Post-quantum security models for authenticated encryption

Vladimir Soukharev

David R. Cheriton School of Computer Science

UNIVERSITY OF WATERLOO

February 24, 2016

CENTRE FOR APPLIED CRYPTOGRAPHIC RESEARCH (CACR)

Introduction

- Bellare and Namprempre in 2008, have shown that in order to obtain a secure (IND-CCA) Authenticated Encryption construction, we only need:
  - IND-CPA encryption scheme.
  - SUF-CMA signature or MAC scheme.
  - Use *Encrypt-then-MAC* technique.
- The question arises how to do this for quantum-resistant schemes.
- We will adopt the definitions for the scenario with a quantum adversary and will show how to obtain quantum-resistant authenticated encryption schemes.

Definition: IND-qCPA (Boneh and Zhandry, 2013)

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

Key Gen: The challenger picks a random key k and bit b.

Queries: A is allowed to make two types of queries:

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

$$\sum_{m,c} \psi_{m,c} |m, c\rangle \longrightarrow \sum_{m,c} \psi_{m,c} |m, c \oplus \text{Encrypt}(k, m; r)\rangle$$

Guess: A produces a bit b', and wins if $b = b'$.

IND-qCPA - Definition Notes

- Can not use natural extension of IND-CPA definition.
- Allowing full unrestricted quantum queries, makes the definition too powerful.

Definition: IND-qCCA (Boneh and Zhandry, 2013)

Same definition as for IND-qCPA, except that we also allow the decryption queries for messages that do not contain the challenge messages.

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

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

  where

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

Guess: A produces a bit b', and wins if $b = b'$.

Definition: SUF-qCMA (Boneh and Zhandry, 2013)

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

KeyGen: The challenger runs $(sk, pk) \leftarrow G(\lambda)$, and gives pk to A.

Signing Queries: The adversary makes a polynomial q chosen message queries. For each query, the challenger chooses randomness r, and responds by signing each message in the query:

$$\sum_{m,s} \psi_{m,s} |m, s\rangle \longrightarrow \sum_{m,s} \psi_{m,s} |m, s \oplus Sign(sk, m; r)\rangle$$

Forgeries: The adversary is required to produce $q + 1$ message/signature pairs.

SUF-qCMA - Definition Notes

- Can not use the classical definition directly, as the adversary can feed the queries in superposition.
- Instead of asking to produce 'new' valid pair, we ask to produce '$q + 1$' valid pairs after q queries.

Definition: WUF-qCMA (Boneh and Zhandry, 2013)

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.

About Definitions

- Bellare and Namprempre make use of the definitions for the classical cryptographic notions.
- Boneh and Zhandry show that we need to "upgrade" the definitions to be able to talk about quantum adversary scenario.
- In order to be able to prove the main result, following the approach analogous to Bellare and Namprempre's, we need more definitions.
- Using the same ideas as Boneh and Zhandry, we define the missing definitions (or "upgrade" them).

Definition: INT-qCTXT

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

Key Gen: The challenger picks a random key k.

Encryption queries: The adversary makes a polynomial q such queries. For each such query, the challenger chooses and randomness r, and encrypts each message in the superposition:

$$\sum_{m,c} \psi_{m,c} |m, c\rangle \longrightarrow \sum_{m,c} \psi_{m,c} |m, c \oplus \text{Encrypt}(k, m; r)\rangle$$

Definition: INT-qCTXT

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

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

where

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

Forgeries: The adversary 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 challenger reports that the adversary wins.

Definition: INT-qPTXT

An encryption scheme $\mathcal{E} = (\mathsf{Encrypt}, \mathsf{Decrypt})$ 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.

Bellare and Namprempre Results

- WUF-CMA (MAC) $\implies$ INT-PTXT (AE).
- SUF-CMA (MAC) $\implies$ INT-CTXT (AE).
- IND-CPA (Enc) $\implies$ IND-CPA (AE).
- INT-CTXT and IND-CPA $\implies$ IND-CCA.

Main Theorem

IND-CPA (Enc) and SUF-CMA (MAC) $\implies$ IND-CCA (AE).

Our Results

- WUF-qCMA (MAC) $\implies$ INT-qPTXT (AE).
- SUF-qCMA (MAC) $\implies$ INT-qCTXT (AE).
- IND-qCPA (Enc) $\implies$ IND-qCPA (AE).
- INT-qCTXT and IND-qCPA $\implies$ IND-qCCA.

Main Theorem

IND-qCPA (Enc) and SUF-qCMA (MAC) $\implies$ IND-qCCA (AE).

Theorem: SUF-qCMA (MAC) $\Longrightarrow$ INT-qCTXT (AE)

Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be a symmetric 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 and adversary F such that

$$Adv_{\overline{\mathcal{SE}}}^{INT-qCTXT}(I) \leq Adv_{\mathcal{SE}}^{SUF-qCMA}(F).$$

Theorem: INT-qCTXT and IND-qCPA $\implies$ IND-qCCA

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let 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 A_c and IND-qCPA adversary A_p such that

$$Adv_{\mathcal{SE}}^{IND-qCCA}(A) \leq 2 \cdot Adv_{\mathcal{SE}}^{INT-qCTXT}(A_c) + Adv_{\mathcal{SE}}^{IND-qCPA}(A_p).$$

Furthermore, A_c runs in time $O(t)$ and makes q_e Enc queries and q_d Verification queries, while A_p runs in time $O(t)$ and makes q_e queries of target messages M_i.

Main Theorem

Theorem

IND-qCPA (Enc) and SUF-qCMA (MAC) $\implies$ IND-qCCA (AE).

Proof.

- Since $\mathcal{MA}$ is SUF-qCMA, we get that $\overline{\mathcal{SE}}$ is INT-qCTXT.
- 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, we get that it is IND-qCCA.

$\square$

Constructing Quantum-Resistant Signatures

- Most classical signature schemes are insecure in the quantum model.
- We can apply a transformation (Boneh and Zhandry, 2013) to some of the existing signature schemes.
- In order to be able to make a classical signature scheme quantum resistant, we need it to be:
  - Secure classically.
  - Classically reduce to a quantum-resistant problem.

Signature Construction (Boneh and Zhandry, 2013)

Let $S_c = (G_c, Sign_c, Ver_c)$ 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 $S = (G, Sign, Ver)$ where:

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

If the original signature scheme S_c is SUF-CMA against a classical chosen message attack performed by a quantum adversary, then the transformed scheme S is SUF-qCMA.

Quantum-resistant authenticated encryption schemes

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.

Quantum-resistant authenticated encryption schemes

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 $\sigma = Sign(s, h; t)$.
6. The ciphertext is (c, r, σ).

Quantum-resistant authenticated encryption schemes

Decryption: Suppose Alice receives ciphertext (c, r, σ) from Bob.

1. Compute the value $h = H(c, r)$.
2. Using h and Bob's public signing key p, compute the verification function $Ver(s, h, r, \sigma)$, 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 $m = \mathcal{D}(e, c)$.

Elliptic curves

We assume F is a *finite field* of characteristic *greater than* 3.
"Finite field" is essential, because cryptography uses finite fields.
"Characteristic greater than 3" is not essential, but it simplifies matters greatly.

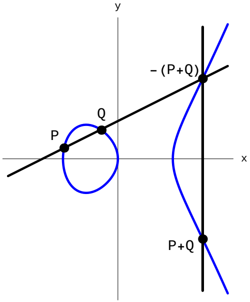
Definition

An *elliptic curve* over F is the set of solutions $(x, y) \in F^2$ to an equation

$$y^2 = x^3 + ax + b, \quad a, b \in F,$$

plus an additional point ∞ (at infinity).

Group law



Elliptic curves admit an abelian group operation with identity element ∞. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then

$$P + Q = \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, \right.$$
$$\left. - \left(\frac{y_2 - y_1}{x_2 - x_1} \right) \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - 2x_1 - x_2 \right) - y_1 \right)$$

Isogenies

Definition

Let E and E' be elliptic curves over F.

- An *isogeny* $\phi\colon E \to E'$ is a non-constant algebraic morphism

  $$\phi(x,y) = \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)} \right)$$

  satisfying $\phi(\infty) = \infty$ (equivalently, $\phi(P+Q) = \phi(P) + \phi(Q)$).
- The *degree* of an isogeny is its degree as an algebraic map.
- The *endomorphism ring* $\mathrm{End}(E)$ is the set of isogenies from $E(\bar{F})$ to itself, together with the constant homomorphism. This set forms a ring under pointwise addition and composition.

Examples

Example (Scalar multiplication)

- Let $E : y^2 = x^3 + ax + b$.
- For $n \in \mathbb{Z}$, define $[n]\colon E \to E$ by $[n](P) = nP$. Then $[n]$ is an isogeny of degree n^2.
- When $n = 2$,

$$[2](x,y) = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \right.$$
$$\left. \frac{(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b - a)y}{8(x^3 + ax + b)^2} \right)$$

- An explicit formula for $[n]$ is given recursively by the so-called *division polynomials*.
- The map $\mathbb{Z} \to \mathrm{End}(E)$ given by $n \mapsto [n]$ is an injective ring homomorphism.

Why Isogenies?

- Finding isogeny between given supersingular elliptic curves over a finite field is believed to be computationally infeasible problem for quantum computers.
- Childs, Jao and Soukharev in 2011 have shown that isogenies over ordinary elliptic curves cannot be used as cryptographic primitives for quantum-resistant protocols.
- Jao and De Feo in 2011 have constructed quantum-resistant key exchange protocol based on isogenies between supersingular elliptic curves.
- Jao and Soukharev in 2014 have constructed quantum-resistant undeniable signature protocol based on isogenies between supersingular elliptic curves.

Isogeny-based authenticated encryption schemes

- We present an example of the quantum-resistant authenticated encryption scheme, which is based on elliptic curve isogenies.
- For the signature/MAC component, we make use of the idea presented in work by Sun, Tian and Wang 2012, together with the work on signature construction by Boneh and Zhandry 2013.
- Key exchange component is based on De Feo and Jao's protocol presented in 2011.

Isogeny-based authenticated encryption schemes

Setup:

1. Choose primes $\ell_A, \ell_B, \ell_{A'}, \ell_{B'}, p, p'$ and exponents $e_A, e_B, e_{A'}, e_{B'}$ such that $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$ and $p' = \ell_{A'}^{e_{A'}} \ell_{B'}^{e_{B'}} \cdot f' \pm 1$ give us supersingular elliptic curves $E/\mathbb{F}_{p^2}$ (which denote simply by E) and $E/\mathbb{F}_{p'^2}$ (which denote simply by E').
2. Choose bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$, which generate $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$, respectively.
3. Choose bases $\{P_{A'}, Q_{A'}\}$ and $\{P_{B'}, Q_{B'}\}$, which generate $E'[\ell_{A'}^{e_{A'}}]$ and $E'[\ell_{B'}^{e_{B'}}]$, respectively.
4. Let $H_1, H_2 : \{0,1\}^* \to \{0,1\}^k$ be independent secure hash functions (with parameter k).

Isogeny-based authenticated encryption schemes

Key Generation:

1. Alice chooses random integers $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ not divisible by ℓ_A and $m'_A, n'_A \in \mathbb{Z}/\ell_{A'}^{e_{A'}}\mathbb{Z}$ not divisible by $\ell_{A'}$. Then, using these values, computes $\phi_A\colon E \to E_A = E/\langle [m_A]P_A + [n_A]Q_A \rangle$ and $\phi'_A\colon E' \to E'_A = E'/\langle [m'_A]P_{A'} + [n'_A]Q_{A'} \rangle$. Then, she computes $\phi_A(P_B), \phi_A(Q_B), \phi'_A(P_{B'}), \phi'_A(Q_{B'})$ and publishes her public key as $\{E_A, E'_A, \phi_A(P_B), \phi_A(Q_B), \phi'_A(P_{B'}), \phi'_A(Q_{B'})\}$. Her private key is $\{m_A, n_A, m'_A, n'_A\}$.
2. Bob chooses random integers $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ not divisible by ℓ_B and $m'_B, n'_B \in \mathbb{Z}/\ell_{B'}^{e_{B'}}\mathbb{Z}$ not divisible by $\ell_{B'}$. Then, similarly to Alice, publishes his public key as $\{E_B, E'_B, \phi_B(P_A), \phi_B(Q_A), \phi'_B(P_{A'}), \phi'_B(Q_{A'})\}$. His private key is $\{m_B, n_B, m'_B, n'_B\}$.

$$
\begin{tikzcd}
& E_A \arrow[r, "{\langle [m_B]\phi_A(P_B)+[n_B]\phi_A(Q_B)\rangle}"] \arrow[dd, dashed, shift left] & E_{BA} \arrow[d, equal] \\
E \arrow[ur, "{\ker(\phi_A)=\langle [m_A]P_A+[n_A]Q_A\rangle}", "{\phi_A(P_B),\phi_A(Q_B)}"'] \arrow[dr, "{\phi_B(P_A),\phi_B(Q_A)}", "{\ker(\phi_B)=\langle [m_B]P_B+[n_B]Q_B\rangle}"'] & & E_{AB} \\
& E_B \arrow[uu, dashed, shift left] \arrow[ur, "{\langle [m_A]\phi_B(P_A)+[n_A]\phi_B(Q_A)\rangle}"'] &
\end{tikzcd}
$$

$$
\begin{tikzcd}
& E'_A \arrow[r, "{\langle [m'_B]\phi'_A(P_{B'})+[n'_B]\phi'_A(Q_{B'})\rangle}"] \arrow[dd, dashed, shift left] & E'_{BA} \arrow[d, equal] \\
E' \arrow[ur, "{\ker(\phi'_A)=\langle [m'_A]P_{A'}+[n'_A]Q_{A'}\rangle}", "{\phi'_A(P_{B'}),\phi'_A(Q_{B'})}"'] \arrow[dr, "{\phi'_B(P_{A'}),\phi'_B(Q_{A'})}", "{\ker(\phi'_B)=\langle [m'_B]P_{B'}+[n'_B]Q_{B'}\rangle}"'] & & E'_{AB} \\
& E'_B \arrow[uu, dashed, shift left] \arrow[ur, "{\langle [m'_A]\phi'_B(P_{A'})+[n'_A]\phi'_B(Q_{A'})\rangle}"'] &
\end{tikzcd}
$$

Isogeny-based authenticated encryption schemes

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

1. Compute ciphertext $c = \mathcal{E}(j(E_{AB}), m)$.
2. Select $r \in \{0,1\}^k$ at random.
3. Bob computes the value $h = H_1(c, r)$.
4. Using h and $j(E'_{AB})$, Bob computes the authentication tag $\sigma = H_2(h || j(E'_{AB}))$.
5. The ciphertext is (c, r, σ).

Isogeny-based authenticated encryption schemes

Decryption: Suppose Alice receives ciphertext (c, r, σ) from Bob.

1. Alice computes the value $h = H_1(c, r)$.
2. Using h and $j(E'_{AB})$, Alice computes $H_2(h||j(E'_{AB}))$ and compares it to the authentication tag σ. If it matches, she continues, if not, stops.
3. Obtains $m = \mathcal{D}(j(E_{AB}), c)$.

Communication Overhead

- 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.
- 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.

Public Key Overhead

- The public key sizes that apply to the AE setting, come from the key-exchange section.
- We aim for 128-bit quantum security.
- 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.

Table: Key transmission overhead

Signature scheme	Bits
Ring-LWE	11600
NTRU	5544
Code-based	52320
Multi-variate	7672000
Isogeny-based	3073

Conclusion and Future Work

- We propose a security model for authenticated encryption against fully quantum adversaries, based on the classical security model of Bellare and Namprempre.
- We apply 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.
- Next step would be to come up with a quantum-resistant protocol, that does not require authenticated public keys (using ideas of ESSR).
- We proposed a composed AE scheme, but the next step would be to come up with atomic (i.e. "one-step") protocols (using ideas of Signcryption, AES-GCM).