Identity-Based Encryption Secure Against Chosen-Ciphertext Selective Opening Attack

Junzuo Lai, Robert H. Deng, Shengli Liu*, Jian Weng, and Yunlei Zhao

*Shanghai Jiao Tong University, Shanghai 200030, China
SOA Security

- IBE and Selective Opening Attack.
- SIM-SO-CCA Security.
- IBE with SIM-SO-CCA Security.
  - Extractable 1SPO-IBE;
  - Cross-Authentication Codes.
- Conclusion
Identity-Based Encryption

An IBE scheme consists of the following four algorithms:

**Setup**($1^k$) $\rightarrow$ (PK, MSK). PK: public parameter; MSK: master secret key.

**KeyGen**(PK, MSK, ID) $\rightarrow$ SK$_{ID}$. SK$_{ID}$ is the private key for identity ID.

**Enc**(PK, ID, M) $\rightarrow$ CT. CT: ciphertext.

**Dec**(PK, SK$_{ID}$, CT) $\rightarrow$ M/⊥.

An IBE scheme has completeness error $\epsilon$ if the correct decryption holds with probability at least $1-\epsilon$, where the probability is taken over the coins used in encryption.
Identity-Based Encryption

An IBE scheme consists of the following four algorithms:

**Setup**($1^k$) → (PK, MSK). PK: public parameter; MSK: master secret key.

**KeyGen**(PK, MSK, ID) → SK_ID. SK_ID is the private key for identity ID.

**Enc**(PK, ID, M) → CT. CT: ciphertext.

**Dec**(PK, SK_ID, CT) → M/⊥.

An IBE scheme has completeness error $\epsilon$ if the correct decryption holds with probability at least $1-\epsilon$, where the probability is taken over the coins used in encryption.
Identity-Based Encryption

An IBE scheme consists of the following four algorithms:

**Setup**$(1^κ) \rightarrow (PK, MSK)$. PK: public parameter; MSK: master secret key.

**KeyGen**(PK, MSK, ID) $\rightarrow$ SK$_{ID}$. SK$_{ID}$ is the private key for identity ID.

**Enc**(PK, ID, $M$) $\rightarrow$ $CT$. $CT$: ciphertext.

**Dec**(PK, SK$_{ID}$, $CT$) $\rightarrow$ $M$/$\bot$.

An IBE scheme has completeness error $\epsilon$ if the correct decryption holds with probability at least $1 - \epsilon$, where the probability is taken over the coins used in encryption.
Identity-Based Encryption

An IBE scheme consists of the following four algorithms:

Setup(1^k) \rightarrow (PK, MSK). PK: public parameter; MSK: master secret key.

KeyGen(PK, MSK, ID) \rightarrow SK_{ID}. SK_{ID} is the private key for identity ID.

Enc(PK, ID, M) \rightarrow CT. CT: ciphertext.

Dec(PK, SK_{ID}, CT) \rightarrow M/ \bot.

An IBE scheme has completeness error \( \epsilon \) if the correct decryption holds with probability at least \( 1 - \epsilon \), where the probability is taken over the coins used in encryption.
Selective Opening Attack: a vector of ciphertexts, adaptive corruptions exposing not only some message but also the random coins.
Selective Opening Attack: a vector of ciphertexts, adaptive corruptions exposing not only some message but also the random coins.
SIM-SO-CPA(CCA2) Security:

**SIM-SOA security** requires that anything that can be computed by a PPT adversary from all the ciphertexts and the opened messages together with the corresponding randomness can also be computed by a PPT simulator with only the opened messages.
Related works

- Bellare, Hofheinz and Yilek formalize the security model of SOA, including IND-SOA, SIM-SOA.
  - SIM-SOA security is stronger than IND-SOA security.
- How to construct IBE with SIM-SO-CCA2 Security remains open.
Related works

- Bellare, Hofheinz and Yilek formalize the security model of SOA, including IND-SOA, SIM-SOA.
- SIM-SOA security is stronger than IND-SOA security.
- How to construct IBE with SIM-SO-CCA2 Security remains open.
Related works

- Bellare, Hofheinz and Yilek formalize the security model of SOA, including IND-SOA, SIM-SOA.
- SIM-SOA security is stronger than IND-SOA security.
- How to construct IBE with SIM-SO-CCA2 Security remains open.
Related works

- Bellare, Hofheinz and Yilek formalize the security model of SOA, including IND-SOA, SIM-SOA.
- SIM-SOA security is stronger than IND-SOA security.
- How to construct IBE with SIM-SO-CCA2 Security remains open.
Related works

- Bellare, Hofheinz and Yilek formalize the security model of SOA, including IND-SOA, SIM-SOA.
- SIM-SOA security is stronger than IND-SOA security.
- How to construct IBE with SIM-SO-CCA2 Security remains open.
SIM-SO-CCA2 Security: $\text{Exp}_{\mathcal{A},\mathcal{M},\mathcal{R}}^{\text{cca-so-real}}(1^\kappa)$

**Challenger**

$(PK, MSK) \leftarrow \text{Setup}(1^\kappa)$

$\alpha, \overrightarrow{ID} \leftarrow \mathcal{A}_1^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(PK)$

$\overrightarrow{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)$

$\overrightarrow{R} = (R^{(1)}, \ldots, R^{(n)}) \leftarrow \mathcal{R}$

$\overrightarrow{CT} = \text{Enc}(PK, \overrightarrow{ID}, \overrightarrow{M}; \overrightarrow{R})$

$I \leftarrow \mathcal{A}_2^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(\overrightarrow{CT})$

$(M^{(i)}, R^{(i)})_{i \in I} \leftarrow \mathcal{A}_3^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(\overrightarrow{M}, \overrightarrow{R})$

$\overrightarrow{M}, I, \text{out}_A \leftarrow R(\overrightarrow{ID}, \overrightarrow{M}, I, \text{out}_A)$
**SIM-SO-CCA2 Security: Exp\(_{\mathcal{A}, \mathcal{M}, R}(1^\kappa)\)**

**Challenger**

\[(PK, \text{MSK}) \leftarrow \text{Setup}(1^\kappa) \quad \xrightarrow{PK} \quad \mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)\]

\[\begin{align*}
\vec{M} &= (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha) \\
\vec{R} &= (R^{(1)}, \ldots, R^{(n)}) \leftarrow \mathcal{R} \\
\vec{CT} &= \text{Enc}(PK, \vec{ID}, \vec{M}; \vec{R}) \\
& \xrightarrow{\vec{CT}} \\
& \overset{I}{\leftarrow} \mathcal{A}_2 \\
& \overset{(M^{(i)}, R^{(i)})_{i \in I}}{\leftarrow} \\
& \overset{\text{out}_A}{\leftarrow} \mathcal{A}_3 \overset{\text{KeyGen}(\cdot), \text{Dec}(\cdot)}{\leftarrow} ((M^{(i)}, R^{(i)})_{i \in I}, \text{out}_A) \end{align*}\]
SIM-SO-CCA2 Security: \( \text{Exp}_{\mathcal{A}, \mathcal{M}, \mathcal{R}}^{\text{cca-so-real}}(1^\kappa) \)

**Challenger**

\[
\begin{align*}
\text{(PK, MSK)} &\leftarrow \text{Setup}(1^\kappa) \\
\text{(PK)} &\rightarrow \text{PK} \\
(\alpha, \overrightarrow{ID}) &\leftarrow \mathcal{A}_1^{\text{KeyGen}(\cdot), \text{Dec}(\cdot)}(\text{PK}) \\
\overrightarrow{M} = (M^{(1)}, \ldots, M^{(n)}) &\leftarrow \mathcal{M}(\alpha) \\
\overrightarrow{R} = (R^{(1)}, \ldots, R^{(n)}) &\leftarrow \mathcal{R} \\
\overrightarrow{CT} = \text{Enc}(\text{PK}, \overrightarrow{ID}, \overrightarrow{M}; \overrightarrow{R}) &\rightarrow \overrightarrow{CT} \\
I &\leftarrow \mathcal{A}_2^{\text{KeyGen}(\cdot), \text{Dec}(\cdot)}(\overrightarrow{CT}) \\
(M^{(i)}, R^{(i)})_{i \in I} &\leftarrow (I) \\
\text{out}_A &\leftarrow \mathcal{A}_3^{\text{KeyGen}(\cdot), \text{Dec}(\cdot)}((M^{(i)}, R^{(i)})_{i \in I}) \\
R(\overrightarrow{ID}, \overrightarrow{M}, I, \text{out}_A) &\leftarrow \mathcal{A}_3^{\text{KeyGen}(\cdot), \text{Dec}(\cdot)}((M^{(i)}, R^{(i)})_{i \in I}) 
\end{align*}
\]
SIM-SO-CCA2 Security: $\text{Exp}_{\mathcal{A}, \mathcal{M}, R}^{\text{cca-so-ideal}}(1^k)$

Challenger

\[
\hat{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)
\]

\[
I \nsubseteq [n] \leftarrow S_2(1^{|M(i)|})
\]

\[
(M^{(i)})_{i \in I} \rightarrow \text{Out}_S \leftarrow S_3 \left( (M^{(i)})_{i \in I} \right)
\]

\[
R(\overrightarrow{ID}, \hat{M}, I, \text{out}_S)
\]

SIM-SO-CCA2 Security: \( \forall \) PPT \( \mathcal{A} \), \( \forall \) PPT \( \mathcal{R} \), \( \forall \) PPT \( \mathcal{M} \), \( \exists S \) such that

\[
\left| \Pr \left[ R(\overrightarrow{ID}, \hat{M}, I, \text{out}_A) = 1 \right] - \Pr \left[ R(\overrightarrow{ID}, \hat{M}, I, \text{out}_S) = 1 \right] \right| \text{ is negligible.}
\]
SIM-SO-CCA2 Security: \( \text{Exp}^{\text{cca-so-ideal}}_{\mathcal{A}, \mathcal{M}, R}(1^k) \)

**Challenger**

\[
\begin{align*}
S &= (S_1, S_2, S_3) \\
\vec{M} &= (M^{(1)}, \ldots, M^{(n)}) \leftarrow M(\alpha) \\
I &\subseteq [n] \\
(M^{(i)})_{i \in I} &\rightarrow \text{Out}_S \leftarrow S_3 ((M^{(i)})_{i \in I}) \\
R(\vec{ID}, \vec{M}, I, \text{out}_S)
\end{align*}
\]

**SIM-SO-CCA2 Security:** \( \forall \) PPT \( \mathcal{A} \), \( \forall \) PPT \( R \), \( \forall \) PPT \( \mathcal{M} \), \( \exists \) \( S \) such that

\[
\left| \Pr \left[ R(\vec{ID}, \vec{M}, I, \text{out}_A) = 1 \right] - \Pr \left[ R(\vec{ID}, \vec{M}, I, \text{out}_S) = 1 \right] \right| \quad \text{is negligible.}
\]
How to get SIM-SO-CCA2 Security: the idea

Challenger

\[
\vec{M} = (M^{(1)}, \ldots, M^{(n)})
\]

\[
\vec{M} = (M^{(1)}, \ldots, M^{(n)})
\]

\[
S = (S_1, S_2, S_3)
\]

\[
S = (S_1, S_2, S_3)
\]

\[
(\alpha, \vec{ID}) \leftarrow S_1(1^\kappa)
\]

\[
(\alpha, \vec{ID}) \leftarrow S_1(1^\kappa)
\]

\[
I \leftarrow S_2(1^{|M^{(i)}|})
\]

\[
I \leftarrow S_2(1^{|M^{(i)}|})
\]

\[
(M^{(i)})_{i \in I} \rightarrow \text{Out}_S \leftarrow S_3\left((M^{(i)})_{i \in I}\right)
\]

\[
(M^{(i)})_{i \in I} \rightarrow \text{Out}_S \leftarrow S_3\left((M^{(i)})_{i \in I}\right)
\]

Aim: \(\left(\vec{ID}, \vec{M}, I, out_A\right) \approx_c \left(\vec{ID}, \vec{M}, I, out_S\right)\)
How to get SIM-SO-CCA2 Security: the idea

Challenger

\[ S = (S_1, S_2, S_3) \]

\[ \alpha, \overrightarrow{ID} \leftarrow S_1(1^\kappa) \]

\[ (\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_{1^{\text{KeyGen,Dec}(\cdot)}(PK)} \]

\[ \vec{M} \leftarrow M(\alpha) \]

\[ \vec{M} = (M^{(1)}, \ldots, M^{(n)}) \]

\[ I \leftarrow S_2(1^{|M^{(i)}|}) \]

\[ \frac{(M^{(i)})_{i \in I}}{\text{Out}_S} \leftarrow S_3 \left( \left( M^{(i)} \right)_{i \in I} \right) \]

Aim: \( \left( \overrightarrow{ID}, \vec{M}, I, \text{out}_A \right) \approx_c \left( \overrightarrow{ID}, \vec{M}, I, \text{out}_S \right) \)
How to get SIM-SO-CCA2 Security: the idea

**Challenger**

\[ \vec{M} = (M^{(1)}, \ldots, M^{(n)}) \]

\[ \vec{M} = M(\alpha) \]

\[ \vec{I} = S_2(1^{\mid M^{(i)} \mid}) \]

\[ \{ I \leftarrow \mathcal{A}_2^{\text{KeyGen}(\cdot), \text{Dec}(\cdot)}(\vec{CT}) \} \]

\[ \text{Out}_S \leftarrow S_3 \left( \left( M^{(i)} \right)_{i \in I} \right) \]

**Aim:**

\[ \left( \vec{ID}, \vec{M}, I, \text{out}_A \right) \approx_c \left( \vec{ID}, \vec{M}, I, \text{out}_S \right) \]
How to get SIM-SO-CCA2 Security: the idea

<table>
<thead>
<tr>
<th>Challenger</th>
<th>S = (S₁, S₂, S₃)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>(α, ID)</td>
<td>(α, ID) ← S₁(1^k)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>M ← M(α)</td>
<td></td>
</tr>
<tr>
<td>M = (M⁽¹⁾, ..., M⁽ⁿ⁾)</td>
<td>I ← S₂(1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>I ← S₂(M⁽ⁱ⁾)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Outₜ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Aim: ID, M, I, outₜ ≈ₜ ID, M, I, outₜ</td>
<td></td>
</tr>
</tbody>
</table>
SIM-SO-CPA Security for single bit messages

- IBE1 encrypts **single** bits.
- IBE1 is **IND-ID-CPA** secure.
- IBE1 is **One-Sided Publicly Openable (1SPO)**.

IBE1 is **SIM-SO-CPA Secure**.

**Definition 1 (1SPO-IBE1)**

Let \( C = \text{Enc}_1(\text{PK}, \text{ID}, 0; R) \). Let

\[
\text{Coins}(\text{PK}, \text{ID}, C, 0) := \{ R' \mid C = \text{IBE1.Enc}(\text{PK}, \text{ID}, 0; R') \}.
\]

An IBE1 scheme is **One-Sided Publicly Openable** if \( R' \leftarrow \text{POpen}(\text{PK}, \text{ID}, C) \) outputs a random \( R' \) in \( \text{Coins}(\text{PK}, \text{ID}, C, 0) \).
SIM-SO-CPA Security for single bit messages

- IBE1 encrypts **single** bits.
- IBE1 is **IND-ID-CPA** secure.
- IBE1 is **One-Sided Publicly Openable** (1SPO).

IBE1 is **SIM-SO-CPA Secure**.

**Definition 1 (1SPO-IBE1)**

Let \( C = \text{Enc}_1(PK, ID, 0; R) \). Let

\[
\text{Coins}(PK, ID, C, 0) := \{ R' | C = \text{IBE1.Enc}(PK, ID, 0; R') \}.
\]

An IBE1 scheme is **One-Sided Publicly Openable** if \( R' \leftarrow \text{POpen}(PK, ID, C) \) outputs a random \( R' \) in \( \text{Coins}(PK, ID, C, 0) \).
SIM-SO-CPA Security for single bit messages

\[ C[0] = \begin{cases} C[0] & \text{opened with the original randomness} \\ C[0] & \text{opened with } \text{POpen} \end{cases} \]

\[ C[1] = \begin{cases} C[1] & \text{opened with the original randomness} \\ C[0] & \text{opened with } \text{POpen} \end{cases} \]
SIM-SO-CPA Security for multi-bit messages


IBE=(Setup, KeyGen, Enc, Dec) encrypting multi-bits.

IBE.Setup=IBE1.Setup; IBE.KeyGen=IBE1.KeyGen;

IBE.Enc:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>⋮</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>$C_2$</td>
<td>$\cdots$</td>
<td>$C_\ell$</td>
</tr>
<tr>
<td>↑</td>
<td>↑</td>
<td>⋮</td>
<td>↑</td>
</tr>
<tr>
<td>IBE1.Enc</td>
<td>IBE1.Enc</td>
<td>$\cdots$</td>
<td>IBE1.Enc</td>
</tr>
<tr>
<td>↑</td>
<td>↑</td>
<td>⋮</td>
<td>↑</td>
</tr>
<tr>
<td>$m_1(0/1)$</td>
<td>$m_2(0/1)$</td>
<td>$\cdots$</td>
<td>$m_\ell(0/1)$</td>
</tr>
</tbody>
</table>

$CT = (C_1, C_2, \ldots, C_\ell)$

SIM-SO-CPA Security for multi-bit messages


<table>
<thead>
<tr>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$\ldots$</th>
<th>$C_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>↓</td>
<td>↓</td>
<td>$\ldots$</td>
<td>↓</td>
</tr>
<tr>
<td>IBE1.Dec</td>
<td>IBE1.Dec</td>
<td>$\ldots$</td>
<td>IBE1.Dec</td>
</tr>
<tr>
<td>↓</td>
<td>↓</td>
<td>$\ldots$</td>
<td>↓</td>
</tr>
<tr>
<td>$m_1$</td>
<td>$m_2$</td>
<td>$\ldots$</td>
<td>$m_\ell$</td>
</tr>
</tbody>
</table>

SIM-SO-CCA2 Security for multi-bit messages

- 2-level IND-ID-CPA $\xrightarrow{\text{CHK Transform}}$ IND-ID-CCA2.

- SIM-SO-CPA $\xrightarrow{\text{CHK Transform}}$ SIM-SO-CCA2

The signing key of OTS might be disclosed in the opening!

Bit-wise Encryption from 1-bit IND-ID-CCA secure 1SPO-IBE?

<table>
<thead>
<tr>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$\ldots$</th>
<th>$C_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>↑</td>
<td>↑</td>
<td>$\ldots$</td>
<td>↑</td>
</tr>
<tr>
<td>IBE1.Enc</td>
<td>IBE1.Enc</td>
<td>$\ldots$</td>
<td>IBE1.Enc</td>
</tr>
<tr>
<td>$m_1(0/1)$</td>
<td>$m_2(0/1)$</td>
<td>$\ldots$</td>
<td>$m_\ell(0/1)$</td>
</tr>
</tbody>
</table>

IBE is NOT CCA2 secure even if IBE1 is!

Junzuo Lai, Robert H. Deng, Shengli Liu*, Jian Weng, and Yunlei Zhao (SJTU-CIS)
SIM-SO-CCA2 Security for multi-bit messages

- SIM-SO-CPA ⇔ CHK Transform ⇔ SIM-SO-CCA2

The signing key of OTS might be disclosed in the opening!

Bit-wise Encryption from 1-bit IND-ID-CCA secure 1SPO-IBE?

<table>
<thead>
<tr>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$C_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>↑</td>
<td>↑</td>
<td>↑</td>
</tr>
<tr>
<td>IBE1.Enc</td>
<td>IBE1.Enc</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>↑</td>
<td>↑</td>
<td>$\ldots$</td>
</tr>
</tbody>
</table>

IBE is NOT CCA2 secure even if IBE1 is!
SIM-SO-CCA2 Security for multi-bit messages

- 2-level IND-ID-CPA $\xrightarrow{\text{CHK Transform}}$ IND-ID-CCA2.
- SIM-SO-CPA $\xleftrightarrow{\text{CHK Transform}}$ SIM-SO-CCA2

The signing key of OTS might be disclosed in the opening!

Bit-wise Encryption from 1-bit IND-ID-CCA secure 1SPO-IBE?

<table>
<thead>
<tr>
<th>$C_1$</th>
<th>$C_2$</th>
<th>...</th>
<th>$C_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>...</td>
<td>$\uparrow$</td>
</tr>
<tr>
<td>IBE1.Enc</td>
<td>IBE1.Enc</td>
<td>...</td>
<td>IBE1.Enc</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>...</td>
<td>$\uparrow$</td>
</tr>
</tbody>
</table>

$m_1(0/1)$ | $m_2(0/1)$ | ... | $m_\ell(0/1)$

IBE is NOT CCA2 secure even if IBE1 is!
SIM-SO-CCA2 Security for multi-bit messages

- 2-level IND-ID-CPA $\xRightarrow{\text{CHK Transform}}$ IND-ID-CCA2.
- SIM-SO-CPA $\not\Rightarrow\xRightarrow{\text{CHK Transform}}$ SIM-SO-CCA2

The signing key of OTS might be disclosed in the opening!

Bit-wise Encryption from 1-bit IND-ID-CCA secure 1SPO-IBE?

<table>
<thead>
<tr>
<th>$C_1$</th>
<th>$C_2$</th>
<th>...</th>
<th>$C_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>...</td>
<td>$\uparrow$</td>
</tr>
</tbody>
</table>

IBE.Enc: IBE1.Enc IBE1.Enc ... IBE1.Enc

| $m_1(0/1)$ | $m_2(0/1)$ | ... | $m_\ell(0/1)$ |

IBE is NOT CCA2 secure even if IBE1 is!
SIM-SO-CCA2: Our approach

**IBE.Enc:** $CT = (C_1, C_2, \ldots, C_\ell, T)$,

$$T = XAuth(K_1, \ldots, K_\ell).$$

<table>
<thead>
<tr>
<th>$C_1, K_1$</th>
<th>$C_2, K_2$</th>
<th>$\ldots$</th>
<th>$C_\ell, K_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>$\ldots$</td>
<td>$\uparrow$</td>
</tr>
<tr>
<td>IBE$_{ex}$.Enc</td>
<td>IBE$_{ex}$.Enc</td>
<td>$\ldots$</td>
<td>IBE$_{ex}$.Enc</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>$\ldots$</td>
<td>$\uparrow$</td>
</tr>
<tr>
<td>$m_1(0/1)$</td>
<td>$m_2(0/1)$</td>
<td>$\ldots$</td>
<td>$m_\ell(0/1)$</td>
</tr>
</tbody>
</table>

New Primitives: IBE$_{ex}$ and X-Authentication Code.

Junzuo Lai, Robert H. Deng, Shengli Liu*, Jialing Identity-Based Encryption Secure Against Chosen-Ciphertext Attack
IBE.Enc: $CT = (C_1, C_2, \ldots, C_\ell, T)$,

$T = \text{XAuth}(K_1, \ldots, K_\ell)$.

<table>
<thead>
<tr>
<th>$C_1, K_1$</th>
<th>$C_2, K_2$</th>
<th>$\ldots$</th>
<th>$C_\ell, K_\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>$\ldots$</td>
<td>$\uparrow$</td>
</tr>
<tr>
<td>$\text{IBE}_{ex}.\text{Enc}$</td>
<td>$\text{IBE}_{ex}.\text{Enc}$</td>
<td>$\ldots$</td>
<td>$\text{IBE}_{ex}.\text{Enc}$</td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$\uparrow$</td>
<td>$\ldots$</td>
<td>$\uparrow$</td>
</tr>
<tr>
<td>$m_1(0/1)$</td>
<td>$m_2(0/1)$</td>
<td>$\ldots$</td>
<td>$m_\ell(0/1)$</td>
</tr>
</tbody>
</table>

New Primitives: $\text{IBE}_{ex}$ and X-Authentication Code.
Extractable 1SPO-IBE

Extractable 1SPO-IBE: $\text{IBE}_{ex} = (\text{Setup}_{ex}, \text{KeyGen}_{ex}, \text{Enc}_{ex}, \text{Dec}_{ex})$

- $\text{IBE}_{ex}$ encrypts a single bit.
- $\text{IBE}_{ex}$ is One-Sided Publicly Openable.
- $\text{IBE}_{ex}$ also encapsulates a key, when encrypting “1”.
- $\text{IBE}_{ex}$ is IND-ID-CCA2 secure, i.e, for random $K'$,

$$\text{Enc}_{ex}(\text{PK}_{ex}, \text{ID}, 1; R) \overset{c}{\approx} (\text{Enc}_{ex}(\text{PK}_{ex}, \text{ID}, 0; R'), K')$$

$$(C, K) \overset{c}{\approx} (C', K')$$
Extractable 1SPO-IBE

**IBE_{ex}** encrypts a single bit.

**IBE_{ex}** is **One-Sided Publicly Openable**.

**IBE_{ex}** also encapsulates a key, when encrypting “1”.

**IBE_{ex}** is **IND-ID-CCA2** secure, i.e., for random \( K' \),

\[
Enc_{ex}(PK_{ex}, ID, 1; R) \overset{c}{\approx} (Enc_{ex}(PK_{ex}, ID, 0; R'), K')
\]

\[
(C, K) \overset{c}{\approx} (C', K')
\]
Extractable 1SPO-IBE

Extractable 1SPO-IBE: \( \text{IBE}_{\text{ex}} = (\text{Setup}_{\text{ex}}, \text{KeyGen}_{\text{ex}}, \text{Enc}_{\text{ex}}, \text{Dec}_{\text{ex}}) \)

- \( \text{IBE}_{\text{ex}} \) encrypts a single bit.
- \( \text{IBE}_{\text{ex}} \) is One-Sided Publicly Openable.
- \( \text{IBE}_{\text{ex}} \) also encapsulates a key, when encrypting “1”.
- \( \text{IBE}_{\text{ex}} \) is IND-ID-CCA2 secure, i.e., for random \( K' \),

\[
\text{Enc}_{\text{ex}}(\text{PK}_{\text{ex}}, \text{ID}, 1; R) \overset{c}{\approx} (\text{Enc}_{\text{ex}}(\text{PK}_{\text{ex}}, \text{ID}, 0; R'), K')
\]

\[
(C, K) \overset{c}{\approx} (C', K')
\]
Extractable 1SPO-IBE

Extractable 1SPO-IBE: $\text{IBE}_{ex} = (\text{Setup}_{ex}, \text{KeyGen}_{ex}, \text{Enc}_{ex}, \text{Dec}_{ex})$

- $\text{IBE}_{ex}$ encrypts a single bit.
- $\text{IBE}_{ex}$ is One-Sided Publicly Openable.
- $\text{IBE}_{ex}$ also encapsulates a key, when encrypting “1”.
- $\text{IBE}_{ex}$ is IND-ID-CCA2 secure, i.e., for random $K'$,

$$\text{Enc}_{ex}(\text{PK}_{ex}, \text{ID}, 1; R) \overset{c}{\approx} (\text{Enc}_{ex}(\text{PK}_{ex}, \text{ID}, 0; R'), K')$$

$$(C, K) \overset{c}{\approx} (C', K')$$
\(\ell\)-Cross-authentication code


\(\ell\)-Cross-authentication code: \(\ell\text{-XAC} = (\text{XAuth, XVer})\)

\[ T \leftarrow \text{XAuth}(K_1, \ldots, K_\ell); \]
\[ 1/0 \leftarrow \text{XVer}(K, T); \]

Correctness.

\[ \text{fail}_{\text{XAC}}(\kappa) := \text{Pr}[\text{XVer}(K_i, \text{XAuth}(K_1, \ldots, K_\ell)) \neq 1], \]

is negligible, where \(K_1, \ldots, K_\ell \leftarrow \mathcal{K}\) in the probability.
\[ \ell \]-Cross-authentication code


\[ \ell \]-Cross-authentication code: $\ell$-XAC=$(XAuth, XVer)$

- $T \leftarrow XAuth(K_1, \ldots, K_\ell)$;
- $1/0 \leftarrow XVer(K, T)$;

Correctness.

$\text{fail}_{XAC}(\kappa) := \Pr[XVer(K_i, XAuth(K_1, \ldots, K_\ell)) \neq 1]$, is negligible, where $K_1, \ldots, K_\ell \leftarrow \mathcal{K}$ in the probability.
\(\ell\)-Cross-authentication code


\(\ell\)-Cross-authentication code: \(\ell\)-XAC=(XAuth, XVer)

- \(T \leftarrow \text{XAuth}(K_1, \ldots, K_\ell)\);
- \(1/0 \leftarrow \text{XVer}(K, T)\);

**Correctness.**

\[
\text{fail}_{\text{XAC}}(\kappa) := \Pr[\text{XVer}(K_i, \text{XAuth}(K_1, \ldots, K_\ell)) \neq 1],
\]

is negligible, where \(K_1, \ldots, K_\ell \leftarrow \mathcal{K}\) in the probability.
Security of $\ell$-Cross-authentication code

Security against impersonation and substitution attacks.

$\text{Adv}^{\text{imp}}_{\text{XAC}}(\kappa) := \max_{T'} \Pr[\text{XVer}(K, T') = 1 | K \leftarrow \mathcal{K}]$

where the max is over all $T' \in \mathcal{X}T$, and

$\text{Adv}^{\text{sub}}_{\text{XAC}}(\kappa) := \max_{i, K \neq i, F} \Pr[\text{XVer}(K_i, T') = 1 \mid T' \neq T \land T := \text{XAuth}(K_1, \ldots, K_\ell), T' \leftarrow F(T)]$

where the max is over all $i \in [\ell]$, all $K \neq i = (K_j)_{j \neq i} \in \mathcal{K}^{\ell-1}$ and all (possibly randomized) functions $F : \mathcal{T} \rightarrow \mathcal{T}$.
Security of $\ell$-Cross-authentication code

Security against impersonation and substitution attacks.

\[
\text{Adv}_{XAC}^{\text{imp}}(\kappa) := \max_{T'} \Pr[X\text{Ver}(K, T') = 1 | K \leftarrow \mathcal{K}]
\]

where the max is over all $T' \in \mathcal{X}T$, and

\[
\text{Adv}_{XAC}^{\text{sub}}(\kappa) := \max_{i, K_{\neq i}, F} \Pr[T' \neq T \land X\text{Ver}(K_i, T') = 1]
\]

\[
\begin{align*}
T' &\leftarrow F(T) \\
K_i &\leftarrow \mathcal{K}, \\
T &:= X\text{Auth}(K_1, \ldots, K_{\ell})
\end{align*}
\]

where the max is over all $i \in [\ell]$, all $K_{\neq i} = (K_j)_{j \neq i} \in \mathcal{K}^{\ell-1}$ and all (possibly randomized) functions $F : \mathcal{T} \rightarrow \mathcal{T}$.
Properties of $\ell$-XAC

Definition 2 (Strong and semi-unique $\ell$-XAC.)

Strongness: $K_1, \ldots, K_\ell \leftarrow \mathcal{K}$. $T \leftarrow \text{XAuth}(K_1, \ldots, K_\ell)$. Given $i$, $(K_j)_{j \neq i}$ and $T$,

$$\hat{K}_i \leftarrow \text{ReSamp}(K_{\neq i}, T)$$

such that, conditioned on $(K_j)_{j \neq i}$ and $T$,

$$\hat{K}_i \approx K_i.$$

Semi-Uniqueness: The key space $\mathcal{K} = \mathcal{K}_a \times \mathcal{K}_b$. Given tag $T$ and $K_a \in \mathcal{K}_a$, there exists at most one $K_b \in \mathcal{K}_b$ such that $X\text{Ver}((K_a, K_b), T) = 1$. 
Construction from Extractable 1SPO-IBE and XAC

Construct $\text{IBE} = (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec})$ from

- $(\ell + 1)$-XAC = (XAuth, XVer)
- $\text{IBE}_{\text{ex}} = (\text{Setup}_{\text{ex}}, \text{KeyGen}_{\text{ex}}, \text{Enc}_{\text{ex}}, \text{Dec}_{\text{ex}})$

$\text{Setup}(1^\kappa) : (\text{PK}_{\text{ex}}, \text{MSK}_{\text{ex}}) \leftarrow \text{Setup}_{\text{ex}}(1^\kappa)$.

$K_a \leftarrow K_a$ and $H : ID \times C \times \cdots \times C \rightarrow K_b$.

$\text{PK} = (\text{PK}_{\text{ex}}, H, K_a), \text{MSK} = \text{MSK}_{\text{ex}}$.

$\text{KeyGen}(\text{PK}, \text{MSK}, \text{ID}) : \text{SK}_{\text{ID}} \leftarrow \text{KeyGen}_{\text{ex}}(\text{PK}_{\text{ex}}, \text{MSK}_{\text{ex}}, \text{ID})$. 
Construction from Extractable 1SPO-IBE and XAC

Construct $\text{IBE} = (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec})$ from

1. $(\ell + 1)$-XAC = $(\text{XAuth}, \text{XVer})$

2. $\text{IBE}_{ex} = (\text{Setup}_{ex}, \text{KeyGen}_{ex}, \text{Enc}_{ex}, \text{Dec}_{ex})$

**Setup**($1^\kappa$) :

$(\text{PK}_{ex}, \text{MSK}_{ex}) \leftarrow \text{Setup}_{ex}(1^\kappa)$.

$K_a \leftarrow K_a$ and $H : \mathcal{ID} \times C \times \cdots \times C \rightarrow \mathcal{K}_b$.

$\text{PK} = (\text{PK}_{ex}, H, K_a)$, $\text{MSK} = \text{MSK}_{ex}$.

**KeyGen**($\text{PK}, \text{MSK}, \text{ID}$) :

$\text{SK}_{ID} \leftarrow \text{KeyGen}_{ex}(\text{PK}_{ex}, \text{MSK}_{ex}, \text{ID})$. 

Junzuo Lai, Robert H. Deng, Shengli Liu*, Jian Weng, and Yunlei Zhao (SJTU-CIS)
Construction from Extractable 1SPO-IBE and XAC

Construct $\text{IBE} = (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec})$ from

- $(\ell + 1)$-XAC = (XAuth, XVer)
- $\text{IBE}_{ex} = (\text{Setup}_{ex}, \text{KeyGen}_{ex}, \text{Enc}_{ex}, \text{Dec}_{ex})$

**Setup$(1^\kappa)$**: $(\text{PK}_{ex}, \text{MSK}_{ex}) \leftarrow \text{Setup}_{ex}(1^\kappa)$.

$$K_a \leftarrow K_a \text{ and } H : \mathcal{ID} \times C \times \cdots \times C \rightarrow K_b.$$  

$\text{PK} = (\text{PK}_{ex}, H, K_a)$, $\text{MSK} = \text{MSK}_{ex}$.

**KeyGen**(PK, MSK, ID) : $\text{SK}_{ID} \leftarrow \text{KeyGen}_{ex}(\text{PK}_{ex}, \text{MSK}_{ex}, \text{ID})$. 
Construction

\[ \text{Enc}(\mathsf{PK}, \mathsf{ID}, M) : \text{To encrypt a message } M = m_1 || \cdots || m_{\ell} \in \{0, 1\}^{\ell} \]

\[
\begin{cases}
(C_i, K_i) \leftarrow \text{Enc}_{\mathsf{ex}}(\mathsf{PK}_{\mathsf{ex}}, \mathsf{ID}, 1) & \text{if } m_i = 1 \\
C_i \leftarrow \text{Enc}_{\mathsf{ex}}(\mathsf{PK}_{\mathsf{ex}}, \mathsf{ID}, 0), \ K_i \leftarrow \mathcal{K} & \text{if } m_i = 0
\end{cases},
\]

\[ K_{\ell+1} = (K_a, K_b), \text{ where } K_b = \mathsf{H}(\mathsf{ID}, C_1, \ldots, C_{\ell}) ,
\]

\[ T = \mathsf{XAuth}(K_1, \ldots, K_{\ell+1}).
\]

\[ CT = (C_1, \ldots, C_{\ell}, T). \]
Construction

\[ \text{Enc}(\text{PK}, \text{ID}, M) : \text{To encrypt a message } M = m_1 || \cdots || m_\ell \in \{0, 1\}^\ell \]

\[
\begin{cases}
(C_i, K_i) \leftarrow \text{Enc}_{ex}(\text{PK}_{ex}, \text{ID}, 1) & \text{if } m_i = 1 \\
C_i \leftarrow \text{Enc}_{ex}(\text{PK}_{ex}, \text{ID}, 0), K_i \leftarrow \mathcal{K} & \text{if } m_i = 0
\end{cases}

, K_{\ell+1} = (K_a, K_b), \text{ where } K_b = H(\text{ID}, C_1, \ldots, C_\ell),

T = \text{XAuth}(K_1, \ldots, K_{\ell+1}).

CT = (C_1, \ldots, C_\ell, T).\]
Construction

**Enc(PK, ID, M)**: To encrypt a message $M = m_1 \| \cdots \| m_\ell \in \{0, 1\}^\ell$

$$
egin{cases}
(C_i, K_i) \leftarrow \text{Enc}_{ex}(PK_{ex}, ID, 1) & \text{if } m_i = 1 \\
C_i \leftarrow \text{Enc}_{ex}(PK_{ex}, ID, 0), K_i \leftarrow \mathcal{K} & \text{if } m_i = 0 \\
K_{\ell+1} = (K_a, K_b), \text{ where } K_b = H(ID, C_1, \ldots, C_\ell), \\
T = XAuth(K_1, \ldots, K_{\ell+1}).
\end{cases}
$$

$CT = (C_1, \ldots, C_\ell, T)$. 
Construction

Enc(PK, ID, M) : To encrypt a message $M = m_1 || \cdots || m_\ell \in \{0, 1\}^\ell$

\[
\begin{cases}
(C_i, K_i) \leftarrow \text{Enc}_{ex}(PK_{ex}, ID, 1) & \text{if } m_i = 1 \\
C_i \leftarrow \text{Enc}_{ex}(PK_{ex}, ID, 0), K_i \leftarrow \mathcal{K} & \text{if } m_i = 0
\end{cases}
\]

$K_{\ell+1} = (K_a, K_b)$, where $K_b = \text{H}(ID, C_1, \ldots, C_\ell)$,

$T = \text{XAuth}(K_1, \ldots, K_{\ell+1})$.

$CT = (C_1, \ldots, C_\ell, T)$. 
Construction

\[ \text{Dec}(PK, SK_{ID}, CT) : \text{ To decrypt } CT = (C_1, \ldots, C_{\ell}, T), \]

\[ K'_b = H(ID, C_1, \ldots, C_{\ell}); \text{ Set } K'_{\ell+1} = (K_a, K'_b) \]

\[ \text{XVer}(K'_{\ell+1}, T) = 1? \text{ If not, output } M'' = 0 \cdots 0. \]

Otherwise, for \( i \in [\ell], \)

\[ (m'_i, K'_i) \leftarrow \text{Dec}_{ex}(PK_{ex}, SK_{ID}, C_i) \]

and sets

\[ m''_i = \text{XVer}(K'_i, T) \]

Outputs the message \( M'' = m''_1 \| \cdots \| m''_{\ell}. \)
Construction

\textbf{Dec}(\text{PK}, \text{SK}_\text{ID}, CT) : \text{To decrypt } CT = (C_1, \ldots, C_\ell, T),

\[ K'_b = H(\text{ID}, C_1, \ldots, C_\ell); \text{ Set } K'_{\ell+1} = (K_a, K'_b) \]

\[ \text{XVer}(K'_{\ell+1}, T) = 1? \text{ If not, output } M'' = 0 \cdot \cdots \cdot 0. \]

Otherwise, for \( i \in [\ell], \)

\[ (m'_i, K'_i) \leftarrow \text{Dec}_{ex}(\text{PK}_{ex}, \text{SK}_\text{ID}, C_i) \]

and sets

\[ m''_i = \text{XVer}(K'_i, T) \]

Outputs the message \( M'' = m''_1 \| \cdots \| m''_\ell. \)
Construction

Dec(PK, SK_ID, CT) : To decrypt $CT = (C_1, \ldots, C_\ell, T)$,

\[ K'_b = H(ID, C_1, \ldots, C_\ell); \text{ Set } K'_{\ell+1} = (K_a, K'_b) \]

$XVer(K'_{\ell+1}, T) = 1$? If not, output $M'' = 0 \cdots 0$.

Otherwise, for $i \in [\ell]$,

\[
(m'_i, K'_i) \leftarrow \text{Dec}_\text{ex}(PK_{\text{ex}}, SK_{\text{ID}}, C_i)
\]

and sets

\[
m''_i = XVer(K'_i, T)
\]

Outputs the message $M'' = m''_1 \Vert \cdots \Vert m''_\ell$. 

Junzuo Lai, Robert H. Deng, Shengli Liu\textsuperscript{*}, Jian Weng, and Yunlei Zhao (SJTU-CIS)
Construction

Dec(PK, SK_ID, CT) : To decrypt $CT = (C_1, \ldots, C_\ell, T)$,

$$K'_b = H(ID, C_1, \ldots, C_\ell); \text{ Set } K'_{\ell+1} = (K_a, K'_b)$$

$XVer(K'_{\ell+1}, T) = 1$? If not, output $M'' = 0 \cdots 0$.

Otherwise, for $i \in [\ell],

$$\left( m'_i, K'_i \right) \leftarrow \text{Dec}_e(PK_e, SK_{ID}, C_i)$$

and sets

$$m''_i = XVer(K'_i, T)$$

Outputs the message $M'' = m''_1 \| \cdots \| m''_\ell$. 
Simulator

Challenger

\[ S = (S_1, S_2, S_3) \]

\[ \left( \alpha, \overrightarrow{ID} \right) \leftarrow S_1(1^\kappa) \{ (PK, MSK) \leftarrow \text{Setup}(1^\kappa) \} \]

\[ \left( \alpha, \overrightarrow{ID} \right) \leftarrow \mathcal{A}_1^{\text{KeyGen,Dec}(\cdot)}(PK) \} \]

\[ M' \leftarrow M(\alpha) \]

\[ = (M^{(1)}, \ldots, M^{(n)}) \]

\[ I \leftarrow S_2(1^{\left| M^{(i)} \right|}) \{ CT^{(i)} = \text{Enc}(PK, \overrightarrow{ID^{(i)}}, \overrightarrow{1 \cdots 1}), \]

\[ I \leftarrow \mathcal{A}_2^{\text{KeyGen,Dec}(\cdot)}(CT) \} \]

\[ (M^{(i)})_{i \in I} \]

\[ \text{Out}_S \leftarrow S_3 \left( (M^{(i)})_{i \in I} \right) \{ \text{If } m_{j}^{(i)} = 0, \]

\[ \hat{K}_{j}^{(i)} \leftarrow \text{ReSamp}(K_{j \neq j}^{(i)}, T) \]

\[ R_{j}^{(i)} \leftarrow \left( \text{POpen}(PK, ID, C_{j}^{(i)}), \hat{K}_{j}^{(i)} \right) \]

\[ \text{Out}_A \leftarrow \mathcal{A}_3^{\text{KeyGen,Dec}(\cdot)} \left( (M^{(i)}, R^{(i)})_{i \in I} \right) \} \]
Security Proof: Hybrid Argument

Suppose that the first challenger ciphertext is $CT = (C_1, C_2, C_3, T)$. 

<table>
<thead>
<tr>
<th>Game 0:</th>
<th>$C_1[m_1]$</th>
<th>$C_2[m_2]$</th>
<th>$C_3[m_3]$</th>
<th>$T = \text{XAuth}(K_1, K_2, K_3, K_4)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Game 1:</td>
<td>$C_1[1]$</td>
<td>$C_2[m_2]$</td>
<td>$C_3[m_3]$</td>
<td>$T = \text{XAuth}(K_1, K_2, K_3, K_4)$</td>
</tr>
</tbody>
</table>

The green parts will be opened with POpen and ReSample.

We will prove that

Game $0 \approx_c$ Game $1 \approx_c$ Game $2 \approx_c$ Game $3$. 

Junzuo Lai, Robert H. Deng, Shengli Liu*, Jia Identity-Based Encryption Secure Against Chc
Security Proof: Hybrid Argument (Game 1 $\approx_c$ Game 2)

- if $m_2 = 1$, Game 1 = Game 2;
- if $m_2 = 0$, reduction to the IND-ID-CCA2 security of $\text{IBE}_{ex}$.

The IND-ID-CCA2 adversary $B^{\text{KeyGen}_{ex}, \text{Dec}_{ex}}(ID^*, C^*, K^*)$ for $\text{IBE}_{ex}$ prepares the challenge ciphertext

<table>
<thead>
<tr>
<th>Game 1:</th>
<th>$C_1[1]$</th>
<th>$C_2[0]$</th>
<th>$C_3[m_3]$</th>
<th>$T = \text{XAuth}(K_1, K_2, K_3, K_4)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Game:</td>
<td>$C_1[1]$</td>
<td>$C^*$</td>
<td>$C_3[m_3]$</td>
<td>$T = \text{XAuth}(K_1, K^*, K_3, K_4)$</td>
</tr>
</tbody>
</table>

- It opens $C^*$ with $\hat{K}^* \leftarrow \text{ReSamp}(K_1, K_3, K_4, T)$,

  $$R_2 \leftarrow \left(\text{POpen}(PK, ID^*, C^*), \hat{K}^*\right)$$
Security Proof: Hybrid Argument

\( \mathcal{B}^{KeyGen_{ex}, Dec_{ex}}(ID^*, C^*, K^*) \) answers \( \mathcal{A} \)'s queries his own oracles \( KeyGen_{ex}(\cdot) \).

\( Dec_{ex}(\cdot) \) except

- \( \mathcal{A} \)'s \( Dec \) query for \( \overline{CT} = (\overline{C}_1, \ldots, \overline{C}_\ell, \overline{T}) \) under \( ID^* \) and \( \overline{C}_j = C^* \). In this case \( \mathcal{B}^{KeyGen_{ex}, Dec_{ex}}(ID^*, C^*, K^*) \) answers with

\[
\overline{m}''_j = XVer(K^*, \overline{T}).
\]

- If \((C^*, K^*)\) is an encryption of 1, then \( \overline{m}_j = XVer(K^*, \overline{T}) \) matches the decryption algorithm.

- If \( C^* \) is an encryption of 0, then \( K^* \) is random, and \( XVer(K^*, \overline{T}) = 0 \) except with probability \( \text{Adv}_{\text{XAC}}^{\text{sub}}(\kappa) \).
Security Proof: Hybrid Argument

\( B^{KeyGen_{ex}, Dec_{ex}}(ID^*, C^*, K^*) \) answers \( \mathcal{A} \)'s queries his own oracles \( KeyGen_{ex}(\cdot) \).

\( Dec_{ex}(\cdot) \) except

- \( \mathcal{A} \)'s \( Dec \) query for \( \tilde{C}T = (\tilde{C}_1, \ldots, \tilde{C}_\ell, \tilde{T}) \) under \( ID^* \) and \( \tilde{C}_j = C^* \). In this case \( B^{KeyGen_{ex}, Dec_{ex}}(ID^*, C^*, K^*) \) answers with

  \[ \tilde{m}''_j = XVer(K^*, \tilde{T}). \]

- If \((C^*, K^*)\) is an encryption of \(1\), then \( \tilde{m}_j = XVer(K^*, \tilde{T}) \) matches the decryption algorithm.

- If \( C^* \) is an encryption of \(0\), then \( K^* \) is random, and \( XVer(K^*, \tilde{T}) = 0 \) except with probability \( \text{Adv}_{\text{XAC}}^{\text{sub}}(\kappa) \).
Security Proof: Hybrid Argument

$\mathcal{B}^{\text{KeyGen}_{ex}, \text{Dec}_{ex}}(ID^*, C^*, K^*)$ answers $\mathcal{A}$’s queries his own oracles $\text{KeyGen}_{ex}(\cdot)$.

$\text{Dec}_{ex}(\cdot)$ except

- $\mathcal{A}$’s $\text{Dec}$ query for $\tilde{C}T = (\tilde{C}_1, \ldots, \tilde{C}_\ell, \tilde{T})$ under $ID^*$ and $\tilde{C}_j = C^*$. In this case $\mathcal{B}^{\text{KeyGen}_{ex}, \text{Dec}_{ex}}(ID^*, C^*, K^*)$ answers with

  $$\tilde{m}''_j = \text{XVer}(K^*, \tilde{T}).$$

- If $(C^*, K^*)$ is an encryption of 1, then $\tilde{m}_j = \text{XVer}(K^*, \tilde{T})$ matches the decryption algorithm.

- If $C^*$ is an encryption of 0, then $K^*$ is random, and $\text{XVer}(K^*, \tilde{T}) = 0$ except with probability $\text{Adv}_{\text{subXAC}}(\kappa)$. 
Security Proof: Hybrid Argument

- Since $\overline{CT} \neq CT^{(i)}$ for $i \in [n]$, then we have $\overline{T} \neq T^{(i)}$, due to the collision resistance of H and semi-unique property of XAC.
- The Resamplable property of XAC ensures that $K^*$ is not disclosed during the corruption.
Construction of extractable 1SPO-IBEs

- We construct **two one-bit 1SPO-IBEs**, one based on the anonymous extension of Lewko-Waters IBE scheme by De Caro, Iovino and Persiano and the other based on the Boyen-Waters anonymous IBE. Both schemes rely on a pairing $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

- The 1SPO property of the two one-bit IBE schemes is guaranteed by the fact that $\mathbb{G}$ is an *efficiently samplable and explainable domain*, which is characterized by two PPT algorithms $\text{Sample}''$ and $\text{Sample}''^{-1}$ for group $\mathbb{G}$.

- The IND-ID-CCA2 security of extractable 1SPO-IBEs makes use of 2-hierarchical IBE technique.

The construction of XAC follows that in [FKHW10].
Conclusion

- We introduced a new primitive “extractable IBE”, defined its IND-ID-CCA security, and proposed two instantiations;
- Combined with strengthened “Cross Authentication Code”, we construct the first IBE with SIM-SO-CCA2 security.