Post-quantum security models for authenticated encryption

Vladimir Soukharev[1], David Jao[2], and Srinath Seshadri[3]

[1] David R. Cheriton School of Computer Science
[2] Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
{djao,vsoukhar}@uwaterloo.ca
[3] Department of Mathematics and Computer Science
Sri Sathya Sai Institute of Higher Learning,Prasanthi Nilayam, Puttaparthi,
Anantapur, Andhra Pradesh,515134 India
srinathms@sssihl.edu.in

Abstract. We propose a security model for evaluating the security of authenticated encryption schemes in the post-quantum setting. Our security model is based on a combination of the classical Bellare-Namprempre security model for authenticated encryption together with modifications from Boneh and Zhandry to handle message authentication against quantum adversaries. We give a generic construction based on the Bellare-Namprempre model for producing an authenticated encryption protocol from any quantum-resistant symmetric-key encryption scheme together with any authentication scheme (digital signature scheme or MAC) admitting a classical security reduction to a quantum-computationally hard problem. We give examples of suitable authentication schemes under the quantum random oracle model using the Boneh-Zhandry transformation. We also provide tables of communication overhead calculations and comparisons for various choices of component primitives in our construction.

Keywords: authenticated encryption, security models, post-quantum cryptography

1 Introduction

Authenticated encryption (AE) forms a critical component of our existing internet infrastructure, with many widely used protocols such as TLS, SSH, and IPsec depending on AE for their basic functionality. Despite this importance, there is relatively little existing literature on the subject of combining post-quantum authentication and encryption schemes in a provably secure way. A few works [6,7,14] have dealt with the problem of post-quantum authenticated key exchange, but do not provide any self-contained discussion of AE outside of the (much) more complicated context of key exchange; moreover, [6] and [14] simply use RSA and DH respectively for long-term authentication keys, on the grounds that there is no immediate need for quantum-safe authenticity. In this

work, we adopt a different goal: we propose security definitions for post-quantum AE with the goal of achieving authentication and confidentiality against fully quantum adversaries, and give examples of such AE schemes constructed from existing underlying symmetric-key and digital signature primitives, using the quantum random oracle for the latter. Although our definitions are technically new, they are largely based on combinations of existing ideas, allowing us to reuse security proofs from other settings in the present context.

Note that our emphasis in this work is on constructing generic compositions of confidentiality and authentication primitives, rather than specialized authenticated encryption modes of operation as in the CAESAR competition [13]. While specialized first-class primitives are certainly valuable, we feel that understanding composed primitives represents a natural first step.

2 Security definitions

Bellare and Namprempre [2] showed that an IND-CPA encryption scheme combined with a SUF-CMA message authentication code under the Encrypt-then-MAC paradigm yields an IND-CCA authenticated encryption scheme. We wish to obtain a generalization of this construction which works against quantum adversaries. As a starting point, we review the security definitions of Boneh and Zhandry [5] for symmetric-key encryption schemes and digital signatures.

The most natural extension of IND-CPA security to the quantum setting consists of allowing full unrestricted quantum queries to the encryption oracle. However, Boneh and Zhandry showed [5, Theorems 4.2 and 4.4] that this definition is too powerful, in the sense that no encryption scheme satisfies this security definition. In place of full quantum queries, Boneh and Zhandry propose a definition in which challenge messages can only be encrypted classically [5, Definition 4.5]:

Definition 2.1 (IND-qCPA). *We say a symmetric-key encryption scheme* $\mathcal{E} = (\mathrm{Enc}, \mathrm{Dec})$ *is indistinguishable under a quantum chosen message attack (IND-qCPA secure) if no efficient adversary* $\mathcal{A}$ *can win in the following game, except with probability at most* $1/2 + \epsilon$*:*

Key generation: *The challenger picks a random key* k *and a random bit* b*.*
Queries: $\mathcal{A}$ *is allowed to make two types of queries:*

- **Challenge queries:** $\mathcal{A}$ *sends two messages* m_0, m_1*, to which the challenger responds with* $c* = \mathrm{Enc}(k, m_b)$*.*
- **Encryption queries:** *For each such query, the challenger chooses randomness* r*, and encrypts each message in the superposition using* r *as randomness:*

$$\sum_{m,c} \psi_{m,c} |m, c\rangle \mapsto \sum_{m,c} \psi_{m,c} |m, c \oplus \mathrm{Enc}(k, m; r)\rangle$$

Guess: $\mathcal{A}$ *produces a bit* b'*, and wins if* $b = b'$*.*

Similarly, Boneh and Zhandry define the notion of quantum chosen ciphertext security [5, Definition 4.6]:

Definition 2.2 (IND-qCCA). *We say a symmetric-key encryption scheme* $\mathcal{E} = (\mathrm{Enc}, \mathrm{Dec})$ *is indistinguishable under a quantum chosen ciphertext attack (IND-qCCA secure) if no efficient adversary* $\mathcal{A}$ *can win in the following game, except with probability at most* $1/2 + \epsilon$*:*

Key generation: *The challenger picks a random key* k *and a random bit* b*. It also creates creates a list* $\mathcal{C}$ *which will store challenger ciphertexts.*

Queries: $\mathcal{A}$ *is allowed to make three types of queries:*

Challenge queries: $\mathcal{A}$ *sends two messages* m_0, m_1*, to which the challenger responds with* $c* = \mathrm{Enc}(k, m_b)$*.*

Encryption queries: *For each such query, the challenger chooses randomness* r*, and encrypts each message in the superposition using* r *as randomness:*

$$\sum_{m,c} \psi_{m,c} |m, c\rangle \mapsto \sum_{m,c} \psi_{m,c} |m, c \oplus \mathrm{Enc}(k, m; r)\rangle$$

Decryption queries: *For each such query, the challenger decrypts all ciphertexts in the superposition, except those that were the result of a challenge query:*

$$\sum_{c,m} \psi_{c,m} |c, m\rangle \mapsto \sum_{c,m} \psi_{c,m} |c, m \oplus f(c)\rangle$$

where

$$f(c) = \begin{cases} \perp & \text{if } c \in \mathcal{C} \\ \mathrm{Dec}(k, c) & \text{otherwise.} \end{cases}$$

Guess: $\mathcal{A}$ *produces a bit* b'*, and wins if* $b = b'$*.*

We now discuss Boneh and Zhandry's quantum security definition for signatures. It is assumed that the adversary can query for signatures of superpositions of messages. In this situation, the definition of existential unforgeability needs to be modified, since a naive reading of the definition would allow the adversary simply to measure a superposition and claim the resulting signature as an existential forgery. To solve this problem we simply require the adversary to produce $q + 1$ signatures from q queries [5, Definition 3.2]:

Definition 2.3 (SUF-qCMA). *A signature scheme* $\mathcal{S} = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Ver})$ *is strongly unforgeable under a quantum chosen message attack (SUF-qCMA secure) if, for any efficient quantum algorithm* $\mathcal{A}$ *and any polynomial* q*, the algorithm* $\mathcal{A}$*'s probability of success in the following game is negligible in* λ*:*

Key generation: *The challenger runs* $(sk, pk) \leftarrow \mathrm{Gen}(\lambda)$*, and gives* pk *to* $\mathcal{A}$*.*

Signing Queries: *$\mathcal{A}$ makes a polynomial q chosen message queries. For each query, the challenger chooses randomness r, and responds by signing each message in the query using r as randomness:*

$$\sum_{m,t} \psi_{m,t}|m,t\rangle \mapsto \sum_{m,t} \psi_{m,t}|m,t \oplus \mathrm{Sign}(sk,m;r)\rangle$$

Forgeries: *$\mathcal{A}$ is required to produce $q+1$ message-signature pairs. The challenger then checks that all the signatures are valid, and that all message-signature pairs are distinct. If so, the adversary wins.*

Definition 2.4 (WUF-qCMA). *A signature scheme $\mathcal{S}$ is weakly unforgeable under a quantum chosen message attack (WUF-qCMA secure) if it satisfies the same definition as SUF-qCMA, except that we require the $q+1$ message-signature pairs to have distinct messages.*

Note that our terminology differs slightly from Boneh and Zhandry [5], although the content of the definitions is identical: Boneh and Zhandry use the terms "strongly EUF-qCMA" and "weakly EUF-qCMA" instead of SUF-qCMA and WUF-qCMA. In addition, Boneh and Zhandry have similar definitions for SUF-qCMA and WUF-qCMA secure message authentication codes [4].

Finally, we give our definitions of INT-qCTXT and INT-qPTXT. We constructed these definitions by starting with the classical security definitions of INT-CTXT and INT-PTXT from Bellare and Namprempre [2, §2], and modifying them in a manner similar to Boneh and Zhandry's definition for digital signatures (Definition 2.3).

Definition 2.5 (INT-qCTXT). *An encryption scheme $\mathcal{E} = (\mathrm{Enc}, \mathrm{Dec})$ satisfies integrity of ciphertext under a quantum attack (INT-qCTXT security) if, for any efficient quantum algorithm $\mathcal{A}$ and any polynomial q, the probability of success of $\mathcal{A}$ in the following game is negligible in λ:*

Key generation: *The challenger picks a random key k.*

Encryption queries: *$\mathcal{A}$ makes a polynomial q such queries. For each such query, the challenger chooses and randomness r, and encrypts each message in the superposition using r as randomness:*

$$\sum_{m,c} \psi_{m,c}|m,c\rangle \mapsto \sum_{m,c} \psi_{m,c}|m,c \oplus \mathrm{Enc}(k,m;r)\rangle$$

Decryption queries: *For each such query, the challenger decrypts all ciphertexts in the superposition, except those that were the result of a challenge query:*

$$\sum_{c,m} \psi_{c,m}|c,m\rangle \mapsto \sum_{c,m} \psi_{c,m}|c,m \oplus f(c)\rangle$$

where

$$f(c) = \begin{cases} \perp & \text{if } c \in \mathcal{C} \\ Dec(k,c) & \text{otherwise.} \end{cases}$$

Forgeries: *$\mathcal{A}$ is required to produce $q+1$ message-ciphertext pairs. The challenger then checks that all the ciphertexts are valid, and that all message-ciphertexts pairs are distinct. If so, the adversary wins.*

Definition 2.6 (INT-qPTXT). *An encryption scheme $\mathcal{E} = (\mathrm{Enc}, \mathrm{Dec})$ satisfies the integrity of plaintext under a quantum attack (INT-qPTXT secure) if it satifies the same definition as INT-qCTXT, except that we require the $q+1$ message-ciphertext pairs to have distinct messages.*

3 Main theorem

In this section, we prove that an IND-qCPA encryption scheme together with a SUF-qCMA signature or MAC scheme yields an authenticated encryption scheme via the Encrypt-then-MAC method, satisfying the respective privacy and integrity guarantees of IND-qCCA (Definition 2.2) and INT-qCTXT (Definition 2.5), the quantum analogues of the classical notions of IND-CCA and INT-CTXT security used in Bellare and Namprempre [2]. We begin by showing a WUF-qCMA MAC implies INT-qPTXT security:

Theorem 3.1. *Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be a symmetric-key encryption scheme, let $\mathcal{MA} = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$ be a message authentication scheme, and let $\overline{\mathcal{SE}} = (\bar{\mathcal{K}}, \bar{\mathcal{E}}, \bar{\mathcal{D}})$ be the authenticated encryption scheme obtained from $\mathcal{SE}$ and $\mathcal{MA}$ via the Encrypt-then-MAC method. Given any adversary I against $\overline{\mathcal{SE}}$, we can construct an adversary F such that*

$$\mathrm{Adv}^{\text{INT-qPTXT}}_{\overline{\mathcal{SE}}}(I) \leq \mathrm{Adv}^{\text{WUF-qCMA}}_{\mathcal{SE}}(F).$$

Proof. (Based on [2, Theorem 4.1]) We construct the adversary F as follows:

1. Use the key $\mathcal{K}_e$.
2. Run I.
3. On query $\mathrm{Enc}(M)$ (where M can be in superposition):

$$C' \leftarrow \mathcal{E}(K_e, M); \tau \leftarrow \mathrm{Tag}(C');\ \text{Return } C' \parallel \tau \text{ to } I$$

4. On query $\mathrm{Ver}(C)$:

$$\text{Parse } C \text{ as } C' \parallel \tau'; v \leftarrow \mathrm{Ver}(C', \tau');\ \text{Return } v \text{ to } I$$

until I halts.

Let $C_i = C'_i \parallel \tau_i$ for $i \in \{1, \ldots, q+1\}$ be the Ver queries of I that lead to winning game INT-qPTXT$_{\overline{\mathcal{SE}}}$, after q queries to Enc. Let $M_i = \mathcal{D}(K_e, C'_i)$. We know that due to the property of INT-qPTXT of $\overline{\mathcal{SE}}$, at most q of them were obtained from the q queries to Enc of I; hence $C'_i s$ were the result of at most q queries of F to Tag, but we obtained $q+1$ valid tags. Hence, F wins whenever WUF-qCMA$_{\mathcal{MA}}$ I wins INT-qPTXT$_{\overline{\mathcal{SE}}}$.

Although our proof of Theorem 3.1 is for MACs, the same proof works for digital signatures (replacing the Tag oracle with the Sign oracle).

Next we show that a SUF-qCMA signature or MAC implies an INT-qCTXT authenticated encryption scheme.

Theorem 3.2. *Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be a symmetric-key encryption scheme, let $\mathcal{MA} = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$ be a message authentication scheme, and let $\overline{\mathcal{SE}} = (\bar{\mathcal{K}}, \bar{\mathcal{E}}, \bar{\mathcal{D}})$ be the authenticated encryption scheme obtained from $\mathcal{SE}$ and $\mathcal{MA}$ via encrypt-then-MAC composition method. Given any adversary I against $\overline{\mathcal{SE}}$, we can construct an adversary F such that*

$$\mathrm{Adv}^{\text{INT-qCTXT}}_{\overline{\mathcal{SE}}}(I) \leq \mathrm{Adv}^{\text{SUF-qCMA}}_{\mathcal{SE}}(F).$$

Proof. (Based on [2, Theorem 4.4]) Here we use the same adversary as in Theorem 3.1. Let $C_i = C'_i \parallel \tau_i$ for $i \in \{1, \ldots, q+1\}$ be the Ver queries of I that lead to winning game INT-qCTXT$_{\overline{\mathcal{SE}}}$, after q queries to Enc. If only at most q of the C_i's were returned to I by Enc, then at most q were queried by F with Tag (i.e., the corresponding $C'_i s$). Hence, F wins whenever SUF-qCMA$_{\mathcal{MA}}$ I wins INT-qCTXT$_{\overline{\mathcal{SE}}}$.

Again, the proof of Theorem 3.2 carries over to digital signatures as well, replacing the Tag oracle with a Sign oracle.

We now show that the authenticated encryption scheme in Encrypt-then-MAC inherits the IND-qCPA property from the underlying encryption scheme:

Theorem 3.3. *Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be a symmetric-key encryption scheme, let $\mathcal{MA} = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$ be a message authentication scheme, and let $\overline{\mathcal{SE}} = (\bar{\mathcal{K}}, \bar{\mathcal{E}}, \bar{\mathcal{D}})$ be the authenticated encryption scheme obtained from $\mathcal{SE}$ and $\mathcal{MA}$ via the Encrypt-then-MAC composition method. Given any adversary $\mathcal{A}$ against $\overline{\mathcal{SE}}$, we can construct an adversary $\mathcal{A}_p$ such that*

$$\mathrm{Adv}^{\text{IND-qCPA}}_{\overline{\mathcal{SE}}}(\mathcal{A}) \leq \mathrm{Adv}^{\text{IND-qCPA}}_{\mathcal{SE}}(\mathcal{A}_p).$$

Furthermore, $\mathcal{A}_p$ uses the same resources as $\mathcal{A}$.

Proof. (Based on [2, Theorem 4.3]) We construct $\mathcal{A}_p$ as follows:

$\mathcal{K}_m \leftarrow \mathcal{K}_m$
Run $\mathcal{A}$
On query to Enc
$C \leftarrow Enc(M)$
$\tau \leftarrow \mathrm{Tag}(\mathcal{K}_m, C)$
Return $C \parallel \tau$ to $\mathcal{A}$
Until $\mathcal{A}$ halts and returns b
Return b.

We can see that if $\mathcal{A}$ wins, then so does $\mathcal{A}_p$, since a winning output for $\mathcal{A}$ is a winning output for $\mathcal{A}_p$; the tag can be ignored.

Games G_0 and $\boxed{G_1}$:	Game G_2 :
proc Initialize	**proc Initialize**
$K \xleftarrow{\$} \mathcal{K}; b \xleftarrow{\$} \{0,1\}; S \leftarrow \emptyset$	$K \xleftarrow{\$} \mathcal{K}; b \xleftarrow{\$} \{0,1\}$
proc Challenge(M_0, M_1)	**proc Challenge**(M_0, M_1)
$C \xleftarrow{\$} \mathrm{Enc}(K, M_b); S \leftarrow S \cup \{C\}$; Return C	$C \xleftarrow{\$} \mathrm{Enc}(K, M_b)$; Return C
proc Enc(M)	**proc Enc**(M)
$C \xleftarrow{\$} \mathrm{Enc}^*(K, M); S \leftarrow S \cup \{C\}$; Return C	$C \xleftarrow{\$} \mathrm{Enc}^*(K, M)$; Return C
proc Dec(C)	**proc Dec**(C)
$M \leftarrow \mathrm{Dec}^*(C)$	Return $\perp$
If $M \neq \perp$ then bad $\leftarrow$ true; $\boxed{M \leftarrow \perp}$	
Return M	
proc Finalize(d)	**proc Finalize**(d)
Return $(d = b)$	Return $(d = b)$

Fig. 1: Games G_0, G_1, and G_2. Game G_1 contains the code in the box while G_0 does not. The functions Enc^* and Dec^* refer to the encryption and decryption oracle functions from Definition 2.2.

Finally, we prove that INT-qCTXT and IND-qCPA security imply IND-qCCA security (Theorem 3.6). The proof relies on three games G_0, G_1, and G_2 as defined in Figure 1. These games are based on the corresponding three games from Figure 7 of [2], except that we modify the games mutadis mutandis to conform to our quantum definitions (Definitions 2.1 and 2.2).

The proof of Theorem 3.6 uses the identical until bad lemma [2, Lemma 2.1]:

Lemma 3.4. *(Identical until bad lemma) Let G_i and G_j be identical until bad games, and $\mathcal{A}$ an adversary. Then for any y: $Pr[G_i^{\mathcal{A}} \implies y] - Pr[G_j^{\mathcal{A}} \implies y] \leq Pr[G_j \text{ sets bad}]$.*

It is not immediately clear (to us, anyway) that the identical until bad lemma holds for quantum adversaries. Fortunately, in Theorem 3.6, we only need the special case $i = 0$, $j = 1$, and $y =$ true, and in this case we can prove the result for quantum adversaries. We use the following lemma of Shoup [15, Lemma 1].

Lemma 3.5. *Let E, E', and F be events defined on a probability space such that $Pr[E \wedge \neg F] = Pr[E' \wedge \neg F]$. Then we have $|Pr[E] - Pr[E']| \leq Pr[F]$.*

This lemma holds regardless of whether or not the adversary is classical or quantum, as it is a mathematical statement. Define the event E to be $[G_0^{\mathcal{A}} \implies \text{true}]$ and E' to be $[G_1^{\mathcal{A}} \implies \text{true}]$. Define F to be $[G_1^{\mathcal{A}} \text{ sets bad}]$. Observe that in this case $E \wedge \neg F$ corresponds to the outcome $M = \perp$ in the game G_0, meaning

that A wins the game. Similarly, $E' \wedge \neg F$ corresponds to the outcome $M = \perp$ in G_1, meaning that $\mathcal{A}$ wins the game. Note that for $M = \perp$, both G_0 and G_1 return the same responses, and hence have the same probability of winning. Hence, $Pr[E \wedge \neg F] = Pr[E' \wedge \neg F]$, which means Lemma 1 of [15] can be applied to obtain $|Pr[E] - Pr[E']| \leq Pr[F]$. Finally, we need to remove the absolute values, to obtain $Pr[E'] \leq Pr[E]$. It is easy to see that we can do so, because for G_0 we sometimes return the message, while for G_1, we always return $M = \perp$, so that the success probability of G_0 is at least that of G_1. Hence the identical until bad lemma holds for quantum adversaries in the special case where $i = 0$, $j = 1$, and $y = \text{true}$.

We recall Definition (1) in [2]:

$$\text{Adv}^{\text{IND-CCA}}_{\mathcal{SE}}(\mathcal{A}) = 2 \cdot \Pr[\text{IND-CCA}^{\mathcal{A}}_{\mathcal{SE}} \implies 1] - 1.$$

The quantum version of this definition is:

$$\text{Adv}^{\text{IND-qCCA}}_{\mathcal{SE}}(\mathcal{A}) = 2 \cdot \Pr[\text{IND-qCCA}^{\mathcal{A}}_{\mathcal{SE}} \implies 1] - 1.$$

Theorem 3.6. *Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $\mathcal{A}$ be an IND-qCCA adversary against $\mathcal{SE}$ running in time t and making q_e Enc queries and q_d Dec queries. Then, we can construct an INT-qCTXT adversary $\mathcal{A}_c$ and IND-qCPA adversary $\mathcal{A}_p$ such that*

$$\text{Adv}^{\text{IND-qCCA}}_{\mathcal{SE}}(\mathcal{A}) \leq 2 \cdot \text{Adv}^{\text{INT-qCTXT}}_{\mathcal{SE}}(\mathcal{A}_c) + \text{Adv}^{\text{IND-qCPA}}_{\mathcal{SE}}(\mathcal{A}_p).$$

Furthermore, $\mathcal{A}_c$ runs in time $O(t)$ and makes q_e Enc queries and q_d Ver queries, while $\mathcal{A}_p$ runs in time $O(t)$ and makes q_e queries of target messages M_i.

Proof. We have:

$$\begin{aligned}
\Pr[\text{IND-qCCA}^{\mathcal{A}}_{\mathcal{SE}} \implies \text{true}] &= \Pr[G_0^{\mathcal{A}} \implies \text{true}] \\
&= \Pr[G_1^{\mathcal{A}} \implies \text{true}] + \\
&\quad (\Pr[G_0^{\mathcal{A}} \implies \text{true}] - Pr[G_1^{\mathcal{A}} \implies \text{true}]) \\
&\leq \Pr[G_1^{\mathcal{A}} \implies \text{true}] + \Pr[G_1^{\mathcal{A}} \text{ sets bad}] \qquad (1)
\end{aligned}$$

The last inequality follows from the identical until bad lemma in the special case $i = 0$, $j = 1$, and $y = \text{true}$ (which we proved above). Now, observe that for Dec, G_1 always returns $\perp$, and hence

$$\Pr[G_1^{\mathcal{A}} \implies \text{true}] = \Pr[G_2^{\mathcal{A}} \implies \text{true}]. \qquad (2)$$

Let us now define the adversary $\mathcal{A}_p$. It simply runs $\mathcal{A}$, answering $\mathcal{A}$'s challenge and encryption queries with its own queries, and answering $\mathcal{A}$'s queries for decryption with $\perp$. It outputs whatever $\mathcal{A}$ outputs. Hence, we get:

$$\Pr[G_2^{\mathcal{A}} \implies \text{true}] \leq \Pr[\text{IND-qCPA}^{\mathcal{A}_p}_{\mathcal{SE}} \implies \text{true}]. \qquad (3)$$

Next, we define the adversary $\mathcal{A}_c$. The adversary $\mathcal{A}_c$ picks a random bit b, then runs $\mathcal{A}$ and answers its queries as follows. For challenge and encryption queries, $\mathcal{A}_c$ submits challenge and encryption queries and returns the results to $\mathcal{A}$. For the Dec query, $\mathcal{A}_c$ submits it to the Ver oracle, and, regardless of the response, returns $\perp$ to $\mathcal{A}$. Hence, we get:

$$\Pr[G_1^{\mathcal{A}} \text{ sets bad}] \leq \Pr[\text{INT-qCTXT}_{\mathcal{SE}}^{\mathcal{A}_c} \implies \text{true}]. \tag{4}$$

Combining the definition

$$\text{Adv}_{\mathcal{SE}}^{\text{IND-qCCA}}(\mathcal{A}) = 2 \cdot \Pr[\text{IND-qCCA}_{\mathcal{SE}}^{\mathcal{A}} \implies 1] - 1$$

with Equations (1), (2), (3), and (4), we obtain

$$\text{Adv}_{\mathcal{SE}}^{\text{IND-qCCA}}(\mathcal{A}) \leq 2 \cdot \text{Adv}_{\mathcal{SE}}^{\text{INT-qCTXT}}(\mathcal{A}_c) + \text{Adv}_{\mathcal{SE}}^{\text{IND-qCPA}}(\mathcal{A}_p).$$

Combining Theorems 3.2, 3.3, and 3.6, we obtain our main theorem:

Theorem 3.7. *Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be a symmetric-key encryption scheme, let $\mathcal{MA} = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$ be a message authentication scheme, and let $\overline{\mathcal{SE}} = (\bar{\mathcal{K}}, \bar{\mathcal{E}}, \bar{\mathcal{D}})$ be the authenticated encryption scheme obtained from $\mathcal{SE}$ and $\mathcal{MA}$ via the Encrypt-then-MAC composition method. Given that $\mathcal{SE}$ is IND-qCPA and $\mathcal{MA}$ is SUF-qCMA, then the resulting $\overline{\mathcal{SE}}$ is IND-qCCA.*

Proof. By Theorem 3.2, since $\mathcal{MA}$ is SUF-qCMA, we get that $\overline{\mathcal{SE}}$ is INT-qCTXT. Also, by Theorem 3.3, since $\mathcal{SE}$ is IND-qCPA, we get that $\overline{\mathcal{SE}}$ is also IND-qCPA. Finally, because $\overline{\mathcal{SE}}$ is INT-qCTXT and IND-qCPA, by Theorem 3.6, we get that it is IND-qCCA.

As with Theorems 3.1 and 3.2, Theorem 3.7 also holds with digital signature schemes used in place of MACs.

4 Quantum-resistant strongly unforgeable signature schemes

In this section we examine some concrete choices of strongly unforgeable signature/MAC schemes which could be suitable for our AE construction. We limit ourselves to only a few representative examples to illustrate the general idea. We focus on signature schemes as in our view they are somewhat more interesting, but similar ideas apply to MACs [4]. We begin with a review of the Boneh-Zhandry transformation [5, Construction 3.12] for transforming any classically strongly secure digital signature scheme into a SUF-qCMA scheme:

Construction 4.1 *Let $S_c = (\text{Gen}_c, \text{Sign}_c, \text{Ver}_c)$ be a be a signature scheme, H be a hash function, and $\mathcal{Q}$ be a family of pairwise independent functions mapping messages to the randomness used by Sign_c, and k some polynomial in λ. Define $S = (\text{Gen}, \text{Sign}, \text{Ver})$ where:*

- $\mathrm{Gen}(\lambda) = \mathrm{Gen}_c(\lambda)$
- $\mathrm{Sign}(sk, m)$:
  - *Select* $Q \in \mathcal{Q}$, $r \in \{0,1\}^k$ *at random.*
  - *Set* $s = Q(m), h = H(m, r), \sigma = \mathrm{Sign}_c(sk, h; s)$. *Output* (r, σ).
- $\mathrm{Ver}(pk, m, (r, \sigma))$:
  - *Set* $h = H(m, r)$. *Output* $\mathrm{Ver}_c(pk, h, \sigma)$.

If the original signature scheme S_c is SUF-CMA against a classical chosen message attack performed by a quantum adversary, then by [5, Corollary 3.17] the transformed scheme S is SUF-qCMA in the quantum random oracle model.

Furthermore, if the verification function in the signature scheme S_c involves independently deriving the value of σ and checking whether or not the derived value matches the value which was originally sent, a further optimization is possible: one can hash σ to reduce its length to a minimum. We employ this optimization in our examples.

4.1 Strong designated verifier signatures from isogenies

A strong designated verifier signature (SDVS) scheme [10] is a digital signature scheme in which only a designated party (specified at the time of signing) can verify signatures, and verification requires that party's private key. Note that an SDVS is enough for AE, since only the two parties participating in the AE protocol need to be able to verify signatures.

Sun, Tian, and Wang in [17] present an isogeny-based SDVS scheme, and give a classical security reduction to the SSDDH problem [11], which is believed to be infeasible on quantum computers. This reduction qualifies as a straight-line reduction in the sense of the security framework of Song [16], and hence remains valid for quantum adversaries. However, the reduction only establishes SUF-CMA security, not SUF-qCMA security. Applying the Boneh-Zhandry transformation (Construction 4.1), we obtain the following SDVS scheme, which is SUF-qCMA:

Setup: Fix a prime $p = \ell_A^{e_A}\ell_B^{e_B} \cdot f \pm 1$, a supersingular base curve E over $\mathbb{F}_{p^2}$, generators $\{P_A, Q_A\}$ of $E[\ell_A^{e_A}]$, and generators $\{P_B, Q_B\}$ of $E[\ell_B^{e_B}]$. Let $H_1, H_2 \colon \{0,1\}^* \to \{0,1\}^k$ be independent secure hash functions (with parameter k), and $\mathcal{Q}$ a family of pairwise independent functions mapping messages to the randomness used in signing.

Key generation: A signer selects at random $m_S, n_S \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, not both divisible by ℓ_A, and then computes an isogeny $\phi_S \colon E \to E_S = E/\langle [m_S]P_A + [n_S]Q_A \rangle$ and the values $\phi_S(P_B)$ and $\phi_S(Q_B)$. The private key is (m_S, n_S) and the public key is the curve E_S and the points $\phi_S(P_B)$ and $\phi_S(Q_B)$.
A designated verifier selects at random $m_V, n_V \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, not both divisible by ℓ_B, and then computes an isogeny $\phi_V \colon E \to E_V = E/\langle [m_V]P_B + [n_V]Q_B \rangle$ and the values $\phi_V(P_A)$ and $\phi_V(Q_A)$. The private key is (m_V, n_V) and the public key is the curve E_V and the points $\phi_V(P_A)$ and $\phi_V(Q_A)$.

Signing: Select at random $Q \in \mathcal{Q}, r \in \{0,1\}^k$ for use in the Boneh-Zhandry transformation. Compute $s = Q(m)$, $h = H_1(m, r)$, and $\phi'_S \colon E_V \to E_{SV} = E_V/\langle [m_S]\phi_V(P_A) + [n_S]\phi_V(Q_A)\rangle$. Set $\sigma = H_2(h||j(E_{SV})||s)$. The signature is (r, σ).

Verification: Compute $\phi'_V \colon E_S \to E_{SV} = E_S/\langle [m_V]\phi_S(P_B) + [n_V]\phi_S(Q_B)\rangle$ and $h = H_1(m, r)$. Set $\sigma' = H_2(h||j(E_{SV})||Q(m))$. Verify that $\sigma' \stackrel{?}{=} \sigma$.

4.2 Ring-LWE signatures

As another example, we combine the Ring-LWE signature scheme of Güneysu et al. [8] with Construction 4.1 from [5] to obtain a SUF-qCMA signature scheme based on Ring-LWE:

Setup: Set $R = \mathbb{F}_q/\langle x^n + 1\rangle$ where n is a power of 2. Let $H_1 \colon \{0,1\}^* \to \{0,1\}^k$ and $H_3 \colon \{0,1\}^* \to R$ be independent secure hash functions (with parameter k) and $\mathcal{Q}$ a family of pairwise independent functions mapping messages to the randomness used in the signing function. Choose a bound B on the maximum coefficient size.

Key generation: A signer generates two small polynomials $s_1(x), s_2(x) \in R$, selects $a(x) \in R$ at random, and computes the public key $t(x) = as_1(x) + s_2(x)$.

Signing: Select $Q \in \mathcal{Q}$, $r \in \{0,1\}^k$ at random for the Boneh-Zhandry transformation, and $y_1(x), y_2(x) \in R$ at random for the signature scheme. Compute $s = Q(m)$, $h = H_1(m, r)$, and $c(x) = H_3(\text{BitString}(a(x)y_1(x) + y_2(x))||h||s)$. Finally, compute $z_1(x) = s_1(x)c(x) + y_1(x)$ and $z_2(x) = s_2(x)c(x) + y_2(x)$. Check that the coefficients of the polynomials $z_1(x), z_2(x)$ are within the bound B; if not, restart. The signature is $(r, z_1(x), z_2(x), c(x))$

Verification: Check that the coefficients of the polynomials $z_1(x), z_2(x)$ are within the bound B; if not, reject. Compute x $h = H_1(m, r)$, and check whether $c(x) \stackrel{?}{=} H_3(a(x)z_1(x) + z_2(x) - t(x)c(x)||h||Q(m))$. If so, accept; otherwise reject.

5 Quantum-resistant authenticated encryption schemes

We give a generic construction of authenticated encryption schemes which are provably quantum-resistant in the sense of IND-qCTXT and IND-qCCA. For the underlying encryption scheme, we assume that a classical symmetric-key block cipher $\mathcal{E}$ in a suitable block cipher mode of operation with random IVs will suffice to provide quantum security, taking care to use 2ℓ key sizes to obtain ℓ bits of security. We refer to [1] for a discussion of the choice of the mode of operation. For the MAC/signature scheme we can employ the Boneh-Zhandry transformation on any SUF-CMA scheme secure against quantum adversaries as described in Section 4. Combining those two components, we obtain an IND-qCCA and IND-qCTXT authenticated encryption scheme as follows:

Setup:

1. Choose parameters for the underlying encryption and signature schemes.
2. Let $H\colon \{0,1\}^* \to \{0,1\}^k$ be a secure hash function (with security parameter k).
3. Let $\mathcal{Q}$ be a family of pairwise independent functions mapping messages to the randomness used in the signature scheme.

Key generation:

1. Alice chooses her private parameters for the encryption and signature schemes. If required, she produces and publishes the corresponding public keys.
2. Bob chooses his private parameters for the encryption and signature schemes. If required, he produces and published the corresponding public keys.

Encryption:

Suppose Bob wants to send a message $m \in \{0,1\}^*$ to Alice.

1. Using the common encryption key e that he shares with Alice, encrypt the message using the underlying symmetric-key encryption scheme to obtain $c = \mathcal{E}(e, m)$.
2. Select $Q \in \mathcal{Q}$, $r \in \{0,1\}^k$ at random.
3. Compute $t = Q(m)$.
4. Computes the value $h = H(c, r)$.
5. Using h and his private signing key s, Bob computes the authentication tag $\sigma = \mathrm{Sign}(s, h; t)$.
6. The ciphertext is $\{c, r, \sigma\}$.

Decryption:

Suppose Alice receives ciphertext $\{c, r, \sigma\}$ from Bob.

1. Compute the value $h = H(c, r)$.
2. Using h and Bob's public signing key p, compute the verification function $\mathrm{Ver}(s, h, r, \sigma)$, if it returns true, continue; if not, stop.
3. Using the common encryption key e that she shares with Bob, decrypt the message and obtain $m = \mathcal{D}(e, c)$.

Again, in the case where the verification function in the signature scheme involves independently deriving the value of σ and checking that the derived value matches the value which was originally sent, we can hash σ prior to transmission to reduce its length to a minimum.

6 Overhead calculations and comparisons

In this section we study the communication costs of our AE scheme, from the point of view of both per-message communication overhead and key transmission overhead.

6.1 Communication overhead

Recall that the ciphertext which Bob sends to Alice consists of the triplet (c, r, σ), where c is the underlying ciphertext content, r is a k-bit nonce, and σ is the signature tag. In the case where the verification function in the signature scheme involves independently deriving the value of σ, we can hash σ down to k bits as well. For a security level of ℓ bits, the minimum value of k required for collision resistance is 2ℓ bits in the quantum setting [3]. The per-message communication overhead of the scheme is thus 4ℓ bits in the case where the signature tag can be hashed, and $2\ell + |\sigma|$ bits otherwise. Note that in the former case the per-message communications overhead is always the same, independent of which component schemes are chosen.

6.2 Public key overhead

For the overhead involved in transmitting the public keys to be used for the signature scheme, we use the table of Fujioka et al. [7], augmented with some more recent results as described below. Although [7] deals with the case of post-quantum authenticated key exchange, the same key sizes apply to the AE setting.

With the exception of Ring-LWE as explained below, we aim for 128-bit quantum security. For Ring-LWE, we use the numbers from [8]. Since the scheme in [8] is based on power-of-2 cyclotomic rings, there is a large jump in parameter size between $n = 2^9$ and $n = 2^{10}$, with the former providing 80 bits of security and the latter 256 bits of security. There is no intermediate power of 2 that would provide 128 bits of security. For this reason, we list both 80-bit and 256-bit security levels in our table. The numbers for NTRU are from Schanck et al. [14]. For isogeny-based SDVS schemes we use the recent results of [12]. Note that SDVS schemes require two-way transmission of public keys even if the encrypted communication is one-way, whereas standard signature schemes require two-way transmission of public keys only for two-way communication.

Signature scheme	**Bits**
Ring-LWE (80-bit security) [8]	11600
Ring-LWE (256-bit security) [8]	25000
NTRU [14]	5544
Code-based [7]	52320
Multivariate polynomials [9] (via [7])	7672000
Isogeny-based [12]	3073

Table 1: Key transmission overhead

7 Conclusion

We propose a security model for authenticated encryption against fully quantum adversaries, based on the classical security model of Bellare and Namprempre together with the Boneh and Zhandry framework for modeling quantum adversaries. We provide concrete examples of authenticated encryption schemes satisfying our security model along with estimates of overhead costs for such schemes.

8 Acknowledgments

This work was supported by the CryptoWorks21 NSERC CREATE Training Program in Building a Workforce for the Cryptographic Infrastructure of the 21st Century, and the Indian Space Research Organization (ISRO) through the Sponsored Research (RESPOND) program.

References

1. 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. PQCrypto 2016, to appear.
2. Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *J. Cryptol.*, 21(4):469–491, September 2008.
3. Daniel J. Bernstein. Cost analysis of hash collisions: will quantum computers make SHARCS obsolete? In *Workshop Record of SHARCS'09: Special-purpose Hardware for Attacking Cryptographic Systems*, pages 51–82, 2009.
4. Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer, 2013.
5. Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Proc. of Crypto*, volume 8043 of *LNCS*, pages 361–379, 2013.
6. Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. Cryptology ePrint Archive, Report 2014/599, 2014. `http://eprint.iacr.org/`.
7. Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 83–94, New York, NY, USA, 2013. ACM.
8. Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Lattice-based signatures: Optimization and implementation on reconfigurable hardware. *IEEE Trans. Computers*, 64(7):1954–1967, 2015.

9. Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang. Public-key cryptography from new multivariate quadratic assumptions. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography — PKC 2012*, volume 7293 of *Lecture Notes in Computer Science*, pages 190–205. Springer Berlin Heidelberg, 2012.
10. Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In Ueli M. Maurer, editor, *Advances in Cryptology — EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 143–154. Springer, 1996.
11. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *PQCrypto*, volume 7071 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2011.
12. David Jao, Kassem Kalach, and Christopher Leonardi. Key compression for isogeny-based cryptography. In preparation.
13. Diana Maimut and Reza Reyhanitabar. Authenticated encryption: Toward next-generation algorithms. *IEEE Security & Privacy*, 12(2):70–72, Mar 2014.
14. John Schanck, William Whyte, and Zhenfei Zhang. A quantum-safe circuit-extension handshake for tor. Cryptology ePrint Archive, Report 2015/287, 2015. `http://eprint.iacr.org/`.
15. Victor Shoup. OAEP reconsidered. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 239–259. Springer, 2001.
16. Fang Song. A note on quantum security for post-quantum cryptography. Cryptology ePrint Archive, Report 2014/709, 2014. `http://eprint.iacr.org/`.
17. Xi Sun, Haibo Tian, and Yumin Wang. Toward quantum-resistant strong designated verifier signature from isogenies. In Fatos Xhafa, Leonard Barolli, Florin Pop, Xiaofeng Chen 0001, and Valentin Cristea, editors, *INCoS*, pages 292–296. IEEE, 2012.