Identity-based Encryption Tightly Secure under Chosen-ciphertext Attacks

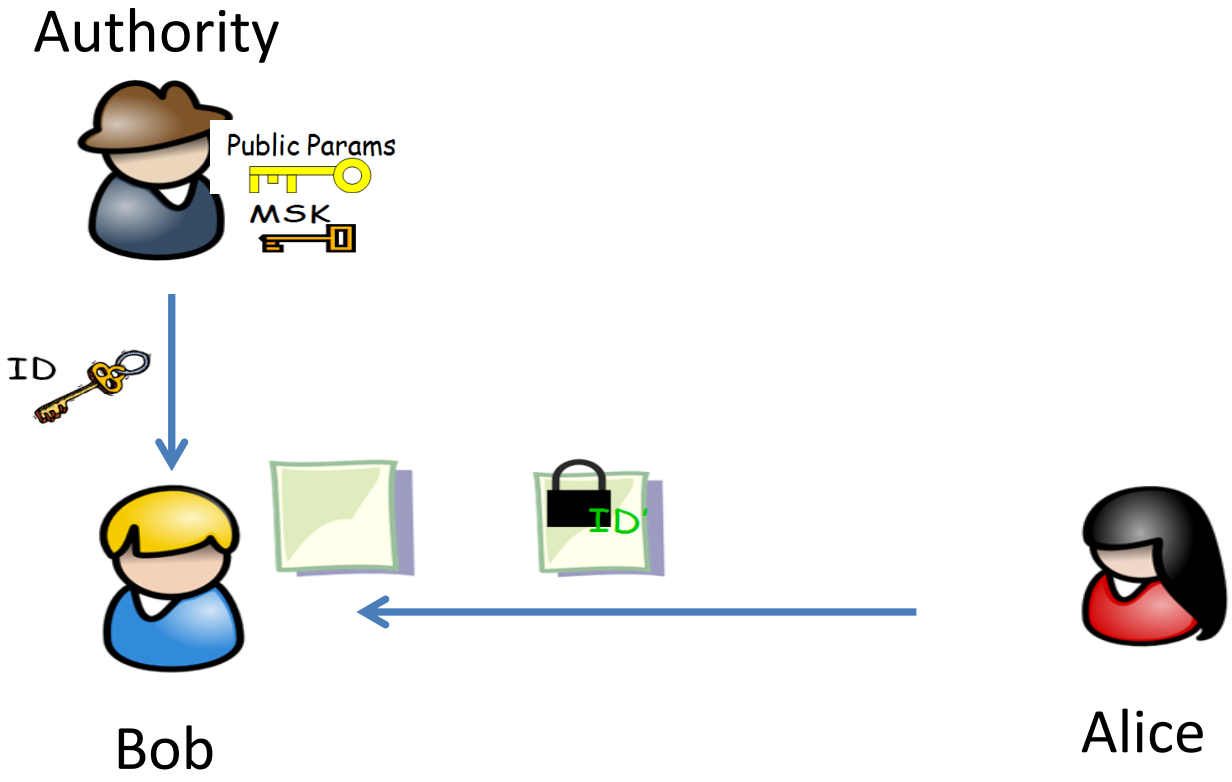
Dennis Hofheinz, Dingding Jia, Jiaxin Pan

KIT IIE,CAS KIT

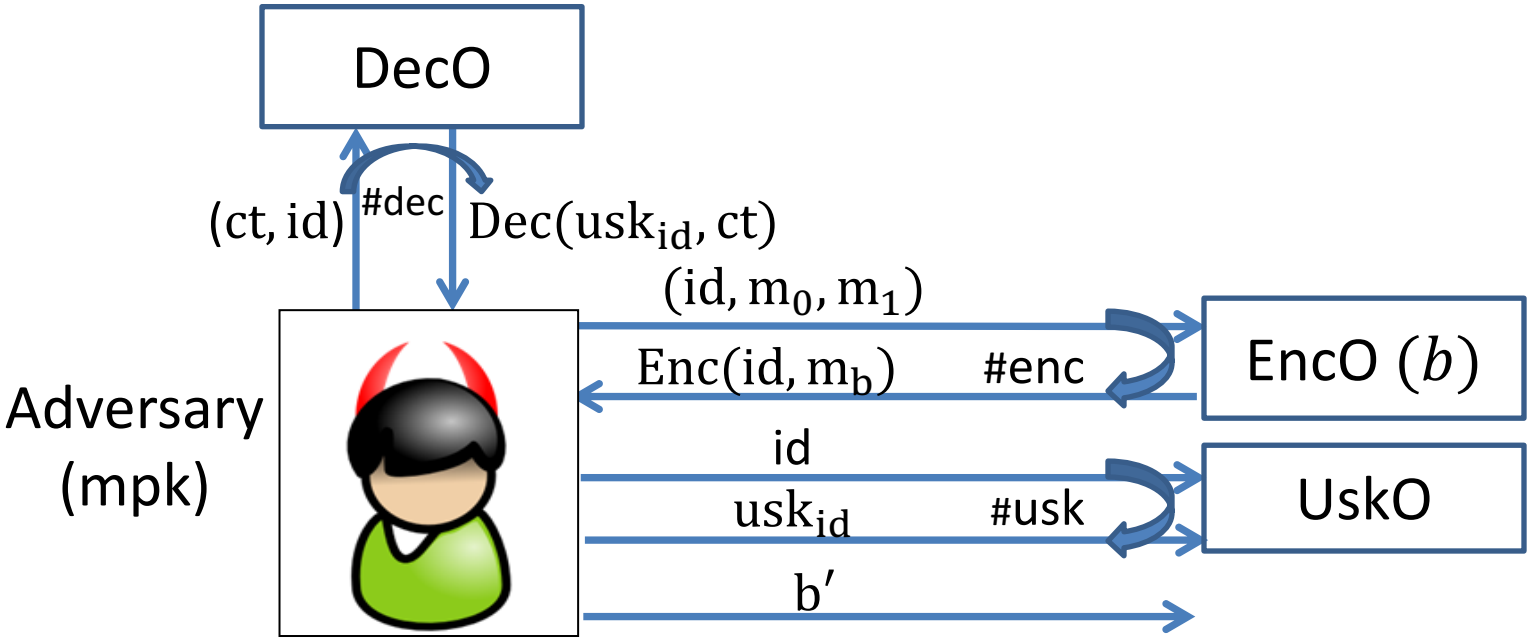
Contribution

- Identity-based Encryption
  - secure against multi-chosen-ciphertext-attack
  - tightly secure based on MDDH assumption
  - efficient

Identity-based Encryption



Chosen Ciphertext Security



Adv=Pr[b=b'] - $\frac{1}{2}$

Multi-challenge: #enc>>1

Tight Security

[BBM00],[CW13],[HJ12], [GHKW16]....

Adv=ϵ $< 2^{-128}$

Adv'=ϵ/L $< 2^{-158}$

Security loss

L=$\mathrm{O}(\#\mathrm{usk}, \#\mathrm{ct})$, e. g. $\mathrm{L} = 2^{30}$, not tight.

L=constant, $\mathrm{O}(\lambda)$, (almost) tight

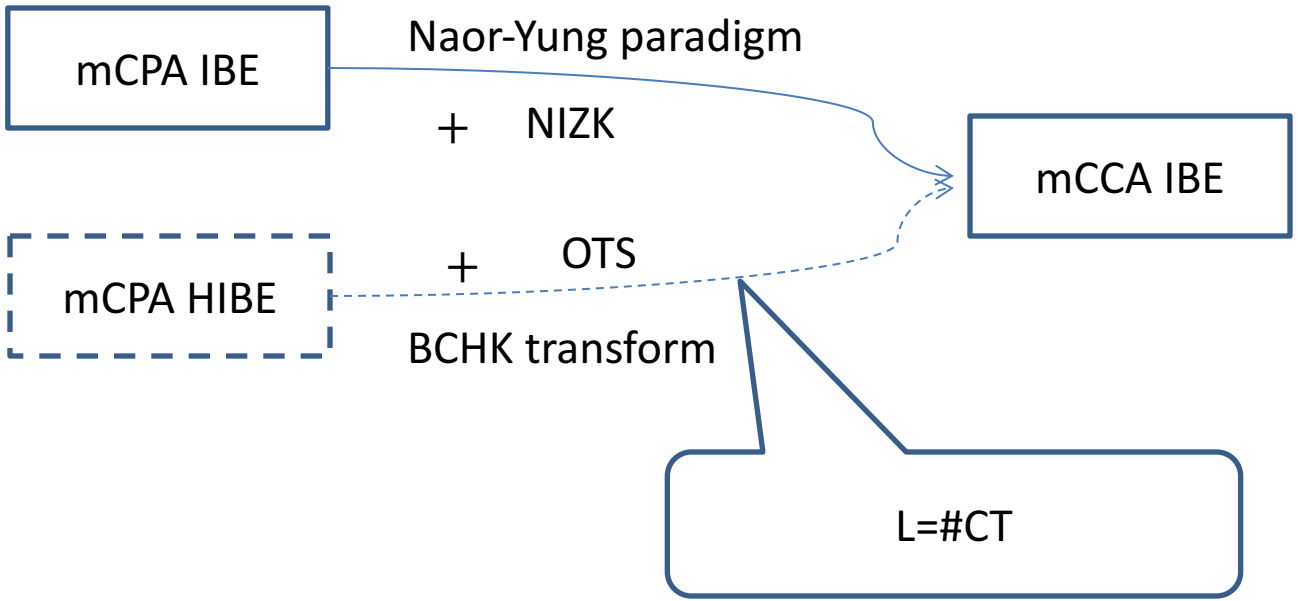
Related work

- CW13: (almost) tightly CPA IBE based on standard assumption
- HKS15: tightly mCPA IBE
- …GDCC16: efficient tightly mCPA IBE in prime order group
- HLQG18: efficient tightly CCA IBE

Our goal

Efficient , tightly multi-CCA secure IBE

General mCCA construction



Naor-Yung Paradigm to mCCA IBE

$\mathrm{Enc}_1(\mathrm{m}), \mathrm{Enc}_2(\mathrm{m}), \mathrm{NIZK}$

Proof strategy:

- Challenge ciphertext: $\mathrm{Enc}_1(\mathrm{m}_0), \mathrm{Enc}_1(\mathrm{m}_1), \mathrm{NIZK}$
- Decryption query:$\mathrm{Enc}_1(\mathrm{m}), \mathrm{Enc}_2(\mathrm{m}), \mathrm{NIZK}$

Tool: tightly multi-simulation-sound NIZK for L=$(\mathrm{Enc}_1(\mathrm{m}), \mathrm{Enc}_2(\mathrm{m}))$

Problem: Not efficient

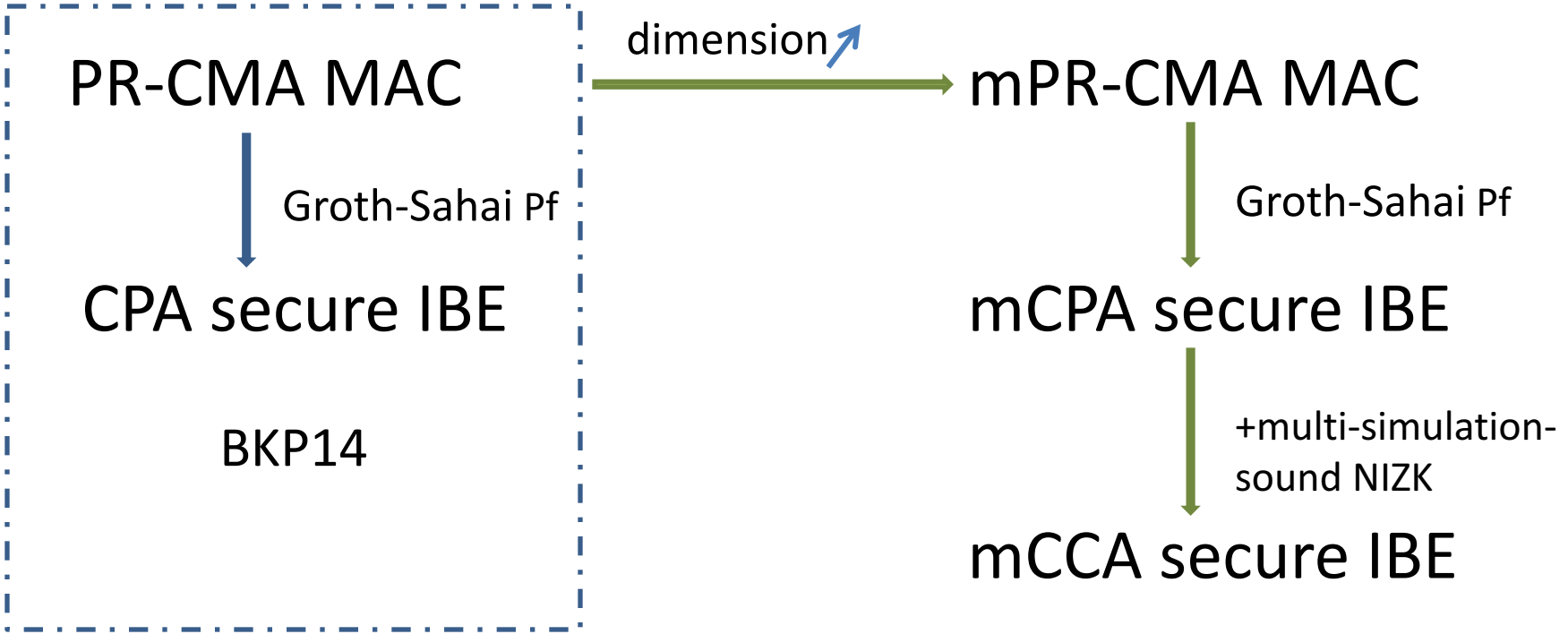
Our goal

Efficient tightly mCCA secure IBE

General construction: not efficient

Our strategy: specific construction

Technique overview

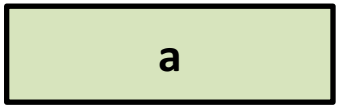


Vector notations

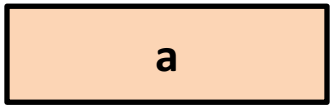
Z_q 

G_T 

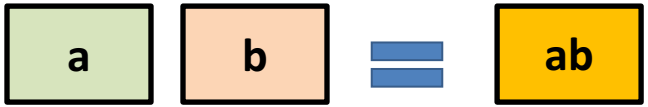
$= \mathrm{g}_{\mathrm{T}}^{\mathbf{a}}$

G_1 

$= \mathrm{g}_{1}^{\mathbf{a}}$

G_2 

$= \mathrm{g}_{2}^{\mathbf{a}}$



mCPA secure IBE

$\text{msk} = \boxed{\mathbf{x}_{j,b}} \leftarrow_R Z_q^3 \quad \text{for } j = 1, \dots, \lambda, b = 0,1; \quad \boxed{\mathbf{x}'} \leftarrow_R Z_q^3$

$\text{mpk} = \boxed{\mathbf{a}^T} \leftarrow_R G_1^{1\times 3}, \boxed{\mathbf{a}^T}\boxed{\mathbf{x}_{j,b}} \in G_1, \boxed{\mathbf{a}^T}\boxed{\mathbf{x}'} \in G_1$

$\text{sk}_{id} = \boxed{t} \leftarrow_R G_2, \boxed{\sum_j \mathbf{x}_{j,id_j}}\boxed{t} + \boxed{\mathbf{x}'} \in G_2^3$

$\text{Enc}(m) = \boxed{\mathbf{a}^T r} \in G_1^{1\times 3}, \boxed{\mathbf{a}^T r}\boxed{\sum_j \mathbf{x}_{j,id_j}}, \boxed{\mathbf{a}^T r}\boxed{\mathbf{x}'} \in G_T$

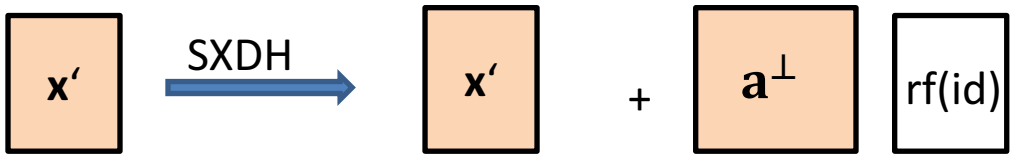
C_1 C_2 Key

Critical ciphertext

if $C_1 \notin span\,(\mathbf{a}^T)$

- For challenge query, session key is randomly distributed
- For decryption query, answer may leak information about $\mathbf{x}'$ more than $\mathbf{a}^T\mathbf{x}'$

Achieve mCPA security

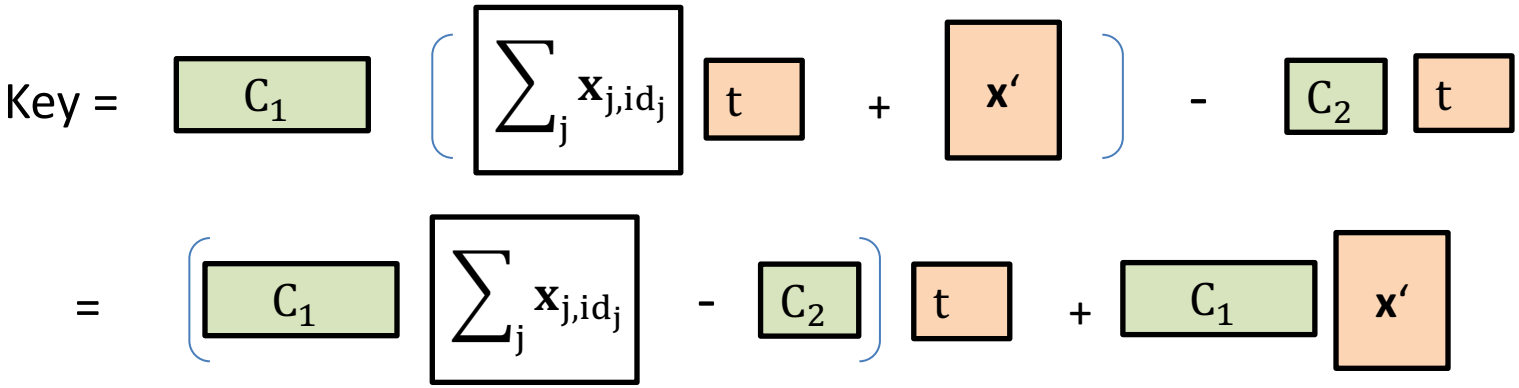


SXDH Ass. $\left(\mathbf{a} \leftarrow_R \mathrm{G}_s^2, \ \mathbf{ar} \right) =_C \left(\mathbf{a} \leftarrow_R \mathrm{G}_s^2, \ \mathbf{u} \leftarrow_R \mathrm{G}_s^2 \right)$

$\mathrm{sk}_{\mathrm{id}}$ leaks no information of $\mathbf{x}'$ other than $\mathbf{a}^{\mathrm{T}}\mathbf{x}'$

If $\mathrm{C}_1 \notin \mathrm{Span}\left(\mathbf{a}^{\mathbf{T}}\right)$, $\mathrm{C}_1\mathbf{x}'$ independent with $\mathbf{a}^{\mathrm{T}}\mathbf{x}'$, encapsulation key is randomly distributed

Critical decryption queries



Observation:

- if $C_1 \notin span\,(\mathbf{a}^T)$, $C_1\mathbf{x}'$ leak information about $\mathbf{x}'$ more than $\mathbf{a}^T\mathbf{x}'$
- if $C_2 \neq C_1(\sum_j \mathbf{x}_{j,id_j})$, leak information about t

To achieve CCA security

Strategy: build unfairness between C_1 w.r.t. challenge answer and decryption query

- Challenge query: $C_1 \notin \text{span}(\mathbf{a}^T)$
- Decryption query: $C_1 \in \text{span}(\mathbf{a}^T)$

Tool: multi-simulation-sound NIZK for linear space $L = \text{span}(\mathbf{a}^T)$

Efficient construction inspired by that in GHKW16

mCCA secure IBE

$\mathrm{Enc}(\mathrm{m}) =$ $\mathbf{a}^{\mathbf{T}}\mathrm{r} \in G_1^{1\times 3}$, $\mathbf{a}^{\mathbf{T}}\mathrm{r}\ \mathbf{x}_{\mathrm{id}} \in G_1$,

C_1 C_2

3 elements

$\pi = \mathrm{Prov}(\mathrm{C}_2, \mathrm{C}_1, \mathrm{r})$

tag
statement

randomness

Comparison of tightly IBE based on SXDH assumption

Scheme	|pk|	|ct|-|m|	MC	CCA
CW13	$4\lambda + 3$	4	×	×
BKP14	$2\lambda + 2$	3		
HLQG18	$4\lambda + 3$	3		√
AHY15	$16\lambda + 10$	8	√	×
GDCC16	$2\lambda + 4$	4		
This work	$8\lambda + 12$	7		√

Conclusion

- First tightly multi-CCA secure IBE based on MDDH assu.
  - Multi-PR-CMA affine MAC
  - Multi-CPA secure IBE
  - Multi-CCA secure IBE with multi-simulation-sound NIZK

Thank you!