On Security Notions for Encryption in a Quantum World

Céline Chevalier [1] Ehsan Ebrahimi [2] Quoc-Huy Vu [1]

[1]Université Panthéon-Assas Paris II [2]University of Luxembourg

Motivations

Classical Security

Classical adversaries, classical communication

Motivations

Classical Security

Classical adversaries, classical communication

Post-quantum Security

Quantum adversaries, classical communication

Motivations

Classical Security

Classical adversaries, classical communication

Post-quantum Security

Quantum adversaries, classical communication

Fully-Quantum Security [BZ'13, DFNS'14, GHS'16]

Quantum adversaries, **quantum** communication.

- Running classically obfuscated programs in quantum computers
- Exotic quantum attacks: frozen smart-card attack

Motivations

This paper: fully-quantum security for classical **encryption**.

Classical Security

Classical adversaries, classical communication

Post-quantum Security

Quantum adversaries, classical communication

Fully-Quantum Security [BZ'13, DFNS'14, GHS'16]

Quantum adversaries, **quantum** communication.

- Running classically obfuscated programs in quantum computers
- Exotic quantum attacks: frozen smart-card attack

Prior Results

1. Superposition access to encryption oracle

Prior Results

1. Superposition access to encryption oracle

$$\sum_x \alpha_x |x, y\rangle \mapsto \sum_x \alpha_x |x, y \oplus \mathsf{Enc}(x)\rangle$$

Prior Results

1. Superposition access to encryption oracle
2. Superposition access to decryption oracle in chosen-ciphertext security.

Prior Results

1. Superposition access to encryption oracle
2. Superposition access to decryption oracle in chosen-ciphertext security.

BZ'13 Superposition access to encryption and decryption oracles, but challenges are classical, for both PKE and SKE.

Prior Results

1. Superposition access to encryption oracle
2. Superposition access to decryption oracle in chosen-ciphertext security.

BZ'13 Superposition access to encryption and decryption oracles, but challenges are classical, for both PKE and SKE.

GHS'16 Quantum challenges, but restricted to a special minimal oracle, limited to only SKE and CPA security.

Prior Results

1. Superposition access to encryption oracle
2. Superposition access to decryption oracle in chosen-ciphertext security.

BZ'13	Superposition access to encryption and decryption oracles, but challenges are classical, for both PKE and SKE.
GHS'16	Quantum challenges, but restricted to a special minimal oracle, limited to only SKE and CPA security.
Open	Quantum challenges, in the standard oracle model, for both PKE and SKE with CCA security.

- No-cloning Theorem
- Measurement destructiveness
- Impossibility for any Left-or-Right indistinguishability notion [BZ'13]

Our Work

Main Results

An achievable, meaningful quantum notion of chosen-ciphertext security for both secret- and public-key encryption.

Our Work

Main Results

An achievable, meaningful quantum notion of chosen-ciphertext security for both secret- and public-key encryption.

Our Techniques

Our Work

Main Results

An achievable, meaningful quantum notion of chosen-ciphertext security for both secret- and public-key encryption.

Our Techniques

- Switching from a Left-or-Right indistinguishability notion to a Real-or-Random indistinguishability notion.

Our Work

Main Results

An achievable, meaningful quantum notion of chosen-ciphertext security for both secret- and public-key encryption.

Our Techniques

- Switching from a Left-or-Right indistinguishability notion to a Real-or-Random indistinguishability notion.
- Adapting Zhandry's compressed oracle technique to randomized functions.

[Zhandry'19]

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify

   Measuring $\sum_h |h\rangle = h \xleftarrow{\$} \mathcal{U}$

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain

$$\boxed{|x,y\rangle_{\mathcal{A}}|h\rangle_{\mathcal{O}} \mapsto |x, y \oplus h(x)\rangle_{\mathcal{A}}|h\rangle_{\mathcal{O}}} \xRightarrow[\text{Transform}]{\text{Fourier}} \boxed{|x,y\rangle_{\mathcal{A}}|h\rangle_{\mathcal{O}} \mapsto |x,y\rangle_{\mathcal{A}}|h \oplus P_{x,y}\rangle_{\mathcal{O}}}$$

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain
3. Compress

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain
3. Compress

   Initial Oracle State $D = \{\}$. Query(x, y, D):
   1. If $\nexists (x, y') \in D$, $D = D \cup \{(x, 0)\}$
   2. $D = D \setminus \{(x, y')\} \cup \{(x, y \oplus y')\}$
   3. $D = D \setminus \{(x, 0)\}$ if $\exists (x, 0) \in D$

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

   The oracle now has information about the adversary's queries.

[1] © Zhandry, CRYPTO'19

Zhandry's Recording Technique [Zhandry'19][1]

- Goal: on-the-fly simulation of random oracles in the quantum setting.

Four steps

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

Perfect Simulability

This is a perfect simulation for quantum random oracles.

[1] © Zhandry, CRYPTO'19

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

Recording Technique for Randomized Functions

Consider a randomized function $f(x;r)$

1. Quantum-ify

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

1. Quantum-ify

   Measuring $\sum_r |r\rangle = r \xleftarrow{\$} \mathcal{U}$

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

1. Quantum-ify
2. Look at Fourier Domain

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

1. Quantum-ify
2. Look at Fourier Domain

$$\boxed{|x, y\rangle_{\mathcal{A}} |r, f_r\rangle_{\mathcal{O}} \mapsto |x, y \oplus f(x; r)\rangle_{\mathcal{A}} |r, f_r\rangle_{\mathcal{O}}} \xRightarrow{\text{QFT}} \boxed{|x, y\rangle_{\mathcal{A}} |r, f_r\rangle_{\mathcal{O}} \mapsto |x, y\rangle_{\mathcal{A}} |r, f_r \oplus P_{x,y}\rangle_{\mathcal{O}}}$$

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress

Recording Technique for Randomized Functions

Consider a randomized function $f(x;r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress

   Initial Oracle State $D = \{\}$. Query(x, y, D):

   1. If $\nexists (r, x, y') \in D$, $D = D \cup \{(r, x, f(x;r))\}$
   2. $D = D \setminus \{(r, x, y')\} \cup \{(r, x, f(x;r) \oplus y')\}$
   3. $D = D \setminus \{(r, x, 0)\}$ if $\exists (r, x, 0) \in D$

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

Recording Technique for Randomized Functions

Consider a randomized function $f(x;r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

Caveat!

The above simulation needs 3 applications of U_f. Thus it is not useful for:

Recording Technique for Randomized Functions

Consider a randomized function $f(x;r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

Caveat!

The above simulation needs 3 applications of U_f. Thus it is not useful for:

- Proving one-time security

Recording Technique for Randomized Functions

Consider a randomized function $f(x;r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

Caveat!

The above simulation needs 3 applications of U_f. Thus it is not useful for:

- Proving one-time security
- Security reductions (Encrypt-then-Mac)

Recording Technique for Randomized Functions

Consider a randomized function $f(x; r)$

1. Quantum-ify
2. Look at Fourier Domain
3. Compress
4. Revert back to Primal Domain

Caveat!

The above simulation needs 3 applications of U_f. Thus it is not useful for:

- Proving one-time security
- Security reductions (Encrypt-then-Mac)

Simulation with 1 call to U_f

In the randomized setting, the database is always initialized to "zero", thus we can simulate with only one call to U_f.

IND-CCA (Real-or-Random)[2]

$\underline{\mathsf{Expt}^b_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $(x, \mathsf{state}) \leftarrow \mathcal{A}_1^{\mathsf{Enc}_\mathtt{k}, \mathsf{Dec}_\mathtt{k}}(\lambda)$
3. $x_0 \leftarrow x, x_1 \xleftarrow{\$} \mathcal{X}$
4. $y^\star \leftarrow \mathsf{Enc}_\mathtt{k}(x_b)$
5. $b' \leftarrow \mathcal{A}_2^{\mathsf{Enc}_\mathtt{k}, \mathsf{Dec}^\star_\mathtt{k}}(y^\star, \mathsf{state})$
6. **return** b'

- $\mathsf{Dec}^\star_\mathtt{k}(y) = \begin{cases} \perp & \text{if } \quad y = y^\star \\ \mathsf{Dec}_\mathtt{k}(y) \end{cases}$

$$\left|\Pr\left[\mathsf{Expt}^1_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{Expt}^0_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right]\right| \leq \epsilon$$

[2] Single-Challenge

IND-CCA (Real-or-Random)[2]

$\underline{\mathsf{Expt}^b_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $(x, \mathsf{state}) \leftarrow \mathcal{A}_1^{\mathsf{Enc}_\mathtt{k}, \mathsf{Dec}_\mathtt{k}}(\lambda)$
3. $x_0 \leftarrow x, x_1 \xleftarrow{\$} \mathcal{X}$
4. $y^\star \leftarrow \mathsf{Enc}_\mathtt{k}(x_b)$
5. $b' \leftarrow \mathcal{A}_2^{\mathsf{Enc}_\mathtt{k}, \mathsf{Dec}^\star_\mathtt{k}}(y^\star, \mathsf{state})$
6. **return** b'

- $\mathsf{Dec}^\star_\mathtt{k}(y) = \begin{cases} \perp & \text{if} \quad y = y^\star \\ \mathsf{Dec}_\mathtt{k}(y) \end{cases}$

$$\left|\Pr\left[\mathsf{Expt}^1_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{Expt}^0_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right]\right| \leq \epsilon$$

[2] Single-Challenge

IND-CCA (Real-or-Random)[2]

$\underline{\mathsf{Expt}^b_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $(x, \mathsf{state}) \leftarrow \mathcal{A}_1^{\mathsf{Enc}_{\mathtt{k}}, \mathsf{Dec}_{\mathtt{k}}}(\lambda)$
3. $x_0 \leftarrow x, x_1 \xleftarrow{\$} \mathcal{X}$
4. $y^\star \leftarrow \mathsf{Enc}_{\mathtt{k}}(x_b)$
5. $b' \leftarrow \mathcal{A}_2^{\mathsf{Enc}_{\mathtt{k}}, \mathsf{Dec}^\star_{\mathtt{k}}}(y^\star, \mathsf{state})$
6. **return** b'

- $\mathsf{Dec}^\star_{\mathtt{k}}(y) = \begin{cases} x & \text{if} \quad y = y^\star \\ \mathsf{Dec}_{\mathtt{k}}(y) & \end{cases}$

$$\left|\Pr\left[\mathsf{Expt}^1_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{Expt}^0_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right]\right| \leq \epsilon$$

[2] Single-Challenge

IND-CCA (Real-or-Random)[2]

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $(x, \mathsf{state}) \leftarrow \mathcal{A}_1^{\mathsf{Enc}_{\mathtt{k}}, \mathsf{Dec}_{\mathtt{k}}}(\lambda)$
3. $x_0 \leftarrow x, x_1 \xleftarrow{\$} \mathcal{X}$
4. $y^\star \leftarrow \mathsf{Enc}_{\mathtt{k}}(x_b)$
5. $b' \leftarrow \mathcal{A}_2^{\mathsf{Enc}_{\mathtt{k}}, \mathsf{Dec}^\star_{\mathtt{k}}}(y^\star, \mathsf{state})$
6. **return** b'

- $\mathsf{Dec}^\star_{\mathtt{k}}(y) = \begin{cases} x & \text{if} \quad y = y^\star \\ \mathsf{Dec}_{\mathtt{k}}(y) & \end{cases}$

$$\left|\Pr\left[\mathsf{Expt}^{1}_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{Expt}^{0}_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right]\right| \leq \epsilon$$

[2] Single-Challenge

IND-CCA (Real-or-Random)[2]

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $(x, \mathsf{state}) \leftarrow \mathcal{A}_1^{\mathsf{Enc}_{\mathtt{k}}, \mathsf{Dec}_{\mathtt{k}}}(\lambda)$
3. $\pi \xleftarrow{\$} \Pi$
4. $y^\star \leftarrow \mathsf{Enc}_{\mathtt{k}}(\pi^b(x))$
5. $b' \leftarrow \mathcal{A}_2^{\mathsf{Enc}_{\mathtt{k}}, \mathsf{Dec}^\star_{\mathtt{k}}}(y^\star, \mathsf{state})$
6. **return** b'

- $\mathsf{Dec}^\star_{\mathtt{k}}(y) = \begin{cases} x & \text{if} \quad y = y^\star \\ \mathsf{Dec}_{\mathtt{k}}(y) \end{cases}$
- $\pi^b = \begin{cases} \pi & \text{if} \quad b = 1 \\ \mathbb{1} & \text{if} \quad b = 0 \end{cases}$

$$\left|\Pr\left[\mathsf{Expt}^{1}_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{Expt}^{0}_{\mathcal{SE}}(\lambda, \mathcal{A}) = 1\right]\right| \leq \epsilon$$

[2] Single-Challenge

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})\text{:}}$

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})\text{:}}$

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $\underbrace{\sum_{x,y} \alpha_{x,y} |x, y, \phi_{x,y}\rangle}_{|\Phi\rangle} \leftarrow \mathcal{A}_1^{|\mathsf{Enc}_{\mathtt{k}}\rangle, |\mathsf{Dec}_{\mathtt{k}}\rangle}(\lambda)$

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})\text{:}}$

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $\underbrace{\sum_{x,y} \alpha_{x,y} \left|x, y, \phi_{x,y}\right\rangle}_{|\Phi\rangle} \leftarrow \mathcal{A}_1^{|\mathsf{Enc}_{\mathtt{k}}\rangle, |\mathsf{Dec}_{\mathtt{k}}\rangle}(\lambda)$
3. $\pi \xleftarrow{\$} \Pi$

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^b_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $\underbrace{\sum_{x,y} \alpha_{x,y} |x, y, \phi_{x,y}\rangle}_{|\Phi\rangle} \leftarrow \mathcal{A}_1^{|\mathsf{Enc}_\mathtt{k}\rangle, |\mathsf{Dec}_\mathtt{k}\rangle}(\lambda)$
3. $\pi \xleftarrow{\$} \Pi$
4. $\sum_{x,y} \alpha_{x,y} \underbrace{|x, y \oplus \mathsf{Enc}_\mathtt{k}(\pi^b(x)), \phi_{x,y}\rangle}_{|\Psi\rangle} \otimes D_{x,y} \leftarrow \mathsf{Enc}_\mathtt{k} \circ \pi^b |\Phi\rangle$

Use compressed oracle here

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $\underbrace{\sum_{x,y} \alpha_{x,y} |x, y, \phi_{x,y}\rangle}_{|\Phi\rangle} \leftarrow \mathcal{A}_1^{|\mathsf{Enc}_{\mathtt{k}}\rangle, |\mathsf{Dec}_{\mathtt{k}}\rangle}(\lambda)$
3. $\pi \xleftarrow{\$} \Pi$
4. $\sum_{x,y} \alpha_{x,y} \underbrace{|x, y \oplus \mathsf{Enc}_{\mathtt{k}}(\pi^b(x)), \phi_{x,y}\rangle}_{|\Psi\rangle} \otimes D_{x,y} \leftarrow \mathsf{Enc}_{\mathtt{k}} \circ \pi^b |\Phi\rangle$
5. $b' \leftarrow \mathcal{A}_2^{|\mathsf{Enc}_{\mathtt{k}}\rangle, |\mathsf{Dec}^{\star}_{\mathtt{k}}\rangle}(|\Psi\rangle)$

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^b_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $\underbrace{\sum_{x,y} \alpha_{x,y} |x, y, \phi_{x,y}\rangle}_{|\Phi\rangle} \leftarrow \mathcal{A}_1^{|\mathsf{Enc}_\mathtt{k}\rangle, |\mathsf{Dec}_\mathtt{k}\rangle}(\lambda)$
3. $\pi \xleftarrow{\$} \Pi$
4. $\sum_{x,y} \alpha_{x,y} \underbrace{|x, y \oplus \mathsf{Enc}_\mathtt{k}(\pi^b(x)), \phi_{x,y}\rangle}_{|\Psi\rangle} \otimes D_{x,y} \leftarrow \mathsf{Enc}_\mathtt{k} \circ \pi^b |\Phi\rangle$
5. $b' \leftarrow \mathcal{A}_2^{|\mathsf{Enc}_\mathtt{k}\rangle, |\mathsf{Dec}^\star_\mathtt{k}\rangle}(|\Psi\rangle)$
6. **return** b'

qIND-qCCA (Real-or-Random)

$\underline{\mathsf{Expt}^{b}_{\mathcal{SE}}(\lambda, \mathcal{A})}$:

1. $\mathtt{k} \xleftarrow{\$} \mathcal{K}()$
2. $\underbrace{\sum_{x,y} \alpha_{x,y} \left|x, y, \phi_{x,y}\right\rangle}_{|\Phi\rangle} \leftarrow \mathcal{A}_1^{|\mathsf{Enc}_{\mathtt{k}}\rangle, |\mathsf{Dec}_{\mathtt{k}}\rangle}(\lambda)$
3. $\pi \xleftarrow{\$} \Pi$
4. $\sum_{x,y} \alpha_{x,y} \underbrace{\left|x, y \oplus \mathsf{Enc}_{\mathtt{k}}(\pi^b(x)), \phi_{x,y}\right\rangle}_{|\Psi\rangle} \otimes D_{x,y} \leftarrow \mathsf{Enc}_{\mathtt{k}} \circ \pi^b \left|\Phi\right\rangle$
5. $b' \leftarrow \mathcal{A}_2^{|\mathsf{Enc}_{\mathtt{k}}\rangle, |\mathsf{Dec}^{\star}_{\mathtt{k}}\rangle}(|\Psi\rangle)$
6. **return** b'

$$\mathsf{Dec}^{\star}_{\mathtt{k}} \left|y, z\right\rangle \otimes D = \begin{cases} \left|y, z \oplus \mathsf{Dec}_{\mathtt{k}}(y)\right\rangle & \text{if } \nexists (w, y) \in D \\ \left|y, z \oplus w\right\rangle & \text{if } \exists (w, y) \in D \end{cases}$$

Properties & Achievability

Properties & Achievability

Properties

- qIND security $\Rightarrow$ IND security
- Composability
- IND-qCCA $\not\Leftrightarrow$ qIND-qCPA

Properties & Achievability

Properties

- qIND security $\Rightarrow$ IND security
- Composability
- IND-qCCA $\not\Leftrightarrow$ qIND-qCPA
  - One-time pad encryption style (stream cipher, GCM, CFB, OFB, CTR ...) is insecure.

Properties & Achievability

Properties

- qIND security $\Rightarrow$ IND security
- Composability
- IND-qCCA $\not\Leftrightarrow$ qIND-qCPA
  - One-time pad encryption style (stream cipher, GCM, CFB, OFB, CTR ...) is insecure.

Achievability

- Encrypt-then-MAC is qIND-qCCA
- IND-qCCA PKE + OWF $\Rightarrow$ qIND-qCCA PKE

Thank you!