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

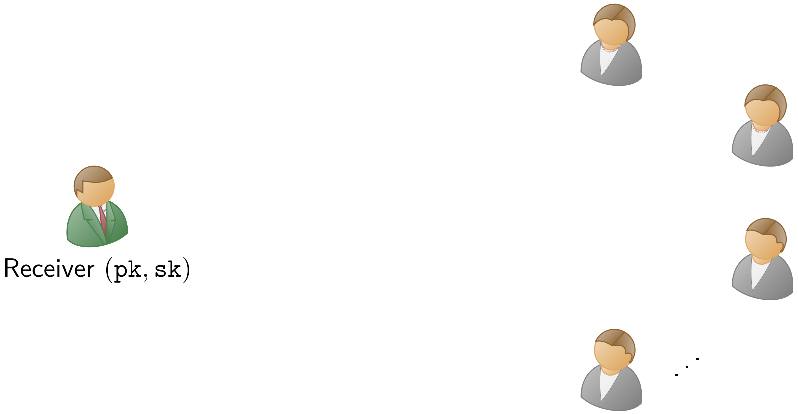
Asiacrypt 2022

Jiaxin Pan and Runzhi Zeng

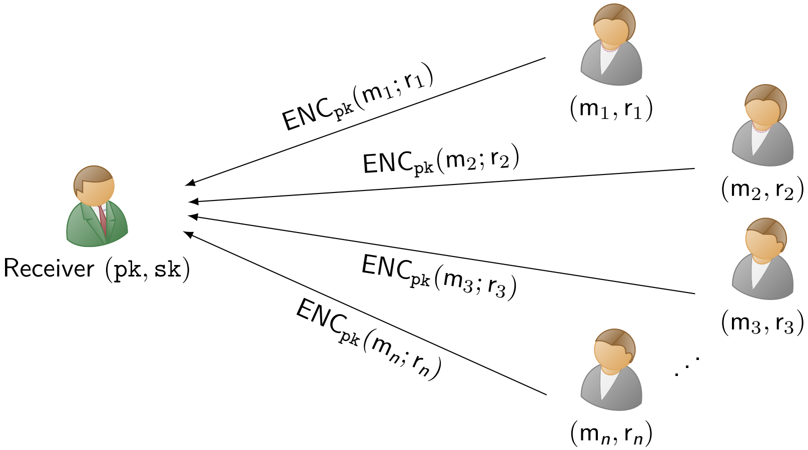
December 7, 2022

Norwegian University of Science and Technology

(Sender) Selective Opening Security

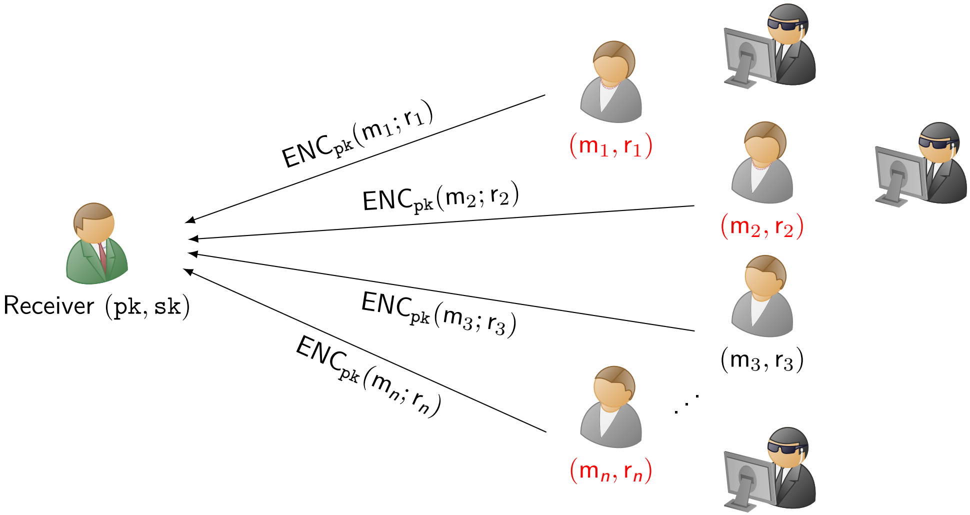


(Sender) Selective Opening Security

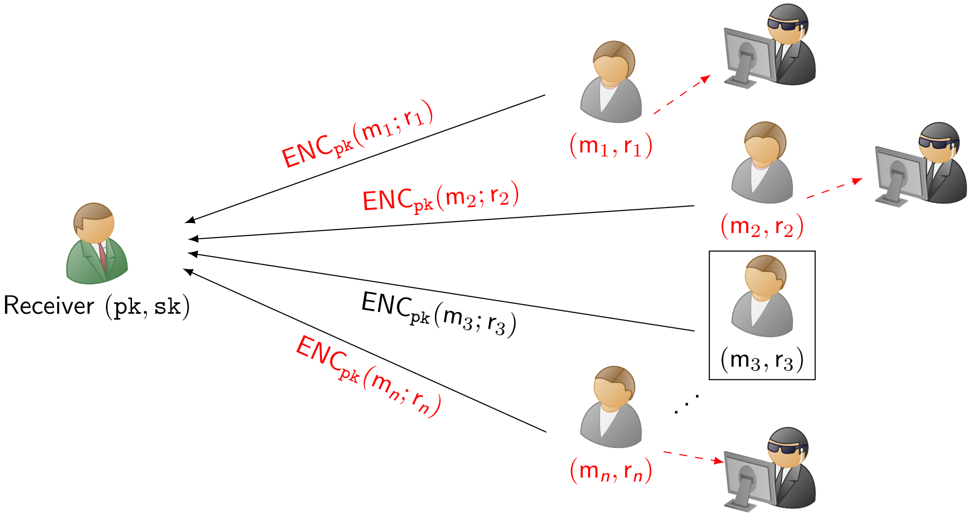


NTNU

(Sender) Selective Opening Security

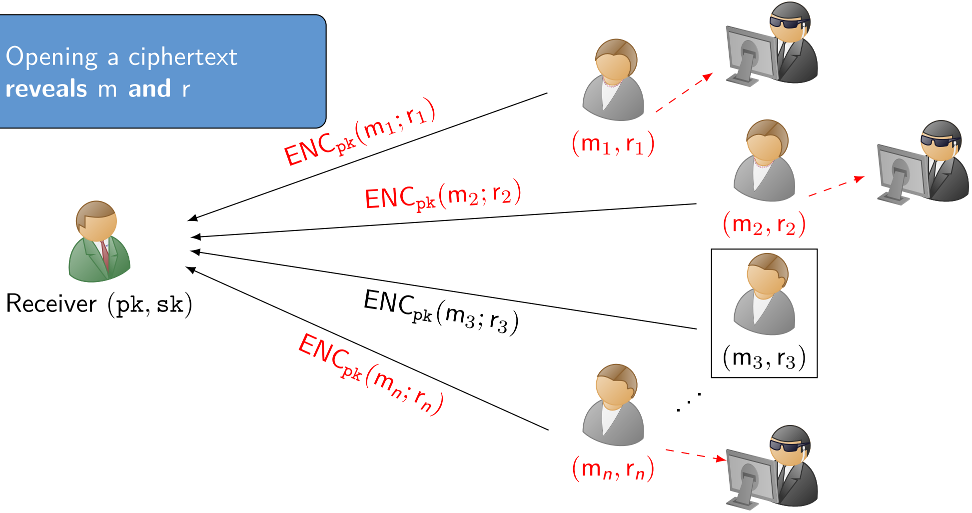


(Sender) Selective Opening Security



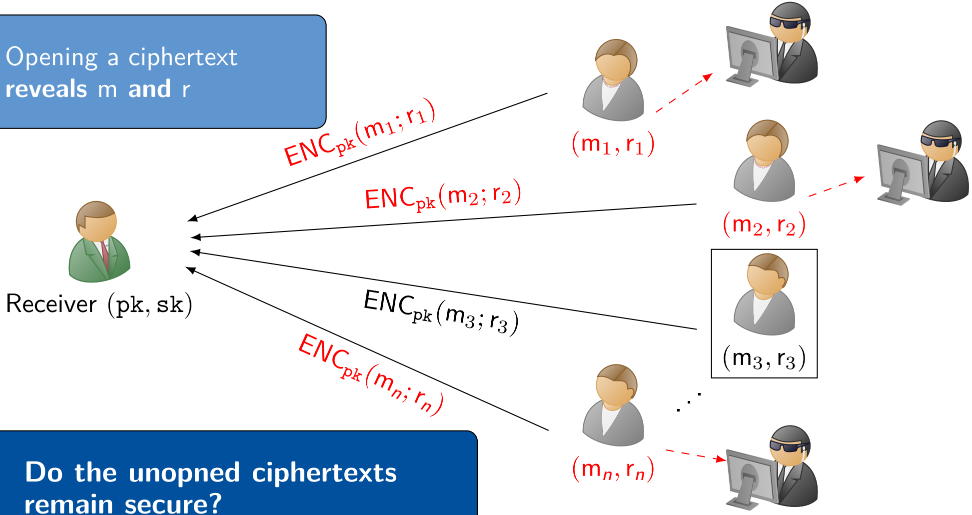
(Sender) Selective Opening Security

Opening a ciphertext
reveals m **and** r



(Sender) Selective Opening Security

Opening a ciphertext
reveals m **and** r



Do the unopned 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

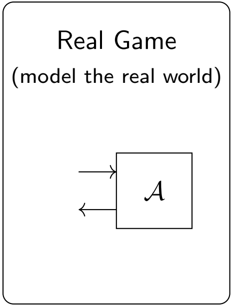
- Two flavors of SO(-CCA) security notions.
  - Indistinguishability-based SO (IND-SO) Security [BHY09, BHK12]
  - Simulation-based SO (SIM-SO) Security [DNRS99, BHY09]

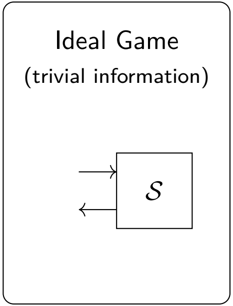
Selective Opening Security

- 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]

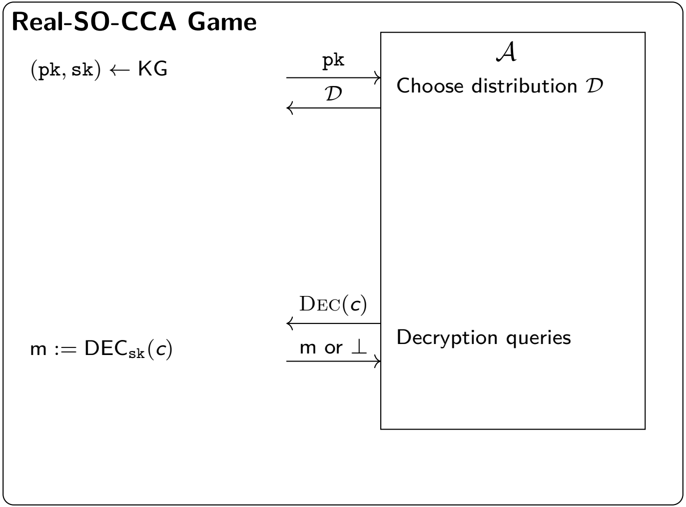
SIM-SO-CCA Security

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





SIM-SO-CCA Security - Real Game



SIM-SO-CCA Security - Real Game

Real-SO-CCA Game

Challenger		$\mathcal{A}$
$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{KG}$	$\xrightarrow{\mathrm{pk}}$	
	$\xleftarrow{\mathcal{D}}$	Choose distribution $\mathcal{D}$
$(\mathsf{m}_1, \dots, \mathsf{m}_n) \leftarrow \mathcal{D}$ $(\mathsf{r}_1, \dots, \mathsf{r}_n) \leftarrow \$$ $\forall i : \mathsf{c}_i := \mathsf{ENC}_{\mathrm{pk}}(\mathsf{m}_i, \mathsf{r}_i)$	$\xrightarrow{\mathsf{c}_1, \dots, \mathsf{c}_n}$	
Require $c \notin \{\mathsf{c}_1, \dots, \mathsf{c}_n\}$ $\mathsf{m} := \mathsf{DEC}_{\mathrm{sk}}(c)$	$\xleftarrow{\textsc{Dec}(c)}$ $\xrightarrow{\mathsf{m} \text{ or } \perp}$	Decryption queries

SIM-SO-CCA Security - Real Game

Real-SO-CCA Game

Challenger		$\mathcal{A}$
$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{KG}$	$\xrightarrow{\mathrm{pk}}$	Choose distribution $\mathcal{D}$
	$\xleftarrow{\mathcal{D}}$	
$(\mathsf{m}_1, \dots, \mathsf{m}_n) \leftarrow \mathcal{D}$ $(\mathsf{r}_1, \dots, \mathsf{r}_n) \leftarrow \$$ $\forall i : \mathsf{c}_i := \mathsf{ENC}_{\mathrm{pk}}(\mathsf{m}_i, \mathsf{r}_i)$	$\xrightarrow{\mathsf{c}_1, \dots, \mathsf{c}_n}$	
	$\xleftarrow{\textsc{Open}(i)}$	
$\mathcal{I} := \mathcal{I} \cup \{i\}$	$\xrightarrow{\mathsf{m}_i, \mathsf{r}_i}$	Opening queries
	$\xleftarrow{\textsc{Dec}(c)}$	
Require $c \notin \{\mathsf{c}_1, \dots, \mathsf{c}_n\}$ $\mathsf{m} := \mathsf{DEC}_{\mathrm{sk}}(c)$	$\xrightarrow{\mathsf{m} \text{ or } \perp}$	Decryption queries

NTNU

SIM-SO-CCA Security - Real Game

Real-SO-CCA Game

		$\mathcal{A}$
$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{KG}$	$\xrightarrow{\mathrm{pk}}$	Choose distribution $\mathcal{D}$
	$\xleftarrow{\mathcal{D}}$	
$(\mathsf{m}_1, \ldots, \mathsf{m}_n) \leftarrow \mathcal{D}$ $(\mathsf{r}_1, \ldots, \mathsf{r}_n) \leftarrow \$$ $\forall i : \mathsf{c}_i := \mathsf{ENC}_{\mathrm{pk}}(\mathsf{m}_i, \mathsf{r}_i)$	$\xrightarrow{\mathsf{c}_1, \ldots, \mathsf{c}_n}$	
	$\xleftarrow{\textsc{Open}(i)}$	
$\mathcal{I} := \mathcal{I} \cup \{i\}$	$\xrightarrow{\mathsf{m}_i, \mathsf{r}_i}$	Opening queries
	$\xleftarrow{\textsc{Dec}(c)}$	
Require $c \notin \{\mathsf{c}_1, \ldots, \mathsf{c}_n\}$ $\mathsf{m} := \mathsf{DEC}_{\mathrm{sk}}(c)$	$\xrightarrow{\mathsf{m} \text{ or } \perp}$	Decryption queries
	$\xleftarrow{out_{\mathcal{A}}}$	Produce an output $out_{\mathcal{A}}$

SIM-SO-CCA Security - Real Game

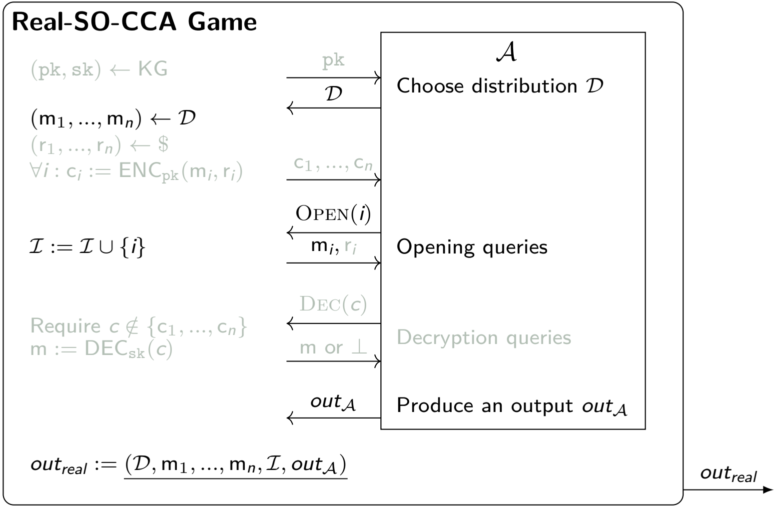
Real-SO-CCA Game

		$\mathcal{A}$
$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{KG}$	$\xrightarrow{\mathrm{pk}}$	Choose distribution $\mathcal{D}$
	$\xleftarrow{\mathcal{D}}$	
$(\mathsf{m}_1, \ldots, \mathsf{m}_n) \leftarrow \mathcal{D}$ $(\mathsf{r}_1, \ldots, \mathsf{r}_n) \leftarrow \$$ $\forall i : \mathsf{c}_i := \mathsf{ENC}_{\mathrm{pk}}(\mathsf{m}_i, \mathsf{r}_i)$	$\xrightarrow{\mathsf{c}_1, \ldots, \mathsf{c}_n}$	
	$\xleftarrow{\textsc{Open}(i)}$	
$\mathcal{I} := \mathcal{I} \cup \{i\}$	$\xrightarrow{\mathsf{m}_i, \mathsf{r}_i}$	Opening queries
	$\xleftarrow{\textsc{Dec}(c)}$	
Require $c \notin \{\mathsf{c}_1, \ldots, \mathsf{c}_n\}$ $\mathsf{m} := \mathsf{DEC}_{\mathrm{sk}}(c)$	$\xrightarrow{\mathsf{m} \text{ or } \perp}$	Decryption queries
	$\xleftarrow{out_{\mathcal{A}}}$	Produce an output $out_{\mathcal{A}}$

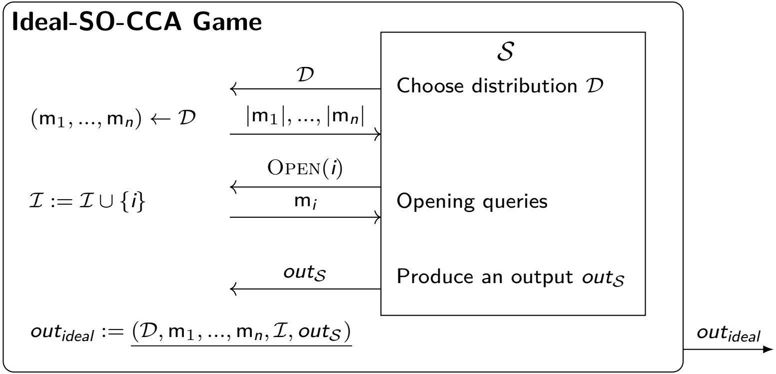
$out_{real} := \underline{(\mathcal{D}, \mathsf{m}_1, \ldots, \mathsf{m}_n, \mathcal{I}, out_{\mathcal{A}})}$

$\xrightarrow{out_{real}}$

SIM-SO-CCA Security - Real Game

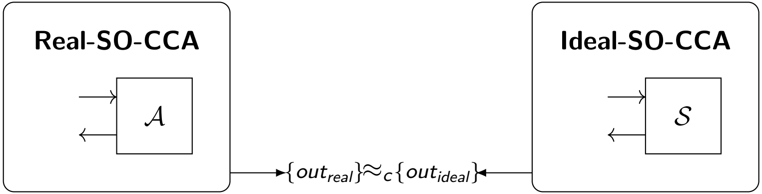


SIM-SO-CCA Security - Ideal Game



SIM-SO-CCA Security

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



- $\mathcal{S}$ simulates the "behavior" of $\mathcal{A}$ (e.g., they choose the same messages distribution, open the same ciphertexts, produce the same output...)

NTNU

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

$$\boxed{c_1} \quad \boxed{c_2} \quad \cdots \quad \boxed{c_i} \quad \cdots \quad \boxed{c_n}$$

SIM-SO-CCA

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

$$\boxed{c_1} \quad \boxed{c_2} \quad \cdots \quad \boxed{c_i} \quad \cdots \quad \boxed{c_n}$$

SIM-SO-CCA

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

$$\boxed{c_1} \quad \boxed{c_2} \quad \cdots \quad \boxed{c_i} \quad \cdots \quad \boxed{c_n}$$

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: $\epsilon_{\mathcal{A}} \leq L \cdot \epsilon_P$
  - $\epsilon_{\mathcal{A}}$: Advantage of breaking SO security
  - ϵ_P: Advantage of breaking some hard problem P
  - L: Security loss
- Tight security: $L = O(1)$.
- Non-tight: $L = O(n)$, $L = O(\ \#\mathrm{RO\ queries}\ )$,...

Tightness and Compactness

- Security reduction: $\epsilon_{\mathcal{A}} \leq L \cdot \epsilon_P$
  - $\epsilon_{\mathcal{A}}$: Advantage of breaking SO security
  - ϵ_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

Scheme	$\lvert\text{public key}\rvert_{\mathbb{G}}$	$\lvert\text{ciphertext}\rvert_{\mathbb{G}}$
[HJR16]	$O(\ell^2)$	$O(1)$
[LLHG18]	$O(1)$	$O(\ell)$
[JL21]	$O(\ell^2)$	$O(\ell/\log\lambda)$

* λ: security parameter
* ℓ: Length of message
* $|\cdot|_{\mathbb{G}}$: The number of group element

NTNU

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

Scheme	$\lvert\text{public key}\rvert_{\mathbb{G}}$	$\lvert\text{ciphertext}\rvert_{\mathbb{G}}$
[HJR16]	$O(\ell^2)$	$O(1)$
[LLHG18]	$O(1)$	$O(\ell)$
[JL21]	$O(\ell^2)$	$O(\ell/\log\lambda)$

* λ: security parameter
* ℓ: Length of message
* $\lvert\cdot\rvert_{\mathbb{G}}$: 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 tranformation [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]

- $\mathtt{pk} = g^x \in \mathbb{G},\ \mathtt{sk} = x \in \mathbb{Z}_p$

Our Contributions

The DHIES scheme in [HJKS15]

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

Our Contributions

The DHIES scheme in [HJKS15]

- $\mathtt{pk} = g^x \in \mathbb{G}$, $\mathtt{sk} = x \in \mathbb{Z}_p$
- Encrypt a plaintext m:
  1. $r \leftarrow \mathbb{Z}_p$
  2. $R := g^r, Z = \mathtt{pk}^r$
  3. $(K, k) = H(R,\ Z)$ (where H is a hash function)
  4. $d = K \oplus \mathrm{m}$
  5. $t = \mathrm{MAC}_k(R, d)$
  6. Output (R, d, t)

Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:

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

- Randomness: $r \leftarrow \mathbb{Z}_p$

Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:

$$\left(R = g^r,\ d = K \oplus \mathrm{m},\ t = \mathrm{MAC}_k(R, d)\right) \text{ , where } (K, k) = H(R, \mathtt{pk}^r)$$

- Randomness: $r \leftarrow \mathbb{Z}_p$

Proof Sketch (SIM-SO-CCA security).

- Use n-stDH: Given $\left(X, \{R_i\}_{i \in [n]}\right)$ and DDH_X oracle, find $\mathrm{CDH}(X, R_i)$.

Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:

$$\left(R = g^r,\ d = K \oplus \mathrm{m},\ t = \mathrm{MAC}_k(R, d)\right)\ \text{, where } (K, k) = H(R, \mathtt{pk}^r)$$

- Randomness: $r \leftarrow \mathbb{Z}_p$

Proof Sketch (SIM-SO-CCA security).

- Use n-stDH: Given $\left(X, \{R_i\}_{i\in[n]}\right)$ and DDH_X oracle, find $\mathrm{CDH}(X, R_i)$.
- n challenge ciphertexts: $(g^{r_1}, d_1, t_1), \ldots, (g^{r_n}, d_n, t_n)$.

Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:

$$\left(R = g^r,\ d = K \oplus \mathrm{m},\ t = \mathrm{MAC}_k(R, d)\right)\ \text{, where } (K, k) = H(R, \mathtt{pk}^r)$$

- Randomness: $r \leftarrow \mathbb{Z}_p$

Proof Sketch (SIM-SO-CCA security).

- Use n-stDH: Given $\left(X, \{R_i\}_{i \in [n]}\right)$ and DDH_X oracle, find $\mathrm{CDH}(X, R_i)$.
- n challenge ciphertexts: $(R_1, d_1, t_1), \ldots, (R_n, d_n, t_n)$.

Our Contributions

The DHIES scheme in [HJKS15]

- The ciphertext has this form:

$$\left(R = g^r,\ d = K \oplus \mathrm{m},\ t = \mathrm{MAC}_k(R, d)\right) \text{ , where } (K, k) = H(R, \mathtt{pk}^r)$$

- Randomness: $r \leftarrow \mathbb{Z}_p$

Proof Sketch (SIM-SO-CCA security).

- Use n-stDH: Given $\left(X, \{R_i\}_{i \in [n]}\right)$ and DDH_X oracle, find $\mathrm{CDH}(X, R_i)$.
- 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:

$$\left(R = g^r,\ d = K \oplus \mathrm{m},\ t = \mathrm{MAC}_k(R, d)\right)\ ,\ \text{where } (K, k) = H(R, \mathtt{pk}^r)$$

- Randomness: $r \leftarrow \mathbb{Z}_p$

Proof Sketch (SIM-SO-CCA security).

- Use n-stDH: Given $\left(X, \{R_i\}_{i\in[n]}\right)$ and DDH_X oracle, find $\mathrm{CDH}(X, R_i)$.
- 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	Randomness
DHIES:	$(R = g^r,\ d = \mathsf{m} \oplus K,\ t = \mathsf{MAC}_k(R))$	$r \leftarrow \mathbb{Z}_p$

Our Contributions

Our approach: "Dual" Naor-Yung technique

	Ciphertext	Randomness
DHIES:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0 = g^{r_0}, R_1 = g^{r_1},\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	

NTNU

Our Contributions

Our approach: "Dual" Naor-Yung technique

	Ciphertext	Randomness
DHIES:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0 = g^{r_0}, R_1 = g^{r_1},\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	

- (K, k) is derived from $CDH(\mathtt{pk}, R_0)$ or $CDH(\mathtt{pk}, R_1)$

Our Contributions

Our approach: "Dual" Naor-Yung technique

	Ciphertext	Randomness
DHIES:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0 = g^{r_0}, R_1 = g^{r_1},\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	

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

Our Contributions

Our approach: "Dual" Naor-Yung technique

	Ciphertext	Randomness
DHIES:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathsf{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0 = g^{r_0}, R_1 = g^{r_1},\ d = \mathrm{m} \oplus K,\ t = \mathsf{MAC}_k(R_0, R_1, d)\big)$	

- $(K, k) = H(b, R_0, R_1, \mathrm{pk}^{r_b})$, where $b \leftarrow \{0, 1\}$
- Forget the dlog: Oblivious randomness

Our Contributions

Our approach: “Dual” Naor-Yung technique

	Ciphertext	**Randomness**
DHIES:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0 = g^{r_0}, R_1 = g^{r_1},\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	

- $(K, k) = H(b, R_0, R_1, \mathtt{pk}^{r_b})$, 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

	Ciphertext	Randomness
DHIES:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0 = g^{r_0}, R_1 = g^{r_1},\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	

- $(K, k) = H(b, R_0, R_1, \mathrm{pk}^{r_b})$, 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...)

Our Contributions

Our approach: "Dual" Naor-Yung technique

	Ciphertext	**Randomness**
Original:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0, R_1,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	$b \leftarrow \{0,1\}, r_b \leftarrow \mathbb{Z}_p$ $R_{1-b} \leftarrow \mathbb{G}$

- $(K, k) = H(b, R_0, R_1, \mathrm{pk}^{r_b})$, where $b \leftarrow \{0,1\}$ and $R_b := g^{r_b}$
- Forget the dlog: Oblivious randomness
- Use oblivious randomness to respond OPEN queries...

NTNU

Our Contributions

Our approach: "Dual" Naor-Yung technique

	Ciphertext	**Randomness**
Original:	$(R = g^r,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R, d))$	$r \leftarrow \mathbb{Z}_p$
Our:	$\big(R_0, R_1,\ d = \mathrm{m} \oplus K,\ t = \mathrm{MAC}_k(R_0, R_1, d)\big)$	$b \leftarrow \{0,1\}, r_b \leftarrow \mathbb{Z}_p$ $R_{1-b} \leftarrow \mathbb{G}$

- $(K, k) = H(b, R_0, R_1, \mathrm{pk}^{r_b})$, 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

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

Proof sketch

- Use n-stDH assumption...
- Embed challenge into R_0 or R_1...

Our Contributions

Our approach: “Dual” Naor-Yung technique

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

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?	$\lvert c\rvert_{\mathbb{G}}$	$\lvert \mathtt{pk}\rvert_{\mathbb{G}}$	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

Q & A

Thank you!