 3 and 6. We show that there exists an Encrypt-then-MAC composition of an IND-qCPA secure symmetric encryption scheme \widehat{SE} with a PO secure MAC F where the resulting authenticated encryption scheme AE is neither PO-CTXT nor IND-qCCA secure. Theorem 1 represents the main result of this section.

Theorem 1. If IND-qCPA secure encryption schemes and qPRFs exist, then there exists an IND-qCPA secure encryption scheme \widehat{SE} and a Plus-One unforgeable MAC F, such that the Encrypt-then-MAC composition of \widehat{SE} and F is IND-qCCA insecure.

Roadmap for this Section. We start by defining \widehat{SE} in Definition 9 which is IND-qCPA secure (Lemma 3), but not IND-qCCA secure (Lemma 4).

Next, we define the MAC $F = F_{p,f,g,h,\mathbf{R}}$. Definition 10 recalls the function $M = M_{p,f,g,h}$ from [AMRS20, Construction 3], which is PO secure ([AMRS20, Theorem 21]). We use M to specify F in Definition 11. As it turns out, F inherits the PO security from M (Lemma 6). In Lemma 7 we show that F also inherits the weakness from M: an adversary can successfully predict a valid authentication tag for a specific input.

Finally, we apply the EtM composition to \widehat{SE} and F. The resulting authenticated encryption scheme AE is described in Definition 12. Our main result (Theorem 1) follows from the fact that AE is not IND-qCCA secure (Lemma 8).

For completeness, we show that AE is PO-CTXT secure (Theorem 2).

5.1 The Symmetric Encryption Scheme SE

Definition 9. Let SE = (E, D) be a symmetric encryption algorithm. Further, let $K \in \{0, 1\}^{\kappa}$ be a secret key, $M, C \in \{0, 1\}^n$ be the plain- and ciphertext respectively and $N \in \{0, 1\}^{\nu}$ be a nonce or initialisation vector for statefulness or randomization. We construct a symmetric encryption scheme $\widehat{SE} = (\widehat{E}, \widehat{D})$:

$$\begin{split} \widehat{E}_K^N(M) &= \begin{cases} 0^n & \text{if } M = K \text{ and } N = 0^\nu, \\ E_K^N(M) & \text{else.} \end{cases} \\ \widehat{D}_K^N(C) &= \begin{cases} K & \text{if } C = 0^n \text{ and } N = 0^\nu, \\ D_K^N(C) & \text{else.} \end{cases} \end{split}$$

Note that \widehat{SE} is formally an encryption scheme, as specified in Section 2, but an incorrect one: For $M_0 = D_K^N(0^{\nu})$ it holds that $\widehat{D}_K^N(\widehat{E}_K^N(M_0)) = K$, and most likely $K \neq M_0$.

Lemma 3. If SE is IND-qCPA secure, then \widehat{SE} is also IND-qCPA secure.

Proof. [Lemma 3] We will employ the semi-classical O2H theorem from [AHU19]. Start by defining two functions:

$$H(X,Y) = E_K^I(X)$$

$$G(X,Y) = \begin{cases} 0^n & \text{if } X = K \text{ and } Y = 0^\nu, \\ E_K^Y(X) & \text{else.} \end{cases}$$

Let \mathcal{A} be a *q*-query IND-qCPA adversary. The goal of \mathcal{A} is to distinguish the outputs of H from the one of G. We observe that H and G are identical except for the case where $(X, Y) = (K, 0^{\nu})$. Let the event FIND be defined as follows:

- For G: FIND occurs if the oracle returns 0^n .
- For *H*: Since *H* does not have a special case for $(X, Y) = (K, 0^{\nu})$, FIND will not occur when interacting with *H*. The output will always be $E_K^Y(X)$ and thus be pseudorandom.

Further, let P_{find} be the probability that FIND occurs. Let $ADV^{H,G}(\mathcal{A})$ denote \mathcal{A} 's advantage to distinguish H from G. The semi-classical O2H theorem [AHU19, Theorem 1] allows us to bound this advantage:

$$\operatorname{ADV}^{H,G}(\mathcal{A}) \leq 2\sqrt{(q+1)P_{\operatorname{find}}}.$$

Let P_{max} be the maximal probability that \mathcal{A} finds K. We have:

$$P_{\max} = \frac{1}{2^n}.$$

In [AHU19, Corrollary 1] the adversary is defined as having an input z. In our case, z is the empty string. Let \mathcal{S} denote the set of all inputs (X, Y) for which $H(X, Y) \neq G(X, Y)$. It holds that $\mathcal{S} = \{(K, 0^{\nu})\}$. Clearly, z and \mathcal{S} are independent. Given this fact, we can use [AHU19, Corrollary 1], to deduce

$$P_{\text{find}} \le 4q \cdot P_{\text{max}} \le 4q \cdot \frac{1}{2^n}.$$

Thus, A's advantage to distinguish F from G is

$$\operatorname{ADV}^{F,G}(\mathcal{A}) \le 4\sqrt{(q+1) \cdot \frac{q}{2^n}}$$

Since P_{find} is negligible for a sufficiently large *n*, we conclude our proof.

Lemma 4. \widehat{SE} is not IND-qCCA secure. Namely, there exists an adversary \mathcal{A} that can win the IND-qCCA game against \widehat{SE} with advantage

$$ADV_{\widehat{SE}}^{IND-qCCA}(\mathcal{A}) = 1.$$

Proof. [Lemma 4] An IND-qCCA adversary can ask for the decryption of $(0^n, 0^n)$ to receive the secret key K with probability 1.

5.2 The MAC F

Definition 10. Let $p \in \{0,1\}^n$ be a random period and $f, g, h : \{0,1\}^n \to \{0,1\}^n$ be random functions. For the secret key (p, f, g, h), we define

$$M_{p,f,g,h}(b,x) = \begin{cases} g(x \mod p) & || & f(x) & \text{if } b = 1, \\ 0^n & || & h(x) & \text{if } b = 0, x \neq p, \\ 0^n & || & 0^n & \text{if } b = 0, x = p. \end{cases}$$

Lemma 5 ([AMRS20, Theorem 21]). The function $M_{p,f,g,h}$ is PO secure.

Definition 11. Assume M, p, f, g, h from Definition 10 and a qPRF $\mathbf{R} : (\{0, 1\}^*)^3 \to \{0, 1\}^{n-1}$. We construct the MAC F under key (p, f, g, h, \mathbf{R}) for inputs of nonce $N \in \{0, 1\}^{\nu}$, associated data A and message X which can be of variable length from 0 to n.

$$F_{p,f,g,h,\mathbf{R}}^{N}(X,A) = \begin{cases} M_{p,f,g,h}(0,(0||A)) & \text{if } N = 0^{\nu}, X = 0^{n} \text{ and } |A| = n - 1, \\ M_{p,f,g,h}(1,A) & \text{if } N = 1^{\nu}, |X| = 0 \text{ and } |A| = n \\ M_{p,f,g,h}(0,(1||\mathbf{R}(N,X,A))) & \text{else.} \end{cases}$$

Lemma 6. $F_{p,f,g,h,\mathbf{R}}$ is plus-one unforgeable. Namely, there does not exist any q-query PO adversary \mathcal{A} against F that can return q + 1 disjoint quadruples (N_j, X_j, A_j, T_j) with $T_j = F_{p,f,g,h,\mathbf{R}}^{N_j}(X_j, A_j)$ with non-negligible probability.

Proof. [Lemma 6] Assume F not to be PO secure. I.e., an efficient \mathcal{A} exists, which makes q queries of form $(N_i, |X_i\rangle, |A_i\rangle)$ to receive $|T_i\rangle = |F_{p,f,g,h,\mathbf{R}}^{N_i}(X_i, A_i)\rangle$ and then produces q+1 disjoint classical quadruples of (N_j, X_j, A_j, T_j) with $T_j = F_{p,f,g,h,\mathbf{R}}^{N_j}(X_j, A_j)$.

Observe that each evaluation of $F_{p,f,g,h,\mathbf{R}}$ implies making exactly one call to the function $M_{p,f,g,h}$. Additionally, checking if $F_{p,f,g,h,\mathbf{R}}^{N_j}(X_j, A_j) = T_j$ implies one evaluation of $M_{p,f,g,h}(b_j, x_j)$ with input parameters (b_j, x_j) derived from (N_j, X_j, A_j) . If all those input parameters are disjoint with $(b_i, x_i) \neq (b_j, x_j)$ for all $i \neq j$, then we have a set of q + 1 disjoint inputs to $M_{p,f,g,h}$, after making only q queries. This implies breaking the PO security of $M_{p,f,g,h}$, which is infeasible, according to Lemma 5.

So for the rest of this proof, assume there is some $i \neq j$ with $(b_i, x_i) = (b_j, x_j)$. To finish the proof, we argue that it is infeasible to find any $(N_i, X_i, A_i) \neq (N_j, X_j, A_j)$ with $(b_i, x_i) = (b_j, x_j)$.

Definition 11 derives (b, x) from (N, X, A) by applying either of these three cases:

- 1. If $N = 0^{\nu}$, $X = 0^{n}$ and |A| = n 1, then (b, x) = (0, (0||A)),
- 2. if $N = 1^{\nu}$, |X| = 0 and |A| = n, then (b, x) = (1, A),
- 3. otherwise: $(b, x) = (0, (1 || \mathbf{R}(N, X, A))).$

Note that F sets b = 1 in case 2, and b = 0 in both case 1 and case 3. In case 1, the first bit of x is 0 while in case 3, the first bit of x is 1. Thus, $(b_i, x_i) = (b_j, x_j)$ can only hold if both (b_i, x_i) and (b_j, x_j) are derived by applying the same case.

If (b_i, x_i) and (b_j, x_j) are both derived using case 1, then $(N_i, X_i, A_i) = (0^{\nu}, 0^n, A_i)$ and $(N_j, X_j, A_j) = (0^{\nu}, 0^n, A_j)$. Thus, $(b_i, x_i) = (b_j, x_j)$ would imply $x_i = x_j$, which would imply $A_i = A_j$ in contradiction to $(N_i, X_i, A_i) \neq (N_j, X_j, A_j)$. Similarly, if (b_i, x_i) and (b_j, x_j) are both derived using case 2, it holds that $b_i = b_j$, and $x_i = x_j$ would contradict $(N_i, X_i, A_i) \neq (N_j, X_j, A_j)$.

So $(N_i, X_i, A_i) \neq (N_j, X_j, A_j)$ with $(b_i, x_i) = (b_j, x_j)$ can only occur if both (b_i, x_i) and (b_j, x_j) are derived using case 3. In fact, $(b_i, x_i) = (b_j, x_j)$ is equivalent to finding a collision $\mathbf{R}(N_i, X_i, A_i) \neq \mathbf{R}(N_j, X_j, A_j)$ for a random function. Zhandry's qPRP/qPRF switching lemma states that finding such a collision is infeasible. More precisely, it requires $\Omega(2^{n/3})$ queries to \mathbf{R} [Zha13].

We conclude that any successful PO adversary \mathcal{A} would have to solve an infeasible problem. \Box

Lemma 7. An adversary \mathcal{A} queries $F_{p,f,g,h,\mathbf{R}}$ with $N = 1^{\nu}$, |X| = 0 and $|A\rangle$ in superposition. When $p < 2^{\frac{n}{2}}$, \mathcal{A} can predict the authentication tag $T^* = 0^{2n}$ for a triple (N^*, X^*, A^*) with $N^* = 0^{\nu}$, $X^* = 0^n$ and $A^* = p$ with $|A^*| = n - 1$.

Proof. [Lemma 7] It is known that $M_{p,f,g,h}$ is not BU secure [AMRS20, AMRS18]. This observation is based on applying period finding to recover p. The proof of Lemma 7 is based on a similar idea.

Consider \mathcal{A} choosing a classical nonce N and making one query of form

$$\sum_{a \in \{0,1\}^n} \alpha_a \left| a \right\rangle \otimes \sum_{t \in \{0,1\}^{2n}} \alpha_t \left| t \right\rangle$$

to $F_{p,f,q,h,\mathbf{R}}$, which transforms the state to

¢

$$\sum_{a \in \{0,1\}^n} \alpha_a \left| a \right\rangle \otimes \sum_{t \in \{0,1\}^{2n}} \alpha_t \left| t \oplus F_{p,f,g,h,\mathbf{R}}^N(\epsilon,a) \right\rangle$$

Note that \mathcal{A} has left the message X empty. For each "entry" of this superposition state, $F_{p,f,g,h,\mathbf{R}}$ calls $M_{p,f,g,h}$ with bit b = 1. The state can therefore be represented as

$$\sum_{a \in \{0,1\}^n} \alpha_a |a\rangle \otimes \sum_{t \in \{0,1\}^{2n}} \alpha_t |t \oplus M_{p,f,g,h}(1)|a\rangle$$

This triggers $M_{p,f,g,h}$ to evaluate the function g, which contains the hidden period p:

$$\sum_{a \in \{0,1\}^n} \alpha_a \left| a \right\rangle \otimes \sum_{t \in \{0,1\}^{2n}} \alpha_t \left| t \oplus \left(g(a \bmod p) || f(a) \right) \right\rangle$$

Whereas the output from g is always an n-bit value. \mathcal{A} can efficiently extract p from the transformed state by using quantum period finding (e.g. Shor's Algorithm [Sho94, Mer07]).

Having calculated p, \mathcal{A} sets $N^* = 0^{\nu}$, $X^* = 0^n$ and A^* to the n-1-bit representation of p. Observe that, since $p < 2^{n/2}$, n-1 bits for A^* suffice. For this specific choice of inputs, \mathcal{A} can predict the authentication tag $T^* = F_{p,f,g,h,\mathbf{R}}^{N^*}(X^*, A^*) = 0^{2n}$. \Box

5.3 The Authenticated Encryption Scheme AE

Definition 12. Let $M, C \in \{0, 1\}^n$, $A \in \{0, 1\}^*$, $N \in \{0, 1\}^\nu$ and $T \in \{0, 1\}^{2n}$. Following Definition 1, the Encrypt-then-MAC composition of $\widehat{SE} = (\widehat{E}, \widehat{D})$ and F as $AE = (\mathbf{E}, \mathbf{D})$

is given by:

$$\mathbf{E}_{K,f,g,h,p}^{N}(M,A) = \left(\widehat{E}_{K}^{N}(M), F_{f,g,h,p,\mathbf{R}}^{N}(\widehat{E}_{K}^{N}(M),A)\right)$$
$$\mathbf{D}_{K,f,g,h,p}^{N}(C,A,T) = \begin{cases} \widehat{D}_{K}^{N}(C) & \text{if } F_{f,g,h,p,\mathbf{R}}^{N}(C,A) = T, \\ \bot & \text{else.} \end{cases}$$

Lemma 8. AE is not IND-qCCA secure. Namely, there exists an adversary \mathcal{A} that can win the IND-qCCA game against AE with advantage

$$ADV_{AE}^{IND-qCCA}(\mathcal{A}) = 1.$$

Proof. [Lemma 8] Consider the IND-qCCA adversary \mathcal{A} querying AE. \mathcal{A} posts one encryption query of form (N_1, M_1, A_1) to \mathbf{E}_K and receives tuples (C_1, T_1) . Following the approach from Lemma 7, \mathcal{A} can exploit the periodicity of function g in F to efficiently extract the period p using quantum period finding. \mathcal{A} is now able to predict a valid authentication tag $T^* = 0^{2n}$ for the ciphertext $(N^*, C^*, A^*) = (0^{\nu}, 0^n, p)$ with $|A^*| = n - 1$. \mathcal{A} makes a single, valid decryption query to \mathbf{D}_K for (N^*, C^*, A^*, T^*) and receives M^* . Since $\widehat{D}_K(C^*, A^*)$ will always return $M^* = K$ when $C^* = 0^n$, \mathcal{A} will receive the secret key K with probability 1.

Proof. [Theorem 1] \widehat{SE} from Definition 9 is IND-qCPA secure (Lemma 3) and F from Definition 11 is PO secure (Lemma 6). The EtM composition of \widehat{SE} and F is IND-qCCA insecure (Lemma 8).

For the classical proof of IND-CCA security for EtM, [BN00, BN08] consider the INT-CTXT security of an authenticated encryption scheme as an intermediate step. In Definition 7, we define a quantum equivalent of the classical INT-CTXT definition using PO unforgeability and in Theorem 2, we show that the scheme AE from Definition 12 is PO-CTXT secure.

Theorem 2. AE is PO-CTXT secure.

Proof. [Theorem 2] The proof is similar to the proof of Lemma 6. Consider the q-query PO-CTXT adversary \mathcal{B} querying AE. From their q chosen-message queries, \mathcal{B} can either extract q classical ciphertext-tag triples (C_q, A_q, T_q) or they can find the hidden period p in $F_{p,f,g,h,\mathbf{R}}$. Finding the hidden period would mean that \mathcal{B} can construct a forgery. Again, as explained in the proof of Lemma 6, \mathcal{B} may not extract both q valid ciphertext-tag pairs **and** the hidden period p in non-negligible time. This means that \mathcal{B} is not able to produce q+1 valid quadruples of ciphertext, tag, associated data and nonce. Every such adversary \mathcal{B} which could win the PO-CTXT game against AE could also be used as a sub-program to win the PO game against F.

6 Encrypt-then-MAC with a qPRF

In Section 5, we study the Encrypt-then-MAC (EtM) composition of an IND-qCPA secure symmetric encryption scheme and a PO secure MAC with the conclusion that this composition does not guarantee IND-qCCA security. Evidently, our proof relies on a specific MAC construction, which has been proven to be PO secure while still suffering from the weakness of not being "blindly unforgeable" as defined in [AMRS20]. Can we replace PO unforgeability by some other (possibly stronger) notion, such as blind unforgeability? Arguably, the strongest possible security definition for a MAC is a pseudorandom function (PRF), or a quantum PRF (qPRF) in the case of quantum algorithms. A qPRF is strictly stronger than either a PO secure MAC or a blindly unforgeable MAC. In this section,

Table 1: Relevant security definitions for our work. The "Challenge" column differentiates between classical and superposition challenge queries, "Nonce" indicates the usage of nonces ("no" means randomness), and "LoR/RoR" distinguishes security in the left-or-right sense from real-or-random security. *\$IND-q{CPA,CCA}* from [BZ13b] are not used in Section 6, but listed for completeness.

Notation	Challenge	Nonce	LoR/RoR	Reference
\$qIND-q{CPA,CCA}	Quantum	No	RoR	[CEV22b, CEV22a]
$IND-q\{CPA,CCA\}[RoR]$	Classical	Yes	RoR	Definition 5
$IND-q\{CPA,CCA\}$	Classical	Yes	LoR	Definitions 2 and 3 $$
$qIND-q\{CPA,CCA\}$	Quantum	Yes	RoR	Definition 4
\$IND-q{CPA,CCA}	Classical	No	LoR	[BZ13b]

our objective is to prove or disprove that using a MAC which behaves like a qPRF and combining it with an IND-qCPA secure symmetric encryption scheme through the EtM composition achieves IND-qCCA secure authenticated encryption.

Roadmap for this Section. This section traverses through several security notions, listed in Table 1. We start with \$qIND-qCCA-security (quantum challenges, randomness-based, real-or-random) by quoting [CEV22a, Theorem 2] as Lemma 9. It states the \$qIND-qCCA security of the EatM composition using a \$qIND-CPA secure encryption scheme and a qPRF. Theorem 3 extends this to IND-qCCA[RoR] security (classical challenges, noncebased, real-or-random). This result is based on the proof given in [CEV22b, Appendix C.4], for [CEV22a, Theorem 2], which we outline below.

Theorem 4 proves the IND-qCCA security (classical challenges, nonce-based, left-or-right) of the EatM composition of an IND-qCPA secure symmetric encryption scheme and a qPRF. As a byproduct, we show that the same argument as in [CEV22b, Appendix C.4] can be used to show the qIND-qCCA security (quantum challenges, nonce-based, left-or-right) of the EatM composition of an qIND-qCPA secure encryption scheme and a qPRF (cf. Lemma 10).

As we are more concerned about the EtM composition (and, to some degree, EaM) and less about the EatM composition, Theorem 5 provides a reduction between the generic composition types EatM, EtM and EaM when constructed from an IND-qCPA secure encryption scheme and a qPRF. The IND-qCCA security of one composition implies IND-qCCA security of the other two. Finally, Corollary 1 highlights this section's main result: The EtM composition and the EaM composition of an IND-qCPA secure symmetric encryption scheme and a qPRF both are IND-qCCA secure.

Lemma 9 (Theorem 2 from [CEV22a]; Theorem 3 from $[CEV22b]^2$). The EatM composition of a \$qIND-qCPA secure symmetric encryption scheme SE and a qPRF F (used as a MAC) is \$qIND-qCCA secure.

This result is not directly useful to us due to the following issues:

- 1. the \$qIND-qCPA notion is too strong for our purposes. Existing state-of-the-art AE schemes are rarely based on a \$qIND-qCPA secure symmetric encryption scheme.
- 2. The EatM composition has never been used in state-of-the-art AE schemes (to the best of our knowledge). Instead, they are often composed through EtM and

 $^{^{2}}$ [CEV22b] is the full paper version of [CEV22a]. Theorem numbering did change between versions.

sometimes through the alternatives of EaM or MtE.

3. The \$qIND-qCPA and \$qIND-qCCA notions use random initialization vectors. As outlined in Section 1.2, we instead use nonces in our definition of qIND-qCCA (Definition 4). For our results, this difference does not pose an obstacle as outlined in the proof for Theorem 3 as well as Lemma 10.

6.1 From \$qIND-qCCA to IND-qCCA

Theorem 3. The EatM composition of an IND-qCPA[RoR] secure symmetric encryption scheme SE and a qPRF F (used as a MAC) is IND-qCCA[RoR] secure.

Proof. [Theorem 3] The proof is almost identical to the proof of Theorem 3 in [CEV22b, Appendix C.4]. We use the same sequence of games G_0 to G_8 with very few modifications. For each of the eight games in the original proof, we briefly revisit the main idea of the original proof before we explain how it must be adapted to fit our argument.

Game G_0 : This is the \$qIND-qCCA attack game³ from [CEV22b, Definition 2].

 \rightarrow In our case, this is the IND-qCCA[RoR] game from Definition 5.

Game G_1 : Here, the qPRF is replaced with a random function H'.

Due to a secure qPRF being indistinguishable from a random function (except with negligible probability), this game is indistinguishable from G_0 .

 \rightarrow The transformations in this game are identical in our case.

Game G_2 : Now, in the random world, [CEV22b] implement H' in Zhandry's compressed standard random oracle [Zha19]. The compressed random oracle takes queries of form $|C||X\rangle |Y_2\rangle$ with $|Y_2\rangle$ being \mathcal{A} 's response register. The compressed random oracle's database \mathcal{E} holds a collection of pairs (C||X,T) with X being called the *associated input* for a pair (X,T) such that $(C||X,T) \in \mathcal{E}$. Note that there is only one call to the compressed oracle for each challenge query. Due to the equivalence of the compressed random oracle and the standard ("uncompressed") random oracle, \mathcal{A} 's distinguishing advantage between G_2 and G_1 is 0.

 \rightarrow Our game restricts challenge queries to classical inputs and outputs. The original game, with superpositions in challenge queries, covers our game, since classical data is in a specific superposition: one amplitude is 1, all other amplitudes are 0.

Game G_3 : The decryption oracle in the random world is redefined. A measurement $\mathbb{M}_{\mathcal{E},P}$ is introduced which checks if there exists a pair (X,T) in database \mathcal{E} satisfying the relation $X = D(C) \wedge H'(C||X) = T$ (note that D is the honest unauthenticated decryption). The result is placed into an ancilla register P. If the ciphertext is already part of an entry in database \mathcal{D} , the associated input of said entry is returned. Otherwise, the honest authenticated decryption is called in conjunction with the previously defined measurement $\mathbb{M}_{\mathcal{E},P}$. [CEV22b] show that $\mathbb{M}_{\mathcal{E},P}$ and the authenticated decryption almost commute, therefore those are indistinguishable to \mathcal{A} .

 \rightarrow This game is identical in our case, as decryption queries in IND-qCCA[RoR] are handled in the same way as those in \$qIND-qCCA.

 $^{^{3}}$ Note that, by Lemma 10, the original proof from [CEV22b] also holds when considering the qIND-qCCA attack game from Definition 4 instead of the qIND-qCCA game.

Game G_4 : In the random world, the honest authenticated decryption is replaced by a unitary U_K which uses the ancilla register P which is filled by calling $\mathbb{M}_{\mathcal{E},P}$. The difference to G_3 is that \mathcal{A} can distinguish G_3 and G_4 only if they send a decryption query where the ciphertext is (i) either in \mathcal{E} but not in \mathcal{D} , or (ii) neither in \mathcal{D} nor \mathcal{E} .

For these two options, it holds that

- (i) the authenticated decryption and $\mathbb{M}_{\mathcal{E},P}$ return the same output each time.
- (ii) the adversary can only gain a distinguishing advantage if they pose a valid decryption query which is not associated with any previous query.

[CEV22b] show that the probability to pose such a query is negligible.

 \rightarrow Again, this game is identical in our case, as decryption queries in IND-qCCA[RoR] are handled in the same way as those in \$qIND-qCCA.

Game G_5 : Now, the usage of $\mathbb{M}_{\mathcal{E},P}$ is replaced by a direct database lookup to \mathcal{E} instead. Before this game, the database \mathcal{E} was implicitly used by the projective measurement $\mathbb{M}_{\mathcal{E},P}$. The database lookup to \mathcal{E} grants the same functionality as before. Except for this change, this game is identical to G_4 . This does not impact \mathcal{A} 's advantage.

 \rightarrow This game is identical in our case, as decryption queries in IND-qCCA[RoR] are handled in the same way as those in \$qIND-qCCA.

Game G_6 : Moving to the real world, the decryption oracle now is implemented with a database lookup to \mathcal{E} . From this point onwards, the *authenticated* decryption is no longer needed. Technically, this modification of the real world could have already been introduced in G_3 to G_6 without changing anything substantially about those games. Therefore, the distinguishing advantage of \mathcal{A} remains negligible.

 \rightarrow As with the games before, this game is identical in our case, as decryption queries in IND-qCCA[RoR] are handled in the same way as those in \$qIND-qCCA.

Game G_7 : In the random world, the response to a challenge encryption query is different: now, the adversary receives H'(C||X) with input X and C being the encryption of a random plaintext X'. In G_6 , the adversary receives H'(C||X') instead. A cannot distinguish G_7 from G_6 following from the indistinguishability of H'(C||X) and H'(C||X') due to H'being a random oracle.

 \rightarrow As with the argument for Game G_2 , in our proof, we restrict the adversary to classical challenge queries only. This does not increase \mathcal{A} 's advantage.

Game G_8 : In the final game, the usage of database \mathcal{D} is removed from the decryption oracle in the random world. The only case where the adversary may distinguish G_8 from G_7 is when they pose a decryption query which is in $\mathcal{D} \setminus \mathcal{E}$ with non-negligible weight. Then, the oracle in G_8 responds with \bot , while the oracle in G_7 responds with $X \neq \bot$.

[CEV22b] show that the existence of an efficient distinguisher for G_8 and G_7 would also imply an adversary breaking the bound from Lemma 5 in [Zha19].

 \rightarrow Again, this game is identical in our case, as decryption queries in IND-qCCA[RoR] are handled in the same way as those in \$qIND-qCCA.

Observe that, neither the original nor our modified proof requires any randomness or nonces.

Following the argument from [CEV22b], \mathcal{A} 's advantage in G_8 can be reduced to their advantage against the (unauthenticated) symmetric encryption algorithm SE at hand.

We introduce a separate adversary \mathcal{B} , which runs \mathcal{A} as a subroutine and implements the compressed random oracle for the MAC at hand for each encryption or challenge query. \mathcal{B} forwards \mathcal{A} 's plaintext query states to their challenger, receiving the corresponding ciphertext state. Then, \mathcal{B} computes the tag using their compressed random oracle MAC for this ciphertext state and returns the result to \mathcal{A} .

The advantage of \mathcal{B} against SE is equal to the advantage of \mathcal{A} in G_8 . This leads to

$$\operatorname{Adv}_{G8}^{\operatorname{IND-qCCA[RoR]}}(\mathcal{A}) \leq \operatorname{Adv}_{\operatorname{SE}}^{\operatorname{IND-qCPA[RoR]}}(\mathcal{A}).$$

Theorem 4. The EatM composition of an IND-qCPA secure symmetric encryption scheme SE and a qPRF F (used as a MAC) is IND-qCCA secure.

Proof. [Theorem 4] In Theorem 3, we prove that the result from Lemma 9 also applies to the IND-qCCA[RoR] security of an EatM composition of an IND-qCPA[RoR] encryption scheme and a qPRF. Recall that Lemmas 1 and 2 show the equivalence of IND-q{CPA,CCA}[RoR] to IND-q{CPA,CCA}, respectively. The proof for Theorem 4 therefore follows from combining Lemmas 1 and 2 and Theorem 3.

6.2 Proving qIND-qCCA Security

A by-product from the proof for Theorem 3 above is the following observation, which may be of independent interest.

Lemma 10. The EatM composition of a qIND-qCPA secure symmetric encryption scheme SE and a qPRF F (used as a MAC) is qIND-qCCA secure.

Proof. [Lemma 10] The proof for Lemma 9 (Theorem 2 from [CEV22b]) as well as our proof for Theorem 3 below employ a series of eight games G_i . None of those games requires randomness for the inputs to encryption queries, and none of the arguments made in the proof is based on such randomness.

We remark, that the proofs of Lemma 9 and Theorem 3 also do not rely on unique inputs, which implies the following lemma: The EatM composition of a stateless deterministic qIND-qCPA secure symmetric encryption scheme SE and a $qPRF \ F$ (used as a MAC) is a stateless deterministic qIND-qCCA secure authenticated encryption scheme. This lemma is trivial and of no actual use. As pointed out in Section 1.2, there is no correct stateless deterministic qIND-qCPA secure symmetric encryption scheme SE to begin with.

6.3 From EatM to EtM

In [CEV22a], the authors analyse a generic composition which they refer to as follows: "For the symmetric-key setting, our construction follows the classical Encrypt-then-Mac paradigm, in which we use a pseudorandom function in the role of the MAC scheme" [CEV22a, Page 597]. In fact, they denote with *Encrypt-then-MAC* what we denote with *Encrypt-and+then-MAC* (EatM) as defined in Figure 1. They do not consider other composition methods (e.g. EaM, MtE, EtM) nor do they mention any alternative definitions. It is clear that EatM and EtM are different types of compositions. The definition of EatM is very beneficial to their proof for Lemma 9, and we do not see any obvious way to tweak the proof in order to apply it to EtM instead. The reason is as follows:

As pointed out in Section 6.1, the database \mathcal{E} stemming from the compressed oracle replacing the qPRF maintains a collection of pairs ((C||X), T), where (C||X) is the input

to the oracle and T the matching output. This database holds exactly the information needed to implement the random function H'. But this very same database also holds the information needed to provide an answer X to a decryption query (C,T). For EtM, the input to the oracle would be C, and the output would be T. Thus, a database holding the information needed to implement the random function H' would now hold pairs (C,T) of ciphertext and authentication tag, but no information about the plaintext X. This would be insufficient to respond to decryption queries.

Instead of trying to tweak the proof for Lemma 9, in order to apply it to EtM instead of EatM, we provide a direct reduction between those types of generic composition, which will also include EaM compositions.

Theorem 5. Let SE denote an IND-qCPA secure symmetric encryption scheme, and F be a qPRF. If one of the following three schemes $AE_i = (\mathbf{E}, \mathbf{D})$ is IND-qCCA secure, then all three schemes are IND-qCCA secure:

- AE₁: the Encrypt-and+then-MAC (EatM) composition of SE and F,
- AE₂: the Encrypt-then-MAC (EtM) composition of SE and F, and
- AE₃: the Encrypt-and-MAC (EaM) composition of SE and F.

Corollary 1. Let SE denote an IND-qCPA secure symmetric encryption scheme, and F a qPRF. If the EatM composition AE_3 of SE and F is IND-qCCA secure, then both the EtM composition AE_2 of SE and F and the EaM composition AE_3 of SE and F are also IND-qCCA secure.

We stress that EtM, EaM, and EatM are not of equivalent security in general. E.g., if SE is IND-qCPA secure but the MAC F is not a qPRF, the EtM composition of SE and F is IND-qCPA secure, and it could possibly also be IND-qCCA secure. But, depending on F, the EaM and EatM compositions of SE and F might not even be IND-qCPA insecure.

Proof. [Theorem 5] For two AE schemes AE and AE', we write $AE \approx AE'$ to indicate that no efficient adversary \mathcal{A} can distinguish interacting with AE from interacting with AE'. As usual, \mathcal{A} makes encryption queries, challenge queries and decryption queries. To prove Theorem 5, we will show that $AE_1 \approx AE_2$ and $AE_1 \approx AE_3$ and $AE_2 \approx AE_3$.

Each of AE_1 , AE_2 and AE_3 employs the same symmetric encryption scheme SE. Thus, only the authentication tags $T = F_L(...)$ possibly provide \mathcal{A} with the information required to distinguish AE_i from AE_j for $i \neq j$. As it will turn out, no efficient \mathcal{A} can distinguish the output distributions of the calls to the quantum pseudorandom functions from each other.

Consider the EatM construction from Definition 1 and an input (S, A) for F_L^N . Recall that A denotes the associated data. This input is called "K-good", if S can be written as S = Y || X where $Y = E_K^N(X)$. Otherwise, the input is called "K-bad". Since (E, D) is a symmetric encryption scheme, $X = D_K^N(Y)$ is equivalent to $Y = E_K^N(X)$. Thus, for each evaluation of either $\mathbf{E}_{K,L}$ or $\mathbf{D}_{K,L}$, the function F_L is called exactly once and is always called with K-good inputs.

Let $G_{L,K}^N$ be defined by $G_{L,K}^N(S,A) = \bot$ if (S,A) is K-bad. If (S,A) is K-good, let $G_{L,K}$ be pseudorandom. By AE'_1 we denote an authenticated encryption scheme, which is defined as follows:

$$\mathbf{E}_{K,L}^{N,A}(M) = \left(E_K^N(M), G_{L,K}^N(E_K^N(M) \| M, A) \right),$$

$$\mathbf{D}_{K,L}^{N,A}(C,T) = \begin{cases} D_K^N(C) & \text{if } G_{L,K}^N(C \| D_K^N(C), A) = T \\ \bot & \text{else.} \end{cases}$$

In other words, AE'_1 stems from the application of Encrypt-and+then-MAC to SE and

 $G_{L,K}$ – except that this application is no "generic composition", since the keys K for SE and (L, K) for G are not independent. When running AE_1 , the qPRF F is never called with K-bad inputs. Thus, $AE_1 \approx AE'_1$.

Define $F_L^N(C) = G_{L,K}^N(D_K^N(C) || C, A)$. Clearly, the input to G is K-good and if $G_{L,K}$ is a qPRF for K-good inputs, then F_L is a qPRF over its entire input space. Similar to AE'_1 , we define AE'_2 as stemming from the application of Encrypt-then-MAC to SE and F. Thus, we get $AE'_1 \approx AE'_2$ and $AE'_2 \approx AE_2$, which implies $AE_1 \approx AE_2$.

The same argument applies if we set $F_L^N(M) = G_{L,K}^N(E_K^N(M) || M, A)$ and define AE'_3 as stemming from the application of Encrypt-and-MAC to SE and F_L : $AE'_1 \approx AE'_3$ and $AE'_3 \approx AE_3$, which implies $AE_1 \approx AE_3$. From $AE_1 \approx AE_2$ and $AE_1 \approx AE_3$ we conclude $AE_2 \approx AE_3$.

As a consequence, any attack against either scheme is also an attack against both of the other two schemes with the same advantage, up to a negligible difference. \Box

7 Final Remarks

The motivation for this work was to investigate whether cryptographic state-of-the-art authenticated encryption schemes can still be secure against quantum (Q2) adversaries, possibly by increasing the built-in security parameters such as the key size.

A sufficient criterion for the IND-qCCA security of a generically composed authenticated encryption scheme is the fulfilment of the following three properties:

- 1. the generic composition is Encrypt-then-MAC, Encrypt-and-MAC or Encrypt-and+then-MAC,
- 2. the underlying encryption scheme is IND-qCPA secure, and
- 3. the underlying authentication scheme (MAC) is a qPRF.

The first two properties give a positive response to our motivation. The EtM composition is common in practice, and so are modes of operation, such as CBC, CFB and CTR, which have been proven to be IND-qCCA secure (under certain assumptions on the underlying block cipher). In addition, we deliver a negative result: if the generic composition is Encrypt-then-MAC and the underlying encryption scheme is IND-qCPA secure, then a PO secure MAC is insufficient for the composed scheme to be IND-qCCA secure. The third property and the negative result are both unfortunate. PO secure MACs are not necessarily strong enough for secure authenticated encryption. We are not aware of any practical MAC, which has been proven to be a qPRF. In fact, most common practical MACs (e.g. most variants of the CBC-MAC, the PMAC, MACs based on polynomial hashing) are known to be vulnerable to attacks in the Q2 model, such as quantum period finding or quantum linearization, and thus are not even PO secure [KLLNP16, BLNPS21]. One of few exceptions is the nonce-prefix variant of the CBC-MAC, which is PO secure [LL23]. Had it not been for our negative result, the generic composition of e.g. counter mode and nonce prefix MAC could have been considered a promising option for generic composition.

Future Work. We argue that, while a PO secure MAC is too weak for generic composition in our setting, the requirement for the MAC to be a qPRF is quite stringent, and there is a lack of practical options for the MAC. Is there an in-between notion, such that the EtM composition of an IND-qCPA secure encryption scheme and a MAC satisfying it is IND-qCCA secure? A possible choice for such a notion could be *blind unforgeability*. In order to answer this question, an analysis similarly to Section 5 would be helpful. The relationship between plus-one and blind unforgeability definitely deserves further research. Is blind unforgeability strictly stronger than plus-one unforgeability (cf. Section 4)?

Even beyond the specific need for good MACs as components for generic composition, it makes sense to search for practical and efficient variable-input-length functions, which can serve as a qPRF. In that context, it could be interesting to revisit the nonce prefix variant of the CBC-MAC [LL23] and to prove or disprove it being a qPRF.

Most related work on post-quantum security assumes randomization instead of adversarially chosen unique nonces. It is of general interest to analyse related work and new proposals if security is preserved in nonce-based scenarios.

References

- [AGM18] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable quantum encryption. In Annual international conference on the theory and applications of cryptographic techniques, pages 489–519. Springer, 2018.
- [AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II, volume 11693 of Lecture Notes in Computer Science, pages 269–295. Springer, 2019.
- [AMRS18] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantumsecure message authentication via blind-unforgeability. IACR Cryptol. ePrint Arch., page 1150, 2018.
- [AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantumaccess-secure message authentication via blind-unforgeability. In Advances in Cryptology-EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III 39, pages 788-817. Springer, 2020.
- [ATTU16] Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. Post-quantum security of the cbc, cfb, ofb, ctr, and XTS modes of operation. In Tsuyoshi Takagi, editor, Post-Quantum Cryptography
 - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings, volume 9606 of Lecture Notes in Computer Science, pages 44-63. Springer, 2016.
- [BBC⁺21] Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, and Yannick Seurin. Qcb: efficient quantum-secure authenticated encryption. In Advances in Cryptology-ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27, pages 668–698. Springer, 2021.
- [BDJR97] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In 38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997, pages 394–403. IEEE Computer Society, 1997.
- [BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography* -

18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers, volume 7118 of Lecture Notes in Computer Science, pages 320–337. Springer, 2011.

- [BLNPS21] Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, and André Schrottenloher. Quantum linearization attacks. In Advances in Cryptology-ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27, pages 422–452. Springer, 2021.
- [BN00] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In International Conference on the Theory and Application of Cryptology and Information Security, pages 531–545. Springer, 2000.
- [BN08] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of cryptology*, 21(4):469–491, 2008.
- [BRW04] Mihir Bellare, Phillip Rogaway, and David A. Wagner. The EAX mode of operation. In Bimal K. Roy and Willi Meier, editors, Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers, volume 3017 of Lecture Notes in Computer Science, pages 389–407. Springer, 2004.
- [BZ13a] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Advances in Cryptology-EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings 32, pages 592–608. Springer, 2013.
- [BZ13b] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Advances in Cryptology-CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II, pages 361–379. Springer, 2013.
- [CETU21] Tore Vincent Carstens, Ehsan Ebrahimi, Gelo Noel Tabia, and Dominique Unruh. Relationships between quantum ind-cpa notions. In *Theory of* Cryptography Conference, pages 240–272. Springer, 2021.
- [CEV22a] Céline Chevalier, Ehsan Ebrahimi, and Quoc-Huy Vu. On security notions for encryption in a quantum world. In Takanori Isobe and Santanu Sarkar, editors, Progress in Cryptology - INDOCRYPT 2022 - 23rd International Conference on Cryptology in India, Kolkata, India, December 11-14, 2022, Proceedings, volume 13774 of Lecture Notes in Computer Science, pages 592–613. Springer, 2022.
- [CEV22b] Céline Chevalier, Ehsan Ebrahimi, and Quoc-Huy Vu. On the security notions for encryption in a quantum world (revision 2022-09-03). IACR Cryptol. ePrint Arch., page 237, 2022.
- [Die82] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.
- [Dw007] Morris Dworkin. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC – NIST Special publication 800-38D. National Institute of Standards and Technology (NIST), 2007.
- [GHS16] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic

security and indistinguishability in the quantum world. In Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III 36, pages 60–89. Springer, 2016.

- [KLLNP16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36, pages 207–237. Springer, 2016.
- [LL23] Nathalie Lang and Stefan Lucks. On the post-quantum security of classical authenticated encryption schemes. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, Progress in Cryptology - AFRICACRYPT 2023 -14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21, 2023, Proceedings, volume 14064 of Lecture Notes in Computer Science, pages 79–104. Springer, 2023.
- [Mer07] N David Mermin. *Quantum computer science: an introduction*. Cambridge University Press, 2007.
- [MS16] Shahram Mossayebi and Rüdiger Schack. Concrete security against adversaries with quantum superposition access to encryption and decryption oracles. *arXiv* preprint arXiv:1609.03780, 2016.
- [NRS14] Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton. Reconsidering generic composition. In Phong Q. Nguyen and Elisabeth Oswald, editors, Advances in Cryptology EUROCRYPT 2014 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings, volume 8441 of Lecture Notes in Computer Science, pages 257–274. Springer, 2014.
- [RBB03] Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur., 6(3):365–403, 2003.
- [Rog02] Phillip Rogaway. Authenticated-encryption with associated-data. In Vijayalakshmi Atluri, editor, Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002, pages 98–107. ACM, 2002.
- [Rog04] Phillip Rogaway. Nonce-based symmetric encryption. In Bimal K. Roy and Willi Meier, editors, Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers, volume 3017 of Lecture Notes in Computer Science, pages 348–359. Springer, 2004.
- [Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
- [SJS16] Vladimir Soukharev, David Jao, and Srinath Seshadri. Post-quantum security models for authenticated encryption. In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography*, pages 64–78, Cham, 2016. Springer International Publishing.
- [TMC⁺24] Meltem Sönmez Turan, Kerry McKay, Donghoon Chang, Jinkeon Kang, and John Kelsey. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions – NIST Special publication 800-232 (Initial Public Draft). National Institute of

Standards and Technology (NIST), 2024.

- [WWZ82] William K. Wootters, William K. Wootters, and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.
- [Zha13] Mark Zhandry. A note on the quantum collision and set equality problems. arXiv preprint arXiv:1312.1027, 2013.
- [Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II, volume 11693 of Lecture Notes in Computer Science, pages 239–268. Springer, 2019.
- [Zha21] Mark Zhandry. How to construct quantum random functions. J. ACM, 68(5):33:1-33:43, 2021.