Anonymous Public Key Encryption under Corruptions

Zhengan Huang

Peng Cheng Laboratory

Junzuo Lai

Jinan University

Shuai Han

Shanghai Jiao Tong University

Lin Lyu

Bergische Universität Wuppertal

Jian Weng

Jinan University

ASIACRYPT 2022

Background

- For PKE under corruptions, both the secret keys and messages could be leaked.
- The first notion of anonymity for PKE under corruptions (ANON-COR security) is proposed by Benhamouda et al. [BGG+20, TCC].
- In [BGG+20, TCC], ANON-COR secure and RSO secure PKE is employed to build an Evolving-Committee proactive secret sharing (ECPSS) Scheme.

Background

- For PKE under corruptions, both the secret keys and messages could be leaked.
- The first notion of anonymity for PKE under corruptions (ANON-COR security) is proposed by Benhamouda et al. [BGG+20, TCC].
- In [BGG+20, TCC], ANON-COR secure and RSO secure PKE is employed to build an Evolving-Committee proactive secret sharing (ECPSS) Scheme.

Unfortunately …

- No known PKE achieves ANON-COR security
- Non-adaptive: the adversary is *not* allowed to obtain any sk *before* seeing ct
- Single-challenge: each pk is used to encrypt a single message

Background

- For PKE under corruptions, both the secret keys and messages could be leaked.
- The first notion of anonymity for PKE under corruptions (ANON-COR security) is proposed by Benhamouda et al. [BGG+20, TCC].
- In [BGG+20, TCC], ANON-COR secure and RSO secure PKE is employed to build an Evolving-Committee proactive secret sharing (ECPSS) Scheme.

Unfortunately …

- No known PKE achieves ANON-COR security
- N
  se
- Si

- Confidentiality: RSO security [HPW15] ($\mathcal{A}$ is able to open a specified subset of the challenge ciphertexts)
- Anonymity: ANON-COR security ($\mathcal{A}$ is **not** able to specify some challenge ciphertexts and open them)

Background

- For PKE under corruptions, both the secret keys and messages could be leaked.
- The first notion of anonymity for PKE under corruptions (ANON-COR security) is proposed by Benhamouda et al. [BGG+20, TCC].
- In [BGG+20, TCC], ANON-COR secure and RSO secure PKE is employed to build an Evolving-Committee proactive secret sharing (ECPSS) Scheme.

Unfortunately …

- No known PKE achieves ANON-COR security
- Non-adaptive: the adversary is *not* allowed to obtain any sk *before* seeing ct
- Single-challenge: each pk is used to encrypt a single message
- ANON-COR and RSO are formalized under different types of corruptions

Our Contributions

- **Define ANON-RSO$_k$&C security for PKE**

  (ANON-RSO$_k$&C security: ANONymity under Receiver Selective Opening attacks (in the k-challenge setting) and adaptive user Corruptions)

- **Define SIM-RSO$_k$&C security for PKE**

  (SIM-RSO$_k$&C security: confidentiality under the same types of corruptions like ANON-RSOk&C security)

- **Show a framework of constructing PKE achieving both ANON-RSO$_k$&C-CCA and SIM-RSO$_k$&C-CCA security**

Definition: ANON-RSO$_k$&C-CPA security

Real Game

$pk_1, \cdots, pk_n$

$\mathcal{D}_{\mathrm{pk}}, (m_{j,\gamma})_{j\in[t],\gamma\in[k]}$

$(i_j)_{j\in[t]} \leftarrow \mathcal{D}_{\mathrm{pk}}$

$(c_{j,\gamma} \leftarrow \mathbf{Enc}(pk_{i_j}, m_{j,\gamma}))_{j\in[t],\gamma\in[k]}$

$(c_{j,\gamma})_{j\in[t],\gamma\in[k]}$

out

Return $((i_j, (m_{j,\gamma})_{\gamma\in[k]})_{j\in[t]}, \mathcal{D}_{\mathrm{pk}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out)$

Definition: ANON-RSO$_k$&C-CPA security

Real Game

$pk_1, \cdots, pk_n$ →

$\mathcal{O}_{\mathbf{cor}}(\cdot)$

$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

← i

← sk_i

$(i_j)_{j\in[t]} \leftarrow \mathcal{D}_{\mathrm{pk}}$

← $\mathcal{D}_{\mathrm{pk}}, (m_{j,\gamma})_{j\in[t],\gamma\in[k]}$

$(c_{j,\gamma} \leftarrow \mathbf{Enc}(pk_{i_j}, m_{j,\gamma}))_{j\in[t],\gamma\in[k]}$

$(c_{j,\gamma})_{j\in[t],\gamma\in[k]}$ →

$\mathcal{O}_{\mathbf{cor}}(\cdot)$

$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

← i

← sk_i

$\mathcal{O}_{\mathbf{open}}(\cdot)$

$I_{\mathrm{op}} = I_{\mathrm{op}} \cup \{j\}$

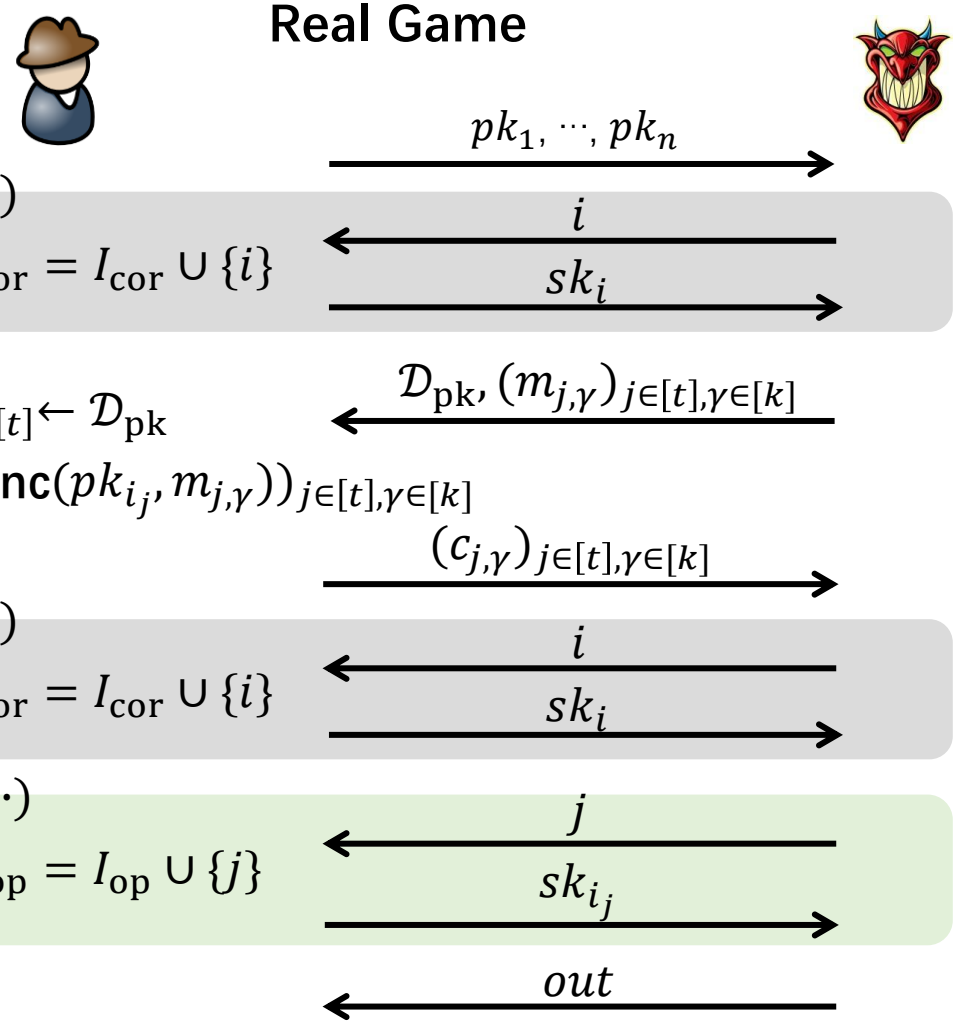
← j

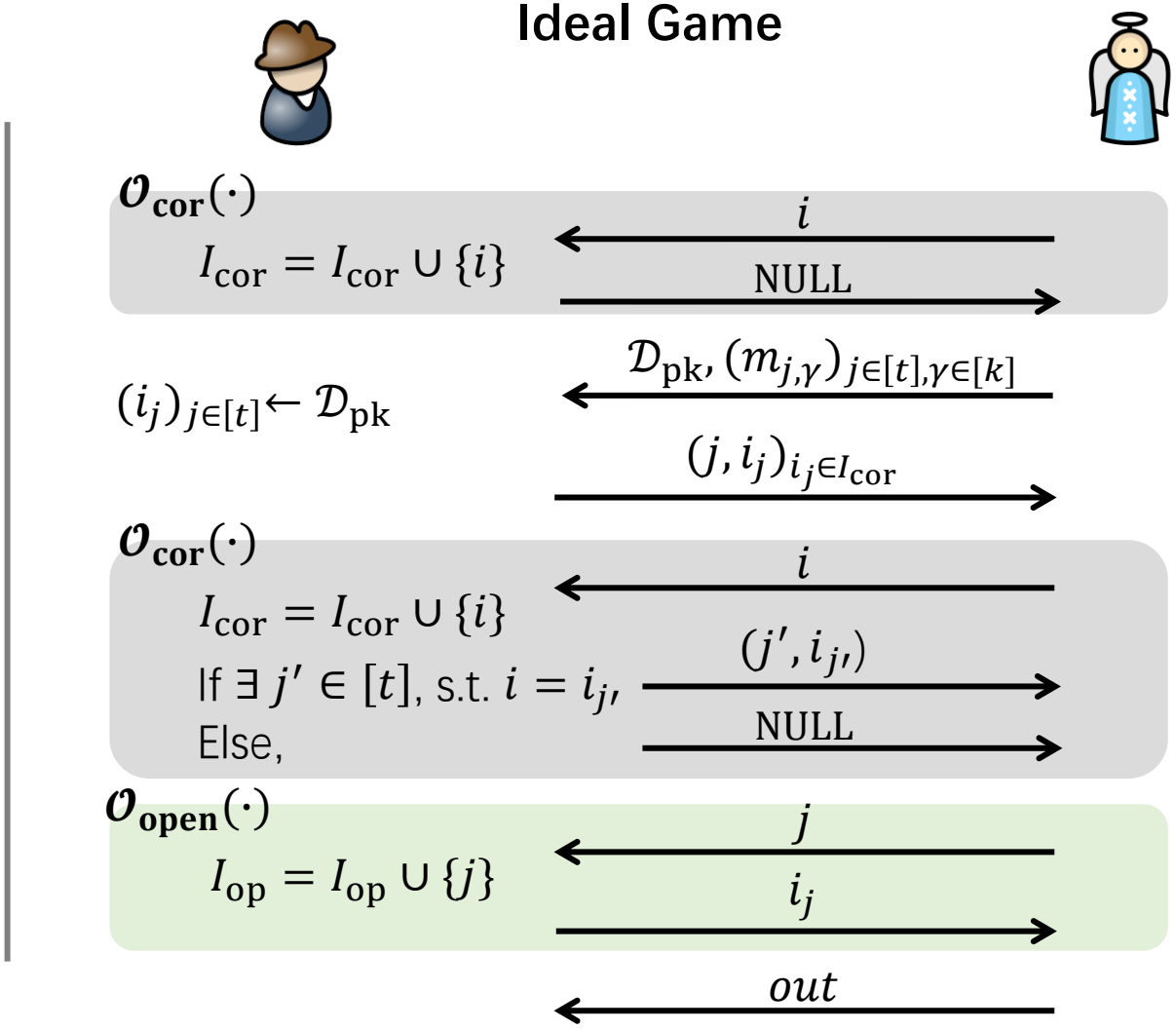
← sk_{i_j}

← out

Return $((i_j, (m_{j,\gamma})_{\gamma\in[k]})_{j\in[t]}, \mathcal{D}_{\mathrm{pk}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out)$

Definition: ANON-RSO$_k$&C-CPA security





Return $((i_j, (m_{j,\gamma})_{\gamma\in[k]})_{j\in[t]}, \mathcal{D}_{\mathrm{pk}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out)$

$\approx$

Return $((i_j, (m_{j,\gamma})_{\gamma\in[k]})_{j\in[t]}, \mathcal{D}_{\mathrm{pk}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out)$

Definition: SIM-RSOk&C-CPA security (confidentiality)

Real Game

$pk_1, \cdots, pk_n$

$\mathcal{O}_{\mathrm{cor}}(\cdot)$

$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

i

sk_i

$\mathcal{D}_{\mathrm{m}}$

$(m_{i,\gamma})_{i\in[n],\gamma\in[k]} \leftarrow \mathcal{D}_{\mathrm{m}}$

$(c_{i,\gamma} \leftarrow \mathsf{Enc}(pk_i, m_{i,\gamma}))_{i\in[n],\gamma\in[k]}$

$(c_{i,\gamma})_{i\in[n],\gamma\in[k]}$

$\mathcal{O}_{\mathrm{cor}}(\cdot)$

$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

i

sk_i

$\mathcal{O}_{\mathrm{open}}(\cdot)$

$I_{\mathrm{op}} = I_{\mathrm{op}} \cup \{i\}$

i

$sk_i, (m_{i,\gamma})_{\gamma\in[k]}$

out

Return $\left((m_{i,\gamma})_{i\in[n],\gamma\in[k]}, \mathcal{D}_{\mathrm{m}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out\right)$

$\approx$

Ideal Game

$\mathcal{O}_{\mathrm{cor}}(\cdot)$

$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

i

NULL

$\mathcal{D}_{\mathrm{m}}$

$(m_{i,\gamma})_{i\in[n],\gamma\in[k]} \leftarrow \mathcal{D}_{\mathrm{m}}$

$(i, (m_{i,\gamma})_{\gamma\in[k]})_{i\in I_{\mathrm{cor}}}$

$\mathcal{O}_{\mathrm{cor}}(\cdot)$

$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

i

$(m_{i,\gamma})_{\gamma\in[k]}$

$\mathcal{O}_{\mathrm{open}}(\cdot)$

$I_{\mathrm{op}} = I_{\mathrm{op}} \cup \{i\}$

i

$(m_{i,\gamma})_{\gamma\in[k]}$

out

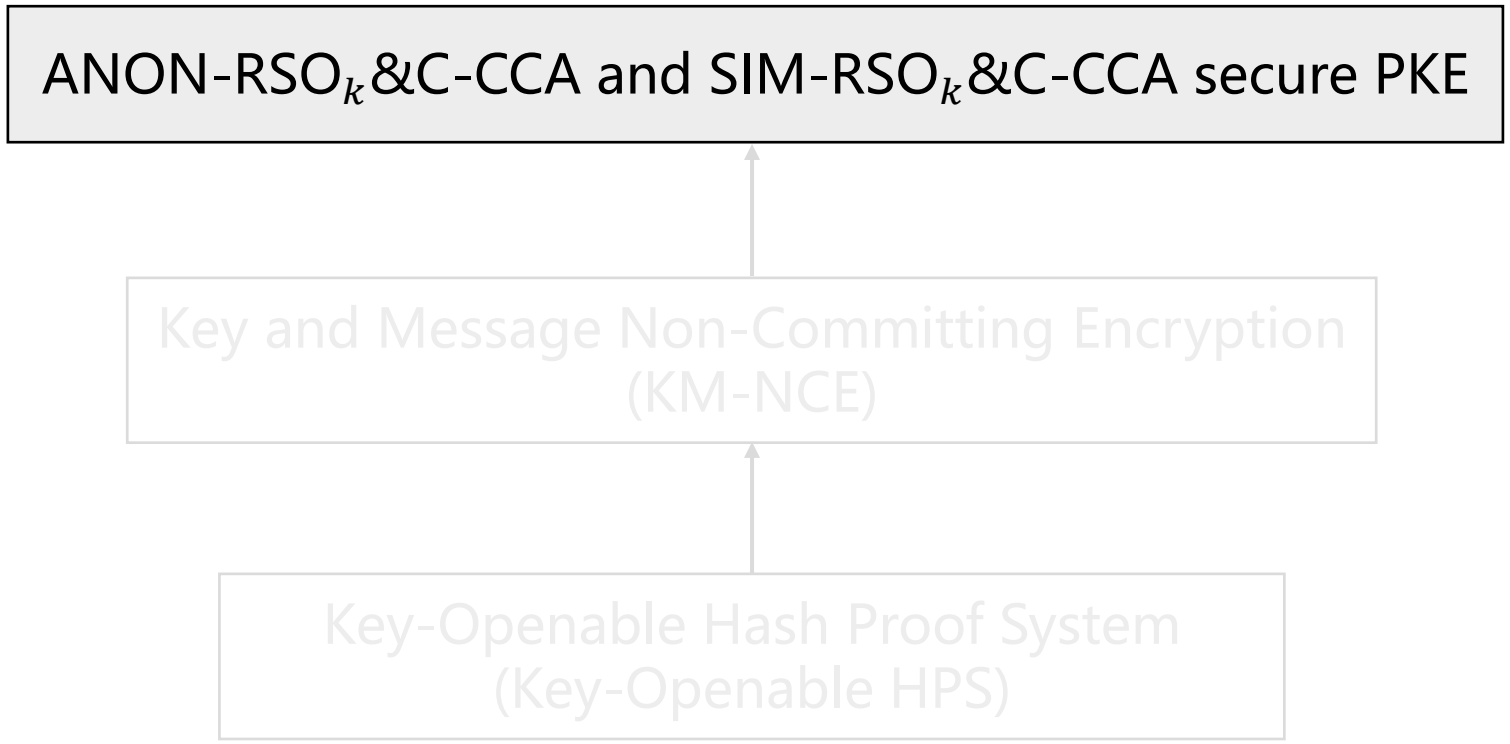
Return $\left((m_{i,\gamma})_{i\in[n],\gamma\in[k]}, \mathcal{D}_{\mathrm{m}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out\right)$

Relations among security notions

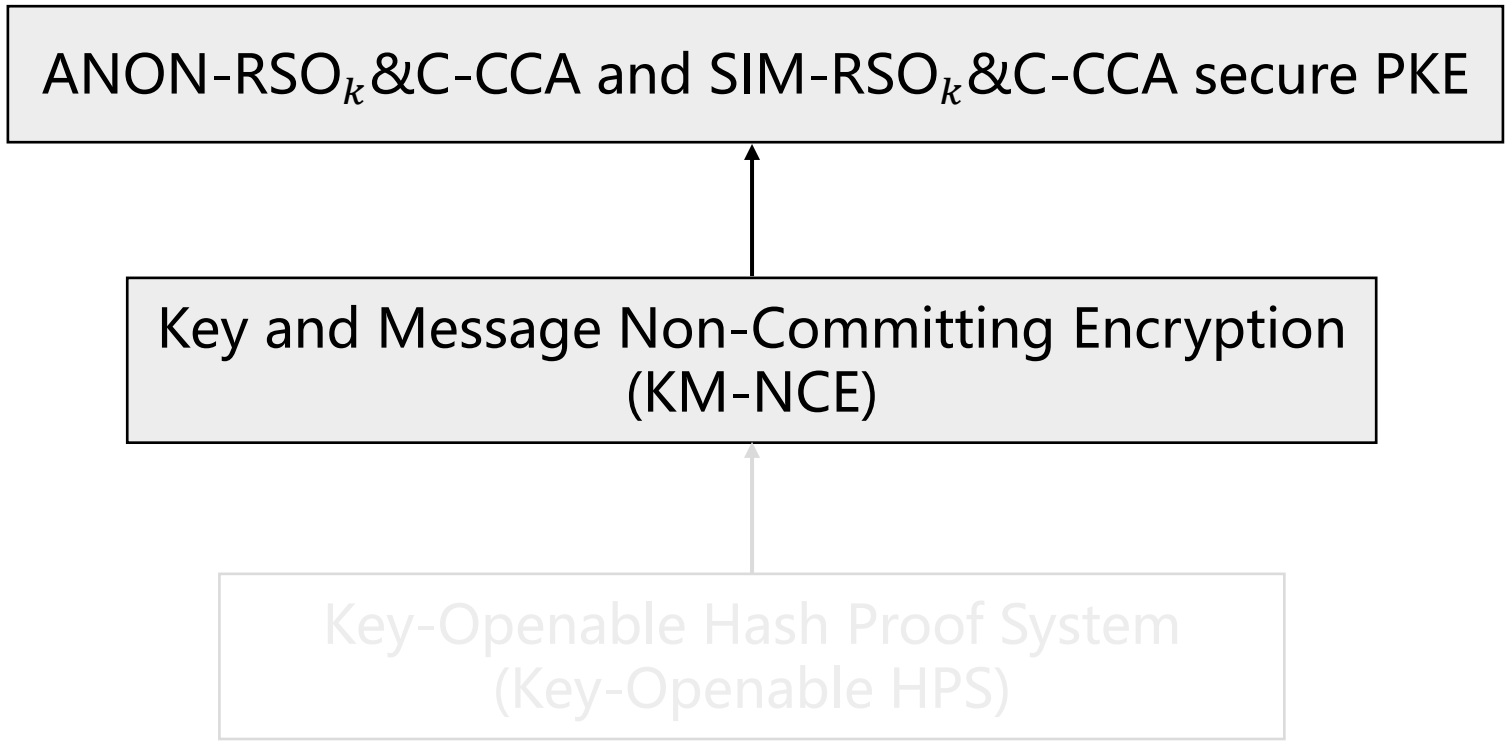
- **Anonymity:** ANON-RSOk&C-CPA ⇒ ANON-COR ([BGG+20, TCC])

- **Confidentiality:** SIM-RSOk&C-ATK ⇒ SIM-RSOk-ATK ([YLH+20, ASIACRYPT])

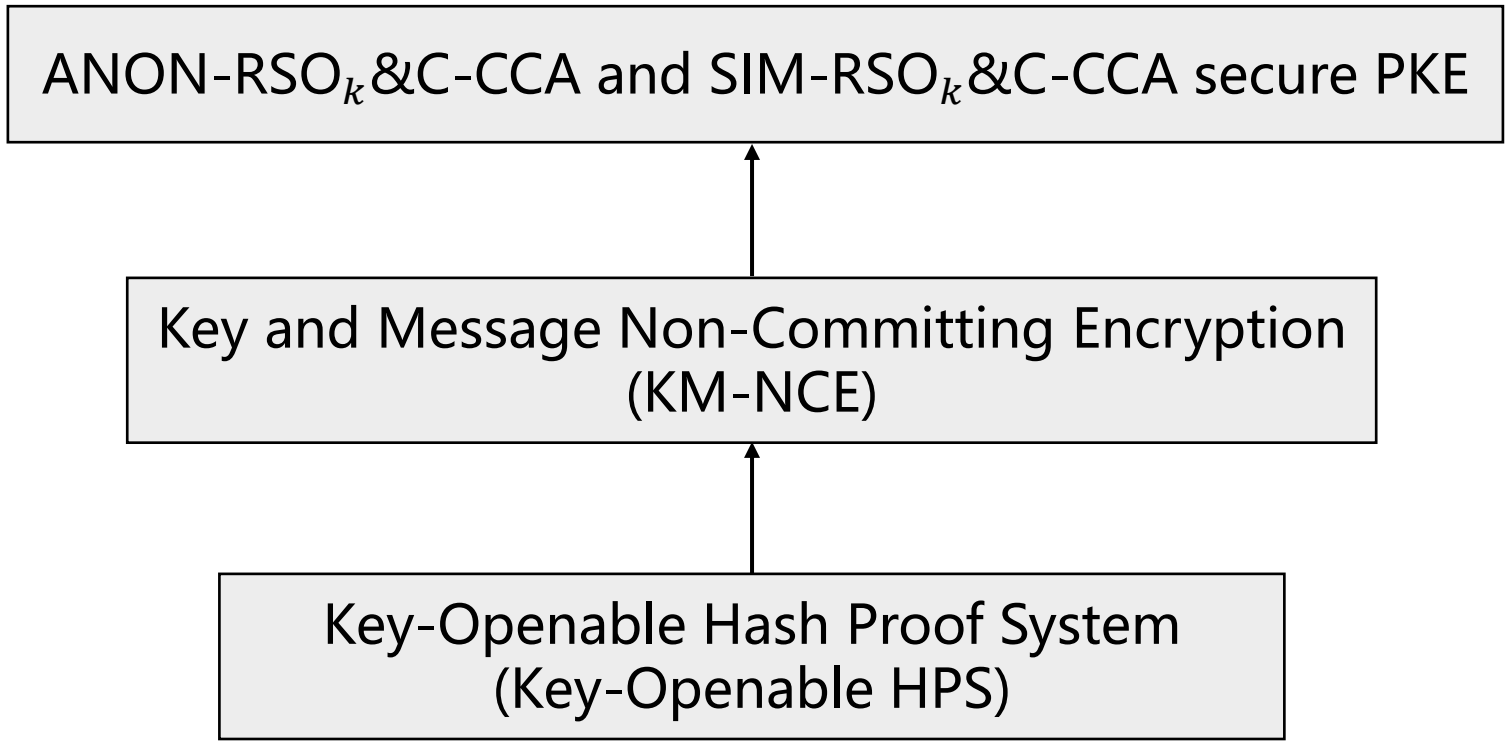
Construction – technical overview



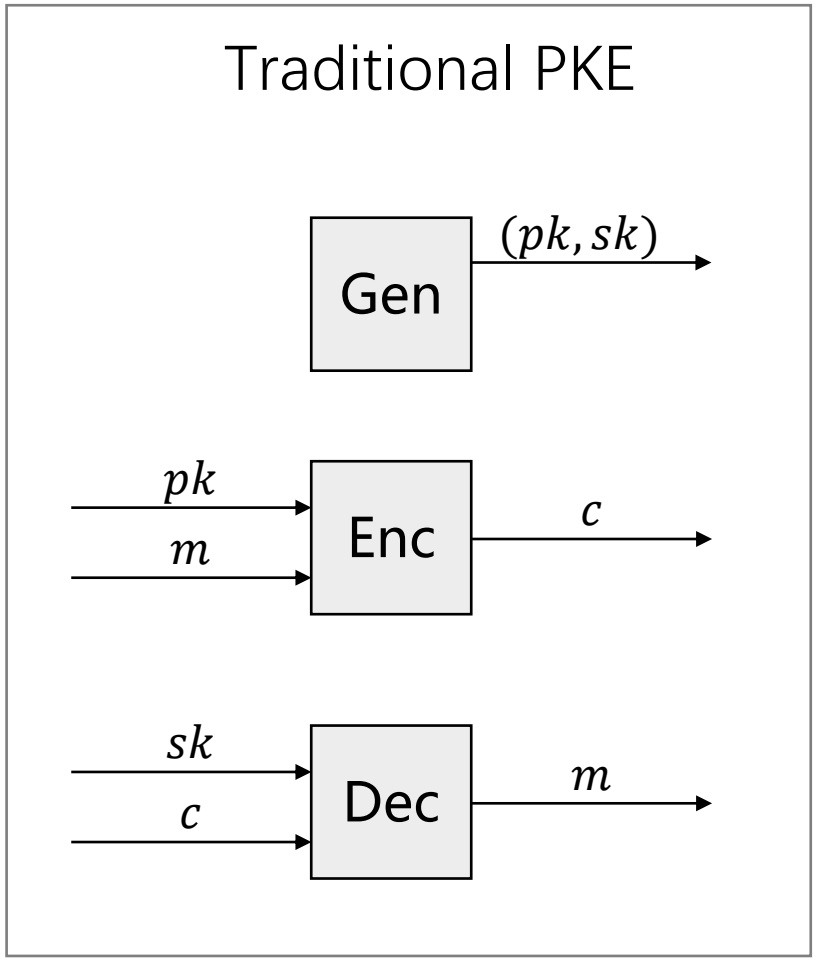
Construction – technical overview



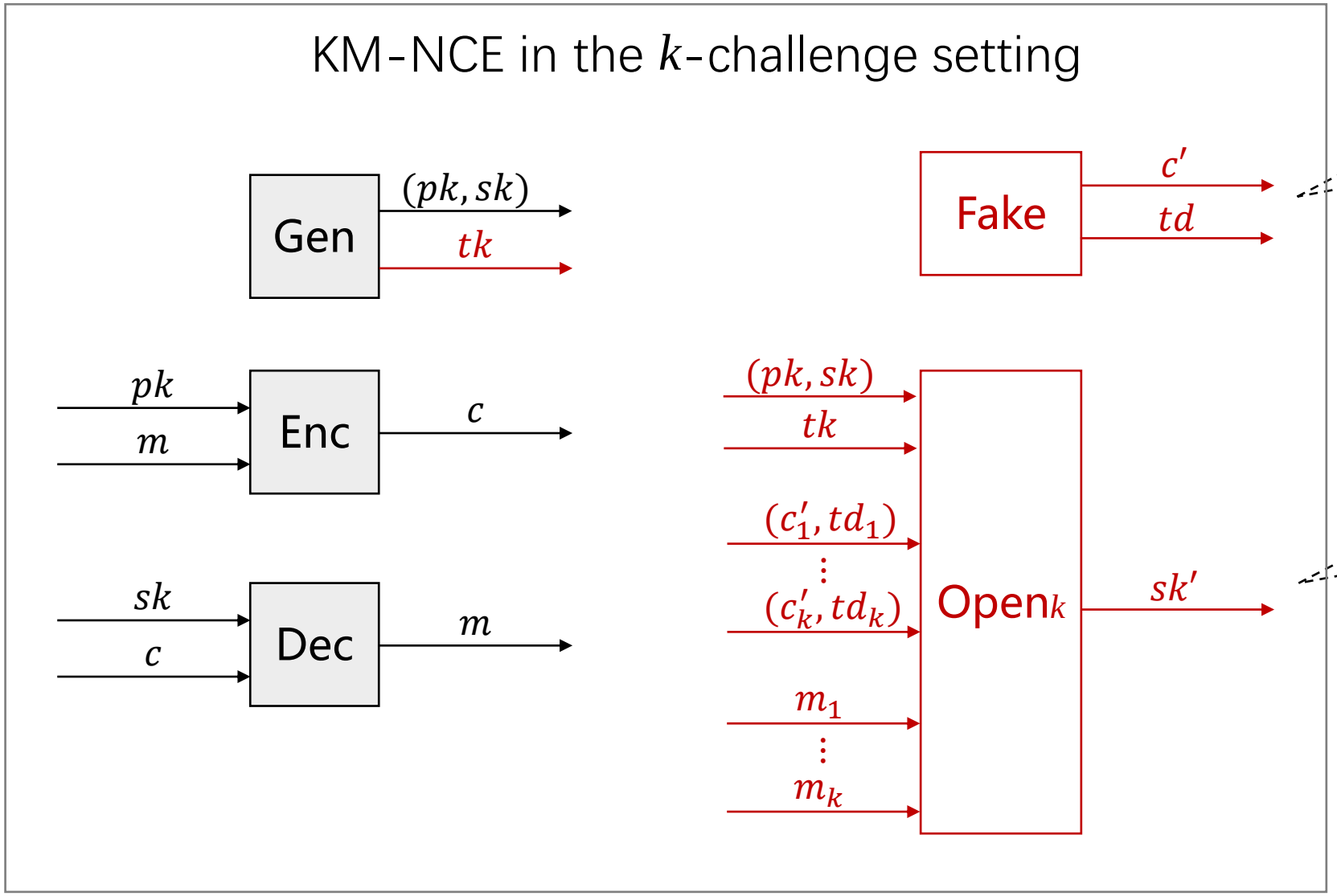
Construction – technical overview



Key and Message Non-Committing Encryption



Key and Message Non-Committing Encryption



Generate fake ciphertexts without pk.

Open k fake ciphertexts to any k messages.

KM-NCE is an extension of Receiver NCE [CHK05, HPW15, HKM+18]

Security requirements of KM-NCE

KMNC$_k$-CPA security

For any $m_1, \dots, m_k$, for $(pk, sk, tk) \leftarrow \mathbf{Gen}(\lambda)$,

- k real ciphertexts:

  $(c_\gamma \leftarrow \mathbf{Enc}(pk, m_\gamma))_{\gamma \in [k]}$

- k fake ciphertexts and secret keys:

  $((c_\gamma^{\mathrm{fk}}, td_\gamma) \leftarrow \mathbf{Fake}(\lambda))_{\gamma \in [k]}$

  $sk^{\mathrm{op}} \leftarrow \mathbf{Open}_k(tk, pk, sk, (c_\gamma^{\mathrm{fk}}, td_\gamma, m_\gamma)_{\gamma \in [k]})$

$$(pk, sk, c_1, \dots, c_k) \approx (pk, sk^{\mathrm{op}}, c_1^{\mathrm{fk}}, \dots, c_k^{\mathrm{fk}})$$

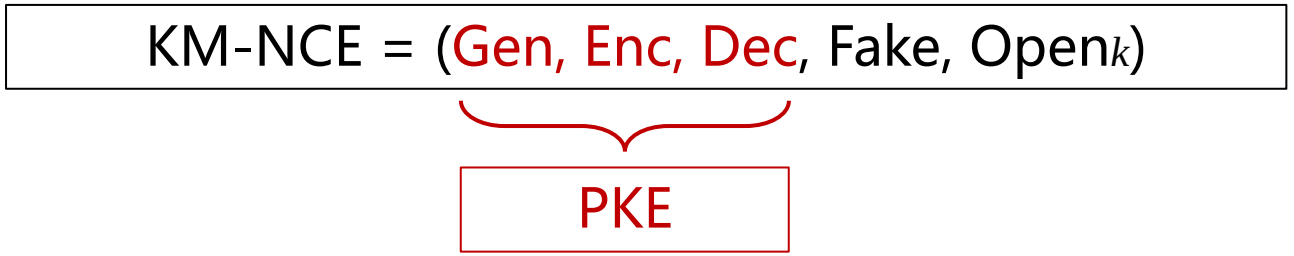
- KMNC$_k$-CCA security is similarly defined.

Robustness

For $(pk, sk, tk) \leftarrow \mathbf{Gen}(\lambda)$, $(c, td) \leftarrow \mathbf{Fake}(\lambda)$,

$\Pr[\mathbf{Dec}(sk, c) = \perp]$ is overwhelming.

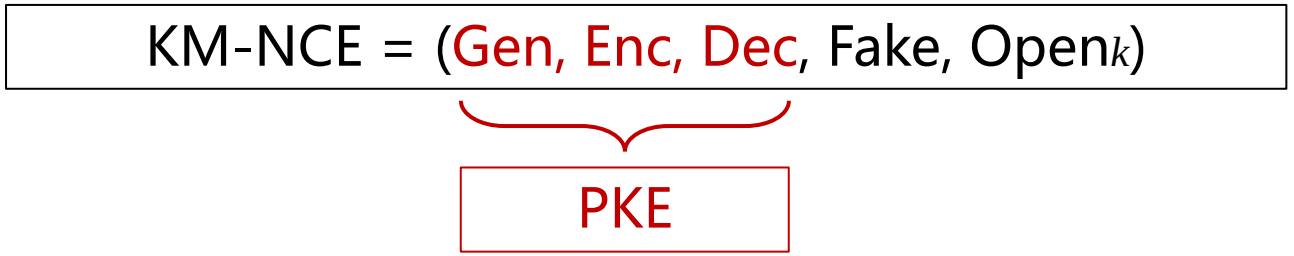
ANON / SIM -RSO$_k$&C secure PKE from KM-NCE



Theorem 1

- If **KM-NCE** is KMNC$_k$-CPA secure, then **PKE** is ANON-RSO$_k$&C-CPA secure and SIM-RSO$_k$&C-CPA secure .
- If **KM-NCE** is KMNC$_k$-CCA secure and robust, then **PKE** is ANON-RSO$_k$&C-CCA secure and SIM-RSO$_k$&C-CCA secure .

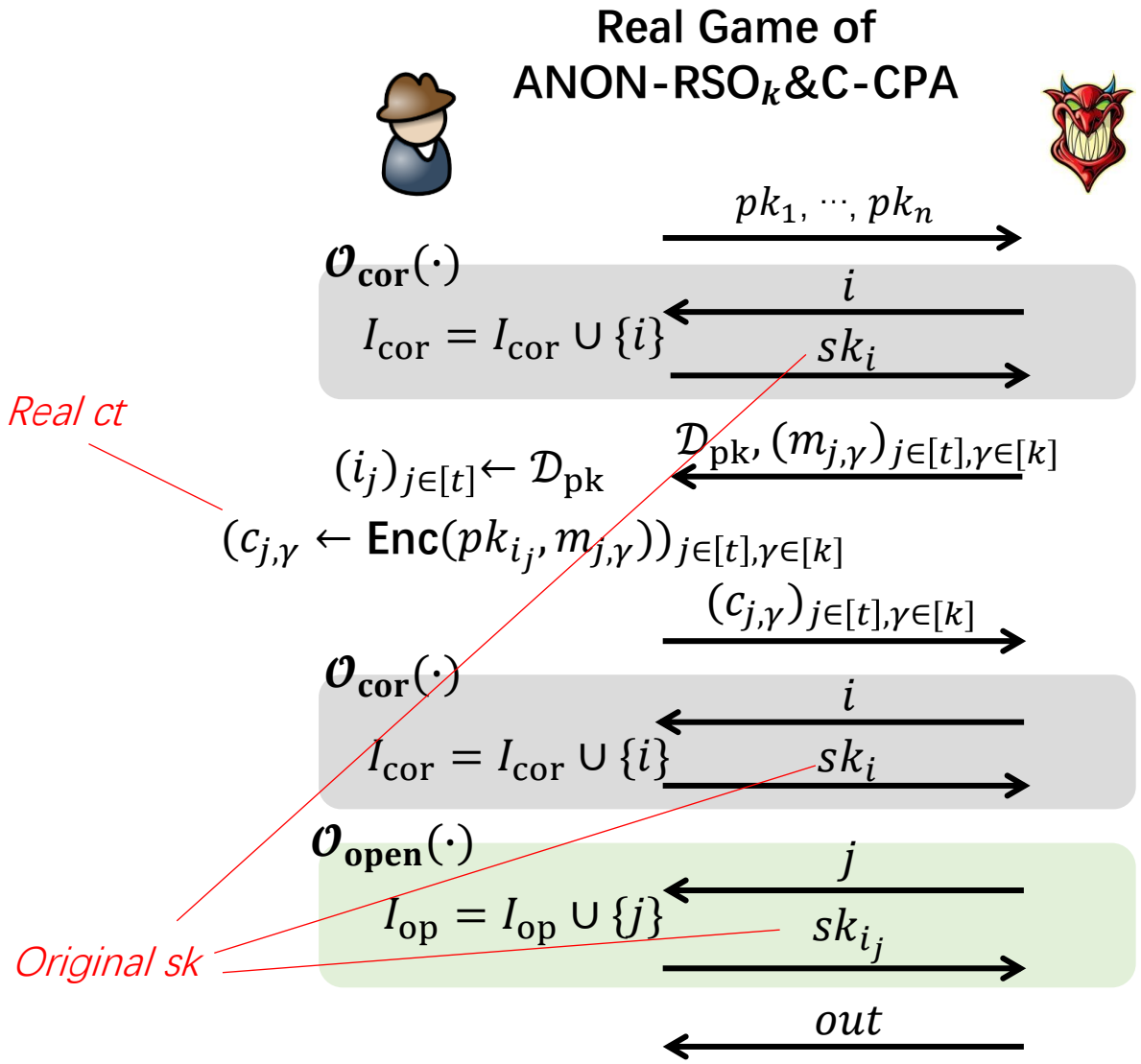
ANON / SIM -RSO$_k$&C secure PKE from KM-NCE



Theorem 1

- If **KM-NCE** is KMNC$_k$-CPA secure, then **PKE** is **ANON-RSO$_k$&C-CPA** secure and SIM-RSO$_k$&C-CPA secure .
- If **KM-NCE** is KMNC$_k$-CCA secure and robust, then **PKE** is ANON-RSO$_k$&C-CCA secure and SIM-RSO$_k$&C-CCA secure .

Proof: ANON-RSO$_k$&C-CPA secure PKE from KM-NCE



Proof: ANON-RSO$_k$&C-CPA secure PKE from KM-NCE

Ideal Game of ANON-RSO$_k$&C-CPA

$\mathcal{O}_{\mathbf{cor}}(\cdot)$
$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$

i ←
→ NULL

$(i_j)_{j\in[t]} \leftarrow \mathcal{D}_{\mathrm{pk}}$

$\mathcal{D}_{\mathrm{pk}}, (m_{j,\gamma})_{j\in[t],\gamma\in[k]}$ ←
$(j, i_j)_{i_j \in I_{\mathrm{cor}}}$ →

$\mathcal{O}_{\mathbf{cor}}(\cdot)$
$I_{\mathrm{cor}} = I_{\mathrm{cor}} \cup \{i\}$
If $\exists\, j' \in [t]$, s.t. $i = i_{j'}$,
Else,

i ←
$(j', i_{j'})$ →
→ NULL

$\mathcal{O}_{\mathbf{open}}(\cdot)$
$I_{\mathrm{op}} = I_{\mathrm{op}} \cup \{j\}$

j ←
i_j →
out ←

Return $((i_j, (m_{j,\gamma})_{\gamma\in[k]})_{j\in[t]}, \mathcal{D}_{\mathrm{pk}}, I_{\mathrm{cor}}, I_{\mathrm{op}}, out)$

$((pk_i, sk_i, tk_i) \leftarrow \mathrm{Gen}(\lambda))_{i\in[n]}$

For $j \in [t]$:
If $i_j \in I_{\mathrm{cor}}$: $(c_{j,\gamma} \leftarrow \mathbf{Enc}(pk_{i_j}, m_{j,\gamma}))_{\gamma\in[k]}$ — *Real ct*
If $i_j \notin I_{\mathrm{cor}}$: $(c_{j,\gamma} \leftarrow \mathbf{Fake}(\lambda))_{\gamma\in[k]}$ — *Fake ct*

If $(c_{j,\gamma})_{\gamma\in[k]}$ (or $(c_{j',\gamma})_{\gamma\in[k]}$) are real ct:
return sk_{i_j} (or $sk_{i_{j'}}$) as a response
If $(c_{j,\gamma})_{\gamma\in[k]}$ (or $(c_{j',\gamma})_{\gamma\in[k]}$) are fake ct:
return sk' generated with **Open**$_k$ as a response

Real Game of ANON-RSO$_k$&C-CPA

$pk_1, \cdots, pk_n$ →

$\mathcal{O}_{\mathbf{cor}}(\cdot)$
i ←
sk_i →

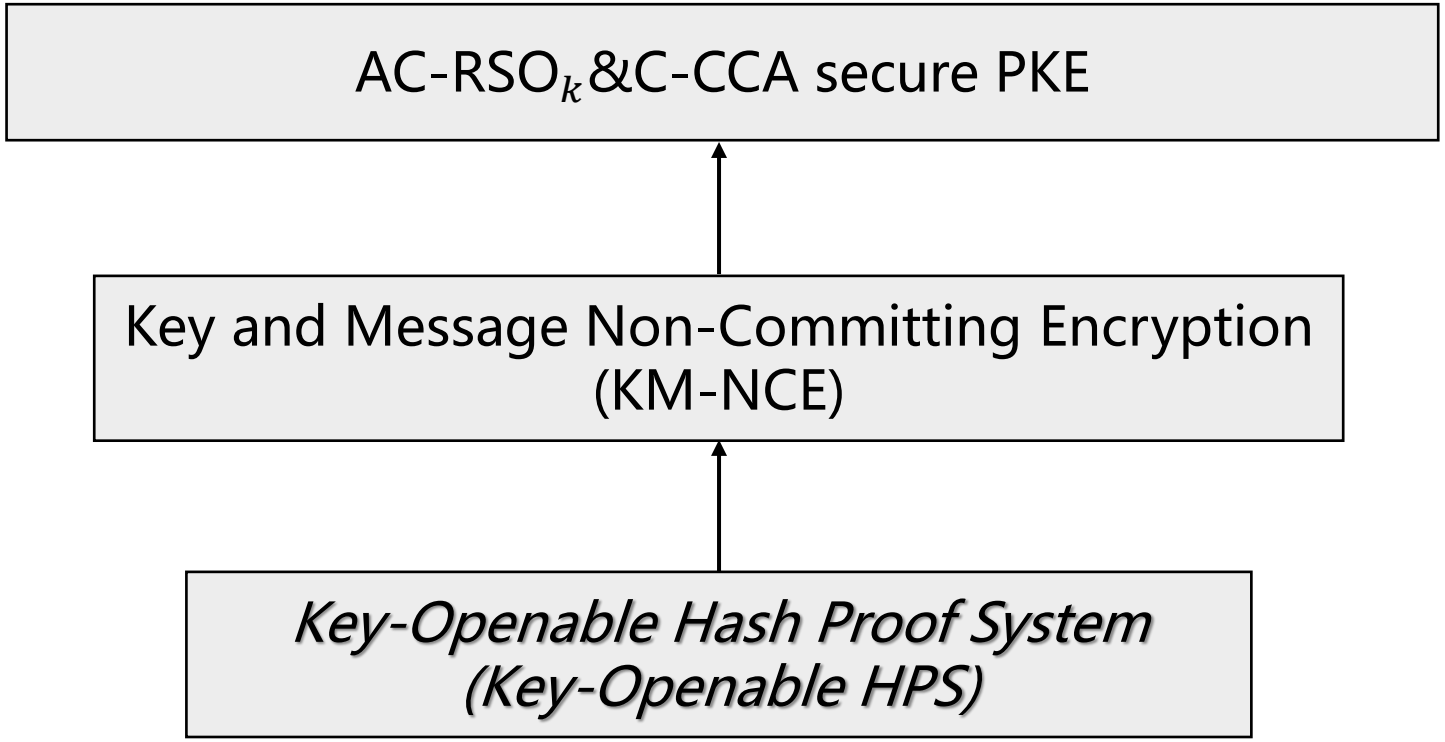
$\mathcal{D}_{\mathrm{pk}}, (m_{j,\gamma})_{j\in[t],\gamma\in[k]}$ ←

$(c_{j,\gamma})_{j\in[t],\gamma\in[k]}$ →

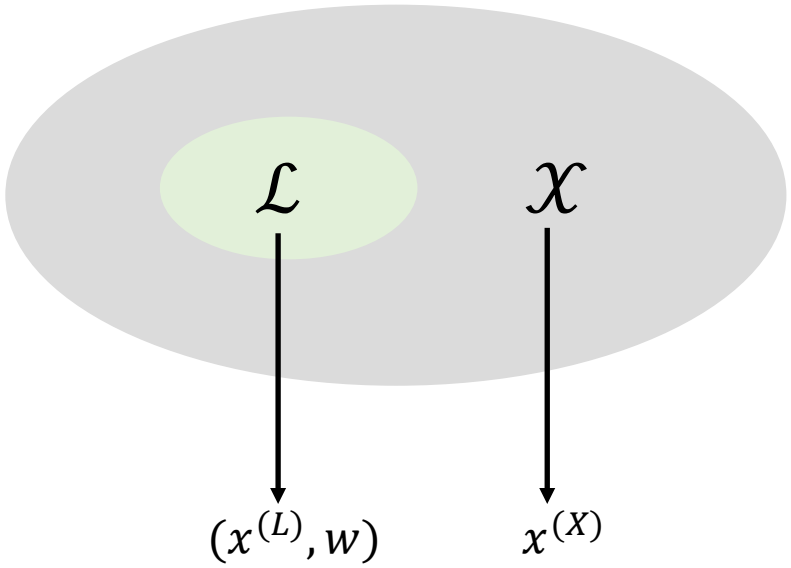
$\mathcal{O}_{\mathbf{cor}}(\cdot)$
i ←
sk_i →

$\mathcal{O}_{\mathbf{open}}(\cdot)$
j ←
sk_{i_j} →
out ←

Construction – technical overview



Key-Openable Hash Proof System



$Par(1^\lambda) \to (par, td)$, $KeyGen(par) \to (sk, pk)$

$Priv(sk, x) \to \pi$, $Pub(pk, x, w) \to \pi$

$HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma, r_{\pi_\gamma}\right)_{\gamma \in [k]}) \to sk'/\perp$

Projectivity: For any $(x, w) \leftarrow \mathcal{L}$, $Priv\,(sk, x) = Pub\,(pk, x, w)$

Openability$_k$: $(par, td) \leftarrow Par$, $(sk_0, pk) \leftarrow KeyGen(par)$,

$(x_\gamma \leftarrow \mathcal{X}$ with uniform random $r_{x_\gamma})_{\gamma \in [k]}$, $(\pi_\gamma^{(0)} = Priv(sk_0, x_\gamma))_{\gamma \in [k]}$,

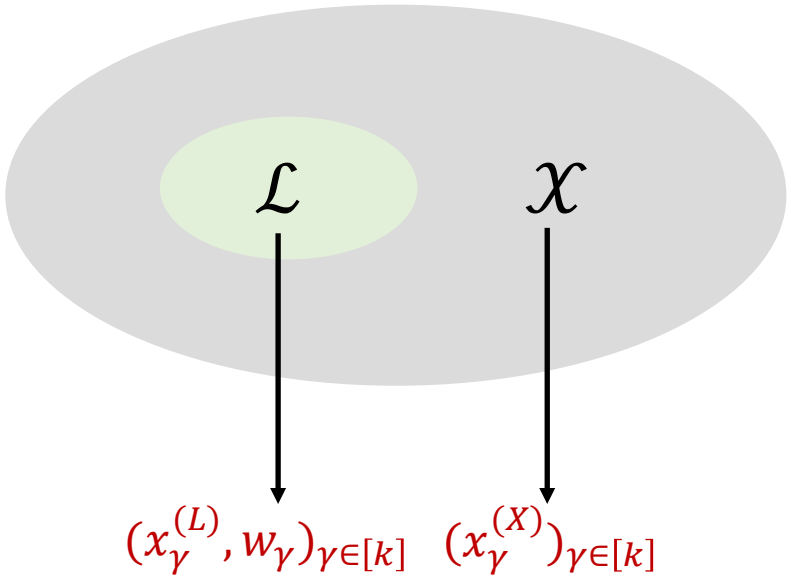
$(\pi_\gamma^{(1)} \leftarrow \Pi$ with uniform random $r_{\pi_\gamma^{(1)}})_{\gamma \in [k]}$,

$sk_1 \leftarrow HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}, r_{\pi_\gamma^{(1)}}\right)_{\gamma \in [k]})$,

$(td, pk, sk_0, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(0)}\right)_{\gamma \in [k]}) \approx_s (td, pk, sk_1, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}\right)_{\gamma \in [k]})$.

SMP: $x^{(L)} \approx_c x^{(X)}$

Key-Openable Hash Proof System



Multi-fold SMP:

$$(x_\gamma^{(L)})_{\gamma\in[k]} \approx_c (x_\gamma^{(X)})_{\gamma\in[k]}$$

Informally, guarantee that $HOpen_k$ can open uniformly sampled $(\pi_\gamma)_{\gamma\in[k]}$ to uniformly sampled $(x_\gamma)_{\gamma\in[k]}$

$$Par(1^\lambda) \to (par, td),\ KeyGen(par) \to (sk, pk)$$
$$Priv(sk, x) \to \pi,\ Pub(pk, x, w) \to \pi$$
$$HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma, r_{\pi_\gamma}\right)_{\gamma\in[k]}) \to sk'/\perp$$

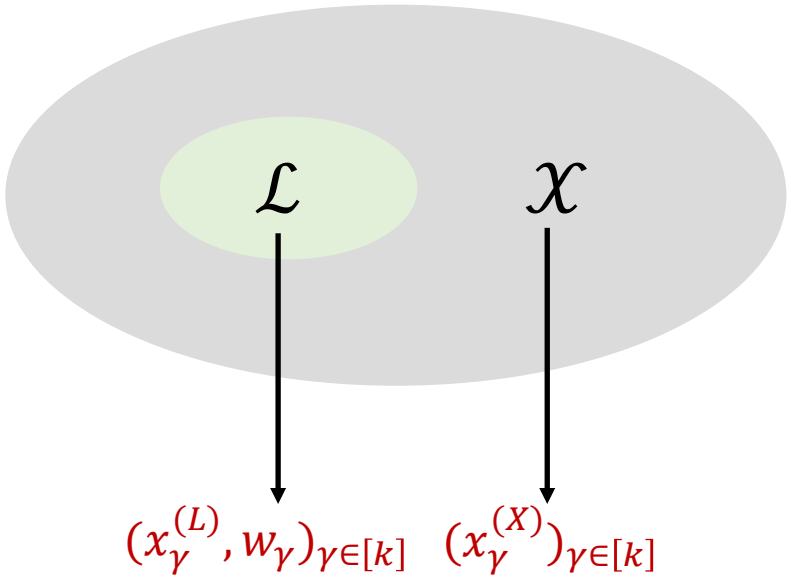
Projectivity: For any $(x, w) \leftarrow \mathcal{L}$, $Priv\,(sk, x) = Pub\,(pk, x, w)$

Openability$_k$: $(par, td) \leftarrow Par$, $(sk_0, pk) \leftarrow KeyGen(par)$,
$(x_\gamma \leftarrow \mathcal{X}$ with uniform random $r_{x_\gamma})_{\gamma\in[k]}$, $(\pi_\gamma^{(0)} = Priv(sk_0, x_\gamma))_{\gamma\in[k]}$,
$(\pi_\gamma^{(1)} \leftarrow \Pi$ with uniform random $r_{\pi_\gamma^{(1)}})_{\gamma\in[k]}$,

$$sk_1 \leftarrow HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}, r_{\pi_\gamma^{(1)}}\right)_{\gamma\in[k]}),$$

$$(td, pk, sk_0, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(0)}\right)_{\gamma\in[k]}) \approx_s (td, pk, sk_1, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}\right)_{\gamma\in[k]}).$$

Key-Openable Hash Proof System



Multi-fold SMP:

$$(x_\gamma^{(L)})_{\gamma\in[k]} \approx_c (x_\gamma^{(X)})_{\gamma\in[k]}$$

$Par(1^\lambda) \to (par, td)$, $KeyGen(par) \to (sk, pk)$

$Priv(sk, x) \to \pi$, $Pub(pk, x, w) \to \pi$

$$HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma, r_{\pi_\gamma}\right)_{\gamma\in[k]}) \to sk'/\perp$$

Projectivity: For any $(x, w) \leftarrow \mathcal{L}$, $Priv\,(sk, x) = Pub\,(pk, x, w)$

Openability$_k$: $(par, td) \leftarrow Par$, $(sk_0, pk) \leftarrow KeyGen(par)$,
$(x_\gamma \leftarrow \mathcal{X}$ with uniform random $r_{x_\gamma})_{\gamma\in[k]}$, $(\pi_\gamma^{(0)} = Priv(sk_0, x_\gamma))_{\gamma\in[k]}$,
$(\pi_\gamma^{(1)} \leftarrow \Pi$ with uniform random $r_{\pi_\gamma^{(1)}})_{\gamma\in[k]}$,

$$sk_1 \leftarrow HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}, r_{\pi_\gamma^{(1)}}\right)_{\gamma\in[k]}),$$

$$(td, pk, sk_0, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(0)}\right)_{\gamma\in[k]}) \approx_s (td, pk, sk_1, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}\right)_{\gamma\in[k]}).$$

Efficient randomness resampling on Π: there is a PPT $ReSmp_\Pi$, s.t., $\pi \leftarrow \Pi$ with uniform random r_π, $\pi' \leftarrow \Pi$, and $r_{\pi'} \leftarrow ReSmp_\Pi(\pi')$,

$$(\pi, r_\pi) \approx_s (\pi', r_{\pi'}).$$

Key-Openable Hash Proof System

MDDH-based Instantiation

(a generalization of the DDH-based HPS [CS02])

$Par(1^\lambda) \to (par, td)$, $KeyGen(par) \to (sk, pk)$

$Priv(sk, x) \to \pi$, $Pub(pk, x, w) \to \pi$

$HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma, r_{\pi_\gamma}\right)_{\gamma\in[k]}) \to sk'/\perp$

Projectivity: For any $(x, w) \leftarrow \mathcal{L}$, $Priv\,(sk, x) = Pub\,(pk, x, w)$

Openability$_k$: $(par, td) \leftarrow Par$, $(sk_0, pk) \leftarrow KeyGen(par)$,
$(x_\gamma \leftarrow \mathcal{X}$ with uniform random $r_{x_\gamma})_{\gamma\in[k]}$, $(\pi_\gamma^{(0)} = Priv(sk_0, x_\gamma))_{\gamma\in[k]}$,
$(\pi_\gamma^{(1)} \leftarrow \Pi$ with uniform random $r_{\pi_\gamma^{(1)}})_{\gamma\in[k]}$,

$sk_1 \leftarrow HOpen_k(td, pk, sk, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}, r_{\pi_\gamma^{(1)}}\right)_{\gamma\in[k]})$,

$(td, pk, sk_0, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(0)}\right)_{\gamma\in[k]}) \approx_s (td, pk, sk_1, \left(x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}\right)_{\gamma\in[k]})$.

Efficient randomness resampling on Π: there is a PPT $ReSmp_\Pi$, s.t., $\pi \leftarrow \Pi$ with uniform random r_π, $\pi' \leftarrow \Pi$, and $r_{\pi'} \leftarrow ReSmp_\Pi(\pi')$, $(\pi, r_\pi) \approx_s (\pi', r_{\pi'})$.

https://eprint.iacr.org/2022/1176

Construction of KM-NCE from Key-Openable HPS

HPS $=$ (HPS.Par, HPS.$KeyGen$, HPS.$Priv$, HPS.Pub, HPS.$HOpen_k$) is a key-openable hash proof system, whose hash value space supports efficient randomness resampling (w.r.t. HPS.$ReSmp_\Pi$).

KM-NCE = (Gen, Enc, Dec, Fake, Open$_k$)

Gen(1^λ):
$(par, td) \leftarrow$ HPS.$Par(1^\lambda)$
$(sk, pk) \leftarrow$ HPS.$KeyGen(par)$
$SK = sk$
$PK = (par, pk)$
$TK = td$

Enc(pk, m):
$x \leftarrow \mathcal{L}$ with witness w
$\pi =$ HPS.$Pub(pk, x, w) + m \in \Pi$
$C = (x, \pi)$

Dec$(sk, C = (x, \pi))$:
$m = \pi -$ HPS.$Priv(sk, x)$

Fake(1^λ):
$x \leftarrow \mathcal{X}$ with randomness r_x
$\pi \leftarrow \Pi$
$C = (x, \pi)$
$TD = r_x$

Open$_k(PK, SK, TK, (C_\gamma, TD_\gamma, m_\gamma)_{\gamma\in[k]})$:
Parse $TK = td$, $(C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]}$, $(TD_\gamma = r_{x_\gamma})_{\gamma\in[k]}$
For $\gamma \in [k]$:
$e_\gamma = \pi_\gamma - m_\gamma,\ r_{e_\gamma} \leftarrow$ HPS.$ReSmp_\Pi(e_\gamma)$
$sk' \leftarrow$ HPS.$HOpen_k(td, pk, sk, (x_\gamma, r_{x_\gamma}, e_\gamma, r_{e_\gamma})_{\gamma\in[k]})$
$SK' = sk'$

KMNC_k-CPA Security of the KM-NCE construction

KMNC_k-CPA security

For any $m_1, \ldots, m_k$, for $(pk, sk, tk) \leftarrow \mathbf{Gen}(\lambda)$,

- k real ciphertexts:

  $(c_\gamma \leftarrow \mathbf{Enc}(pk, m_\gamma))_{\gamma \in [k]}$

- k fake ciphertexts and secret keys:

  $((c_\gamma^{\mathrm{fk}}, td_\gamma) \leftarrow \mathbf{Fake}(\lambda))_{\gamma \in [k]}$

  $sk^{\mathrm{op}} \leftarrow \mathbf{Open}_k(tk, pk, sk, (c_\gamma^{\mathrm{fk}}, td_\gamma, m_\gamma)_{\gamma \in [k]})$

$$(pk, sk, c_1, \ldots, c_k) \approx (pk, sk^{\mathrm{op}}, c_1^{\mathrm{fk}}, \ldots, c_k^{\mathrm{fk}})$$

KMNC_k-CPA Security of the KM-NCE construction

Real: $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$

$\equiv$

G_0 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{L}$ with witness w_γ; $\pi_\gamma = \mathrm{HPS}.Pub(pk, x_\gamma, w_\gamma) + m_\gamma$

Projectivity

G_1 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{L}$ with witness w_γ; $\pi_\gamma = \mathrm{HPS}.Priv(sk, x_\gamma) + m$

Multi-fold SMP

G_2 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{X}$ with rendomness r_{x_γ}; $\pi_\gamma = \mathrm{HPS}.Priv(sk, x_\gamma) + m$

Openability$_k$

G_3 : $(PK, SK = sk', (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{X}$ with rendomness r_{x_γ}; $\pi_\gamma \leftarrow \Pi$;

$e_\gamma = \pi_\gamma - m_\gamma$, $r_{e_\gamma} \leftarrow \mathrm{HPS}.ReSmp_\Pi(e_\gamma)$,

$sk' \leftarrow \mathrm{HPS}.HOpen_k(td, pk, sk, (x_\gamma, r_{x_\gamma}, e_\gamma, r_{e_\gamma})_{\gamma\in[k]})$

Fake: $(PK, SK = sk', (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$

KMNC$_k$-CPA Security of the KM-NCE construction

Real: $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$

$\equiv$

G_0 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{L}$ with witness w_γ; $\pi_\gamma = \text{HPS}.Pub(pk, x_\gamma, w_\gamma) + m_\gamma$

Projectivity

G_1 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{L}$ with witness w_γ; $\pi_\gamma = \text{HPS}.Priv(sk, x_\gamma) + m$

Multi-fold SMP

G_2 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{X}$ with rendomness r_{x_γ}; $\pi_\gamma = \text{HPS}.Priv(sk, x_\gamma) + m$

Openability$_k$

G_3 : $(PK, SK = sk', (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{X}$ with rendomness r_{x_γ}; $\pi_\gamma \leftarrow \Pi$;

$e_\gamma = \pi_\gamma - m_\gamma$, $r_{e_\gamma} \leftarrow \text{HPS}.ReSmp_\Pi(e_\gamma)$,

$sk' \leftarrow \text{HPS}.HOpen_k(td, pk, sk, (x_\gamma, r_{x_\gamma}, e_\gamma, r_{e_\gamma})_{\gamma\in[k]})$

$\equiv$

Fake: $(PK, SK = sk', (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$

Open$_k$

KMNC_k-CPA Security of the KM-NCE construction

Real: $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$

II

G_0 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{L}$ with witness w_γ; $\pi_\gamma = \mathrm{HPS}.Pub(pk, x_\gamma, w_\gamma) + m_\gamma$

Projectivity

G_1 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{L}$ with witness w_γ; $\pi_\gamma = \mathrm{HPS}.Priv(sk, x_\gamma) + m$

Multi-fold SMP

G_2 : $(PK, SK = sk, (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{X}$ with rendomness r_{x_γ}; $\pi_\gamma = \mathrm{HPS}.Priv(sk, x_\gamma) + m$

Openability$_k$

G_3 : $(PK, SK = sk', (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$: $x_\gamma \leftarrow \mathcal{X}$ with rendomness r_{x_γ}; $\pi_\gamma \leftarrow \Pi$;

$e_\gamma = \pi_\gamma - m_\gamma$, $r_{e_\gamma} \leftarrow \mathrm{HPS}.ReSmp_\Pi(e_\gamma)$,

$sk' \leftarrow \mathrm{HPS}.HOpen_k(td, pk, sk, (x_\gamma, r_{x_\gamma}, e_\gamma, r_{e_\gamma})_{\gamma\in[k]})$

II

Fake: $(PK, SK = sk', (C_\gamma = (x_\gamma, \pi_\gamma))_{\gamma\in[k]})$

Open$_k$

For the CCA secure KM-NCE construction, please refer to https://eprint.iacr.org/2022/1176

Summary

- We formalize the notion of ANON-RSO$_k$&C security for PKE
  - ✓ANON-RSO$_k$&C-CPA ⇒ ANON-COR ([BGG+20, TCC])

- We formalize the notion of SIM-RSO$_k$&C security for PKE
  - ✓SIM-RSO$_k$&C-ATK ⇒ SIM-RSO$_k$-ATK ([YLH+20, ASIACRYPT])

- We show a framework of PKE achieving both ANON-RSO$_k$&C-CCA and SIM-RSO$_k$&C-CCA security
  - ✓The obtained MDDH-based scheme
    - ✓ has compact ciphertexts (i.e., ciphertext overhead is the size of a constant number of group elements);
    - ✓ has tight security reduction;
    - ✓ is the first PKE scheme achieving ANON-COR security ([BGG+20, TCC]).

https://eprint.iacr.org/2022/1176

References

[BGG+20] Fabrice Benhamouda, Craig Gentry, Sergey Gorbunov, Shai Halevi, Hugo Krawczyk, Chengyu Lin, Tal Rabin, and Leonid Reyzin. Can a public blockchain keep a secret? In TCC 2020, pages 260–290. Springer, 2020.

[CHK05] Ran Canetti, Shai Halevi, and Jonathan Katz. Adaptively-secure, noninteractive public-key encryption. In TCC 2005, pages 150–168. Springer, 2005.

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In EUROCRYPT 2002, pages 45–64, 2002.

[HKM+18] Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka. Simulation-based receiver selective opening CCA secure PKE from standard computational assumptions. In Security and Cryptography for Networks 2018, pages 140–159. Springer, 2018

[HPW15] Carmit Hazay, Arpita Patra, and Bogdan Warinschi. Selective opening security for receivers. In ASIACRYPT 2015, pages 443–469. Springer, 2015

[YLH+20] Rupeng Yang, Junzuo Lai, Zhengan Huang, Man Ho Au, Qiuliang Xu, and Willy Susilo. Possibility and impossibility results for receiver selective opening secure PKE in the multi-challenge setting. In ASIACRYPT 2020, pages 191–220. Springer, 2020.

Thanks for your Attention!