Non-Committing Identity Based Encryption: Constructions and Applications

Mahesh Sreekumar Rajasree
CISPA Helmholtz

PKC 2025

Joint work with Rishab Goyal (UW-Madison), Fuyuki Kitagawa (NTT Japan), Venkata Koppula (IITD), Ryo Nishimaki (NTT Japan) and Takashi Yamakawa (NTT Japan)

Standard Security : Definition

Challenger

[Goldwasser-Micali'84]

Adversary

$(sk, pk) \leftarrow Setup()$

pk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$b' \in \{0,1\}$

Adversary wins if $b = b'$

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has entire ciphertext and entire secret key due to correctness.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model
  - Make ciphertext large so that long-term storage is expensive.
  - Adversary gets a challenge ciphertext ct^* for m_0, m_1 and then it has to compress/reduce its storage which contains ct^*.
  - After which it receives sk, but still should not be able to distinguish.

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]

Challenger

Adversary 1

$(pk, sk) \leftarrow Setup()$

pk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$state$

$|state| \leq S$

Adversary 2

$pk, sk, state$

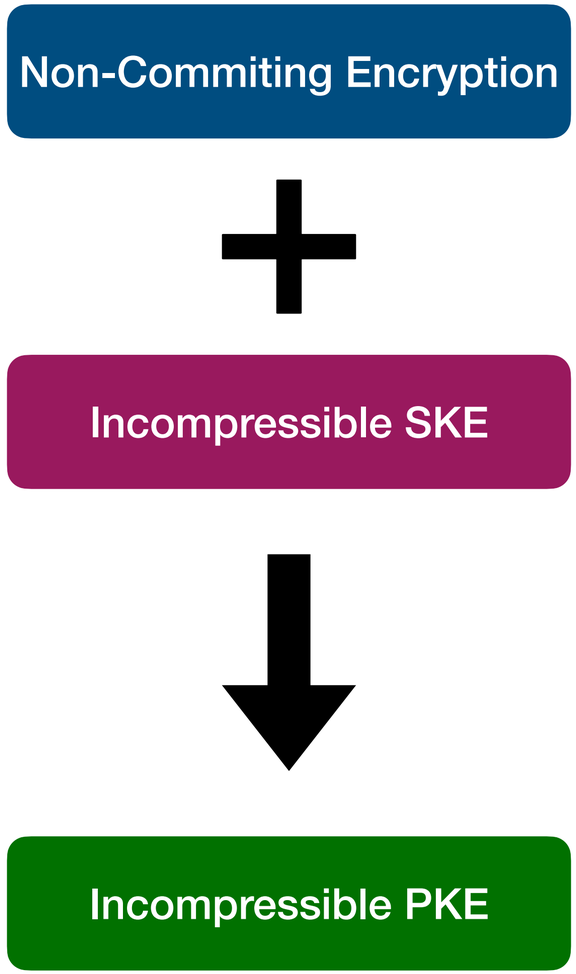
$b' \in \{0,1\}$

Adversaries win if $b = b'$

Prior works

Dziembowski'06	Introduced and constructed the first Incompressible SKE.
Guan-Wichs-Zhandry'22	Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).
Branco-Döttling-Dujmovic'23	Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.
Guan-Wichs-Zhandry'23	Extended the notion to Multi-user Incompressible PKE setting.
Bhushan-Goyal-Koppula-Narayanan-Prabhakaran-Rajasree'24	Extended the notion to leakage-resilience.
Goyal-Koppula-Rajasree-Verma'25	Extended the notion to FE, ABE and **IBE**

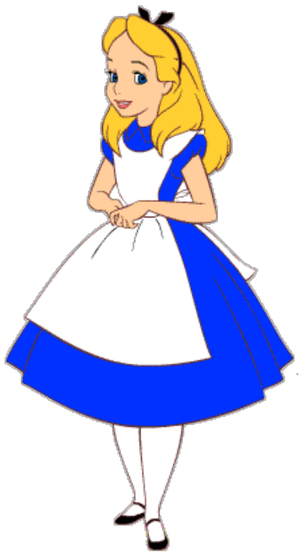
Incompressible PKE from NCE



Can be build from OWF

Non-Committing Encryption (NCE)

[CFGN'96]



pk sk

pk

m

ct sk

$m \leftarrow Dec(sk, ct)$

$ct \leftarrow Enc(pk, m)$

ct **is committed to** m

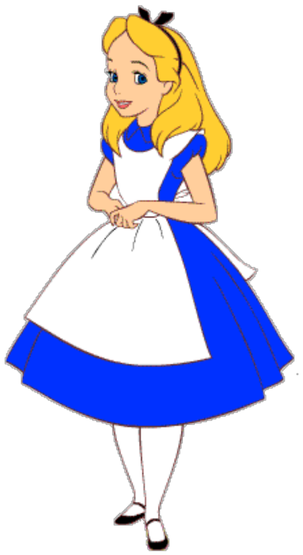
Non-Committing Encryption (NCE)

[CFGN'96]

pk

m

ct sk



pk ct

$m \leftarrow Dec(sk, ct)$

Generate fake sk

Adaptivity in MPC

Certified Deletion

Incompressible Cryptography

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk, secret key sk

$Enc(pk, m) \rightarrow$ ciphertext ct

$Dec(sk, ct) \rightarrow m / \perp$

Security

$$\underbrace{\{pk, sk, ct_m\}}_{Real} \approx_c \underbrace{\{pk^*, sk^*, ct^*\}}_{Simulated}$$

$Sim_1(\lambda) \rightarrow$ fake public key pk^*, fake ciphertext ct^*

$Sim_2(m) \rightarrow$ fake secret key sk^*

Identity Based Encryption

[Shamir'85]

- Generalisation of PKE.
- n users in the system each with a distinct identity. **Secret keys** are associated with identity id
- To encrypt a message m, a master public key mpk is used along with id.
  - Adversary gets a challenge ciphertext ct^* for m_0, m_1 encrypted under the identity id^* and then it has to distinguish it.
  - Also obtains multiple sk_{id} where $id \neq id^*$.

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk, master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, id) \rightarrow$ Secret key sk_{id}

$Dec(sk_{id}, ct) \rightarrow m$

$Sim_1(\lambda) \rightarrow$ fake master public key mpk^*, fake ciphertext ct^*

$Sim_2(id) \rightarrow$ Fake secret key sk_{id}

$Sim_3(id^*, m) \rightarrow$ Fake master secret key msk^*

Prior works*

Canetti-Feige-Goldreich-Naor’96	Introduced NCE to design adaptively secure multiparty computation protocols.
Bea’97,DN’00,CDMW’09,HOR’15,HORR’15,CPR17,YKT’19	Constructions from various assumptions.
Brakerski-Branco-Döttling-Garg-Malavolta’20 **Yoshida-Kitagawa-Xagawa-Tanaka'20**	Rate-1 NCE
Hiroka-Morimae-Nishimaki-Yamakawa’21	Introduced **identity based non-committing encryption** to build certified IBE with certified deletion.

Reveals randomness used during setup and encryption algorithm.

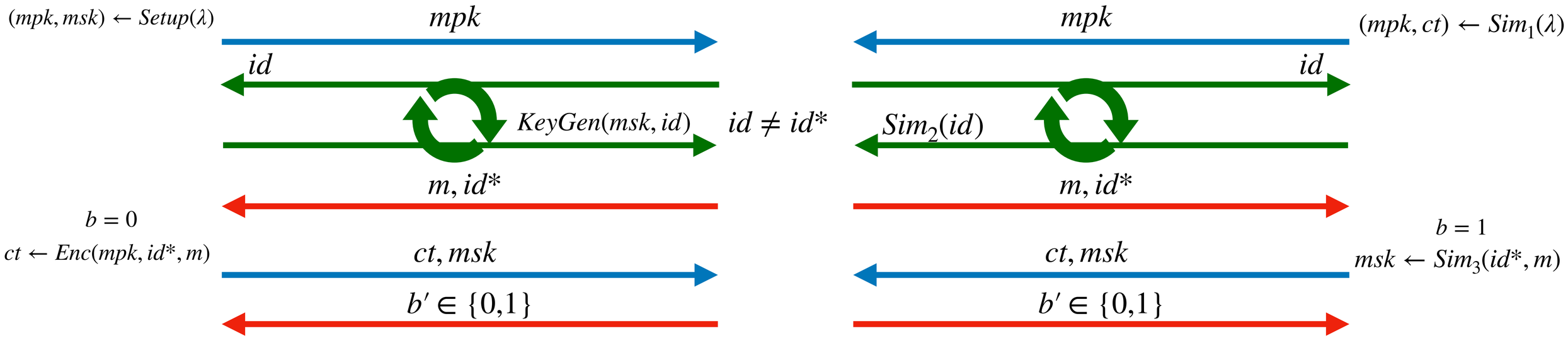
RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]

Challenger

Adversary

Simulator



Adversary wins if $b = b'$

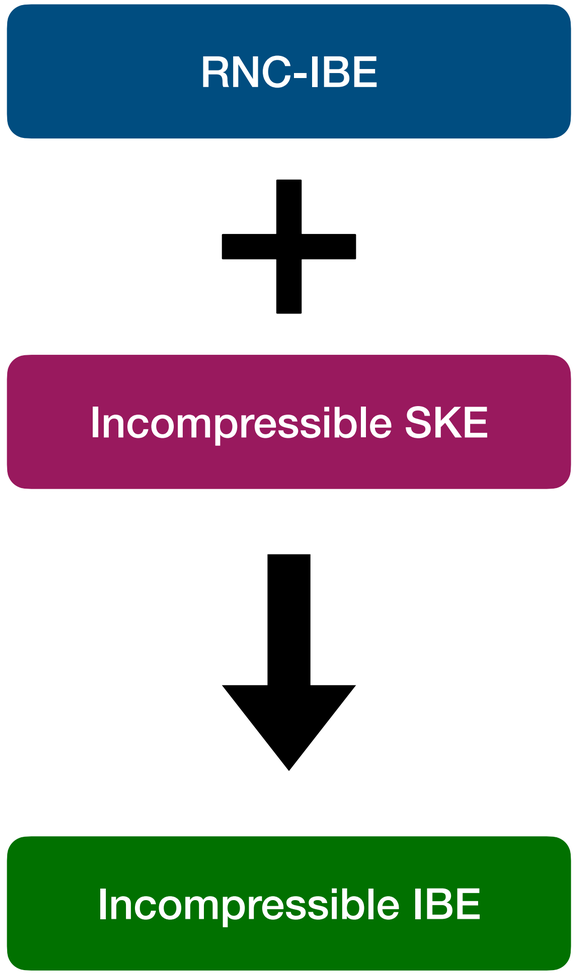
This work

Can we build RNC-IBE from standard assumptions*?

Prior work used indistinguishable obfuscation.

Our Results

- Rate-1 RNC-IBE from bilinear pairings.
  - Rate-1 strong incompressible IBE from bilinear pairings and LWE (or DCR)
- RNC-IBE for polynomially bounded identity space from DDH, LWE.



Bilinear Pairings

$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ where $\mathbb{G}_i$ is a prime order group

$g_1, g_2, e(g_1, g_2)$ are generators of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

$[a]_b$ denotes g_b^a

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2\times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

$$MPK = ([a^T k]_T)$$

$$KeyGen(id) \rightarrow ([sb]_2, [k + s(W_1 + id \cdot W_2)^T b]_2)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow ([ra]_1, [r(W_1 + id \cdot W_2)a]_1, [ra^T k]_T \cdot m)$$

$$Dec(sk_{id}, ct) \rightarrow \frac{[ra^T k]_T \cdot m \times e([r(W_1 + id \cdot W_2)a]_1, [sb]_2)}{e([ra]_1, [k + s(W_1 + id \cdot W_2)^T b]_2)}$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2\times 2}$$

DDH

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1 , [(W_1 + id^* \cdot W_2)u]_1 , [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2 , [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^\top]_2)$$

k_2 **is not used anywhere**

$$Sim_3(m) \rightarrow \text{Set } k_2 = \frac{\frac{r}{m} - u_1 k_1}{u_2} \text{ where } u = u_1 a + u_2 a^\top$$

$$MSK = (k = \frac{k_1}{|a|^2} a + \frac{k_2}{|a^\top|^2} a^\top)$$

Incomp IBE from RNC-IBE

1. **RNC-IBE**
2. **Incompressible SKE scheme**

$$Setup \rightarrow MPK = (\ RNCIBE.MPK\ )$$

$$MSK = (\ RNCIBE.MSK\ )$$

$$KeyGen(id) \rightarrow RNCIBE.KeyGen(\ RNCIBE.MPK\ ,\ id\ )$$

$$Enc(id, m) \rightarrow IncompSKE.Enc(\ incompSK\ ,\ m\ )$$

$$RNCIBE.Enc(\ RNCIBE.MPK\ ,\ id\ ,\ incompSK\ )$$

Hybrid encryption

Future Directions

1. RNC-IBE from LWE and other assumptions.
2. Full NC-IBE from standard assumptions.
3. ~~Rate-1 RNC-ABE from bilinear pairings.~~
4. Strong incompressible IBE and ABE from other standard assumptions.

Thank You

https://mahe94.github.io