Post-quantum Plaintext-awareness

Ehsan Ebrahimi and Jeroen Van Wier
University of Luxembourg

PQCypto 2022

Plaintext-awareness for PKE

- Intuitively, adversary generating a valid ciphertext is aware of its underlying plaintext

Plaintext-awareness for PKE

- Intuitively, adversary generating a valid ciphertext is aware of its underlying plaintext

- It is introduced in the Random Oracle Model to prove the CCA security of the OAEP transform [Bellare-Rogaway, Eurocrypt 1994]

Plaintext-awareness for PKE

- Intuitively, adversary generating a valid ciphertext is aware of its underlying plaintext

- It is introduced in the Random Oracle Model to prove the CCA security of the OAEP transform [Bellare-Rogaway, Eurocrypt 1994]

- It has been formalized in the standard model as well [Bellare-Palacio, ASIACRYPT 2004]

PA Notions : PA0, PA1, PA2

Adversary's goal: Generating a valid ciphertext for which its corresponding plaintext is unknown

PA Notions : PA0, PA1, PA2

Adversary’s goal: Generating a valid ciphertext for which its corresponding plaintext is unknown

- PA0: Adversary can make one decryption query

PA Notions : PA0, PA1, PA2

Adversary's goal: Generating a valid ciphertext for which its corresponding plaintext is unknown

- PA0: Adversary can make one decryption query
- PA1: Adversary can make many decryption queries

PA Notions : PA0, PA1, PA2

Adversary's goal: Generating a valid ciphertexts for which its corresponding plaintext is unknown

- PA0: Adversary can make one decryption query
- PA1: Adversary can make many decryption queries
- PA2: Adversary can make many decryption queries and eavesdrop some ciphertexts

More Formal Definition: PA0, PA1

- For ∀ PT adversary A , ∃ a PT plaintext extractor A^* such that for ∀ PT distinguisher D the following two games are indistinguishable where R is the random tape of A:

Real-world Game:

$x \leftarrow A^{Dec_{sk}}(pk)$

$b \leftarrow D(x)$

Fake Game:

$x \leftarrow A^{A^*(R,pk)}(pk)$

$b \leftarrow D(x)$

More Formal Definition: PA2

- For ∀ PT adversary A , ∃ a PT plaintext extractor A^* such that for ∀ PT plaintext-creator P and for ∀ PT distinguisher D the following two games are indistinguishable where R is the random tape of A:

Real-world Game:

$$m \leftarrow A^{Dec_{sk}}(pk)$$

$$c^* \leftarrow P(m)$$

$$x \leftarrow A^{Dec_{sk}}(pk, c^*)$$

$$b \leftarrow D(x)$$

Fake Game:

$$m \leftarrow A^{A^*(R,pk)}(pk)$$

$$c^* \leftarrow P(m)$$

$$x \leftarrow A^{A^*(R,c^*,pk)}(pk, c^*)$$

$$b \leftarrow D(x)$$

PA Against Quantum Adversaries : Motivations

PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme in a quantum device
    - Does it break PA notions?

PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme in a quantum device
   - Does it break PA notion?

$$\sum \frac{1}{\sqrt{|M|}} |m\rangle$$

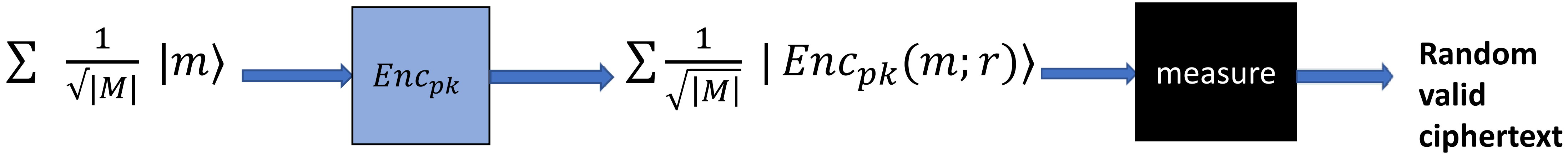
PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme in a quantum device
    - Does it break PA notion?

$$\sum \frac{1}{\sqrt{|M|}} |m\rangle \longrightarrow \boxed{Enc_{pk}} \longrightarrow \sum \frac{1}{\sqrt{|M|}} |Enc_{pk}(m;r)\rangle$$

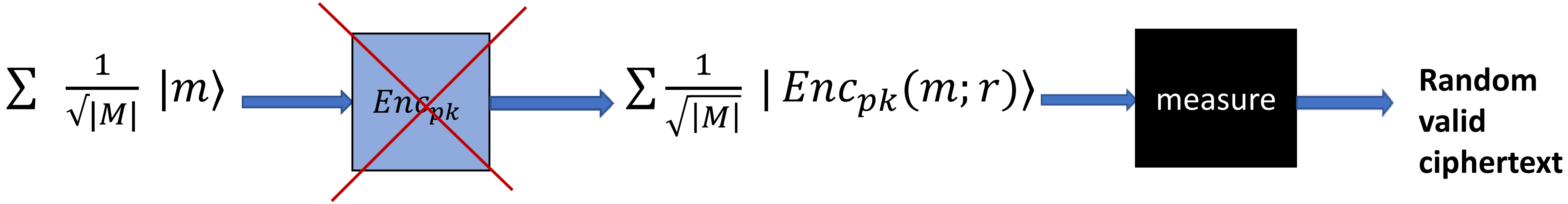
PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme in a quantum device
   - Does it break PA notion?



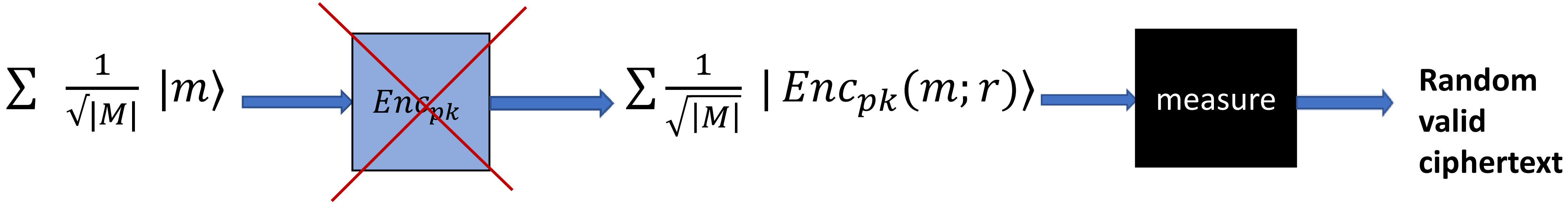
PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme in a quantum device
   - Does it break PA notion?



PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme in a quantum device
   - Does it break PA notion?



- We consider standard implementation: $|\mathrm{m}, \mathrm{y}\rangle \rightarrow |m, y \oplus Enc_{pk}(m;r)\rangle$

PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme

2. It has been used in some existing proof in a high-level [Ebrahimi, PKC 2022]

PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme

2. It has been used in some existing proof in a high-level [Ebrahimi, PKC 2022]

3. PA2 + IND-CPA $\Longrightarrow$ IND-CCA but PA2 + IND-qCPA $\nRightarrow$ IND-qCCA [Boneh-Zhandry's Definition, Crypto 2013]

PA Against Quantum Adversaries : Motivations

1. A quantum adversary given pk can implement the encryption scheme

2. It has been used in some existing proof in a high-level [Ebrahimi, PKC 2022]

3. PA2 + IND-CPA $\Longrightarrow$ IND-CCA but PA2 + IND-qCPA $\not\Rightarrow$ IND-qCCA
   - ? + IND-qCPA $\Longrightarrow$ IND-qCCA

Post-quantum PAs

Post-quantum PAs

- Number of decryption queries:
  - one or many

Post-quantum PAs

- Number of decryption queries:
  - one or many
- Access to the decryption oracle:
  - classical or quantum

Post-quantum PAs

- Number of decryption queries:
  - one or many
- Access to the decryption oracle:
  - classical or quantum
- Eavesdropping ability:
  - only classical

Post-quantum PAs

- Number of decryption queries:
  - one or many
- Access to the decryption oracle:
  - classical or quantum
- Eavesdropping ability:
  - only classical

Six Security notions

pqPA0-C_{Dec}, pqPA1-C_{Dec}

- For ∀ QPT adversary A , ∃ a QPT plaintext extractor A^* such that for ∀ QPT distinguisher D the following two games are indistinguishable where Q_{int} is the internal quantum register of A:

Real-world Game:

$\rho \leftarrow A^{Dec_{sk}}(pk)$

$b \leftarrow D(\rho)$

Fake Game:

$\rho \leftarrow A^{A^*(Q_{int}, pk)}(pk)$

$b \leftarrow D(\rho)$

pqPA0-Q_{Dec}, pqPA1-Q_{Dec}

- For ∀ QPT adversary A , ∃ a QPT plaintext extractor A^* such that for ∀ QPT distinguisher D the following two games are indistinguishable where Q_{int} is the internal quantum register of A:

Real-world Game:

$\rho \leftarrow A^{U_{Dec_{sk}}}(pk)$

$b \leftarrow D(\rho)$

Fake Game:

$\rho \leftarrow A^{A^*(Q_{int}, pk)}(pk)$

$b \leftarrow D(\rho)$

pqPA2-C_{Dec}

- For ∀ QPT adversary A , ∃ a QPT plaintext extractor A^* such that for for ∀ QPT plaintext-creator P, ∀ QPT distinguisher D the following two games are indistinguishable where Q_{int} is the internal quantum register of A:

Real-world Game:

$$m \leftarrow A^{Dec_{sk}}(pk)$$

$$c^* \leftarrow P(m)$$

$$\rho \leftarrow A^{Dec_{sk}}(pk, c^*)$$

$$b \leftarrow D(\rho)$$

Fake Game:

$$m \leftarrow A^{A^*(Q_{int})}(pk)$$

$$c^* \leftarrow P(m)$$

$$\rho \leftarrow A^{A^*(Q_{int}, c^*, pk)}(pk, c^*)$$

$$b \leftarrow D(\rho)$$

pqPA2-Q_{Dec}

- For ∀ QPT adversary A , ∃ a QPT plaintext extractor A^* such that for ∀ QPT plaintext-creator P, ∀ QPT distinguisher D the following two games are indistinguishable where Q_{int} is the internal quantum register of A:

Real-world Game:

$$m \leftarrow A^{U_{Dec_{sk}}}(pk)$$

$$c^* \leftarrow P(m)$$

$$\rho \leftarrow A^{U_{Dec_{sk}}}(pk, c^*)$$

$$b \leftarrow D(\rho)$$

Fake Game:

$$m \leftarrow A^{A^*(Q_{int})}(pk)$$

$$c^* \leftarrow P(m)$$

$$\rho \leftarrow A^{A^*(Q_{int}, c^*, pk)}(pk, c^*)$$

$$b \leftarrow D(\rho)$$

Table of Implications and non-implications

	pqPA2-Q_{dec}	pqPA2-C_{dec}	pqPA1-Q_{dec}	pqPA1-C_{dec}	pqPA0-Q_{dec}	pqPA0-C_{dec}
pqPA2-Q_{dec}		$\Rightarrow$ Theorem 1	$\Rightarrow$ Theorem 2	$\Rightarrow$	$\Rightarrow$	$\Rightarrow$
pqPA2-C_{dec}	$\nRightarrow$ Theorem 4		$\Rightarrow$	$\Rightarrow$ Theorem 1	$\nRightarrow$ Corollary 2	$\Rightarrow$
pqPA1-Q_{dec}	$\nRightarrow$	$\nRightarrow$ Theorem 5		$\Rightarrow$ Theorem 1	$\Rightarrow$ Theorem 3	$\Rightarrow$
pqPA1-C_{dec}	$\nRightarrow$	$\nRightarrow$	$\nRightarrow$ Theorem 4		$\nRightarrow$	$\Rightarrow$ Theorem 3
pqPA0-Q_{dec}	$\nRightarrow$	$\nRightarrow$	$\nRightarrow$	$\nRightarrow$ Theorem 6		$\Rightarrow$ Theorem 1
pqPA0-C_{dec}	$\nRightarrow$	$\nRightarrow$	$\nRightarrow$	$\nRightarrow$	$\nRightarrow$ Corollary 1	

pqPAi-C_{Dec} $\not\Rightarrow$ pqPAi-Q_{Dec}

pqPAi-C_{Dec} $\nRightarrow$ pqPAi-Q_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PAi - C_{Dec}$. Commit to a valid ciphertext $c_v = Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

pqPAi-C_{Dec} $\not\Rightarrow$ pqPAi-Q_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PAi - C_{Dec}$. Commit to a valid ciphertext $c_v = Enc(m;r)$: $Com(c_v) = (c_{com}, r_{open})$

- Change Dec to Dec':
  - A periodic function f on c_v is embedded in Dec'
  - A query to Dec' on $(\perp, c_v)$ reveals r and r_{open}

pqPAi-C_{Dec} $\nRightarrow$ pqPAi-Q_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PAi - C_{Dec}$. Commit to a valid ciphertext c_v= $Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

- Change Dec to Dec':
  - A periodic function f on c_v is embedded in Dec'
  - A query to Dec' on $(\perp, c_v)$ reveals r and r_{open}

- Distinguisher checks if $c_v := Enc(m; r)$ and $verif\left(c_{com}, c_v, r_{open}\right) = 1$

pqPAi-C_{Dec} $\nRightarrow$ pqPAi-Q_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PAi - C_{Dec}$. Commit to a valid ciphertext $c_v = Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

- Change Dec to Dec':
  - A periodic function f on c_v is embedded in Dec'
    - Simon's algorithm can output c_v using quantum queries
  - A query to Dec' on $(\perp, c_v)$ reveals r and r_{open}

- Distinguisher checks if $c_v := Enc(m; r)$ and $verif(c_{com}, c_v, r_{open}) = 1$

pqPA1-Q_{Dec} $\nRightarrow$ pqPA2-C_{Dec}

pqPA1-Q_{Dec} $\nRightarrow$ pqPA2-C_{Dec}

- Take a $\mathrm{p}qPA1 - Q_{Dec}\ PKE = (Gen, Enc, Dec)$ that is IND-qCPA secure

pqPA1-Q_{Dec} $\nRightarrow$ pqPA2-C_{Dec}

- Take a $\mathrm{p}qPA1 - Q_{Dec}\ PKE = (Gen, Enc, Dec)$ that is IND-qCPA secure

- Make it malleable by defining: $Enc'(m) = Enc(m)||0\ and\ Dec'(c||b) = Dec(c)$

pqPA1-$Q_{Dec} \nRightarrow$ pqPA2-C_{Dec}

- Take a $pqPA1 - Q_{Dec}\ PKE = (Gen, Enc, Dec)$ that is IND-qCPA secure

- Make it malleable by defining: $Enc'(m) = Enc(m)||0\ and\ Dec'(c||b) = Dec(c)$

- Show that PKE'=(Gen, Enc', Dec') is $pqPA1 - Q_{Dec}$

pqPA1-Q_{Dec} $\nRightarrow$ pqPA2-C_{Dec}

- Take a $\text{p}qPA1 - Q_{Dec}\ PKE = (Gen, Enc, Dec)$ that is IND-qCPA secure

- Make it malleable by defining: $Enc'(m) = Enc(m)||0\ and\ Dec'(c||b) = Dec(c)$

- Show that PKE'=(Gen, Enc', Dec') is $\text{p}qPA1 - Q_{Dec}$

- Adversary A sends two messages $0^n, 1^n$ to P and gets a ciphertext $c||0$, queries $c||1$ as a decryption query

pqPA1-Q_{Dec} $\not\Rightarrow$ pqPA2-C_{Dec}

- Take a $pqPA1 - Q_{Dec}$ $PKE = (Gen, Enc, Dec)$ that is IND-qCPA secure
- Make it malleable by defining: $Enc'(m) = Enc(m)||0$ and $Dec'(c||b) = Dec(c)$
- Show that PKE'=(Gen, Enc', Dec') is $pqPA1 - Q_{Dec}$
- Adversary A sends two messages $0^n, 1^n$ to P and gets a ciphertext $c||0$, queries $c||1$ as a decryption query
- Show that if PKE=(Gen, Enc', Dec') is $pqPA2 - C_{Dec}$, then it is not IND-qCPA secure

pqPA0-Q_{Dec} $\not\Rightarrow$ pqPA1-C_{Dec}

pqPA0-Q_{Dec} $\nRightarrow$ pqPA1-C_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PA0 - Q_{Dec}$. Commit to a valid ciphertext $c_v := Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

pqPA0-Q_{Dec} $\nRightarrow$ pqPA1-C_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PA0 - Q_{Dec}$. Commit to a valid ciphertext $c_v := Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

- Write $c_v = c_v^1 \oplus c_v^2$ and $r_{open} = r_{open}^1 \oplus r_{open}^2$. Change Dec to Dec' that reveals one of c_v^1, c_v^2 and r_{open}^1, r_{open}^2 randomly in each query. It reveals r as well.

pqPA0-Q_{Dec} $\not\Rightarrow$ pqPA1-C_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and $\text{p}qPA0 - Q_{Dec}$. Commit to a valid ciphertext $c_v := Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

- Write $c_v = c_v^1 \oplus c_v^2$ and $r_{open} = r_{open}^1 \oplus r_{open}^2$. Change Dec to Dec' that reveals one of c_v^1, c_v^2 and r_{open}^1, r_{open}^2 randomly in each query. It reveals r as well.

- Show that PKE remains $\text{p}qPA0 - Q_{Dec}$ with this new Dec'

pqPA0-Q_{Dec} $\nRightarrow$ pqPA1-C_{Dec}

- Take a $PKE = (Gen, Enc, Dec)$ that is one-way and pq$PA0 - Q_{Dec}$. Commit to a valid ciphertext $c_v := Enc(m; r)$: $Com(c_v) = (c_{com}, r_{open})$

- Write $c_v = c_v^1 \oplus c_v^2$ and $r_{open} = r_{open}^1 \oplus r_{open}^2$. Change Dec to Dec' that reveals one of c_v^1, c_v^2 and r_{open}^1, r_{open}^2 randomly in each query. It reveals r as well.

- Show that PKE remains pq$PA0 - Q_{Dec}$ with this new Dec'

- Adversary with many decryption queries can get c_v and checks if $c_v := Enc(m; r)$ and $verif\left(c_{com}, c_v, r_{open}\right) = 1$

Relation with IND-qCCA

- Any public-key encryption scheme Enc that is $pqPA2 - Q_{Dec}$ plaintext-aware and IND-qCPA secure is IND-qCCA secure.

Achievability

- We lift a $pqPA2 - C_{Dec}$ plaintext-aware encryption scheme to a $pqPA2 - Q_{Dec}$ plaintext-aware encryption scheme using a quantum secure PRP

Conclusion

- We formalized the plaintext-awareness notions in the superposition-access model that led to six security notions

Conclusion

- We formalized the plaintext-awareness notions in the superposition-access model that led to six security notions

- We studied the relations between these six security notions

Conclusion

- We formalized the plaintext-awareness notions in the superposition-access model that led to six security notions
- We studied the relations between these six security notions
- We show the relation with IND-qCCA notion

Conclusion

- We formalized the plaintext-awareness notions in the superposition-access model that led to six security notions
- We studied the relations between these six security notions
- We show the relation with IND-qCCA notion
- We lift a post-quantum PA2 encryption scheme to a $pqPA2 - Q_{Dec}$ plaintext-aware encryption scheme using a quantum-secure PRP

Thank you for listening