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$(1^\kappa) \rightarrow$ (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) $\rightarrow M/\perp$.

An IBE scheme has completeness error ϵ 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$(1^\kappa) \to$ (PK, MSK). PK: public parameter; MSK: master secret key.

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

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

Dec(PK, $\mathsf{SK}_{\mathsf{ID}}$, CT) $\to M/\perp$.

An IBE scheme has completeness error ϵ 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$(1^\kappa) \rightarrow$ (PK, MSK). PK: public parameter; MSK: master secret key.

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

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

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

An IBE scheme has completeness error ϵ 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:

$\mathsf{Setup}(1^\kappa) \rightarrow (\mathsf{PK}, \mathsf{MSK})$. PK: public parameter; MSK: master secret key.

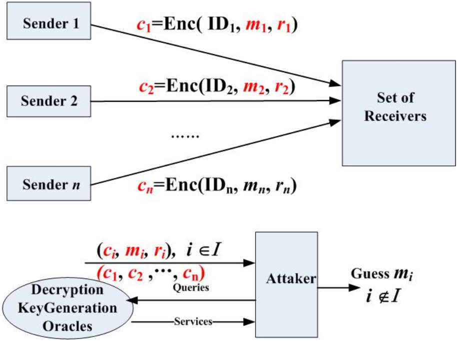
$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID}) \rightarrow \mathsf{SK}_{\mathsf{ID}}$. $\mathsf{SK}_{\mathsf{ID}}$ is the private key for identity ID.

$\mathsf{Enc}(\mathsf{PK}, \mathsf{ID}, M) \rightarrow CT$. CT: ciphertext.

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

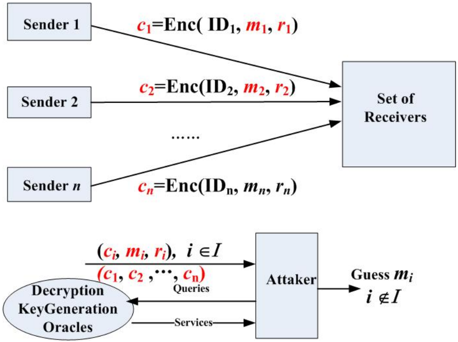
An IBE scheme has completeness error ϵ if the correct decryption holds with probability at least $1-\epsilon$, where the probability is taken over the coins used in encryption.

Selective Opening Attack



Selective Opening Attack: a vector of ciphertexts, adaptive corruptions exposing not only some message but also the random coins.

Selective Opening Attack



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.
- Fehr, Hofheinz, Kiltz, and Wee [FHKW2010] proposed the first construction of PKE with SIM-SO-CCA2 Security.
- Bellare, Waters, and S. Yilek[BWY2011] proposed the first construction of IBE with SIM-SO-CCA2 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.
- Fehr, Hofheinz, Kiltz, and Wee [FHKW2010] proposed the first construction of PKE with SIM-SO-CCA2 Security.
- Bellare, Waters, and S. Yilek[BWY2011] proposed the first construction of IBE with SIM-SO-CCA2 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.
- Fehr, Hofheinz, Kiltz, and Wee [FHKW2010] proposed the first construction of PKE with SIM-SO-CCA2 Security.
- Bellare, Waters, and S. Yilek[BWY2011] proposed the first construction of IBE with SIM-SO-CCA2 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.
- Fehr, Hofheinz, Kiltz, and Wee [FHKW2010] proposed the first construction of PKE with SIM-SO-CCA2 Security.
- Bellare, Waters, and S. Yilek[BWY2011] proposed the first construction of IBE with SIM-SO-CCA2 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.
- Fehr, Hofheinz, Kiltz, and Wee [FHKW2010] proposed the first construction of PKE with SIM-SO-CCA2 Security.
- Bellare, Waters, and S. Yilek[BWY2011] proposed the first construction of IBE with SIM-SO-CCA2 Security.
- How to construct IBE with SIM-SO-CCA2 Security remains open.

SIM-SO-CCA2 Security: $\mathsf{Exp}_{\mathcal{A},\mathcal{M},R}^{cca-so-real}(1^\kappa)$

Challenger		$\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$
(PK, MSK) $\leftarrow$ Setup(1^κ)	PK $\longrightarrow$	
	$\longleftarrow (\alpha, \overrightarrow{ID})$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}(PK)$
$\overrightarrow{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)$		
$\overrightarrow{R} = (R^{(1)}, \ldots, R^{(n)}) \leftarrow \mathcal{R}$		
$\overrightarrow{CT} = \mathsf{Enc}(PK, \overrightarrow{ID}, \overrightarrow{M}; \overrightarrow{R})$	$\overrightarrow{CT} \longrightarrow$	
	$\longleftarrow I$	$I \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}(\overrightarrow{CT})$
	$(M^{(i)}, R^{(i)})_{i \in I} \longrightarrow$	$\mathsf{out}_A \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}((M^{(i)}, R^{(i}$

$R(\overrightarrow{ID}, \overrightarrow{M}, I, out_A)$

SIM-SO-CCA2 Security: $\mathrm{Exp}^{cca-so-real}_{\mathcal{A},\mathcal{M},R}(1^\kappa)$

Challenger		$\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$
(PK, MSK) ← Setup(1^κ)	PK $\longrightarrow$	
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}(PK)$
$\overrightarrow{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)$		
$\overrightarrow{R} = (R^{(1)}, \ldots, R^{(n)}) \leftarrow \mathcal{R}$		
$\overrightarrow{CT} = \mathsf{Enc}(PK, \overrightarrow{ID}, \overrightarrow{M}; \overrightarrow{R})$	$\xrightarrow{\overrightarrow{CT}}$	
	$\xleftarrow{I}$	$I \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}(\overrightarrow{CT})$
	$\xrightarrow{(M^{(i)}, R^{(i)})_{i \in I}}$	$\mathsf{out}_A \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}((M^{(i)}, R^{(i}$

$R(\overrightarrow{ID}, \overrightarrow{M}, I, out_A)$

SIM-SO-CCA2 Security: $\mathrm{Exp}^{cca-so-real}_{\mathcal{A},\mathcal{M},R}(1^\kappa)$

Challenger		$\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$
(PK, MSK)$\leftarrow$ Setup(1^κ)	$\xrightarrow{\text{PK}}$	
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(PK)$
$\overrightarrow{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)$		
$\overrightarrow{R} = (R^{(1)}, \ldots, R^{(n)}) \leftarrow \mathcal{R}$		
$\overrightarrow{CT} = \text{Enc}(PK, \overrightarrow{ID}, \overrightarrow{M}; \overrightarrow{R})$	$\xrightarrow{\overrightarrow{CT}}$	
	$\xleftarrow{I}$	$I \leftarrow \mathcal{A}_2^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(\overrightarrow{CT})$
	$\xrightarrow{(M^{(i)},R^{(i)})_{i\in I}}$	$\text{out}_A \leftarrow \mathcal{A}_3^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}\left(\left(M^{(i)}, R^{(i}\right.\right.$

$R(\overrightarrow{ID}, \overrightarrow{M}, I, out_A)$

SIM-SO-CCA2 Security: $\mathrm{Exp}^{cca-so-ideal}_{\mathcal{A},\mathcal{M},R}(1^\kappa)$

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$
$\vec{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)$		
	$\xleftarrow{I \subsetneq [n]}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\mathsf{Out}_{\mathcal{S}} \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$

$$R(\overrightarrow{ID}, \vec{M}, I, out_{\mathcal{S}})$$

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

$$\left| \Pr\left[R(\overrightarrow{ID}, \vec{M}, I, out_{\mathcal{A}}) = 1 \right] - \Pr\left[R(\overrightarrow{ID}, \vec{M}, I, out_{\mathcal{S}}) = 1 \right] \right|$$ is negligible.

SIM-SO-CCA2 Security: $\mathrm{Exp}^{cca-so-ideal}_{\mathcal{A},\mathcal{M},R}(1^\kappa)$

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$
$\vec{M} = (M^{(1)}, \ldots, M^{(n)}) \leftarrow \mathcal{M}(\alpha)$		
	$\xleftarrow{I \subsetneq [n]}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\mathrm{Out}_S \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$

$$R(\overrightarrow{ID}, \vec{M}, I, out_S)$$

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

$$\left| \Pr\left[R(\overrightarrow{ID}, \vec{M}, I, out_A) = 1 \right] - \Pr\left[R(\overrightarrow{ID}, \vec{M}, I, out_S) = 1 \right] \right|$$ is negligible.

How to get SIM-SO-CCA2 Security: the idea

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$
$\vec{M} = (M^{(1)}, \ldots, M^{(n)})$	$\xleftarrow{I}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\text{Out}_S \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$

Aim: $\left(\overrightarrow{ID}, \vec{M}, I, out_A\right) \approx_c \left(\overrightarrow{ID}, \vec{M}, I, out_S\right)$

How to get SIM-SO-CCA2 Security: the idea

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$
		$\{\ (\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\kappa)$
$\vec{M} \leftarrow \mathcal{M}(\alpha)$		$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}, Dec(\cdot)}(PK)\ \}$
$\vec{M} = (M^{(1)}, \ldots, M^{(n)})$	$\xleftarrow{I}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\mathsf{Out}_S \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$

Aim: $\left(\overrightarrow{ID}, \vec{M}, I, out_A\right) \approx_c \left(\overrightarrow{ID}, \vec{M}, I, out_S\right)$

How to get SIM-SO-CCA2 Security: the idea

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$
		$\{$ (PK, MSK) $\leftarrow$ Setup(1^κ)
$\vec{M} \leftarrow \mathcal{M}(\alpha)$		$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(PK)$ $\}$
$\vec{M} = (M^{(1)}, \ldots, M^{(n)})$	$\xleftarrow{I}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$
		$\{I \leftarrow \mathcal{A}_2^{\text{KeyGen}(\cdot),\text{Dec}(\cdot)}(\overrightarrow{CT})$ $\}$
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\text{Out}_{\mathcal{S}} \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$

Aim: $\left(\overrightarrow{ID}, \vec{M}, I, out_A\right) \approx_c \left(\overrightarrow{ID}, \vec{M}, I, out_S\right)$

How to get SIM-SO-CCA2 Security: the idea

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$
		$\{ (\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\kappa)$
$\vec{M} \leftarrow \mathcal{M}(\alpha)$		$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}(PK) \}$
$\vec{M} = (M^{(1)}, \ldots, M^{(n)})$	$\xleftarrow{I}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$
		$\{I \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}(\overrightarrow{CT}) \}$
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\mathsf{Out}_S \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$
		$\{\mathsf{Out}_A \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot)}\left(\left(M^{(i)}, R^{(i)}\right)_{i \in I}\right) \}$

Aim: $\left(\overrightarrow{ID}, \vec{M}, I, out_A\right) \approx_c \left(\overrightarrow{ID}, \vec{M}, I, out_S\right)$

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 $C = Enc1(PK, ID, 0; R)$. *Let*

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

An IBE1 scheme is One-Sided Publicly Openable if $R' \leftarrow POpen(PK, ID, C)$ *outputs a random* R' *in* $Coins(PK, ID, C, 0)$.

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.

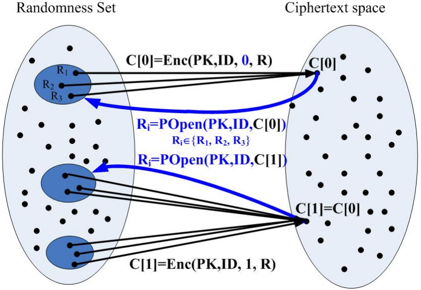
Definition 1 (1SPO-IBE1)

Let $C = \mathit{Enc1}(PK, ID, 0; R)$. *Let*

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

An IBE1 scheme is One-Sided Publicly Openable if $R' \leftarrow \mathit{POpen}(PK, ID, C)$ *outputs a random* R' *in* $\mathit{Coins}(PK, ID, C, 0)$.

SIM-SO-CPA Security for single bit messages



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

$$C[1] = \begin{cases} C[1] & \text{opened with the original randomness} \\ C[0] & \text{opened with POpen} \end{cases}$$

SIM-SO-CPA Security for multi-bit messages

[BWY2011] M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In TCC2011.

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

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

IBE.Enc:

C_1	C_2	$\ldots$	C_ℓ
$\uparrow$	$\uparrow$	$\ldots$	$\uparrow$
IBE1.Enc	IBE1.Enc	$\ldots$	IBE1.Enc
$\uparrow$	$\uparrow$	$\ldots$	$\uparrow$
$m_1(0/1)$	$m_2(0/1)$	$\ldots$	$m_\ell(0/1)$

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

SIM-SO-CPA Security for multi-bit messages

M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In TCC, pages 235 – 252, 2011.

IBE.Dec:

C_1	C_2	$\ldots$	C_ℓ
$\downarrow$ IBE1.Dec $\downarrow$	$\downarrow$ IBE1.Dec $\downarrow$	$\ldots$ $\ldots$ $\ldots$	$\downarrow$ IBE1.Dec $\downarrow$
m_1	m_2	$\ldots$	m_ℓ

SIM-SO-CPA Security for multi-bit messages follows from the SIM-SO-CPA Security of single-bit by hybrid argument.

SIM-SO-CPA Security for multi-bit messages

M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In TCC, pages 235 – 252, 2011.

	C_1	C_2	...	C_ℓ
	↓	↓	...	↓
IBE.Dec:	IBE1.Dec	IBE1.Dec	...	IBE1.Dec
	↓	↓	...	↓
	m_1	m_2	...	m_ℓ

SIM-SO-CPA Security for multi-bit messages follows from the SIM-SO-CPA Security of single-bit by hybrid argument.

SIM-SO-CCA2 Security for multi-bit messages

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

IBE.Enc:

C_1	C_2	...	C_ℓ
↑	↑	...	↑
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 Security for multi-bit messages

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

	C_1	C_2	$\ldots$	C_ℓ
IBE.Enc:	$\uparrow$ IBE1.Enc $\uparrow$	$\uparrow$ IBE1.Enc $\uparrow$	$\ldots$	$\uparrow$ IBE1.Enc $\uparrow$
	$m_1(0/1)$	$m_2(0/1)$	$\ldots$	$m_\ell(0/1)$

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 $\not\Rightarrow \xrightarrow{\text{CHK Transform}} \not\Rightarrow$ 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?

IBE.Enc:

C_1	C_2	$\ldots$	C_ℓ
$\uparrow$	$\uparrow$	$\ldots$	$\uparrow$
IBE1.Enc	IBE1.Enc	$\ldots$	IBE1.Enc
$\uparrow$	$\uparrow$	$\ldots$	$\uparrow$
$m_1(0/1)$	$m_2(0/1)$	$\ldots$	$m_\ell(0/1)$

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 $\not\Rightarrow \xRightarrow{\text{CHK Transform}} \not\Rightarrow$ 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?

IBE.Enc:

	C_1	C_2	$\dots$	C_ℓ
	$\uparrow$	$\uparrow$	$\dots$	$\uparrow$
IBE.Enc:	IBE1.Enc	IBE1.Enc	$\dots$	IBE1.Enc
	$\uparrow$	$\uparrow$	$\dots$	$\uparrow$
	$m_1(0/1)$	$m_2(0/1)$	$\dots$	$m_\ell(0/1)$

IBE is NOT CCA2 secure even if IBE1 is!

SIM-SO-CCA2: Our approach

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

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

C_1, K_1	C_2, K_2	...	C_ℓ, K_ℓ
↑ IBE$_{ex}$.Enc ↑	↑ IBE$_{ex}$.Enc ↑	... ...	↑ IBE$_{ex}$.Enc ↑
$m_1(0/1)$	$m_2(0/1)$	...	$m_\ell(0/1)$

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

SIM-SO-CCA2: Our approach

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

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

C_1, K_1	C_2, K_2	$\ldots$	C_ℓ, K_ℓ
$\uparrow$ $\mathsf{IBE}_{ex}.\mathsf{Enc}$ $\uparrow$	$\uparrow$ $\mathsf{IBE}_{ex}.\mathsf{Enc}$ $\uparrow$	$\ldots$ $\ldots$ $\ldots$	$\uparrow$ $\mathsf{IBE}_{ex}.\mathsf{Enc}$ $\uparrow$
$m_1(0/1)$	$m_2(0/1)$	$\ldots$	$m_\ell(0/1)$

New Primitives: IBE_{ex} and X-Authentication Code.

Extractable 1SPO-IBE

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

- 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',

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

$$(C, K) \overset{c}{\approx} (C', K')$$

Extractable 1SPO-IBE

Extractable 1SPO-IBE: IBE_{ex}=(Setup_{ex},KeyGen_{ex}, Enc_{ex}, Dec_{ex})

- 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',

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

$$(C, K) \overset{c}{\approx} (C', K')$$

Extractable 1SPO-IBE

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

- 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',

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

$$(C, K) \stackrel{c}{\approx} (C', K')$$

Extractable 1SPO-IBE

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

- 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',

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

$$(C, K) \stackrel{c}{\approx} (C', K')$$

ℓ-Cross-authentication code

[FHKW2010] S. Fehr, D. Hofheinz, E. Kiltz, and H. Wee. Encryption schemes secure against chosen-ciphertext selective opening attacks. In EUROCRYPT2010.

ℓ-Cross-authentication code: ℓ-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.

ℓ-Cross-authentication code

[FHKW2010] S. Fehr, D. Hofheinz, E. Kiltz, and H. Wee. Encryption schemes secure against chosen-ciphertext selective opening attacks. In EUROCRYPT2010.

ℓ-Cross-authentication code: ℓ-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.

ℓ-Cross-authentication code

[FHKW2010] S. Fehr, D. Hofheinz, E. Kiltz, and H. Wee. Encryption schemes secure against chosen-ciphertext selective opening attacks. In EUROCRYPT2010.

ℓ-Cross-authentication code: ℓ-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 ℓ-Cross-authentication code

Security against impersonation and substitution attacks.

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

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

$$\mathsf{Adv}^{\mathsf{sub}}_{\mathsf{XAC}}(\kappa) := \max_{i, K_{\neq i}, F} \Pr\left[\begin{array}{c} T' \neq T \wedge \\ \mathsf{XVer}(K_i, T') = 1 \end{array} \middle| \begin{array}{c} K_i \leftarrow \mathcal{K}, \\ T := \mathsf{XAuth}(K_1, \ldots, K_\ell), \\ T' \leftarrow F(T) \end{array}\right]$$

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 ℓ-Cross-authentication code

Security against impersonation and substitution attacks.

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

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

$$\mathsf{Adv}^{\mathsf{sub}}_{\mathsf{XAC}}(\kappa) := \max_{i, K_{\neq i}, F} \Pr\left[\begin{array}{c} T' \neq T \wedge \\ \mathsf{XVer}(K_i, T') = 1 \end{array} \middle| \begin{array}{c} K_i \leftarrow \mathcal{K}, \\ T := \mathsf{XAuth}(K_1, \ldots, K_\ell), \\ T' \leftarrow F(T) \end{array}\right]$$

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 ℓ-XAC

Definition 2 (Strong and semi-unique ℓ-XAC.)

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

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

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

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

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* *XVer*$((K_a, K_b), T) = 1$.

Construction from Extractable 1SPO-IBE and XAC

Construct IBE=(Setup, KeyGen, Enc, Dec) from

- $(\ell + 1)$-XAC=(XAuth, XVer)
- IBE_{ex}=(Setup_{ex},KeyGen_{ex}, Enc_{ex}, Dec_{ex})

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

$$K_a \leftarrow \mathcal{K}_a \text{ and } \text{H}: \mathcal{ID} \times \overbrace{\mathcal{C} \times \cdots \times \mathcal{C}}^{\ell} \rightarrow \mathcal{K}_b.$$

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

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

Construction from Extractable 1SPO-IBE and XAC

Construct IBE=(Setup, KeyGen, Enc, Dec) from

- $(\ell+1)$-XAC=(XAuth, XVer)
- IBE_{ex}=(Setup_{ex},KeyGen_{ex}, Enc_{ex}, Dec_{ex})

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

$$K_a \leftarrow \mathcal{K}_a \text{ and } \mathsf{H}: \mathcal{ID} \times \overbrace{\mathcal{C} \times \cdots \times \mathcal{C}}^{\ell} \rightarrow \mathcal{K}_b.$$

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

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

Construction from Extractable 1SPO-IBE and XAC

Construct IBE=(Setup, KeyGen, Enc, Dec) from

- $(\ell + 1)$-XAC=(XAuth, XVer)
- IBE_{ex}=(Setup_{ex},KeyGen_{ex}, Enc_{ex}, Dec_{ex})

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

$$K_a \leftarrow \mathcal{K}_a \text{ and } \mathsf{H} : \mathcal{ID} \times \overbrace{\mathcal{C} \times \cdots \times \mathcal{C}}^{\ell} \rightarrow \mathcal{K}_b.$$

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

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

Construction

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

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

$K_{\ell+1} = (K_a, K_b)$, 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

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

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

$K_{\ell+1} = (K_a, K_b)$, 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

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

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

$K_{\ell+1} = (K_a, K_b)$, 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

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

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

$K_{\ell+1} = (K_a, K_b)$, 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

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

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

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

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

$$(m'_i, K'_i) \leftarrow \mathsf{Dec}_{ex}(\mathsf{PK}_{ex}, \mathsf{SK}_{\mathsf{ID}}, C_i)$$

and sets

$$m''_i = \mathsf{XVer}(K'_i, T)$$

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

Construction

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

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

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

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

$$(m'_i, K'_i) \leftarrow \mathsf{Dec}_{ex}(\mathsf{PK}_{ex}, \mathsf{SK}_{\mathsf{ID}}, C_i)$$

and sets

$$m''_i = \mathsf{XVer}(K'_i, T)$$

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

Construction

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

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

XVer$(K'_{\ell+1}, T) = 1$? If not, output $M'' = \overbrace{0\cdots0}^{\ell}$.

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

$$(m'_i, K'_i) \leftarrow \mathsf{Dec}_{ex}(\mathsf{PK}_{ex}, \mathsf{SK}_{\mathsf{ID}}, C_i)$$

and sets

$$m''_i = \mathsf{XVer}(K'_i, T)$$

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

Construction

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

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

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

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

$$(m'_i, K'_i) \leftarrow \mathsf{Dec}_{ex}(\mathsf{PK}_{ex}, \mathsf{SK}_{\mathsf{ID}}, C_i)$$

and sets

$$m''_i = \mathsf{XVer}(K'_i, T)$$

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

Simulator

Challenger		$\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$
	$\xleftarrow{(\alpha, \overrightarrow{ID})}$	$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{S}_1(1^\kappa)$ { $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\kappa)$
$\vec{M} \leftarrow \mathcal{M}(\alpha)$		$(\alpha, \overrightarrow{ID}) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}, Dec(\cdot)}(PK)$ }
$= (M^{(1)}, \ldots, M^{(n)})$	$\xleftarrow{I}$	$I \leftarrow \mathcal{S}_2(1^{\lvert M^{(i)} \rvert})$ { $CT^{(i)} = \mathsf{Enc}(\mathsf{PK}, \mathsf{ID}^{(i)}, \overbrace{1 \cdots 1}^{\ell})$,
		$I \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}, Dec(\cdot)}(\overrightarrow{CT})$ }
	$\xrightarrow{(M^{(i)})_{i \in I}}$	$\mathsf{Out}_S \leftarrow \mathcal{S}_3\left(\left(M^{(i)}\right)_{i \in I}\right)$ { If $m_j^{(i)} = 0$,
		$\hat{K}_j^{(i)} \leftarrow \mathsf{ReSamp}(K_{\neq j}^{(i)}, T)$
		$R_j^{(i)} \leftarrow \left(\mathsf{POpen}(\mathsf{PK}, \mathsf{ID}, C_j^{(i)}), \hat{K}_j^{(i)}\right)$
		$\mathsf{Out}_A \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}, Dec(\cdot)}\left(\left(M^{(i)}, R^{(i)}\right)_{i \in I}\right)$ }

Security Proof: Hybrid Argument

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

Game 0:	$C_1[m_1]$	$C_2[m_2]$	$C_3[m_3]$	T = XAuth(K_1, K_2, K_3, K_4)
Game 1:	$C_1[1]$	$C_2[m_2]$	$C_3[m_3]$	T = XAuth(K_1, K_2, K_3, K_4)
Game 2:	$C_1[1]$	$C_2[1]$	$C_3[m_3]$	T = XAuth(K_1, K_2, K_3, K_4)
Game 3:	$C_1[1]$	$C_2[1]$	$C_3[1]$	T = XAuth(K_1, K_2, K_3, K_4)

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.

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 IBE$_{ex}$.

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

Game 1:	$C_1[1]$	$C_2[0]$	$C_3[m_3]$	T = XAuth(K_1, K_2, K_3, K_4)
Game:	$C_1[1]$	C^*	$C_3[m_3]$	T = XAuth(K_1, K^*, K_3, K_4)
Game 2:	$C_1[1]$	$C_2[1]$	$C_3[m_3]$	T = XAuth(K_1, K_2, K_3, K_4)

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

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

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 $\widetilde{CT} = \left(\widetilde{C}_1, \ldots, \widetilde{C}_\ell, \widetilde{T}\right)$ under ID* and $\widetilde{C}_j = C^*$. In this case $\mathcal{B}^{KeyGen_{ex},Dec_{ex}}(ID^*, C^*, K^*)$ answers with

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

- If (C^*, K^*) is an encryption of 1, then $\widetilde{m}_j = \text{XVer}(K^*, \widetilde{T})$ matches the decryption algorithm.
- If C^* is an encryption of 0, then K^* is random, and $\text{XVer}(K^*, \widetilde{T}) = 0$ except with probability $\text{Adv}^{\text{sub}}_{\text{XAC}}(\kappa)$.

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 $\widetilde{CT} = \left(\widetilde{C}_1, \ldots, \widetilde{C}_\ell, \widetilde{T}\right)$ under ID* and $\widetilde{C}_j = C^*$. In this case $\mathcal{B}^{KeyGen_{ex},Dec_{ex}}(ID^*, C^*, K^*)$ answers with

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

- If (C^*, K^*) is an encryption of 1, then $\widetilde{m}_j = \mathsf{XVer}(K^*, \widetilde{T})$ matches the decryption algorithm.
- If C^* is an encryption of 0, then K^* is random, and $\mathsf{XVer}(K^*, \widetilde{T}) = 0$ except with probability $\mathsf{Adv}^{\mathsf{sub}}_{\mathsf{XAC}}(\kappa)$.

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 $\widetilde{CT} = \left(\widetilde{C}_1, \ldots, \widetilde{C}_\ell, \widetilde{T}\right)$ under ID* and $\widetilde{C}_j = C^*$. In this case $\mathcal{B}^{KeyGen_{ex},Dec_{ex}}(ID^*, C^*, K^*)$ answers with

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

- If (C^*, K^*) is an encryption of 1, then $\widetilde{m}_j = \mathsf{XVer}(K^*, \widetilde{T})$ matches the decryption algorithm.
- If C^* is an encryption of 0, then K^* is random, and $\mathsf{XVer}(K^*, \widetilde{T}) = 0$ except with probability $\mathsf{Adv}^{\mathsf{sub}}_{\mathsf{XAC}}(\kappa)$.

Security Proof: Hybrid Argument

- Since $\widetilde{CT} \neq CT^{(i)}$ for $i \in [n]$, then we have $\widetilde{T} \neq T^{(i)}$, 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 Sample$''$ and 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.