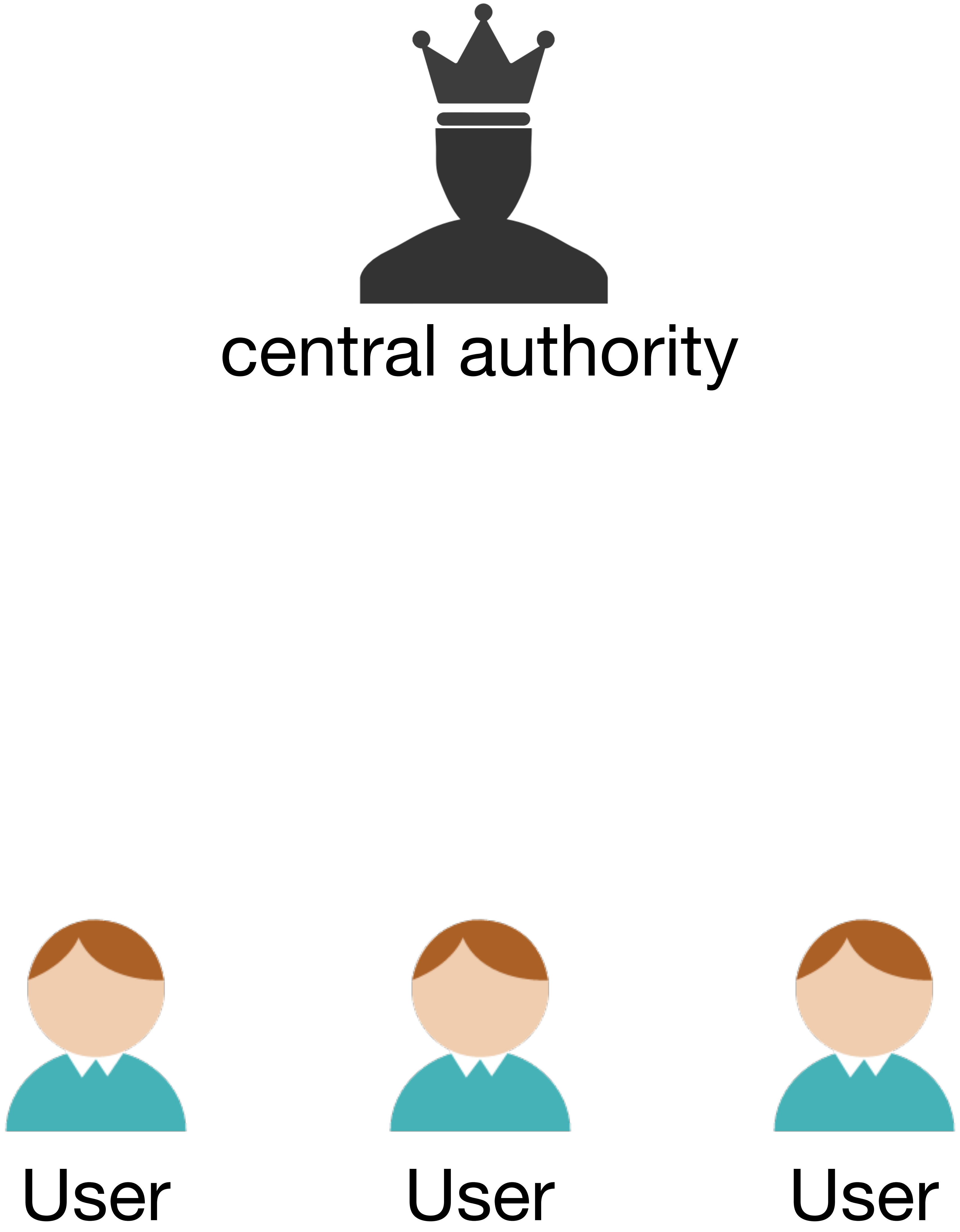
Registered Functional Encryptions from Pairings

Ziqi Zhu Jiangtao Li Kai Zhang Junqing Gong Haifeng Qian

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

Functional Encryption



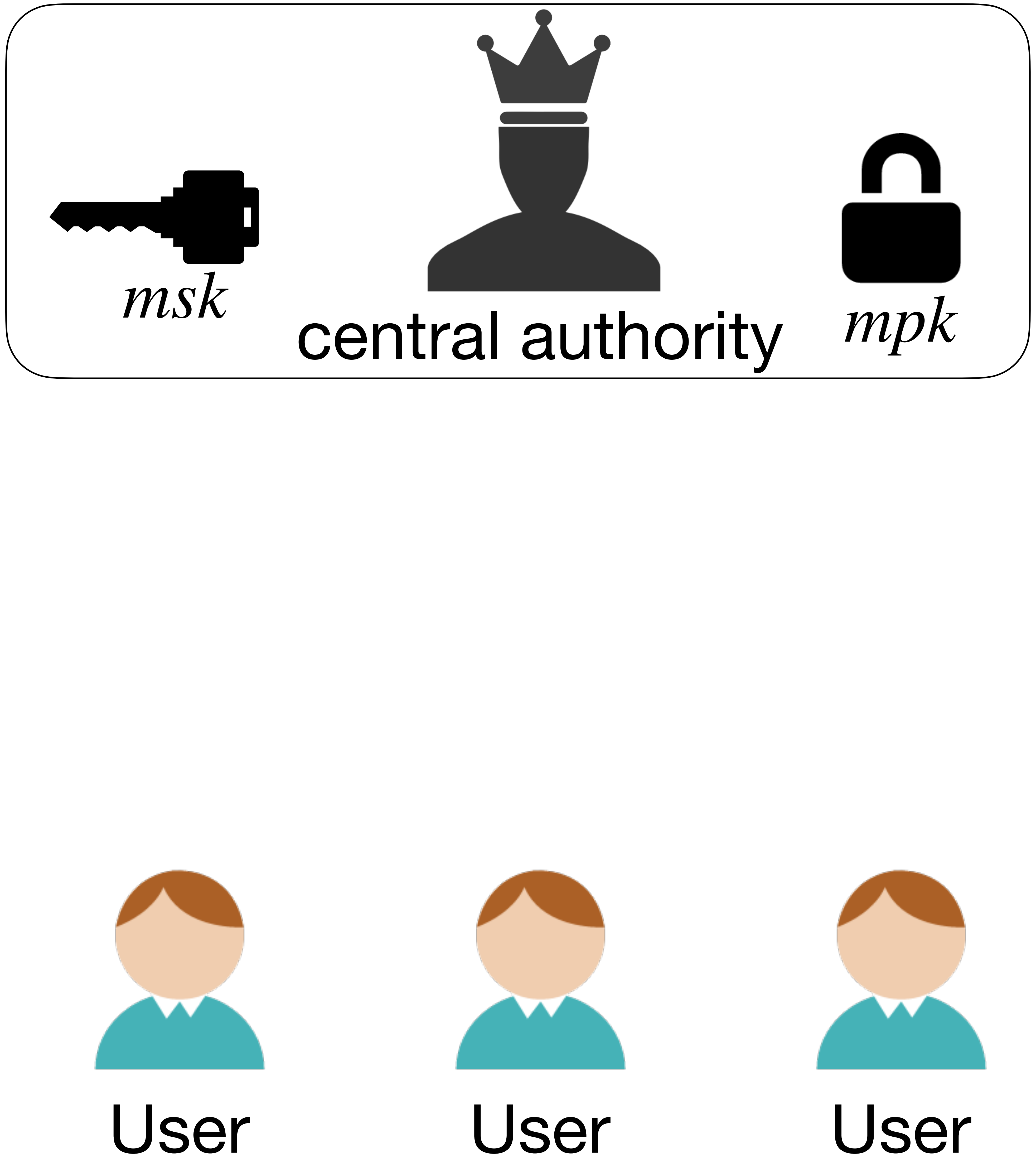
central authority

User

User

User

Functional Encryption



msk

central authority

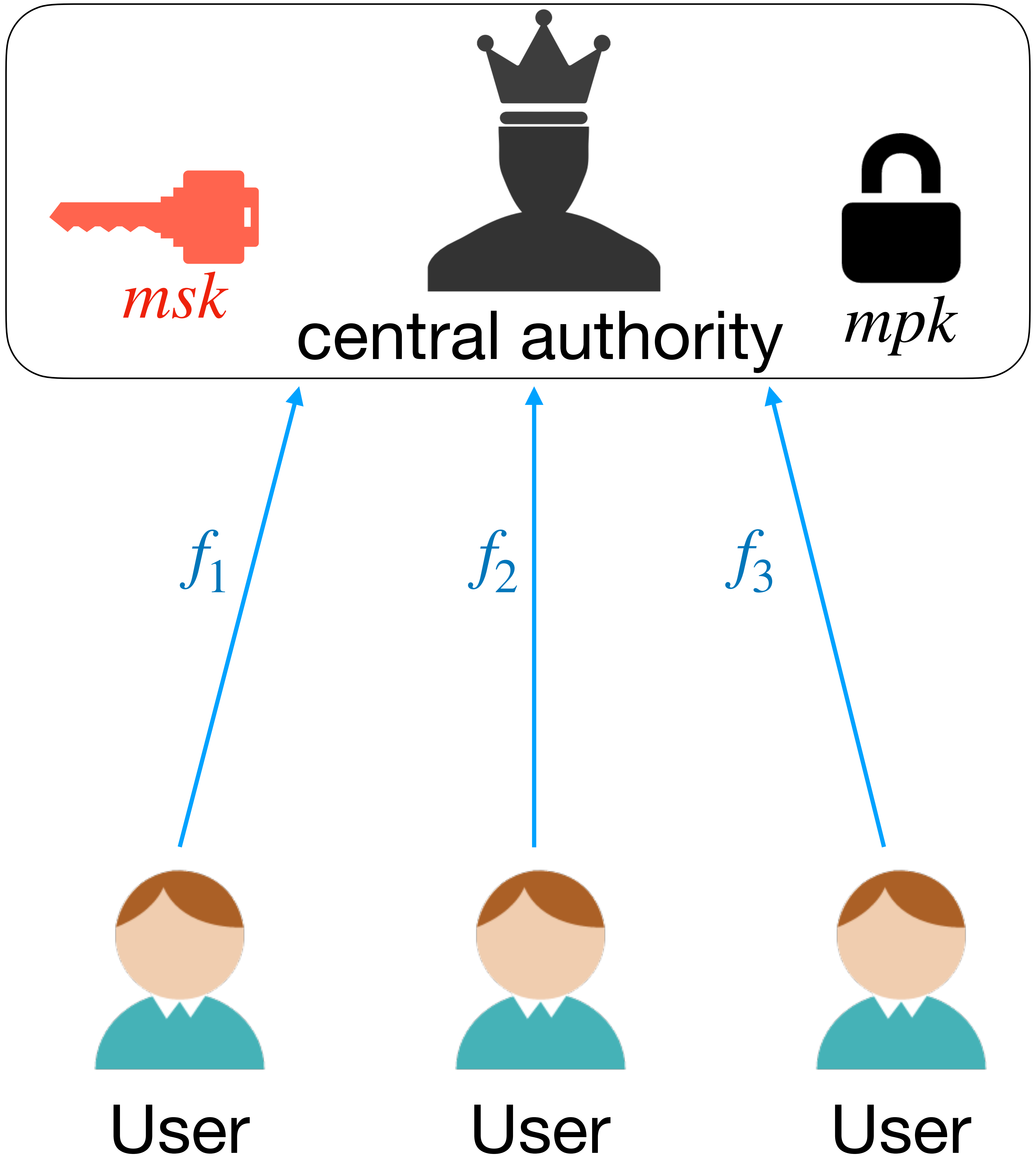
mpk

User

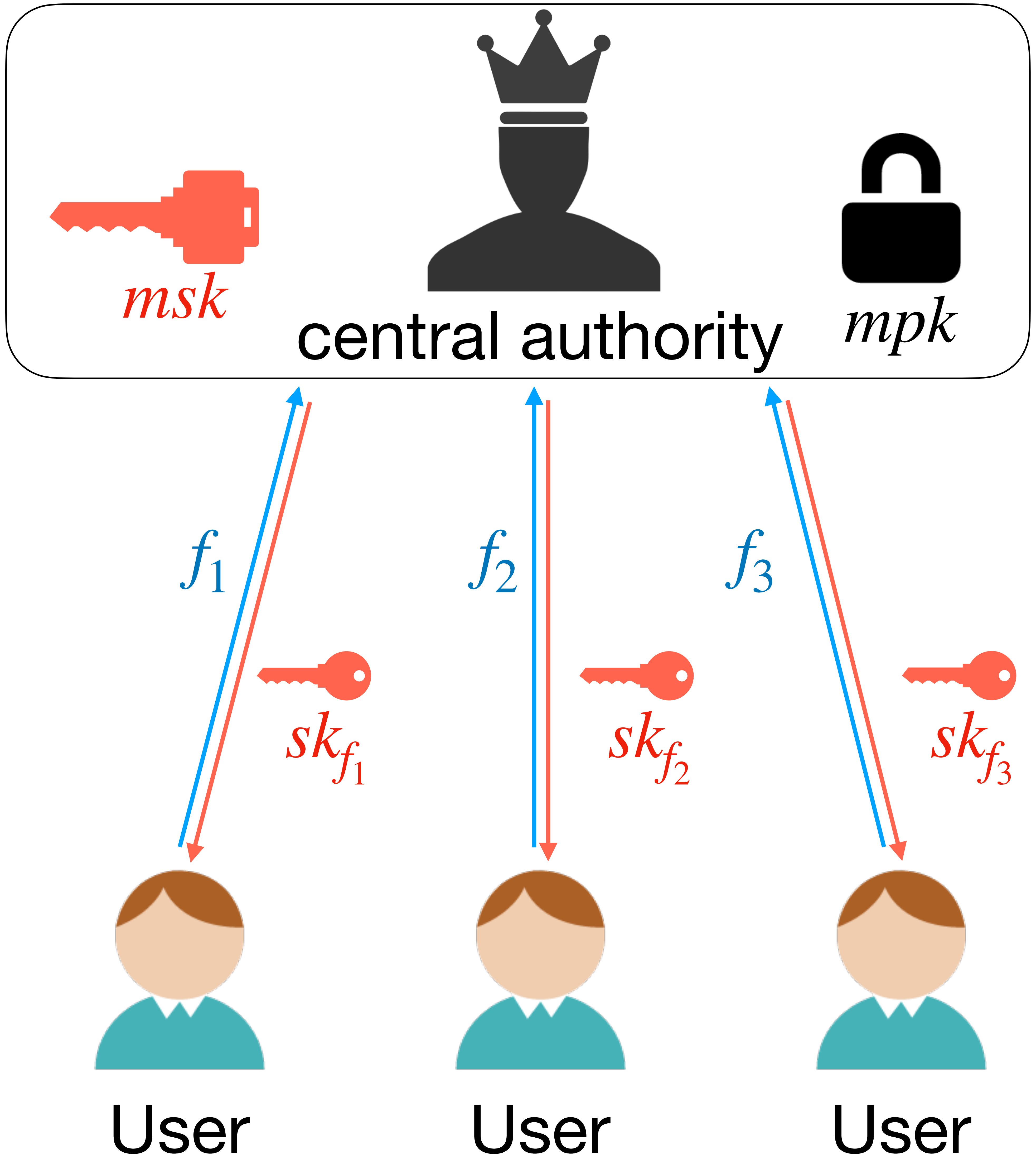
User

User

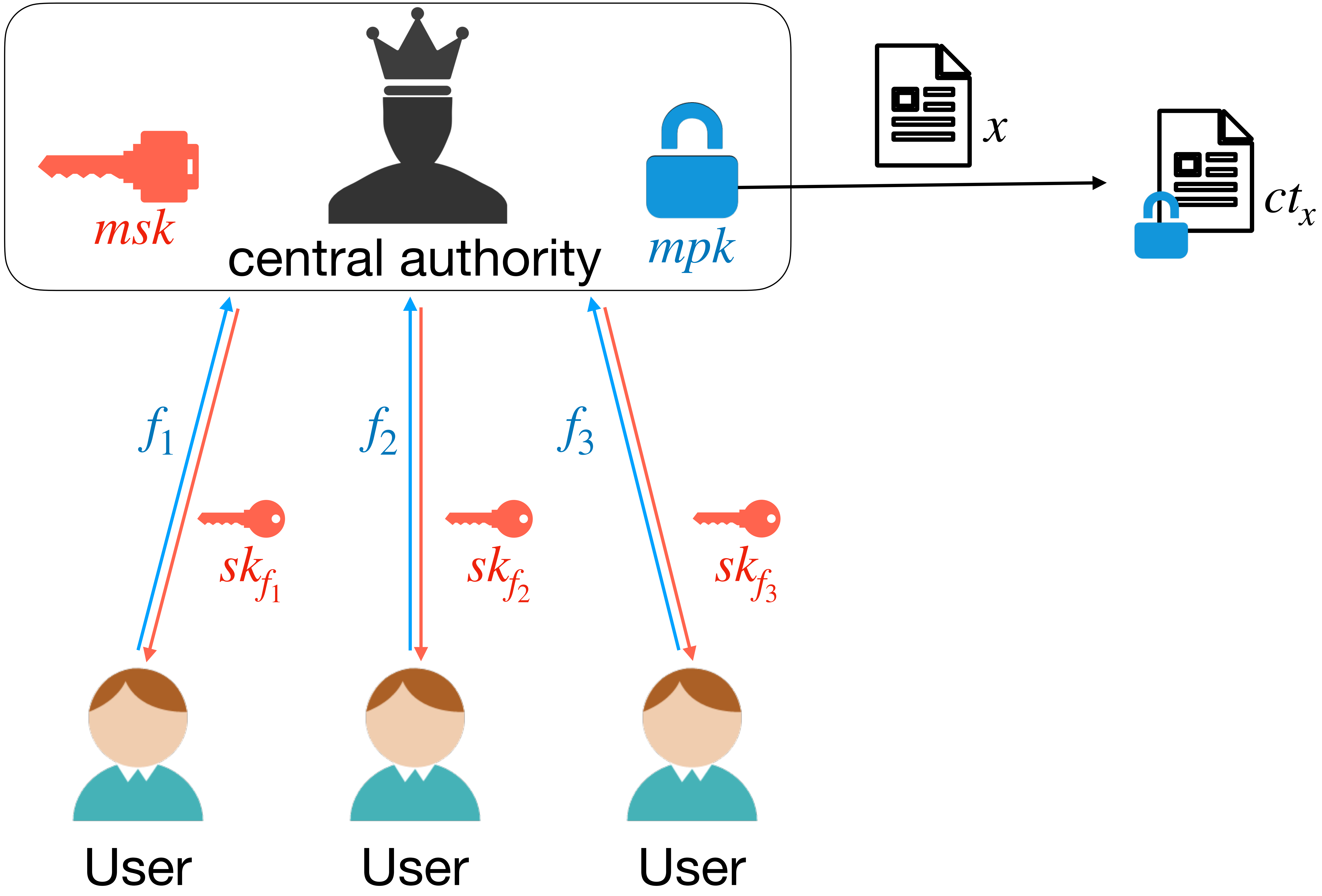
Functional Encryption



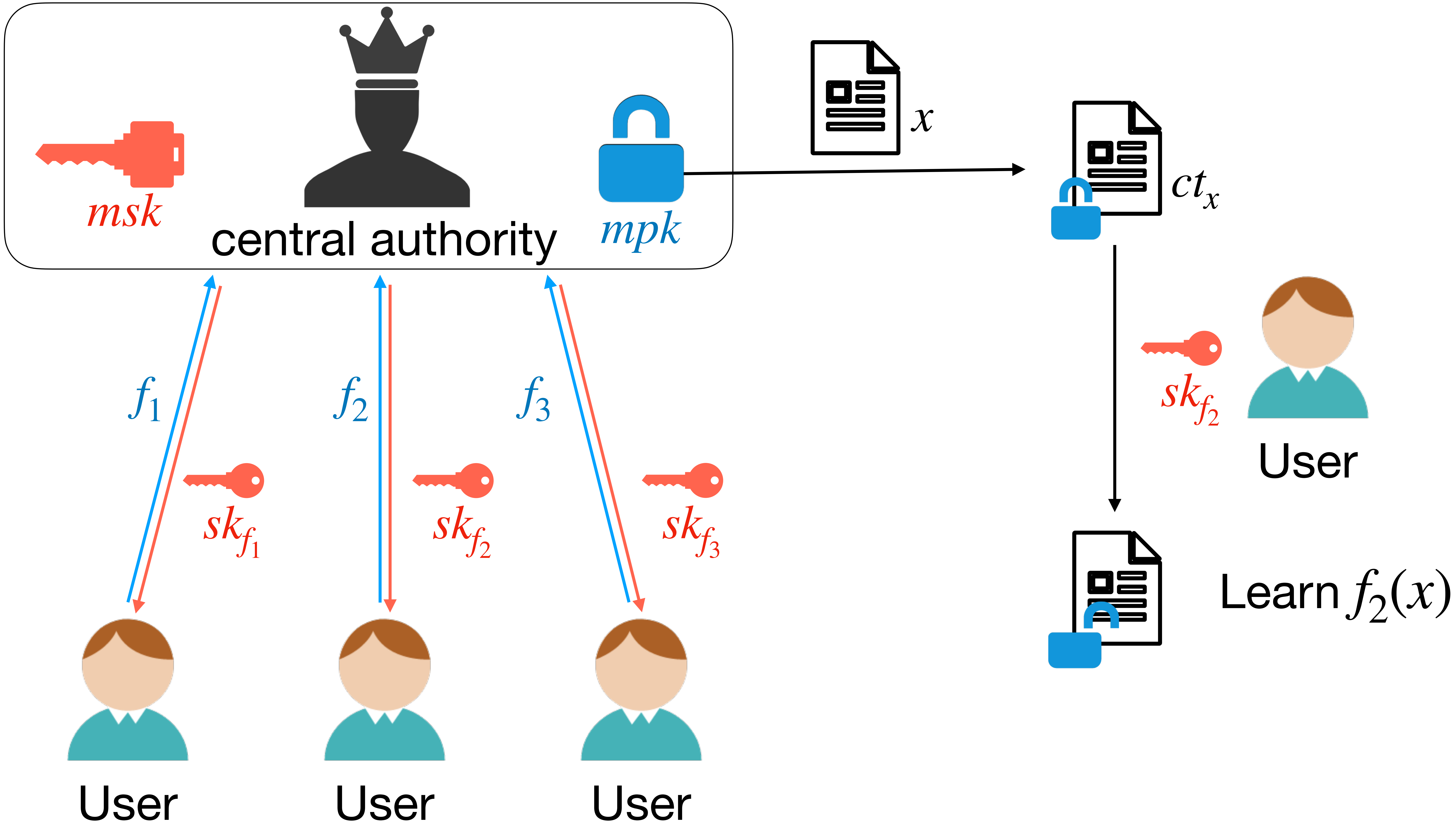
Functional Encryption



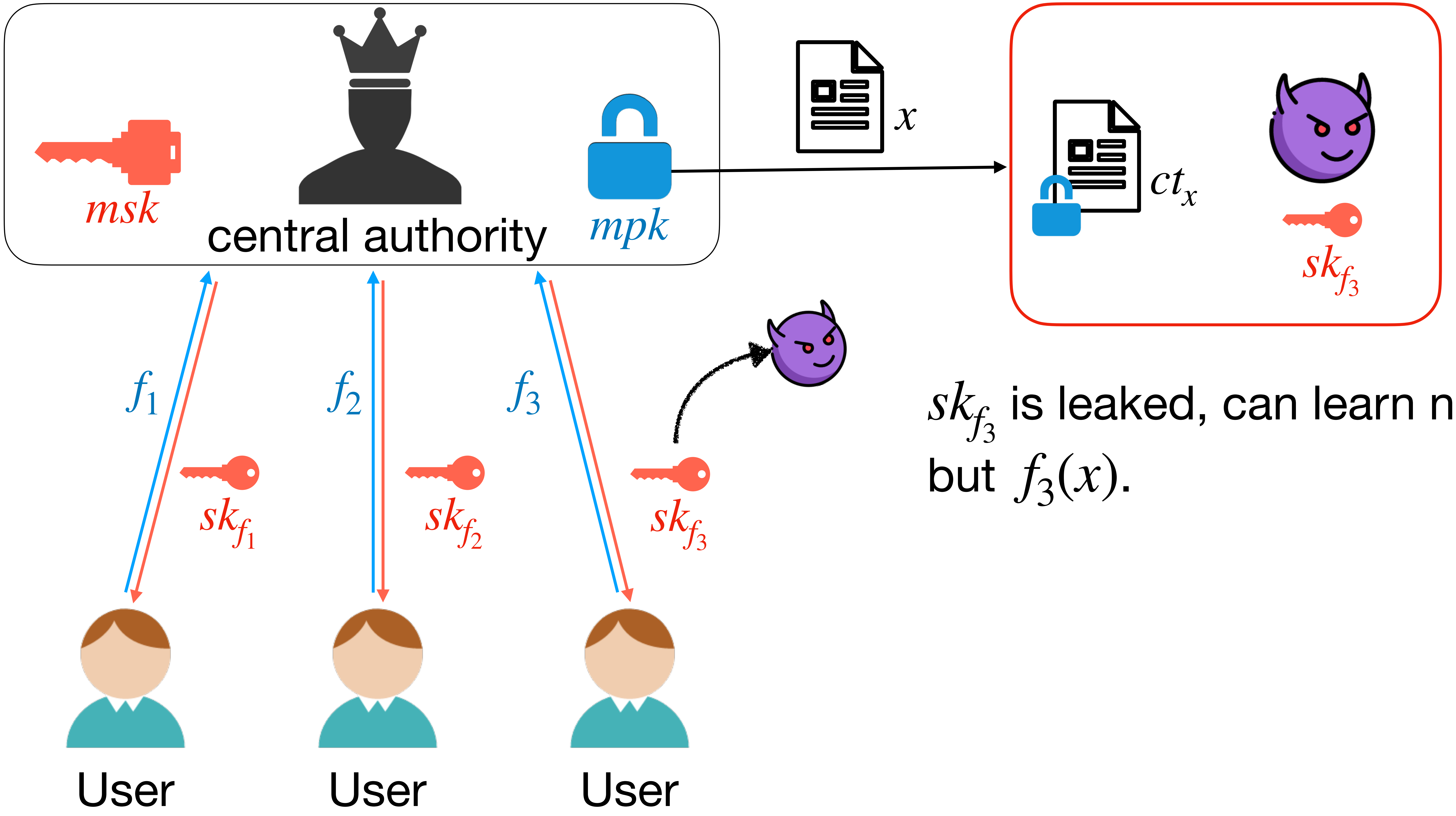
Functional Encryption



Functional Encryption

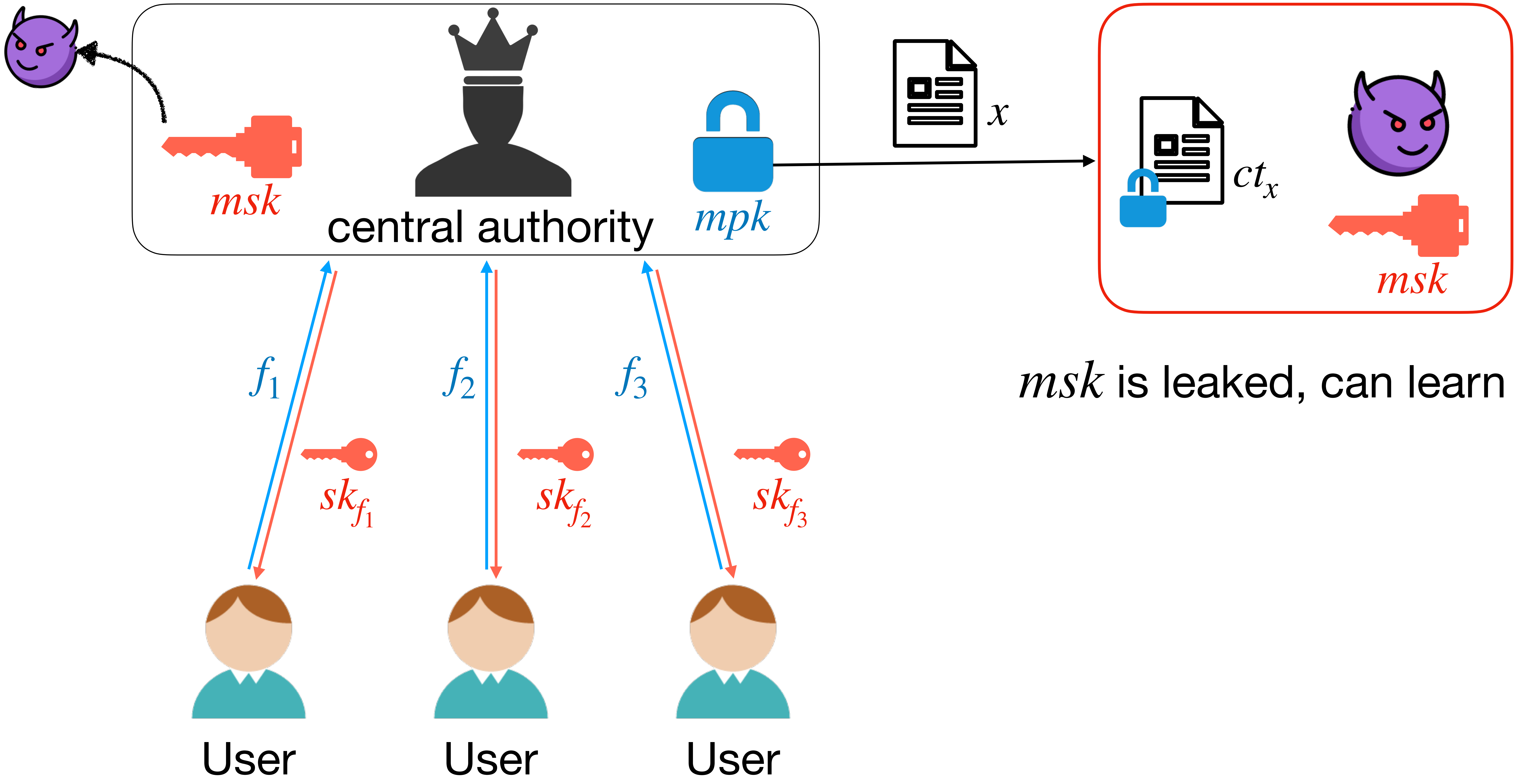


Functional Encryption: Security



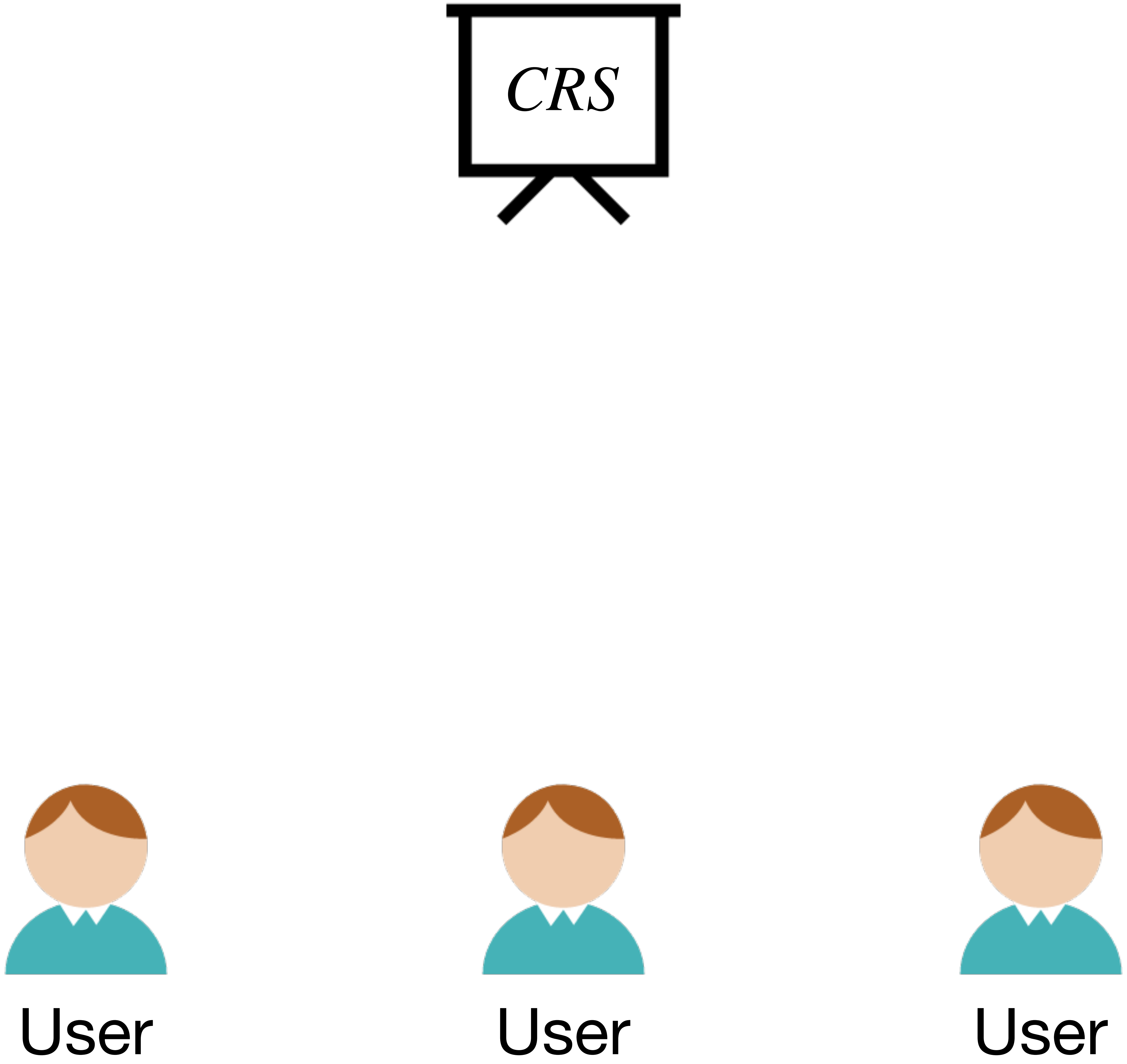
sk_{f_3} is leaked, can learn nothing but $f_3(x)$.

Functional Encryption: Key-Escrow Problem



msk is leaked, can learn any $f(x)$

Registered Functional Encryption



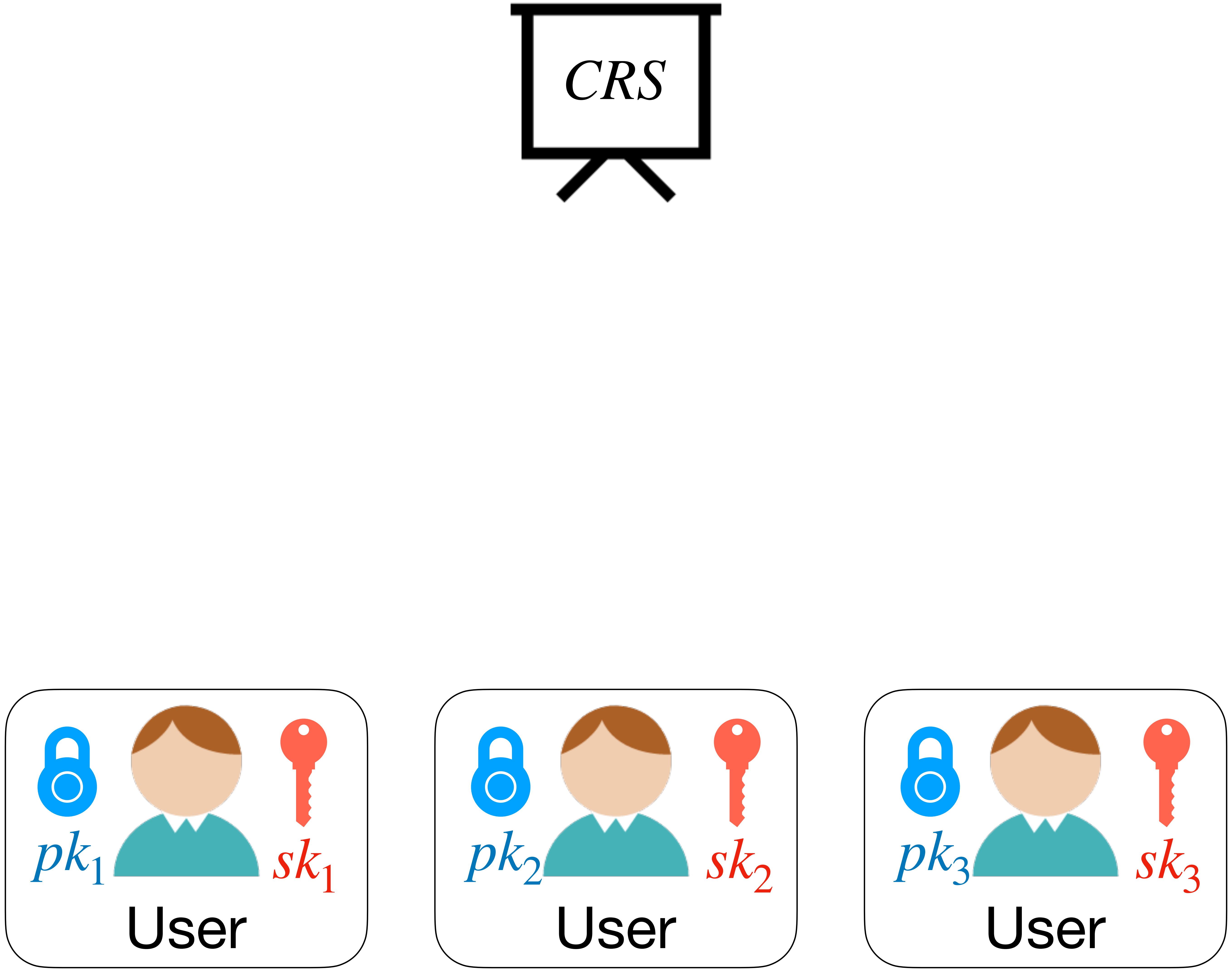
CRS

User

User

User

Registered Functional Encryption



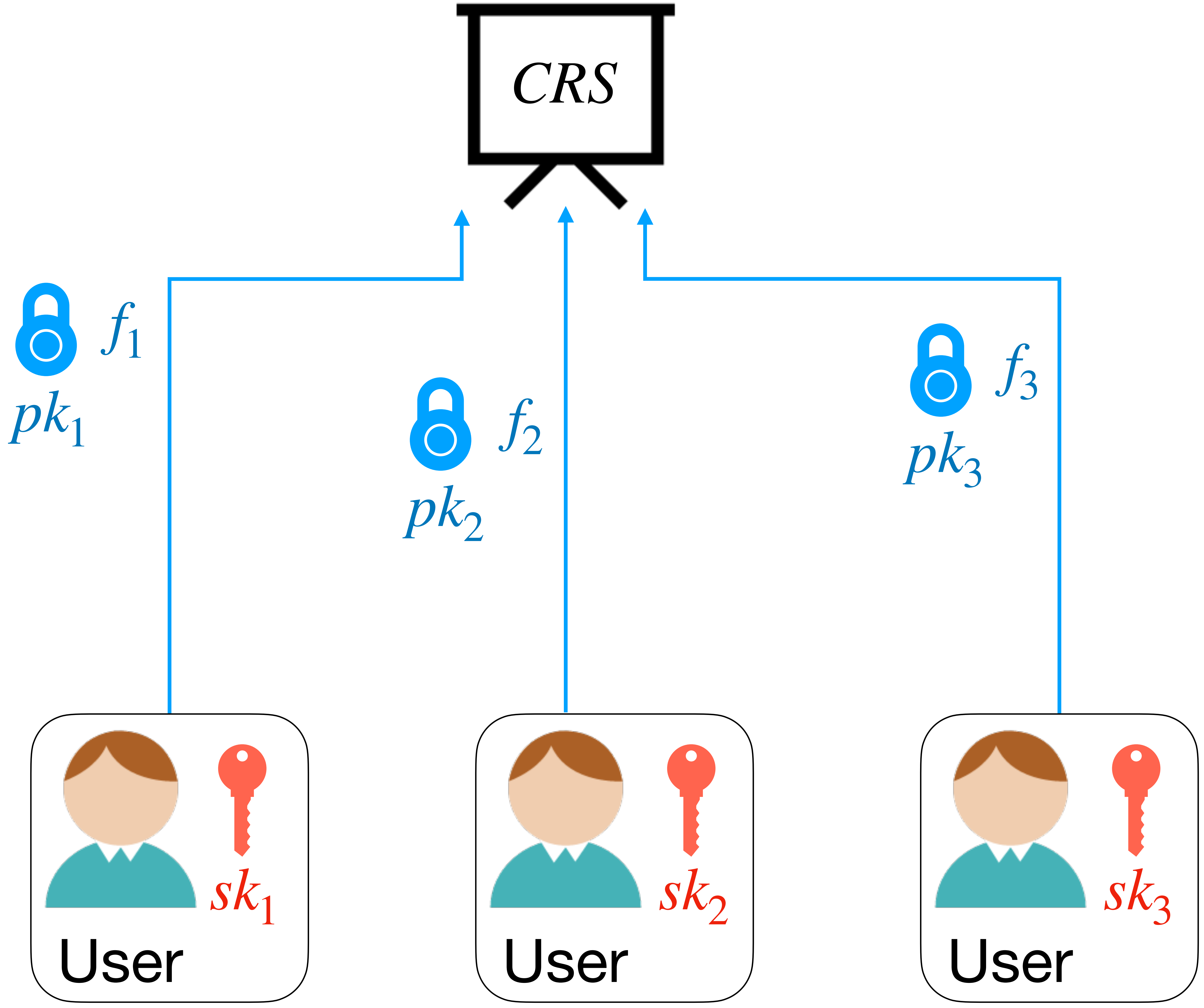
CRS

pk_1 sk_1 User

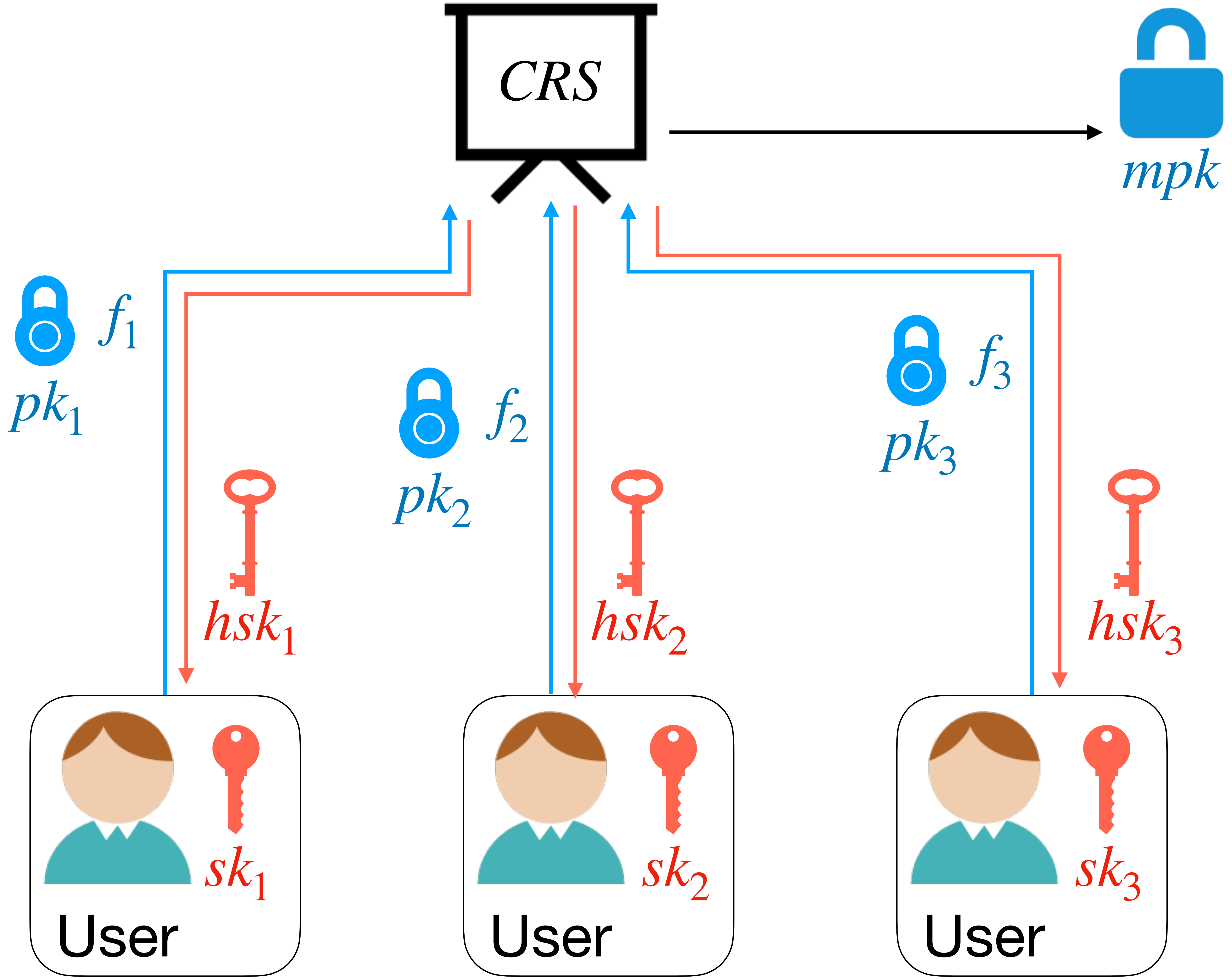
pk_2 sk_2 User

pk_3 sk_3 User

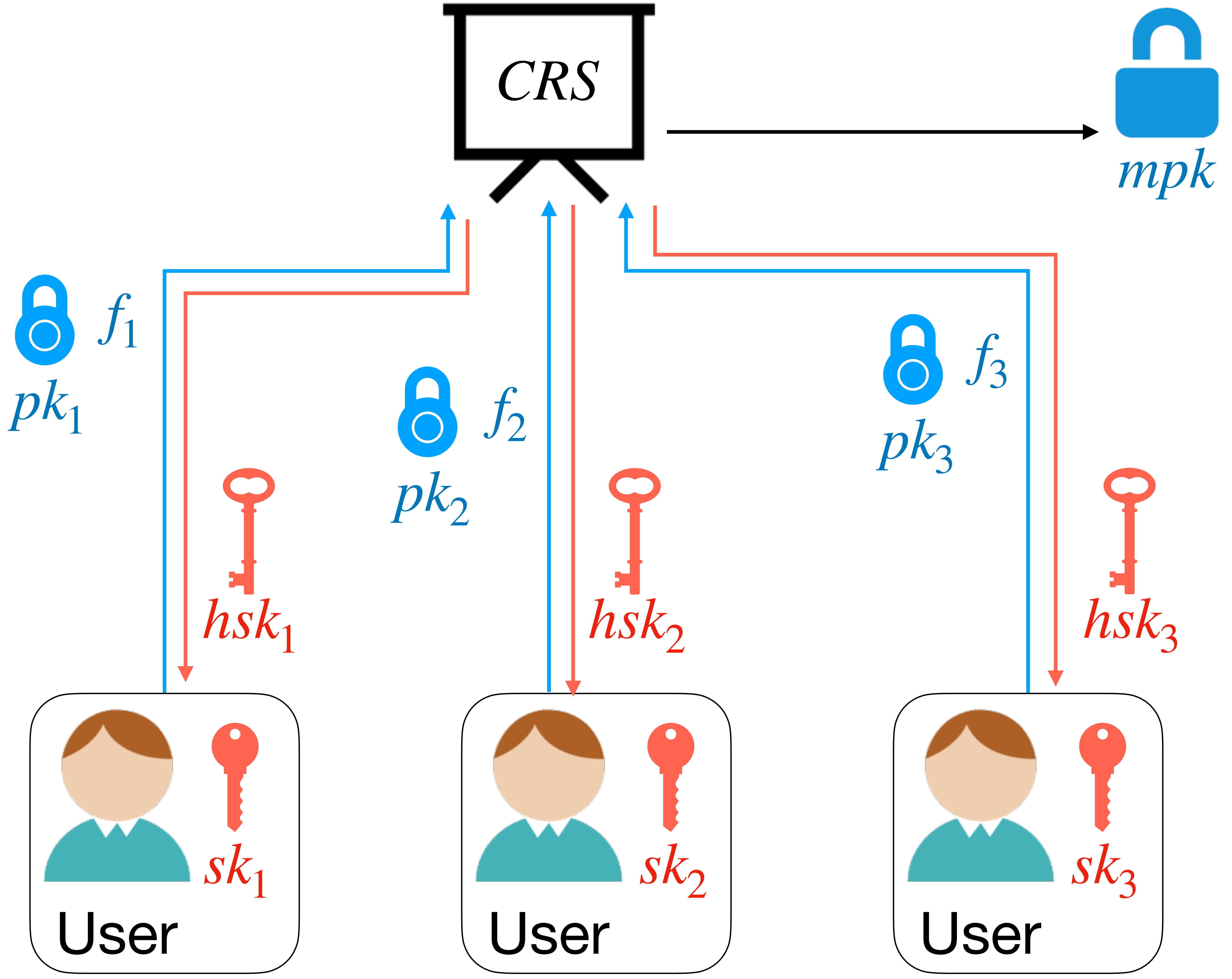
Registered Functional Encryption



Registered Functional Encryption



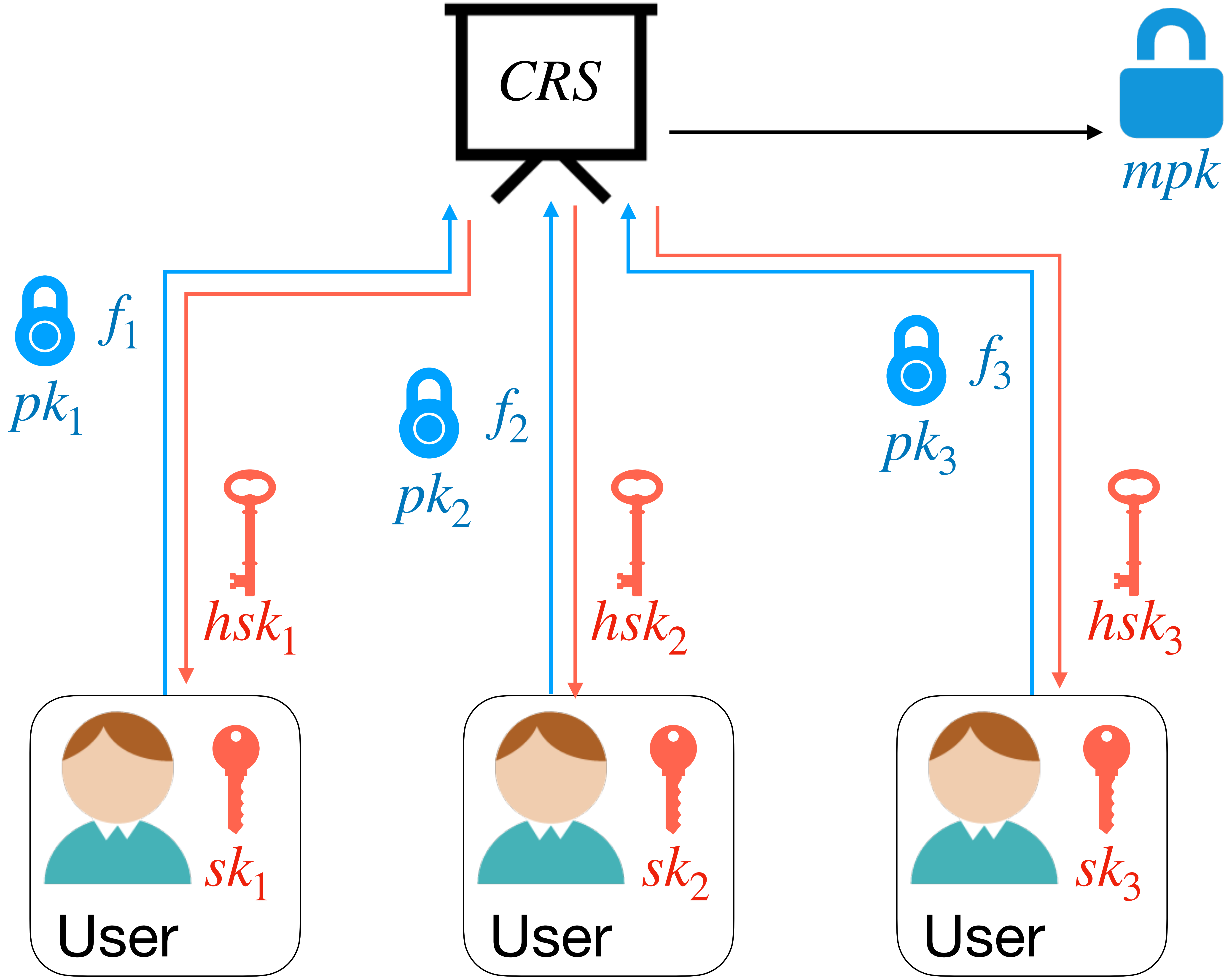
Registered Functional Encryption



full-fledged Reg-FE: register "*one by one*".

mpk and hsk are updatable.

Registered Functional Encryption

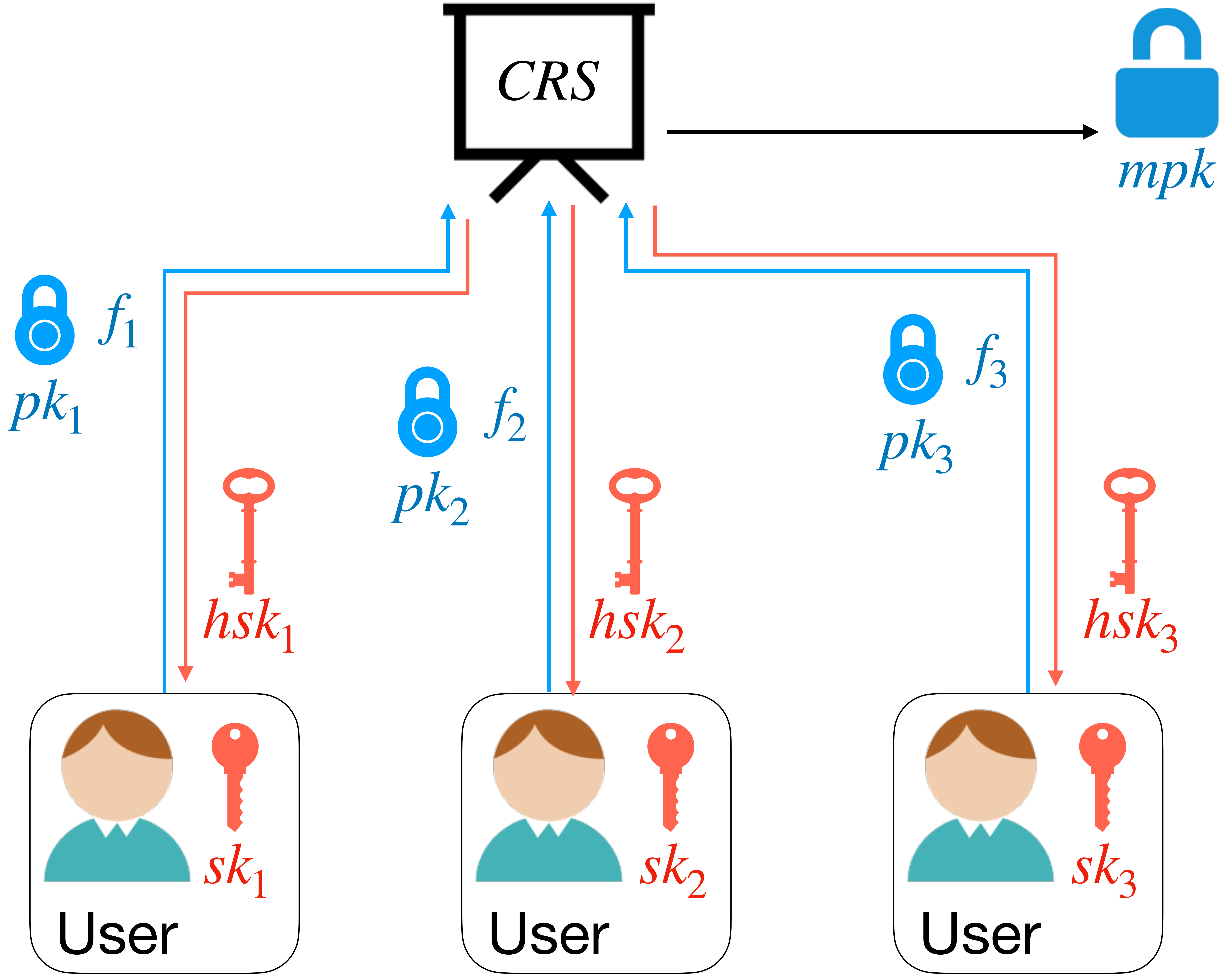


full-fledged Reg-FE: register "*one by one*".

mpk and hsk are updatable.

Size: O(poly(Log L))

Registered Functional Encryption

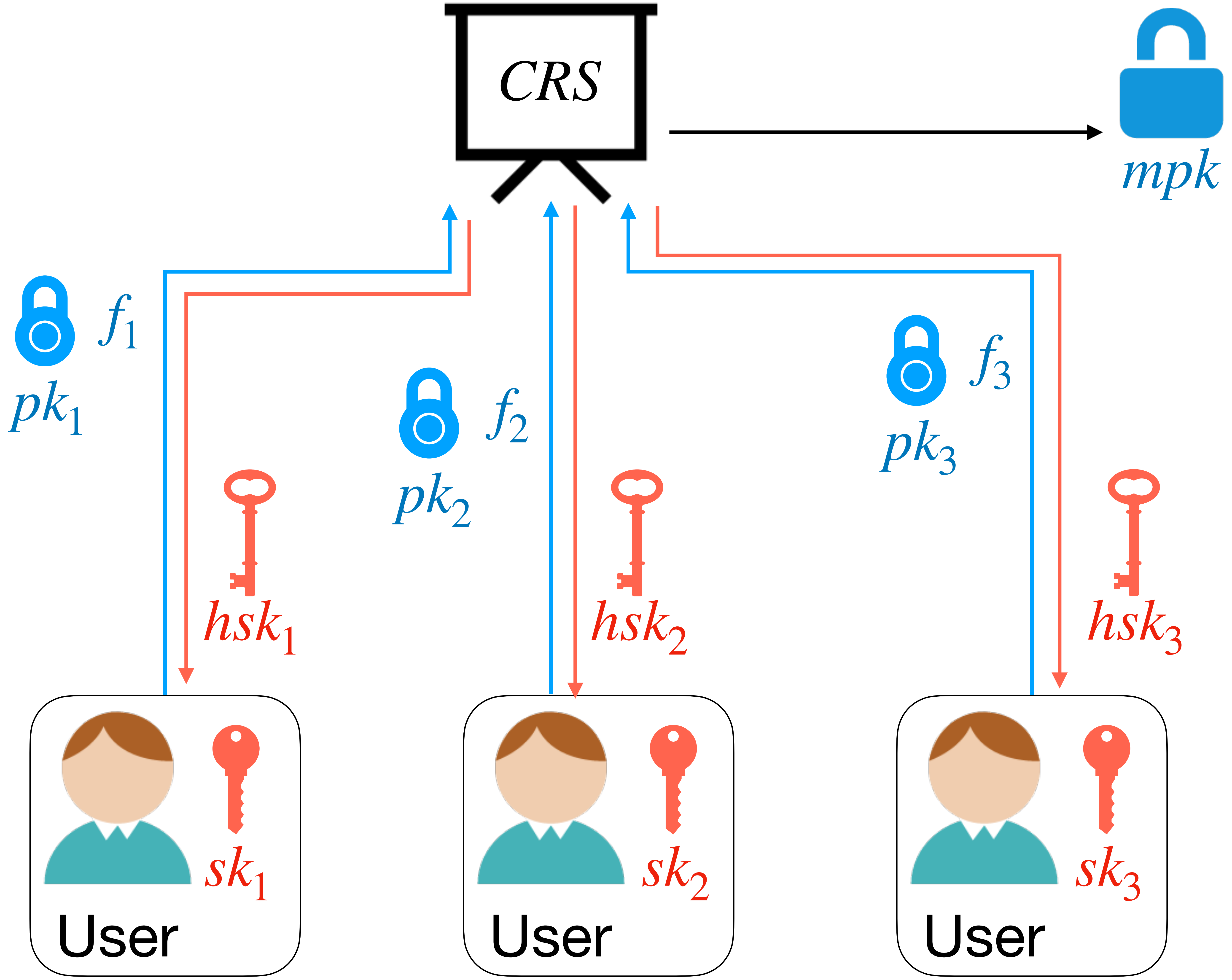


full-fledged Reg-FE: register "*one by one*".

mpk and hsk are updatable.

Update time: O(Log L)

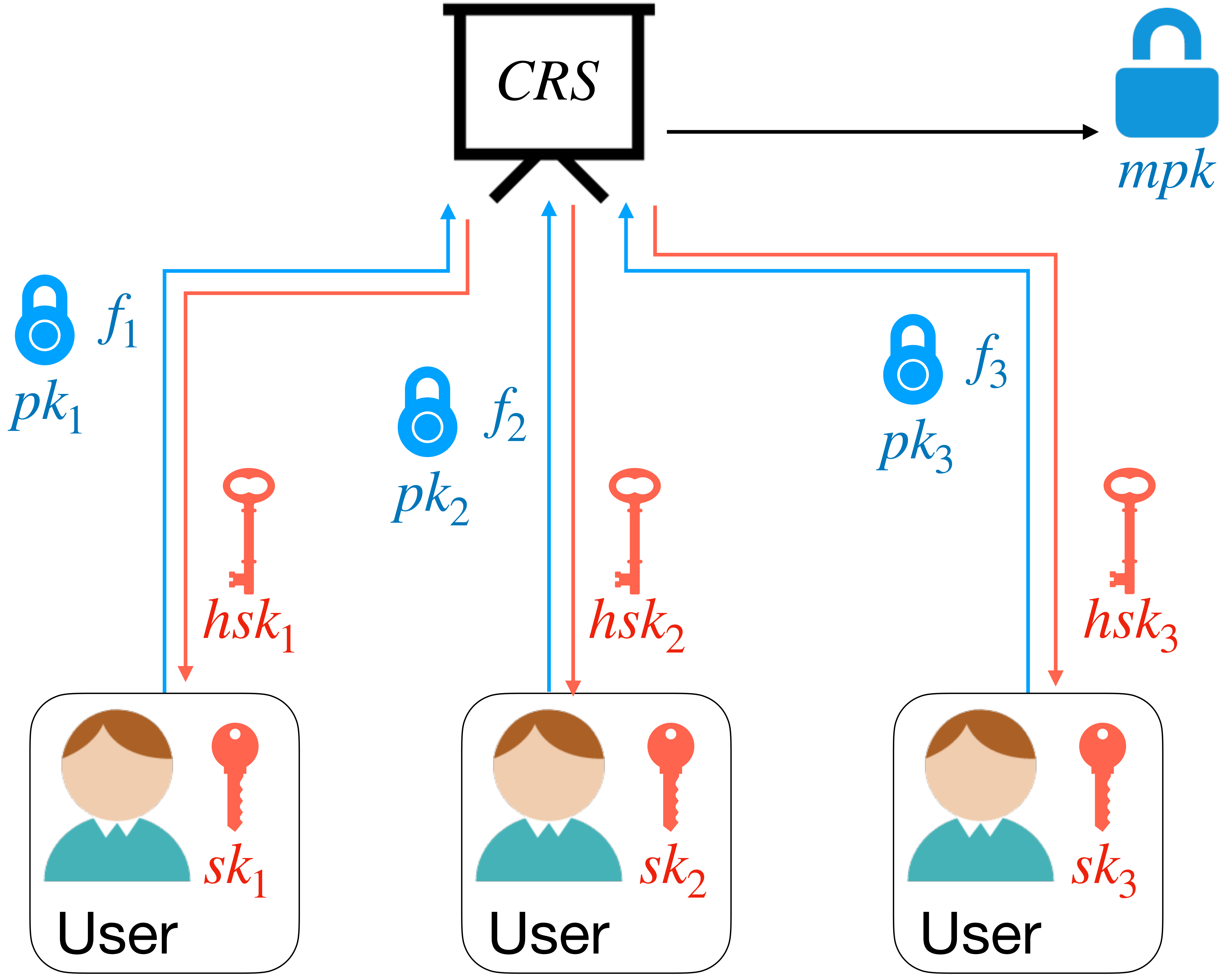
Registered Functional Encryption



slotted Reg-FE: register "*at once time*".

mpk and hsk are generated at once.

Registered Functional Encryption

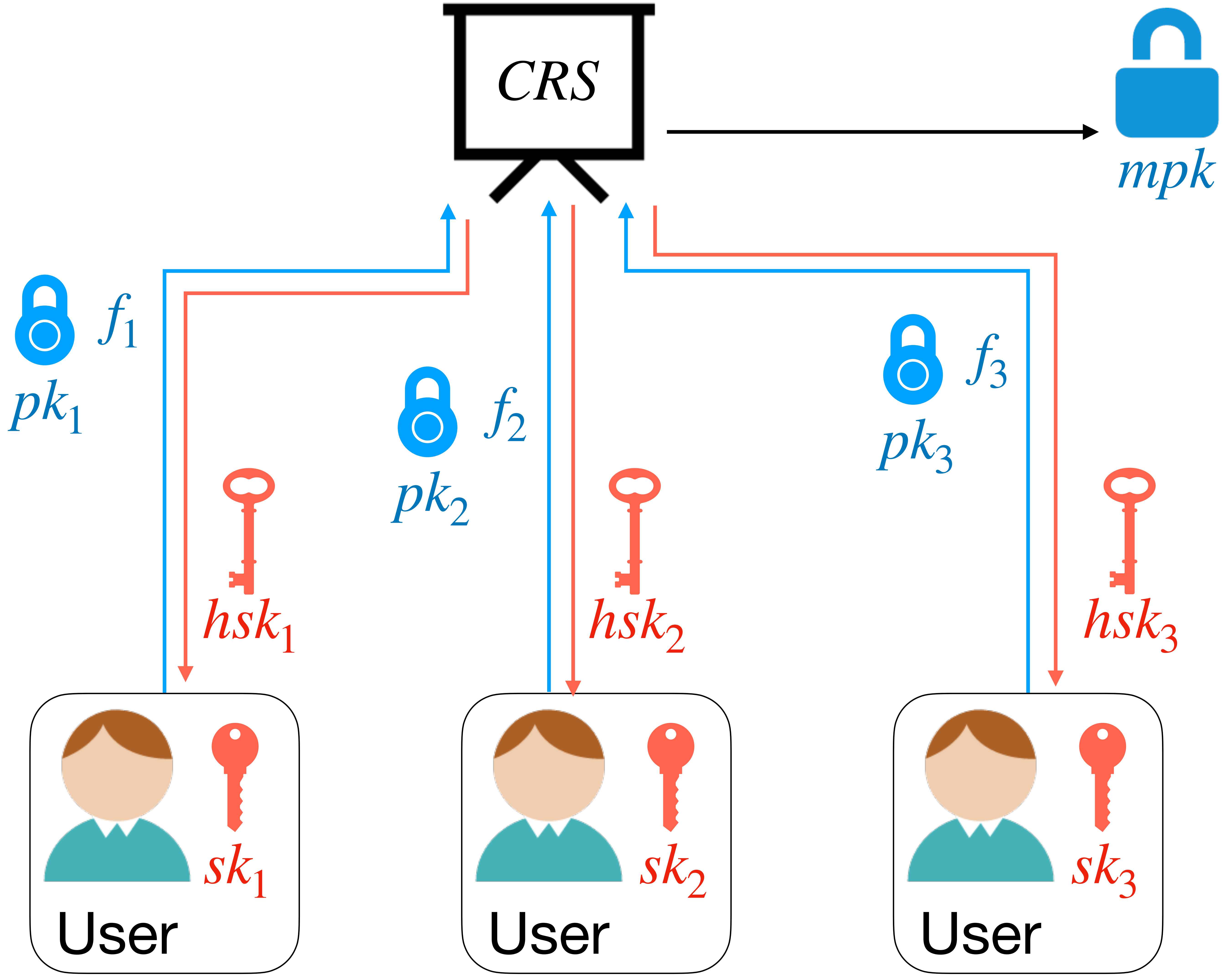


slotted Reg-FE: register "*at once time*".

mpk and hsk are generated at once.

Size: O(poly(Log L))

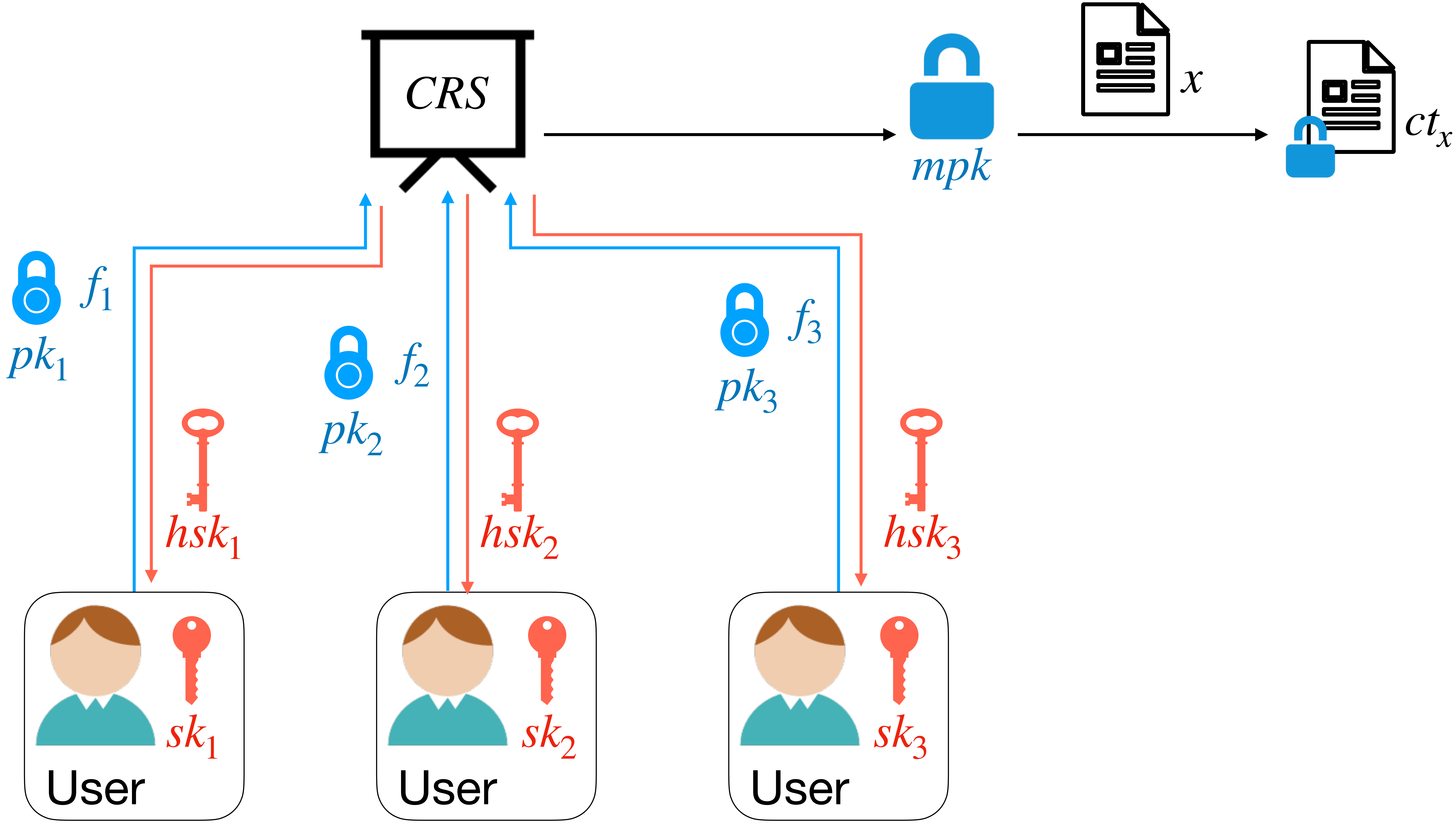
Registered Functional Encryption



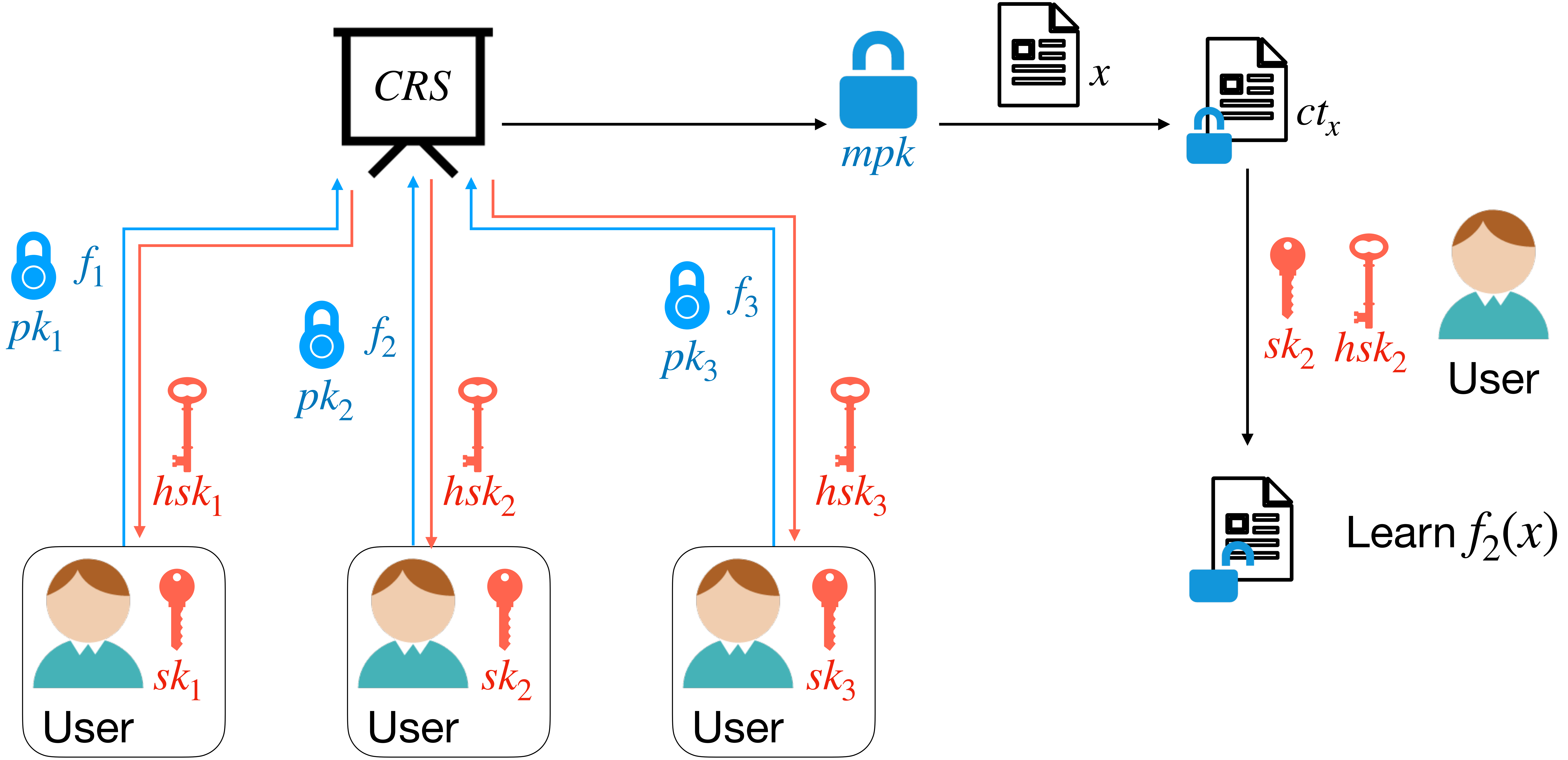
Transformation in [HLWW23]:

Slotted Reg-FE ==> Reg-FE

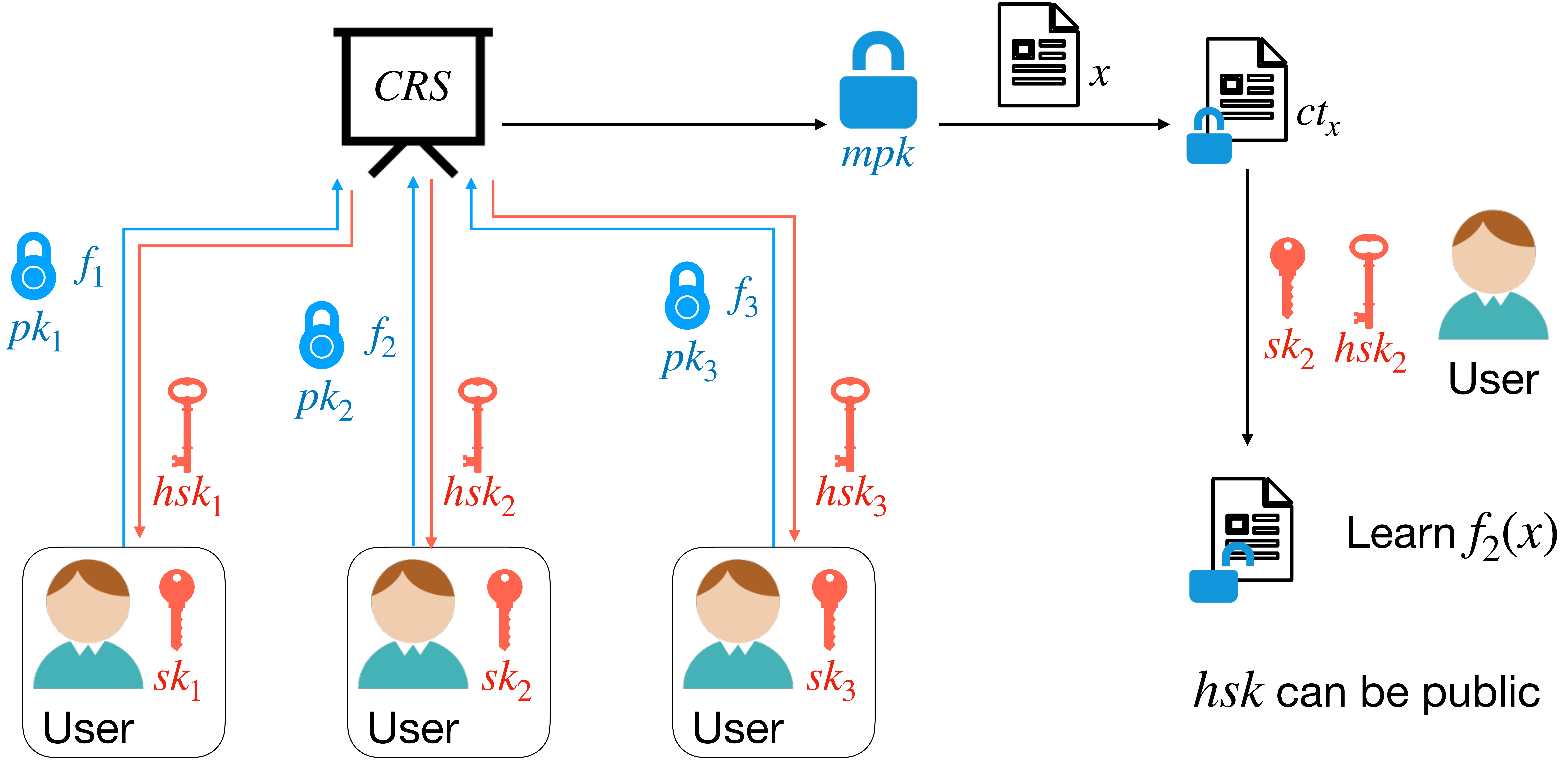
Registered Functional Encryption



Registered Functional Encryption

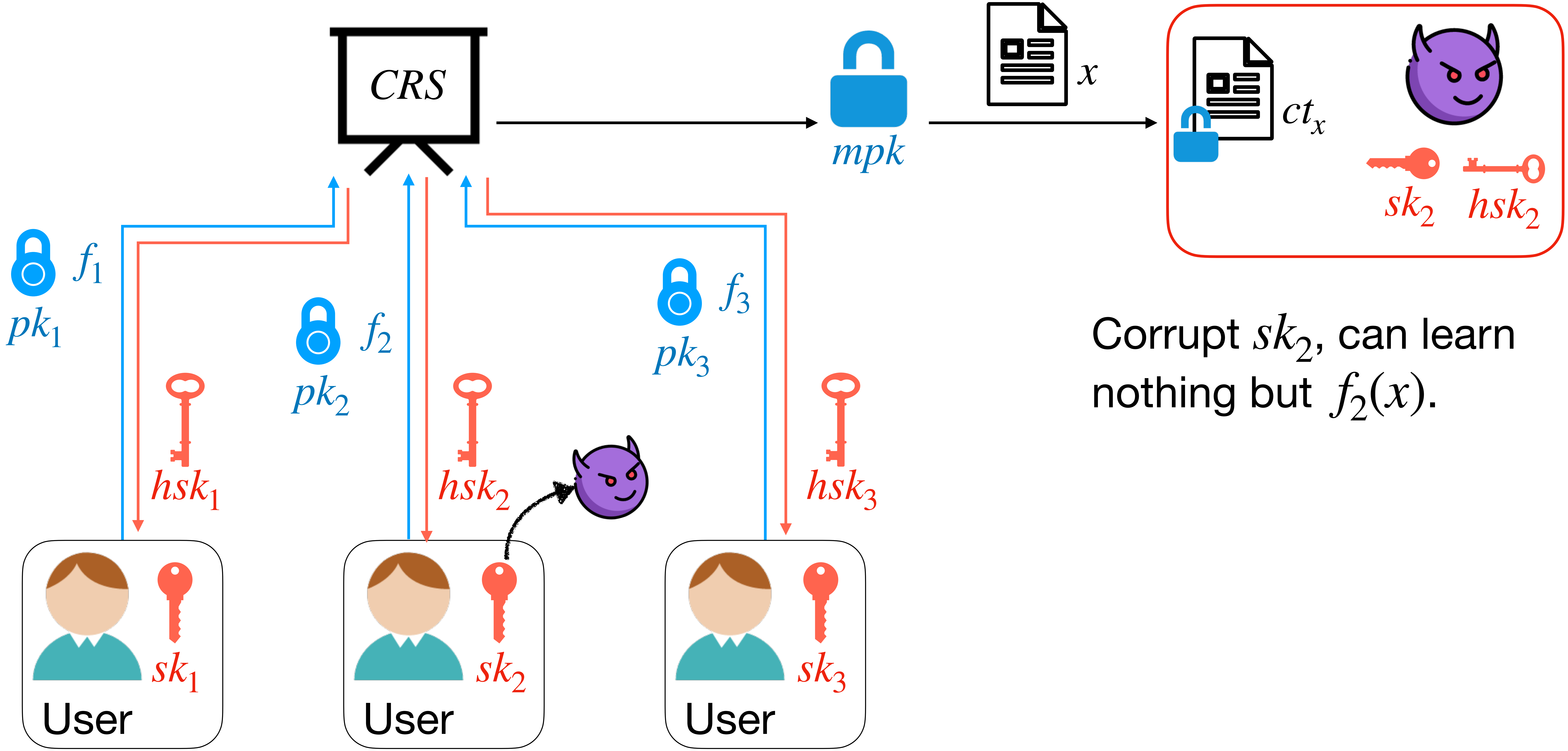


Registered Functional Encryption



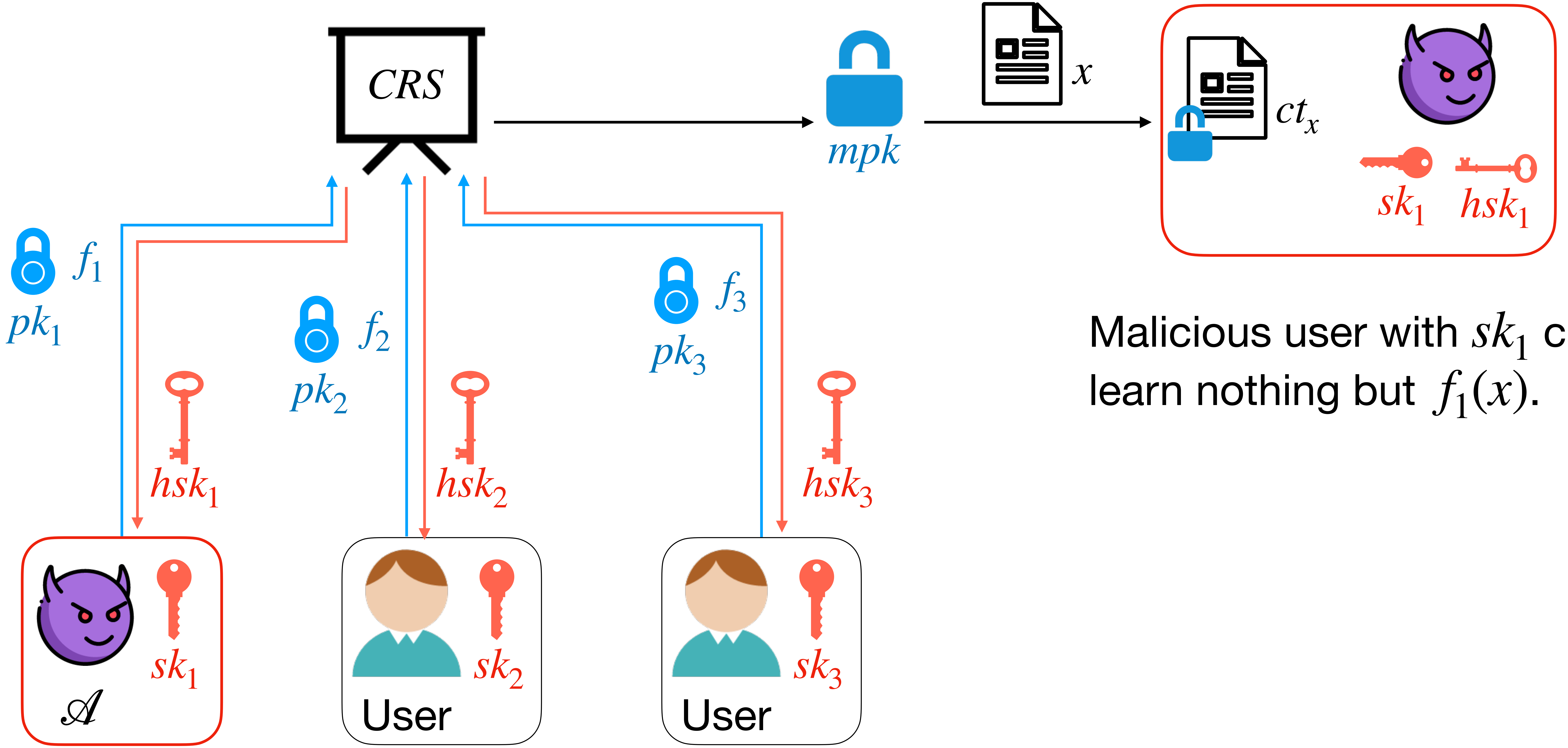
hsk can be public

Registered Functional Encryption: Security



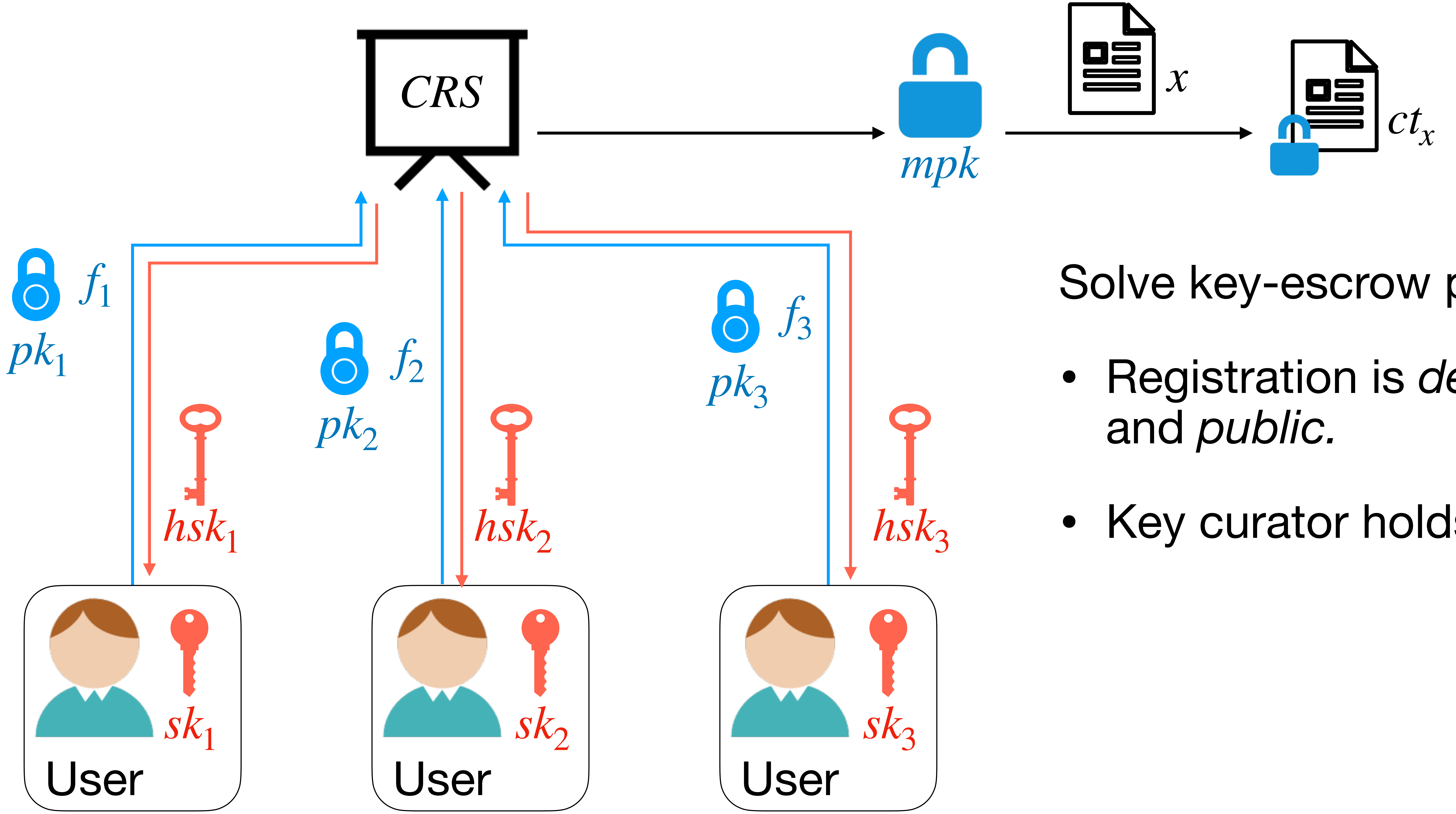
Corrupt sk_2, can learn nothing but $f_2(x)$.

Registered Functional Encryption: Security



Malicious user with sk_1 can learn nothing but $f_1(x)$.

Registered Functional Encryption



Solve key-escrow problem:

- Registration is *deterministic* and *public.*
- Key curator holds *no secret*.

Our Result

Scheme	Function	Security	Assumptions	Size of ciphertext
Main Result				
Reg-IPFE (1)	Linear	Ad-IND	k-lin	n Log L
Reg-QFE	Quadratic	Sel*-SIM	bi-k-lin	n + Log L

Our Result

Scheme	Function	Security	Assumptions	Size of ciphertext
Main Result				
Reg-IPFE (1)	Linear	Ad-IND	k-lin	n Log L
Reg-QFE	Quadratic	Sel*-SIM	bi-k-lin	n + Log L
Related Work				
[DP23, FFM+23]	General	Ad-IND	iO+SSB	n Log L
[HLWW23]	Boolean (ABE)	Ad-IND	Static	n Log L
[ZZGQ23]	Boolean (ABE)	Ad-IND	k-lin	n Log L

Our Result

Scheme	Function	Security	Assumptions	Size of ciphertext
Main Result				
Reg-IPFE (1)	Linear	Ad-IND	k-lin	n Log L
Reg-QFE	Quadratic	Sel*-SIM	bi-k-lin	n + Log L
Related Work				
[DP23, FFM+23]	General	Ad-IND	iO+SSB	n Log L
[HLWW23]	Boolean (ABE)	Ad-IND	Static	n Log L
[ZZGQ23]	Boolean (ABE)	Ad-IND	k-lin	n Log L

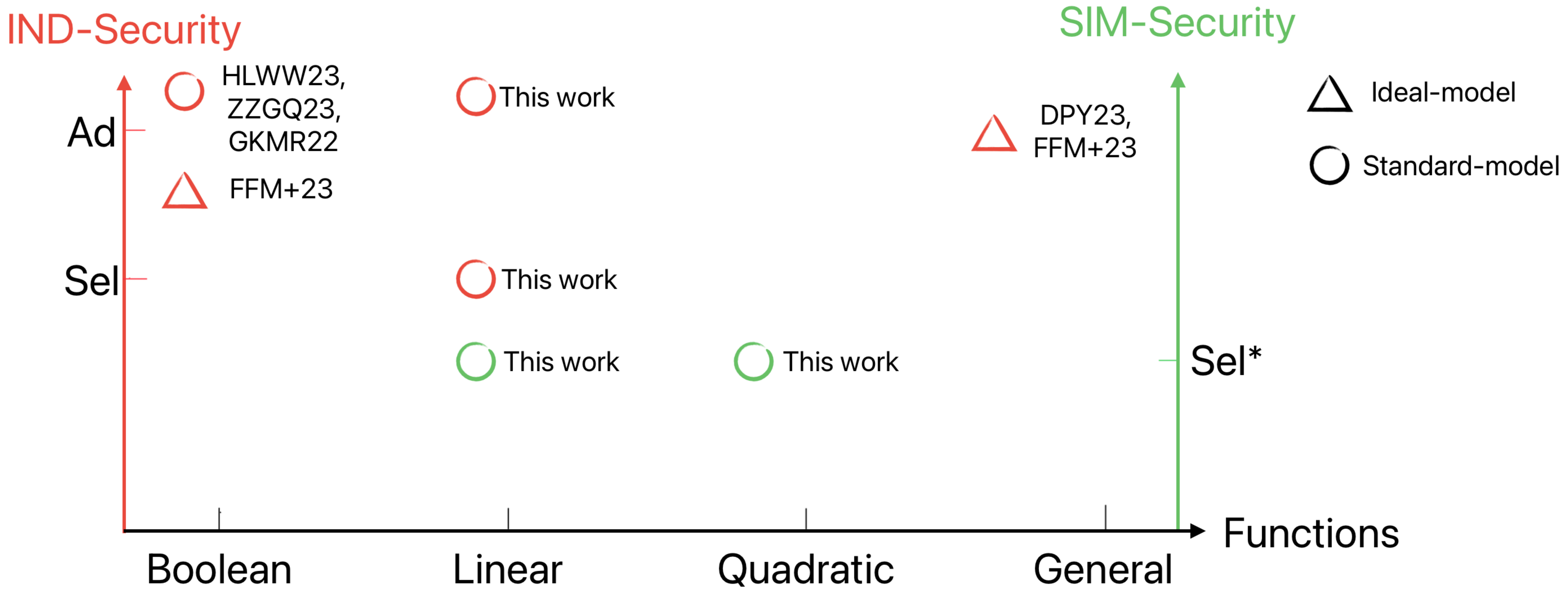
Our Result

Scheme	Function	Security	Assumptions	Size of ciphertext
Main Result				
Reg-IPFE (1)	Linear	Ad-IND	k-lin	n Log L
Reg-QFE	Quadratic	Sel*-SIM	bi-k-lin	n + Log L
Related Work				
[DP23, FFM+23]	General	Ad-IND	iO+SSB	n Log L
[HLWW23]	Boolean (ABE)	Ad-IND	Static	n Log L
[ZZGQ23]	Boolean (ABE)	Ad-IND	k-lin	n Log L

Our Result

Scheme	Function	Security	Assumptions	Size of ciphertext
Main Result				
Reg-IPFE (1)	Linear	Ad-IND	k-lin	n Log L
Reg-QFE	Quadratic	Sel*-SIM	bi-k-lin	n + Log L
Implication				
Reg-IPE	Boolean	Ad-IND & Fully AH	k-lin	n Log L
Reg-IPFE (2)	Linear	Sel-IND	k-lin	n + Log L
Reg-IPFE (3)	Linear	Sel*-SIM	bi-k-lin	n + Log L

Our Result


IND-Security
SIM-Security
Ad
Sel
Sel*
HLWW23,
ZZGQ23,
GKMR22
FFM+23
This work
This work
This work
This work
DPY23,
FFM+23
△ Ideal-model
○ Standard-model
Functions
Boolean
Linear
Quadratic
General

sReg-IPFE with Adaptive IND-Security

IPFE [ABDP15]

$L-$slot Reg-IPFE

$$mpk = [\mathbf{w}]$$

$$sk = \mathbf{w}\mathbf{y}^\top$$

$$ct = [s, s\mathbf{w} + \mathbf{x}]$$

$pk, sk = [\mathrm{u}], u$

Register $(pk, \mathbf{y})$

$$crs = [\mathbf{w}_j], \quad \forall j \in [L]$$

$$pk_i, sk_i = [u_i], u_i$$

$$mpk = [\sum_j \mathbf{w}_j, \sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top)]$$

$$ct = [s, s\sum_j \mathbf{w}_j + \mathbf{x}, s\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top)]$$

sReg-IPFE with Adaptive IND-Security

To L-slot Reg-IPFE: fix the correctness

$$crs = [\mathbf{w}_j], \quad \forall j \in [L]$$

$$pk_i, sk_i = [u_i], u_i$$

$$mpk = [\sum_j \mathbf{w}_j, \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]$$

$$ct = [s, s\sum_j \mathbf{w}_j + \mathbf{x}, s\sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]$$

sk Decrypt:

$$(s\sum_j \mathbf{w}_j + \mathbf{x}) \cdot \mathbf{y}_i^\top - s\sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top) + s \cdot u$$

$$= \mathbf{x}\mathbf{y}_i^\top - s\sum_{j \neq i} (u_j + \mathbf{w}_j \mathbf{y}_j^\top) + s\sum_{j \neq i} \mathbf{w}_j \mathbf{y}_i^\top$$

sReg-IPFE with Adaptive IND-Security

To L-slot Reg-IPFE: fix the correctness

hsk sk

$$crs = [\mathbf{w}_j]_1, \quad \forall j \in [L]$$

$$pk_i, sk_i = [u_i]_1, u_i$$

$$mpk = [\sum_j \mathbf{w}_j, \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_1$$

$$hsk_i = [r_i, r_i \sum_{j \neq i} \mathbf{w}_j, r_i \sum_{j \neq i} (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_2$$

$$ct = [s, s \sum_j \mathbf{w}_j + \boxed{s\mathbf{x}}, s \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_1$$

Decrypt:

$$(sr_i \sum_j \mathbf{w}_j + sr_i \mathbf{x}) \cdot \mathbf{y}_i^\top - sr_i \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top) + sr_i \cdot u$$

$$= sr_i \cdot \mathbf{x}\mathbf{y}_i^\top \cancel{- sr_i \sum_{j \neq i} (u_j + \mathbf{w}_j \mathbf{y}_j^\top) + sr_i \sum_{j \neq i} \mathbf{w}_j \mathbf{y}_i^\top}$$

sReg-IPFE with Adaptive IND-Security

To L-slot Reg-IPFE: proof strategy

Dual-system used in [HLWW23,ZZGQ23]

😈 ?

$$crs = [\mathbf{w}_j]_1, \quad \forall j \in [L]$$

$$[r_i, r_i\mathbf{w}_j]_2, \quad \forall i, j \in [L], i \neq j$$

$$pk_i, sk_i = ([u_i]_1, \{[r_j u_i]_2\}_{j \neq i}), u_i$$

$$mpk = [\sum_j \mathbf{w}_j, \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_1$$

$$hsk_i = [r_i, r_i \sum_{j \neq i} \mathbf{w}_j, r_i \sum_{j \neq i} (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_2$$

$$ct = [s, s \sum_j \mathbf{w}_j + s\mathbf{x}, s \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_1$$

sReg-IPFE with Adaptive IND-Security

To L-slot Reg-IPFE: proof strategy

~~Dual-system used in [HLWW23,ZZGQ23]~~

Nested dual-system method [LW11]

$$crs = [\mathbf{w}_j]_1, \quad \forall j \in [L]$$

$$[r_i, r_i\mathbf{w}_j]_2, \quad \forall i, j \in [L], i \neq j$$

$$pk_i, sk_i = ([u_i]_1, \{[r_j u_i]_2\}_{j \neq i}), u_i$$

$$mpk = [\sum_j \mathbf{w}_j, \sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_1$$

$$hsk_i = [r_i, r_i \sum_{j \neq i} \mathbf{w}_j, r_i \sum_{j \neq i} (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_2$$

$$ct = [s, s\sum_j \mathbf{w}_j + s\mathbf{x}, s\sum_j (u_j + \mathbf{w}_j \mathbf{y}_j^\top)]_1$$

sReg-IPFE to sReg-QFE: Attempt

Attempt: IPFE ==> QFE [Wee20]

$$mpk = [\mathbf{A}_1]_1, [\mathbf{A_2}]_2;$$

$$ct = \underbrace{[\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1]_1}_{\mathbf{y}_1}, \underbrace{[\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2]_2}_{\mathbf{y}_2}, \underbrace{iEnc(\mathbf{x})}_{ct_0};$$

$$sk_{\mathbf{f}} = iKey([\mathbf{M}\mathbf{f}^\top]_2)$$

sReg-IPFE to sReg-QFE: Attempt

Attempt: IPFE ==> QFE [Wee20]

$$mpk = [\mathbf{A}_1]_1, [\mathbf{A}_2]_2;$$

$$ct = [\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2}_{\mathbf{y}_2}]_2, \underbrace{iEnc(\mathbf{x})}_{ct_0};$$

$$sk_{\mathbf{f}} = iKey([\mathbf{M}\mathbf{f}^\top]_2)$$

$$\mathsf{x} = (\mathsf{s}_1 \otimes \mathsf{x}_2 \| \mathsf{x}_1 \otimes \mathsf{s}_2 \| \mathsf{s}_1 \otimes \mathsf{s}_2)$$

$$\mathsf{M} = \begin{pmatrix} \mathsf{A}_1 \otimes \mathsf{I} \\ \mathsf{I} \otimes \mathsf{A}_2 \\ \mathsf{A}_1 \otimes \mathsf{A}_2 \end{pmatrix}$$

sReg-IPFE to sReg-QFE: Attempt

Attempt: IPFE ==> QFE [Wee20]

$$mpk = [\mathbf{A}_1]_1, [\mathbf{A}_2]_2;$$

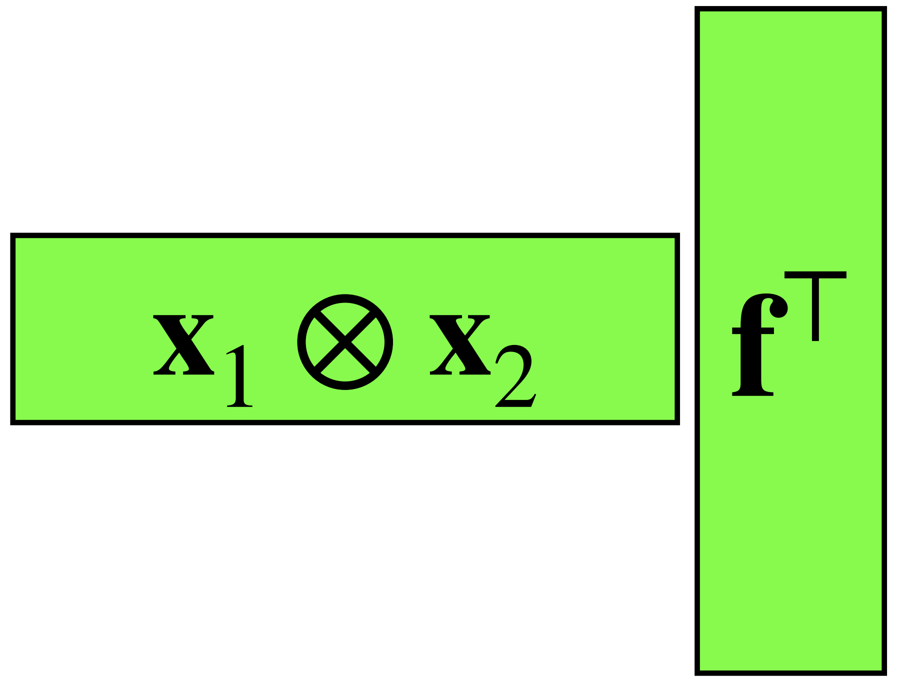
$$ct = \underbrace{[\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1]_1}_{\mathbf{y}_1}, \underbrace{[\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2]_2}_{\mathbf{y}_2}, \underbrace{iEnc(\mathbf{x});}_{ct_0}$$

$$sk_{\mathbf{f}} = iKey([\mathbf{M}\mathbf{f}^\top]_2)$$

$$\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$$

$$\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$$

Decryption goal:



$\mathbf{x}_1 \otimes \mathbf{x}_2$ $\mathbf{f}^\top$

sReg-IPFE to sReg-QFE: Attempt

Attempt: IPFE ==> QFE [Wee20]

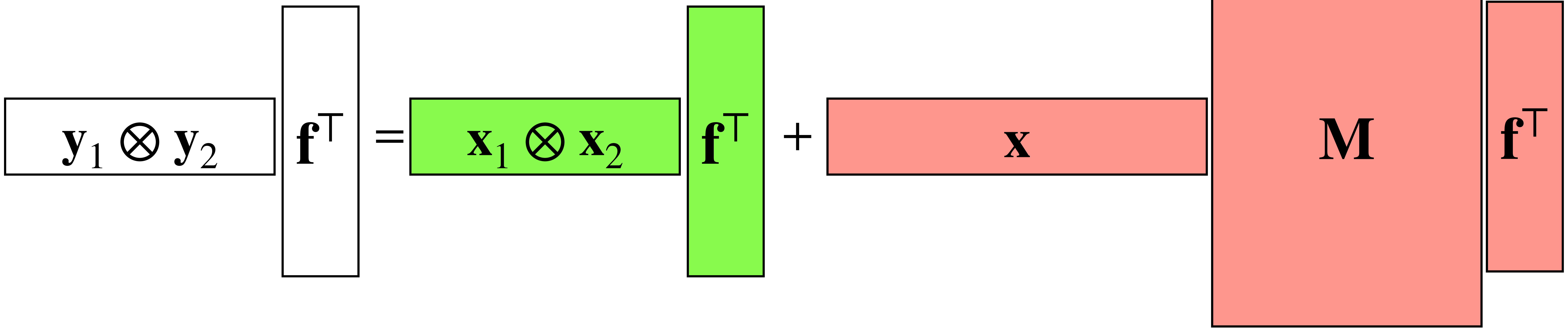
$$mpk = [\mathbf{A}_1]_1, [\mathbf{A}_2]_2;$$

$$ct = \underbrace{[\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1]_1}_{\mathbf{y}_1}, \underbrace{[\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2]_2}_{\mathbf{y}_2}, \underbrace{iEnc(\mathbf{x});}_{ct_0}$$

$$sk_{\mathbf{f}} = iKey([\mathbf{M}\mathbf{f}^\top]_2)$$

$$\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$$

$$\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$$



$$\mathbf{y}_1 \otimes \mathbf{y}_2 \; \mathbf{f}^\top = \mathbf{x}_1 \otimes \mathbf{x}_2 \; \mathbf{f}^\top + \mathbf{x} \; \mathbf{M} \; \mathbf{f}^\top$$

sReg-IPFE to sReg-QFE: Attempt

Attempt: IPFE ==> QFE [Wee20]

$$mpk = [\mathbf{A}_1]_1, [\mathbf{A}_2]_2;$$

$$ct = \underbrace{[\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1]_1}_{\mathbf{y}_1}, \underbrace{[\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2]_2}_{\mathbf{y}_2}, \underbrace{iEnc(\mathbf{x})}_{ct_0};$$

$$sk_{\mathbf{f}} = iKey([\mathbf{M}\mathbf{f}^\top]_2)$$

$$\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$$

$$\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$$

$$\boxed{\mathbf{y}_1 \otimes \mathbf{y}_2}\,\boxed{\mathbf{f}^\top} = \boxed{\mathbf{x}_1 \otimes \mathbf{x}_2}\,\boxed{\mathbf{f}^\top} + \cancel{\boxed{\mathbf{x}}\,\boxed{\mathbf{M}}\,\boxed{\mathbf{f}^\top}} \Leftarrow \boxed{iDec(ct_0, sk_{\mathbf{f}})}$$

sReg-IPFE to sReg-QFE: Challenge-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{xMf}^\top]_T$$

Brute-force search with varied DLOG base

sReg-IPFE to sReg-QFE: Challenge-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{xMf}^\top]_T$$

Brute-force search with varied DLOG base

$$\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$$

$$\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$$

sReg-IPFE to sReg-QFE: Challenge-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{xMf}^\top]_T$$

~~Brute-force search with varied DLOG base~~

$$\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$$

Too Large!

$$\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$$

sReg-IPFE to sReg-QFE: Solution-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{xMf}^\top]_T$$

Need fixed DLOG base

sReg-IPFE to sReg-QFE: Solution-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{x}\mathbf{M}\mathbf{f}^\top]_T$$

Need fixed DLOG base

$$hsk_i = [r_i, r_i \sum_{j \neq i} \mathbf{w}_j, r_i \sum_{j \neq i} (u_j + \mathbf{w}_j \mathbf{M}\mathbf{f}_j^\top)]_2$$

$$ct_0 = [s, s \sum_j \mathbf{w}_j + s\mathbf{x}, s \sum_j (u_j + \mathbf{w}_j \mathbf{M}\mathbf{f}_j^\top)]_1$$

sReg-IPFE to sReg-QFE: Solution-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{x}\mathbf{M}\mathbf{f}^\top]_T$$

Need fixed DLOG base

$$hsk_i = [r_i, r_i\mathbf{w}_i\mathbf{M}\mathbf{f}_i^\top + \mathbf{w}\mathbf{M}\mathbf{f}_i^\top, r_i \sum_{j\neq i} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)]_2$$

$$ct_0 = [s, s\mathbf{w} + \mathbf{x}, s \sum_{j} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)]_1$$

sReg-IPFE to sReg-QFE: Solution-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [sr_i \cdot \mathbf{x}\mathbf{M}\mathbf{f}^\top]_T$$

Need fixed DLOG base

$$hsk_i = [r_i, r_i\mathbf{w}_i\mathbf{M}\mathbf{f}_i^\top + \mathbf{w}\mathbf{M}\mathbf{f}_i^\top, r_i \sum_{j \neq i} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)]_2$$

$$ct_0 = [s, s\mathbf{w} + \mathbf{x}, s \sum_{j} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)]_1$$

Decrypt:

$$\boxed{\begin{aligned}&(s\mathbf{w} + \mathbf{x}) \cdot \mathbf{M}\mathbf{f}_i^\top - s(r_i\mathbf{w}_i\mathbf{M}\mathbf{f}_i^\top + \mathbf{w}\mathbf{M}\mathbf{f}_i^\top) + sr_i \sum_{j} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top) - sr_i \cdot u \\ &= \mathbf{x}\mathbf{M}\mathbf{f}_i^\top + sr_i \sum_{j \neq i} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)\end{aligned}}$$

sReg-IPFE to sReg-QFE: Solution-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [1 \cdot \mathbf{x}\mathbf{M}\mathbf{f}^\top]_T$$

With fixed DLOG base

$$hsk_i = [r_i, r_i\mathbf{w}_i\mathbf{M}\mathbf{f}_i^\top + \mathbf{w}\mathbf{M}\mathbf{f}_i^\top, r_i \sum_{j\neq i} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)]_2$$

$$ct_0 = [s, s\mathbf{w} + \mathbf{x}, s \sum_{j} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)]_1$$

Decrypt:

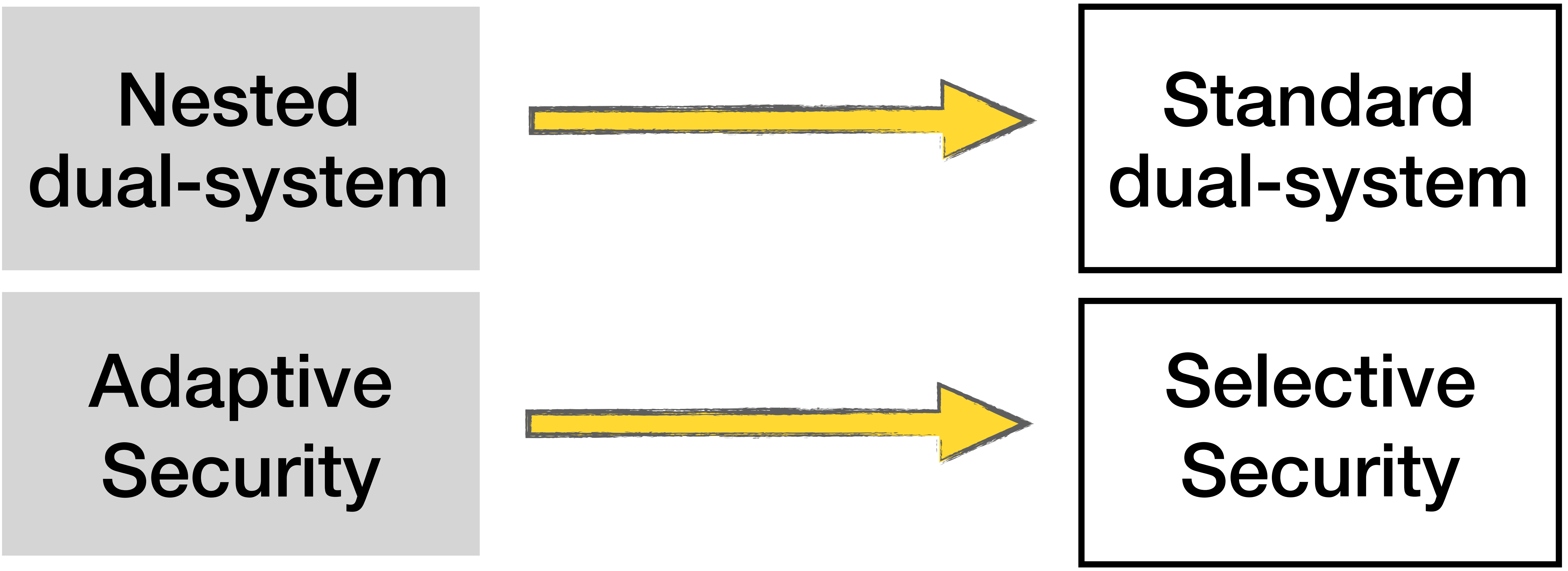
$$(s\mathbf{w} + \mathbf{x}) \cdot \mathbf{M}\mathbf{f}_i^\top - s(r_i\mathbf{w}_i\mathbf{M}\mathbf{f}_i^\top + \mathbf{w}\mathbf{M}\mathbf{f}_i^\top) + sr_i \sum_{j} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top) - sr_i \cdot u$$

$$= \mathbf{x}\mathbf{M}\mathbf{f}_i^\top \cancel{+ sr_i \sum_{j\neq i} (u_j + \mathbf{w}_j\mathbf{M}\mathbf{f}_j^\top)}$$

sReg-IPFE to sReg-QFE: Solution-1

$$iDec(ct_0, sk_i, hsk_i) \longrightarrow [1 \cdot \mathbf{xMf}^\top]_T$$

With fixed DLOG base



sReg-IPFE to sReg-QFE: Challenge-2

$iKey([\mathbf{Mf}^\top]_2)$

[Wee20]: “register” function over $\mathbb{G}_2$

sReg-IPFE to sReg-QFE: Challenge-2

$iKey([\mathbf{M}\mathbf{f}^\top]_2)$ [Wee20]: “register” function over $\mathbb{G}_2$

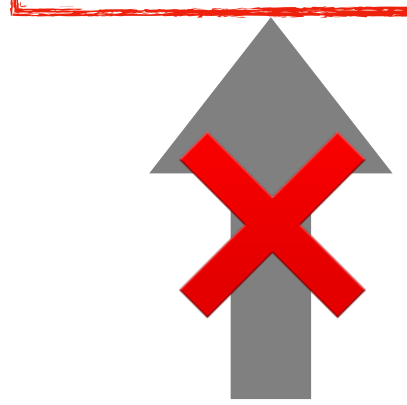
$icrs: [r_i, r_i\mathbf{w}_j]_2, \quad i \neq j$ Our Reg-IPFE: terms for hsk over $\mathbb{G}_2$

sReg-IPFE to sReg-QFE: Challenge-2

$$iKey([\mathbf{M}\mathbf{f}^\top]_2)$$

$$icrs : [r_i, r_i\mathbf{w}_j]_2, \quad i \neq j$$

$$ihsk_i : [\sum_{j \neq i} (r_i u_j + \boxed{r_i \mathbf{w}_j \mathbf{M}\mathbf{f}_j^\top})]_2$$



$$[r_i\mathbf{w}_j]_2, [\mathbf{M}\mathbf{f}_j^\top]_2$$

Cannot multiply them over $\mathbb{G}_2$

sReg-IPFE to sReg-QFE: Solution-2

$$[\mathbf{M}] = \begin{bmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{bmatrix} \xleftarrow{\text{Determine}} [\mathbf{A}_1]\ [\mathbf{A}_2]$$

sReg-IPFE to sReg-QFE: Solution-2

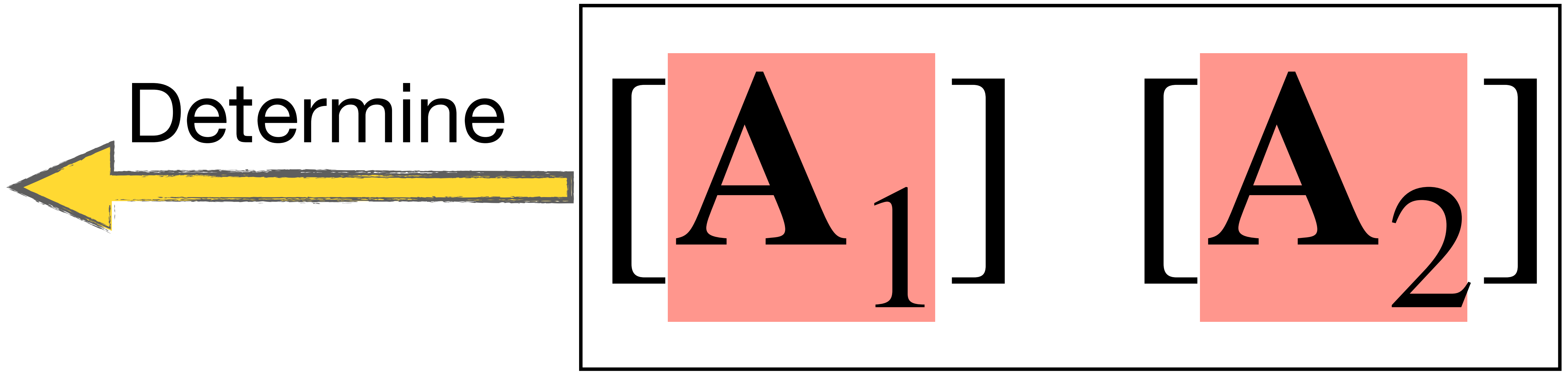
$$[\mathbf{M}] = \begin{bmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{bmatrix} \xleftarrow{\text{Determine}} [\mathbf{A}_1] \quad [\mathbf{A}_2]$$

For security: must be over group, to use MDDH

$$ct = \underbrace{[\boxed{\mathbf{s}_1\mathbf{A}_1} + \mathbf{x}_1]_1}_{\mathbf{y}_1}, \underbrace{[\boxed{\mathbf{s}_2\mathbf{A}_2} + \mathbf{x}_2]_2}_{\mathbf{y}_2}, \underbrace{iEnc(\mathbf{x})}_{ct_0};$$

sReg-IPFE to sReg-QFE: Solution-2

$$[\mathbf{M}] = \begin{bmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{bmatrix}$$

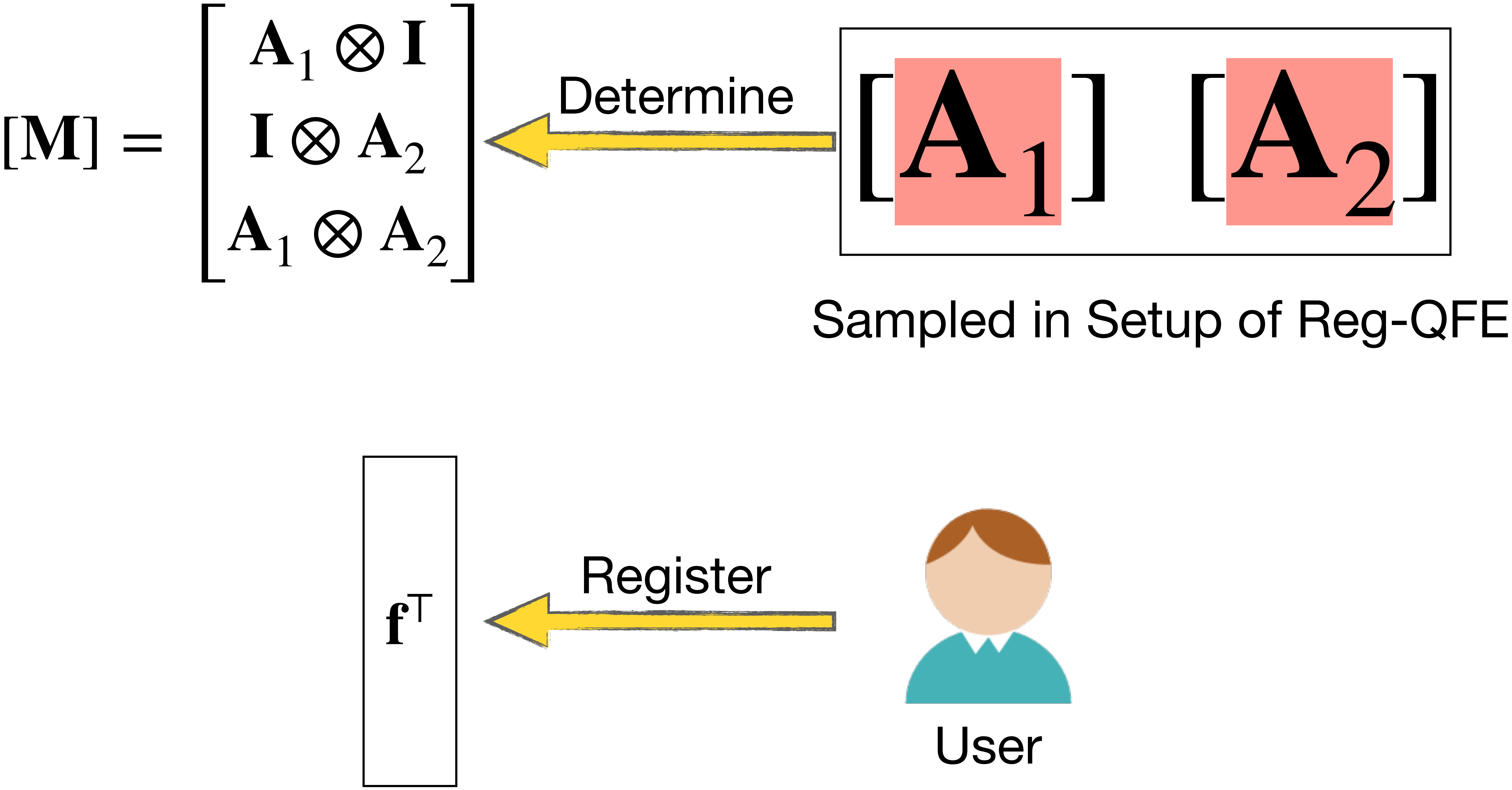


Determine

$[\mathbf{A}_1]$ $[\mathbf{A}_2]$

Sampled in Setup of Reg-QFE

sReg-IPFE to sReg-QFE: Solution-2



$$[\mathbf{M}] = \begin{bmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{bmatrix}$$

Determine

$$[\mathbf{A}_1] \quad [\mathbf{A}_2]$$

Sampled in Setup of Reg-QFE

$$\mathbf{f}^\top$$

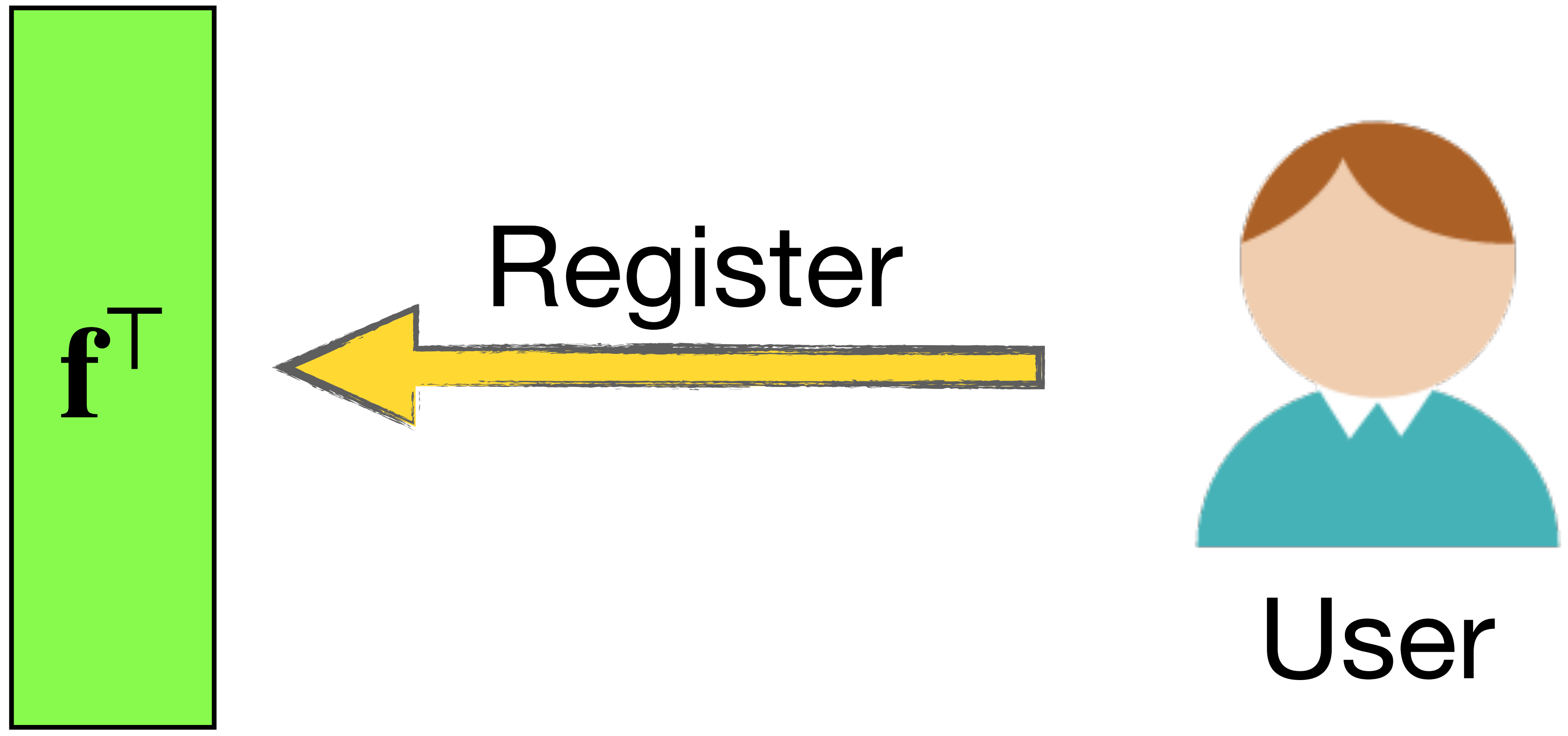
Register

User

sReg-IPFE to sReg-QFE: Solution-2

$$[\mathbf{M}] = \begin{bmatrix} \mathbf{A}_1 \otimes \mathbf{I} \\ \mathbf{I} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{bmatrix} \xleftarrow{\text{Determine}} \boxed{[\mathbf{A}_1] \quad [\mathbf{A}_2]}$$

Sampled in Setup of Reg-QFE



Over $\mathbb{Z}_p$

sReg-IPFE to sReg-QFE: Solution-2

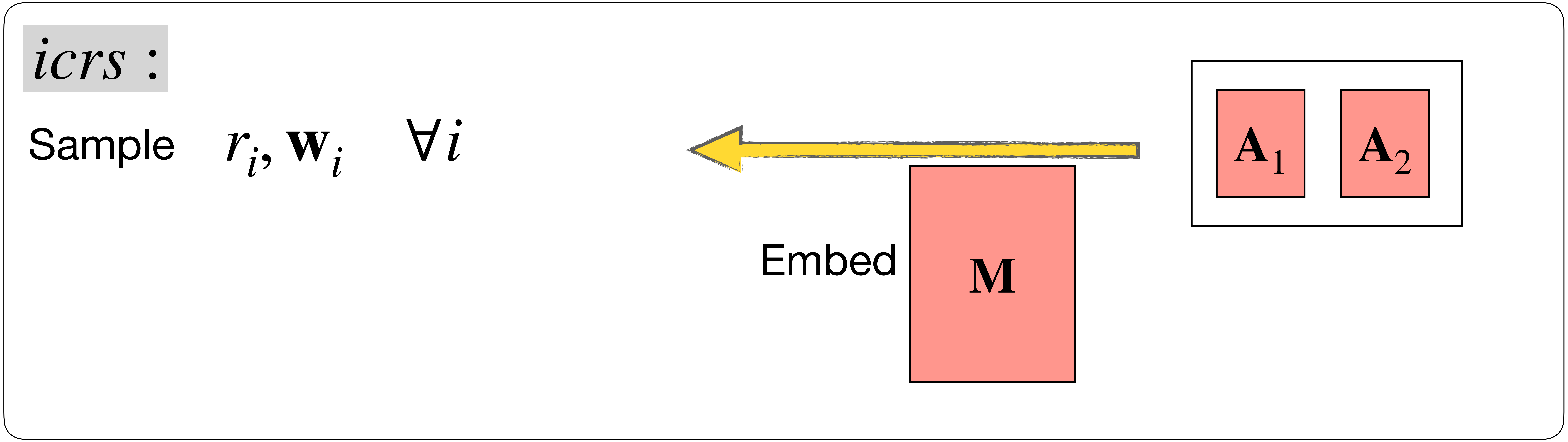
$icrs:$

Sample $r_i, \mathbf{w}_i \quad \forall i$

Sample: $\boxed{\mathbf{A}_1 \quad \mathbf{A}_2}$

Setup of Reg-QFE

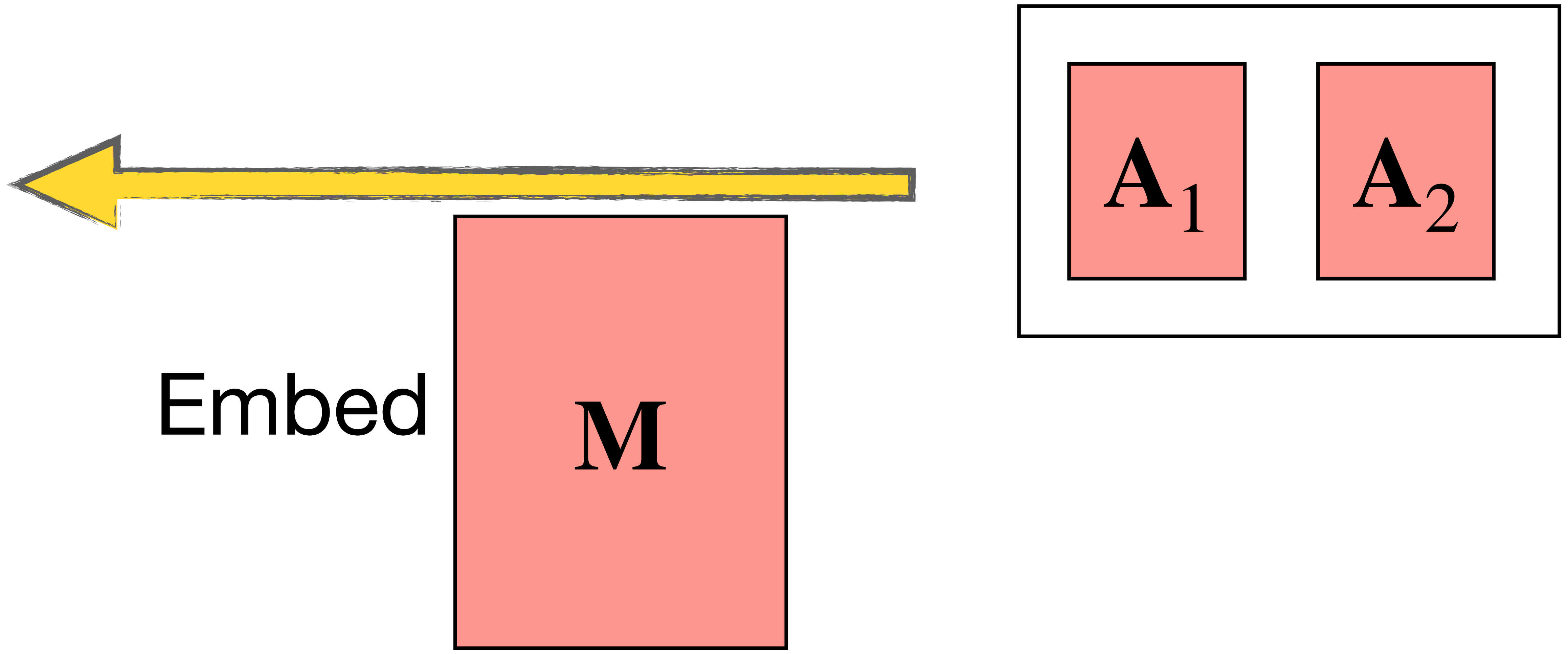
sReg-IPFE to sReg-QFE: Solution-2



Setup of Reg-QFE

sReg-IPFE to sReg-QFE: Solution-2

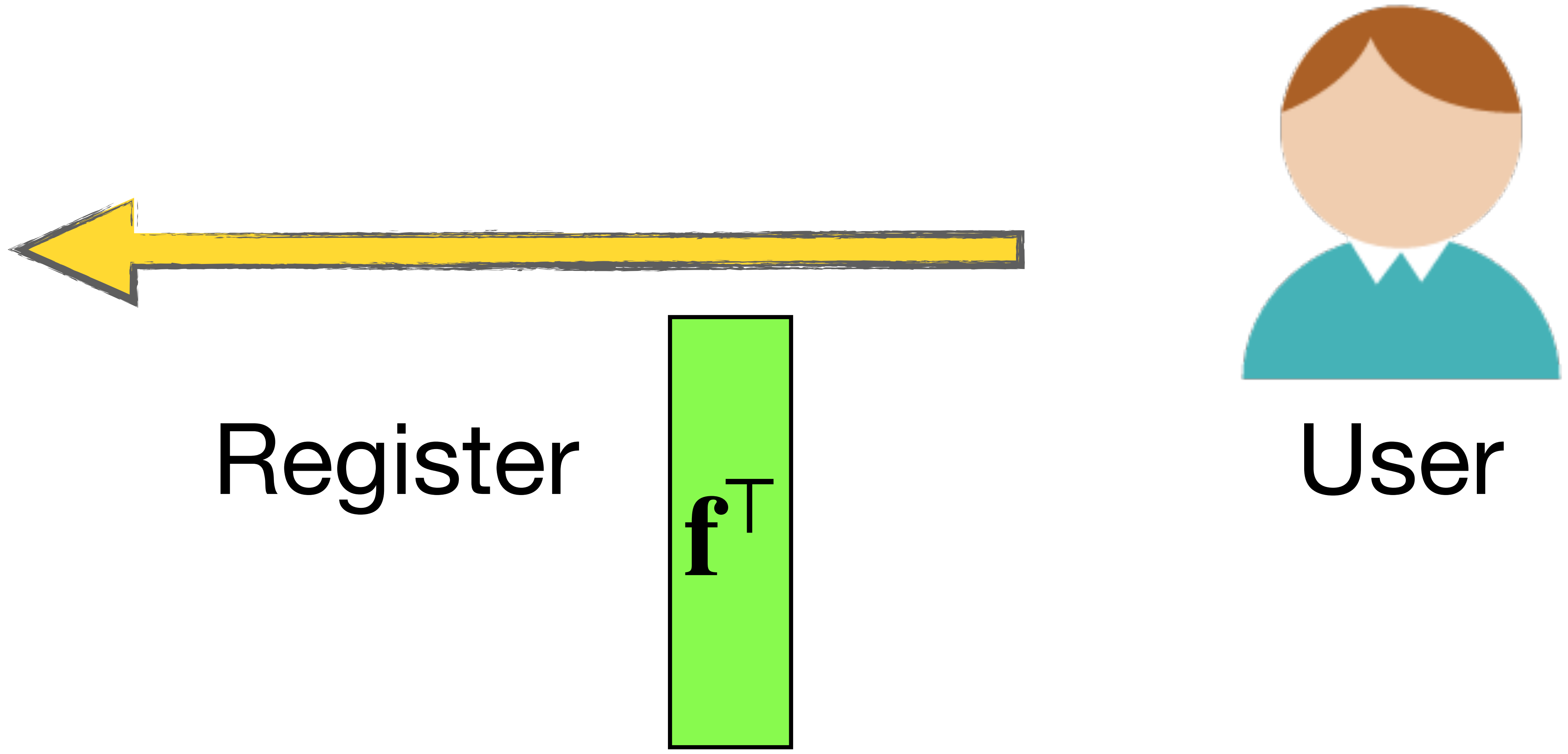
$icrs : [r_i, r_i \mathbf{w}_j \mathbf{M}]_2, \quad i \neq j$



Setup of Reg-QFE

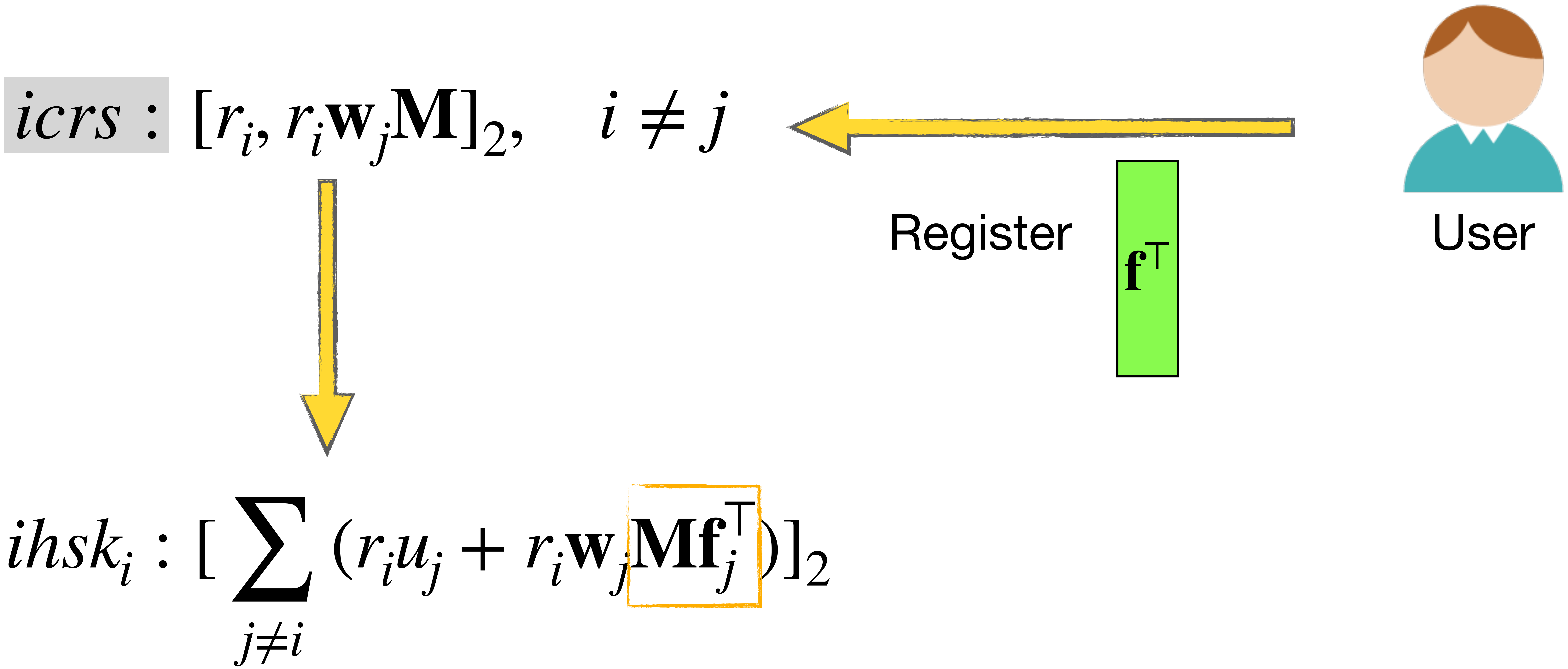
sReg-IPFE to sReg-QFE: Solution-2

$$icrs : [r_i, r_i\mathbf{w}_j\mathbf{M}]_2, \quad i \neq j$$



Register of Reg-QFE

sReg-IPFE to sReg-QFE: Solution-2



$icrs : [r_i, r_i\mathbf{w}_j\mathbf{M}]_2, \quad i \neq j$

Register

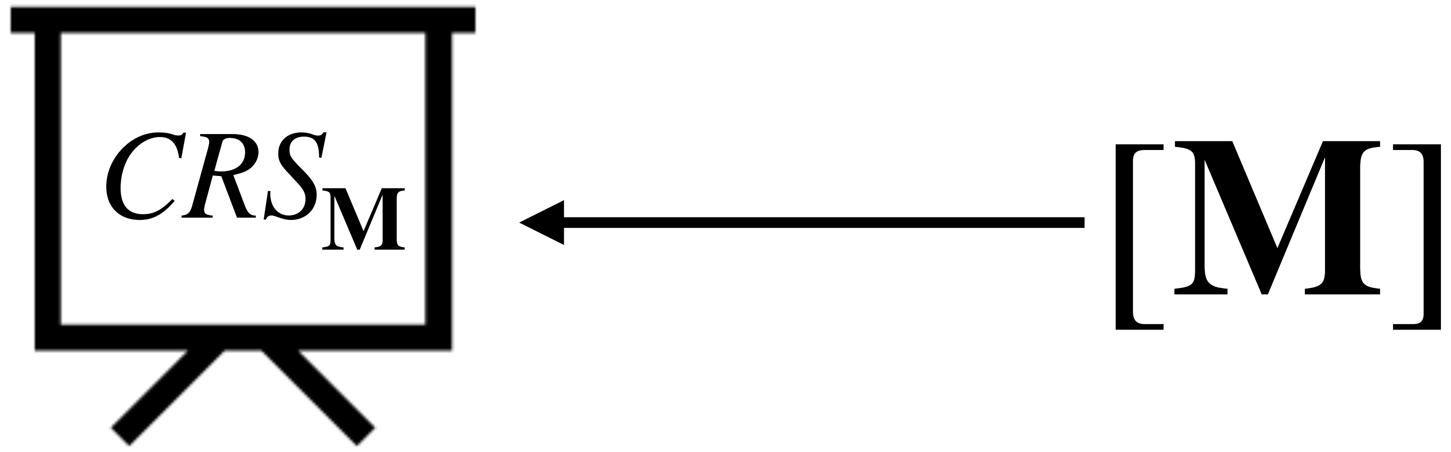
$\mathbf{f}^\top$

User

$$ihsk_i : [\sum_{j\neq i}(r_i u_j + r_i\mathbf{w}_j\boxed{\mathbf{M}\mathbf{f}_j^\top})]_2$$

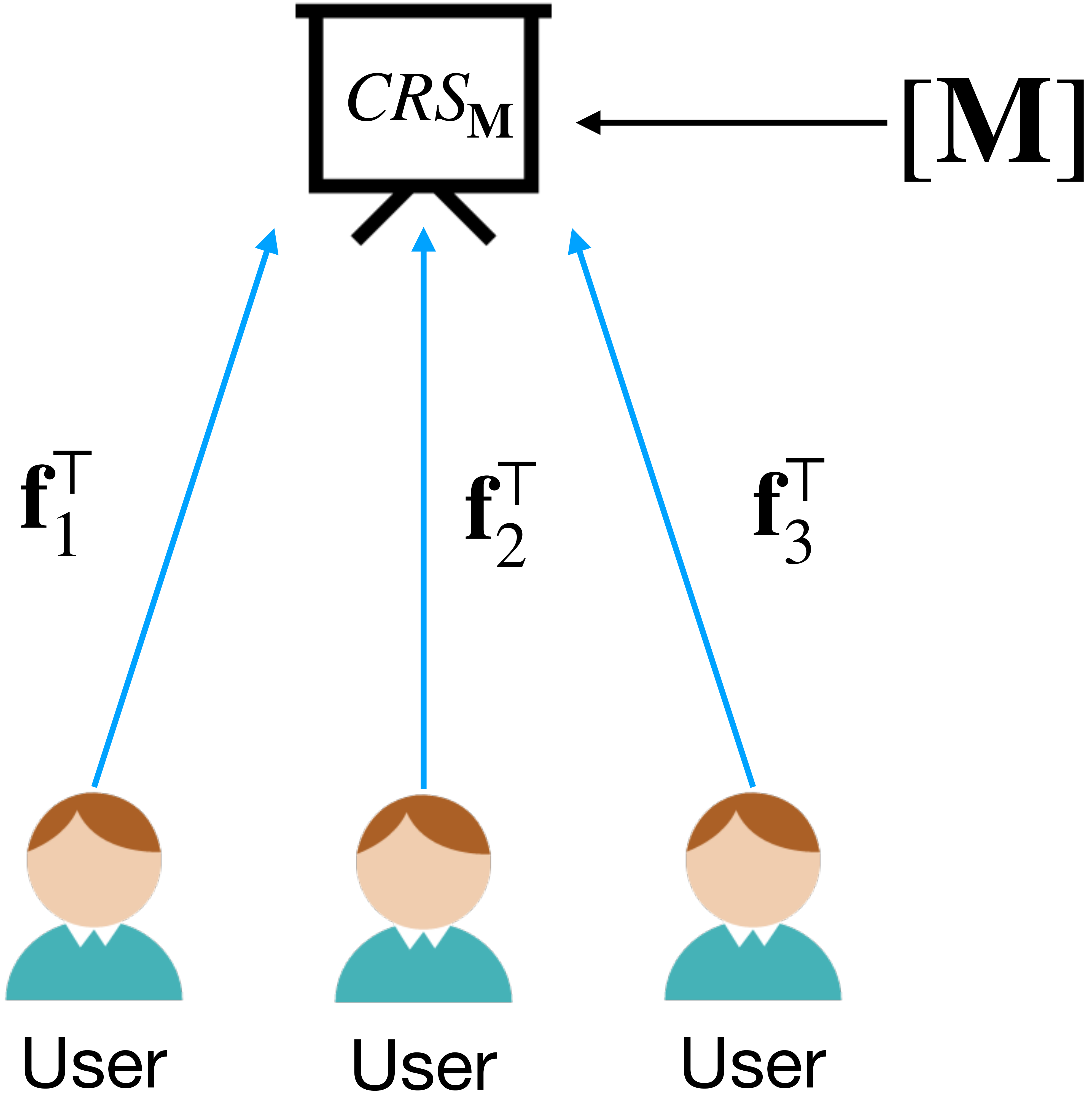
sReg-IPFE to sReg-QFE: Solution-2

New notion: Pre-constrained Reg-IPFE



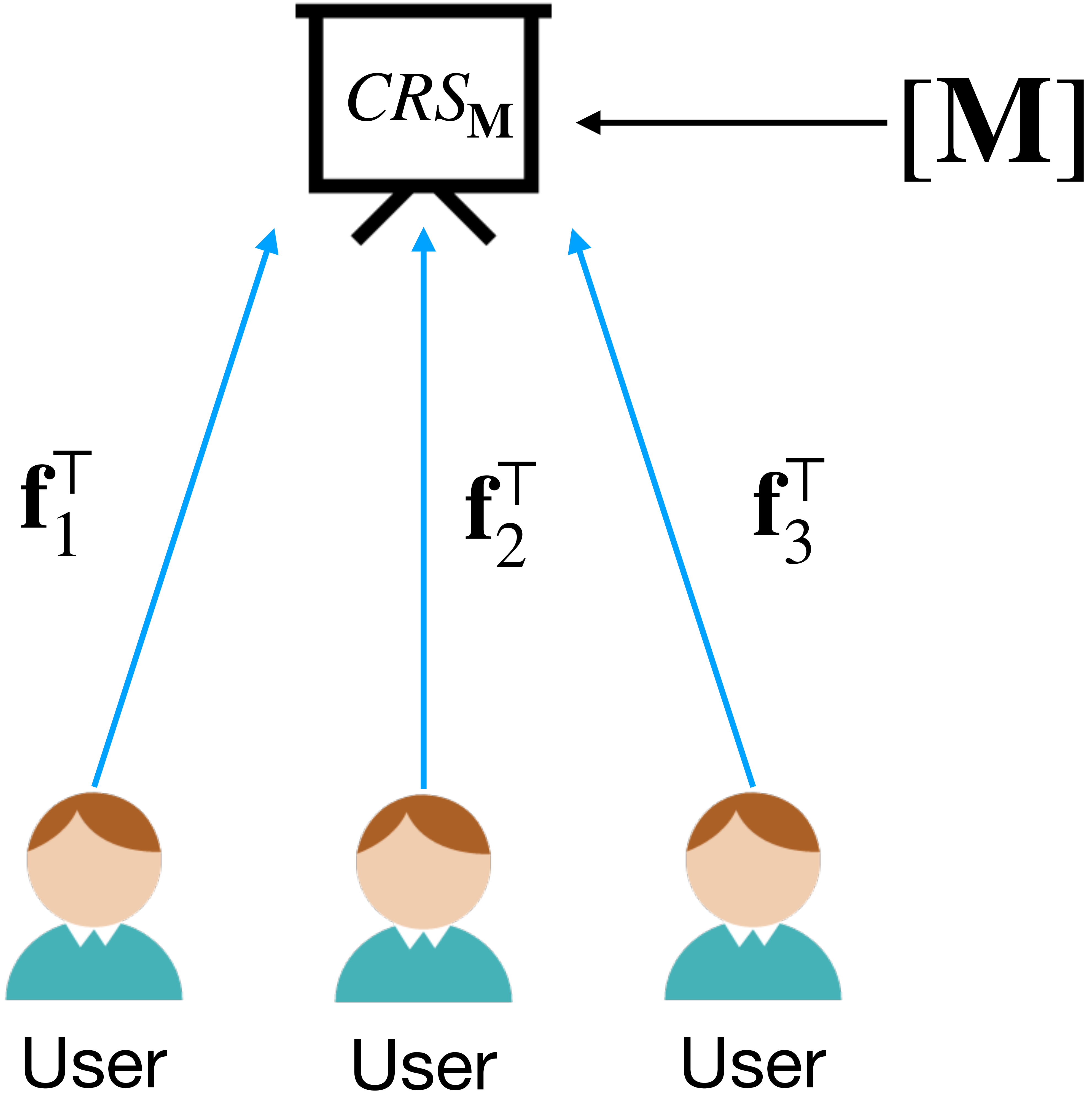
sReg-IPFE to sReg-QFE: Solution-2

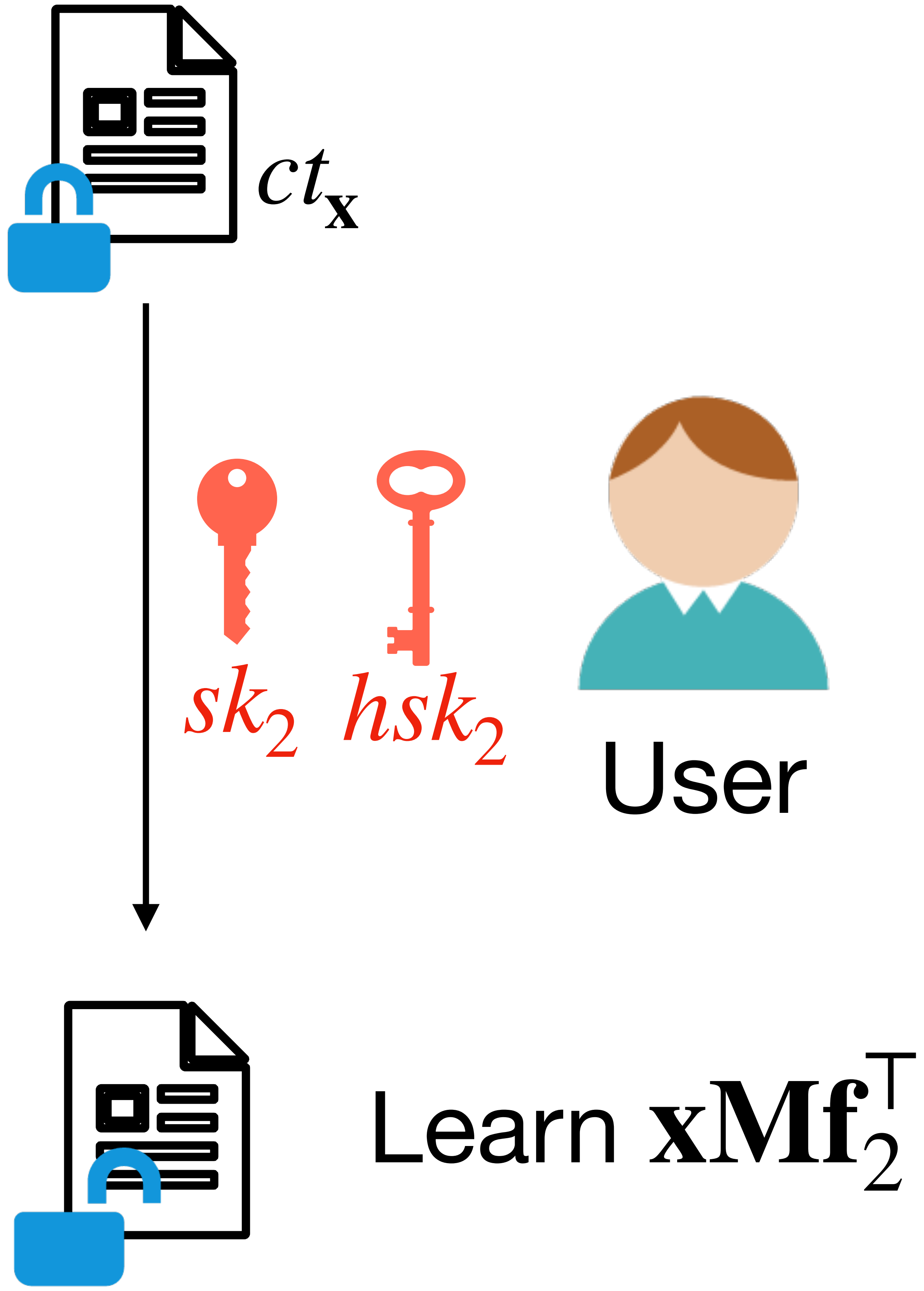
New notion: Pre-constrained Reg-IPFE



sReg-IPFE to sReg-QFE: Solution-2

New notion: Pre-constrained Reg-IPFE

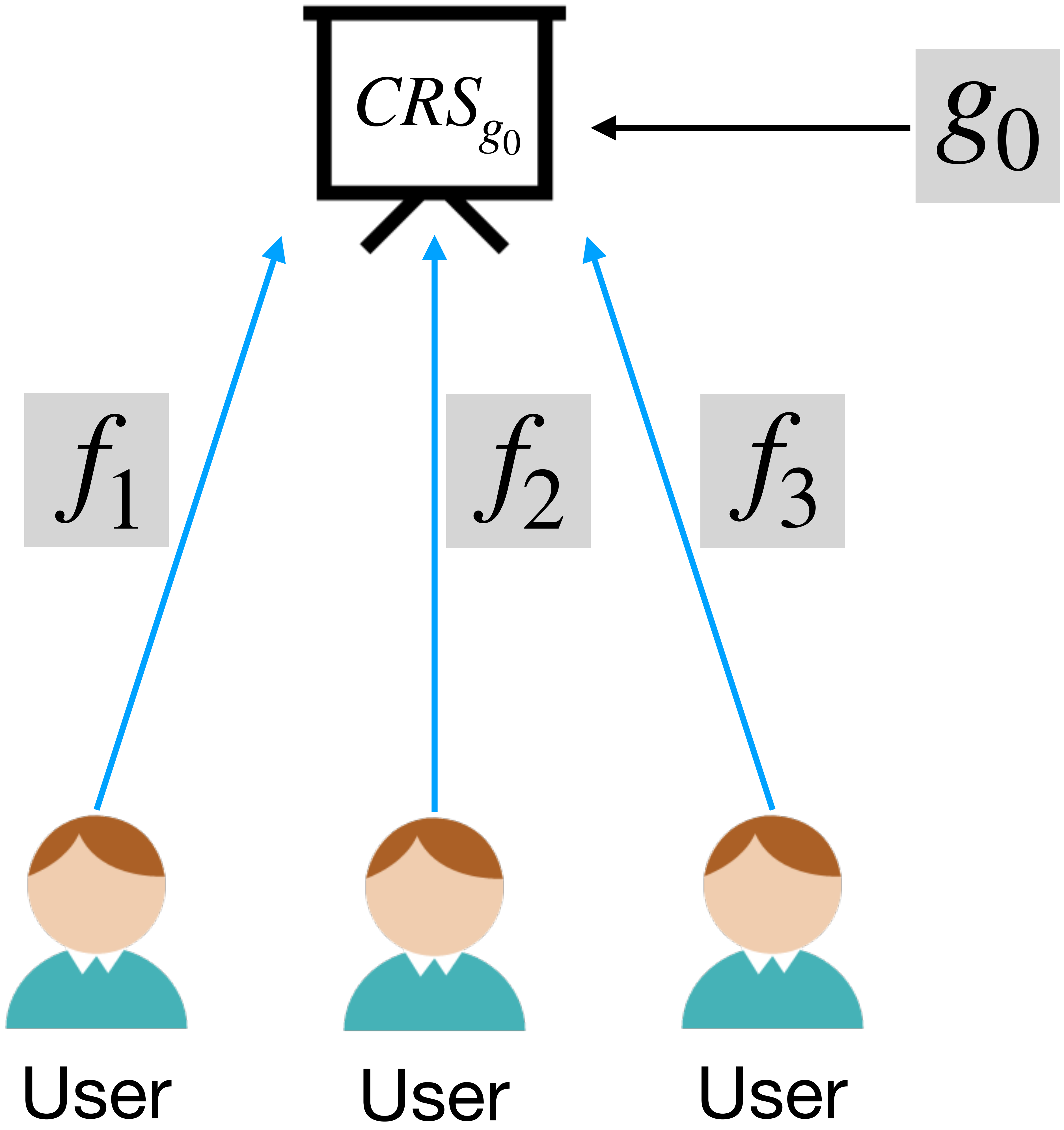


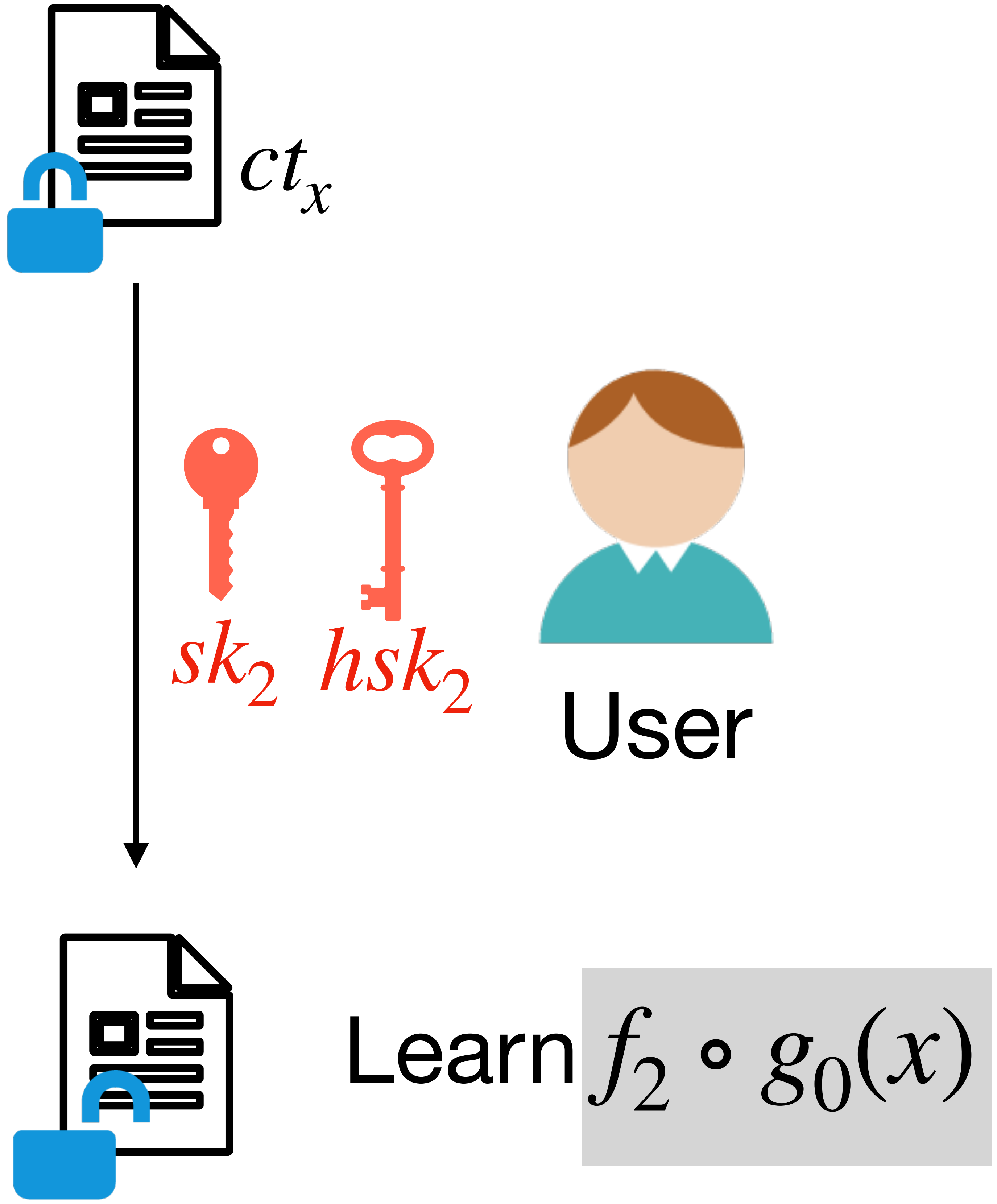


sReg-IPFE to sReg-QFE: Solution-2

New notion (more general): PReg-FE

$$\boxed{\begin{array}{l} G : X \to Y \\ F : Y \to Z \end{array}}$$





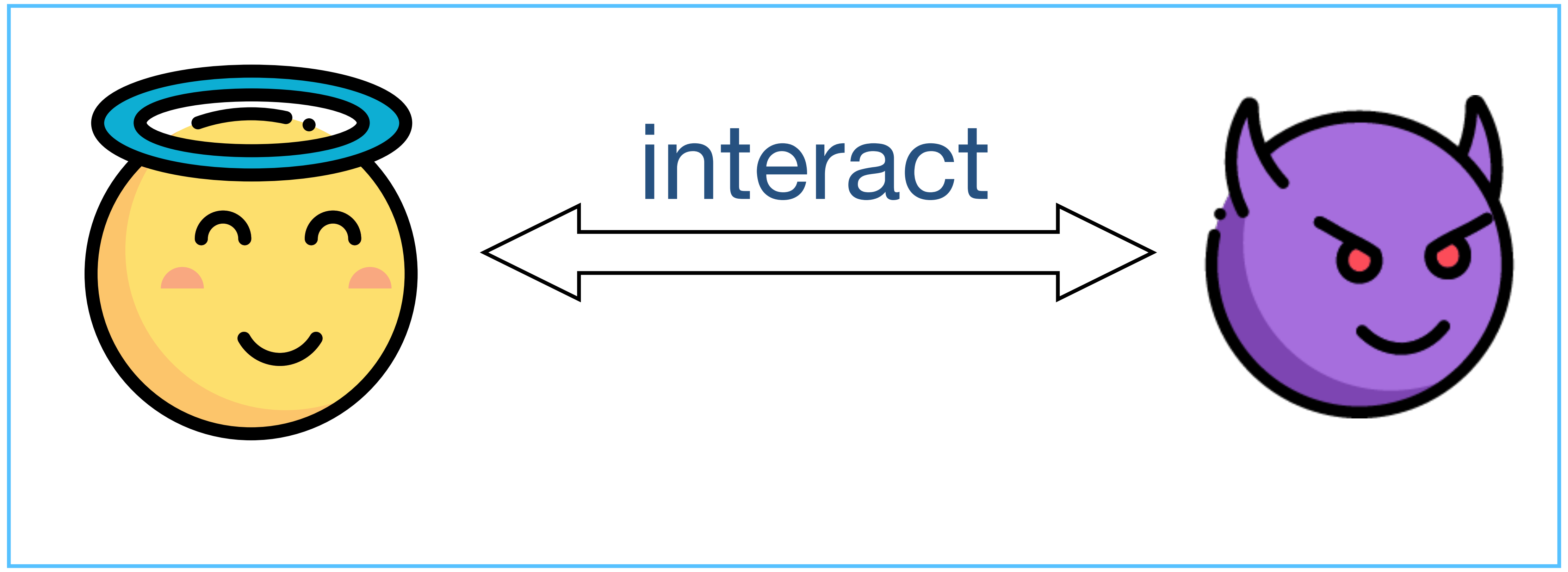
sReg-IPFE to sReg-QFE: Challenge-3

[Wee20]: use sel-SIM-security IPFE

sReg-IPFE to sReg-QFE: Challenge-3

[Wee20]: use sel-SIM-security IPFE

Real



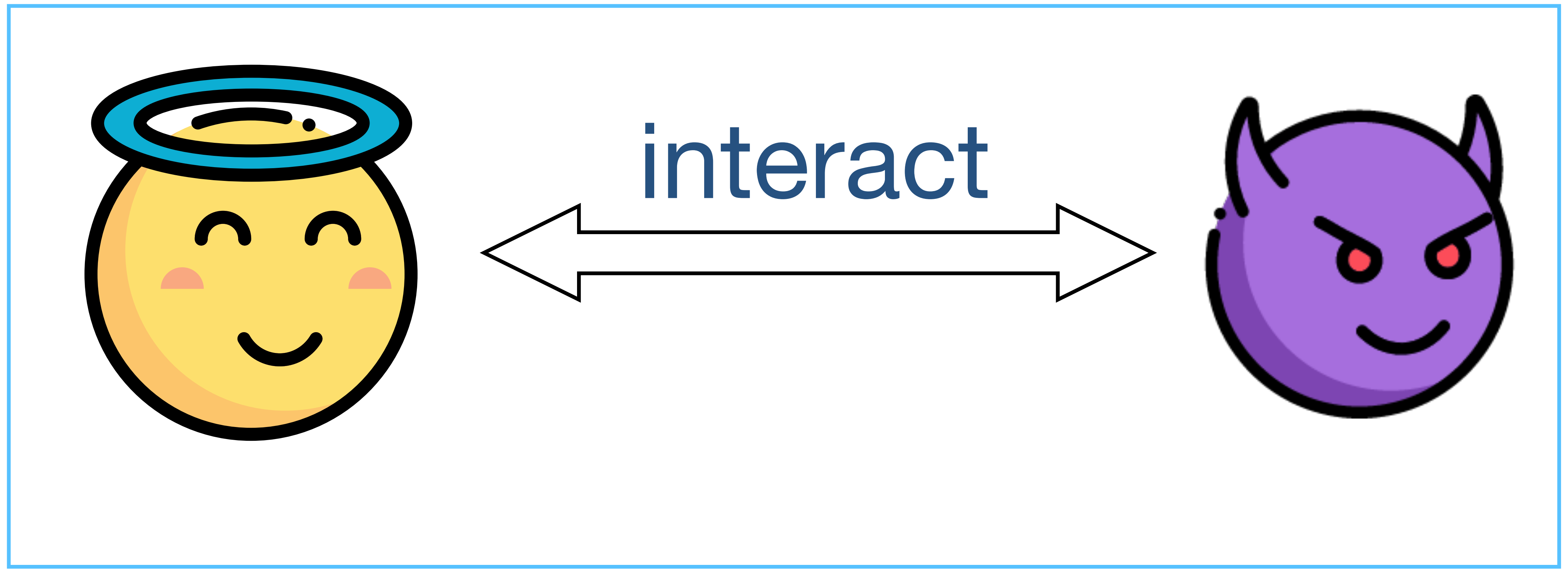
Corrupted $\mathbf{f}$: $sk \leftarrow \boxed{[\mathbf{M}\mathbf{f}^{\top}]_2}$

$ct \leftarrow \boxed{\mathbf{x}}$

sReg-IPFE to sReg-QFE: Challenge-3

[Wee20]: use sel-SIM-security IPFE

Simulator



Corrupted $\mathbf{f}$: $\widetilde{sk} \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}^\top]_2}$

$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

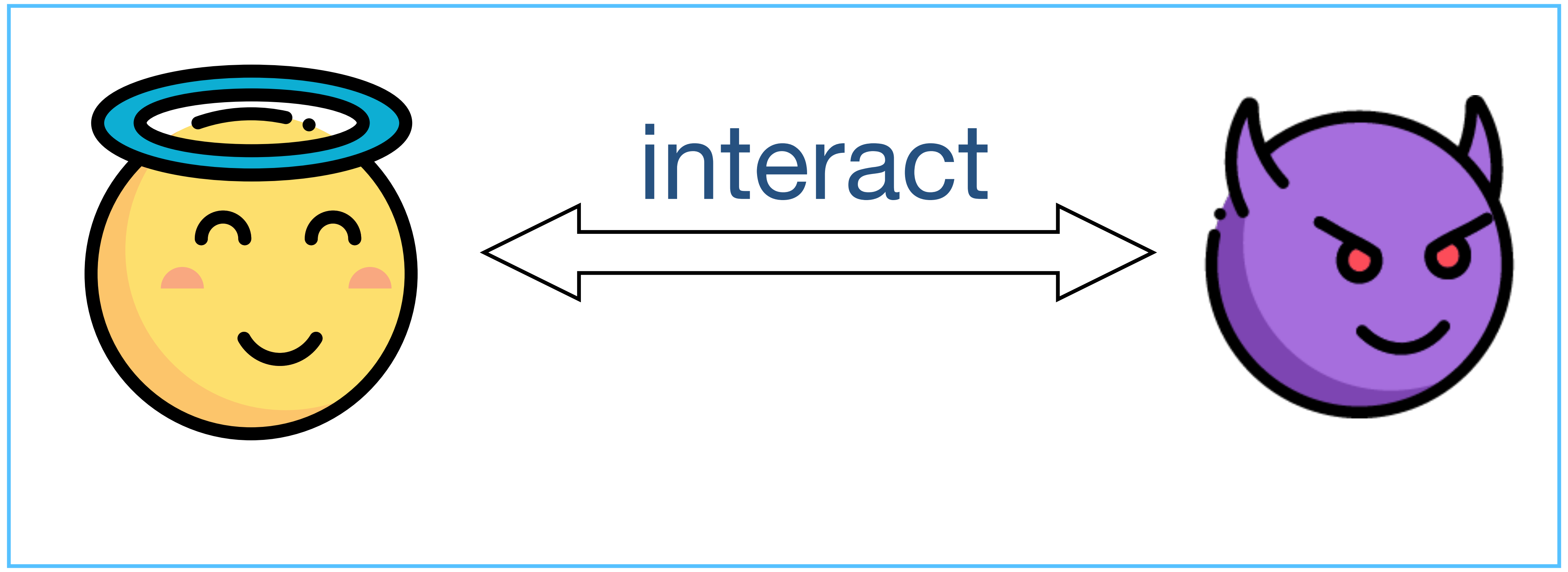
sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Real



$$crs \leftarrow \boxed{[\mathbf{M}]}$$

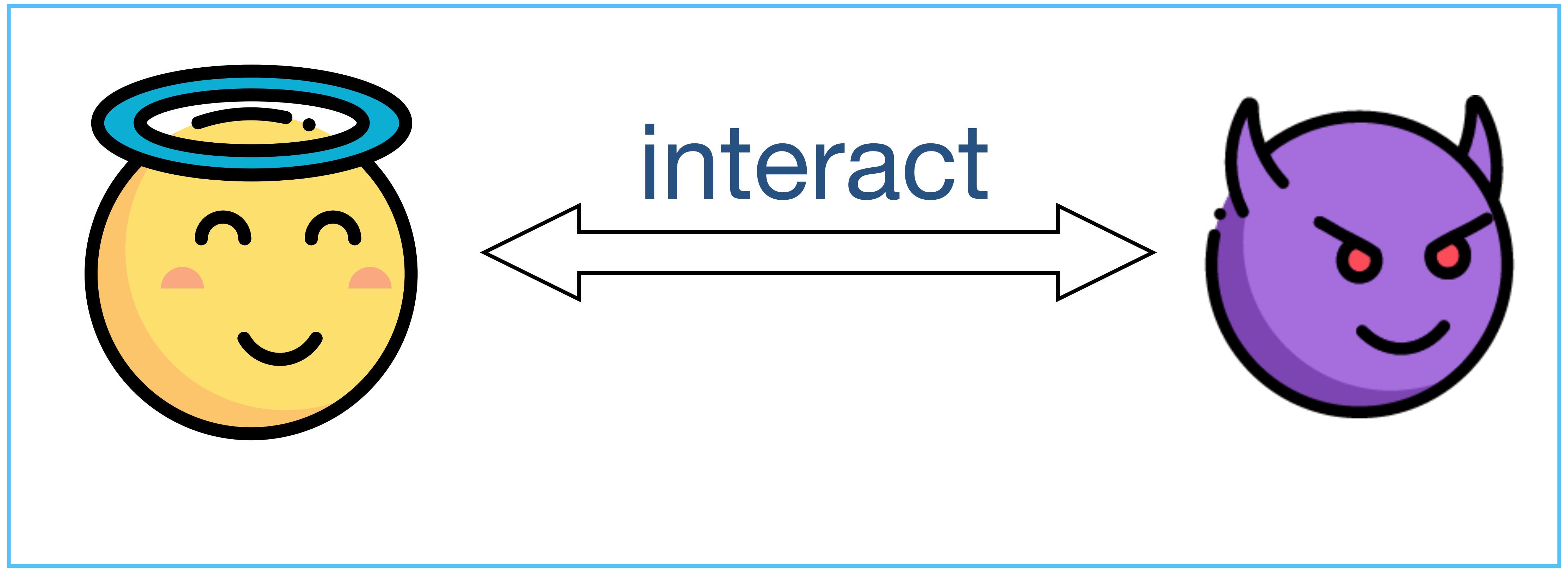
Corrupted & malicious $\mathbf{f}_i$: $$hsk_i \leftarrow \boxed{[\mathbf{M}\mathbf{f}_i^\top]_2}$$

$$ct \leftarrow \boxed{\mathbf{x}}$$

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



$$\widetilde{crs} \leftarrow \boxed{[\mathbf{M}]}$$

Corrupted & malicious $\mathbf{f}_i$: $hsk_i \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

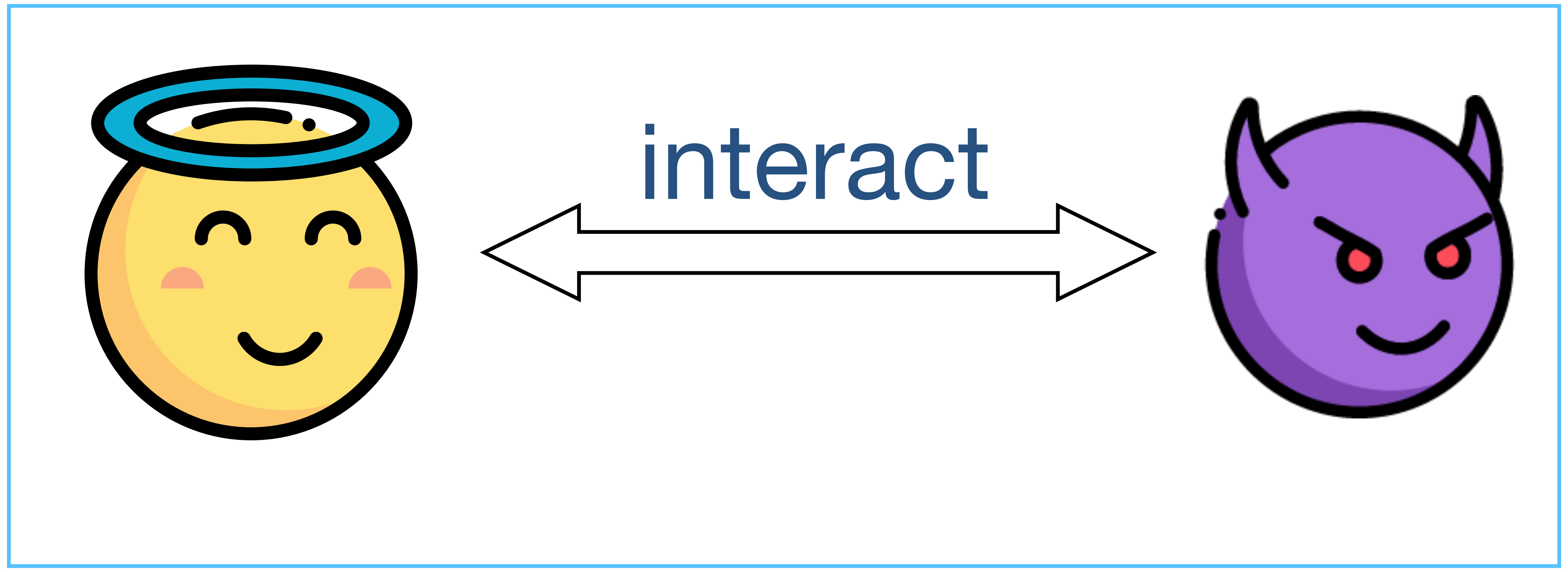
$$\widetilde{ct} \leftarrow \cancel{\boxed{}}$$

Idea from plain IPFE

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



$\widetilde{crs} \leftarrow \boxed{[\mathbf{M}]}$

Corrupted & malicious $\mathbf{f}_i$: $hsk_i \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

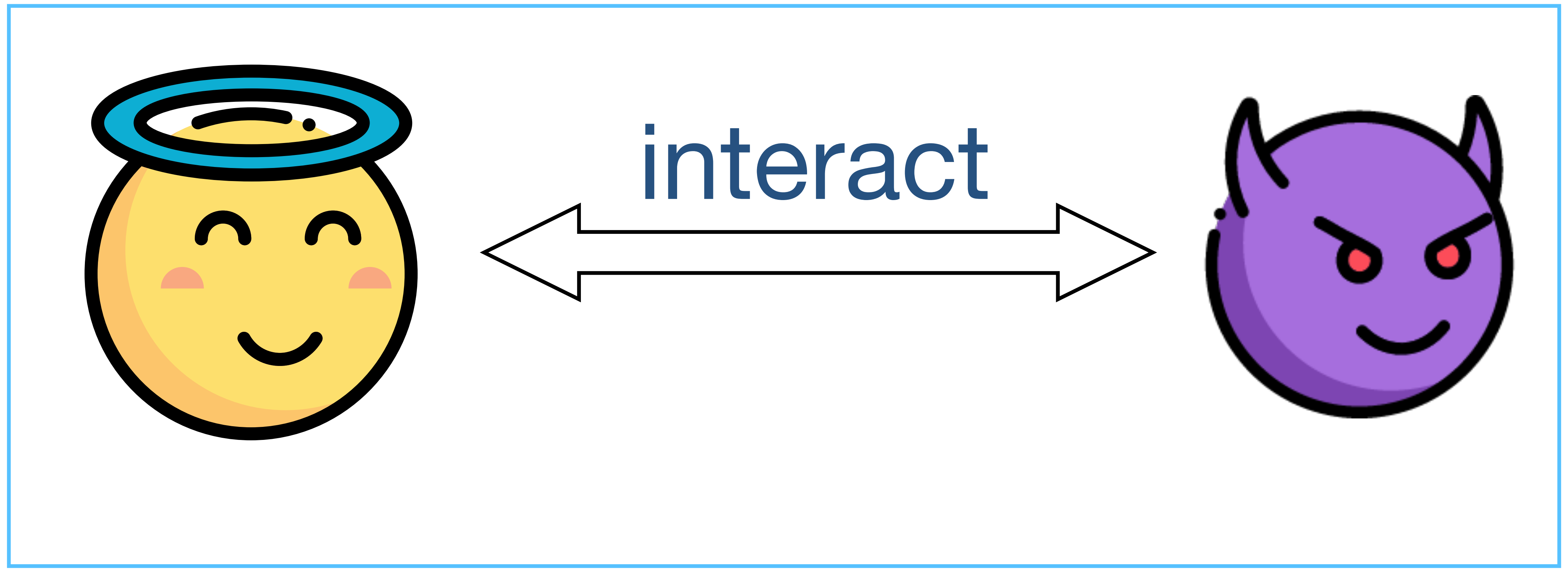
hsk are deterministic!

No chance to embed!

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow \boxed{[\mathbf{xMf}_i^\top]_2}$

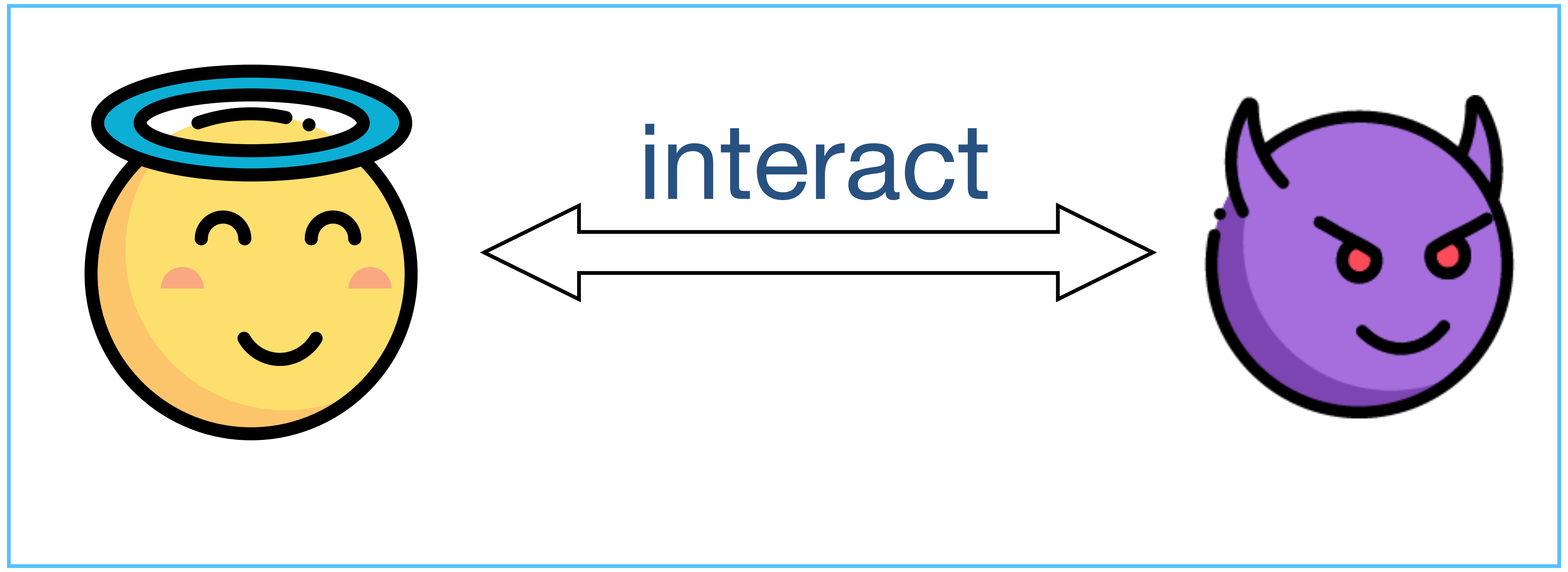
$hsk_i \leftarrow \boxed{[\mathbf{xMf}_i^\top]_2}$

$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

$hsk_i \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

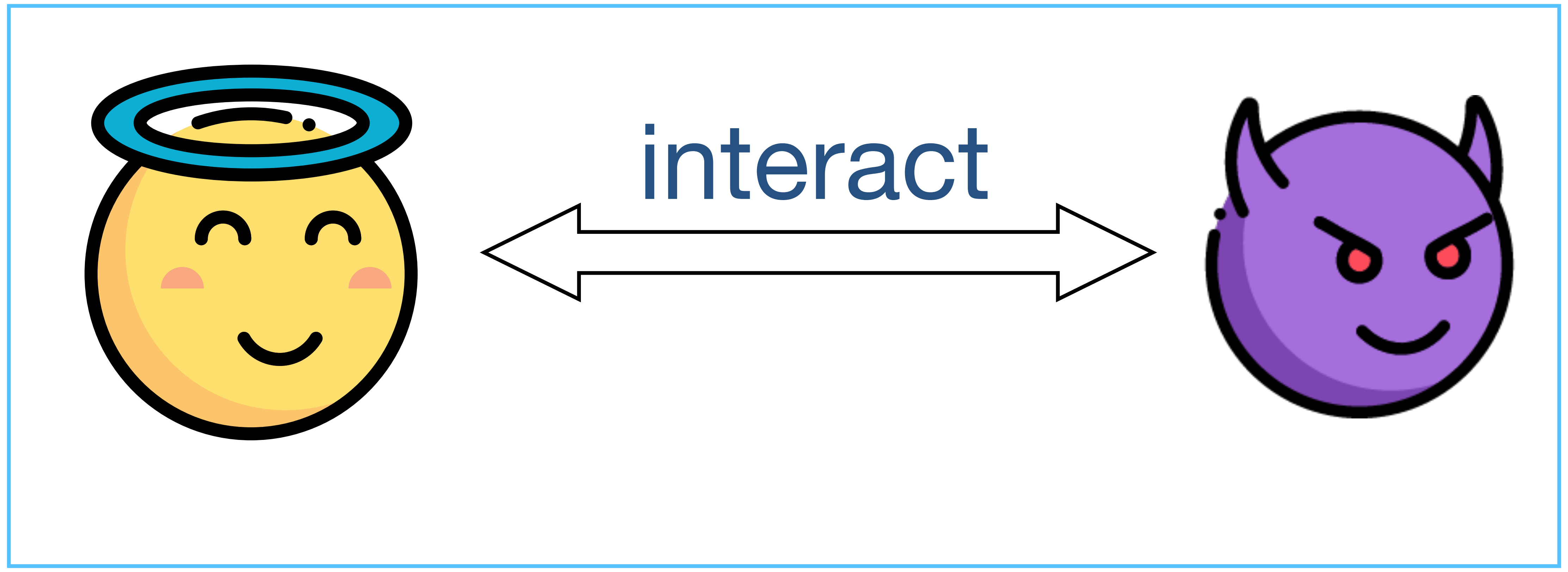
Claim at beginning:

- challenge $\mathbf{x}$
- corrupted & malicious set $\mathscr{C}, \mathscr{M}$
- functions $\mathbf{f}_i$

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow [\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2$

$hsk_i \leftarrow [\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2$

$\widetilde{ct} \leftarrow \cancel{\square}$

Claim at beginning:

challenge $\mathbf{x}$ Requirement of “selective”

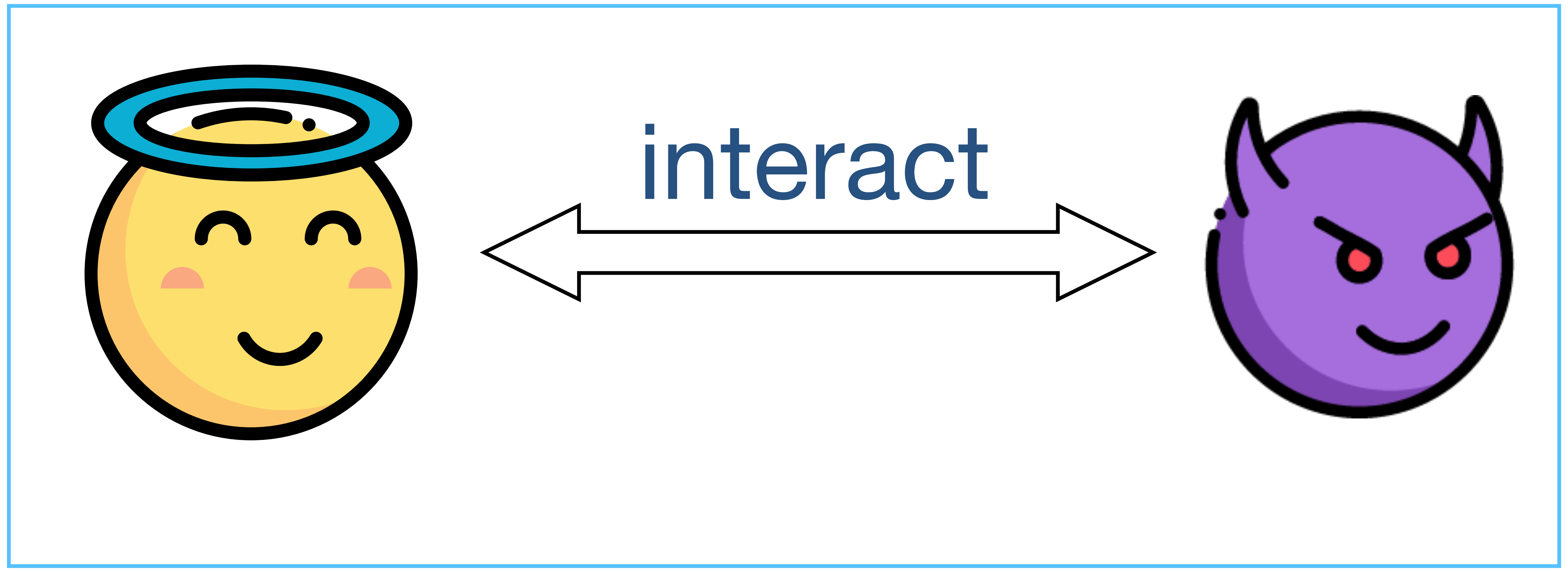
corrupted & malicious set $\mathscr{C}, \mathscr{M}$

functions $\mathbf{f}_i$

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow [\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2$

$hsk_i \leftarrow [\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2$

$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

Claim at beginning:

challenge $\mathbf{x}$

corrupted & malicious set $\mathscr{C}, \mathscr{M}$

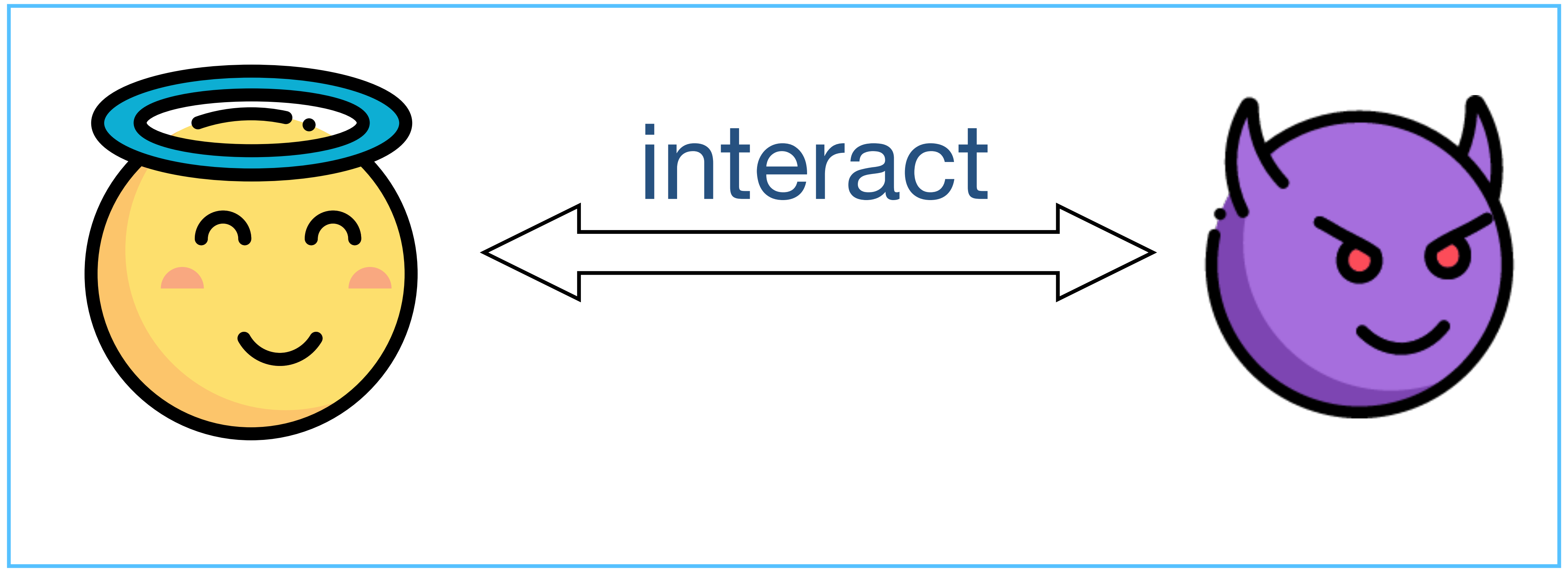
functions $\mathbf{f}_i$

Similar to “very selective” in [AMY19]

sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow [\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2$

$hsk_i \leftarrow [\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2$

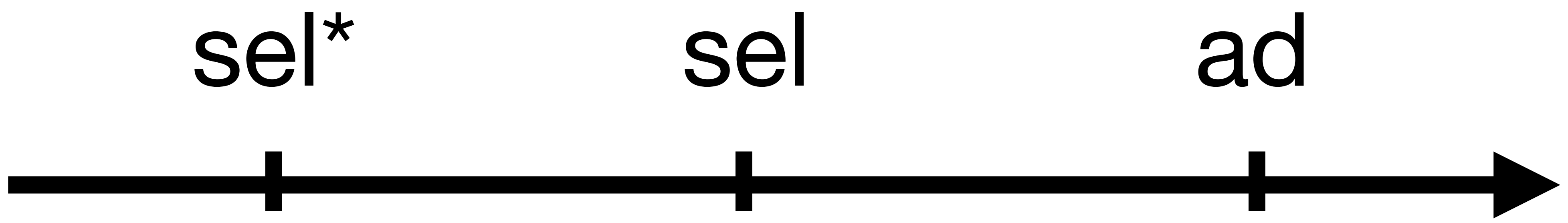
$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

Claim at beginning:

challenge $\mathbf{x}$

corrupted & malicious set $\mathscr{C}, \mathscr{M}$

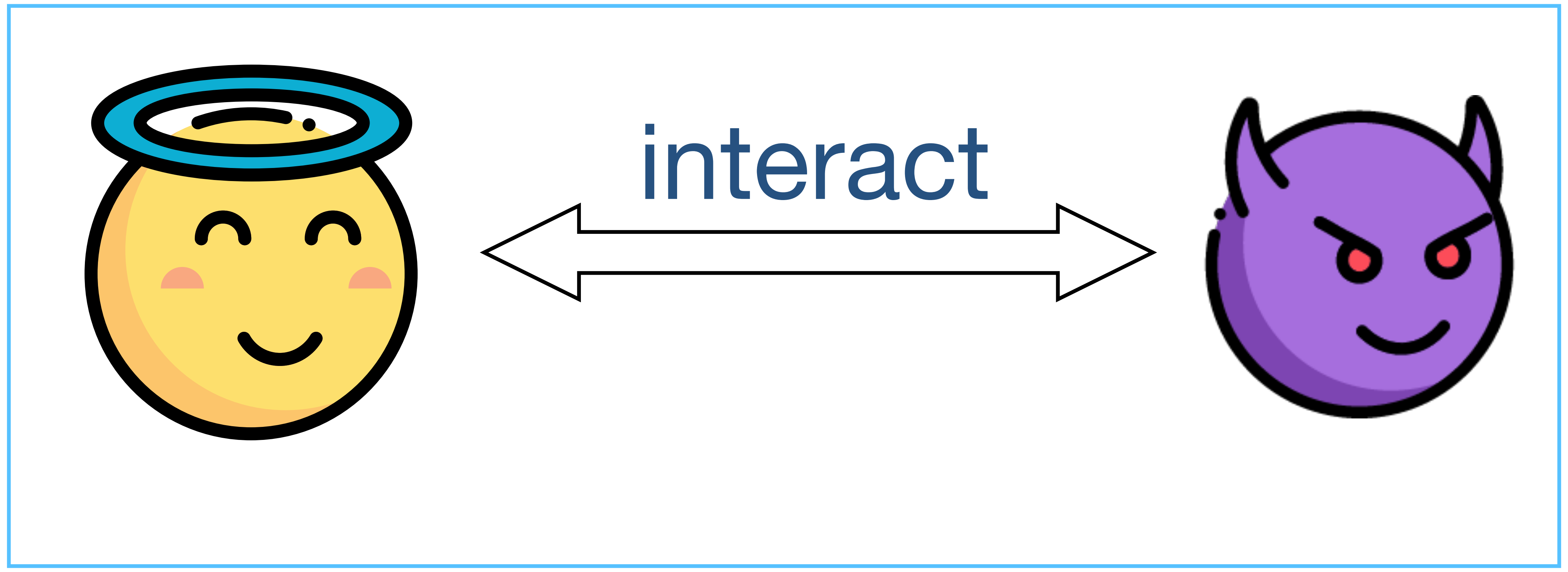
functions $\mathbf{f}_i$



sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

$hsk_i \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

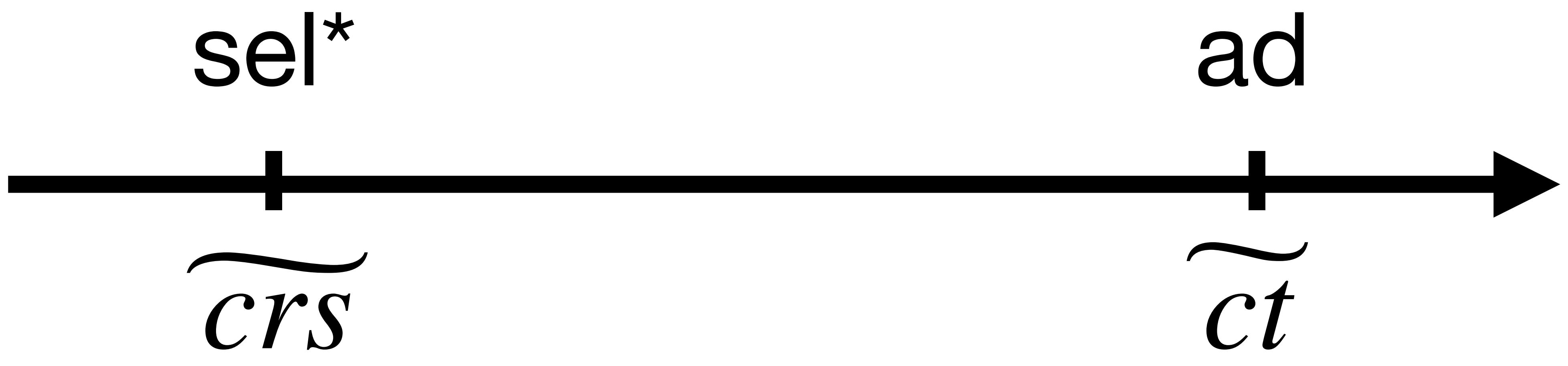
$\widetilde{ct} \leftarrow \cancel{\square}$

Claim at beginning:

challenge $\mathbf{x}$

corrupted & malicious set $\mathscr{C}, \mathscr{M}$

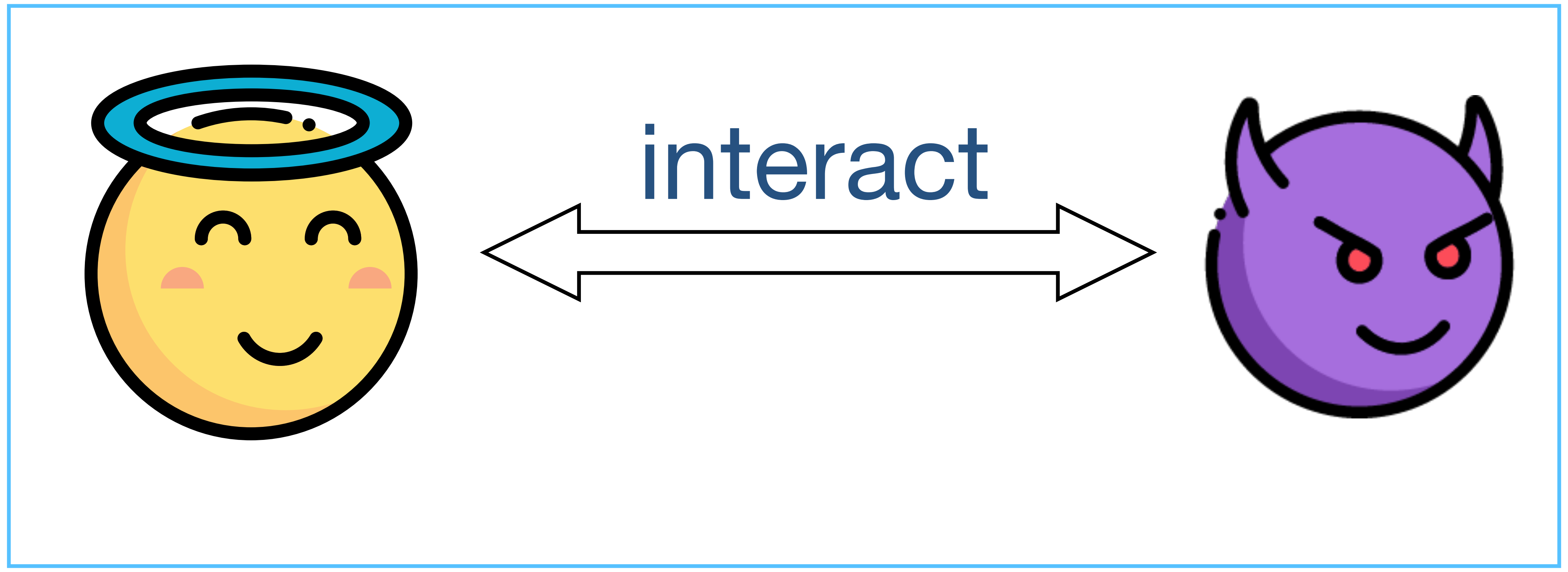
functions $\mathbf{f}_i$



sReg-IPFE to sReg-QFE: Challenge-3

First time consider SIM-security in registration

Simulator



Corrupted & malicious $\mathbf{f}_i$:

$\widetilde{crs} \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

$hsk_i \leftarrow \boxed{[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_2}$

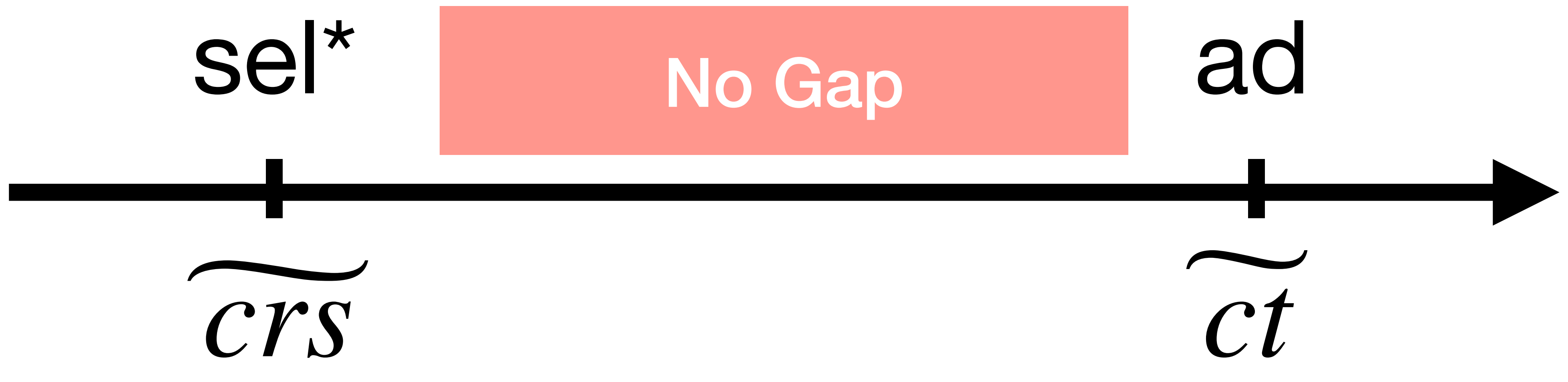
$\widetilde{ct} \leftarrow \cancel{\boxed{}}$

Claim at beginning:

challenge $\mathbf{x}$

corrupted & malicious set $\mathscr{C}, \mathscr{M}$

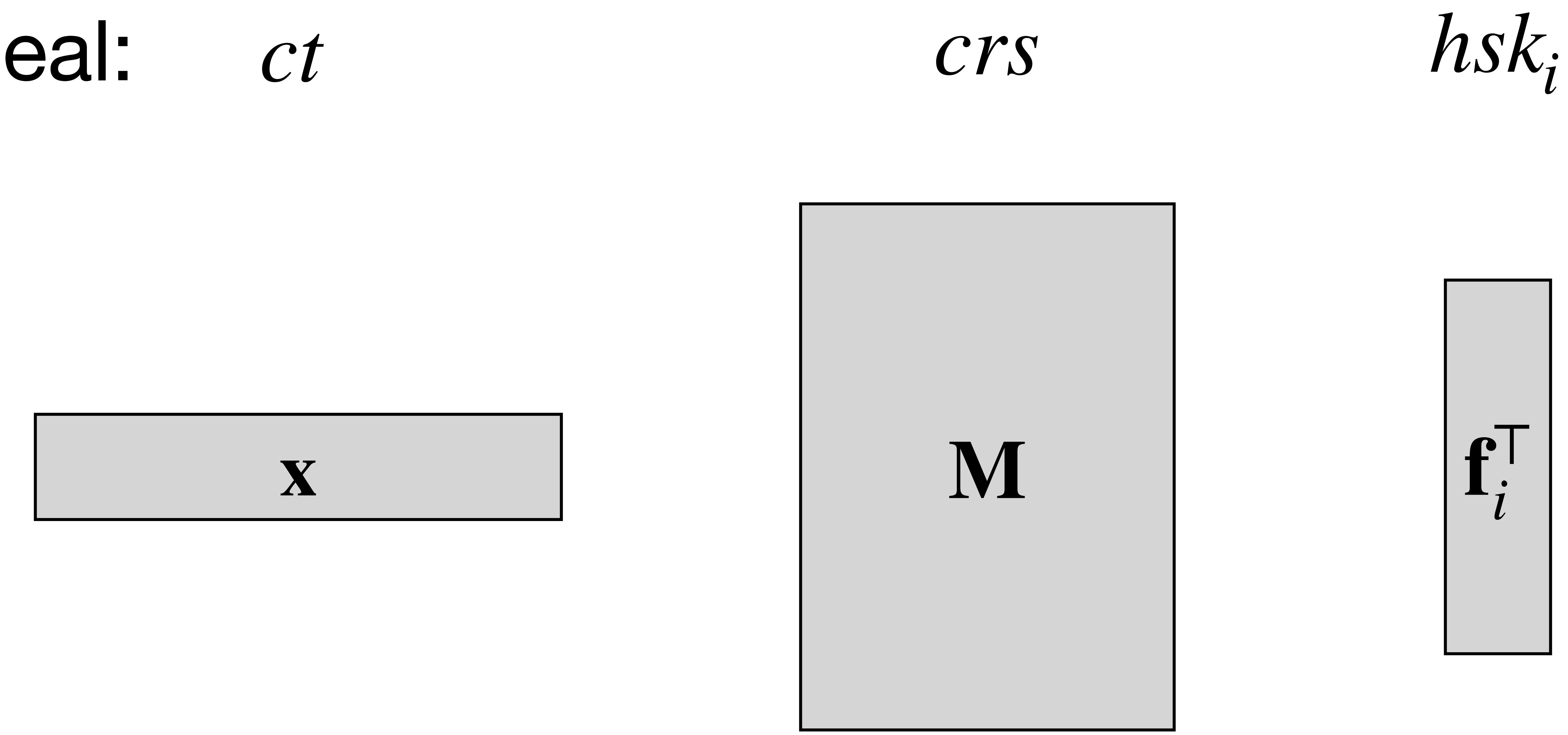
functions $\mathbf{f}_i$



sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE

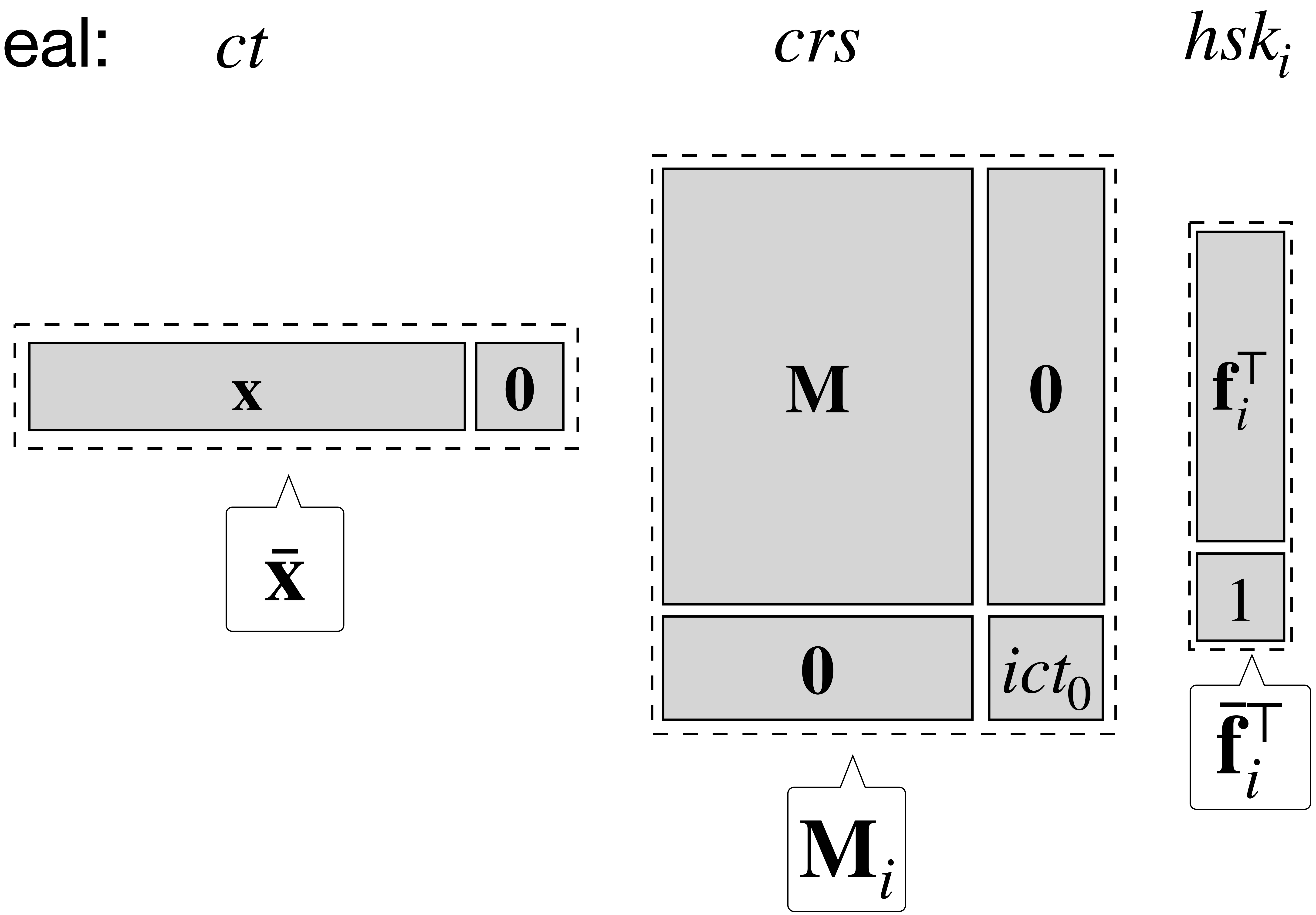
Real:



sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE

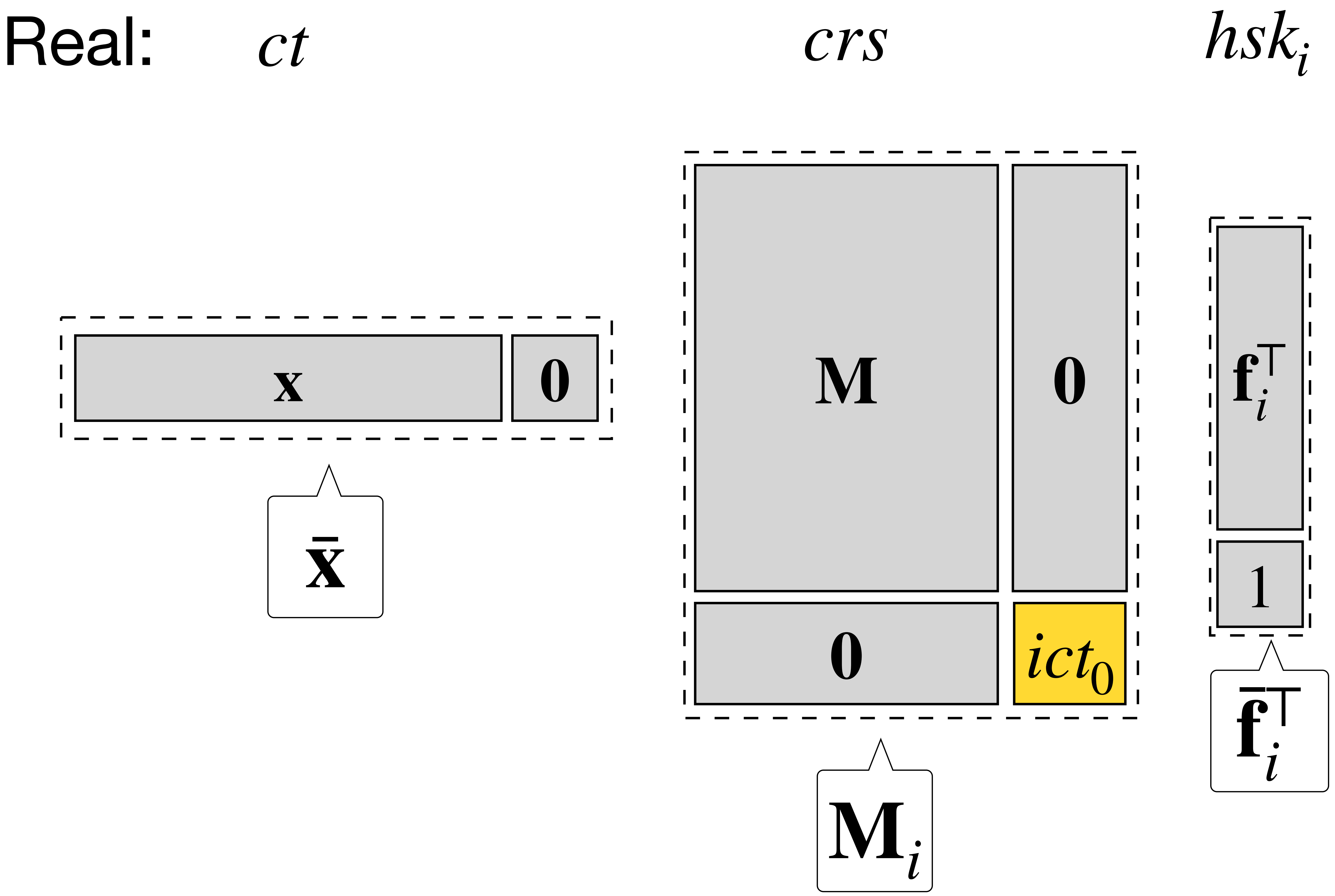
Real:



sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE

Real:



With PKE:

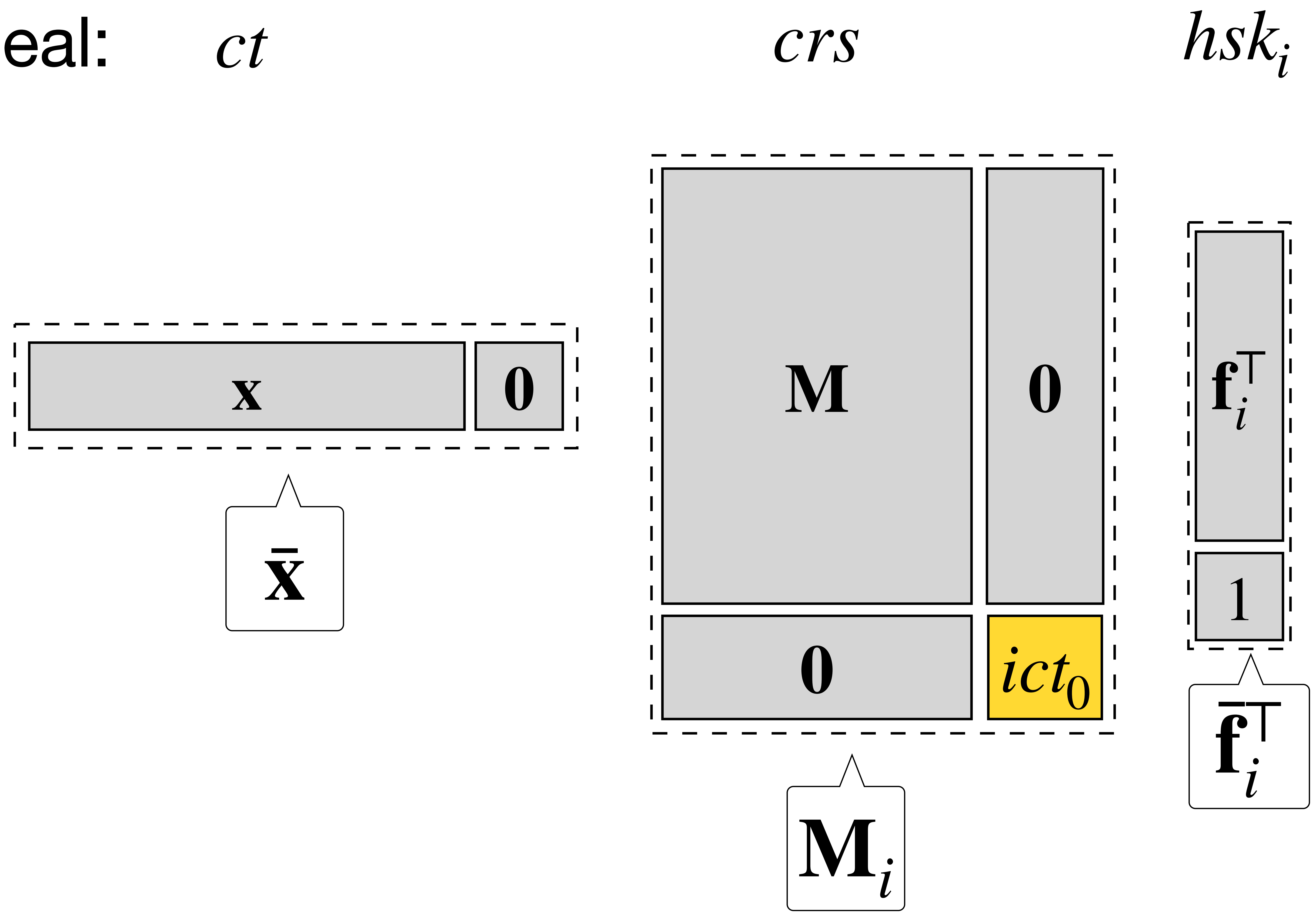
$(ipk, isk) \leftarrow iGen(1^\lambda)$

$ict_0 \leftarrow iEnc(0)$

sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE

Real:



With PKE:

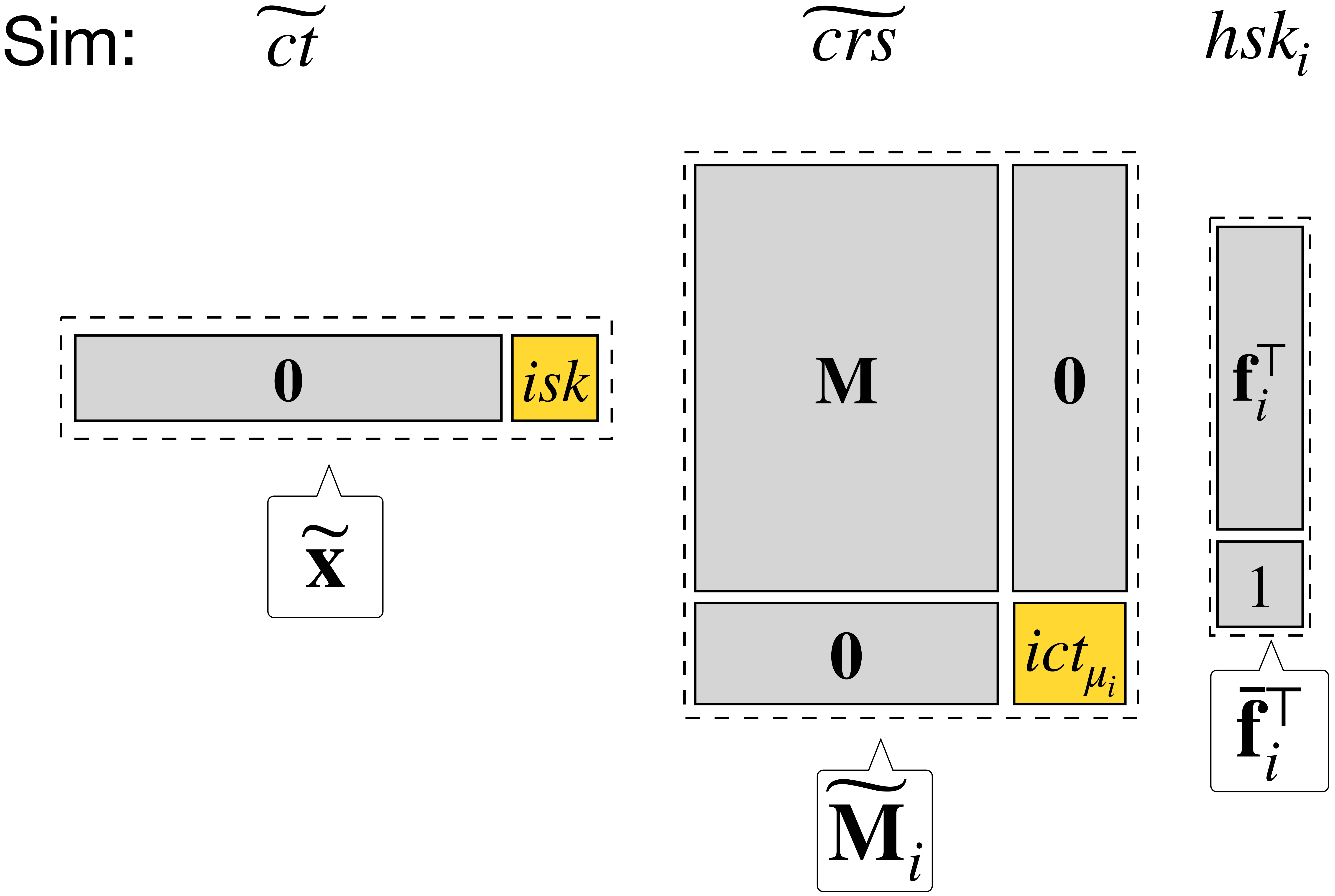
$$(ipk, isk) \leftarrow iGen(1^\lambda)$$

$$\boxed{ict_0} \leftarrow iEnc(0)$$

$$\bar{\mathbf{x}}\mathbf{M}_i\bar{\mathbf{f}}_i^\top = \mathbf{x}\mathbf{M}\mathbf{f}_i^\top$$

sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE



With PKE:

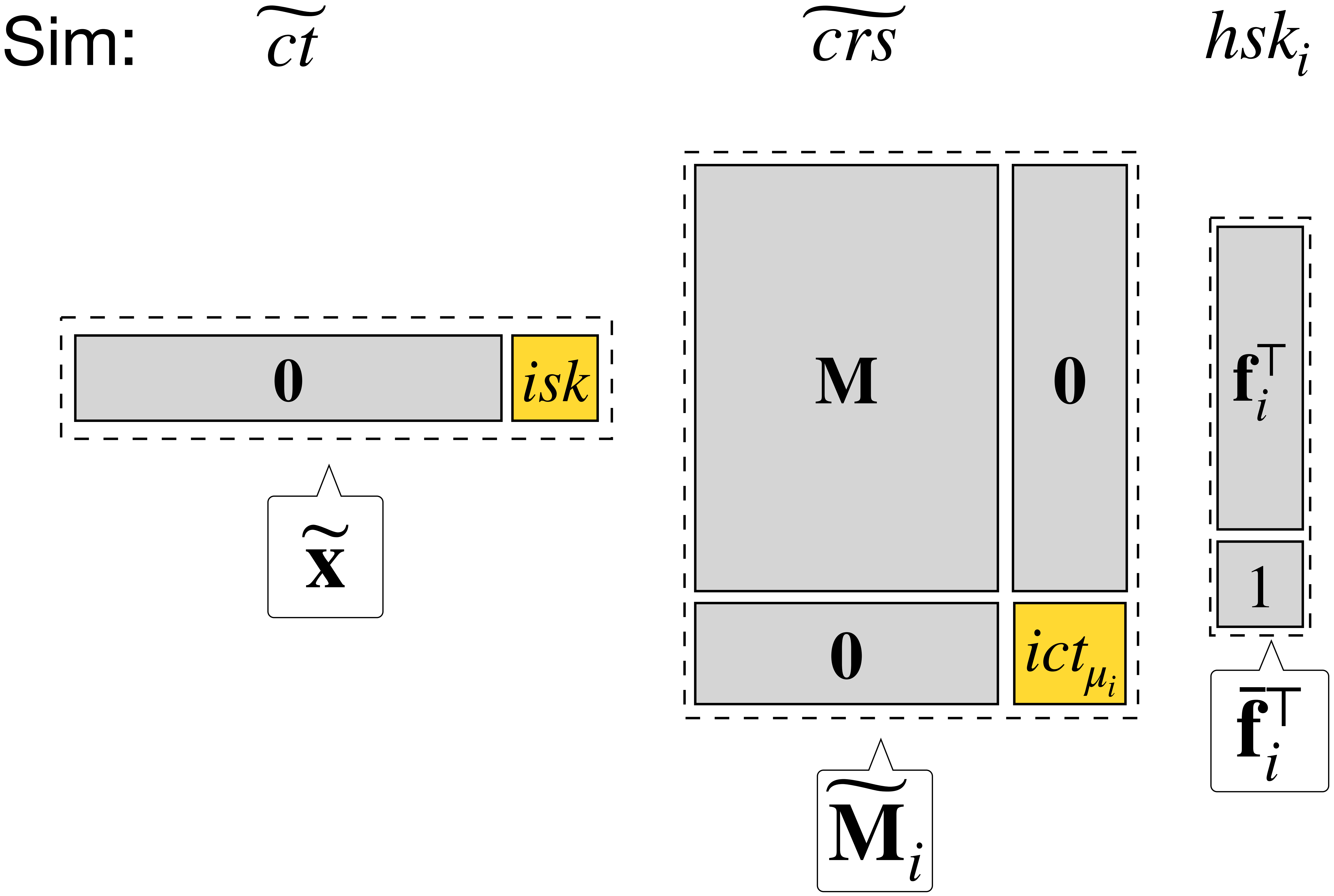
$(ipk, isk) \leftarrow iGen(1^\lambda)$

$ict_{\mu_i} \leftarrow iEnc(\mathbf{x}\mathbf{M}\mathbf{f}_i^\top)$

$i \in \mathscr{C} \cup \mathscr{M}$

sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE



With PKE:

$(ipk, isk) \leftarrow iGen(1^\lambda)$

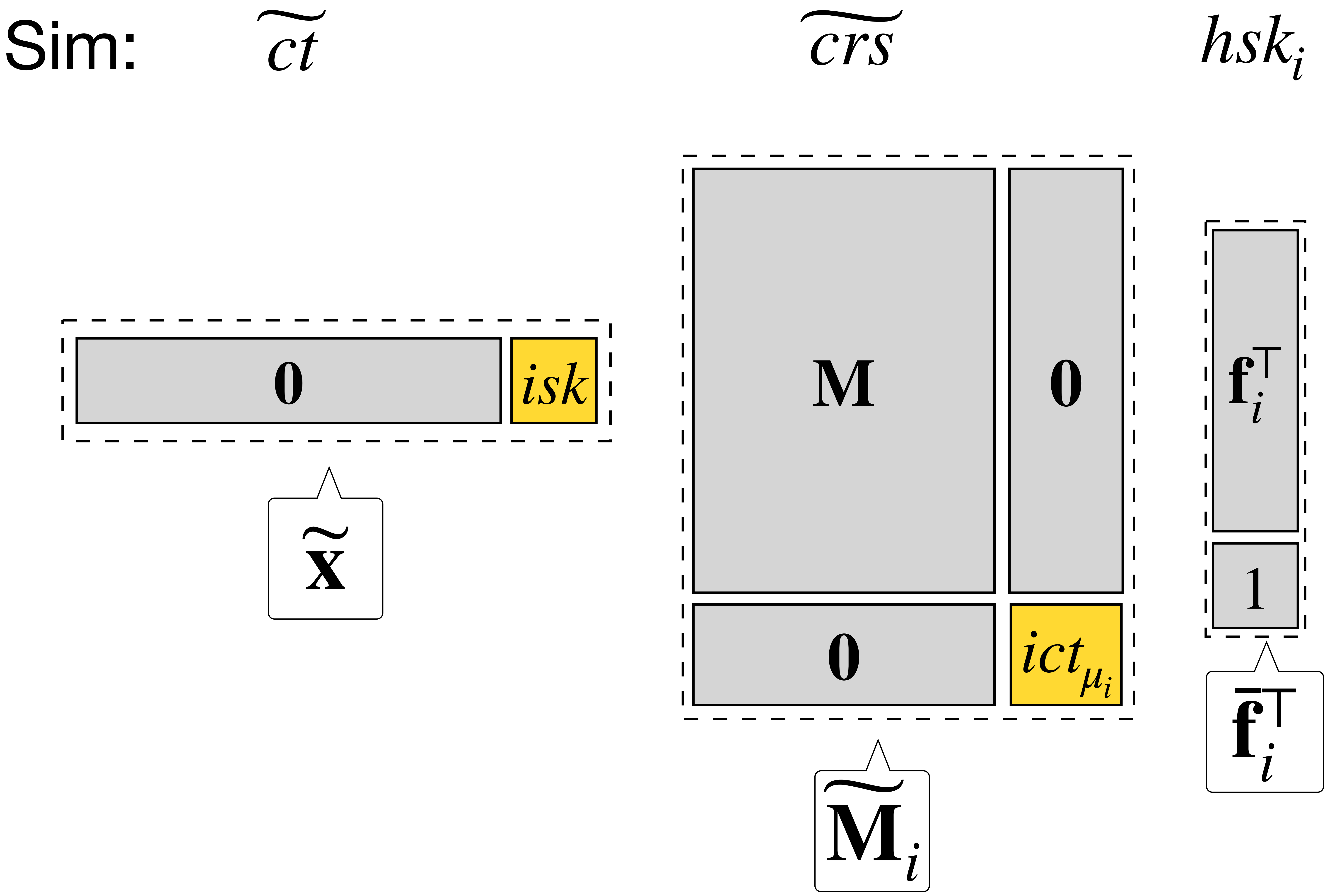
$ict_{\mu_i} \leftarrow iEnc(\mathbf{x}\mathbf{M}\mathbf{f}_i^\top)$

$i \in \mathscr{C} \cup \mathscr{M}$

$$\tilde{\mathbf{x}}\widetilde{\mathbf{M}}_i\bar{\mathbf{f}}_i^\top = < isk, ict_{\mu_i} >$$

sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE



With PKE:

$(ipk, isk) \leftarrow iGen(1^\lambda)$

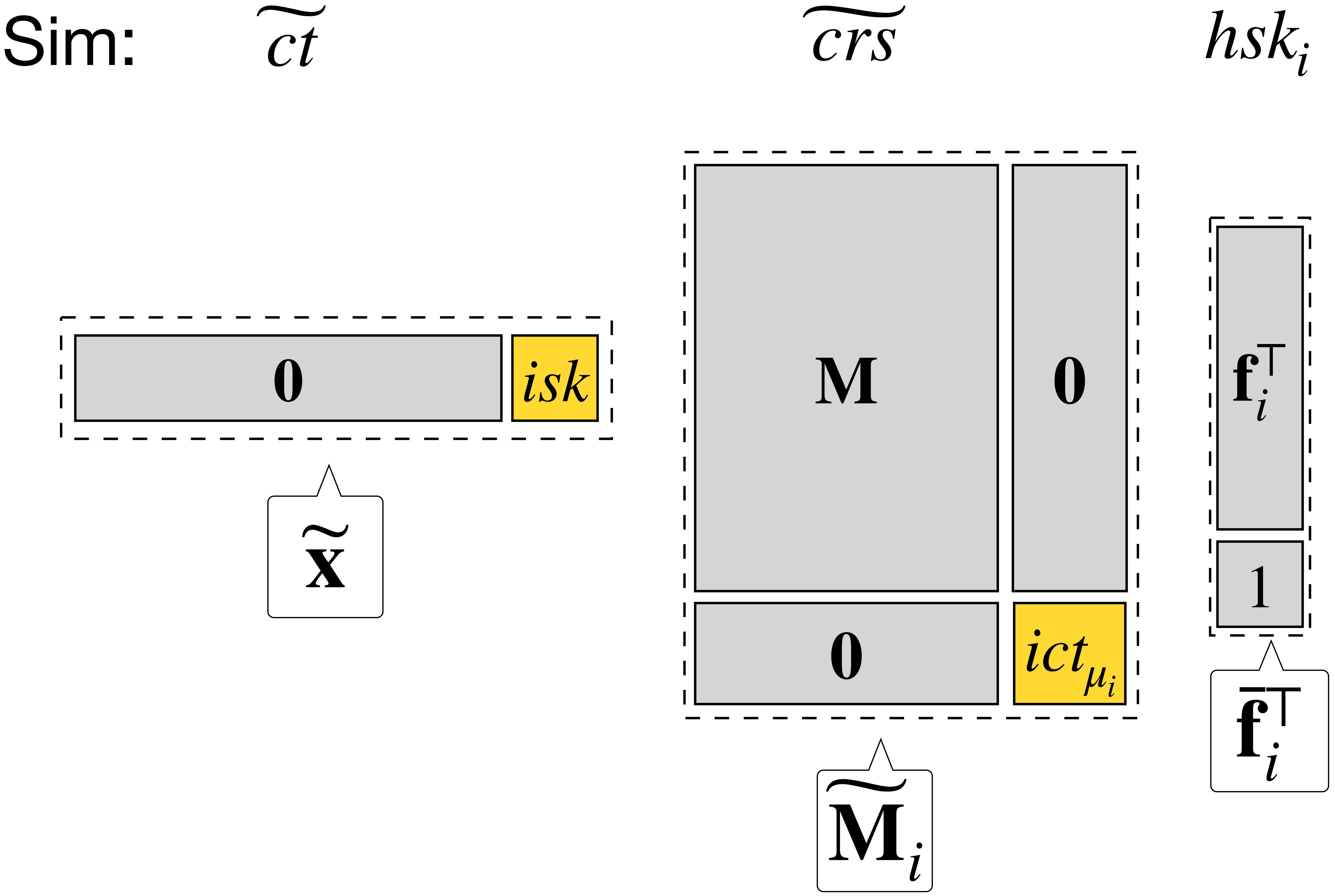
$ict_{\mu_i} \leftarrow iEnc(\mathbf{x}\mathbf{M}\mathbf{f}_i^\top)$

$i \in \mathscr{C} \cup \mathscr{M}$

$$\widetilde{\mathbf{x}}\widetilde{\mathbf{M}}_i\bar{\mathbf{f}}_i^\top = < isk, ict_{\mu_i} > = \mathbf{x}\mathbf{M}\mathbf{f}_i^\top$$

sReg-IPFE to sReg-QFE: Solution-3

To achieve sel*-SIM PReg-IPFE



With PKE:

$(ipk, \boxed{isk}) \leftarrow iGen(1^\lambda)$

$\boxed{ict_{\mu_i}} \leftarrow iEnc(\mathbf{x}\mathbf{M}\mathbf{f}_i^\top)$

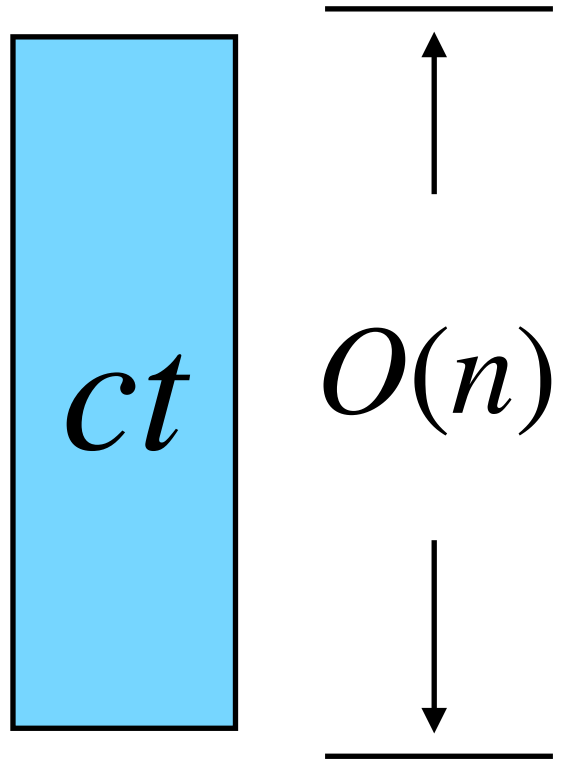
$i \in \mathscr{C} \cup \mathscr{M}$

$$\tilde{\mathbf{x}}\widetilde{\mathbf{M}}_i\bar{\mathbf{f}}_i^\top = \boxed{< isk, ict_{\mu_i} > = \mathbf{x}\mathbf{M}\mathbf{f}_i^\top}$$

linear decryption

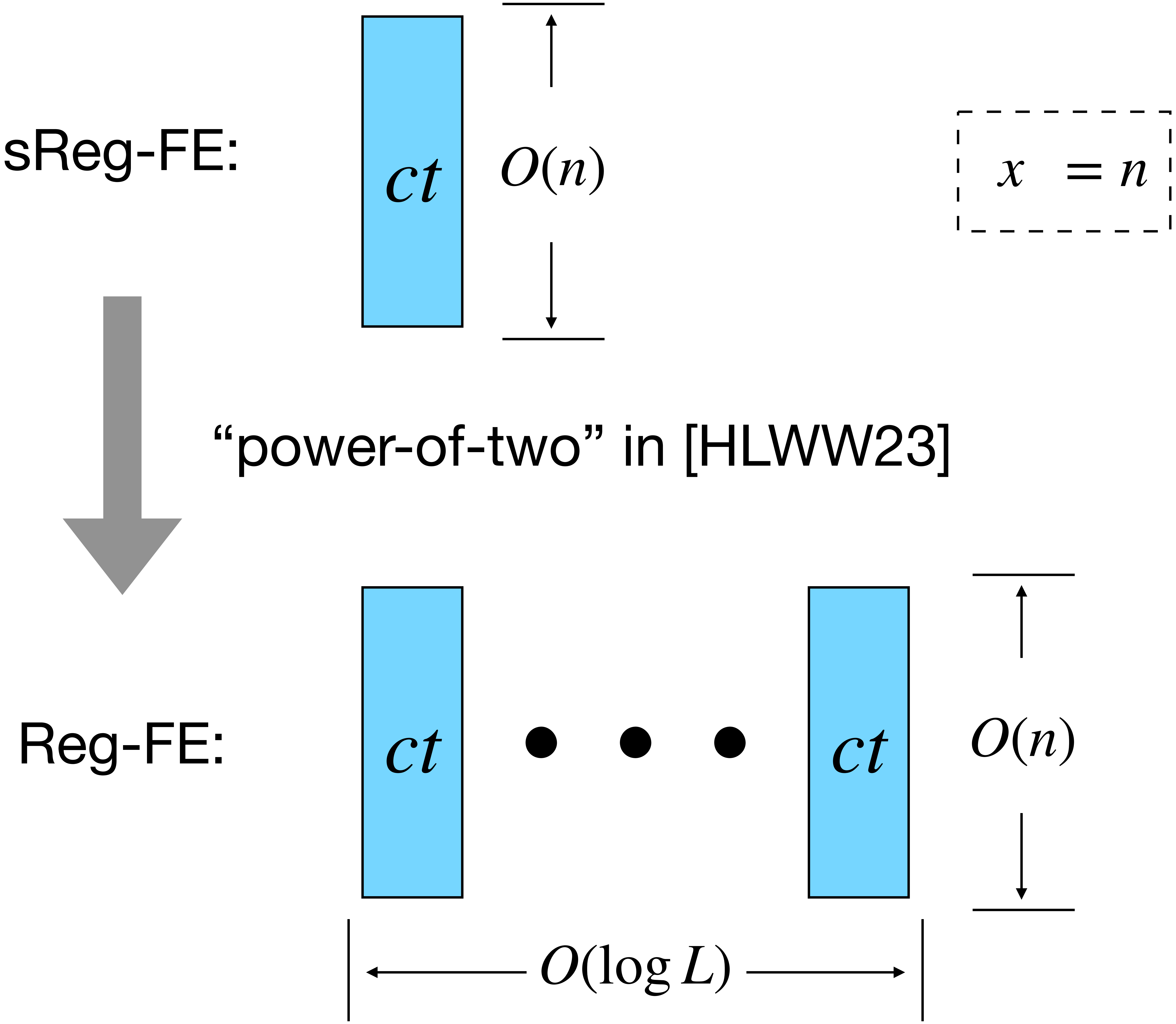
To Compact Ciphertext

sReg-FE:



$x \quad = n$

To Compact Ciphertext



sReg-FE: ct $O(n)$

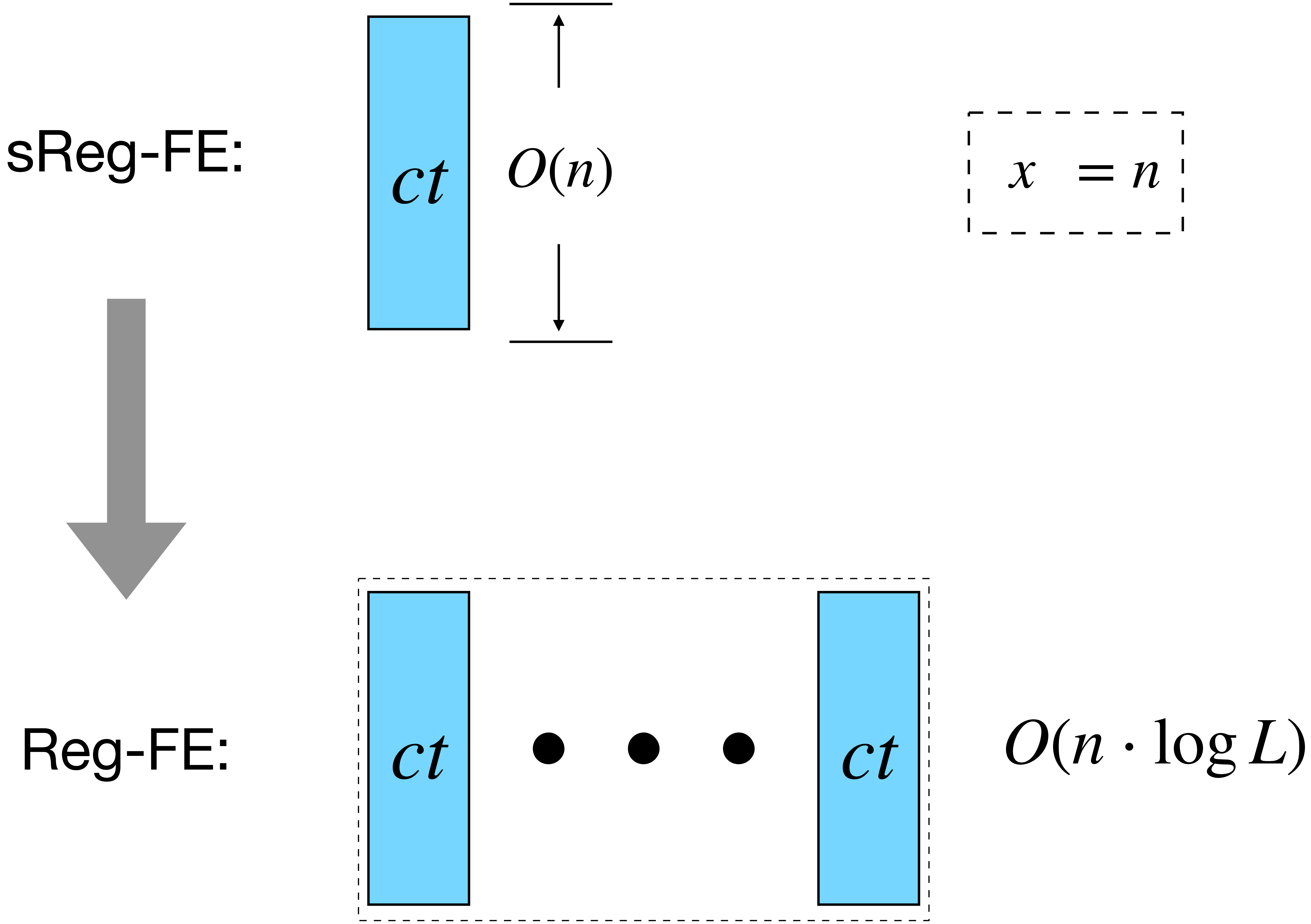
$x = n$

“power-of-two” in [HLWW23]

Reg-FE: ct ● ● ● ct $O(n)$

$O(\log L)$

To Compact Ciphertext



sReg-FE:

ct

$O(n)$

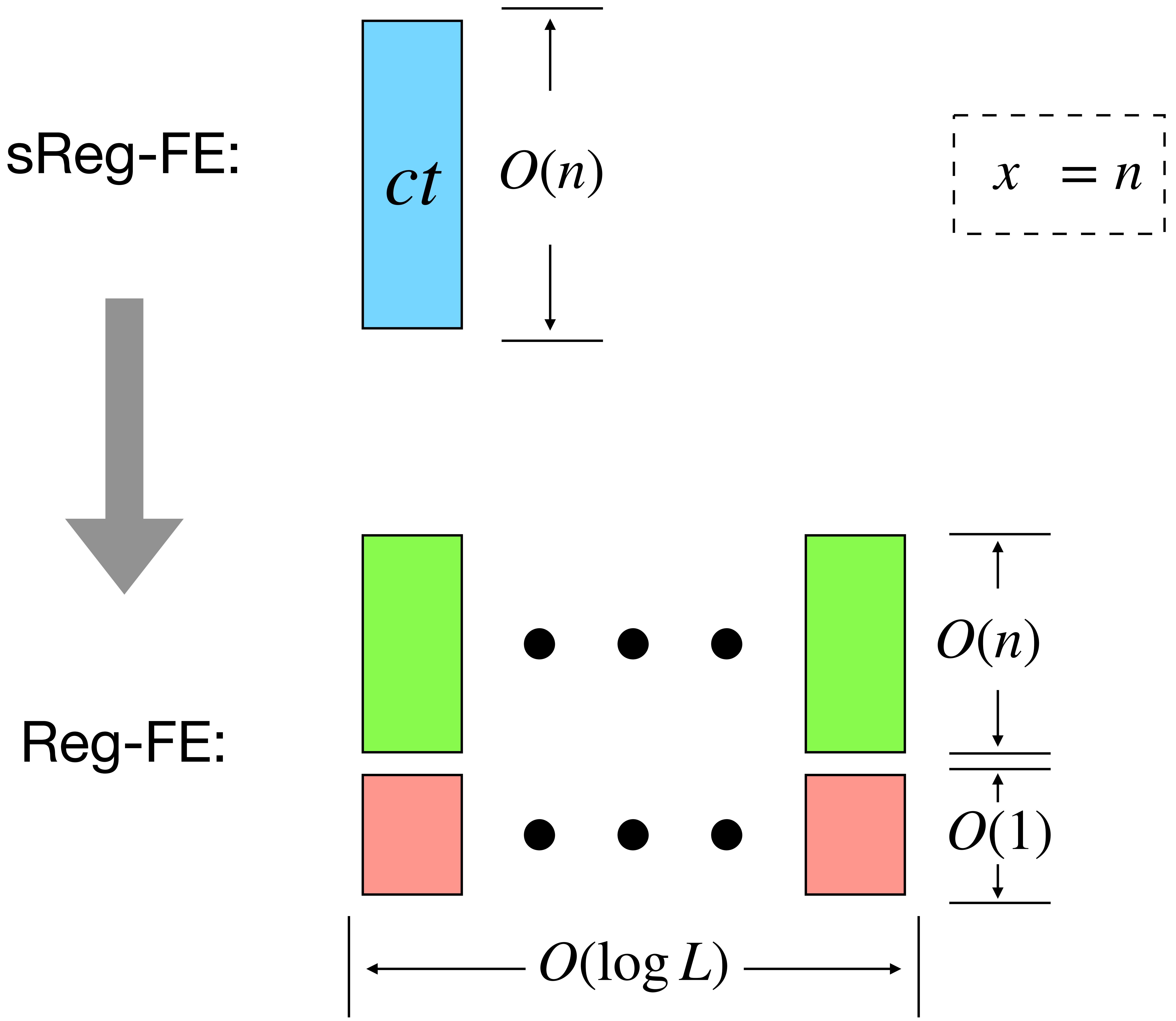
$x \ = n$

Reg-FE:

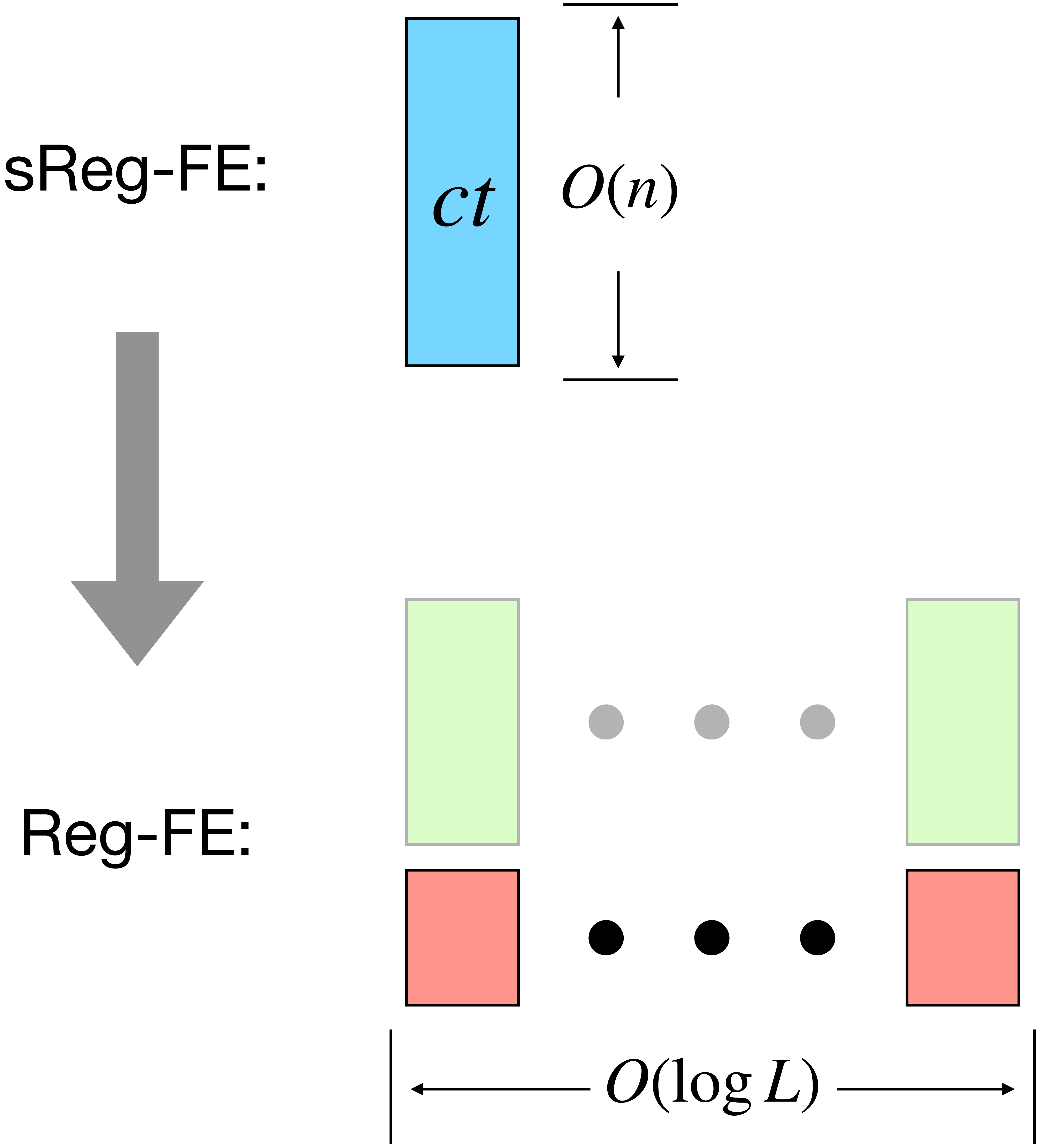
ct ● ● ● ct

$O(n \cdot \log L)$

To Compact Ciphertext



To Compact Ciphertext



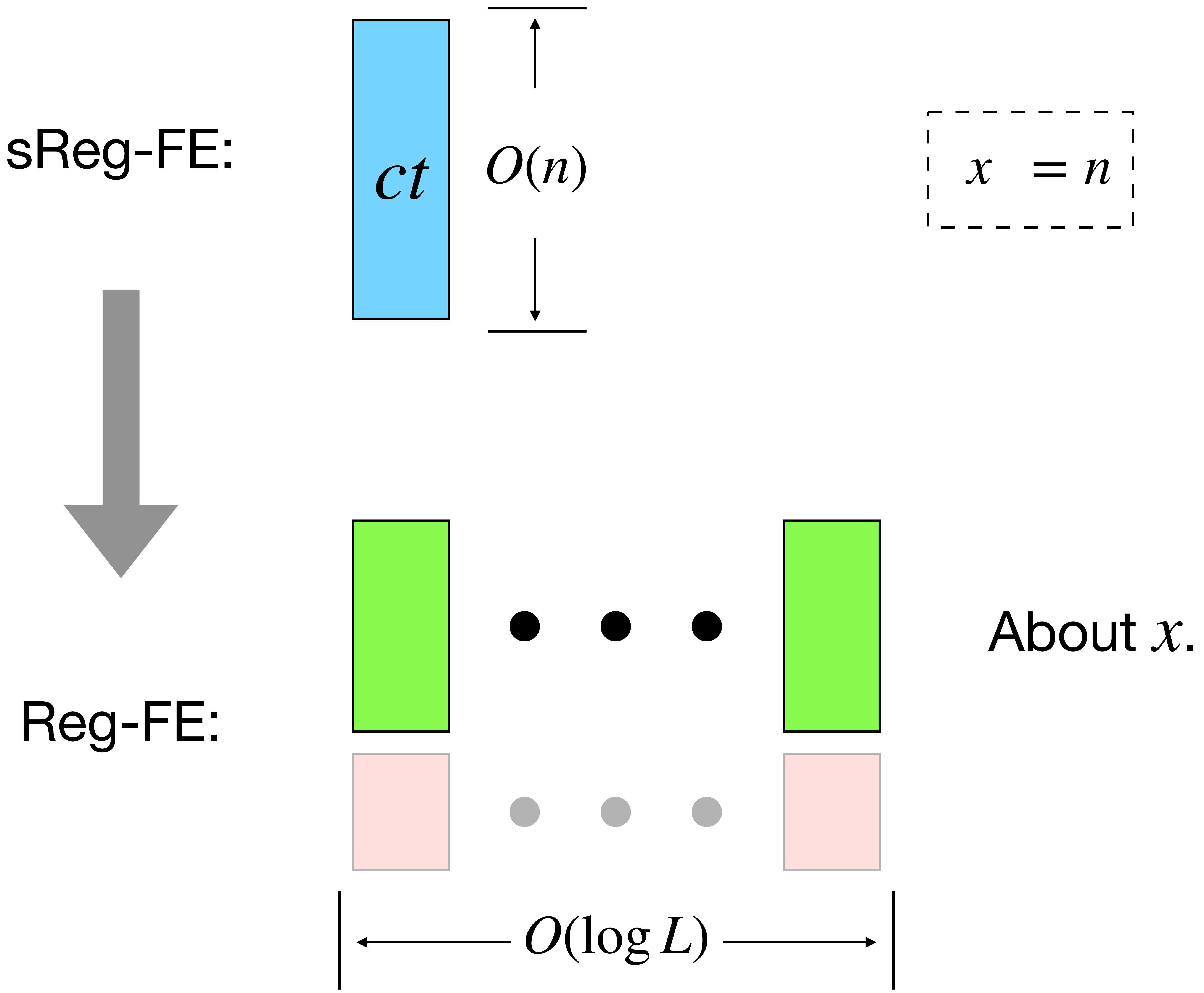
sReg-FE:

Reg-FE:

$x = n$

About users in sReg-FE instance.

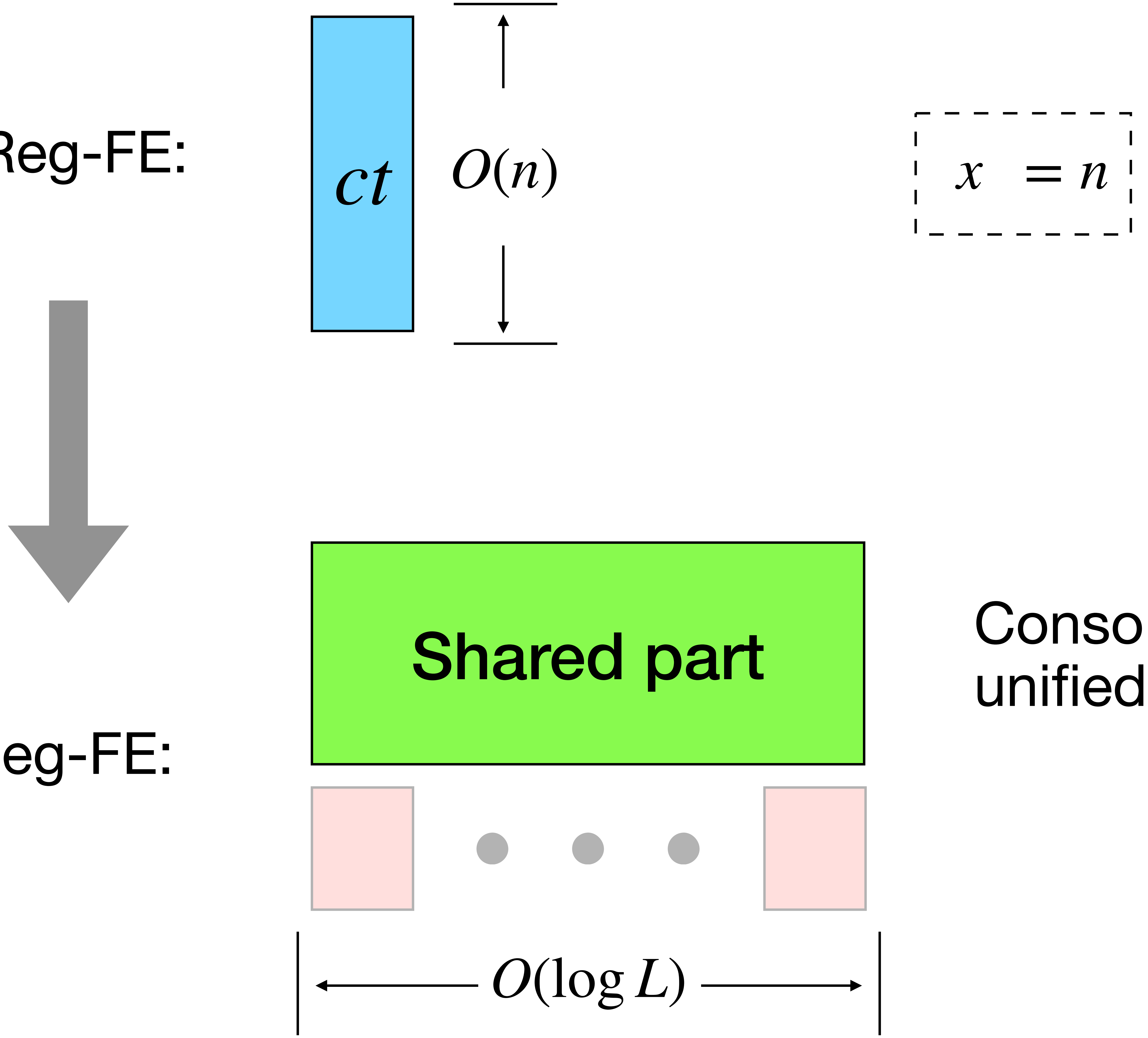
To Compact Ciphertext



To Compact Ciphertext

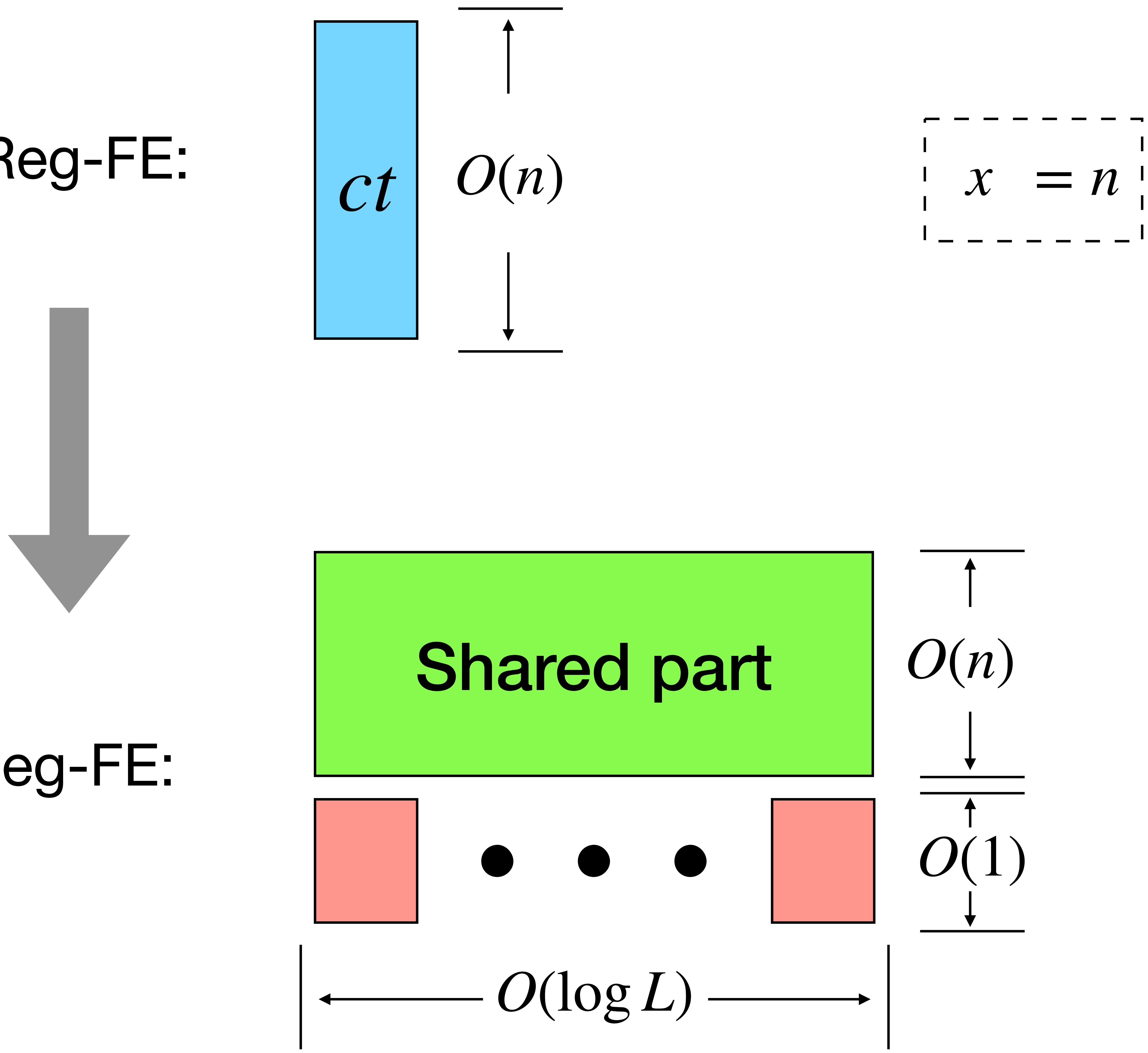
sReg-FE:

Reg-FE:



Consolidate them with a unified random coin.

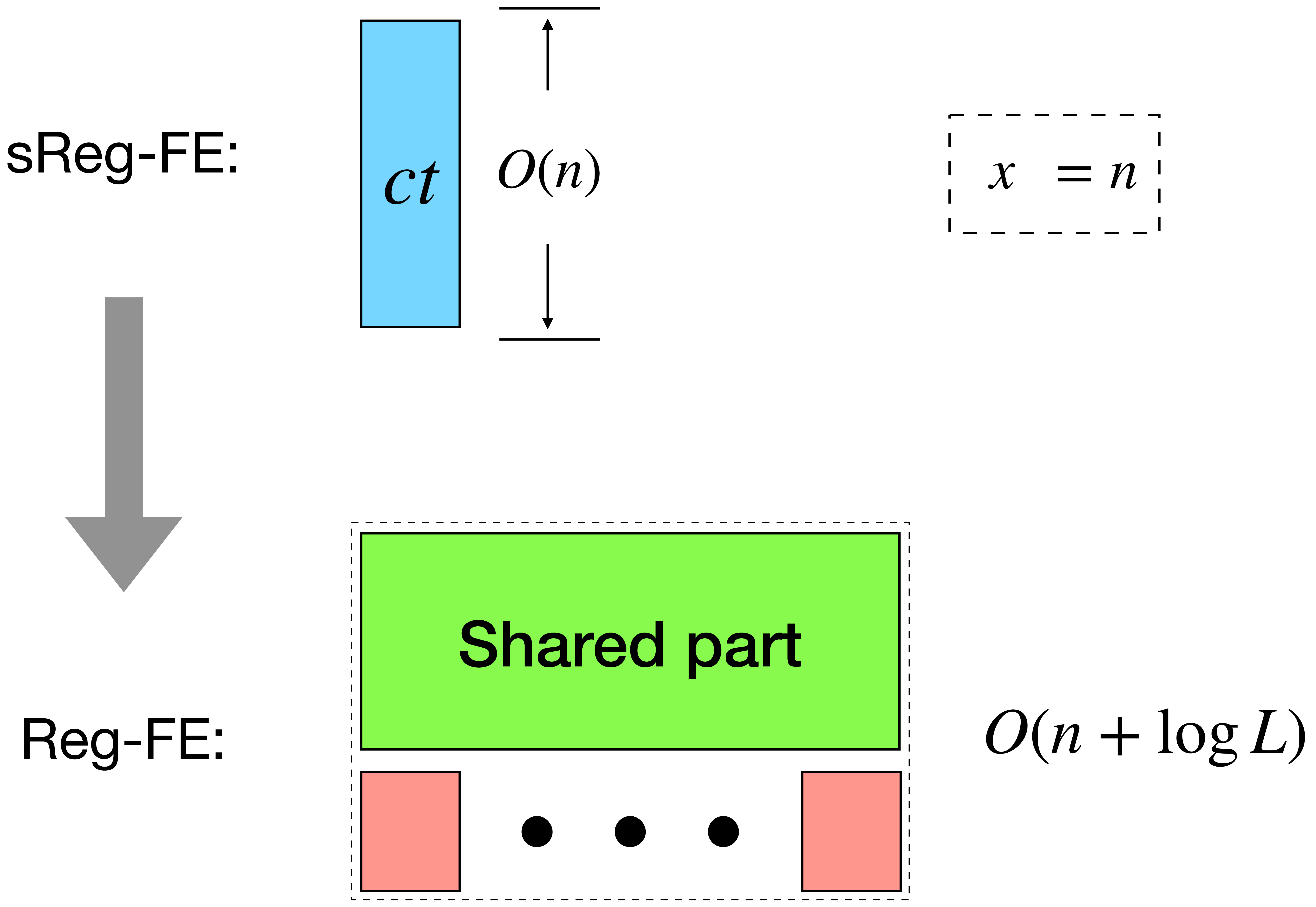
To Compact Ciphertext



sReg-FE:

Reg-FE:

To Compact Ciphertext



sReg-FE:

ct

$O(n)$

$x \quad = n$

Reg-FE:

Shared part

$O(n + \log L)$

Thanks for Your Listening

Ziqi Zhu
ZiqiZhu00@stu.ecnu.edu.cn