QCCA-Secure Generic Transformations in the Quantum Random Oracle Model

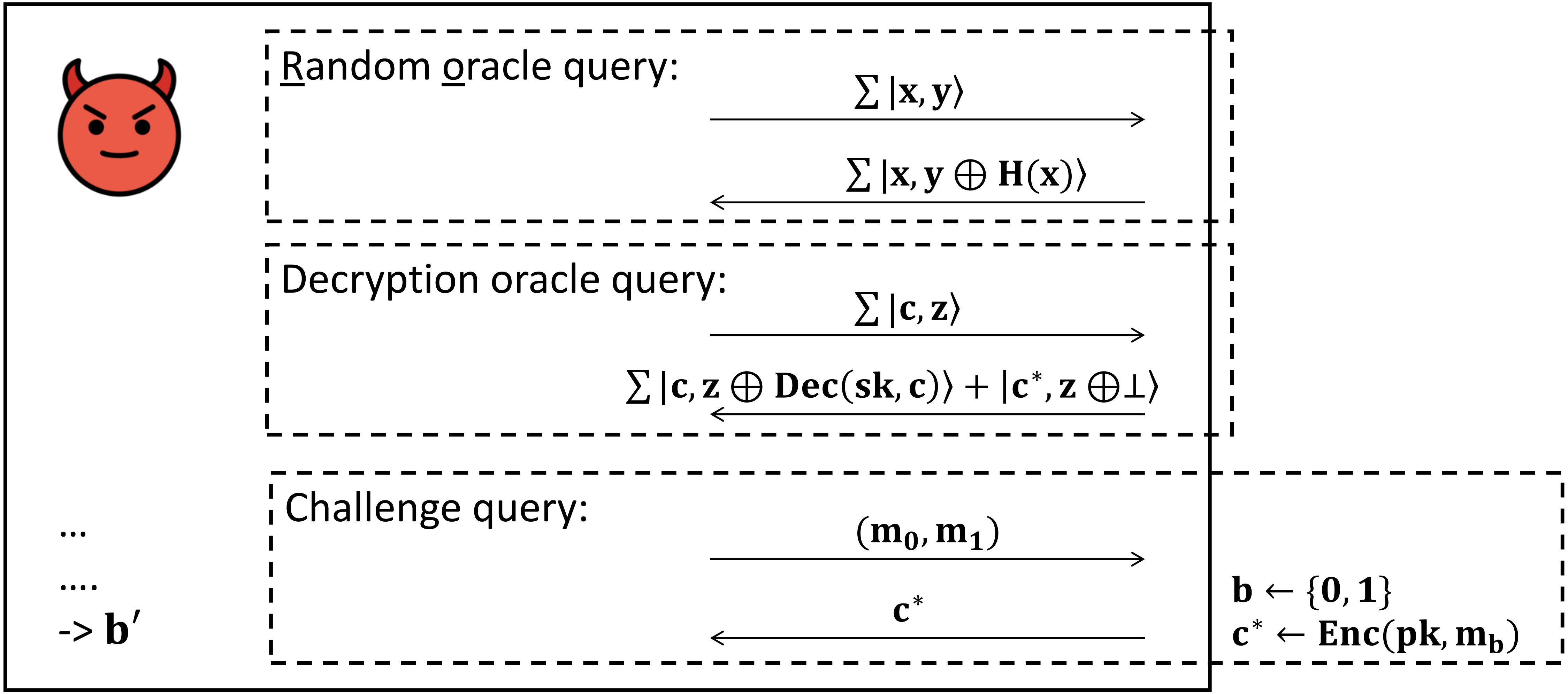
Tianshu Shan Jiangxia Ge Rui Xue

State Key Laboratory of Information Security
Institute of Information Engineering, CAS

PKC 2023

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

IND-qCCA security in the QROM



Compressed Standard Oracle[Z19]

QRO:

$\sum |x, y\rangle \rightarrow$

$H \leftarrow \Omega_H$

$|x, y\rangle \mapsto |x, y \oplus H(x)\rangle$

$\leftarrow \sum |x, y \oplus H(x)\rangle$

$=$

CStO:

$\sum |x, y\rangle \rightarrow$

1. $|x, y\rangle|D\rangle \mapsto |x, y\rangle \mathrm{StdDecomp}_x |D\rangle$
2. $|x, y\rangle|D\rangle \mapsto |x, y \oplus D(x)\rangle|D\rangle$
3. $|x, y\rangle|D\rangle \mapsto |x, y\rangle \mathrm{StdDecomp}_x |D\rangle$

$\leftarrow \sum |x, y \oplus D(x)\rangle$

Result

- **The definition of o-m schemes, including the resulting PKE of FO and REACT.**

Oracle-masked scheme

FO Transformation:

Enc(pk,m;δ)=(c,d)

d=E'(G(δ),m)

c=Enc'(pk,δ;H(δ,d))

Dec(sk,(c,d))=m

δ=Dec'(sk,c)

If c=Enc'(pk,δ;H(δ,d)),

m=D'(G(δ),d)

Otherwise,

m=⊥

δ: Randomness

E': Enc alg. of SKE

Enc': Enc alg. of PKE

H, G: Random oracle

D': Dec alg. of SKE

Dec': Dec alg. of PKE

REACT Transformation:

Enc(pk,m;(R,r))=(c_1, c_2, c_3)

c_1=Enc'(pk,R;r)

c_2=E'(G(R),m)

c_3=H(R,m,c_1, c_2)

Dec(sk,(c_1, c_2, c_3))=m

R=Dec'(sk,c_1)

m'=D'(G(R),c_2)

If c_3=H(R,m',c_1, c_2),

m=m'

Otherwise,

m=⊥

R, r: Randomness

E': Enc alg. of SKE

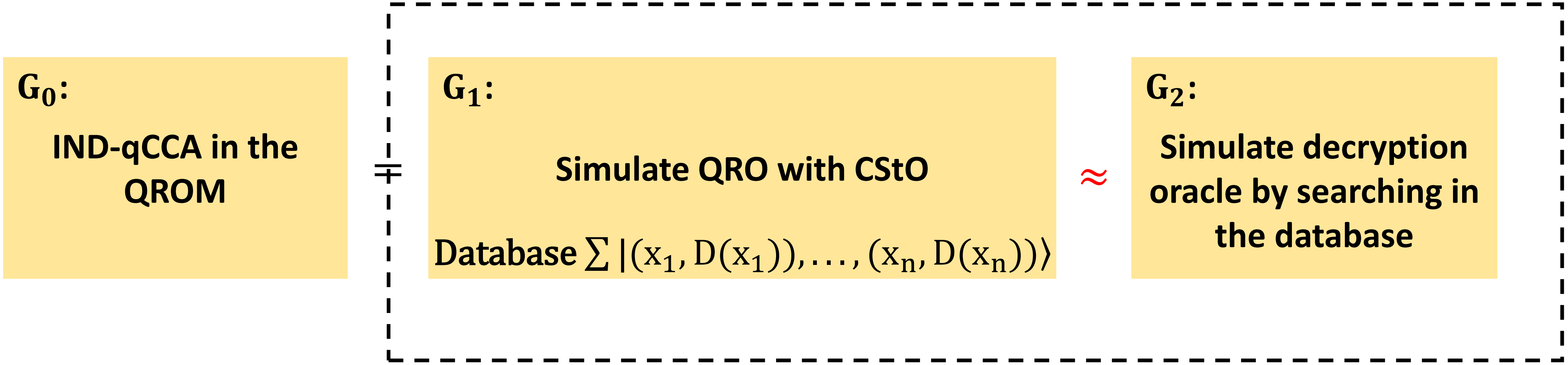
Enc': Enc alg. of PKE

H, G: Random oracle

D': Dec alg. of SKE

Dec': Dec alg. of PKE

- The definition of o-m schemes, including the resulting PKE of FO and REACT.
- An upper bound of the error caused by quantum-accessible decryption oracle simulation for o-m schemes.



- The definition of o-m schemes, including the resulting PKE of FO and REACT.
- An upper bound of the error caused by quantum-accessible decryption oracle simulation for o-m schemes.

G_0: IND-qCCA in the QROM

$=$

G_1: Simulate QRO with CStO

Database $\sum |(x_1, D(x_1)), \ldots, (x_n, D(x_n))\rangle$

$\approx$

G_2: Simulate decryption oracle by searching in the database

FO Transformation

γ-spreadness $\Longrightarrow$ $|\Pr[$ G_1: b'=b, Simulate QRO with CStO $] - \Pr[$ G_2: b'=b, Simulate decryption oracle without sk $]| \leq 5/\sqrt{2^{\gamma}}$

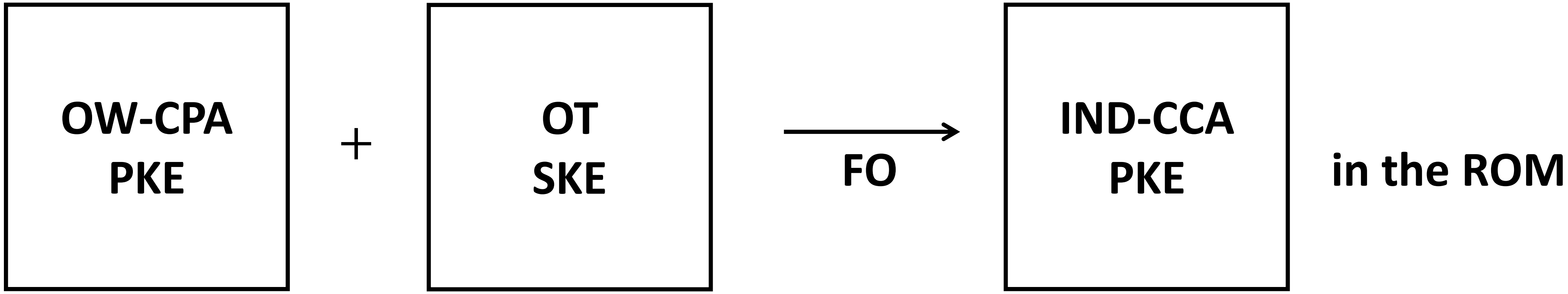
- **The definition of o-m schemes, including the resulting PKE of FO and REACT.**
- **An upper bound of the error caused by quantum-accessible decryption oracle simulation for o-m schemes.**
- **IND-qCCA security proof of FO, REACT and T_{CH} transformation, after revisiting the IND-qCCA security proof of FO by Zhandry [Z19].**

Transformation	Underlying Security	Achieved Security	Requirement
FO	OW-CPA	IND-qCCA	Well-spread
REACT	OW-qPCA	IND-qCCA	
T_{CH}	OW-qPCA	IND-qCCA	

Table. QCCA security of FO, REACT and T_{CH} transformation in the QROM.

Motivation

Classical security of FO[FO99]



Proof by games:

G_0: IND-CCA game in the ROM.

G_1: Simulate H and G on the fly.

G_2: Simulate decryption oracle without secret key.

G_3: Simulate (c^*, d^*) without $G(\delta^*)$, $H(\delta^*, d^*)$.

<u>Enc(pk,m;δ)=(c,d)</u>

d=E'(G(δ),m)

c=Enc'(pk,δ;H(δ,d))

δ: randomness

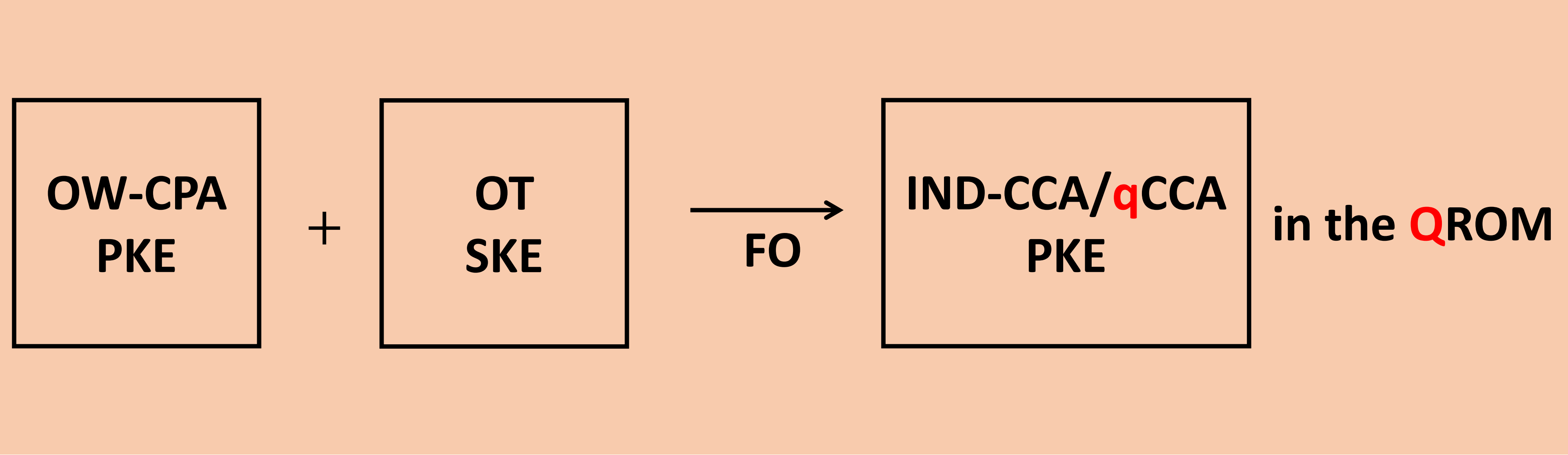
E': Enc alg. of SKE

Enc': Enc alg. of PKE

H, G: random oracle

What about the post-quantum security of FO?

Can we prove



?

Can we lift the ROM proof into the QROM proof?

- **Didn't know how to simulate quantum random oracles on the fly.**
- **Didn't know how to simulate decryption oracle without secret keys.**

We can modify FO to solve it!

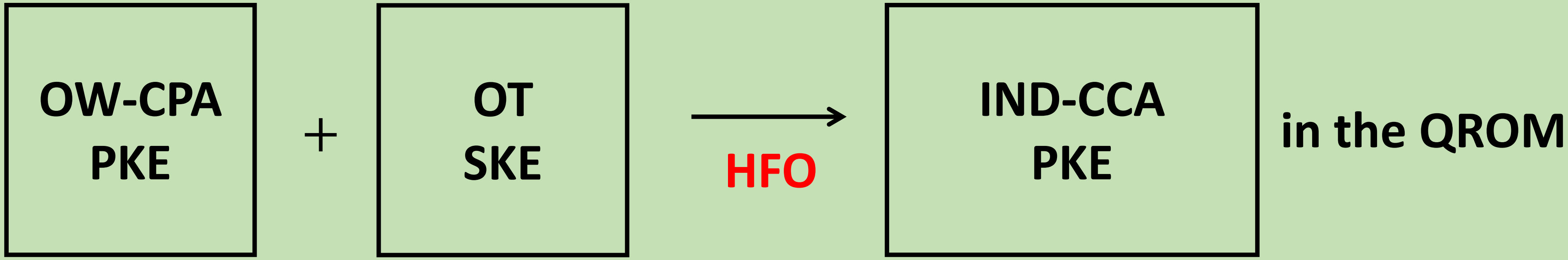
[TU16,AHU19]:

Enc(pk,m;δ)=(c,d)
d=E'(G(δ),m)
c=Enc'(pk,δ;H(δ,d))

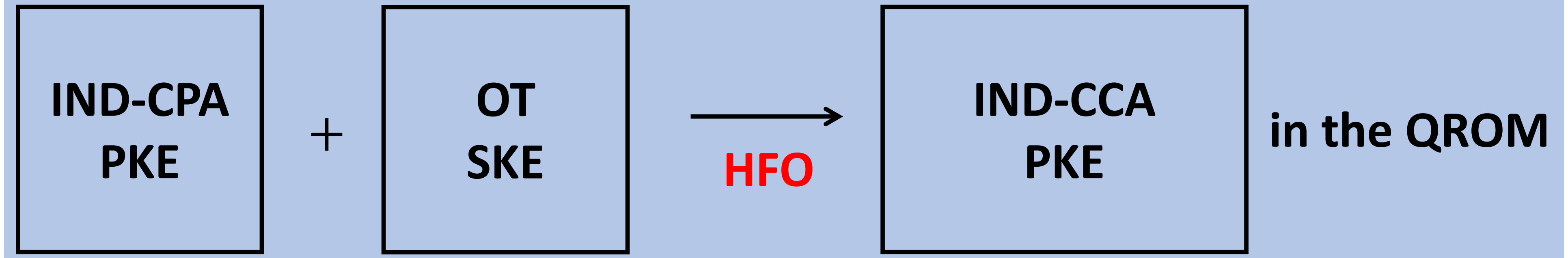
→ **HFO**

Enc(pk,m;δ)=(c,d,e)
e=H'(δ)
d=E'(G(δ),m)
c=Enc'(pk,δ;H(δ,d))

[TU16,AHU19]:



[AHU19]:



After the compressed oracle technique [Z19] being proposed...

Can we lift the ROM proof into the QROM proof?

- ~~Didn't know how to simulate quantum random oracles on the fly.~~
- ~~Didn't know how to simulate decryption oracle without secret keys.~~

Even simulate decryption oracle for quantum queries!

[Z19]:

OW-CPA PKE + **OT SKE** —FO→ **IND-qCCA PKE** **in the QROM**

But…

G_0: IND-qCCA game in the QROM.
G_1: Simulate H with compressed oracle technique.
G_2: …
G_3: …
G_4: …
G_5: … . In G_5, the secret key is not needed.

G_0: IND-CCA game in the ROM.
G_1: Simulate H and G on the fly.
G_2: Simulate decryption oracle without secret keys.

But...

G_0: IND-qCCA game in the QROM.

$\mathbf{G_1}$: Simulate H with compressed oracle technique.

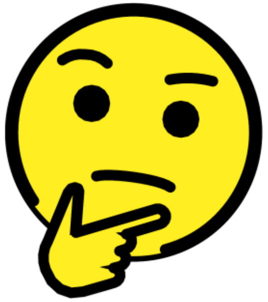
G_2: ...

G_3: ...

G_4: ...

$\mathbf{G_5}$: ... . In G_5, the secret key is not needed.

Emmm...can we give a simpler and tighter proof?



G_0: IND-CCA game in the ROM.

G_1: Simulate H and G on the fly.

G_2: Simulate decryption oracle without secret keys.

Two Points in the Proofs

Take FO as an example

Simulate decryption oracle without sk

G_0:

IND-qCCA game in the QROM

$=$

G_1:

Simulate H with CStO

well-spread

$\approx$

G_2:

Simulate decryption oracle by searching in the database:

U_{Ext}:

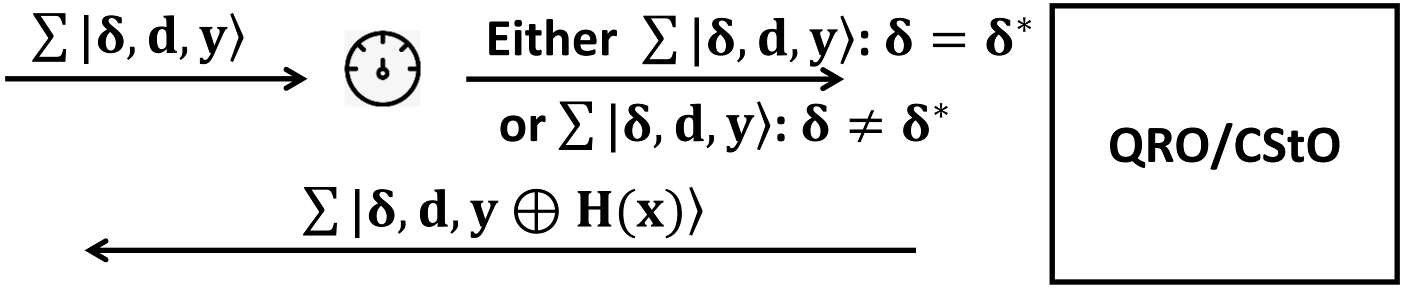
1. **If (c,d)=(c^*,d^*), output ⊥;**
2. **Else if ∄ (δ,d,D(δ,d)) s.t. Enc'(pk,δ;D(δ,d))=c, output ⊥;**
3. **Else, output D'(G(δ),d).**

Simulate (c^*, d^*) without $G(\delta^*), H(\delta^*, d^*)$

$$|\Pr[\ G_2: b'=b \quad (c^*, d^*) \quad d^* = E'(G(\delta^*), m_b) \quad c^* = Enc'(pk, \delta^*; H(\delta^*, d^*))\ ] - \Pr[\ G_3: b'=b \quad (c^*, d^*) \quad d^* = E'(k^*, m_b) \quad c^* = Enc'(pk, \delta^*; r^*)\ ]| \leq ?$$

$G(\delta^*)$, $H(\delta^*, d^*)$ are uniformly random if

- **A never queries δ^* to G;**
- **A never queries (δ^*, d^*) to H;**
- **More conditions?**



U_{Ext} disturbs the simulation of $H(\delta^*, d^*)$

G_2:

(m_0, m_1) →

← (c^*, d^*)

$\sum |c, d, z\rangle$ →

$b \leftarrow \{0,1\}, k^* \leftarrow G(\delta^*), r^* \leftarrow \text{CStO}(\delta^*, d^*)$

$d^* = E'(k^*, m_b), c^* = \text{Enc}'(pk, \delta^*; r^*)$

$\sum |c, d, z\rangle$: $c \neq c^*, d = d^*, \exists\, r$ s.t. $\text{Enc}'(pk, \delta^*; r) = c$

$$|c, d, z\rangle \otimes \text{StdDecomp}_{\delta^*, d^*} |(\delta^*, d^*, r^*)\rangle \xrightarrow{U_{\text{Ext}}} |c, d, z \oplus \bot\rangle |\psi_0\rangle + |c, d, z \oplus m_b\rangle |\psi_1\rangle$$

Patch: change the simulation of decryption oracle

After $(\mathbf{c}^*, \mathbf{d}^*)$ is defined,

$\mathbf{G_2}$:

$$\sum |\mathbf{c}, \mathbf{d}, \mathbf{z}\rangle|\mathbf{D}\rangle \xrightarrow{\mathbf{U_{Ext}}} \sum |\mathbf{c}, \mathbf{d}, \mathbf{z} \oplus \mathbf{m}\rangle|\mathbf{D}\rangle$$

$\mathbf{G_{2a}}$:

$$\sum |\mathbf{c}, \mathbf{d}, \mathbf{z}\rangle|\mathbf{D}\rangle \xrightarrow{\mathbf{StdDecomp}_{\delta^*, \mathbf{d}^*}} \xrightarrow{\mathbf{U_{Ext}}} \xrightarrow{\mathbf{StdDecomp}_{\delta^*, \mathbf{d}^*}} \sum |\mathbf{c}, \mathbf{d}, \mathbf{z} \oplus \mathbf{m}\rangle|\mathbf{D}\rangle$$

$\mathbf{G_2 \approx G_{2a}}$

$\mathbf{G_{2a}}$:

$$\sum|c,d,z\rangle|D\rangle \xrightarrow{\text{StdDecomp}_{\delta^*,d^*}} \xrightarrow{U_{Ext}} \xrightarrow{\text{StdDecomp}_{\delta^*,d^*}} \sum|c,d,z\oplus m\rangle|D\rangle$$

$$\approx \sum|c,d,z\rangle|D\rangle \xrightarrow{\text{StdDecomp}_{\delta^*,d^*}} \xrightarrow{\text{StdDecomp}_{\delta^*,d^*}} \xrightarrow{U_{Ext}} \sum|c,d,z\oplus m\rangle|D\rangle$$

$\mathbf{G_2 \approx G_{2a}}$

$\mathbf{G_{2a}}$:

$$\sum |\mathbf{c}, \mathbf{d}, \mathbf{z}\rangle|\mathbf{D}\rangle \xrightarrow{\mathbf{StdDecomp}_{\delta^*,\mathbf{d}^*}} \xrightarrow{\mathbf{U}_{\mathbf{Ext}}} \xrightarrow{\mathbf{StdDecomp}_{\delta^*,\mathbf{d}^*}} \sum |\mathbf{c}, \mathbf{d}, \mathbf{z} \oplus \mathbf{m}\rangle|\mathbf{D}\rangle$$

$$\approx \sum |\mathbf{c}, \mathbf{d}, \mathbf{z}\rangle|\mathbf{D}\rangle \xrightarrow{\mathbf{StdDecomp}_{\delta^*,\mathbf{d}^*}} \xrightarrow{\mathbf{StdDecomp}_{\delta^*,\mathbf{d}^*}} \xrightarrow{\mathbf{U}_{\mathbf{Ext}}} \sum |\mathbf{c}, \mathbf{d}, \mathbf{z} \oplus \mathbf{m}\rangle|\mathbf{D}\rangle$$

$G_2 \approx G_{2a}$

G_{2a}:

$$\sum |c,d,z\rangle|D\rangle \xrightarrow{\text{StdDecomp}_{\delta^*,d^*}} \xrightarrow{U_{\text{Ext}}} \xrightarrow{\text{StdDecomp}_{\delta^*,d^*}} \sum |c,d,z\oplus m\rangle|D\rangle$$

$$\approx \sum |c,d,z\rangle|D\rangle \xrightarrow{\cancel{\text{StdDecomp}_{\delta^*,d^*}}} \xrightarrow{\cancel{\text{StdDecomp}_{\delta^*,d^*}}} \xrightarrow{U_{\text{Ext}}} \sum |c,d,z\oplus m\rangle|D\rangle$$

G_2:

$$= \sum |c,d,z\rangle|D\rangle \xrightarrow{U_{\text{Ext}}} \sum |c,d,z\oplus m\rangle|D\rangle$$

Thank you for listening