Tighter QCCA-Secure Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model

Jiangxia Ge, Tianshu Shan and Rui Xue

SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences

University of Chinese Academy of Sciences

CRYPTO 2023

中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

中国科学院大学
University of Chinese Academy of Sciences

Overview

Background

NIST's post-quantum cryptography (PQC) standardization

- Public key encryption (PKE)
- Key encapsulation mechanism (KEM)
- Digital signatures (DS)

KEM constructions in the PQC standardization

KEM variants of Fujisaki-Okamoto (FO) transformation [HHK17]

- FO-like transformations: $\mathsf{FO}^{\not\perp}$, $\mathsf{FO}^{\perp}$, $\mathsf{FO}_m^{\not\perp}$, $\mathsf{FO}_m^{\perp}$, $\mathsf{QFO}_m^{\not\perp}$ and $\mathsf{QFO}_m^{\perp}$
- Modular FO transformations: $\mathsf{U}^{\not\perp}$, $\mathsf{U}^{\perp}$, $\mathsf{U}_m^{\not\perp}$, $\mathsf{U}_m^{\perp}$, $\mathsf{QU}_m^{\not\perp}$ and $\mathsf{QU}_m^{\perp}$

OW/IND-CPA-secure PKE⇒IND-CCA-secure KEM (ROM)

KEM constructions in the PQC standardization

KEM variants of Fujisaki-Okamoto (FO) transformation [HHK17]

- FO-like transformations: $\mathsf{FO}^{\not\perp}$, $\mathsf{FO}^{\perp}$, $\mathsf{FO}_m^{\not\perp}$, $\mathsf{FO}_m^{\perp}$, $\mathsf{QFO}_m^{\not\perp}$ and $\mathsf{QFO}_m^{\perp}$
- Modular FO transformations: $\mathsf{U}^{\not\perp}$, $\mathsf{U}^{\perp}$, $\mathsf{U}_m^{\not\perp}$, $\mathsf{U}_m^{\perp}$, $\mathsf{QU}_m^{\not\perp}$ and $\mathsf{QU}_m^{\perp}$

OW/IND-CPA-secure PKE $\Rightarrow$ IND-CCA-secure KEM (ROM)

- $\perp$ (explicit rejection type): Decapsulation algorithm outputs $\perp$ for an invalid ciphertext
- $\not\perp$ (implicit rejection type): Decapsulation algorithm outputs a pseudorandom value for an invalid ciphertext

KEM constructions in the PQC standardization

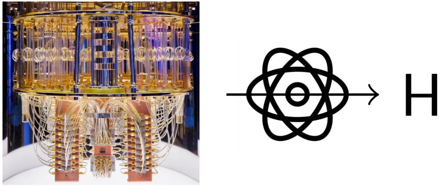
KEM variants of Fujisaki-Okamoto (FO) transformation [HHK17]

- FO-like transformations: $\mathsf{FO}^{\not\perp}$, $\mathsf{FO}^{\perp}$, $\mathsf{FO}^{\not\perp}_m$, $\mathsf{FO}^{\perp}_m$, $\mathsf{QFO}^{\not\perp}_m$ and $\mathsf{QFO}^{\perp}_m$
- Modular FO transformations: $\mathsf{U}^{\not\perp}$, $\mathsf{U}^{\perp}$, $\mathsf{U}^{\not\perp}_m$, $\mathsf{U}^{\perp}_m$, $\mathsf{QU}^{\not\perp}_m$ and $\mathsf{QU}^{\perp}_m$

OW/IND-CPA-secure PKE⇒IND-CCA-secure KEM (ROM)

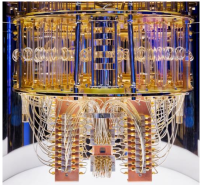
- $\perp$ (explicit rejection type): Decapsulation algorithm outputs $\perp$ for an invalid ciphertext
- $\not\perp$ (implicit rejection type): Decapsulation algorithm outputs a pseudorandom value for an invalid ciphertext
- m: Encapsulation algorithm outputs $G(m^*)$ as the key
- Without m: Encapsulation algorithm outputs $G(m^*, c^*)$ as the key

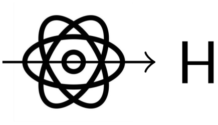
Quantum random oracle model [BDF$^+$11]



- Quantum computer can compute hash function H on an arbitrary superposition of inputs.

Quantum random oracle model [BDF+11]

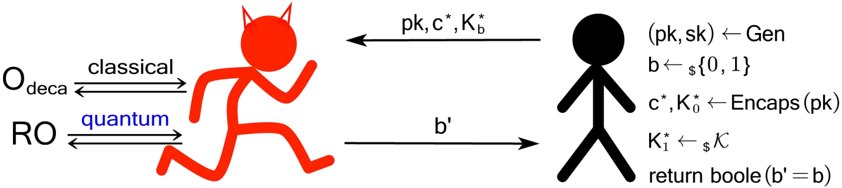




- Quantum computer can compute hash function H on an arbitrary superposition of inputs.
- The ROM should be lifted to the quantum random oracle model (QROM)

IND-CCA and IND-qCCA security [BZ13]

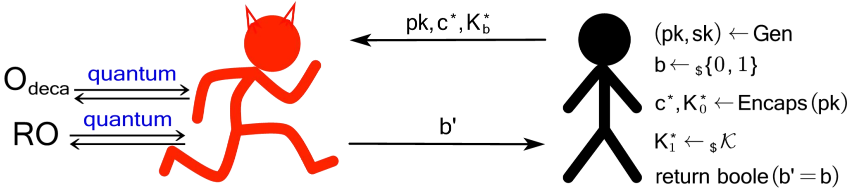
IND-CCA game of KEM (QROM)



IND-CCA and IND-qCCA security [BZ13]

Indistinguishability under quantum chosen-ciphertext attacks (IND-qCCA)

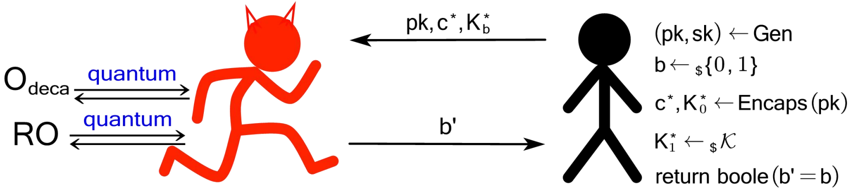
IND-qCCA game of KEM (QROM)



IND-CCA and IND-qCCA security [BZ13]

Indistinguishability under quantum chosen-ciphertext attacks (IND-qCCA)

IND-qCCA game of KEM (QROM)



IND-qCCA security *implies* IND-CCA security (QROM)

Motivation - 1

Appendix A of [HHM22] (eprint 2022/365):

- Security of $\mathsf{FO}_m^{\perp}$ implies security of all the remaining FO-like transformations

  $\mathsf{FO}^{\not\perp}$, $\mathsf{FO}^{\perp}$, $\mathsf{FO}_m^{\not\perp}$, $\mathsf{FO}_m^{\perp}$, $\mathsf{QFO}_m^{\not\perp}$ and $\mathsf{QFO}_m^{\perp}$

Motivation - 1

Appendix A of [HHM22] (eprint 2022/365):

- Security of $\mathsf{FO}_m^{\perp}$ implies security of all the remaining FO-like transformations

$$\mathsf{FO}^{\not\perp},\ \mathsf{FO}^{\perp},\ \mathsf{FO}_m^{\not\perp},\ \mathsf{FO}_m^{\perp},\ \mathsf{QFO}_m^{\not\perp} \text{ and } \mathsf{QFO}_m^{\perp}$$

Transformation	Underlying security	Achieved security	Requirement	Security bound(≈)
$\mathsf{FO}_m^{\perp}$ [DFMS22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q^{1.5} q_D \cdot \sqrt[4]{2^{-\gamma}} + q^2\sqrt{\delta}$
$\mathsf{FO}_m^{\perp}$ [HHM22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathsf{FO}_m^{\perp}$ [HHM22]	IND-CPA	IND-CCA	γ-spread	$\sqrt{q \cdot \epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathsf{FO}^{\not\perp}$ [KSS+20]	IND-CPA	IND-CCA	η-injective	$q^2 \cdot \epsilon + q \cdot \sqrt{\eta} + \cdots$

Motivation - 1

Appendix A of [HHM22] (eprint 2022/365):

- Security of $\mathsf{FO}_m^{\perp}$ implies security of all the remaining FO-like transformations

$$\mathsf{FO}^{\not\perp},\ \mathsf{FO}^{\perp},\ \mathsf{FO}_m^{\not\perp},\ \mathsf{FO}_m^{\perp},\ \mathsf{QFO}_m^{\not\perp} \text{ and } \mathsf{QFO}_m^{\perp}$$

Transformation	Underlying security	Achieved security	Requirement	Security bound($\approx$)
$\mathsf{FO}_m^{\perp}$ [DFMS22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q^{1.5} q_D \cdot \sqrt[4]{2^{-\gamma}} + q^2 \sqrt{\delta}$
$\mathsf{FO}_m^{\perp}$ [HHM22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathsf{FO}_m^{\perp}$ [HHM22]	IND-CPA	IND-CCA	γ-spread	$\sqrt{q \cdot \epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathsf{FO}^{\not\perp}$ [KSS+20]	IND-CPA	IND-CCA	η-injective	$q^2 \cdot \epsilon + q \cdot \sqrt{\eta} + \cdots$

Can we give a security reduction of $\mathsf{FO}_m^{\perp}$ that avoids the quadratic security loss and has a tighter security bound (QROM)?

Motivation - 2

Appendix A of [HHM22] (eprint 2022/365):

- Security of $\mathsf{FO}_m^{\perp}$ implies security of all the remaining FO-like transformations

$$\mathsf{FO}^{\not\perp},\ \mathsf{FO}^{\perp},\ \mathsf{FO}_m^{\not\perp},\ \mathsf{FO}_m^{\perp},\ \mathsf{QFO}_m^{\not\perp} \text{ and } \mathsf{QFO}_m^{\perp}$$

Transformation	Underlying security	Achieved security	Requirement	Security bound($\approx$)
$\mathsf{FO}_m^{\perp}$ [DFMS22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q^{1.5} q_D \cdot \sqrt[4]{2^{-\gamma}} + q^2\sqrt{\delta}$
$\mathsf{FO}_m^{\perp}$ [HHM22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathsf{FO}_m^{\perp}$ [HHM22]	IND-CPA	IND-CCA	γ-spread	$\sqrt{q \cdot \epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathsf{FO}^{\not\perp}$ [KSS+20]	IND-CPA	IND-CCA	η-injective	$q^2 \cdot \epsilon + q \cdot \sqrt{\eta} + \cdots$

Motivation - 2

Appendix A of [HHM22] (eprint 2022/365):

- Security of $\mathrm{FO}_m^{\perp}$ implies security of all the remaining FO-like transformations

$$\mathrm{FO}^{\not\perp},\ \mathrm{FO}^{\perp},\ \mathrm{FO}_m^{\not\perp},\ \mathrm{FO}_m^{\perp},\ \mathrm{QFO}_m^{\not\perp} \text{ and } \mathrm{QFO}_m^{\perp}$$

Transformation	Underlying security	Achieved security	Requirement	Security bound($\approx$)
$\mathrm{FO}_m^{\perp}$ [DFMS22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q^{1.5} q_D \cdot \sqrt[4]{2^{-\gamma}} + q^2\sqrt{\delta}$
$\mathrm{FO}_m^{\perp}$ [HHM22]	OW-CPA	IND-CCA	γ-spread	$q \cdot \sqrt{\epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathrm{FO}_m^{\perp}$ [HHM22]	IND-CPA	IND-CCA	γ-spread	$\sqrt{q \cdot \epsilon} + q q_D \cdot \sqrt{2^{-\gamma}} + \cdots$
$\mathrm{FO}^{\not\perp}$ [KSS+20]	IND-CPA	IND-CCA	η-injective	$q^2 \cdot \epsilon + q \cdot \sqrt{\eta} + \cdots$

Does security of $\mathrm{FO}_m^{\not\perp}$ imply security of $\mathrm{FO}_m^{\perp}$?

Our results - 1

Can we give a security reduction of $\mathsf{FO}_m^{\perp}$ that avoids the quadratic security loss and has a tighter security bound (QROM)?

Theorem 1 (IND-CPA PKE $\overset{\text{QROM}}{\Rightarrow}$ IND-qCCA KEM, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[P,H,G]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-CPA adversary $\mathcal{B}$ against P such that

$$\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}) \leq q^2 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{P}}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

Our results - 2

Does security of $\mathsf{FO}_m^{\not\perp}$ imply security of $\mathsf{FO}_m^{\perp}$?

- If the underlying PKE scheme is γ-spread, then the IND-qCCA security of $\mathsf{FO}_m^{\not\perp}$ implies the IND-qCCA security of $\mathsf{FO}_m^{\perp}$ (QROM)

Core theorem

Theorem 2 (IND-CPA KEM $\overset{\text{QROM}}{\Rightarrow}$ IND-qCCA KEM, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-CPA adversary $\mathcal{B}$ against $\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]$ such that

$$\mathrm{Adv}^{\textsf{IND-qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\textsf{IND-CPA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

Question 1

Can we give a security reduction of $\mathsf{FO}_m^{\perp}$ that avoids the quadratic security loss and has a tighter security bound (QROM)?

Theorem 1 (IND-CPA PKE $\overset{\text{QROM}}{\Rightarrow}$ IND-qCCA KEM, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[P,H,G]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-CPA adversary $\mathcal{B}$ against P such that

$$\mathrm{Adv}^{\text{IND-qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{A}) \leq q^2 \cdot \mathrm{Adv}^{\text{IND-CPA}}_{\mathsf{P}}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

Question 1

Theorem 1 (IND-CPA PKE $\overset{\text{QROM}}{\Rightarrow}$ IND-qCCA KEM, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-CPA adversary $\mathcal{B}$ against P such that

$$\mathrm{Adv}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}^{\mathsf{IND\text{-}qCCA}}(\mathcal{A}) \leq q^2 \cdot \mathrm{Adv}_{\mathsf{P}}^{\mathsf{IND\text{-}CPA}}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- $\mathrm{Adv}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}^{\mathsf{IND\text{-}qCCA}}(\mathcal{A}) \leq \mathrm{Adv}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}^{\mathsf{IND\text{-}CPA}}(\mathcal{A}_1) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$ Our Theorem 2

Question 1

Theorem 1 (IND-CPA PKE $\overset{\text{QROM}}{\Rightarrow}$ IND-qCCA KEM, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-CPA adversary $\mathcal{B}$ against P such that

$$\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}) \leq q^2 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{P}}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- $\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}_1) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$ Our Theorem 2
- Semi-classical O2H [AHU19], Measure-Rewind-Measure O2H [KSS+20]

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}_1) \leq q^2 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{P}}(\mathcal{B})$$

Question 2

Does security of $\mathsf{FO}_m^{\not\perp}$ imply security of $\mathsf{FO}_m^{\perp}$?

Theorem 3 (IND-qCCA $\mathsf{FO}_m^{\not\perp} \Rightarrow$ IND-qCCA $\mathsf{FO}_m^{\perp}$, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}$[P,H,G], issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-qCCA adversary $\mathcal{B}$ against $\mathsf{FO}_m^{\not\perp}$[P,H,G] such that

$$\mathrm{Adv}^{\text{IND-qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\text{IND-qCCA}}_{\mathsf{FO}_m^{\not\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

Question 2

Theorem 3 (IND-qCCA $\mathsf{FO}_m^{\not\perp} \Rightarrow$ IND-qCCA $\mathsf{FO}_m^{\perp}$, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[P,H,G]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-qCCA adversary $\mathcal{B}$ against $\mathsf{FO}_m^{\not\perp}[P,H,G]$ such that

$$\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\not\perp}[\mathsf{P,H,G}]}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- $\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}_1) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$ Our Theorem 2
- $\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}_1) = \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}_m^{\not\perp}[\mathsf{P,H,G}]}(\mathcal{A}_2)$

Question 2

Theorem 3 (IND-qCCA $\mathrm{FO}_m^{\not\perp} \Rightarrow$ IND-qCCA $\mathrm{FO}_m^{\perp}$, informal)

If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathrm{FO}_m^{\perp}[P,H,G]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-qCCA adversary $\mathcal{B}$ against $\mathrm{FO}_m^{\not\perp}[P,H,G]$ such that

$$\mathrm{Adv}^{\text{IND-qCCA}}_{\mathrm{FO}_m^{\perp}[\mathrm{P,H,G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\text{IND-qCCA}}_{\mathrm{FO}_m^{\not\perp}[\mathrm{P,H,G}]}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- $\mathrm{Adv}^{\text{IND-qCCA}}_{\mathrm{FO}_m^{\perp}[\mathrm{P,H,G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\text{IND-CPA}}_{\mathrm{FO}_m^{\perp}[\mathrm{P,H,G}]}(\mathcal{A}_1) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$ Our Theorem 2
- $\mathrm{Adv}^{\text{IND-CPA}}_{\mathrm{FO}_m^{\perp}[\mathrm{P,H,G}]}(\mathcal{A}_1) = \mathrm{Adv}^{\text{IND-CPA}}_{\mathrm{FO}_m^{\not\perp}[\mathrm{P,H,G}]}(\mathcal{A}_2) = \mathrm{Adv}^{\text{IND-qCCA}}_{\mathrm{FO}_m^{\not\perp}[\mathrm{P,H,G}]}(\mathcal{B})$

Proof outline of Theorem 2

Theorem 2 (IND-CPA KEM $\overset{\text{QROM}}{\Longrightarrow}$ IND-qCCA KEM, informal)

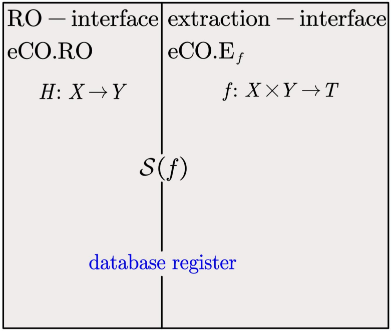
If P is δ-correct and γ-spread, for any IND-qCCA adversary $\mathcal{A}$ against $\mathsf{FO}_m^{\perp}[P,H,G]$, issuing at most q_D queries to the decapsulation oracle Deca, q queries to the random oracles, there exists an IND-CPA adversary $\mathcal{B}$ against $\mathsf{FO}_m^{\perp}[P,H,G]$ such that

$$\mathrm{Adv}^{\text{IND-qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{A}) \leq \mathrm{Adv}^{\text{IND-CPA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P,H,G}]}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- Simulate the decapsulation oracle Deca by using the extractable RO simulator [DFMS22]
- Change the simulation of Deca by a sequences of games: Game 1-Game 4
- Game 4 can be rewritten to an IND-CPA game of $\mathsf{FO}_m^{\perp}$.

The extractable RO-simulator [DFMS22]

$\mathsf{S}(f) = \{\mathsf{eCO.RO}, \mathsf{eCO.E}_f\}$: A general version of the compressed standard oracle [Zha19]



eCO.RO: compressed standard oracle

$\mathrm{eCO.E}_f : |t, D, z\rangle \mapsto |t, D, z \oplus x\rangle$

x is the smallest value that satisfies $f(x, D(x)) = t$

Game 1

$\mathcal{S}(f_1) = \{\mathsf{eCO.RO}, \mathsf{eCO.E}_{f_1}\}$

$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}$
$\mathrm{b} \leftarrow_{\$} \{0, 1\}$
$\mathrm{m}^* \leftarrow_{\$} \mathcal{M}$
$\mathrm{c}^* = \mathrm{Enc}_{\mathrm{pk}}(\mathrm{m}^*, \mathrm{H}(\mathrm{m}^*))$
$\mathrm{K}_0^* = \mathrm{G}(\mathrm{m}^*),\ \mathrm{K}_1^* \leftarrow_{\$} \mathcal{K}$

$\mathrm{b}' \leftarrow \mathcal{A}^{\mathrm{H},\mathrm{G},\mathrm{Deca}}(\mathrm{pk}, \mathrm{c}^*, \mathrm{K}_\mathrm{b}^*)$

$\mathrm{return\ boole}(\mathrm{b}' = \mathrm{b})$

H: eCO.RO

Deca: Query $\mathsf{eCO.E}_{f_1}$
Query G
Query $\mathsf{eCO.E}_{f_1}$ again

$$\left|\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}^{\perp}_{m}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{A}) - \Pr[1 \leftarrow \mathsf{Game}\ 1]\right| \leq q_D \cdot 2^{-\gamma/2}$$

Game 2

$\mathcal{S}(f_2) = \{\mathsf{eCO.RO}, \mathsf{eCO.E}_{f_2}\}$

$$
\begin{array}{|l|}
\hline
(\mathrm{pk},\mathrm{sk}) \leftarrow \mathrm{Gen} \\
\mathrm{b} \leftarrow_{\$} \{0,1\} \\
\mathrm{m}^* \leftarrow_{\$} \mathcal{M} \\
\mathrm{c}^* = \mathrm{Enc}_{\mathrm{pk}}(\mathrm{m}^*, \mathrm{H}(\mathrm{m}^*)) \\
\mathrm{K}_0^* = \mathrm{G}(\mathrm{m}^*),\ \mathrm{K}_1^* \leftarrow_{\$} \mathcal{K} \\
\hline
\end{array}
$$

$$
\begin{array}{|l|}
\hline
\mathrm{b}' \leftarrow \mathcal{A}^{\mathrm{H},\mathrm{G},\mathrm{Deca}}(\mathrm{pk}, \mathrm{c}^*, \mathrm{K}_\mathrm{b}^*) \\
\hline
\end{array}
$$

$$
\begin{array}{|l|}
\hline
\mathrm{return\ boole}(\mathrm{b}' = \mathrm{b}) \\
\hline
\end{array}
$$

H: eCO.RO

Deca: Query $\mathsf{eCO.E}_{f_2}$

Query G

Query $\mathsf{eCO.E}_{f_2}$ again

Compressed oracle O2H lemma [CMSZ19, eprint 2023/792]

$$|\Pr[1 \leftarrow \text{Game } 1] - \Pr[1 \leftarrow \text{Game } 2]| \leq q \cdot \sqrt{\delta}$$

Game 3

$$|\Pr[1 \leftarrow \text{Game } 2] - \Pr[1 \leftarrow \text{Game } 3]| \leq q_D \cdot 2^{-\gamma/2}$$

$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}$
$\mathrm{b} \leftarrow_{\$} \{0, 1\}$
$\mathrm{m}^* \leftarrow_{\$} \mathcal{M}$
$\mathrm{c}^* = \mathrm{Enc}_{\mathrm{pk}}(\mathrm{m}^*, \mathrm{O}(\mathrm{m}^*))$
$\mathrm{K}_0^* = \mathrm{G}(\mathrm{m}^*),\ \mathrm{K}_1^* \leftarrow_{\$} \mathcal{K}$

$\mathrm{b}' \leftarrow \mathcal{A}^{\mathrm{H},\mathrm{G},\mathrm{Deca}}(\mathrm{pk}, \mathrm{c}^*, \mathrm{K}_\mathrm{b}^*)$

return $\mathrm{boole}(\mathrm{b}' = \mathrm{b})$

$$\mathrm{H}:\ |\mathrm{x},\mathrm{y}\rangle|\mathrm{D}\rangle \mapsto \begin{cases} \mathrm{eCO.RO}|\mathrm{x},\mathrm{y}\rangle|\mathrm{D}\rangle & \text{if } \mathrm{x} \neq \mathrm{m}^* \\ |\mathrm{x},\mathrm{y} \oplus \mathrm{O}(\mathrm{m}^*)\rangle|\mathrm{D}\rangle & \text{if } \mathrm{x} = \mathrm{m}^* \end{cases}$$

Deca: Query $\mathsf{eCO.E}_{f_2}$
Query G
Query $\mathsf{eCO.E}_{f_2}$ again

Game 3

$$|\Pr[1 \leftarrow \text{Game } 2] - \Pr[1 \leftarrow \text{Game } 3]| \leq q_D \cdot 2^{-\gamma/2}$$

$(\mathrm{pk},\mathrm{sk}) \leftarrow \mathrm{Gen}$

$\mathrm{b} \leftarrow_{\$} \{0,1\}$

$\mathrm{m}^* \leftarrow_{\$} \mathcal{M}$

$\mathrm{c}^* = \mathrm{Enc}_{\mathrm{pk}}(\mathrm{m}^*, \mathrm{O}(\mathrm{m}^*))$

$\mathrm{K}_0^* = \mathrm{G}(\mathrm{m}^*),\ \mathrm{K}_1^* \leftarrow_{\$} \mathcal{K}$

$\mathrm{b}' \leftarrow \mathcal{A}^{\mathrm{H},\mathrm{G},\mathrm{Deca}}(\mathrm{pk}, \mathrm{c}^*, \mathrm{K}_\mathrm{b}^*)$

$\text{return boole}(\mathrm{b}' = \mathrm{b})$

$$\mathrm{H}: |\mathrm{x},\mathrm{y}\rangle|\mathrm{D}\rangle \mapsto \begin{cases} \mathrm{eCO.RO}|\mathrm{x},\mathrm{y}\rangle|\mathrm{D}\rangle & \text{if } \mathrm{x} \neq \mathrm{m}^* \\ |\mathrm{x}, \mathrm{y} \oplus \mathrm{O}(\mathrm{m}^*)\rangle|\mathrm{D}\rangle & \text{if } \mathrm{x} = \mathrm{m}^* \end{cases}$$

Deca: Query $\mathsf{eCO.E}_{f_2}$

Query G

Query $\mathsf{eCO.E}_{f_2}$ again

$$\mathsf{x} = \mathsf{m}^* \iff \mathsf{Enc}_{\mathsf{pk}}(\mathsf{x}, \mathsf{O}(\mathsf{x})) = \mathsf{c}^*$$

Game 4

$$|\mathsf{Pr}[1 \leftarrow \mathsf{Game}\ 3] = \mathsf{Pr}[1 \leftarrow \mathsf{Game}\ 4]| \leq 2\delta$$

$(\mathrm{pk},\mathrm{sk}) \leftarrow \mathrm{Gen}$
$\mathrm{b} \leftarrow_{\$} \{0,1\}$
$\mathrm{m}^* \leftarrow_{\$} \mathcal{M}$
$\mathrm{c}^* = \mathrm{Enc}_{\mathrm{pk}}(\mathrm{m}^*, \mathrm{O}(\mathrm{m}^*))$
$\mathrm{K}_0^* = \mathrm{G}(\mathrm{m}^*),\ \mathrm{K}_1^* \leftarrow_{\$} \mathcal{K}$

$\mathrm{b}' \leftarrow \mathcal{A}^{\mathrm{H,G,Deca}}(\mathrm{pk}, \mathrm{c}^*, \mathrm{K}_{\mathrm{b}}^*)$

$\mathrm{return\ boole}(\mathrm{b}' = \mathrm{b})$

$$\mathrm{H}\colon |\mathrm{x},\mathrm{y}\rangle|\mathrm{D}\rangle \mapsto \begin{cases} \mathsf{eCO.RO}|\mathrm{x},\mathrm{y}\rangle|\mathrm{D}\rangle & \text{if } \mathrm{Enc}_{\mathrm{pk}}(\mathrm{x},\mathrm{O}(\mathrm{x})) \neq \mathrm{c}^* \\ |\mathrm{x},\mathrm{y} \oplus \mathrm{O}(\mathrm{x})\rangle|\mathrm{D}\rangle & \text{if } \mathrm{Enc}_{\mathrm{pk}}(\mathrm{x},\mathrm{O}(\mathrm{x})) = \mathrm{c}^* \end{cases}$$

Deca: Query $\mathsf{eCO.E}_{f_2}$
Query G
Query $\mathsf{eCO.E}_{f_2}$ again

Rewrite Game 4 to a CPA game

$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}$
$\mathsf{b} \leftarrow_{\$} \{0,1\}$
$\mathsf{m}^* \leftarrow_{\$} \mathcal{M}$
$\mathsf{c}^* = \mathsf{Enc}_{\mathsf{pk}}(\mathsf{m}^*, \mathsf{O}(\mathsf{m}^*))$
$\mathsf{K}_0^* = \mathsf{G}(\mathsf{m}^*),\ \mathsf{K}_1^* \leftarrow_{\$} \mathcal{K}$

$\mathsf{b}' \leftarrow \mathcal{B}^{\mathsf{O},\mathsf{G}}(\mathsf{pk},\mathsf{c}^*,\mathsf{K}_\mathsf{b}^*)$

$\mathsf{return\ boole}(\mathsf{b}' = \mathsf{b})$

$\mathcal{S}(f_2) = \{\mathsf{eCO.RO}, \mathsf{eCO.E}_{f_2}\}$

$\mathsf{b}' \leftarrow \mathcal{A}^{\mathsf{H},\mathsf{G},\mathsf{Deca}}(\mathsf{pk},\mathsf{c}^*,\mathsf{K}_\mathsf{b}^*)$

$$\mathrm{H:}\ |x,y\rangle|D\rangle \mapsto \begin{cases} \mathrm{eCO.RO}|x,y\rangle|D\rangle & \text{if } \mathrm{Enc}_{\mathrm{pk}}(x,O(x)) \neq c^* \\ |x,y \oplus O(x)\rangle|D\rangle & \text{if } \mathrm{Enc}_{\mathrm{pk}}(x,O(x)) = c^* \end{cases}$$

Deca: Query $\mathsf{eCO.E}_{f_2}$
Query G
Query $\mathsf{eCO.E}_{f_2}$ again

$$\Pr[1 \leftarrow \mathsf{Game}\ 4] = \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}^{\perp}_{m}[\mathsf{P},\mathsf{O},\mathsf{G}]}(\mathcal{B}) = \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{FO}^{\perp}_{m}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{B})$$

Summary

- We give an IND-qCCA security reduction of $\mathsf{FO}_m^{\perp}$ in the QROM that avoids the quadratic security loss and has a tighter security bound

$$\mathrm{Adv}_{\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}^{\mathsf{IND\text{-}qCCA}}(\mathcal{A}) \leq q^2 \cdot \mathrm{Adv}_{\mathsf{P}}^{\mathsf{IND\text{-}CPA}}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- In the QROM, if the underlying PKE scheme is γ-spread,

IND-qCCA security of $\mathsf{FO}_m^{\not\perp}$ *implies* IND-qCCA security of $\mathsf{FO}_m^{\perp}$

Summary

- We give an IND-qCCA security reduction of $\mathsf{FO}_m^{\perp}$ in the QROM that avoids the quadratic security loss and has a tighter security bound

$$\mathrm{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{FO}_m^{\perp}[\mathsf{P},\mathsf{H},\mathsf{G}]}(\mathcal{A}) \leq q^2 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{P}}(\mathcal{B}) + q \cdot \sqrt{\delta} + q_D \cdot 2^{-\gamma/2}$$

- In the QROM, if the underlying PKE scheme is γ-spread,

IND-qCCA security of $\mathsf{FO}_m^{\not\perp}$ *implies* IND-qCCA security of $\mathsf{FO}_m^{\perp}$

Thank you for your attention! Full version: eprint 2023/862

gejiangxia@iie.ac.cn