Finanziato dall'Unione europea NextGenerationEU

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

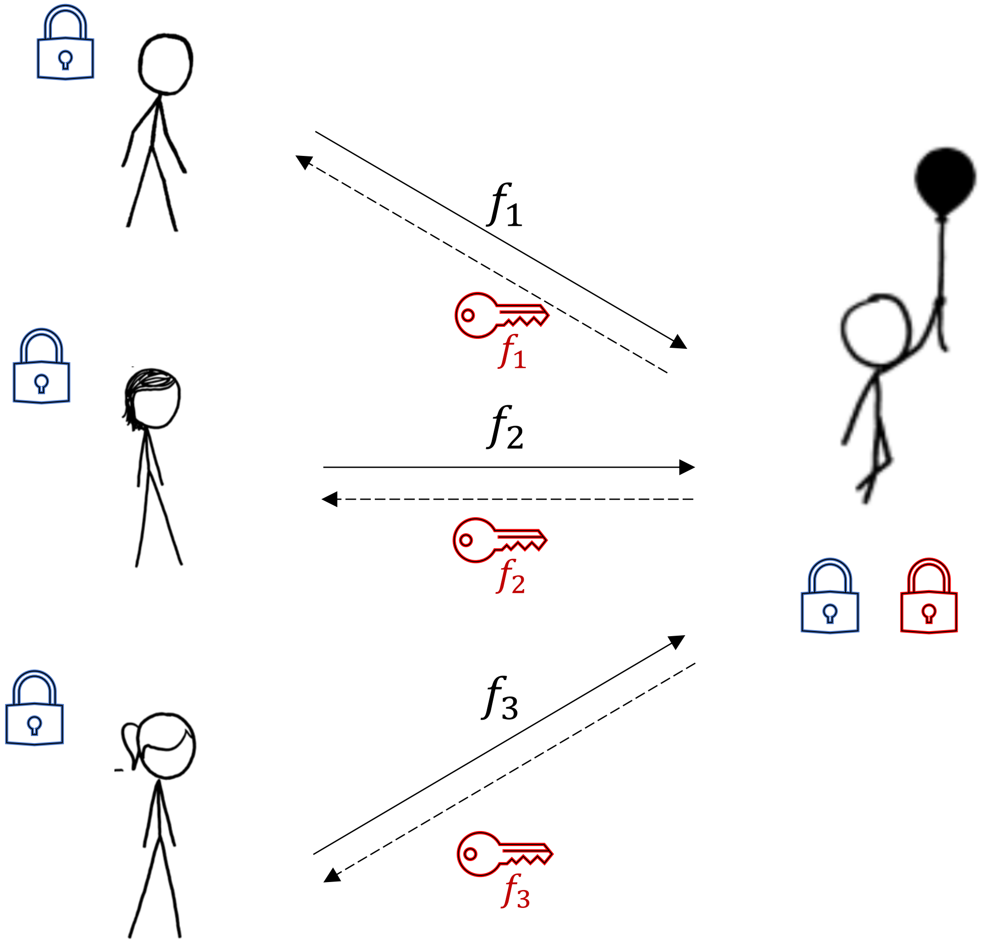
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

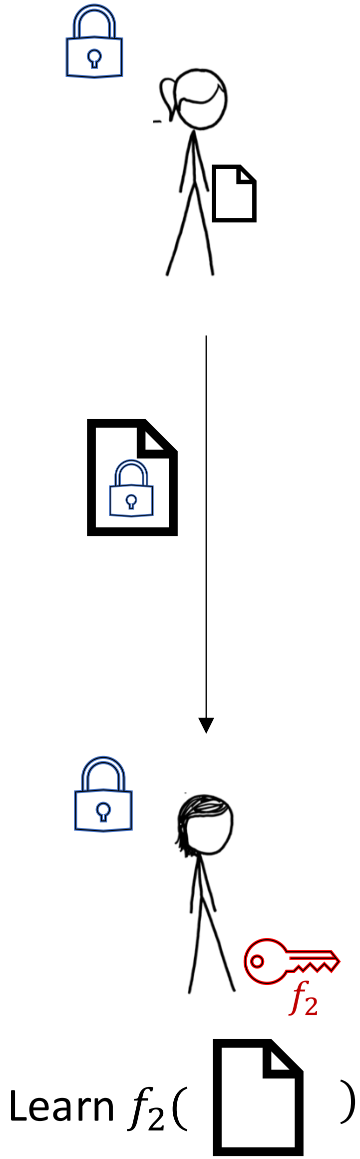
Registered (Inner-Product) Functional Encryption

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

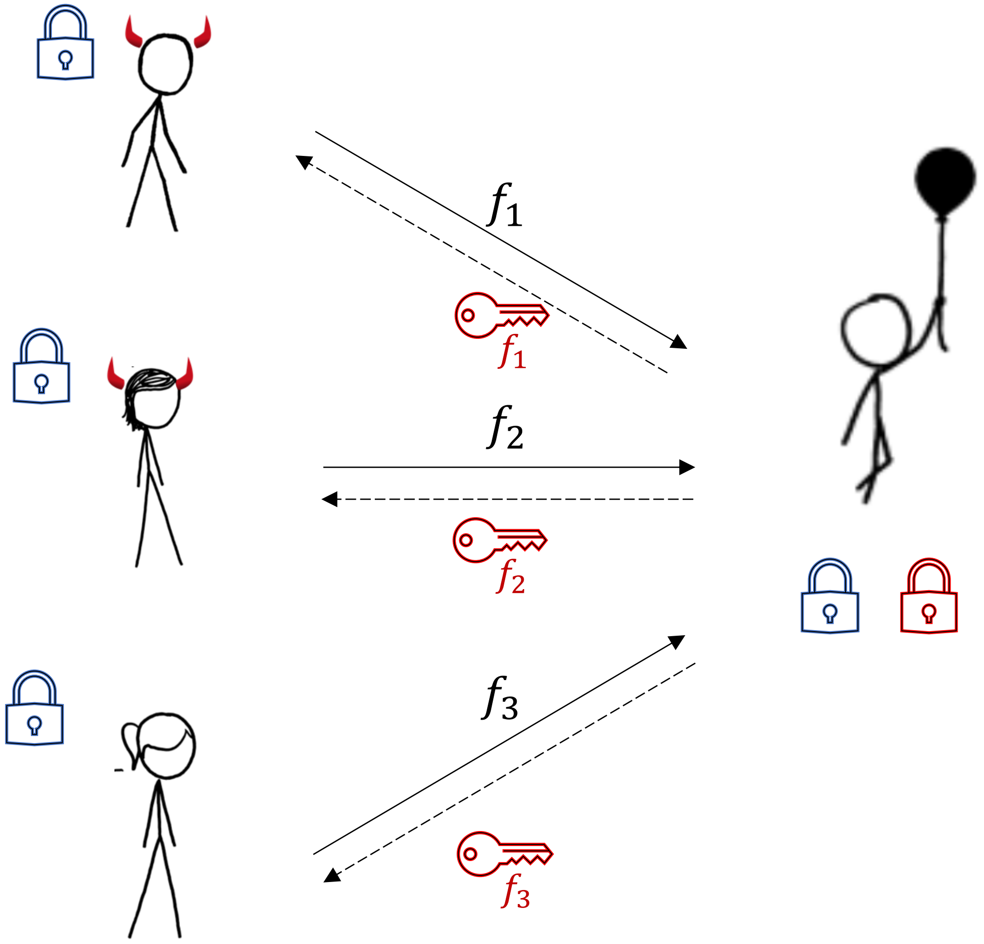
[1]Royal Holloway University of London, England
[2]Sapienza University of Rome
[3]IIT Kharagpur, India
[4]Bocconi University, Italy
[5]Max-Planck Institute for Security and Privacy, Germany

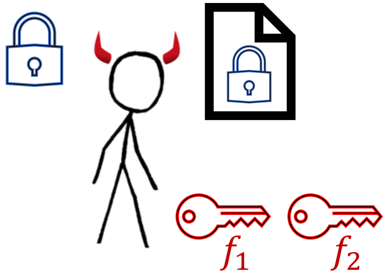
Functional Encryption

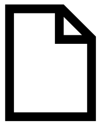




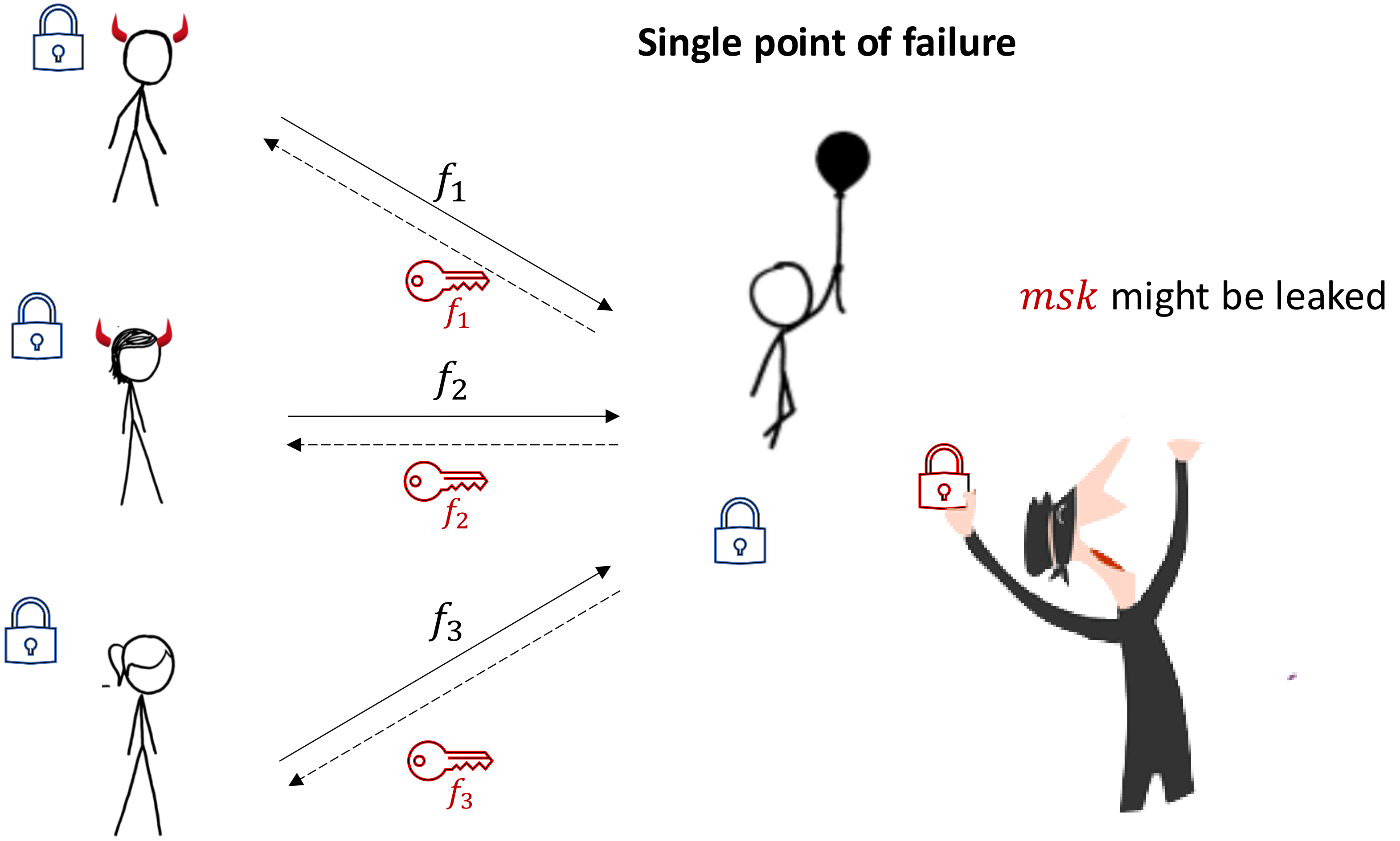
Functional Encryption



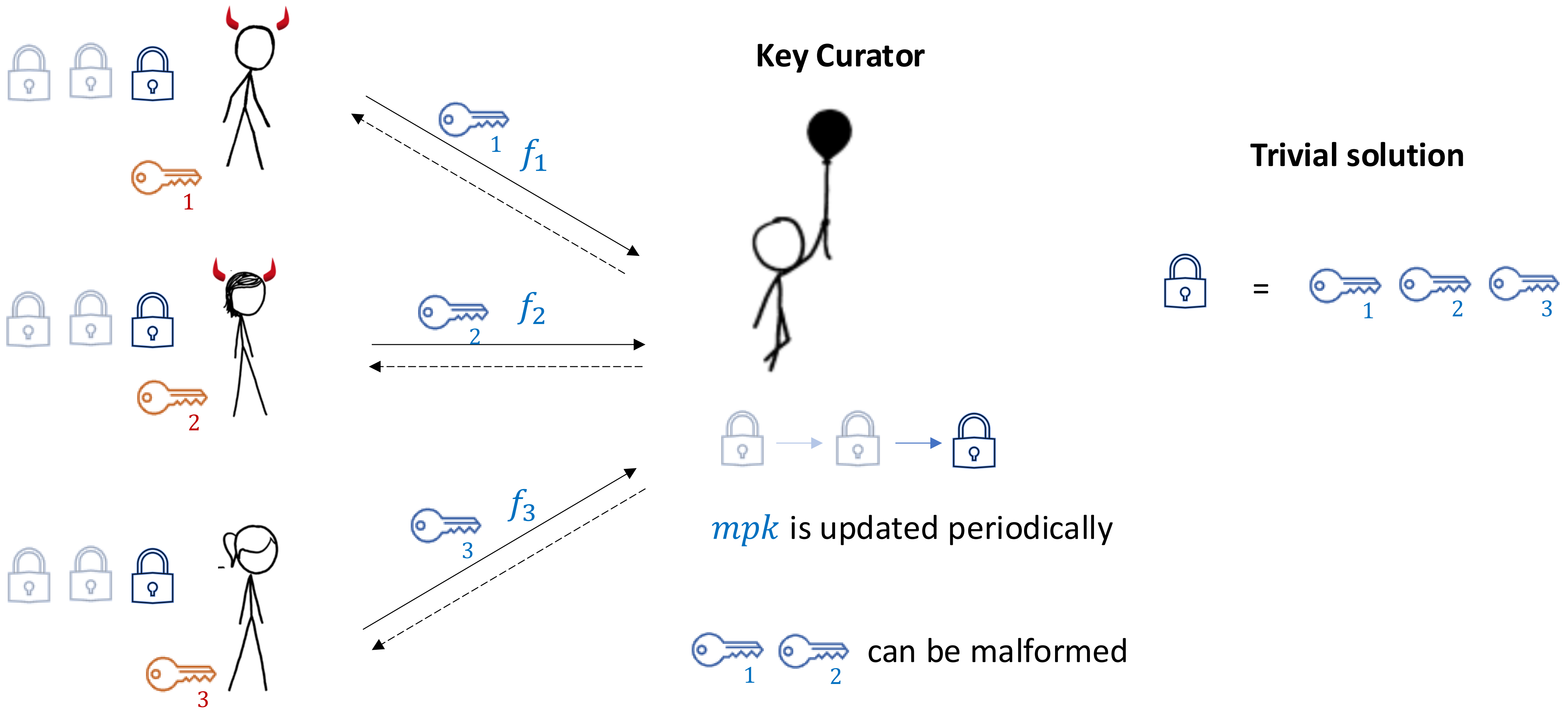


Cannot learn $f_{\neq 1,2}($  $)$

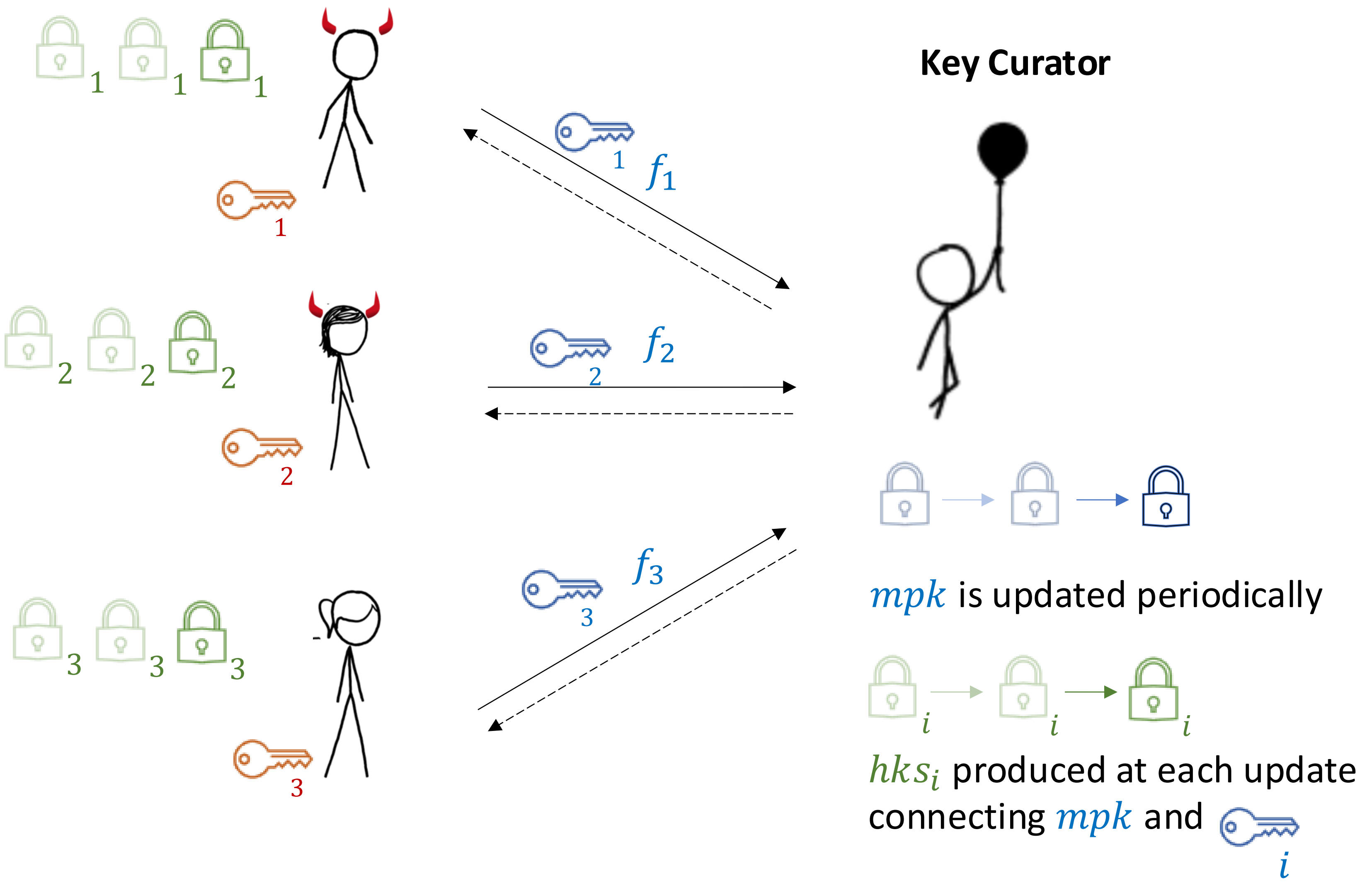
Key-Escrow Problem



Registered Functional Encryption



Registered Functional Encryption



Requirements:

L = #Users

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

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

#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

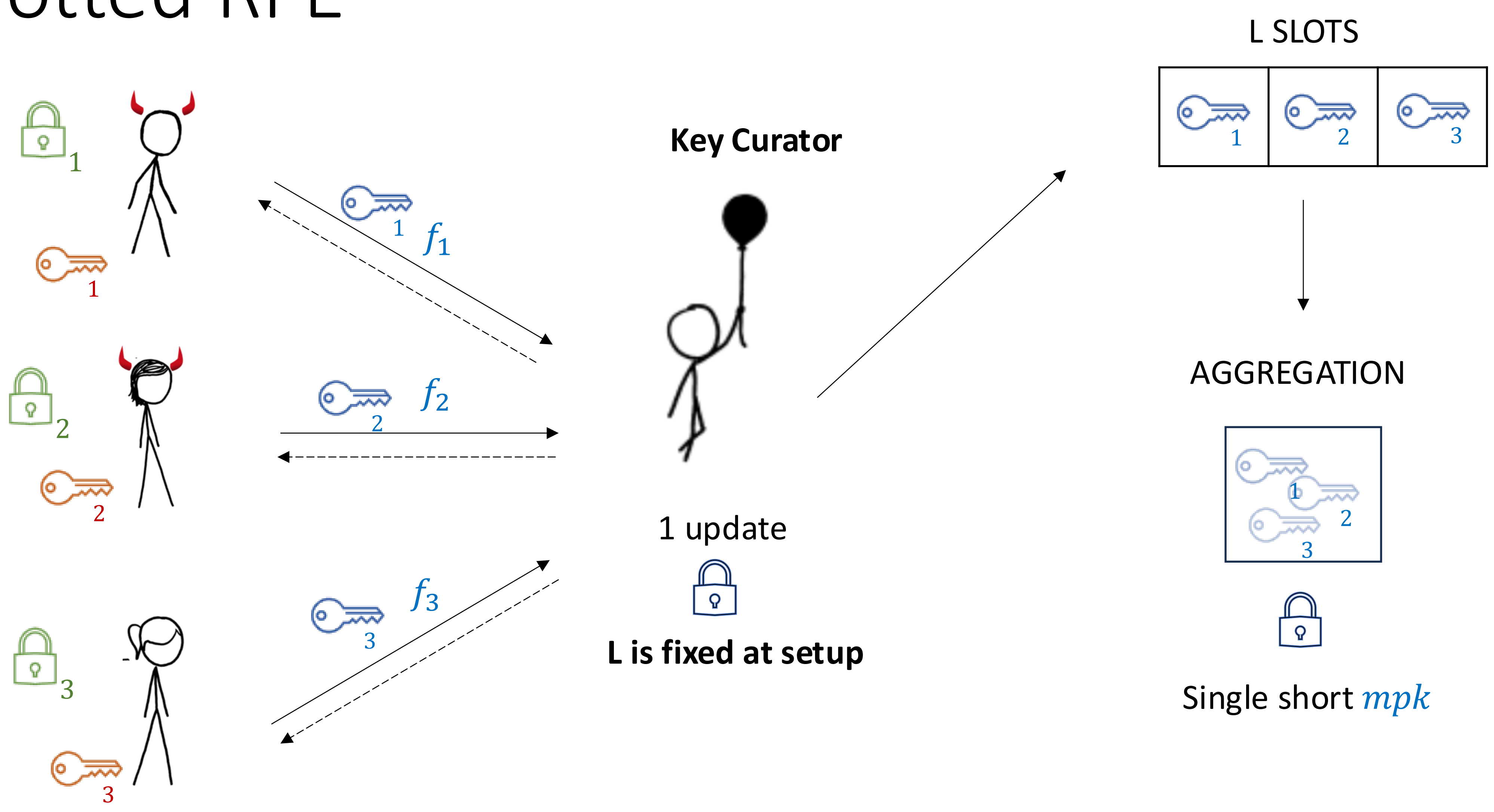
Both CONs:

- 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)

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

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

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

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

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

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

$$\boxed{\begin{aligned} C_{3,w} &= h^{y_w \cdot \boldsymbol{r}+\boldsymbol{s}} \cdot U_w^{-z}, \forall w \in [n] \\ C_{3,n+1} &= h^{\boldsymbol{s}} \cdot U_{n+1}^{-z} \\ C_{3,n+2} &= h^{\boldsymbol{s}} \cdot \left(pk \prod_{w=1}^{n} U_w^{-x_w}\right)^{-z} \end{aligned}}$$

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

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

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

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^\alpha$

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

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

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

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

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

$$C_2 = g_1^s$$

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

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

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

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

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

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

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

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

Slotted RIPE (Single slot)

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

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

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

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

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

$$C_2 = g_1^s$$

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

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

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

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

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

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

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

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

Slotted RIPE (Single slot)

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^\alpha$

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

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

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

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

$C_1 = m \cdot Z^s$

$C_2 = g_1^s$

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

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

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

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

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

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

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

$C_{3,n+2} = h^s$

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$

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

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

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

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

$C_1 = m \cdot Z^s$

$C_2 = g_1^s$

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

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

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

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

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

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

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

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

Slotted RIPE (Single slot)

$\mathcal{G}$ $\quad Z = e(g_1, g_2)^{\alpha}$

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

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

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

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

$C_1 = m \cdot Z^s$

$C_2 = g_1^s$

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

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

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

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

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

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

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

$$C_{3,n+2} = h^s$$

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

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

$$C_2 = g_1^s$$

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

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

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

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

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

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

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

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

Slotted RIPE (2 slots) IDEA:

CRS Generation:

A_1, B_1 $\qquad$ A_2, B_2

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

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

Key Generation:

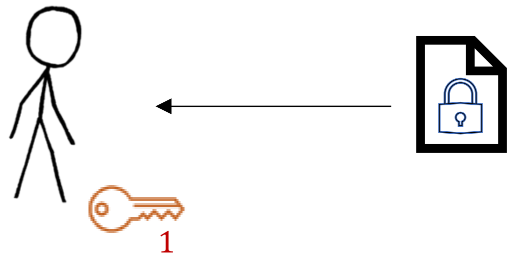
$pk_1 = U_{n+1}^{-sk_1}$ $\qquad$ $\boldsymbol{x_1} = (x_{1,1}, \dots, x_{n,1})$

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

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 $\qquad$ A_2, B_2

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

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

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

Key Generation:

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

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

Key Aggregation:

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

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

Slotted RIPE (2 slots)

$\{U_{w,1} \cdot U_{w,2}\}$ $\quad h, Z \quad$ $pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$ $\quad {}_1 \quad$ A_1, B_1 $\quad \boxed{W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}}$

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

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

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

$$\boxed{C_4 = g_1^z}$$

Slotted RIPE (2 slots)

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

h

$\{U_{w,1} \cdot U_{w,2}\}$ $\quad pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$ $\quad {}_1$ $\quad A_1, B_1$

$\boxed{\Gamma = g_1^{\gamma}}$ $\quad Z$ $\quad \boxed{W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}}$

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

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

$$C_{3,n+2} = h^{s} \cdot U_{n+1,1}^{z\cdot \mathsf{sk}_1} \cdot \boxed{U_{n+1,2}^{z\cdot \mathsf{sk}_2}} \cdot \prod_{w=1}^{n} U_{w,1}^{z\cdot x_{w,1}} \boxed{\prod_{w=1}^{n} U_{w,2}^{z\cdot x_{w,2}}} \qquad \boxed{C_4 = \Gamma^{z}}$$

Slotted RIPE (2 slots)

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

h

$\{U_{w,1} \cdot U_{w,2}\}$ $\quad pk_1 \cdot pk_2 \cdot \prod U_{w,1}^{x_{w,1}} \prod U_{w,2}^{x_{w,2}}$ $\quad {}_1$ $\quad A_1, B_1$

$\boxed{\Gamma = g_1^{\gamma}}$ $\quad Z$ $\quad \boxed{W_{2,1,n+1}^{sk_1} \cdot W_{1,2,n+1}^{sk_2}}$

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

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

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

$$\boxed{C_4 = \Gamma^{z}}$$

Conclusions

- RFE Definition
- Registered IPE from parings in the GGM
- 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

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Thank you for your attention!

https://ia.cr/2023/395