Registered (Inner-Product) Functional Encryption

Danilo Francati[1], Daniele Friolo[2], Monosij Maitra[3,5], Giulio Malavolta[4,5], Ahmadreza Rahimi[5], Daniele Venturi[2]

[1]Aarhus University, Denmark
[2]Sapienza University of Rome
[3]Ruhr-Universität Bochum, Germany
[4]Bocconi University, Italy
[5]Max-Planck Institute for Security and Privacy, Germany

AARHUS UNIVERSITY

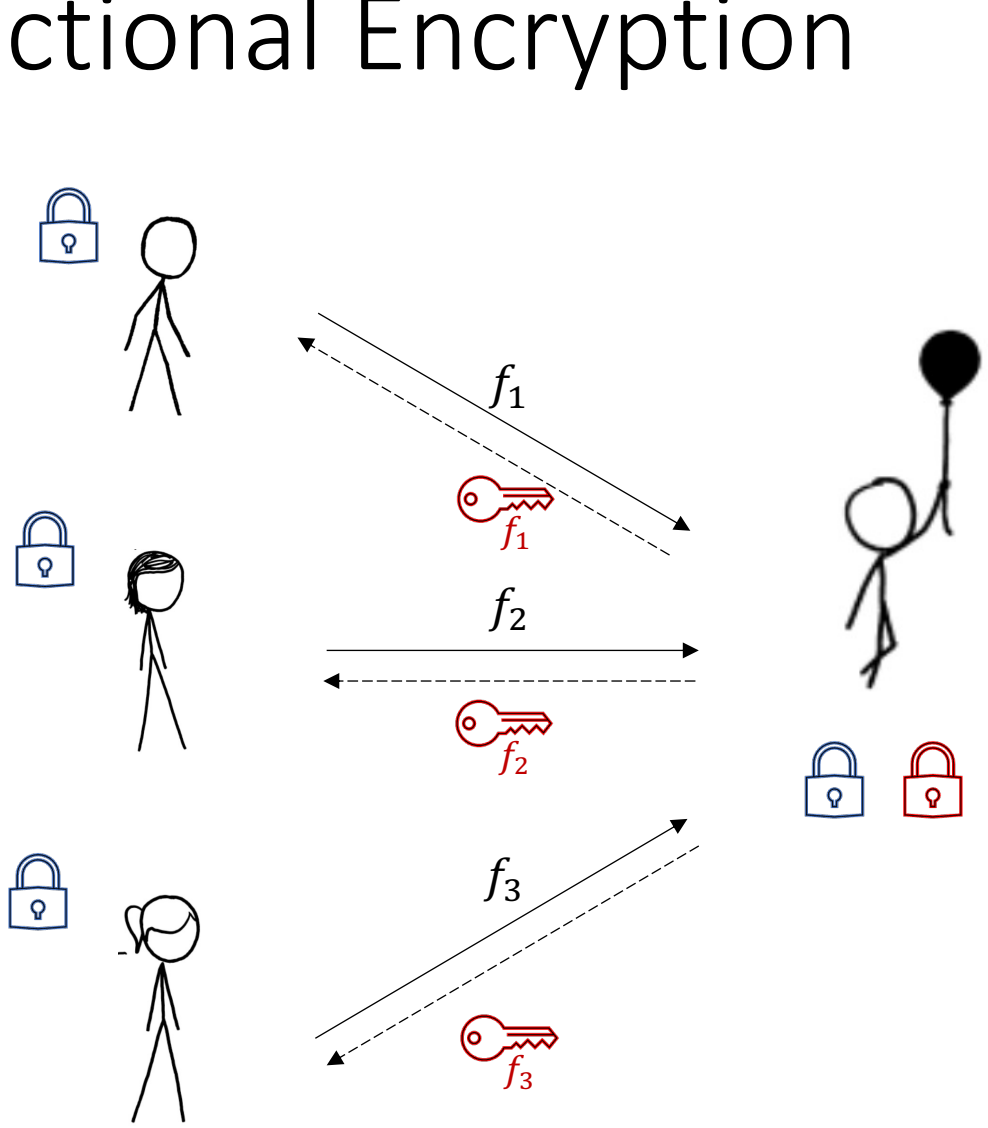
SAPIENZA UNIVERSITÀ DI ROMA

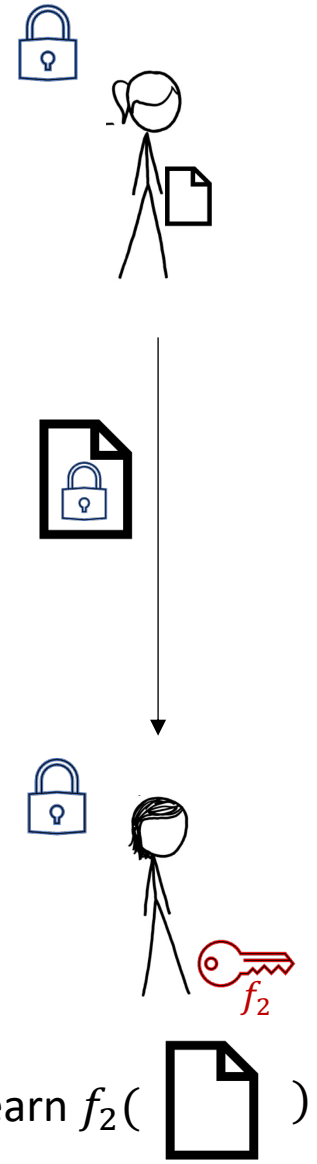
RUHR UNIVERSITÄT BOCHUM RUB

Università Bocconi MILANO

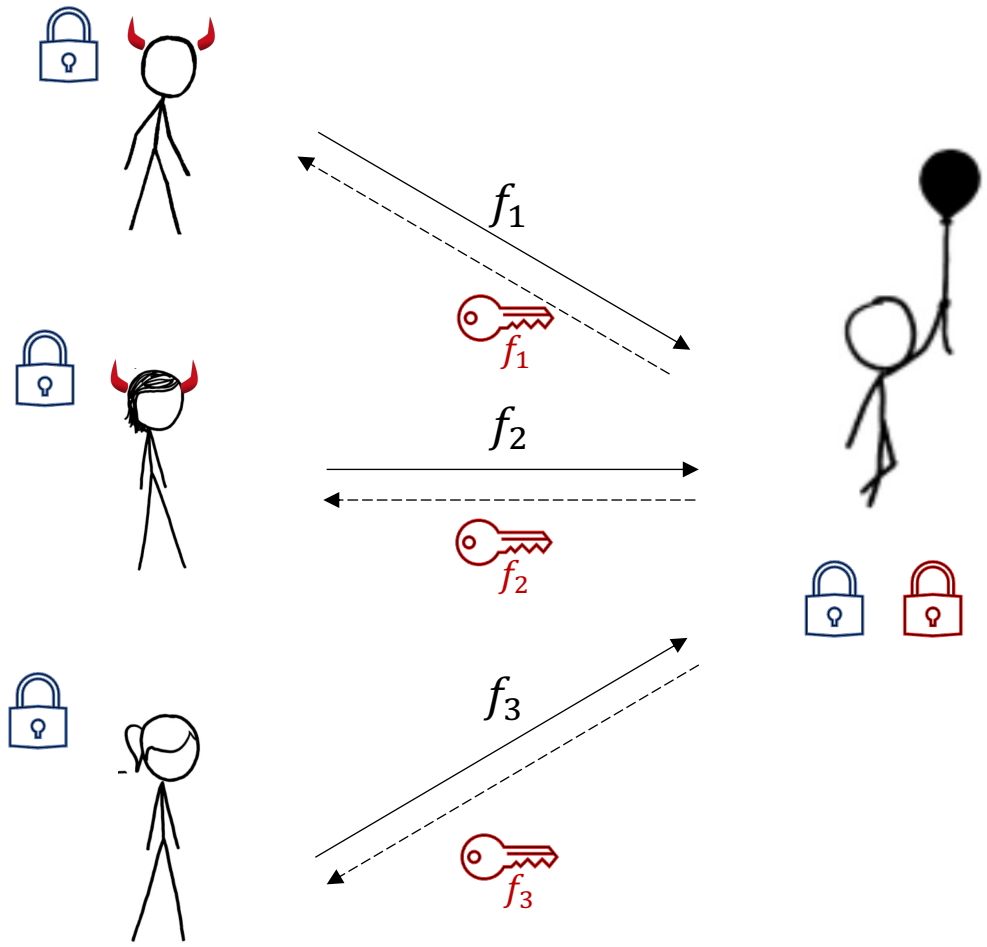
MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

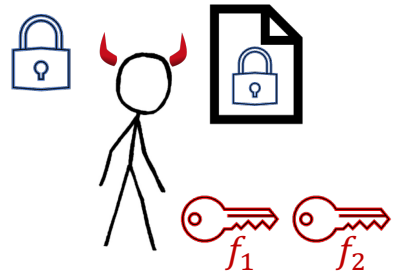
Functional Encryption





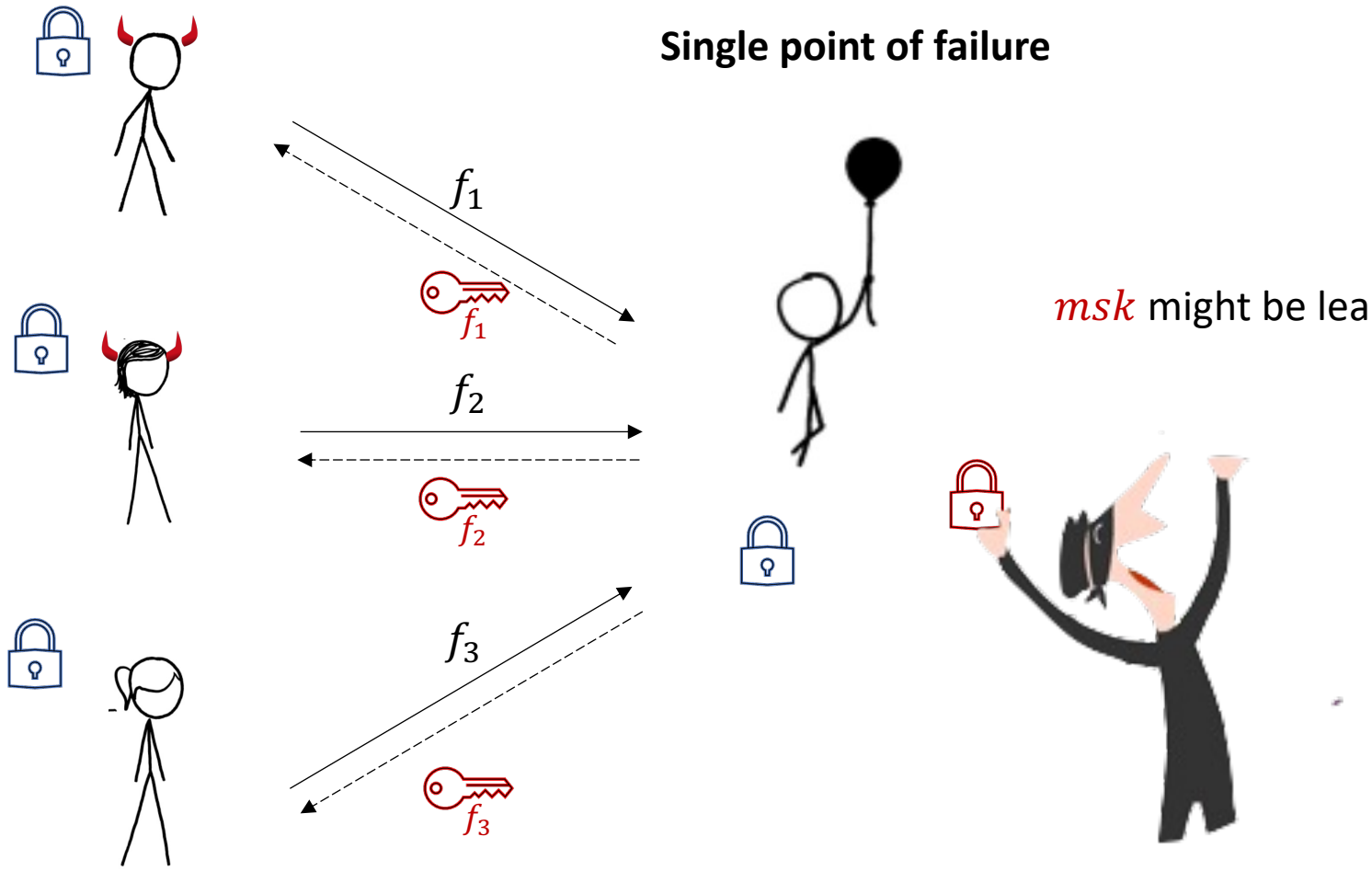
Functional Encryption





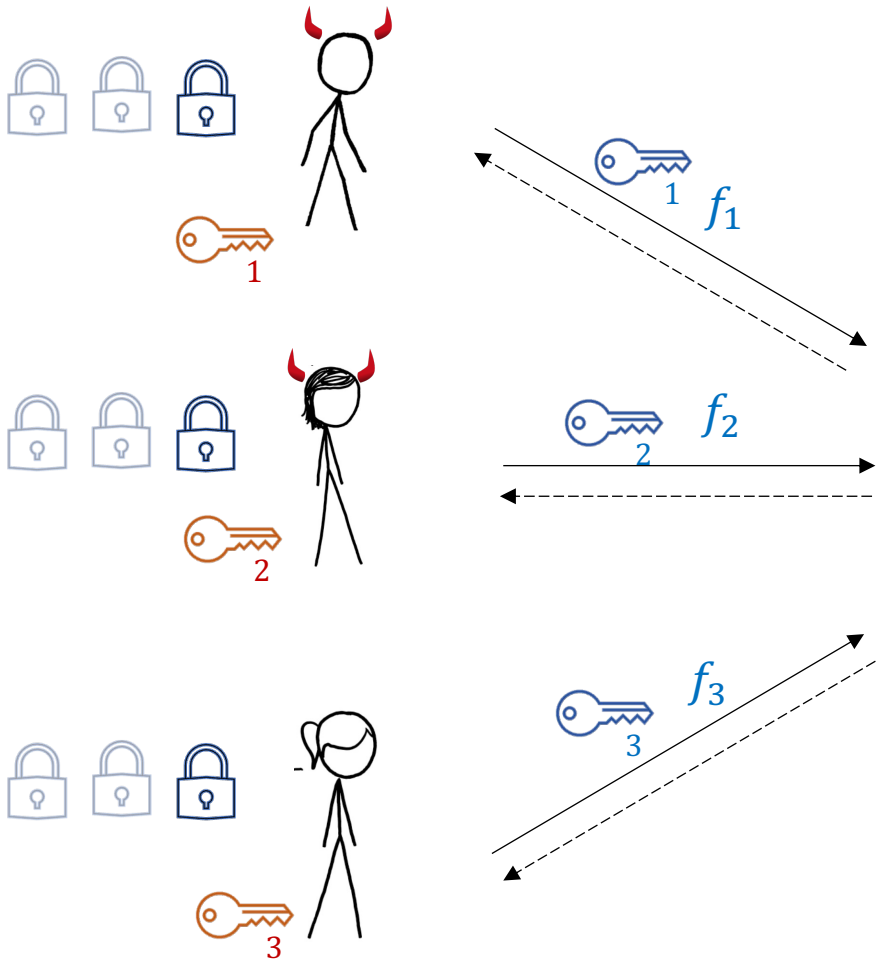
Cannot learn $f_{\neq 1,2}$()

Key-Escrow Problem



msk might be leaked

Registered Functional Encryption



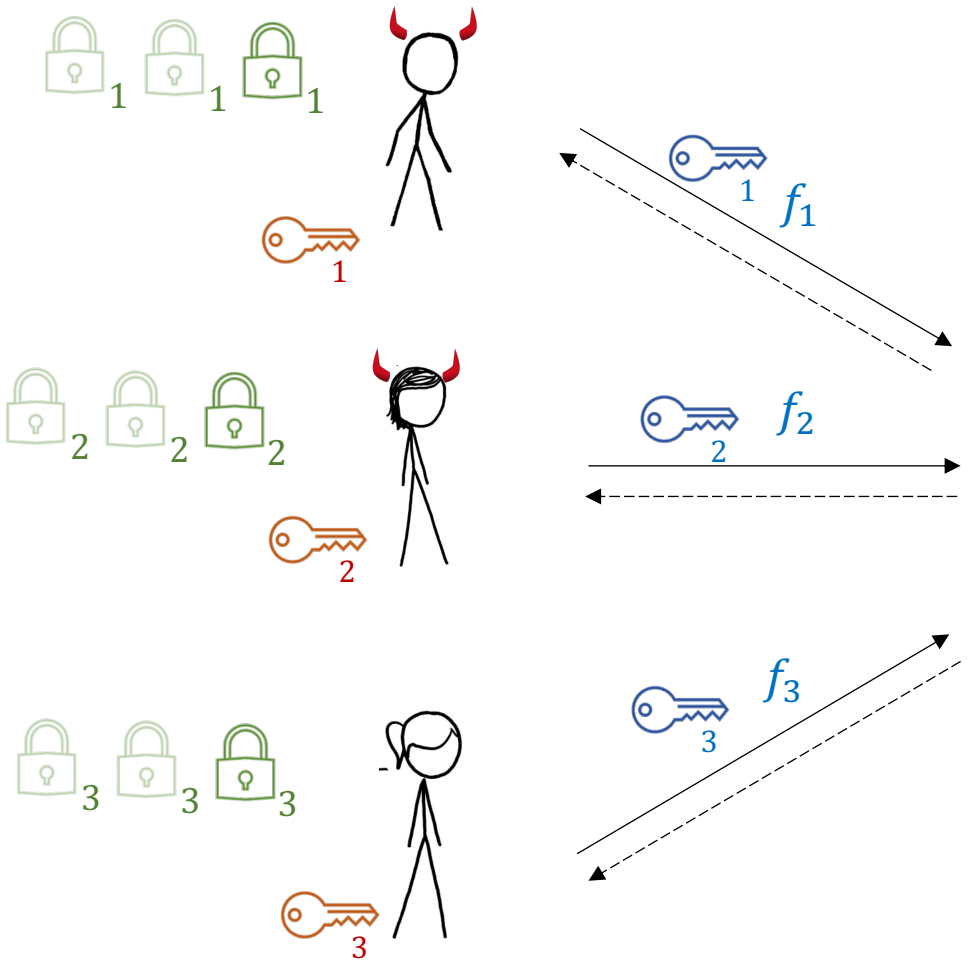
Key Curator

mpk is updated periodically

can be malformed

Trivial solution

Registered Functional Encryption



Key Curator

mpk is updated periodically

hks_i produced at each update connecting mpk and 

Requirements:

$L = \#\text{Users}$

$|crs|, |hks_i|, |mpk|$
= **polylog** in L

Keygen and registration run in **polylog** time in L

$\#\text{Updates} = O(logL)$

Our Contributions

- *Registered (attribute-hiding) Inner Product Encryption*
  from prime order groups in the bilinear GGM. Recasted in RFE as:

$$f_{\mathbf{x}}(m, \mathbf{y}) = \begin{cases} m & \text{if } \langle \mathbf{x}, \mathbf{y} \rangle = 0 \\ \perp & \text{otherwise} \end{cases}$$

- *Registered Functional Encryption*
  from iO and SSB hash functions for generic functionalities and large universe of users

Similar blueprint of [HLWW22] Registered Attribute-Based Encryption

Comparison with [HLWW22] RABE:

- *Our RIPE*

PROS:

- Large function space: n-size vectors
- Strong attribute-hiding:
  - CPA-2-sided security

CONS:

- Inner-Product
- Pairings of prime order + GGM

- *[HLWW22] RABE*

CONS:

- Small attribute space
- Attributes in clear

PROS:

- LSSS policies
- Pairings of composite order

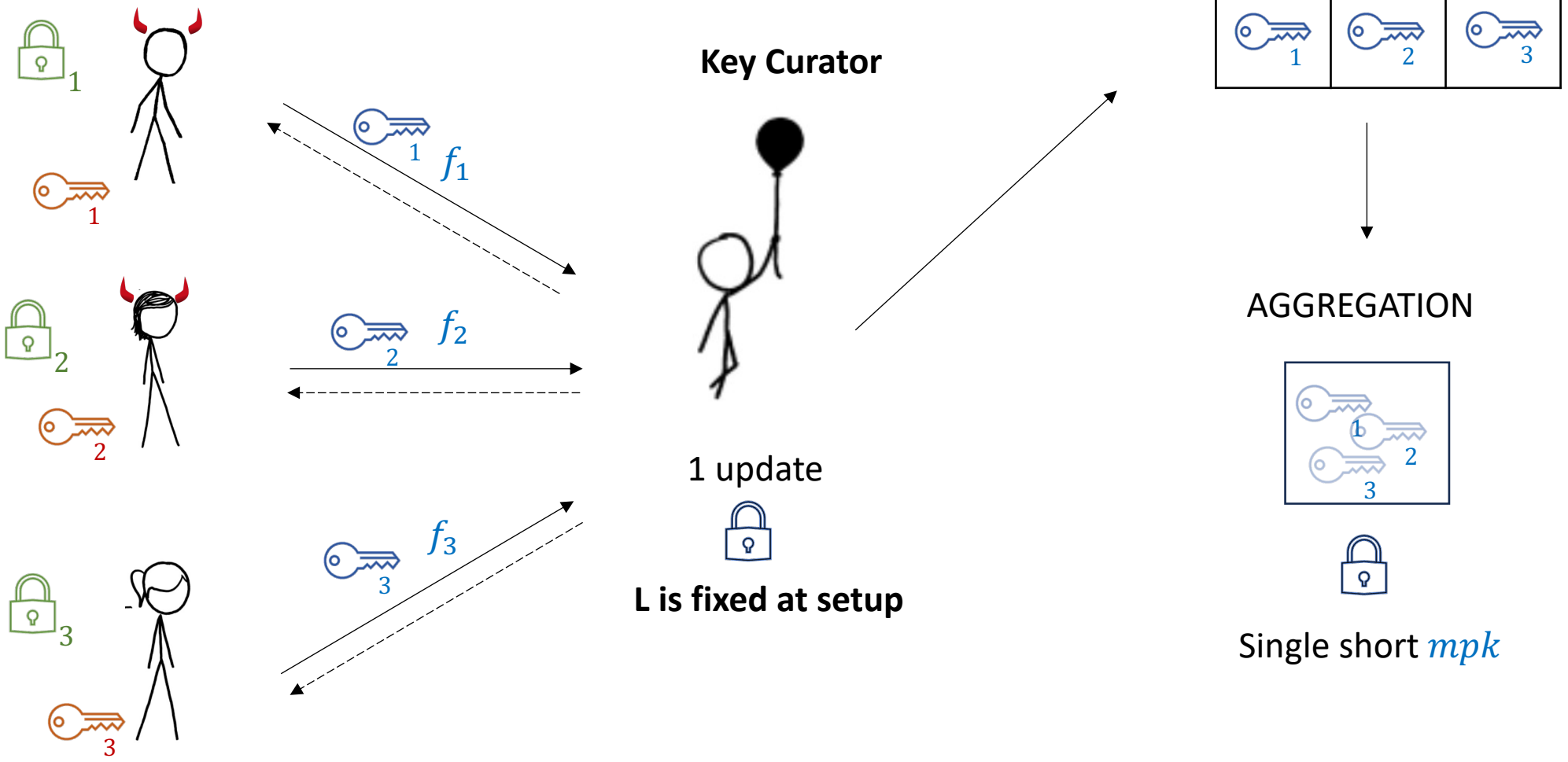
Both CONs:

- Require a bounded number of users
- CRS, Kgen and registration runtime dependent on L

Comparison with [HLWW22] RABE:

Reference	Type	CRS size	Keygen runtime	Registration key runtime	Master public key size	Helper dec. key size	# Updates	Unbounded users	BB	Assumptions
[GHMR18]	IBE	$O(1)$	$O(1)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$O(\log L)$	✓	✗	iO + SSB
[GHMR18]	IBE	$O(1)$	$O(1)$	$O(L)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$O(\log L)$	✓	✗	CDH/LWE
[GHM+19]	Anon. IBE	$O(1)$	$O(1)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$O(\log L)$	✓	✗	CDH/LWE
[GV20]	IBE	$O(1)$	$O(1)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$O(\log L)$	✓	✗	CDH/LWE
[CES21]	IBE	$O(1)$	$O(1)$	$\mathsf{poly}(\log L)$	$O(\sqrt{L})$	$\mathsf{poly}(\log L)$	$O(\log L)$	✓	✗	CDH/LWE
[GKMR22]	IBE $O(1)$-size ciphertexts	$O(\sqrt{L})$	$O(\sqrt{L})$	$O(\sqrt{L})$	$O(\sqrt{L})$	$O(\sqrt{L})$	$O(\sqrt{L})$	✗	✓	Pairings of Prime Order
[GKMR22]	IBE $O(\log L)$-size ciphertexts	$O(\sqrt{L})$	$O(\sqrt{L})$	$O(\sqrt{L}\log L)$	$O(\sqrt{L}\log L)$	$O(\log L)$	$O(\log L)$	✗	✓	Pairings of Prime Order
[DKL+23]	IBE	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$O(L)$	$\mathsf{poly}(\log L)$	$\mathsf{poly}(\log L)$	$O(\log L)$	✓	✓	LWE
[HLWW22]	ABE small attribute space $\mathcal{U}$ LSSS policies	$L^2 \cdot \mathsf{poly}(\lvert\mathcal{U}\rvert, \log L)$	$L \cdot \mathsf{poly}(\lvert\mathcal{U}\rvert, \log L)$	$L \cdot \mathsf{poly}(\lvert\mathcal{U}\rvert, \log L)$	$\lvert\mathcal{U}\rvert \cdot \mathsf{poly}(\log L)$	$\lvert\mathcal{U}\rvert \cdot \mathsf{poly}(\log L)$	$O(\log L)$	✗	✓	Pairings of Composite Order
[HLWW22]	ABE large attribute space $\mathcal{U}$ arbitrary policies	$O(1)$	$O(1)$	$O(L)$	$O(1)$	$O(1)$	$O(\log L)$	✓	✗	iO + SSB
Ours §6	Inner-Product PE large function space $\mathcal{F}$ n-size vectors	$n \cdot L^2 \cdot \mathsf{poly}(\log L)$	$L \cdot \mathsf{poly}(\log L)$	$n \cdot L^2 \cdot \mathsf{poly}(\log L)$	$n \cdot \mathsf{poly}(\log L)$	$n \cdot \mathsf{poly}(\log L)$	$O(\log L)$	✗	✓	Pairings of Prime Order + GGM
Ours §B	FE large function space $\mathcal{F}$ arbitrary functions	$O(1)$	$O(1)$	$O(L)$	$O(1)$	$O(1)$	$O(\log L)$	✓	✗	iO + SSB

Slotted RFE



Slightly modified compiler of [HLWW22] to make L independent with log updates

Slotted RIPE (Single slot)

CRS

- Prime order q:

  $\mathcal{G} = \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e$

- General params:

  $h = g_1^{\boldsymbol{\beta}} \qquad Z = e(g_1, g_2)^{\boldsymbol{\alpha}}$

- Slot-specific:

  $A = g_2^{\boldsymbol{t}} \qquad B = g_2^{\boldsymbol{\alpha}} A^{\boldsymbol{\beta}} = g^{\boldsymbol{\alpha}+\boldsymbol{\beta}\boldsymbol{t}}$

- Key-specific:

  $U_w = g_1^{\boldsymbol{u_w}}$ for each $w \in [n+1]$

Key registration

$pk = U_{n+1}^{-\boldsymbol{sk}} \quad \boldsymbol{x} = (x_1, \ldots, x_n)$

Key aggregation:

$$pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\boldsymbol{\alpha}}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{\boldsymbol{t}}$ $\quad B = g_2^{\boldsymbol{\alpha}} A^{\boldsymbol{\beta}} = g^{\boldsymbol{\alpha}+\boldsymbol{\beta}\boldsymbol{t}}$

$U_w = g_1^{\boldsymbol{u_w}}$ $\quad h = g_1^{\boldsymbol{\beta}}$

Enc $(m, \boldsymbol{y} = (y_1, \dots, y_n))$**:**

$$C_1 = m \cdot Z^{\boldsymbol{s}}$$

$$C_2 = g_1^{\boldsymbol{s}}$$

$$C_{3,w} = h^{y_w \cdot \boldsymbol{r}+\boldsymbol{s}} \cdot U_w^{-z}, \forall w \in [n]$$

$$C_{3,n+1} = h^{\boldsymbol{s}} \cdot U_{n+1}^{-z}$$

$$C_{3,n+2} = h^{\boldsymbol{s}} \cdot (pk \prod_{w=1}^{n} U_w^{-x_w})^{-z}$$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$$m = \frac{C_1}{e(C_2, B)} \cdot e(h^s, A)$$

$$h^s = \left(C_{3,n+2} \cdot C_{3,n+1}^{sk} \cdot \prod_{w=1}^{n} C_{3,w}^{x_w}\right)^{(1+sk+\sum x_w)^{-1}}$$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{t}$ $\quad B = g_2^{\alpha} A^{\beta} = g^{\alpha+\beta t}$

$U_w = g_1^{u_w}$ $\quad h = g_1^{\beta}$

Enc $(m, \boldsymbol{y} = (y_1, \ldots, y_n))$**:**

$C_1 = m \cdot Z^{s}$

$C_2 = g_1^{s}$

$C_{3,w} = h^{y_w \cdot \boldsymbol{r} + \boldsymbol{s}} \cdot U_w^{-\boldsymbol{z}}, \forall w \in [n]$

$C_{3,n+1} = h^{\boldsymbol{s}} \cdot U_{n+1}^{-\boldsymbol{z}}$

$C_{3,n+2} = h^{\boldsymbol{s}} \cdot (pk \prod_{w=1}^{n} U_w^{-x_w})^{-\boldsymbol{z}}$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$m = \frac{C_1}{e(C_2, B)} \cdot e(h^{s}, A)$

$\prod_{w=1}^{n} C_{3,w}^{x_w} = \prod_{w=1}^{n} h^{x_w (y_w \cdot r)}$ $\quad \prod_{w=1}^{n} h^{x_w s}$ $\quad \prod_{w=1}^{n} U_w^{-z \cdot x_w}$

$C_{3,n+1}^{sk} = h^{s \cdot sk}$ $\quad U_{n+1}^{-z \cdot sk}$

$C_{3,n+2} = h^{\boldsymbol{s}}$ $\quad U_{n+1}^{z \cdot sk}$ $\quad \prod_{w=1}^{n} U_w^{z \cdot x_w}$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{t}$ $\quad B = g_2^{\alpha} A^{\beta} = g^{\alpha+\beta t}$

$U_w = g_1^{u_w}$ $\quad h = g_1^{\beta}$

Enc $(m, \boldsymbol{y} = (y_1, \ldots, y_n))$**:**

$C_1 = m \cdot Z^{s}$

$C_2 = g_1^{s}$

$C_{3,w} = h^{y_w \cdot r + s} \cdot U_w^{-z}, \forall w \in [n]$

$C_{3,n+1} = h^{s} \cdot U_{n+1}^{-z}$

$C_{3,n+2} = h^{s} \cdot (pk \prod_{w=1}^{n} U_w^{-x_w})^{-z}$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$m = \frac{C_1}{e(C_2, B)} \cdot e(h^{s}, A)$

$\prod_{w=1}^{n} C_{3,w}^{x_w} = \prod_{w=1}^{n} h^{x_w (y_w \cdot r)}$ $\quad \prod_{w=1}^{n} h^{x_w s}$ $\quad \prod_{w=1}^{n} U_w^{-z \cdot x_w}$

$C_{3,n+1}^{sk} = h^{s \cdot sk}$ $\quad U_{n+1}^{-z \cdot sk}$

$C_{3,n+2} = h^{s}$ $\quad U_{n+1}^{z \cdot sk}$

$\prod_{w=1}^{n} U_w^{z \cdot x_w}$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{t}$ $\quad B = g_2^{\alpha} A^{\beta} = g^{\alpha+\beta t}$

$U_w = g_1^{u_w}$ $\quad h = g_1^{\beta}$

Enc $(m, \boldsymbol{y} = (y_1, \ldots, y_n))$**:**

$C_1 = m \cdot Z^{s}$

$C_2 = g_1^{s}$

$C_{3,w} = h^{y_w \cdot r + s} \cdot U_w^{-z}, \forall w \in [n]$

$C_{3,n+1} = h^{s} \cdot U_{n+1}^{-z}$

$C_{3,n+2} = h^{s} \cdot (pk \prod_{w=1}^{n} U_w^{-x_w})^{-z}$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$$m = \frac{C_1}{e(C_2, B)} \cdot e(h^{s}, A)$$

$\prod_{w=1}^{n} C_{3,w}^{x_w} = \prod_{w=1}^{n} h^{x_w (y_w \cdot r)}$ $\quad \prod_{w=1}^{n} h^{x_w s}$ $\quad \prod_{w=1}^{n} U_w^{-z \cdot x_w}$

$C_{3,n+1}^{sk} = h^{s \cdot sk}$ $\quad U_{n+1}^{-z \cdot sk}$

$C_{3,n+2} = h^{s}$ $\quad U_{n+1}^{-z \cdot sk}$

$\prod_{w=1}^{n} U_w^{z \cdot x_w}$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{t}$ $\quad B = g_2^{\alpha} A^{\beta} = g^{\alpha+\beta t}$

$U_w = g_1^{u_w}$ $\quad h = g_1^{\beta}$

Enc $(m, \boldsymbol{y} = (y_1, \ldots, y_n))$**:**

$$C_1 = m \cdot Z^{s}$$

$$C_2 = g_1^{s}$$

$$C_{3,w} = h^{y_w \cdot \boldsymbol{r} + \boldsymbol{s}} \cdot U_w^{-\boldsymbol{z}}, \forall w \in [n]$$

$$C_{3,n+1} = h^{\boldsymbol{s}} \cdot U_{n+1}^{-\boldsymbol{z}}$$

$$C_{3,n+2} = h^{\boldsymbol{s}} \cdot \left(pk \prod_{w=1}^{n} U_w^{-x_w}\right)^{-\boldsymbol{z}}$$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$$m = \frac{C_1}{e(C_2, B)} \cdot e(h^{s}, A)$$

$$\prod_{w=1}^{n} C_{3,w}^{x_w} = \prod_{w=1}^{n} h^{x_w (y_w \cdot r)} \cdot \prod_{w=1}^{n} h^{x_w s} \cdot \prod_{w=1}^{n} U_w^{-z \cdot x_w}$$

$$C_{3,n+1}^{sk} = h^{s \cdot sk} \cdot U_{n+1}^{-z \cdot sk}$$

$$C_{3,n+2} = h^{s} \cdot U_{n+1}^{z \cdot sk}$$

$$\prod_{w=1}^{n} U_w^{z \cdot x_w}$$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{t}$ $\quad B = g_2^{\alpha} A^{\beta} = g^{\alpha+\beta t}$

$U_w = g_1^{u_w}$ $\quad h = g_1^{\beta}$

Enc $(m, \boldsymbol{y} = (y_1, \ldots, y_n))$**:**

$$C_1 = m \cdot Z^{s}$$

$$C_2 = g_1^{s}$$

$$C_{3,w} = h^{y_w \cdot r + s} \cdot U_w^{-z}, \forall w \in [n]$$

$$C_{3,n+1} = h^{s} \cdot U_{n+1}^{-z}$$

$$C_{3,n+2} = h^{s} \cdot (pk \prod_{w=1}^{n} U_w^{-x_w})^{-z}$$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$$m = \frac{C_1}{e(C_2, B)} \cdot e(h^{s}, A)$$

$$\prod_{w=1}^{n} C_{3,w}^{x_w} = \prod_{w=1}^{n} h^{x_w (y_w \cdot r)} \cdot \prod_{w=1}^{n} h^{x_w s} \cdot \prod_{w=1}^{n} U_w^{-z \cdot x_w}$$

$$C_{3,n+1}^{sk} = h^{s \cdot sk} \cdot U_{n+1}^{-z \cdot sk}$$

$$C_{3,n+2} = h^{s} \cdot U_{n+1}^{z \cdot sk}$$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$ $\quad pk \cdot \prod_{w=1}^{n} U_w^{-x_w}$ $\quad A = g_2^{t}$ $\quad B = g_2^{\alpha} A^{\beta} = g^{\alpha+\beta t}$

$U_w = g_1^{u_w}$ $\quad h = g_1^{\beta}$

Enc $(m, \boldsymbol{y} = (y_1, \ldots, y_n))$**:**

$C_1 = m \cdot Z^{s}$

$C_2 = g_1^{s}$

$C_{3,w} = h^{y_w \cdot \boldsymbol{r}+\boldsymbol{s}} \cdot U_w^{-\boldsymbol{z}}, \forall w \in [n]$

$C_{3,n+1} = h^{\boldsymbol{s}} \cdot U_{n+1}^{-\boldsymbol{z}}$

$C_{3,n+2} = h^{\boldsymbol{s}} \cdot (pk \prod_{w=1}^{n} U_w^{-x_w})^{-\boldsymbol{z}}$

Dec $(C_1, C_2, C_{3,w}, C_{3,n+1}, sk, \boldsymbol{x})$**:**

$m = \frac{C_1}{e(C_2, B)} \cdot e(h^{\boldsymbol{s}}, A)$

$\prod_{w=1}^{n} C_{3,w}^{x_w} = \prod_{w=1}^{n} h^{x_w (y_w \cdot r)}$ $\quad \prod_{w=1}^{n} \boxed{h^{\boldsymbol{x_w s}}} \prod_{w=1}^{n} U_w^{-z \cdot x_w}$

$C_{3,n+1}^{sk} = \boxed{h^{\boldsymbol{s \cdot sk}}}$ $\quad U_{n+1}^{-z \cdot sk}$

$C_{3,n+2} = h^{\boldsymbol{s}}$ $\quad U_{n+1}^{z \cdot sk}$ $\quad \prod_{w=1}^{n} U_w^{z \cdot x_w}$

Slotted RIPE (2 slots) IDEA:

CRS Generation:

A_1, B_1 $\quad$ A_2, B_2

$\{U_{w,1}\}$ $\quad$ $\{U_{w,2}\}$

$\{U_{w,1} \cdot U_{w,2}\}$

Key Generation:

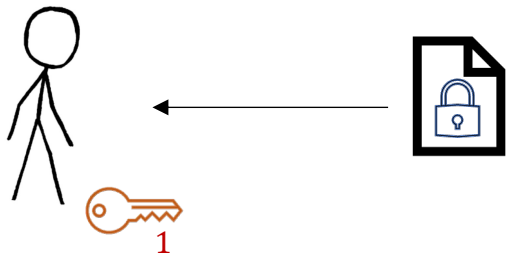
$pk_1 = U_{n+1}^{-sk_1}$ $\quad$ $\boldsymbol{x_1} = (x_{1,1}, \ldots, x_{n,1})$

$pk_2 = U_{n+1}^{-sk_2}$ $\quad$ $\boldsymbol{x_2} = (x_{1,2}, \ldots, x_{n,2})$

Key Aggregation:

$$pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$$

Slotted RIPE (2 slots)



$$\prod_{w\in[n]} C_{3,w}^{x_{w,1}} = \prod_{w\in[n]} h^{(y_w\cdot r+s)\cdot x_{w,1}} \cdot \prod_{w=1}^{n} U_{w,1}^{-z\cdot x_{w,1}} \cdot \boxed{\prod_{w=1}^{n} U_{w,2}^{-z\cdot x_{w,1}}}$$

$$C_{3,n+1}^{\mathsf{sk}_1} = h^{s\cdot \mathsf{sk}_1} \cdot U_{n+1,1}^{-z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{-z\cdot \mathsf{sk}_1}}$$

$$C_{3,n+2} = h^{s} \cdot U_{n+1,1}^{z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{z\cdot \mathsf{sk}_2}} \cdot \prod_{w=1}^{n} U_{w,1}^{z\cdot x_{w,1}} \boxed{\prod_{w=1}^{n} U_{w,2}^{z\cdot x_{w,2}}}$$

Slotted RIPE (2 slots)

CRS Generation:

A_1, B_1 A_2, B_2

$\{W_{1,2,w} = A_1^{u_{2,w}}\}$ $\{W_{2,1,w} = A_2^{u_{1,w}}\}$

$\{U_{w,1} = g^{u_{1,w}}\}$ $\{U_{w,2} = g^{u_{2,w}}\}$

$\{U_{w,1} \cdot U_{w,2}\}$

Key Generation:

$pk_1 = U_{n+1}^{-sk_1}$ $\boldsymbol{x_1} = (x_{1,1}, \ldots, x_{n,1})$ $\{W_{2,1,w}^{sk_1}\}$

$pk_2 = U_{n+1}^{-sk_2}$ $\boldsymbol{x_2} = (x_{1,2}, \ldots, x_{n,2})$ $\{W_{1,2,w}^{sk_2}\}$

Key Aggregation:

$pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$

$W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}$

Slotted RIPE (2 slots)

A_1, B_1

$\{U_{w,1} \cdot U_{w,2}\}$ $\quad h \quad Z$ $\quad pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$ $\quad _1$

$W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}$

$$\prod_{w\in[n]} C_{3,w}^{x_{w,1}} = \prod_{w\in[n]} h^{(y_w\cdot r+s)\cdot x_{w,1}} \cdot \prod_{w=1}^{n} U_{w,1}^{-z\cdot x_{w,1}} \cdot \boxed{\prod_{w=1}^{n} U_{w,2}^{-z\cdot x_{w,1}}}$$

$$C_{3,n+1}^{\mathsf{sk}_1} = h^{s\cdot \mathsf{sk}_1} \cdot U_{n+1,1}^{-z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{-z\cdot \mathsf{sk}_1}}$$

$$C_{3,n+2} = h^{s} \cdot U_{n+1,1}^{z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{z\cdot \mathsf{sk}_2}} \cdot \prod_{w=1}^{n} U_{w,1}^{z\cdot x_{w,1}} \boxed{\prod_{w=1}^{n} U_{w,2}^{z\cdot x_{w,2}}}$$

$C_4 = g_1^z$

Slotted RIPE (2 slots)

$\{W_{1,2,w} = A_1^{u_{2,w}/\gamma}\}$ $\{W_{2,1,w} = A_2^{u_{1,w}/\gamma}\}$

A_1, B_1

$\{U_{w,1} \cdot U_{w,2}\}$

$\Gamma = g_1^{\gamma}$

h

Z

$pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$

$_1$

$W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}$

$$\prod_{w\in[n]} C_{3,w}^{x_{w,1}} = \prod_{w\in[n]} h^{(y_w\cdot r+s)\cdot x_{w,1}} \cdot \prod_{w=1}^{n} U_{w,1}^{-z\cdot x_{w,1}} \cdot \boxed{\prod_{w=1}^{n} U_{w,2}^{-z\cdot x_{w,1}}}$$

$$C_{3,n+1}^{\mathsf{sk}_1} = h^{s\cdot \mathsf{sk}_1} \cdot U_{n+1,1}^{-z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{-z\cdot \mathsf{sk}_1}}$$

$$C_{3,n+2} = h^{s} \cdot U_{n+1,1}^{z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{z\cdot \mathsf{sk}_2}} \cdot \prod_{w=1}^{n} U_{w,1}^{z\cdot x_{w,1}} \boxed{\prod_{w=1}^{n} U_{w,2}^{z\cdot x_{w,2}}}$$

$C_4 = \Gamma^z$

Slotted RIPE (2 slots)

$\{W_{1,2,w} = A_1^{u_{2,w}/\gamma}\}$ $\{W_{2,1,w} = A_2^{u_{1,w}/\gamma}\}$

A_1, B_1

$\{U_{w,1} \cdot U_{w,2}\}$

$\Gamma = g_1^{\gamma}$

h

Z

$pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$

$_1$

$W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}$

$$\prod_{w\in[n]} C_{3,w}^{x_{w,1}} = \prod_{w\in[n]} h^{(y_w\cdot r+s)\cdot x_{w,1}} \cdot \prod_{w=1}^{n} U_{w,1}^{-z\cdot x_{w,1}} \cdot \prod_{w=1}^{n} U_{w,2}^{-z\cdot x_{w,1}}$$

$$C_{3,n+1}^{\mathsf{sk}_1} = h^{s\cdot \mathsf{sk}_1} \cdot U_{n+1,1}^{-z\cdot \mathsf{sk}_1} \cdot U_{n+1,2}^{-z\cdot \mathsf{sk}_1}$$

$$C_{3,n+2} = h^{s} \cdot U_{n+1,1}^{z\cdot \mathsf{sk}_1} \cdot U_{n+1,2}^{z\cdot \mathsf{sk}_2} \cdot \prod_{w=1}^{n} U_{w,1}^{z\cdot x_{w,1}} \prod_{w=1}^{n} U_{w,2}^{z\cdot x_{w,2}}$$

$C_4 = \Gamma^z$

Conclusions

- Registered RFE Definition
- Registered IPE from parings in the GGM
- Registered RFE for P/poly and unbounded users from iO and SSB hash functions
- Open problems
  - RFE from any compact and polynomially-hard FE
  - RFE for specialized function classes from weaker assumptions
  - Prove our pairing-based RIPE in the standard model

Thank you for your attention!

https://ia.cr/2023/395