Registered ABE via Predicate Encodings

Ziqi Zhu Kai Zhang Junqing Gong Haifeng Qian

East China Normal University
Shanghai University of Electric Power
Shanghai QiZhi Institute

Attribute-Based Encryption (ABE) [SW05]

Attribute-Based Encryption (ABE) [SW05]

Setup$(1^\lambda, P)$

Enc(mpk, x, m)

Gen(msk, y)

Dec(sk_y, ct_x)

Attribute-Based Encryption (ABE) [SW05]

mpk

msk

Setup$(1^\lambda, P)$

Enc(mpk, x, m)

Gen(msk, y)

Dec(sk_y, ct_x)

Attribute-Based Encryption (ABE) [SW05]

Setup$(1^\lambda, P)$

Enc(mpk, x, m)

Gen(msk, y)

Dec(sk_y, ct_x)

Attribute-Based Encryption (ABE) [SW05]

Setup$(1^\lambda, P)$

Enc(mpk, x, m)

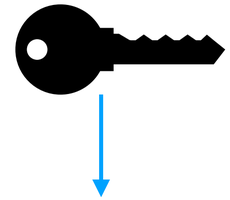
Gen(msk, y)

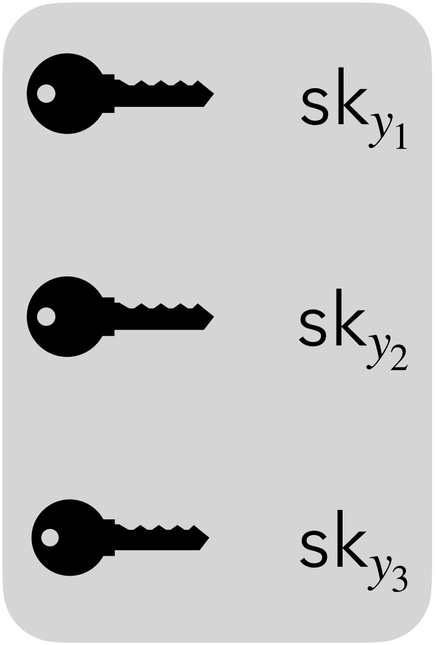
Dec(sk_y, ct_x)

mpk

ct_x

msk





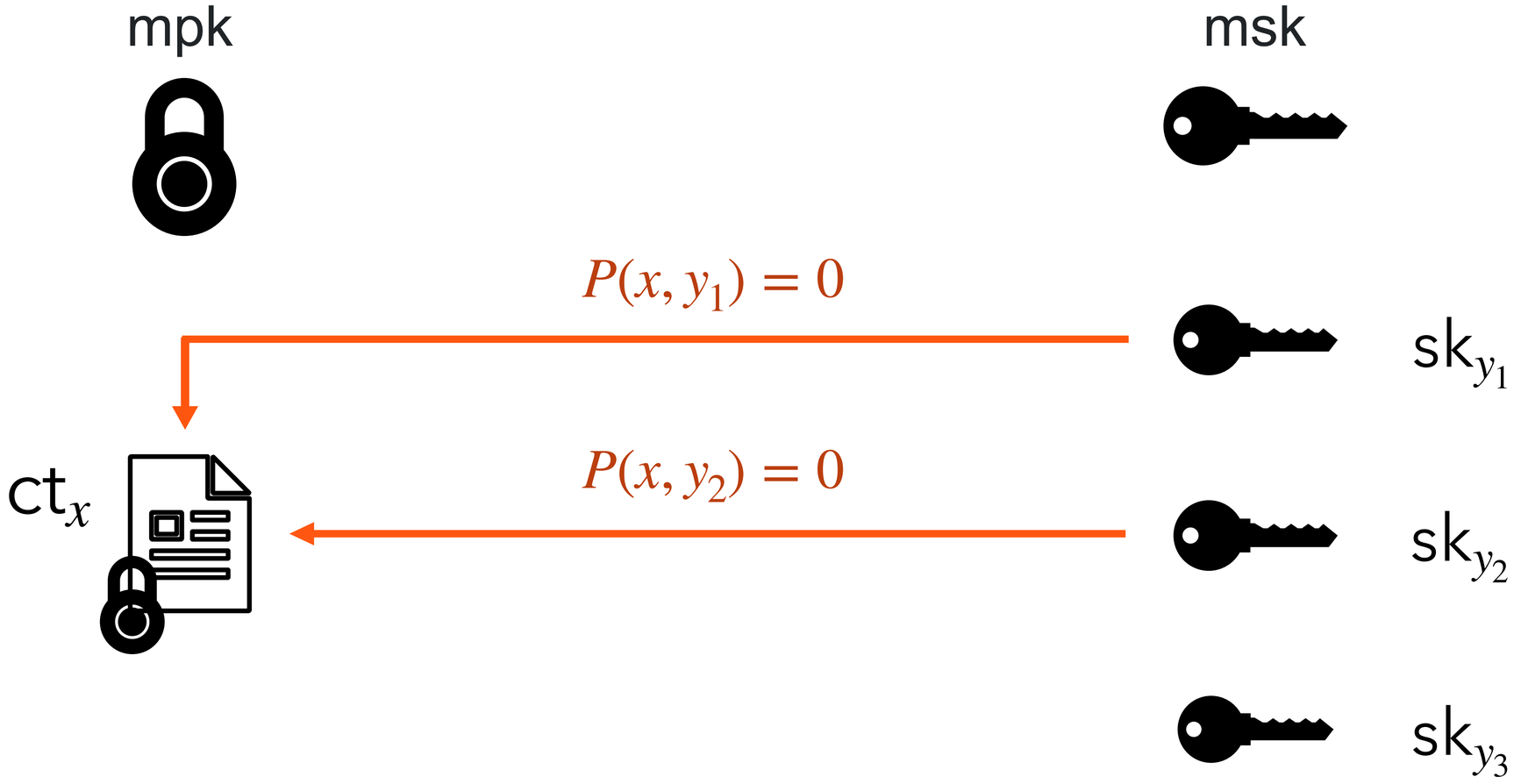
Attribute-Based Encryption (ABE) [SW05]

Setup$(1^\lambda, P)$

Enc(mpk, x, m)

Gen(msk, y)

Dec(sk_y, ct_x)



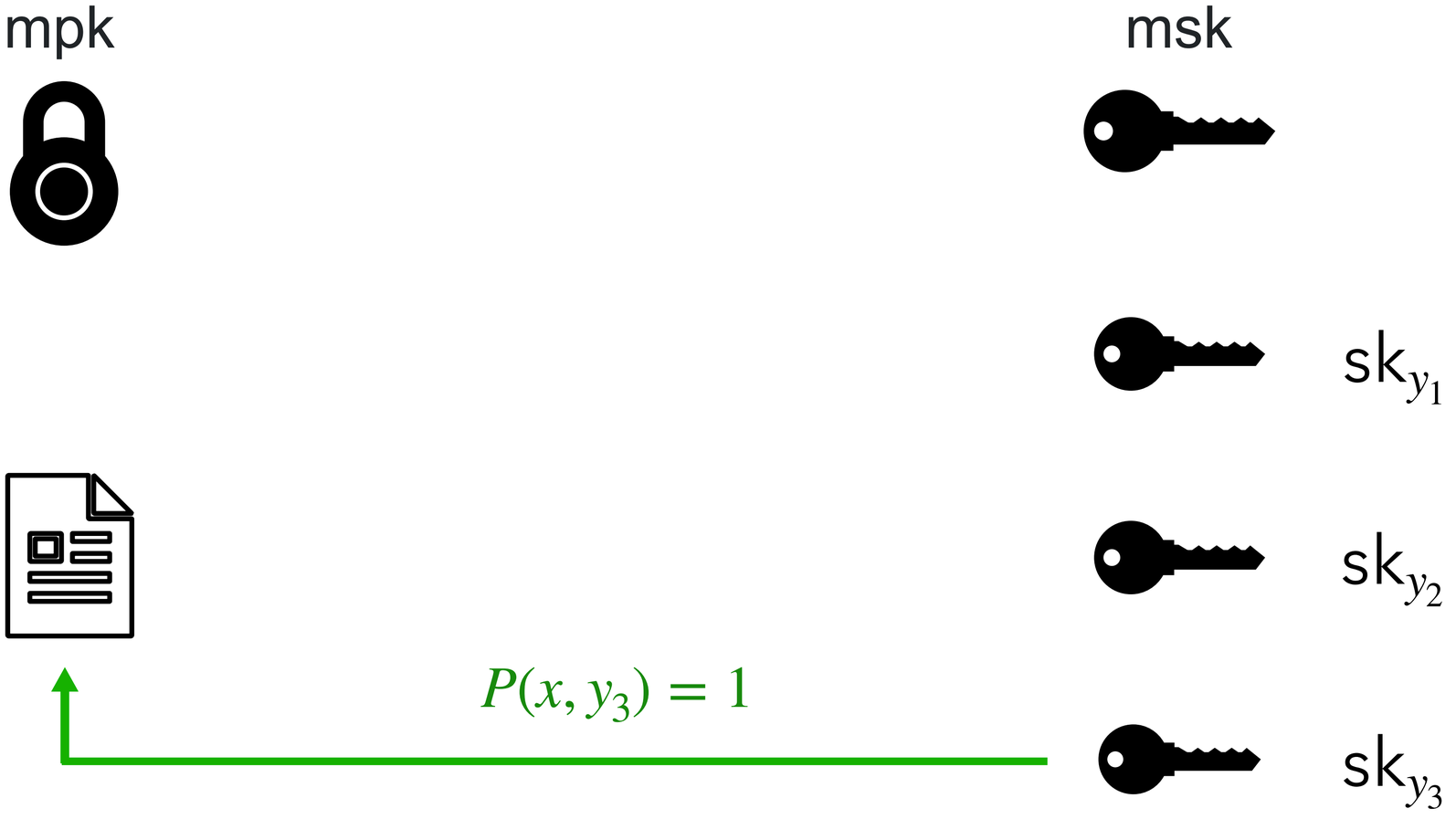
Attribute-Based Encryption (ABE) [SW05]

Setup$(1^\lambda, P)$

Enc(mpk, x, m)

Gen(msk, y)

Dec(sk_y, ct_x)



Slotted Registered ABE (Reg-ABE) [HLWW23]

Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

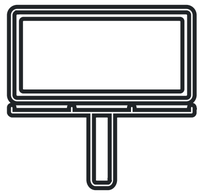
Gen(crs, i)

Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

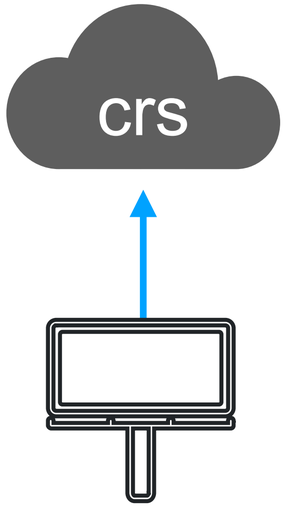
Enc(mpk, x, m)

Dec(sk,hsk,ct)



Slotted Registered ABE (Reg-ABE) [HLWW23]

$\mathsf{Setup}(1^\lambda, P, 1^L)$



$\mathsf{Gen}(\mathsf{crs}, i)$

$\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i)$

$\mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, y_i)_{i\in[L]})$

$\mathsf{Enc}(\mathsf{mpk}, x, \mathsf{m})$

$\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct})$

Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

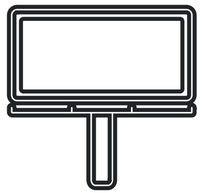
Gen(crs, i)

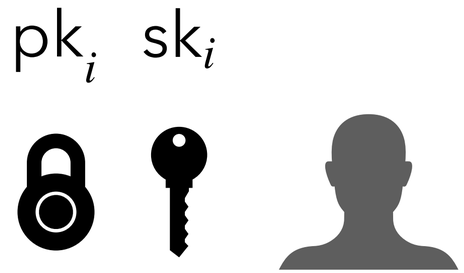
Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

Enc(mpk, x, m)

Dec(sk,hsk,ct)





Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

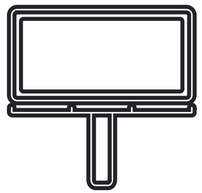
Gen(crs, i)

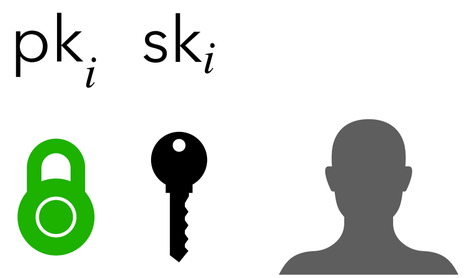
Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

Enc(mpk, x, m)

Dec(sk,hsk,ct)





Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

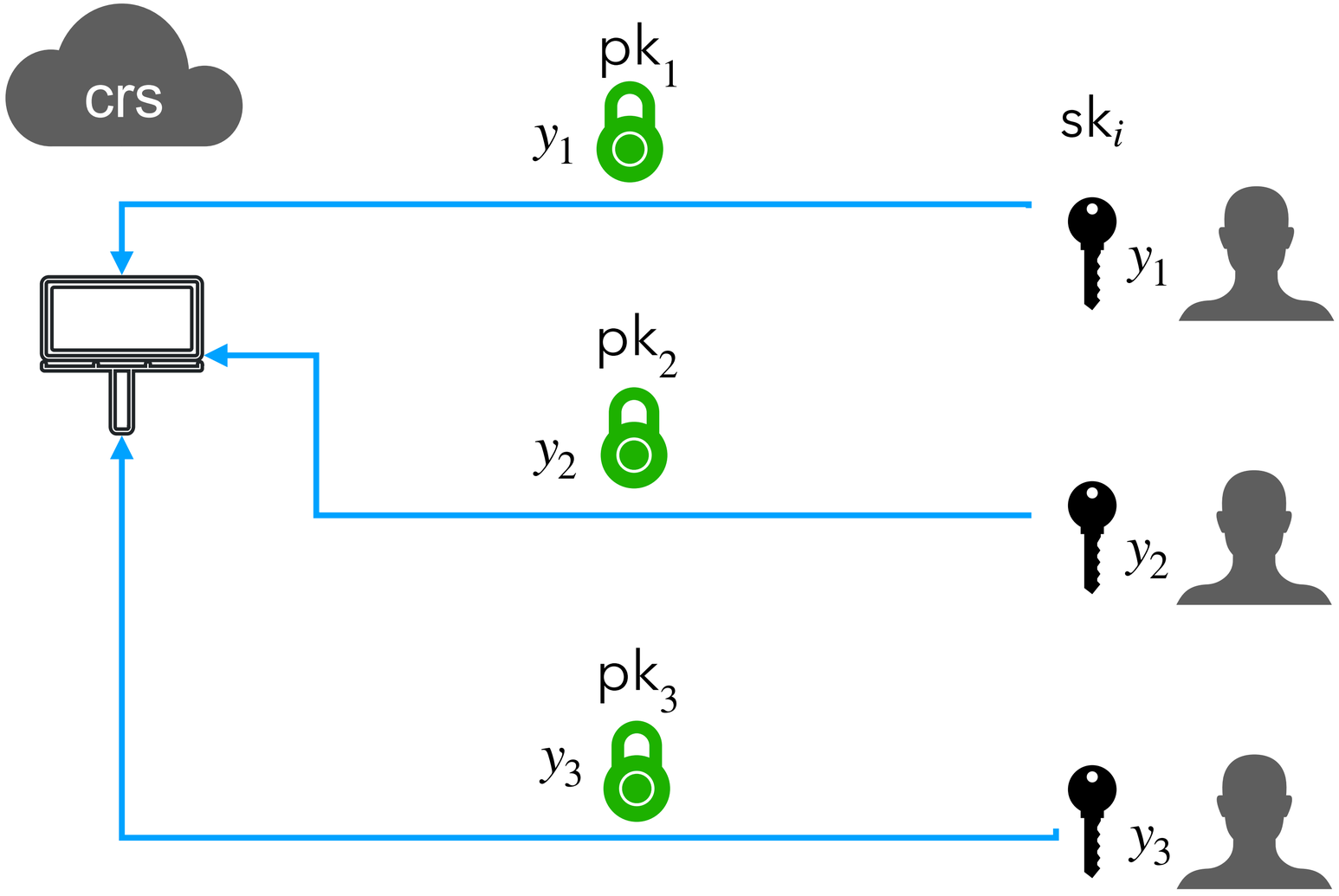
Gen(crs, i)

Ver(crs, i, pk$_i$)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

Enc(mpk, x, m)

Dec(sk,hsk,ct)



Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

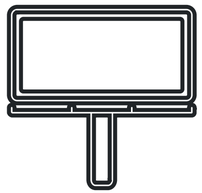
Gen(crs, i)

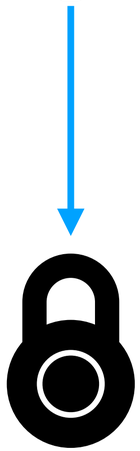
Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

Enc(mpk, x, m)

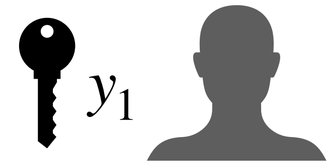
Dec(sk,hsk,ct)

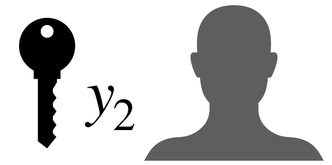


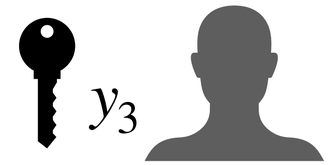


mpk

sk_i







Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

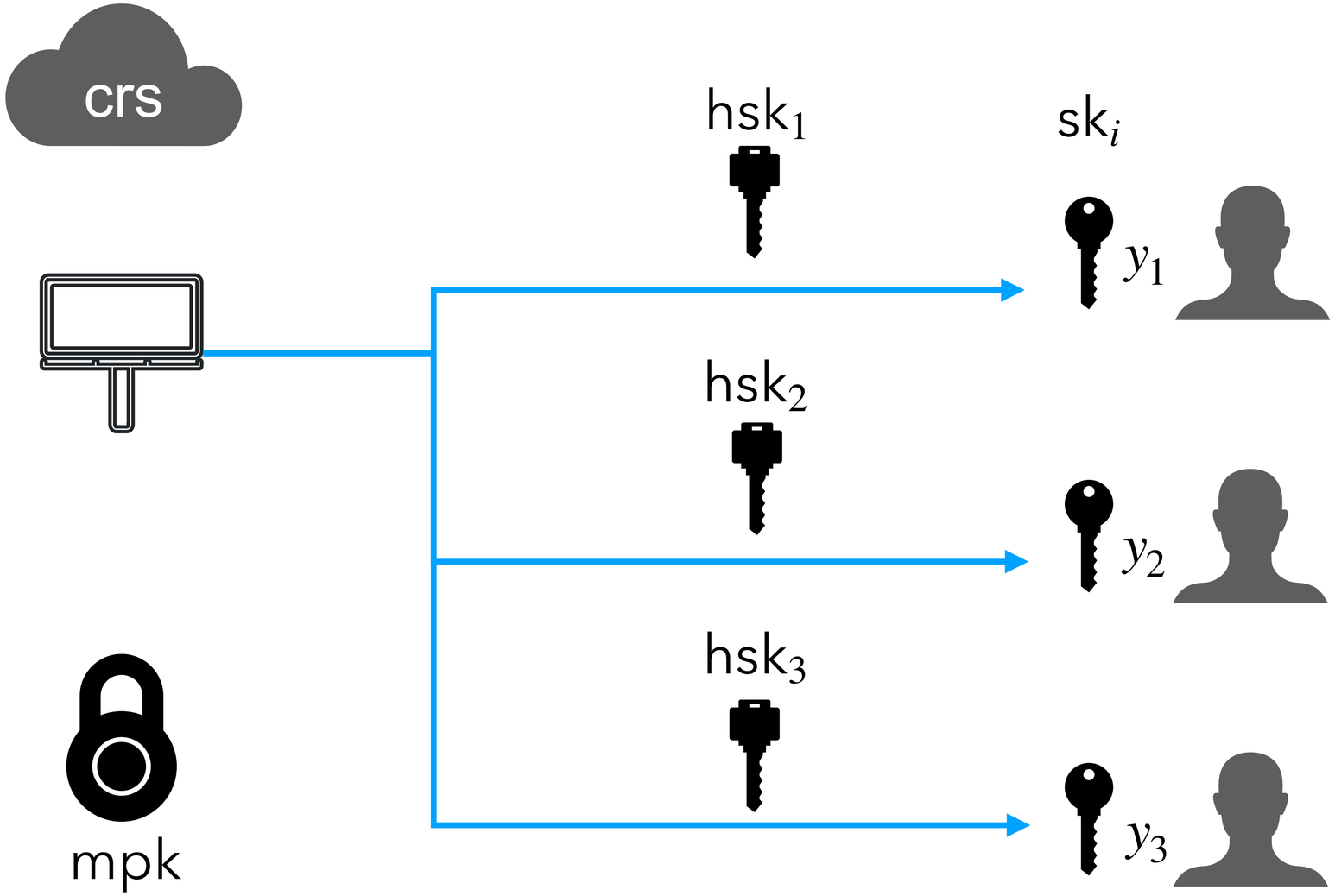
Gen(crs, i)

Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

Enc(mpk, x, m)

Dec(sk,hsk,ct)



Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

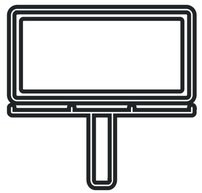
Gen(crs, i)

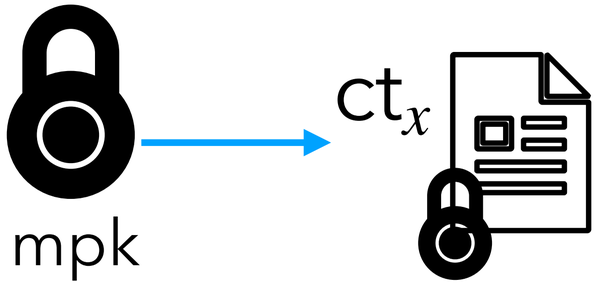
Ver(crs, i, pk_i)

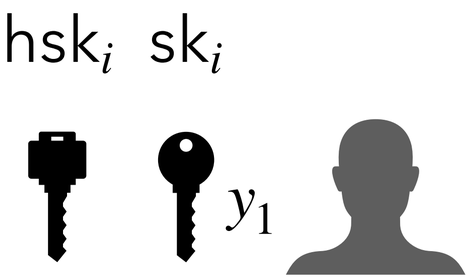
Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

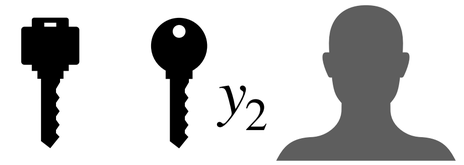
Enc(mpk, x, m)

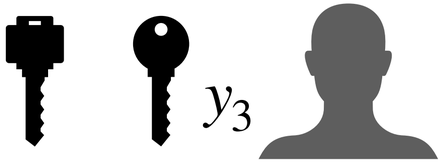
Dec(sk,hsk,ct)











Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

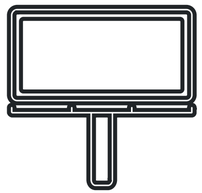
Gen(crs, i)

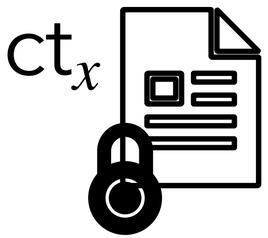
Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

Enc(mpk, x, m)

Dec(sk,hsk,ct)





Slotted Registered ABE (Reg-ABE) [HLWW23]

Setup$(1^\lambda, P, 1^L)$

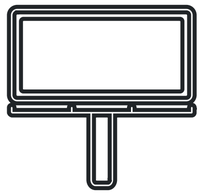
Gen(crs, i)

Ver(crs, i, pk_i)

Agg(crs, $(\mathsf{pk}_i, y_i)_{i\in[L]}$)

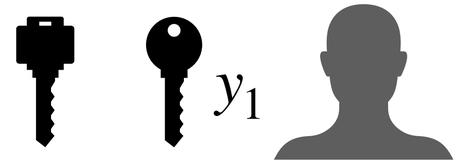
Enc(mpk, x, m)

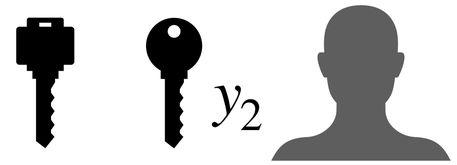
Dec(sk,hsk,ct)



mpk

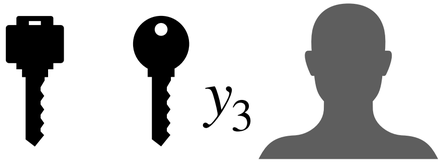
hsk_i sk_i





ct_x

$P(x, y_3) = 1$



Security of Slotted Reg-ABE [HLWW23]

Adversary

Challenger

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger

OGen(i)

1	2	3
$\mathscr{D}_1$	$\mathscr{D}_2$	$\mathscr{D}_3$

$\mathscr{C}$

OCor(i, pk)

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger

OGen(i)

Repeat:

i

pk

1	2	3
$\mathscr{D}_1$	$\mathscr{D}_2$	$\mathscr{D}_3$

$\mathscr{C}$

OCor(i, pk)

Run:

(pk,sk) ← Gen(crs, i)

Update:

$\mathscr{D}_i$[pk] = sk

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger

OGen(i)

1	2	3
$\mathscr{D}_1$	$\mathscr{D}_2$	$\mathscr{D}_3$

$\mathscr{C}$

OCor(i, pk)

Repeat:

i, pk →

← sk

Look up:

$$\text{sk} = \mathscr{D}_i[\text{pk}]$$

Update:

$$\mathscr{C} = \mathscr{C} \cup \{(i, \text{pk})\}$$

Security of Slotted Reg-ABE [HLWW23]

Adversary

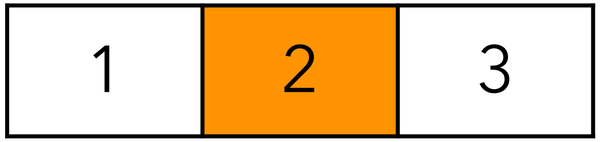
crs

Challenger

OGen(i)

$x^*, \{(\mathsf{pk}_i^*, y_i^*)\}_{i\in[3]}, (\mathsf{m}_0^*, \mathsf{m}_1^*)$

OCor(i, pk)



If $(i, \mathsf{pk}_i^*) \in \mathscr{C}$:
slot i is corrupted
require that:
$P(x^*, y_i^*) = 0$

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger

OGen(i)

$x^*, \{(\mathsf{pk}_i^*, y_i^*)\}_{i\in[3]}, (\mathsf{m}_0^*, \mathsf{m}_1^*)$

OCor(i, pk)

1	2	3
$\mathscr{D}_1$	$\mathscr{D}_2$	$\mathscr{D}_3$

$\mathscr{C}$

If $\mathscr{D}_i[\mathsf{pk}_i^*] = \perp$

slot i is malicious

require that:

$\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1$

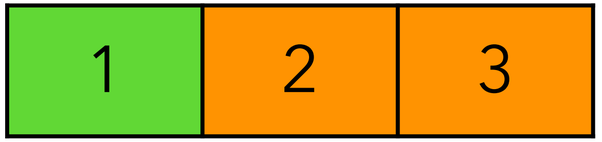
$P(x^*, y_i^*) = 0$

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger



$\mathscr{D}_1$ $\mathscr{D}_2$ $\mathscr{D}_3$ $\mathscr{C}$

OGen(i)

$x^*, \{(\mathsf{pk}_i^*, y_i^*)\}_{i\in[3]}, (\mathsf{m}_0^*, \mathsf{m}_1^*)$

OCor(i, pk)

Else:

slot i is honest

allow:

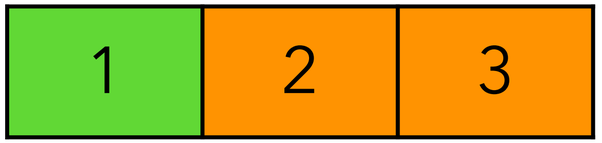
$$P(x^*, y_i^*) = 1$$

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger



$\mathscr{D}_1$ $\mathscr{D}_2$ $\mathscr{D}_3$ $\mathscr{C}$

OGen(i)

$x^*, \{(\mathsf{pk}_i^*, y_i^*)\}_{i\in[3]}, (\mathsf{m}_0^*, \mathsf{m}_1^*)$

$(\mathsf{mpk}, \{\mathsf{hsk}_i\}_{i\in[3]}), \mathsf{ct}^*$

OCor(i, pk)

$(\mathsf{mpk}, \{\mathsf{hsk}_i\}_{i\in[3]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i^*, y_i^*)_{i\in[3]})$

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

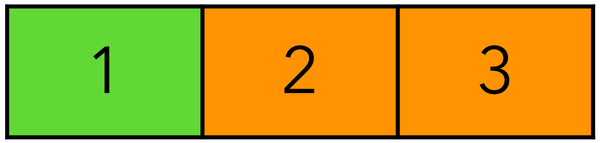
$\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, \mathsf{m}_b^*)$

Security of Slotted Reg-ABE [HLWW23]

Adversary

crs

Challenger



$\mathscr{D}_1$ $\mathscr{D}_2$ $\mathscr{D}_3$ $\mathscr{C}$

OGen(i)

$x^*, \{(\mathsf{pk}_i^*, y_i^*)\}_{i\in[3]}, (\mathsf{m}_0^*, \mathsf{m}_1^*)$

$(\mathsf{mpk}, \{\mathsf{hsk}_i\}_{i\in[3]}), \mathsf{ct}^*$

OCor(i, pk)

$(\mathsf{mpk}, \{\mathsf{hsk}_i\}_{i\in[3]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i^*, y_i^*)_{i\in[3]})$

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

$\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, \mathsf{m}_b^*)$

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

$$\mathsf{Adv} = \left|\Pr[b' = b] - \frac{1}{2}\right| = \mathsf{negl}$$

Current Works

Reference	Policy	Assumption	Prime Order?
[GKMR22]	Equality Check (IBE)	q-type / DBDH	✓
[HLWW23]	Span Program	Subgroup Decision	✗
[FFM+23]	(ah) Inner Product Predicate	GGM	✓
[FKP23]	Equality Check (IBE)	n-BDHE	✓
This work	Span Program	k-Lin	✓
This work	Inner Product Predicate	k-Lin	✓
This work	Arithmetic Branching Program	k-Lin	✓

ABE via Predicate Encodings [Wee14, CGW15]

$$P : X \times Y \to \{0,1\}$$

$$\mathsf{C}_x \in \mathbb{Z}_p^{n \times n_c}, \quad \mathsf{K}_y \in \mathbb{Z}_p^{n \times n_k}, \quad \mathsf{a}_y \in \mathbb{Z}_p^{1 \times n_k}, \quad \mathsf{d}_{x,y} \in \mathbb{Z}_p^{1 \times (n_c + n_k)} .$$

ABE via Predicate Encodings [Wee14, CGW15]

$$P : X \times Y \to \{0,1\}$$

$$\mathsf{C}_x \in \mathbb{Z}_p^{n \times n_c}, \quad \mathsf{K}_y \in \mathbb{Z}_p^{n \times n_k}, \quad \mathsf{a}_y \in \mathbb{Z}_p^{1 \times n_k}, \quad \mathsf{d}_{x,y} \in \mathbb{Z}_p^{1 \times (n_c + n_k)}.$$

$$\mathsf{M}_{x,y} = \begin{pmatrix} \mathsf{a}_y & 0 \\ \mathsf{K}_y & \mathsf{C}_x \end{pmatrix}$$

— $P(x,y) = 1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^\top = \mathsf{e}_1^\top$;

— $P(x,y) = 0$: $\{x, y, \alpha, (\alpha \| \mathsf{w})\mathsf{M}_{x,y}\} \approx_s \{x, y, \alpha, (0 \| \mathsf{w})\mathsf{M}_{x,y}\}$.

— **α-reconstruction**

— **α-privacy**

ABE via Predicate Encodings [Wee14, CGW15]

$$P : X \times Y \to \{0,1\}$$

$$\mathsf{C}_x \in \mathbb{Z}_p^{n \times n_c}, \quad \mathsf{K}_y \in \mathbb{Z}_p^{n \times n_k}, \quad \mathsf{a}_y \in \mathbb{Z}_p^{1 \times n_k}, \quad \mathsf{d}_{x,y} \in \mathbb{Z}_p^{1 \times (n_c + n_k)}.$$

$$\mathsf{M}_{x,y} = \begin{pmatrix} \mathsf{a}_y & 0 \\ \mathsf{K}_y & \mathsf{C}_x \end{pmatrix}$$

— $P(x,y) = 1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^\top = \mathsf{e}_1^\top$;

— $P(x,y) = 0$: $\{x, y, \alpha, (\alpha \| \mathsf{w})\mathsf{M}_{x,y}\} \approx_s \{x, y, \alpha, (0 \| \mathsf{w})\mathsf{M}_{x,y}\}$.

— **α-reconstruction**

— **α-privacy**

$\mathsf{mpk} : [\mathsf{w}, \alpha]$

$\mathsf{ct}_x : [s, s\mathsf{w}\mathsf{C}_x], [s\alpha] \cdot \mathsf{m}$

$\mathsf{sk}_y : \alpha\mathsf{a}_y + \mathsf{w}\mathsf{K}_y$

ABE via Predicate Encodings [Wee14, CGW15]

$$P : X \times Y \to \{0,1\}$$

$$\mathsf{C}_x \in \mathbb{Z}_p^{n \times n_c}, \quad \mathsf{K}_y \in \mathbb{Z}_p^{n \times n_k}, \quad \mathsf{a}_y \in \mathbb{Z}_p^{1 \times n_k}, \quad \mathsf{d}_{x,y} \in \mathbb{Z}_p^{1 \times (n_c + n_k)}.$$

$$\mathsf{M}_{x,y} = \begin{pmatrix} \mathsf{a}_y & 0 \\ \mathsf{K}_y & \mathsf{C}_x \end{pmatrix}$$

— $P(x,y) = 1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^\top = \mathsf{e}_1^\top$;

— $P(x,y) = 0$: $\{x, y, \alpha, (\alpha \| \mathsf{w})\mathsf{M}_{x,y}\} \approx_s \{x, y, \alpha, (0 \| \mathsf{w})\mathsf{M}_{x,y}\}$.

— **α-reconstruction**

— **α-privacy**

$\mathsf{mpk} : [\mathsf{w}, \alpha]$

$\mathsf{ct}_x : [s, s\mathsf{w}\mathsf{C}_x], [s\alpha] \cdot \mathsf{m}$

$\mathsf{sk}_y : \alpha\mathsf{a}_y + \mathsf{w}\mathsf{K}_y$

Decryption: $[(s \cdot (\alpha\mathsf{a}_y + \mathsf{w}\mathsf{K}_y) \| s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^\top] = [s(\alpha \| \mathsf{w})\mathsf{M}_{x,y}\mathsf{d}_{x,y}^\top]$

ABE via Predicate Encodings [Wee14, CGW15]

$$P : X \times Y \to \{0,1\}$$

$$\mathsf{C}_x \in \mathbb{Z}_p^{n \times n_c}, \quad \mathsf{K}_y \in \mathbb{Z}_p^{n \times n_k}, \quad \mathsf{a}_y \in \mathbb{Z}_p^{1 \times n_k}, \quad \mathsf{d}_{x,y} \in \mathbb{Z}_p^{1 \times (n_c + n_k)}.$$

$$\mathsf{M}_{x,y} = \begin{pmatrix} \mathsf{a}_y & 0 \\ \mathsf{K}_y & \mathsf{C}_x \end{pmatrix}$$

— $P(x,y) = 1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^\top = \mathsf{e}_1^\top$;

— $P(x,y) = 0$: $\{x, y, \alpha, (\alpha \| \mathsf{w})\mathsf{M}_{x,y}\} \approx_s \{x, y, \alpha, (0 \| \mathsf{w})\mathsf{M}_{x,y}\}$.

— **α-reconstruction**

— **α-privacy**

$\mathsf{mpk} : [\mathsf{w}, \alpha]$

$\mathsf{ct}_x : [s, s\mathsf{w}\mathsf{C}_x], [s\alpha] \cdot \mathsf{m}$

$\mathsf{sk}_y : \alpha\mathsf{a}_y + \mathsf{w}\mathsf{K}_y$

α-reconstruction

Decryption: $[(s \cdot (\alpha\mathsf{a}_y + \mathsf{w}\mathsf{K}_y) \| s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^\top] = [s(\alpha \| \mathsf{w})\mathsf{M}_{x,y}\mathsf{d}_{x,y}^\top] = [s(\alpha \| \mathsf{w})\mathsf{e}_1^\top] = [s\alpha]$

From ABE to Zero-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{mpk}:[\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

$\mathsf{sk}_y:\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y$

Decryption: $[(s\cdot(\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y)\|s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^{\top}]$

From ABE to Zero-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{mpk}:[\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

$\mathsf{sk}_y:\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y$

Embed y into mpk

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{mpk}_y:[\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s\alpha\mathsf{a}_y+s\mathsf{w}\mathsf{K}_y,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

Decryption: $[(s\cdot(\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y)\|s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^{\top}]$

From ABE to Zero-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{mpk}:[\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

$\mathsf{sk}_y:\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y$

Embed y into mpk

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{mpk}_y:[\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s\alpha\mathsf{a}_y+s\mathsf{w}\mathsf{K}_y,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

Decryption: $[(s\cdot(\alpha\mathsf{a}_y+\mathsf{w}\mathsf{K}_y)\|s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^{\top}]=[s\alpha]$

α-reconstruction

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$$\mathsf{crs}:[\mathsf{w},\alpha]$$

$$\mathsf{pk}:[u]$$

$$\mathsf{sk}:u$$

$$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{w}\mathsf{K}_y,\mathsf{w},\alpha]$$

$$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{w}\mathsf{K}_y,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$$

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{w}\mathsf{K}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{w}\mathsf{K}_y,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{w}\mathsf{K}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{w}\mathsf{K}_y,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

α-reconstruction

Decryption: $[(s\cdot((\alpha+u)\mathsf{a}_y+\mathsf{w}\mathsf{K}_y)\|s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^{\top}]=[s\alpha+su]$

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{w}\mathsf{K}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{w}\mathsf{K}_y,s\mathsf{w}\mathsf{C}_x],[s\alpha]\cdot\mathsf{m}$

Decryption: $[(s\cdot((\alpha+u)\mathsf{a}_y+\mathsf{w}\mathsf{K}_y)\|s\mathsf{w}\mathsf{C}_x)\mathsf{d}_{x,y}^{\top}]=[s\alpha+su]$

$[s\alpha+su]-[su]=[s\alpha]$

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{wK}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{wK}_y,s\mathsf{wC}_x],[s\alpha]\cdot\mathsf{m}$

Security

Honest: u is secret

Corrupted: u is leaked

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{wK}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{wK}_y,s\mathsf{wC}_x],[s\alpha]\cdot\mathsf{m}$

Security

Honest: u is secret

Corrupted: u is leaked

Allow $P(x,y)=1$

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{wK}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{wK}_y,s\mathsf{wC}_x],[s\alpha]\cdot\mathsf{m}$

Security

Honest: u is secret

Corrupted: u is leaked

Allow $P(x,y)=1$

α hidden by u

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{wK}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{wK}_y,s\mathsf{wC}_x],[s\alpha]\cdot\mathsf{m}$

Security

Honest: u is secret

Corrupted: u is leaked

Allow $P(x,y)=1$

Require $P(x,y)=0$

α hidden by u

To One-slot Reg-ABE

— $P(x,y)=1$: $\mathsf{M}_{x,y}\mathsf{d}_{x,y}^{\top}=\mathsf{e}_1^{\top}$; — α-reconstruction

— $P(x,y)=0$: $\{x,y,\alpha,(\alpha\|\mathsf{w})\mathsf{M}_{x,y}\}\approx_s\{x,y,\alpha,(0\|\mathsf{w})\mathsf{M}_{x,y}\}$. — α-privacy

$\mathsf{crs}:[\mathsf{w},\alpha]$

$\mathsf{pk}:[u]$

$\mathsf{sk}:u$

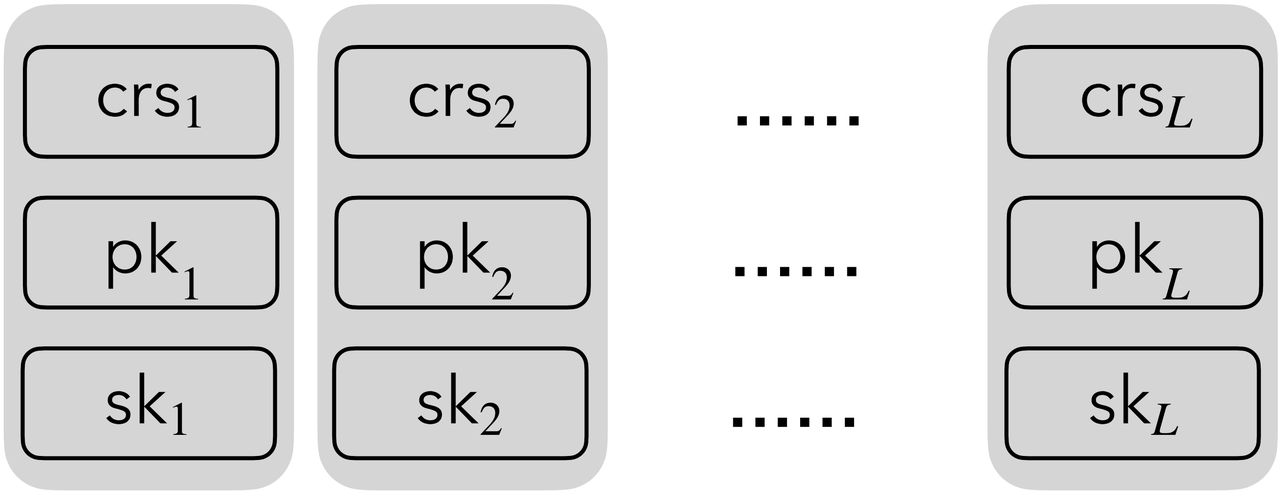
$\mathsf{mpk}_y:[(\alpha+u)\mathsf{a}_y+\mathsf{wK}_y,\mathsf{w},\alpha]$

$\mathsf{ct}_x:[s,s(\alpha+u)\mathsf{a}_y+s\mathsf{wK}_y,s\mathsf{wC}_x],[s\alpha]\cdot\mathsf{m}$

Security	
Honest: u is secret	Corrupted: u is leaked
Allow $P(x,y)=1$	Require $P(x,y)=0$
α hidden by u	α-privacy

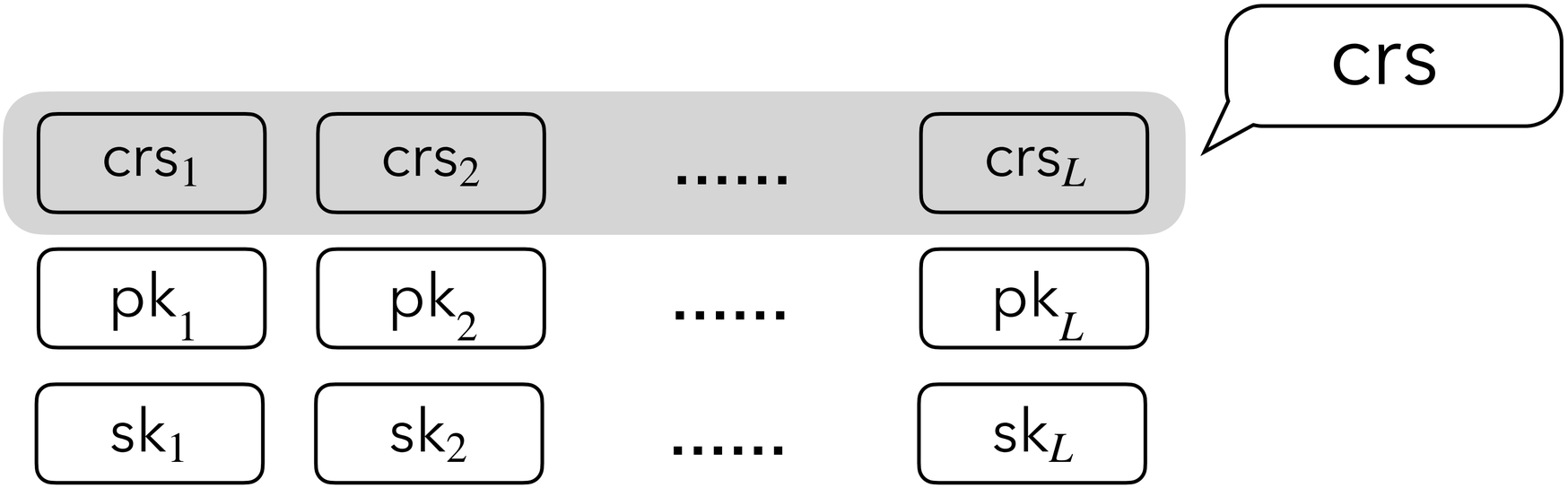
To L-slot Reg-ABE

Generate L parallel one-slot instances



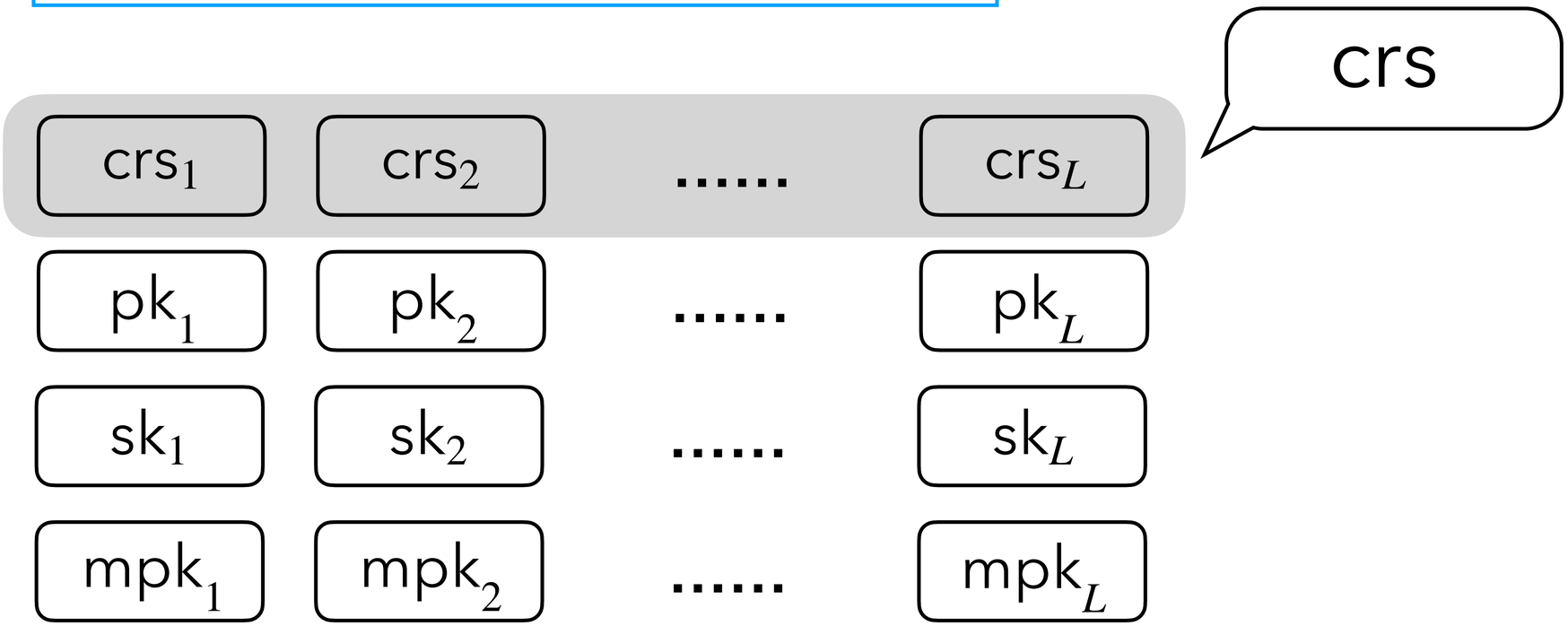
To L-slot Reg-ABE

Generate L parallel one-slot instances



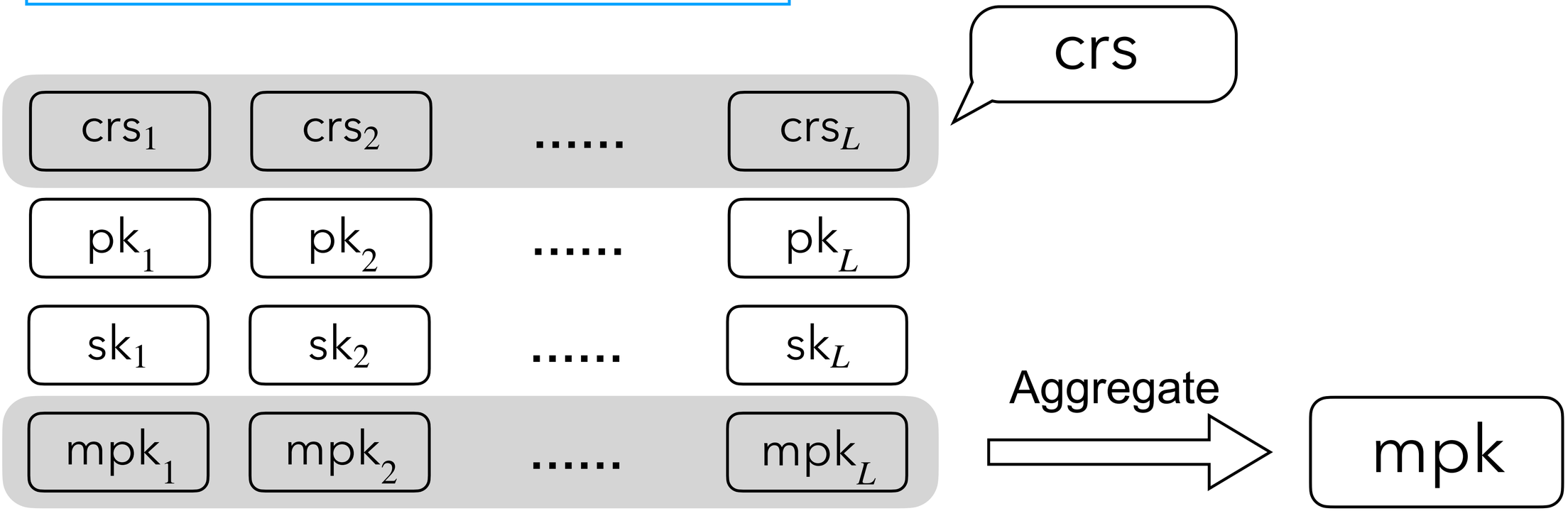
To L-slot Reg-ABE

Aggregate mpk_i of each instance



To L-slot Reg-ABE

Aggregate mpk_i of each instance



To L-slot Reg-ABE

$$\mathsf{crs} : [\mathsf{w}_j, \alpha_j], \quad \forall j$$

$$\mathsf{pk}_i : [u_i]$$

$$\mathsf{sk}_i : \ u_i$$

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j, \sum_j \alpha_j]$$

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

To L-slot Reg-ABE

$\mathsf{crs} : [\mathsf{w}_j, \alpha_j], \quad \forall j$

$\mathsf{pk}_i : [u_i]$

$\mathsf{sk}_i : u_i$

How to decrypt with sk_i, when $P(x, y_i) = 1$?

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j, \sum_j \alpha_j]$$

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

To L-slot Reg-ABE

$\mathsf{crs} : [\mathsf{w}_j, \alpha_j], \quad \forall j$

$\mathsf{pk}_i : [u_i]$

$\mathsf{sk}_i : \ u_i$

How to decrypt with sk_i, when $P(x, y_i) = 1$?

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j, \sum_j \alpha_j]$$

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $\quad [s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]$

// mixed part $\quad [s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]$

To L-slot Reg-ABE

$\mathsf{crs} : [\mathsf{w}_j, \alpha_j], \quad \forall j$

$\mathsf{pk}_i : [u_i]$

$\mathsf{sk}_i : u_i$

How to decrypt with sk_i, when $P(x, y_i) = 1$?

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j, \sum_j \alpha_j]$$

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $\quad [s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x] \longrightarrow$ Handle with sk_i

// mixed part $\quad [s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]$

To L-slot Reg-ABE

$\mathsf{crs} : [\mathsf{w}_j, \alpha_j], \quad \forall j$

$\mathsf{pk}_i : [u_i]$

$\mathsf{sk}_i : u_i$

How to decrypt with sk_i, when $P(x, y_i) = 1$?

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j, \sum_j \alpha_j]$$

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]$ ⟶ Handle with sk_i

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]$ ⟶ How to remove?

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]$

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]$

A naive solution

$$\mathsf{hsk}_i : \sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_{j\neq i} \mathsf{w}_j$$

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]$

// mixed part $[s, s\sum_{j\neq i}((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i}\mathsf{w}_j\mathsf{C}_x]$

A naive solution

$$\mathsf{hsk}_i : \sum_{j\neq i}((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_{j\neq i}\mathsf{w}_j$$

suffer from “mix-and-match” attack

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x], [s\sum_j \alpha_j] \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]$

Introduce random coin and bilinear group

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\sum_j \alpha_j]_T \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]_1$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]_1$

Introduce random coin and bilinear group

$$\mathsf{hsk}_i : [r_i, r_i\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i\sum_{j\neq i} \mathsf{w}_j]_2$$

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\sum_j \alpha_j]_T \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]_1 \xrightarrow{\mathsf{sk}_i} [sr_i\alpha_i]_T$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]_1 \xrightarrow{\mathsf{hsk}_i} [0]_T$

Introduce random coin and bilinear group

$$\mathsf{hsk}_i : [r_i, r_i\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i\sum_{j\neq i} \mathsf{w}_j]_2$$

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\sum_j \alpha_j]_T \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]_1 \xrightarrow{\mathsf{sk}_i} [sr_i\alpha_i]_T$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]_1 \xrightarrow{\mathsf{hsk}_i} [0]_T$

Introduce random coin and bilinear group

$$\mathsf{hsk}_i : [r_i, r_i\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i\sum_{j\neq i} \mathsf{w}_j]_2$$

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\alpha]_T \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]_1 \xrightarrow{\mathsf{sk}_i} [sr_i\alpha_i]_T$

// mixed part $[s, s\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i} \mathsf{w}_j\mathsf{C}_x]_1 \xrightarrow{\mathsf{hsk}_i} [0]_T$

Introduce random coin and bilinear group

$$\mathsf{hsk}_i : [r_i, r_i\sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i\sum_{j\neq i} \mathsf{w}_j]_2, [r_i\alpha_i + \alpha]_2$$

Helper Keys — to Remove Mixed Part

$$\mathsf{ct}_x : [s, s\sum_j((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\alpha]_T \cdot \mathsf{m}$$

// local part $[s, s((\alpha_i + u_i)\mathsf{a}_{y_i} + \mathsf{w}_i\mathsf{K}_{y_i}), s\mathsf{w}_i\mathsf{C}_x]_1 \xrightarrow{\mathsf{sk}_i} [sr_i\alpha_i]_T$

// mixed part $[s, s\sum_{j\neq i}((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s\sum_{j\neq i}\mathsf{w}_j\mathsf{C}_x]_1 \xrightarrow{\mathsf{hsk}_i} [0]_T$

Introduce random coin and bilinear group

$$\mathsf{hsk}_i : [r_i, r_i\sum_{j\neq i}((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i\sum_{j\neq i}\mathsf{w}_j]_2, [r_i\alpha_i + \alpha]_2$$

$$e([s]_1, [r_i\alpha_i + \alpha]_2) \cdot [sr_i\alpha_i]_T^{-1} = [s\alpha]_T$$

Summary of L-slot Reg-ABE

$$\mathsf{crs} : [\alpha]_T, [\alpha_j, \mathsf{w}_j]_1, \quad \forall j$$
$$[r_i, r_i\alpha_i + \alpha, r_i\alpha_j, r_i\mathsf{w}_j]_2, \quad \forall i \neq j$$

$$\mathsf{pk}_i : [u_i]_1, [u_i r_j]_2, \quad \forall j \neq i$$

$$\mathsf{sk}_i : u_i$$

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j]_1, [\alpha]_T$$

$$\mathsf{hsk}_i : [r_i, r_i \sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i \sum_{j\neq i} \mathsf{w}_j, r_i\alpha_i + \alpha]_2$$

$$\mathsf{ct}_x : [s, s \sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s \sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\alpha]_T \cdot \mathsf{m}$$

Summary of L-slot Reg-ABE

$$\mathsf{crs} : [\alpha]_T, [\alpha_j, \mathsf{w}_j]_1, \quad \forall j$$

$$[r_i, r_i\alpha_i + \alpha, r_i\alpha_j, r_i\mathsf{w}_j]_2, \quad \forall i \neq j$$

$$\mathsf{pk}_i : [u_i]_1, [u_i r_j]_2, \quad \forall j \neq i$$

$$\mathsf{sk}_i : u_i$$

$$\mathsf{mpk} : [\sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), \sum_j \mathsf{w}_j]_1, [\alpha]_T$$

$$\mathsf{hsk}_i : [r_i, r_i \sum_{j\neq i} ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), r_i \sum_{j\neq i} \mathsf{w}_j, r_i\alpha_i + \alpha]_2$$

$$\mathsf{ct}_x : [s, s \sum_j ((\alpha_j + u_j)\mathsf{a}_{y_j} + \mathsf{w}_j\mathsf{K}_{y_j}), s \sum_j \mathsf{w}_j\mathsf{C}_x]_1, [s\alpha]_T \cdot \mathsf{m}$$

Gentry-Waters BE [GW09]

L-slot Reg-ABE in Prime Version

With “composite-to-prime-order” transformation in [CGW15]

$$\mathsf{crs}: [\mathsf{A}]_1, [\mathsf{Ak}^\top]_T, [\mathsf{AV}_j, \mathsf{AW}_j]_1, \quad \forall j$$
$$[\mathsf{Br}_i^\top, \mathsf{V}_i\mathsf{Br}_i^\top + \mathsf{k}^\top, \mathsf{V}_j\mathsf{Br}_i^\top, \mathsf{W}_j(\mathsf{I}_n \otimes \mathsf{Br}_i^\top)]_2, \quad \forall i \neq j$$

$$\mathsf{pk}_i: [\mathsf{AU}_i]_1, [\mathsf{U}_i\mathsf{Br}_j^\top]_2, \quad \forall j \neq i$$

$$\mathsf{sk}_i: \mathsf{U}_i$$

$$\mathsf{mpk}: [\mathsf{A}, \sum_j ((\mathsf{AV}_j + \mathsf{AU}_j)(\mathsf{a}_{y_j} \otimes \mathsf{I}_n) + (\mathsf{AW}_j(\mathsf{K}_{y_j} \otimes \mathsf{I}_n)), \sum_j \mathsf{AW}_j]_1, [\mathsf{Ak}^\top]_T$$

$$\mathsf{hsk}_i: [\mathsf{Br}_i^\top, \sum_{j\neq i} ((\mathsf{V}_j\mathsf{Br}_i^\top + \mathsf{U}_j\mathsf{Br}_i^\top)\mathsf{a}_{y_j} + \mathsf{W}_j(\mathsf{I}_n \otimes \mathsf{Br}_i^\top\mathsf{K}_{y_j}), \sum_{j\neq i} \mathsf{W}_j(\mathsf{I}_n \otimes \mathsf{Br}_i^\top, \mathsf{V}_i\mathsf{Br}_i^\top + \mathsf{k}^\top]_2$$

$$\mathsf{ct}_x: [\mathsf{sA}, \mathsf{s}\sum_j ((\mathsf{AV}_j + \mathsf{AU}_j)(\mathsf{a}_{y_j} \otimes \mathsf{I}_n) + (\mathsf{AW}_j(\mathsf{K}_{y_j} \otimes \mathsf{I}_n)), \mathsf{s}\sum_j \mathsf{AW}_j]_1, [\mathsf{sAk}^\top]_T \cdot \mathsf{m}$$

L-slot Reg-ABE in Prime Version

Analogous to the dual-system proof for ABE [Wat09,Wee14,CGW15]

$$\mathsf{crs}: [\mathsf{A}]_1, [\mathsf{Ak}^\top]_T, [\mathsf{AV}_j, \mathsf{AW}_j]_1, \quad \forall j$$
$$[\mathsf{Br}_i^\top, \mathsf{V}_i\mathsf{Br}_i^\top + \mathsf{k}^\top, \mathsf{V}_j\mathsf{Br}_i^\top, \mathsf{W}_j(\mathsf{I}_n \otimes \mathsf{Br}_i^\top)]_2, \quad \forall i \neq j$$

$$\mathsf{pk}_i: [\mathsf{AU}_i]_1, [\mathsf{U}_i\mathsf{Br}_j^\top]_2, \quad \forall j \neq i$$

$$\mathsf{sk}_i: \mathsf{U}_i$$

$$\mathsf{mpk}: [\mathsf{A}, \sum_j ((\mathsf{AV}_j + \mathsf{AU}_j)(\mathsf{a}_{y_j} \otimes \mathsf{I}_n) + (\mathsf{AW}_j(\mathsf{K}_{y_j} \otimes \mathsf{I}_n)), \sum_j \mathsf{AW}_j]_1, [\mathsf{Ak}^\top]_T$$

$$\mathsf{hsk}_i: [\mathsf{Br}_i^\top, \sum_{j\neq i} ((\mathsf{V}_j\mathsf{Br}_i^\top + \mathsf{U}_j\mathsf{Br}_i^\top)\mathsf{a}_{y_j} + \mathsf{W}_j(\mathsf{I}_n \otimes \mathsf{Br}_i^\top\mathsf{K}_{y_j}), \sum_{j\neq i} \mathsf{W}_j(\mathsf{I}_n \otimes \mathsf{Br}_i^\top, \mathsf{V}_i\mathsf{Br}_i^\top + \mathsf{k}^\top]_2$$

$$\mathsf{ct}_x: [\mathsf{sA}, \mathsf{s}\sum_j ((\mathsf{AV}_j + \mathsf{AU}_j)(\mathsf{a}_{y_j} \otimes \mathsf{I}_n) + (\mathsf{AW}_j(\mathsf{K}_{y_j} \otimes \mathsf{I}_n)), \mathsf{s}\sum_j \mathsf{AW}_j]_1, [\mathsf{sAk}^\top]_T \cdot \mathsf{m}$$

Handle Malicious pk

In dual-system proof: Need to simulate $[cU]_1$ without U

pk : $[T = AU]_1$

Handle Malicious pk

In dual-system proof: Need to simulate $[cU]_1$ without U

pk : $[T = AU]_1$
$[Q = RU]_1$

Allow embedding $[c]_1$ into $[R]_1$

Handle Malicious pk

In dual-system proof: Need to simulate $[cU]_1$ without U

$$\text{pk}: \begin{matrix}[T = AU]_1 \\ [Q = RU]_1\end{matrix}$$

Allow embedding $[c]_1$ into $[R]_1$

Inconsistent case:

$$\text{pk}: \begin{matrix}[T = AU]_1 \\ [Q = RU']_1\end{matrix}$$

where $U \neq U'$

Handle Malicious pk

In dual-system proof: Need to simulate $[cU]_1$ without U

$$\mathsf{pk}: \begin{matrix}[T = AU]_1 \\ [Q = RU]_1\end{matrix}$$

Allow embedding $[c]_1$ into $[R]_1$

Inconsistent case:

$$\mathsf{pk}: \begin{matrix}[T = AU]_1 \\ [Q = RU']_1\end{matrix}$$

where $U \neq U'$

Employ QA-NIZK to avoid this case

Open Problems

1. (Weak) attribute-hiding Reg-IPE under standard assumption;
2. Reg-ABE via pair encodings;
3. Directly build full-fledge Reg-ABE without slotted scheme;
4. Improve the efficiency of Reg-ABE;

……

Thank You!