Compact and Tightly Selective-Opening Secure Public-key Encryption Schemes

Asiacrypt 2022

Jiaxin Pan and Runzhi Zeng

December 7, 2022
(Sender) Selective Opening Security

Receiver (pk, sk)
(Sender) Selective Opening Security

Receiver \((pk, sk)\)

\[\text{ENC}_{pk}(m_1, r_1)\]

\[\text{ENC}_{pk}(m_2, r_2)\]

\[\text{ENC}_{pk}(m_3, r_3)\]

\[\vdots\]

\[\text{ENC}_{pk}(m_n, r_n)\]
(Sender) Selective Opening Security

Receiver $(pk, sk)$

$\text{ENC}_{pk}(m_1; r_1)$

$\text{ENC}_{pk}(m_2; r_2)$

$\text{ENC}_{pk}(m_3; r_3)$

$\text{ENC}_{pk}(m_n; r_n)$

$(m_1, r_1)$

$(m_2, r_2)$

$(m_3, r_3)$

$(m_n, r_n)$
(Sender) Selective Opening Security

Receiver \((pk, sk)\)

\[\text{ENC}_{pk}(m_1; r_1)\]
\[\text{ENC}_{pk}(m_2; r_2)\]
\[\text{ENC}_{pk}(m_3; r_3)\]
\[\vdots\]
\[\text{ENC}_{pk}(m_n; r_n)\]

\((m_1, r_1)\)
\((m_2, r_2)\)
\((m_3, r_3)\)
\((m_n, r_n)\)
(Sender) Selective Opening Security

Opening a ciphertext reveals $m$ and $r$
(Sender) Selective Opening Security

Opening a ciphertext reveals $m$ and $r$

Do the unopened ciphertexts remain secure?
Selective Opening Security

- Sender Selective Opening (SO) Security:
  Even if the adversary can open some of the challenge ciphertexts, the unopened challenge ciphertexts remain secure.

- Motivations:
  Sender corruptions, randomness leakage...
Selective Opening Security

- Dates back to [DNRS99]
Selective Opening Security

- Dates back to [DNRS99]
- Definitions for SO security [DNRS99, BHY09, HLOV11, BHK12...]
Selective Opening Security

- Two flavors of SO(-CCA) security notions.
  - Indistinguishability-based SO (IND-SO) Security [BHY09, BHK12]
  - Simulation-based SO (SIM-SO) Security [DNRS99, BHY09]
Selective Opening Security

- Two flavors of SO(-CCA) security notions.
  - Indistinguishability-based SO (IND-SO) Security [BHY09, BHK12]
  - Simulation-based SO (SIM-SO) Security [DNRS99, BHY09]
- SIM-SO implies (weak) IND-SO [BHK12]
SIM-SO-CCA Security

- Real game and Ideal game
  - Real game models real world scenario
  - $S$ learns trivial information in the ideal game

![Diagram of Real Game (model the real world) and Ideal Game (trivial information)]
**SIM-SO-CCA Security - Real Game**

**Real-SO-CCA Game**

\[(pk, sk) \leftarrow KG\]

Choose distribution \(D\)

Decryption queries

\[m := \text{DEC}_{sk}(c)\]
Real-SO-CCA Game

\[(pk, sk) \leftarrow KG\]
\[(m_1, ..., m_n) \leftarrow \mathcal{D}\]
\[(r_1, ..., r_n) \leftarrow \$\]
\[\forall i : c_i := \text{ENC}_{pk}(m_i, r_i)\]

Choose distribution \( \mathcal{D} \)

\[\mathcal{A}\]

\[\exists c \notin \{c_1, ..., c_n\}\]
\[m := \text{DEC}_{sk}(c)\]

Decryption queries

\[m \text{ or } \perp\]
SIM-SO-CCA Security - Real Game

Real-SO-CCA Game

\[(pk, sk) \leftarrow \text{KG}\]

\[(m_1, ..., m_n) \leftarrow \mathcal{D}\]

\[(r_1, ..., r_n) \leftarrow $\]

\[\forall i : c_i := \text{ENC}_{pk}(m_i, r_i)\]

\[\mathcal{I} := \mathcal{I} \cup \{i\}\]

\[\text{Require } c \notin \{c_1, ..., c_n\}\]

\[m := \text{DEC}_{sk}(c)\]

\[
\begin{align*}
\mathcal{A} \quad &\text{Choose distribution } \mathcal{D} \\
\mathcal{A} \quad &\text{Opening queries} \\
\mathcal{A} \quad &\text{Decryption queries}
\end{align*}
\]
(pk, sk) ← KG
(m_1, ..., m_n) ← \mathcal{D}
(r_1, ..., r_n) ← $\$
\forall i : c_i := \text{ENC}_{pk}(m_i, r_i)
\mathcal{I} := \mathcal{I} \cup \{i\}

Choose distribution \mathcal{D}

Opening queries

Decryption queries

Produce an output out_A

\mathcal{A}
SIM-SO-CCA Security - Real Game

**Real-SO-CCA Game**

\[(pk, sk) \leftarrow KG\]

\[(m_1, \ldots, m_n) \leftarrow \mathcal{D}\]

\[(r_1, \ldots, r_n) \leftarrow \$\]

\[\forall i : c_i := \text{ENC}_{pk}(m_i, r_i)\]

\[I := I \cup \{i\}\]

Choose distribution \(\mathcal{D}\)

Opening queries

Decryption queries

\[\text{Produce an output } out_A\]

\[out_{\text{real}} := (\mathcal{D}, m_1, \ldots, m_n, I, out_A)\]
**SIM-SO-CCA Security - Real Game**

**Real-SO-CCA Game**

\[(pk, sk) \leftarrow KG\]

\[(m_1, ..., m_n) \leftarrow D\]

\[(r_1, ..., r_n) \leftarrow \$\]

\[\forall i: c_i := \text{ENC}_{pk}(m_i, r_i)\]

\[\mathcal{I} := \mathcal{I} \cup \{i\}\]

Require \(c \notin \{c_1, ..., c_n\}\)

\[m := \text{DEC}_{sk}(c)\]

\[c_1, ..., c_n\]

\[\text{OPEN}(i)\]

\[\mathcal{I} := \mathcal{I} \cup \{i\}\]

\[\text{DEC}(c)\]

\[m \text{ or } \bot\]

\[\text{Produce an output } out_A\]

\[out_{real} := (D, m_1, ..., m_n, \mathcal{I}, out_A)\]
SIM-SO-CCA Security - Ideal Game

Ideal-SO-CCA Game

\[(m_1, \ldots, m_n) \leftarrow \mathcal{D}\]

\[\mathcal{D} \mid m_1, \ldots, m_n\]

\[I := I \cup \{i\}\]

\[\text{OPEN}(i) \leftarrow m_i\]

\[\text{PRODUCE an output } \text{out}_S\]

\[\text{out}_{\text{ideal}} := (\mathcal{D}, m_1, \ldots, m_n, I, \text{out}_S)\]
SIM-SO-CCA Security

- SIM-SO-CCA security: \( \forall A \), there exists a simulator \( S \) (both are PPT) such that...

\[
\text{Real-SO-CCA} \rightarrow \{\text{out}_{\text{real}}\} \approx_c \{\text{out}_{\text{ideal}}\} \rightarrow \text{Ideal-SO-CCA}
\]

- \( S \) simulates the “behavior” of \( A \) (e.g., they choose the same messages distribution, open the same ciphertexts, produce the same output...).
SIM-SO-CCA

- SIM-SO-CCA is strictly stronger than IND-CCA [BDWY11]
SIM-SO-CCA

- SIM-SO-CCA is strictly stronger than IND-CCA [BDWY11]
- Non-trivial to achieve...
SIM-SO-CCA

- SIM-SO-CCA is strictly stronger than IND-CCA [BDWY11]
- Non-trivial to achieve...
  - Hybrid argument + IND-CCA does not work

\[
\begin{array}{ccccccc}
C_1 & C_2 & \cdots & C_i & \cdots & C_n \\
\end{array}
\]
SIM-SO-CCA

- SIM-SO-CCA is strictly stronger than IND-CCA [BDWY11]
- Non-trivial to achieve...
  - Hybrid argument + IND-CCA does not work

\[ C_1 \quad C_2 \quad \cdots \quad C_i \quad \cdots \quad C_n \]
SIM-SO-CCA

- SIM-SO-CCA is strictly stronger than IND-CCA [BDWY11]
- Non-trivial to achieve...
  - Hybrid argument + IND-CCA does not work

\[
\begin{align*}
C_1 & \quad C_2 & \quad \cdots & \quad C_i & \quad \cdots & \quad C_n
\end{align*}
\]

Cannot open $c_1$...
SIM-SO-CCA

- SIM-SO-CCA is strictly stronger than IND-CCA [BDWY11]
- Non-trivial to achieve...
  - Hybrid argument + IND-CCA does not work
- “Guess” technique?
  - may work [HJKS15], but non-tight...
Tightness and Compactness

- Security reduction: \( \epsilon_A \leq L \cdot \epsilon_P \)
  - \( \epsilon_A \): Advantage of breaking SO security
  - \( \epsilon_P \): Advantage of breaking some hard problem \( P \)
  - \( L \): Security loss

- Tight security: \( L = O(1) \).

- Non-tight: \( L = O(n) \), \( L = O(\text{#RO queries}) \),...
Tightness and Compactness

- Security reduction: $\epsilon_A \leq L \cdot \epsilon_P$
  - $\epsilon_A$: Advantage of breaking SO security
  - $\epsilon_P$: Advantage of breaking some hard problem $P$
  - $L$: Security loss

- Tight security: $L = O(1)$.

- Non-tight: $L = O(n)$, $L = O(\#RO$ queries $)$,...

- Practical relevance:
  - Parameters selection...
Tightness and Compactness

Can we have SIM-SO-CCA scheme with tight security?
Tightness and Compactness

Can we have SIM-SO-CCA scheme with tight security?

Yes, but with long ciphertext or long public key...

Table: Some group-based SIM-SO PKEs with tight security

<table>
<thead>
<tr>
<th>Scheme</th>
<th>public key</th>
<th>ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>[HJR16]</td>
<td>$O(\ell^2)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td>[LLHG18]</td>
<td>$O(1)$</td>
<td>$O(\ell)$</td>
</tr>
<tr>
<td>[JL21]</td>
<td>$O(\ell^2)$</td>
<td>$O(\ell/\log \lambda)$</td>
</tr>
</tbody>
</table>

* $\lambda$: security parameter
* $\ell$: Length of message
* $|\cdot|_G$: The number of group element
Tightness and Compactness

Can we have SIM-SO-CCA scheme with tight security?

Yes, but with long ciphertext or long public key... (Not compact)

Table: Some group-based SIM-SO PKEs with tight security

<table>
<thead>
<tr>
<th>Scheme</th>
<th>public key</th>
<th>ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>[HJR16]</td>
<td>$O(\ell^2)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td>[LLHG18]</td>
<td>$O(1)$</td>
<td>$O(\ell)$</td>
</tr>
<tr>
<td>[JL21]</td>
<td>$O(\ell^2)$</td>
<td>$O(\ell / \log \lambda)$</td>
</tr>
</tbody>
</table>

* $\lambda$: security parameter
* $\ell$: Length of message
* $|\cdot|_G$: The number of group element
Tightness and Compactness

Can we have a SIM-SO-CCA scheme achieves

- Tight security
- Compact public key
- Compact ciphertext

at the same time?
Tightness and Compactness

Can we have a SIM-SO-CCA scheme achieves

- Tight security
- Compact public key
- Compact ciphertext

at the same time? Even in the random oracle model (ROM)?
Our Contributions

Compact and tightly SIM-SO-CCA secure PKE in the ROM:

- **Three direct constructions**
  - Based on strong Diffie-Hellman (stDH)
  - Based on computational Diffie-Hellman (CDH), by using TDH technique [CKS08]
  - Based on decisional Diffie-Hellman (DDH)

- **Generic construction**
  - Fujisaki-Okamoto’s transformation [FO13]
  - Based on lossy encryption [BHY09]
Our Contributions

Compact and tightly SIM-SO-CCA secure PKE in the ROM:

- Three direct constructions
  - Based on strong Diffie-Hellman (stDH)
  - Based on computational Diffie-Hellman (CDH), by using TDH technique [CKS08]
  - Based on decisional Diffie-Hellman (DDH)

- Generic construction
  - Fujisaki-Okamoto’s tranformation [FO13]
  - Based on lossy encryption [BHY09]
Our Contributions

The DHIES scheme in [HJKS15]

$$\text{pk} = g^x \in G, \text{ sk} = x \in \mathbb{Z}_p$$
Our Contributions

The DHIES scheme in [HJKS15]

- \( \text{pk} = g^x \in \mathbb{G}, \ \text{sk} = x \in \mathbb{Z}_p \)
- Encrypt a plaintext \( m \):
  1. \( r \leftarrow \mathbb{Z}_p \)
  2. \( R := g^r, Z = \text{pk}^r \)
  3. \( (K, k) = H(R, Z) \) (where \( H \) is a hash function)
Our Contributions

The DHIES scheme in [HJKS15]

\[ pk = g^x \in \mathbb{G}, \ sk = x \in \mathbb{Z}_p \]

Encrypt a plaintext \( m \):

1. \( r \leftarrow \mathbb{Z}_p \)
2. \( R := g^r, Z = pk^r \)
3. \( (K, k) = H(R, Z) \) (where \( H \) is a hash function)
4. \( d = K \oplus m \)
5. \( t = MAC_k(R, d) \)
6. Output \( (R, d, t) \)
Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:
  \[(R = g^r, \ d = K \oplus m, \ t = MAC_k(R, d))\, , \text{where} \ (K, k) = H(R, pk^r)\]

- Randomness: \(r \leftarrow \mathbb{Z}_p\)
Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:
  
  \[
  (R = g^r, \ d = K \oplus m, \ t = \text{MAC}_k(R, d)) , \text{ where } (K, k) = H(R, pk^r)
  \]

- Randomness: \( r \leftarrow \mathbb{Z}_p \)

Proof Sketch (SIM-SO-CCA security).

- Use \( n \)-stDH: Given \( (X, \{R_i\}_{i \in [n]}) \) and DDH\(_X\) oracle, find CDH\(_X(R_i)\).
Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:
  \[(R = g^r, \ d = K \oplus m, \ t = \text{MAC}_k(R, d))\], where \((K, k) = H(R, pk^r)\)

- Randomness: \(r \leftarrow \mathbb{Z}_p\)

Proof Sketch (SIM-SO-CCA security).

- Use \(n\)-stDH: Given \((X, \{R_i\}_{i \in [n]})\) and DDH\(_X\) oracle, find CDH\((X, R_i)\).

- \(n\) challenge ciphertexts: \((g^{r_1}, d_1, t_1), ..., (g^{r_n}, d_n, t_n)\).
Our Contributions

The DHIES scheme in [HJKS15]

▶ The ciphertext has this form:

\[(R = g^r, \ d = K \oplus m, \ t = \text{MAC}_k(R, d))\] , where \((K, k) = H(R, pk^r)\)

▶ Randomness: \(r \leftarrow \mathbb{Z}_p\)

Proof Sketch (SIM-SO-CCA security).

▶ Use \(n\)-stDH: Given \((X, \{R_i\}_{i \in [n]})\) and DDH\(_X\) oracle, find CDH\((X, R_i)\).

▶ \(n\) challenge ciphertexts: \((R_1, d_1, t_1), ..., (R_n, d_n, t_n)\).
Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:
  \[(R = g^r, \ d = K \oplus m, \ t = \text{MAC}_k(R, d)), \ \text{where} \ (K, k) = H(R, \pk^r)\]

- Randomness: \( r \leftarrow \mathbb{Z}_p \)

Proof Sketch (SIM-SO-CCA security).

- Use \( n \)-stDH: Given \((X, \{R_i\}_{i \in [n]})\) and DDH\(_X\) oracle, find CDH\((X, R_i)\).
- \( n \) challenge ciphertexts: \((R_1, d_1, t_1), \ldots, (R_n, d_n, t_n)\).
- Cannot open \((R_i, d_i, t_i)\), since \( r_i \)'s are unknown
Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:
  \[(R = g^r, \ d = K \oplus m, \ t = \text{MAC}_k(R, d))\], where \((K, k) = H(R, pk^r)\)

- Randomness: \(r \leftarrow \mathbb{Z}_p\)

Proof Sketch (SIM-SO-CCA security).

- Use \(n\)-stDH: Given \((X, \{R_i\}_{i \in [n]})\) and DDH\(_X\) oracle, find CDH\((X, R_i)\).
- \(n\) challenge ciphertexts: \((R_1, d_1, t_1), \ldots, (R_n, d_n, t_n)\).
- Cannot open \((R_i, d_i, t_i)\), since \(r_i\)'s are unknown
- Non-tight reduction:
  - Use “Guess” technique, \(O(n)\).
  - RO does not help for tightness...
Our Contributions

Our approach: “Dual” Naor-Yung technique

**Ciphertext**

\[
\text{DHIES: } (R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R))
\]

**Randomness**

\[
r \leftarrow \mathbb{Z}_p
\]
Our Contributions

Our approach: “Dual” Naor-Yung technique

Ciphertext

DHIES: \((R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R, d))\)

Our: \((R_0 = g^{r_0}, \ R_1 = g^{r_1}, \ d = m \oplus K, \ t = \text{MAC}_k(R_0, R_1, d))\)

Randomness

\(r \leftarrow \mathbb{Z}_p\)
Our Contributions

Our approach: “Dual” Naor-Yung technique

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Randomness</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHIES:</strong> ( R = g^r, d = m \oplus K, t = \text{MAC}_k(R, d) )</td>
<td>( r \leftarrow \mathbb{Z}_p )</td>
</tr>
<tr>
<td><strong>Our:</strong> ( R_0 = g^{r_0}, R_1 = g^{r_1}, d = m \oplus K, t = \text{MAC}_k(R_0, R_1, d) )</td>
<td></td>
</tr>
</tbody>
</table>

- \((K, k)\) is derived from \(\text{CDH}(pk, R_0)\) or \(\text{CDH}(pk, R_1)\)
Our Contributions

Our approach: “Dual” Naor-Yung technique

**Ciphertext**

DHIES: \((R = g^r, \ d = m \oplus K, \ t = MAC_k(R, d))\)

Our: \((R_0 = g^{r_0}, \ R_1 = g^{r_1}, \ d = m \oplus K, \ t = MAC_k(R_0, R_1, d))\)

\[ (K, k) = H(b, R_0, R_1, pk^r b), \] where \(b \leftarrow \{0, 1\} \)

**Randomness**

\(r \leftarrow \mathbb{Z}_p\)
Our Contributions

Our approach: “Dual” Naor-Yung technique

Ciphertext

DHIES: \((R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R, d))\)

Our: \((R_0 = g^{r_0}, \ R_1 = g^{r_1}, \ d = m \oplus K, \ t = \text{MAC}_k(R_0, R_1, d))\)

\(\triangleright\) \((K, k) = H(b, R_0, R_1, \text{pk}^r_b)\), where \(b \leftarrow \{0, 1\}\)

\(\triangleright\) Forget the dlog: Oblivious randomness

Randomness

\(r \leftarrow \mathbb{Z}_p\)
Our Contributions

Our approach: "Dual" Naor-Yung technique

**Ciphertext**

**DHIES:** \( (R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R, d)) \)

**Our:** \( (R_0 = g^{r_0}, \ R_1 = g^{r_1}, \ d = m \oplus K, \ t = \text{MAC}_k(R_0, R_1, d)) \)

- \( (K, k) = H(b, R_0, R_1, pk^{rb}), \) where \( b \leftarrow \{0, 1\} \)
- Forget the dlog: Oblivious randomness
  - \( r_{1-b} \leftarrow \mathbb{Z}_p, \ R_{1-b} := g^{r_{1-b}} \)
Our Contributions

Our approach: “Dual” Naor-Yung technique

\[
\text{Ciphertext}
\]

**DHIES:** \((R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R, d))\)

**Our:** \((R_0 = g^{r_0}, \ R_1 = g^{r_1}, \ d = m \oplus K, \ t = \text{MAC}_k(R_0, R_1, d))\)

- \((K, k) = H(b, R_0, R_1, \text{pk}^r), \text{ where } b \leftarrow \{0, 1\}\)
- Forget the dlog: Oblivious randomness
  - \(r_{1-b} \leftarrow \mathbb{Z}_p, \ R_{1-b} := g^{r_{1-b}}\)
  - Or \(R_{1-b} \leftarrow \mathbb{G}\) (if \(\mathbb{G}\) is sampleable...)

**Randomness**

\(r \leftarrow \mathbb{Z}_p\)
Our Contributions

Our approach: “Dual” Naor-Yung technique

Ciphertext

Original: \((R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R, d))\)

Our: \((R_0, R_1, \ d = m \oplus K, \ t = \text{MAC}_k(R_0, R_1, d))\)

Randomness

\(r \leftarrow \mathbb{Z}_p\)

\(b \leftarrow \{0, 1\}, \ r_b \leftarrow \mathbb{Z}_p, \ R_{1-b} \leftarrow \mathbb{G}\)

\(K, k = H(b, R_0, R_1, \text{pk}^{r_b}), \text{ where } b \leftarrow \{0, 1\} \text{ and } R_b := g^{r_b}\)

▶ Forget the dlog: Oblivious randomness

▶ Use oblivious randomness to respond OPEN queries...
Our Contributions

Our approach: “Dual” Naor-Yung technique

Ciphertext

Original: \( (R = g^r, \ d = m \oplus K, \ t = \text{MAC}_k(R, d)) \)

Our: \( (R_0, R_1, \ d = m \oplus K, \ t = \text{MAC}_k(R_0, R_1, d)) \)

Randomness

\( r \leftarrow \mathbb{Z}_p \)

\( b \leftarrow \{0, 1\}, \ r_b \leftarrow \mathbb{Z}_p \)

\( R_{1-b} \leftarrow G \)

\( (K, k) = H(b, R_0, R_1, \text{pk}^{r_b}), \) where \( b \leftarrow \{0, 1\} \) and \( R_b := g^{r_b}. \)

- Forget the dlog: Oblivious randomness
- Use oblivious randomness to respond OPEN queries...
  - E.g., if \( r_0 \) is unknown, return \( (1, r_1, R_0). \)
Our Contributions

Our approach: “Dual” Naor-Yung technique

\[(R_0, R_1, d, t = \text{MAC}_k(R_0, R_1, d))\], where \(b \leftarrow \{0, 1\}, (K, k) = H(b, R_0, R_1, \text{pk}^r_b)\)

Proof sketch

- Use \(n\)-stDH assumption...
- Embed challenge into \(R_0\) or \(R_1\)...
Our Contributions

Our approach: “Dual” Naor-Yung technique

\[(R_0, R_1, d, t = \text{MAC}_k(R_0, R_1, d)) \text{, where } b \leftarrow \{0, 1\}, (K, k) = H(b, R_0, R_1, \text{pk}^r)\]

Proof sketch

- Use \(n\)-stDH assumption...
- Embed challenge into \(R_0\) or \(R_1\)...
- Can open any challenge ciphertext \((R_0, R_1, d, t)\)
  - E.g., return \((b', r_{b'}, R_{1-b'})\) if \(r_{1-b'}\) is unknown...
Summary

Summary of our tight reduction

- Based on DHIES in [HJKS15]
- “Dual Naor-Yung” technique
  - Two valid randomness
  - Use oblivious randomness to “forget” the dlog
- Can open any challenge ciphertext (tight reduction)
- Ignore some details: Reprogramming ROs...
### Summary

**Table:** Comparison with some group-based SO-CCA PKE

| Scheme                        | Ass.  | Tight? | $|c|_G$  | $|pk|_G$ | ROM/StdM? |
|-------------------------------|-------|--------|---------|---------|-----------|
| DHIES [HJKS15]                | stDH  | ✗      | $O(1)$  | $O(1)$  | ROM       |
| FO [HJKS15]                   | CDH   | ✗      | $O(1)$  | $O(1)$  | ROM       |
| KEM+XAC [LLHG18]              | DDH   | ✓      | $O(\ell)$ | $O(1)$  | StdM      |
| ABO-LTF [JL21]                | DH    | ✓      | $O(\ell / \log \lambda)$ | $O(\ell^2)$ | StdM       |
| stDH-based scheme             | stDH  | ✓      | $O(1)$  | $O(1)$  | ROM       |
| CDH-based scheme              | CDH   | ✓      | $O(1)$  | $O(1)$  | ROM       |
| DDH-based scheme              | DDH   | ✓      | $O(1)$  | $O(1)$  | ROM       |
| FO (based on [BHY09])         | DDH   | ✓      | $O(1)$  | $O(1)$  | ROM       |
Summary

Can we have a SIM-SO-CCA scheme achieves

- Tight security
- Compact public key
- Compact ciphertext

at the same time?
Summary

Can we have a SIM-SO-CCA scheme achieves

▶ Tight security
▶ Compact public key
▶ Compact ciphertext

at the same time?

▶ YES, in the ROM.
Summary

Can we have a SIM-SO-CCA scheme achieves

- Tight security
- Compact public key
- Compact ciphertext

at the same time?

- YES, in the ROM.
- In the StdM? Still Unknown
Thank you!