A General Framework for Registered Functional Encryption via User-Specific Pre-Constraining

Tapas Pal[1] **Robert Schädlich**[2]

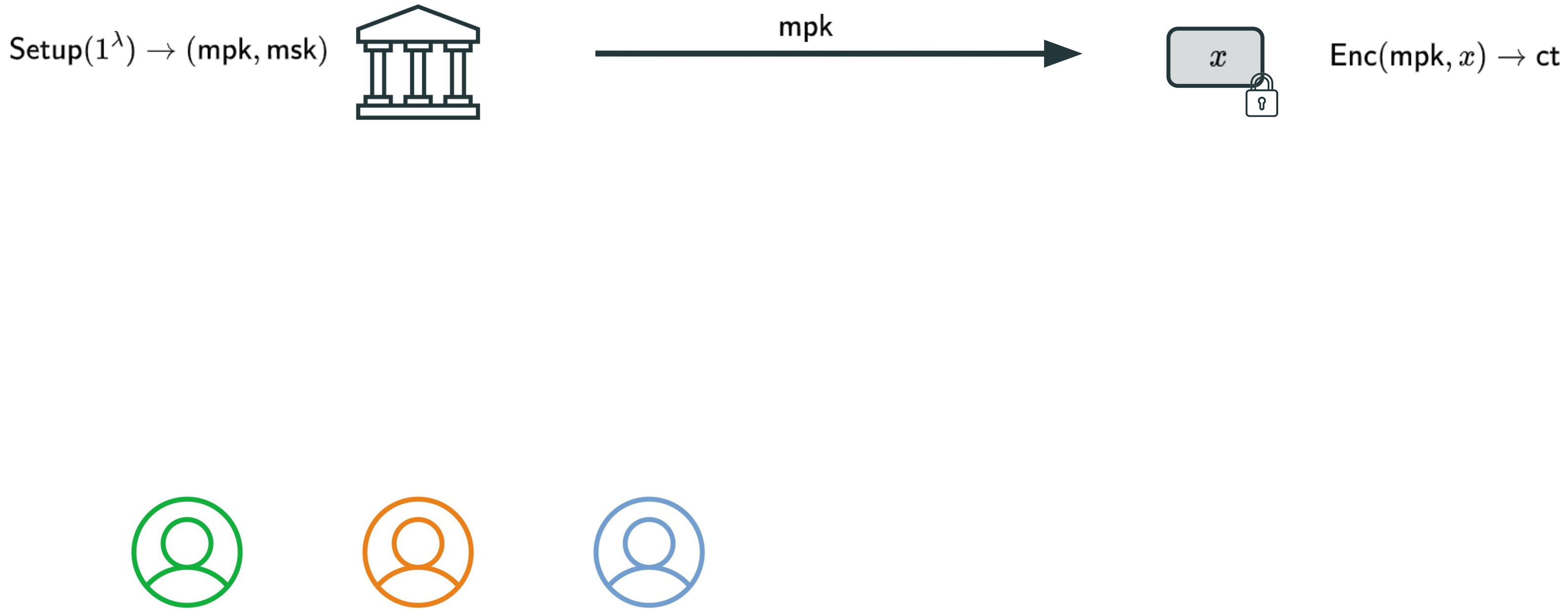
November 6, 2025

[1] Karlsruhe Institute of Technology, KASTEL Security Research Labs
[2] DIENS, École normale supérieure, PSL University, CNRS, Inria

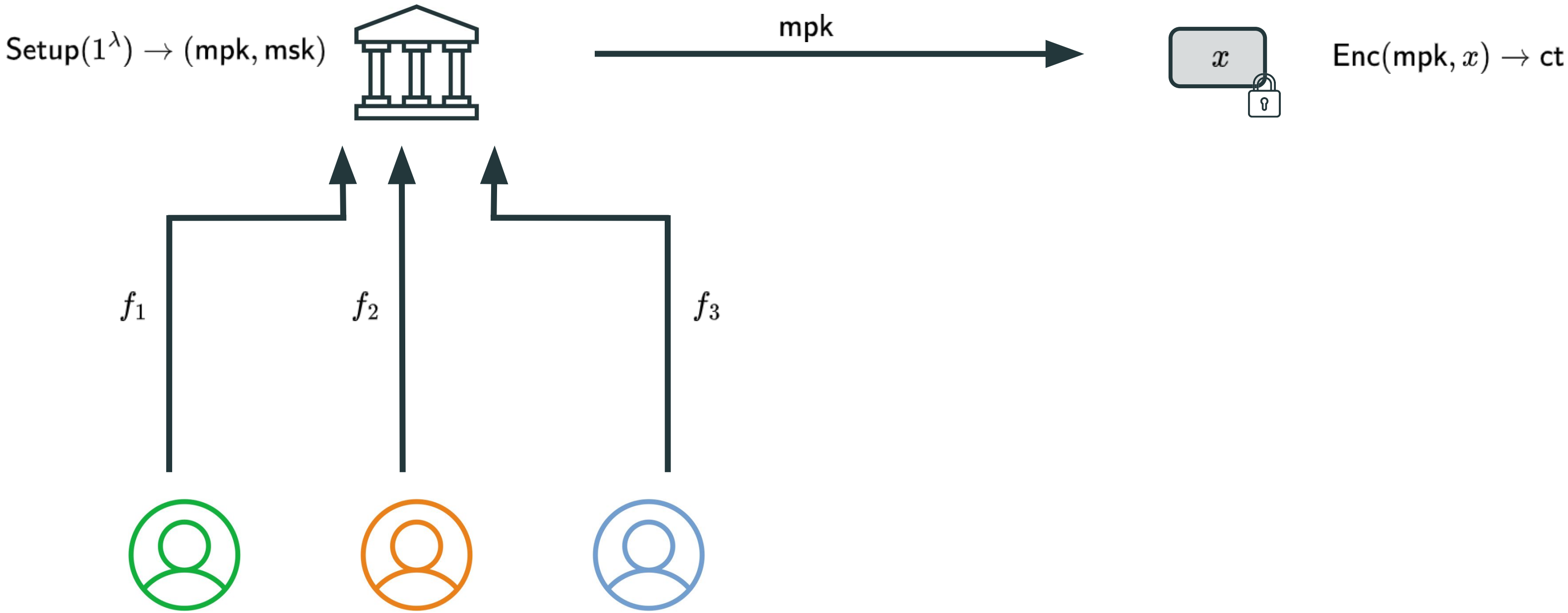
Functional Encryption (FE) [TCC:BSW11]

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$

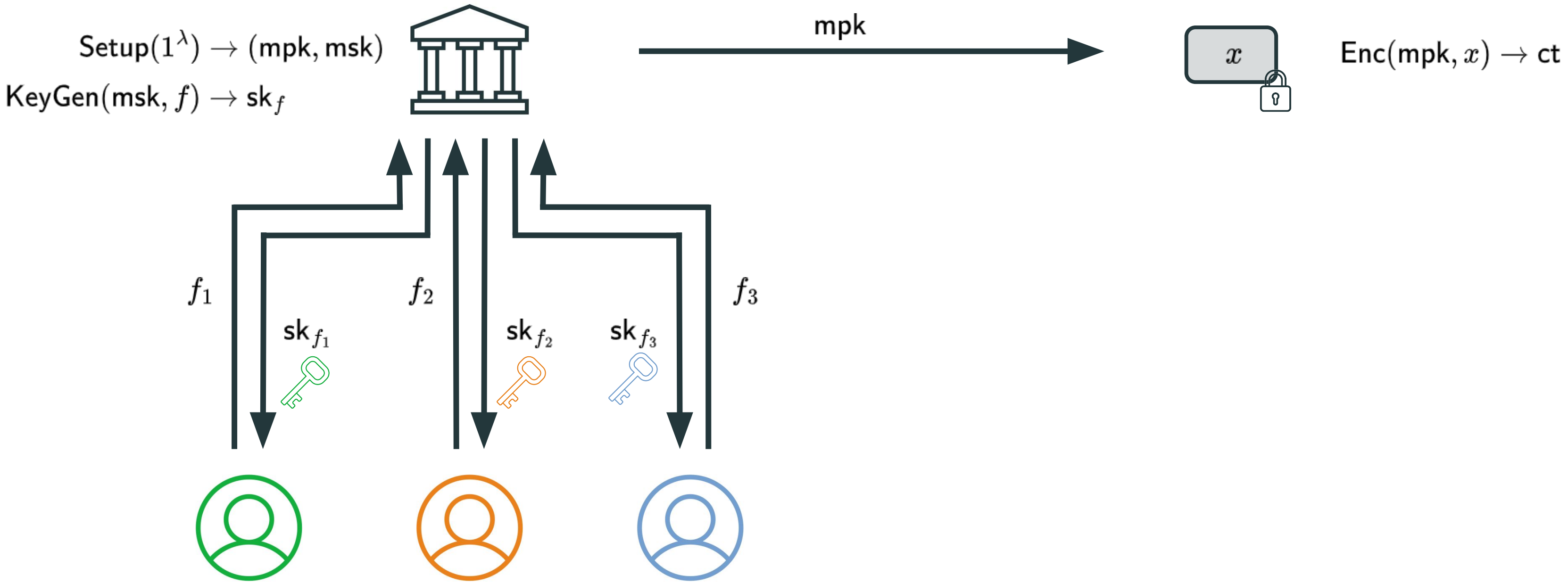
Functional Encryption (FE) [TCC:BSW11]



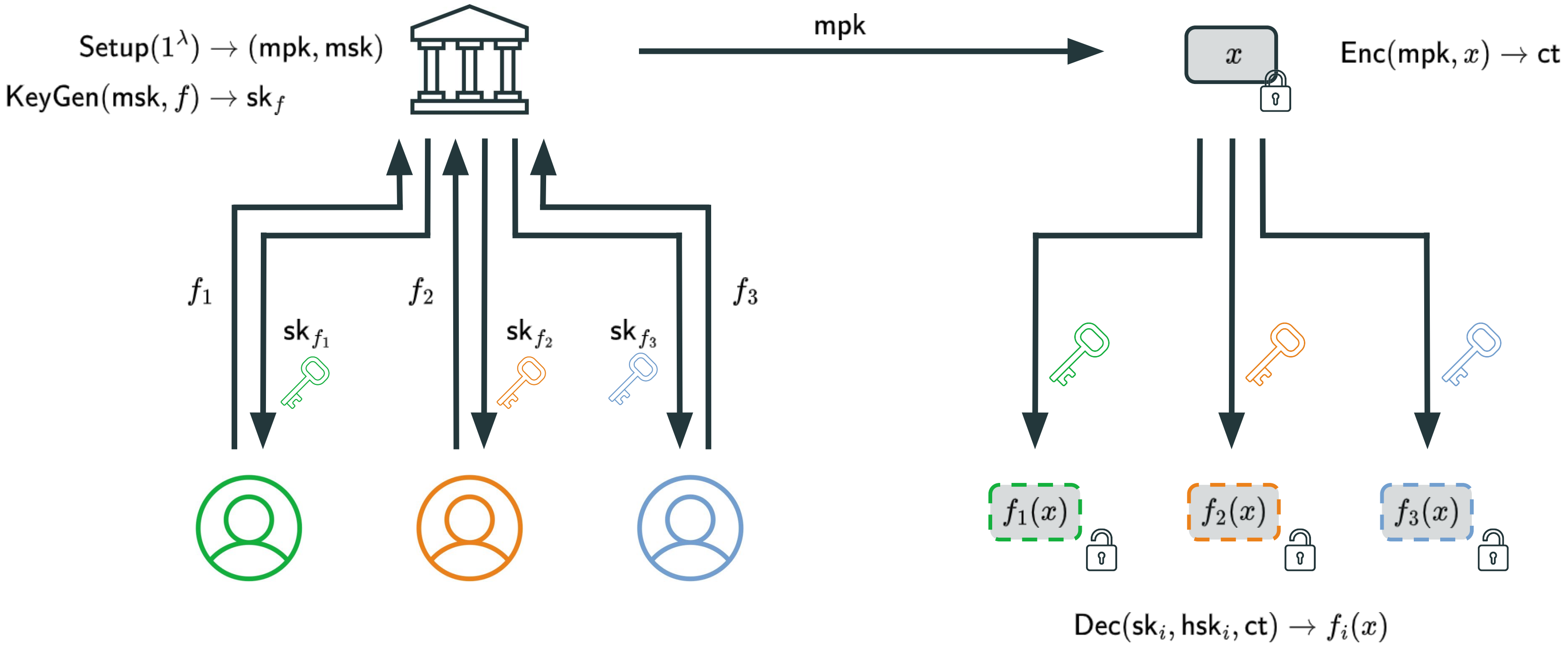
Functional Encryption (FE) [TCC:BSW11]



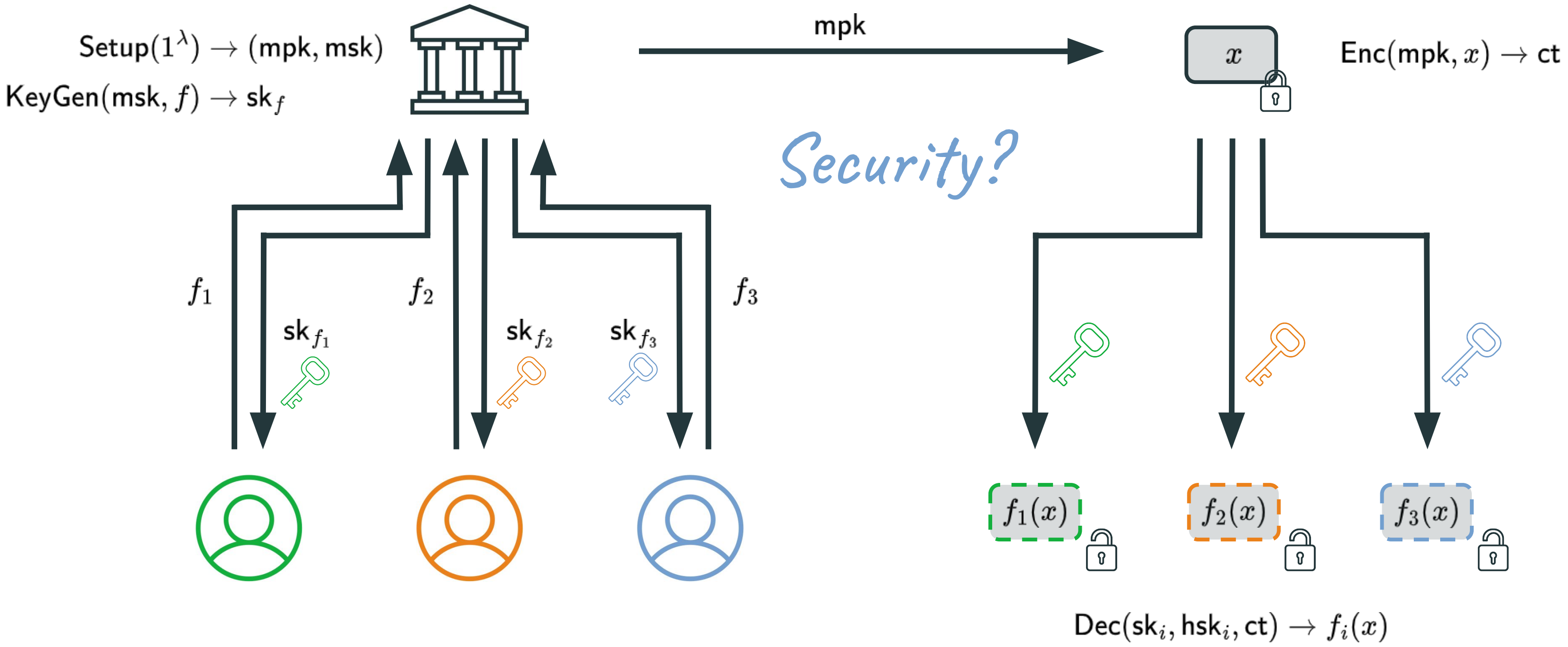
Functional Encryption (FE) [TCC:BSW11]



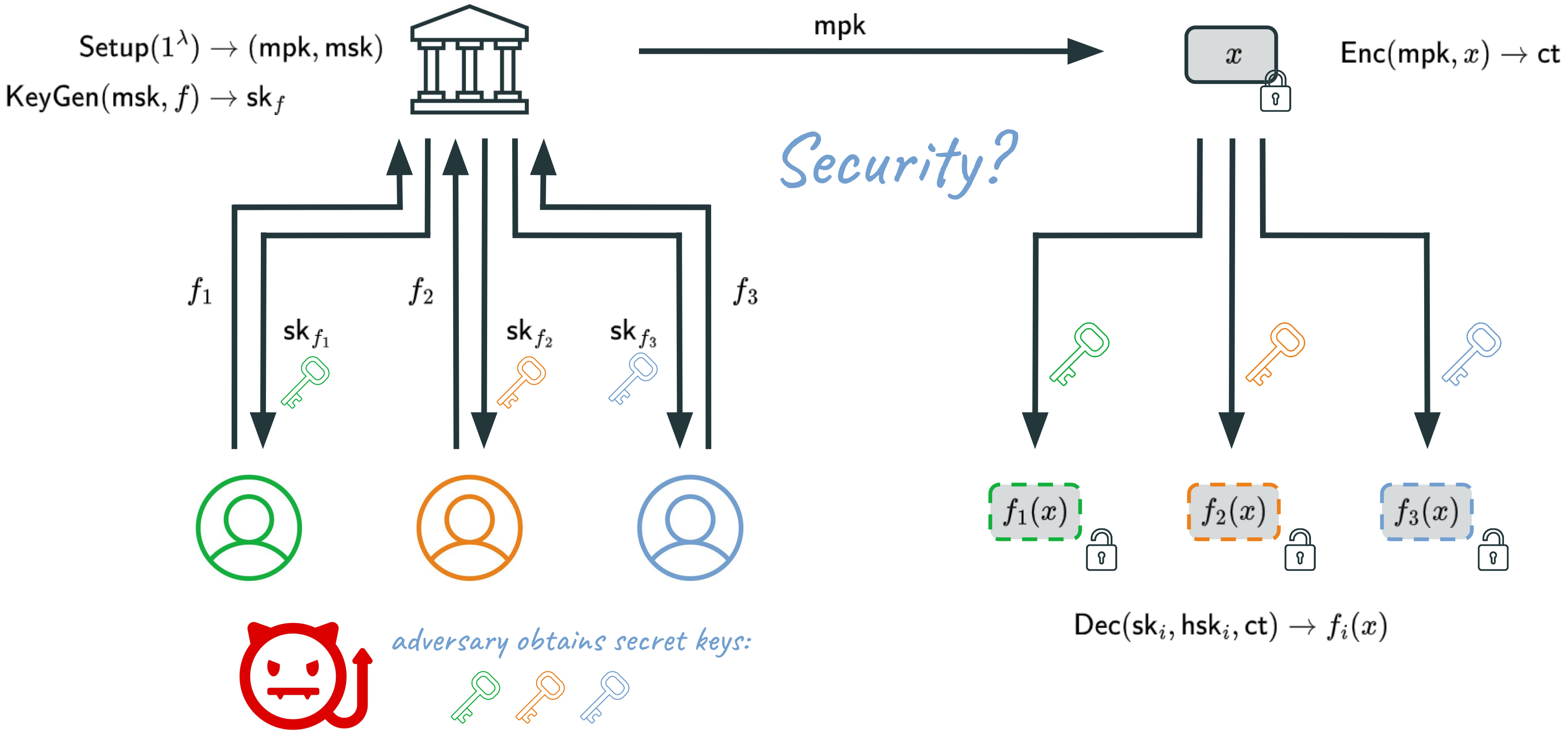
Functional Encryption (FE) [TCC:BSW11]



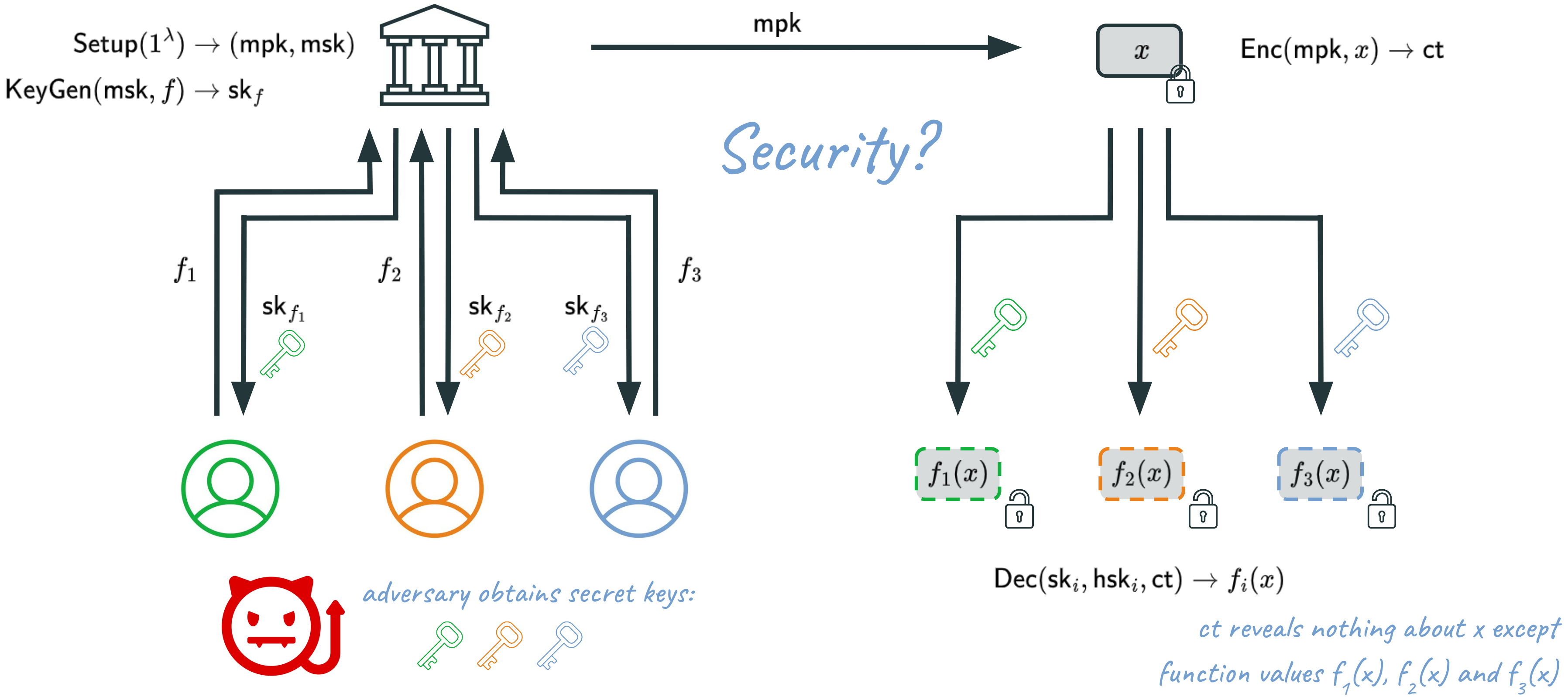
Functional Encryption (FE) [TCC:BSW11]



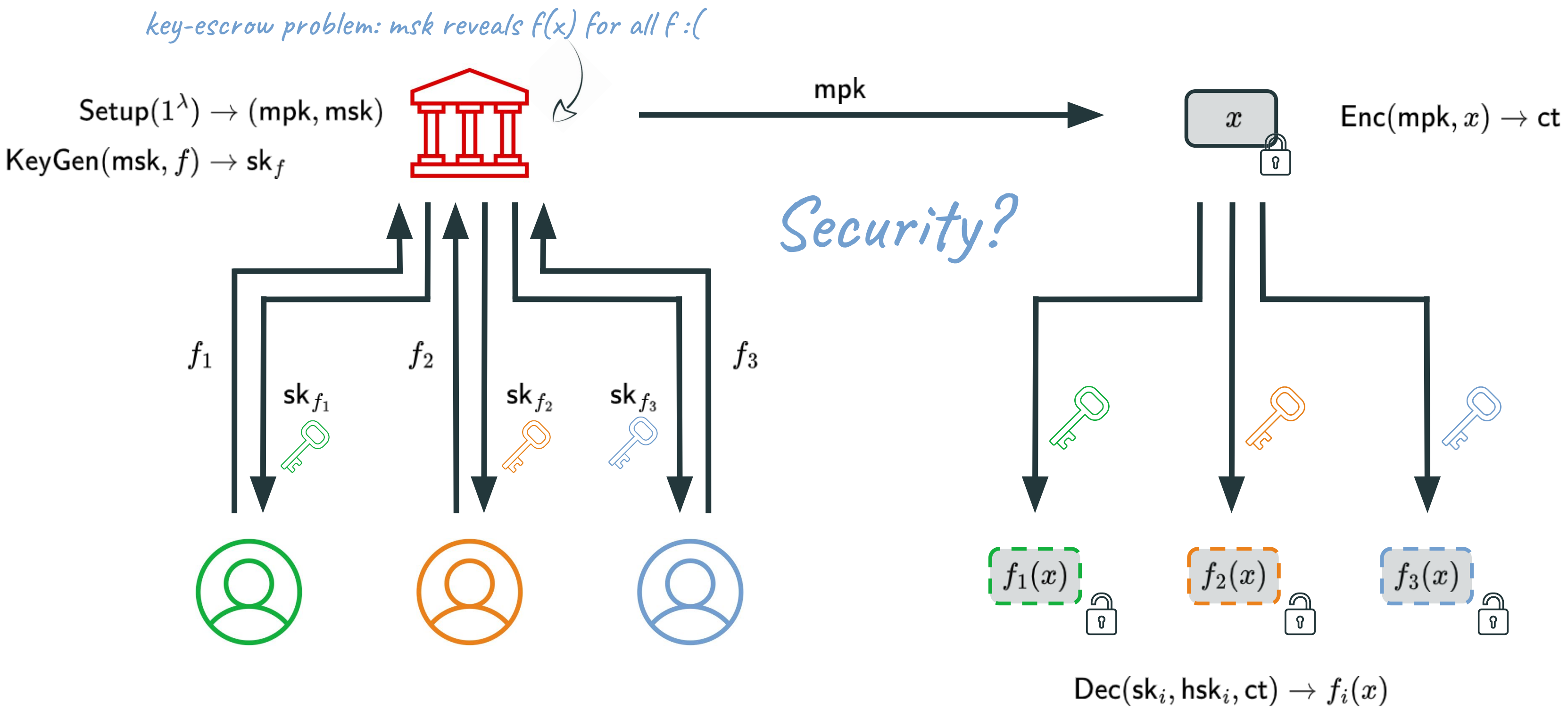
Functional Encryption (FE) [TCC:BSW11]



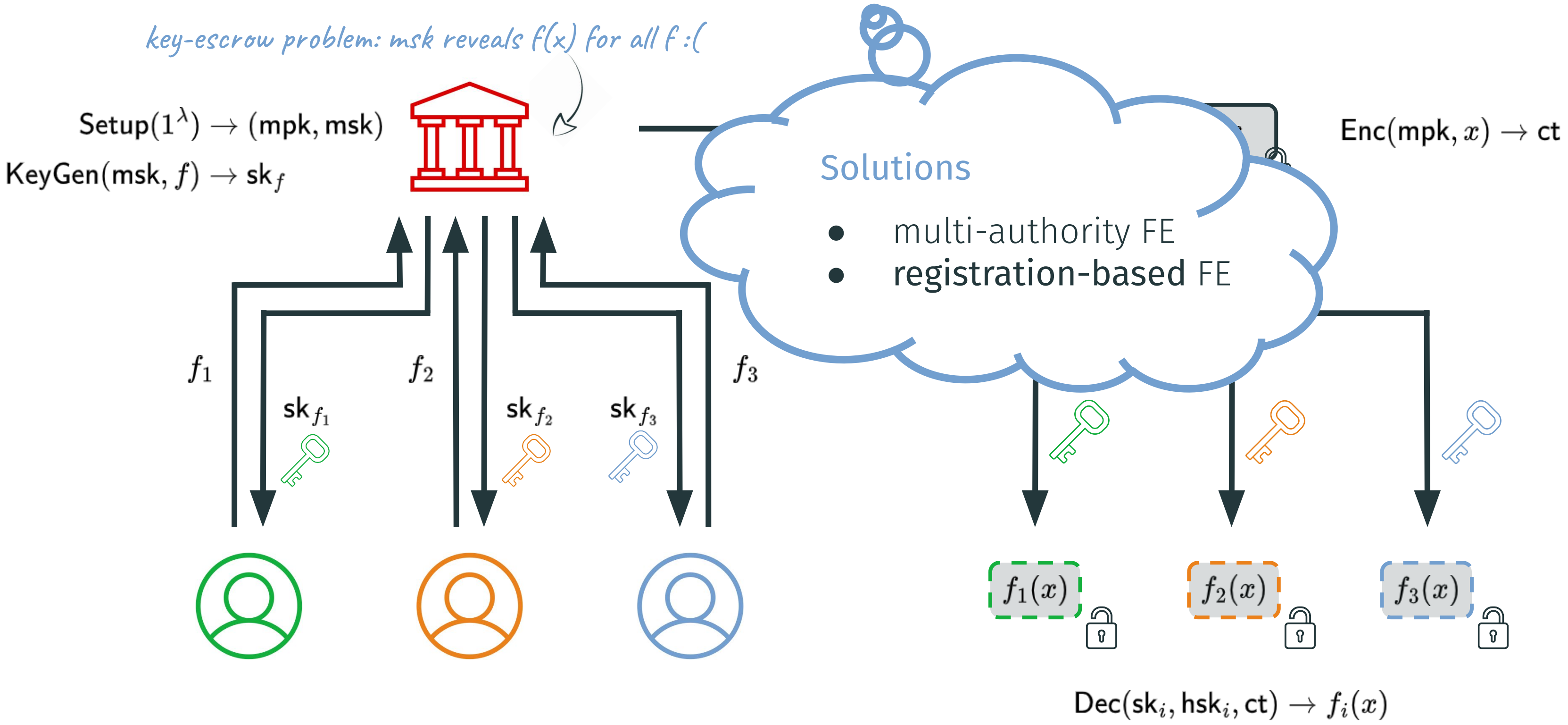
Functional Encryption (FE) [TCC:BSW11]



Functional Encryption (FE) [TCC:BSW11]



Functional Encryption (FE) [TCC:BSW11]

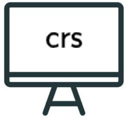


Solutions

- multi-authority FE
- **registration-based** FE

Registered Functional Encryption (RFE) [AC:FFM+23]

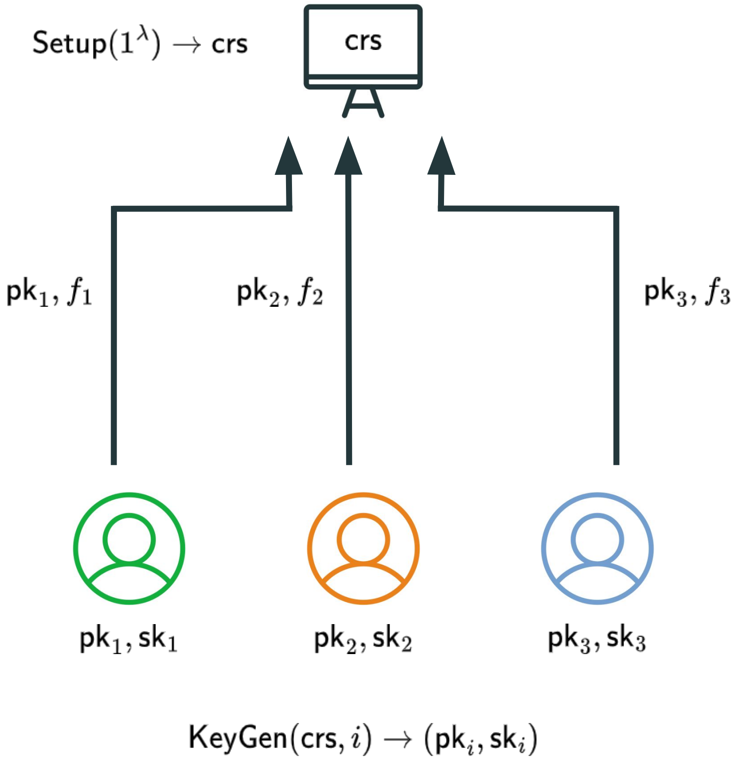
$\mathsf{Setup}(1^\lambda) \rightarrow \mathsf{crs}$



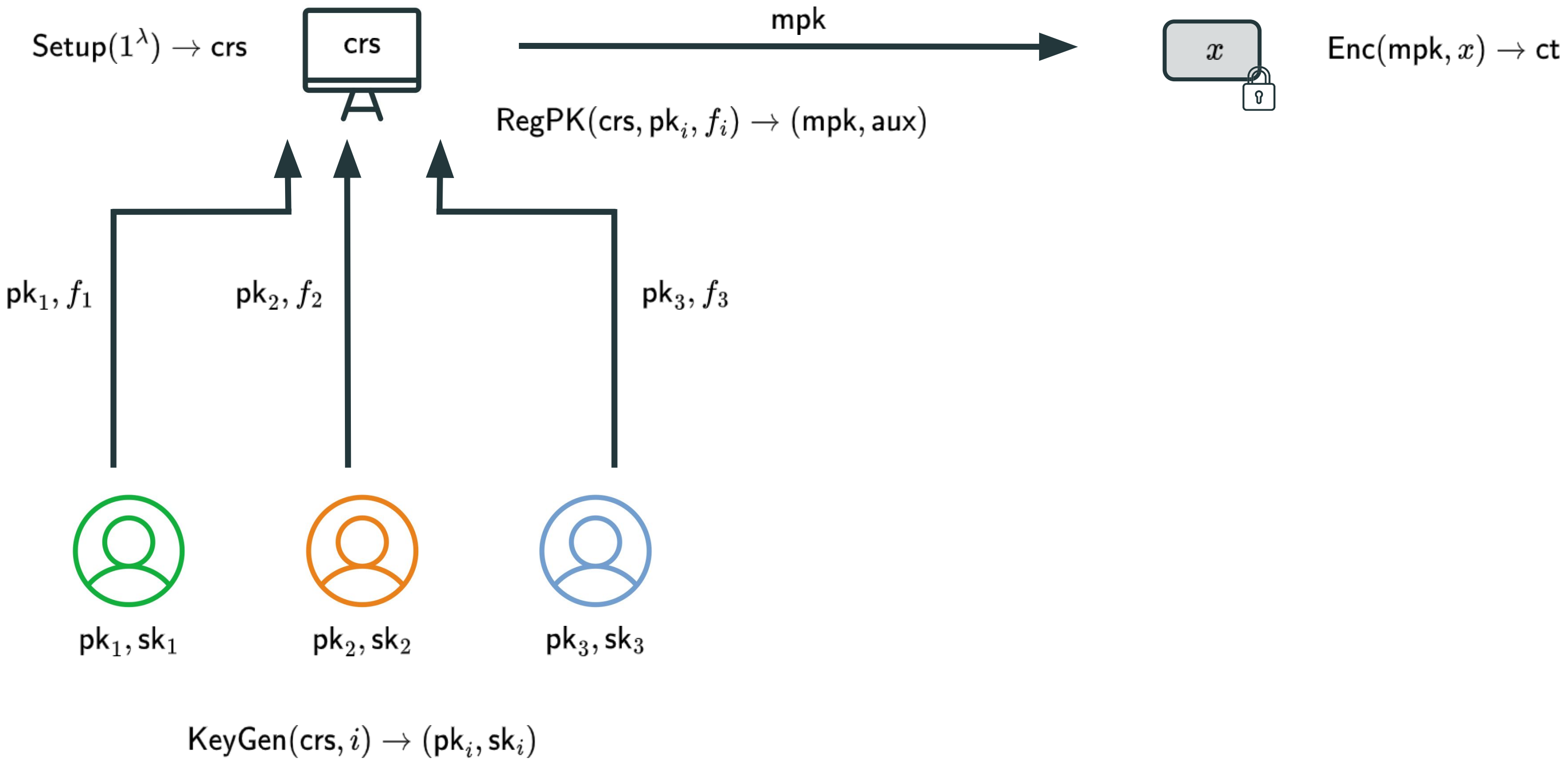
$\mathsf{pk}_1, \mathsf{sk}_1$ $\quad$ $\mathsf{pk}_2, \mathsf{sk}_2$ $\quad$ $\mathsf{pk}_3, \mathsf{sk}_3$

$\mathsf{KeyGen}(\mathsf{crs}, i) \rightarrow (\mathsf{pk}_i, \mathsf{sk}_i)$

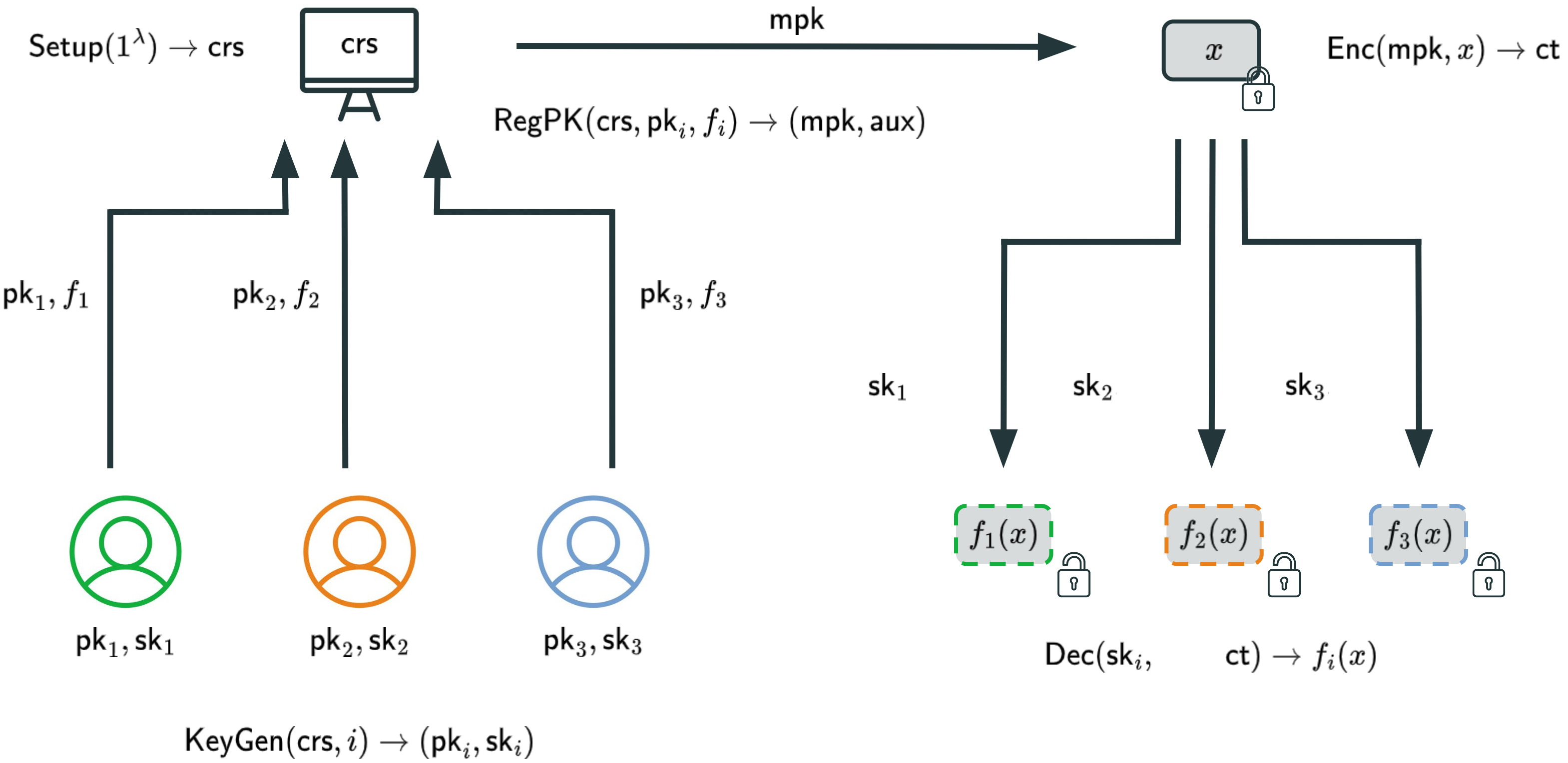
Registered Functional Encryption (RFE) [AC:FFM+23]



Registered Functional Encryption (RFE) [AC:FFM+23]

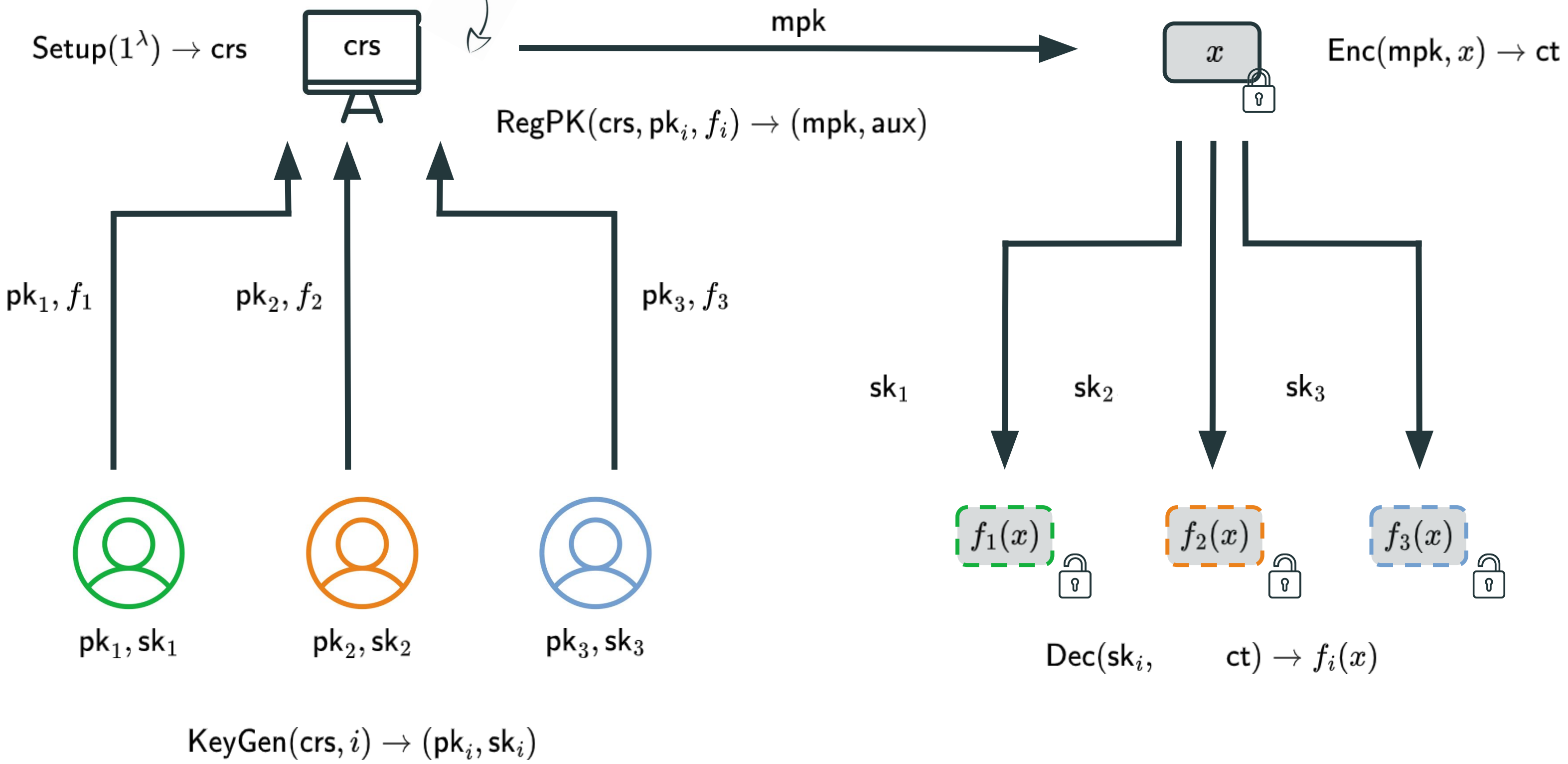


Registered Functional Encryption (RFE) [AC:FFM+23]



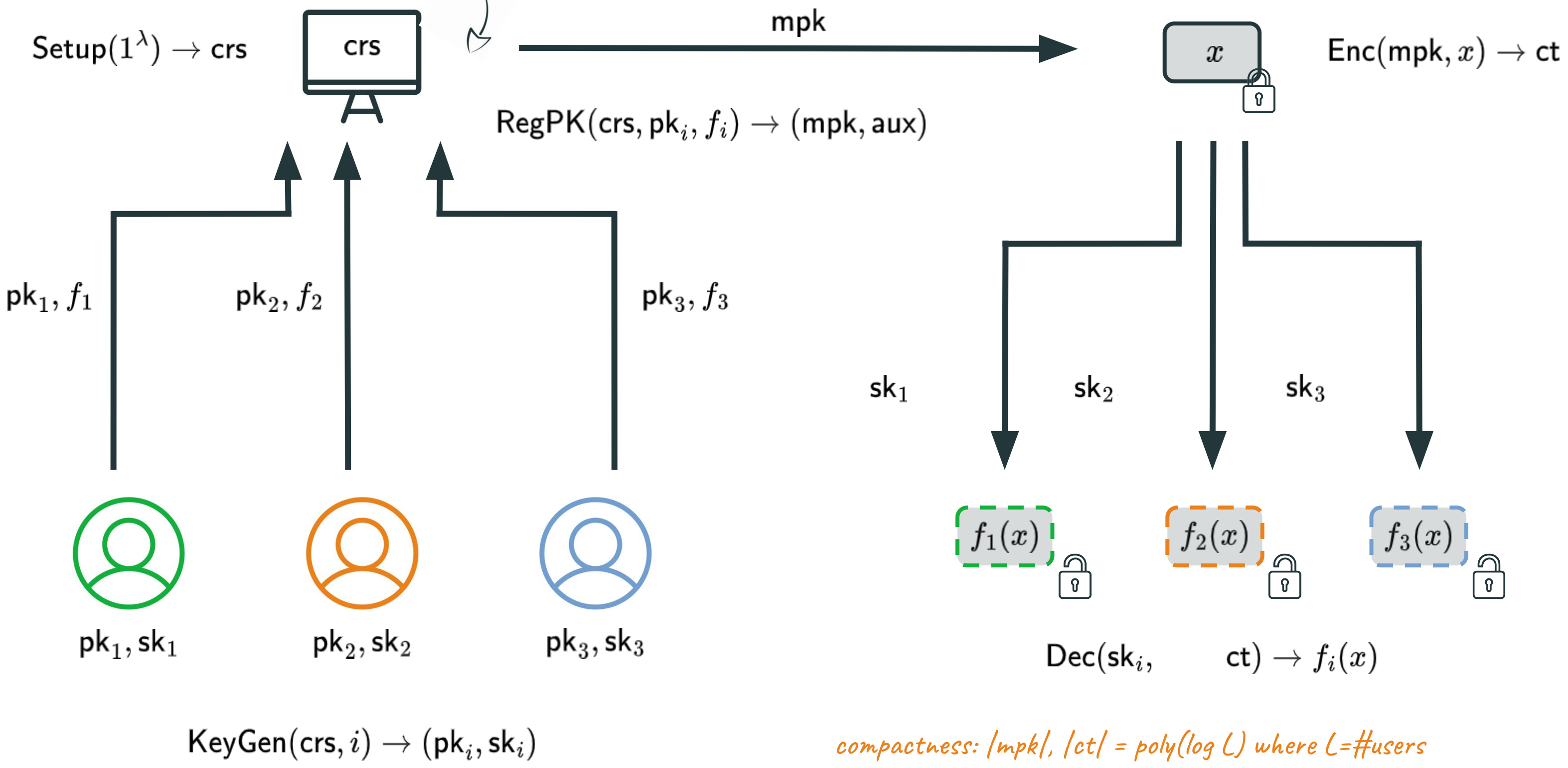
Registered Functional Encryption (RFE) [AC:FFM+23]

key curator is deterministic & holds no secret => key-escrow problem resolved!



Registered Functional Encryption (RFE) [AC:FFM+23]

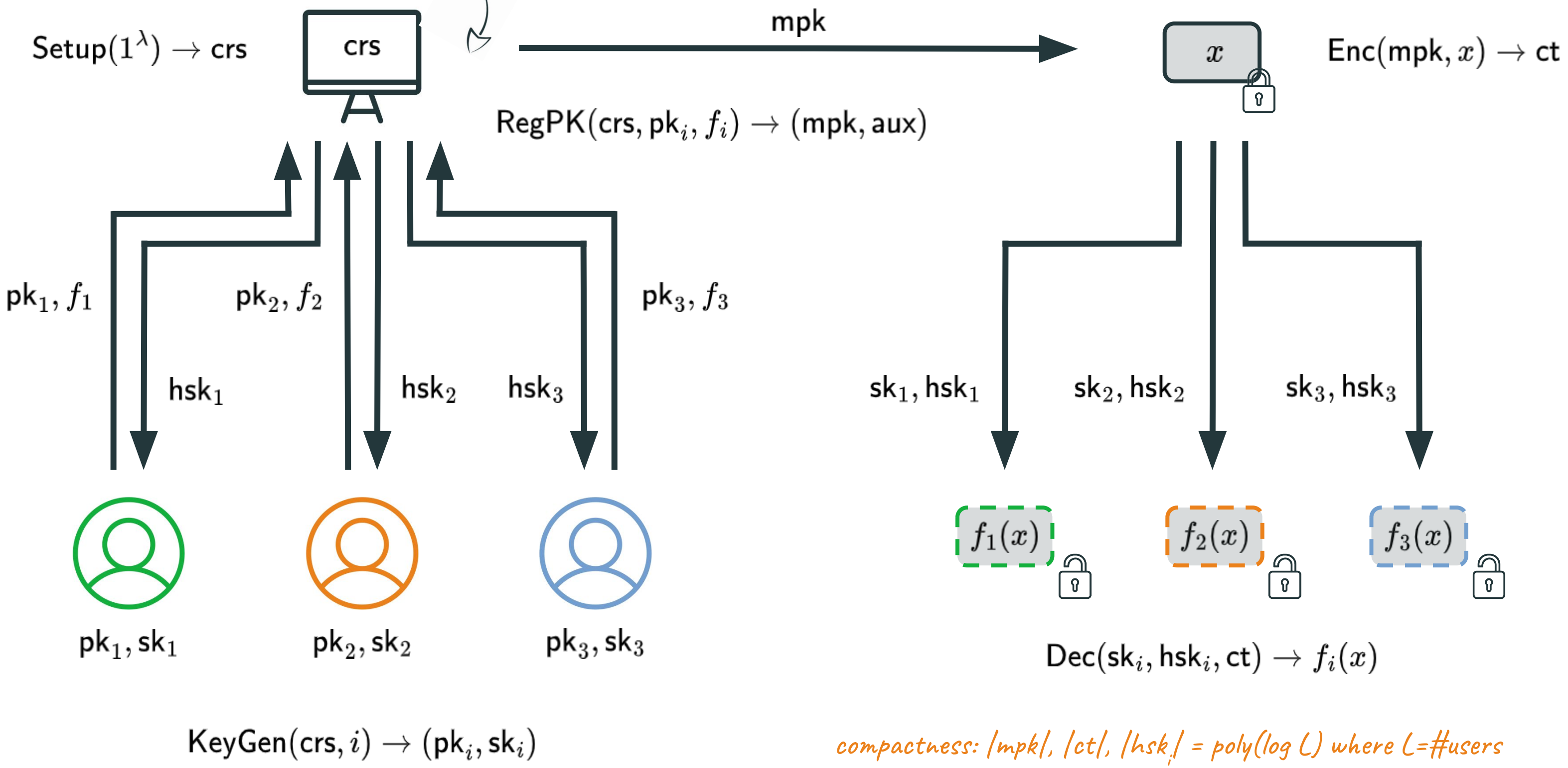
key curator is deterministic & holds no secret => key-escrow problem resolved!



compactness: |mpk|, |ct| = poly(log L) where L=#users

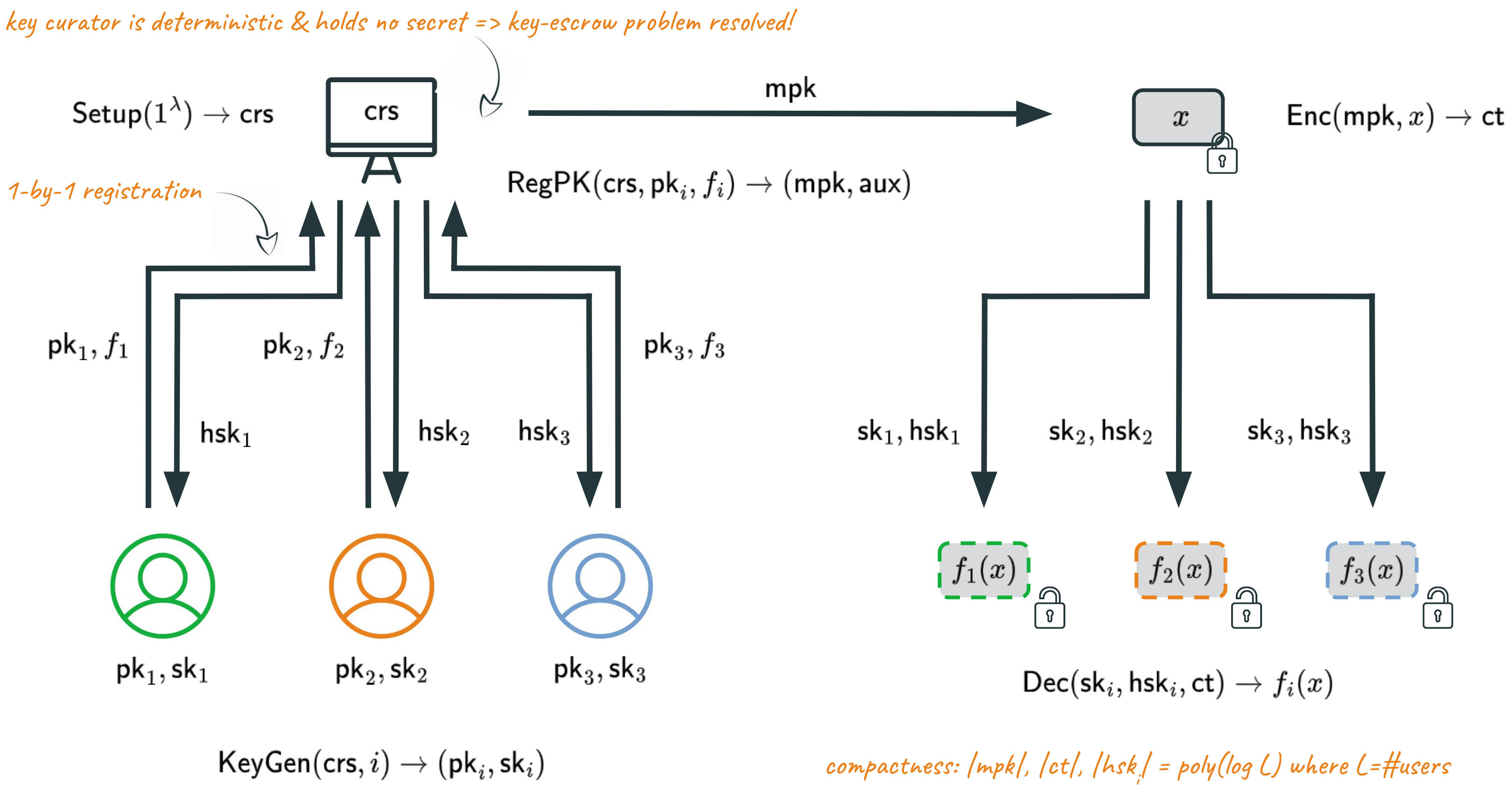
Registered Functional Encryption (RFE) [AC:FFM+23]

key curator is deterministic & holds no secret => key-escrow problem resolved!

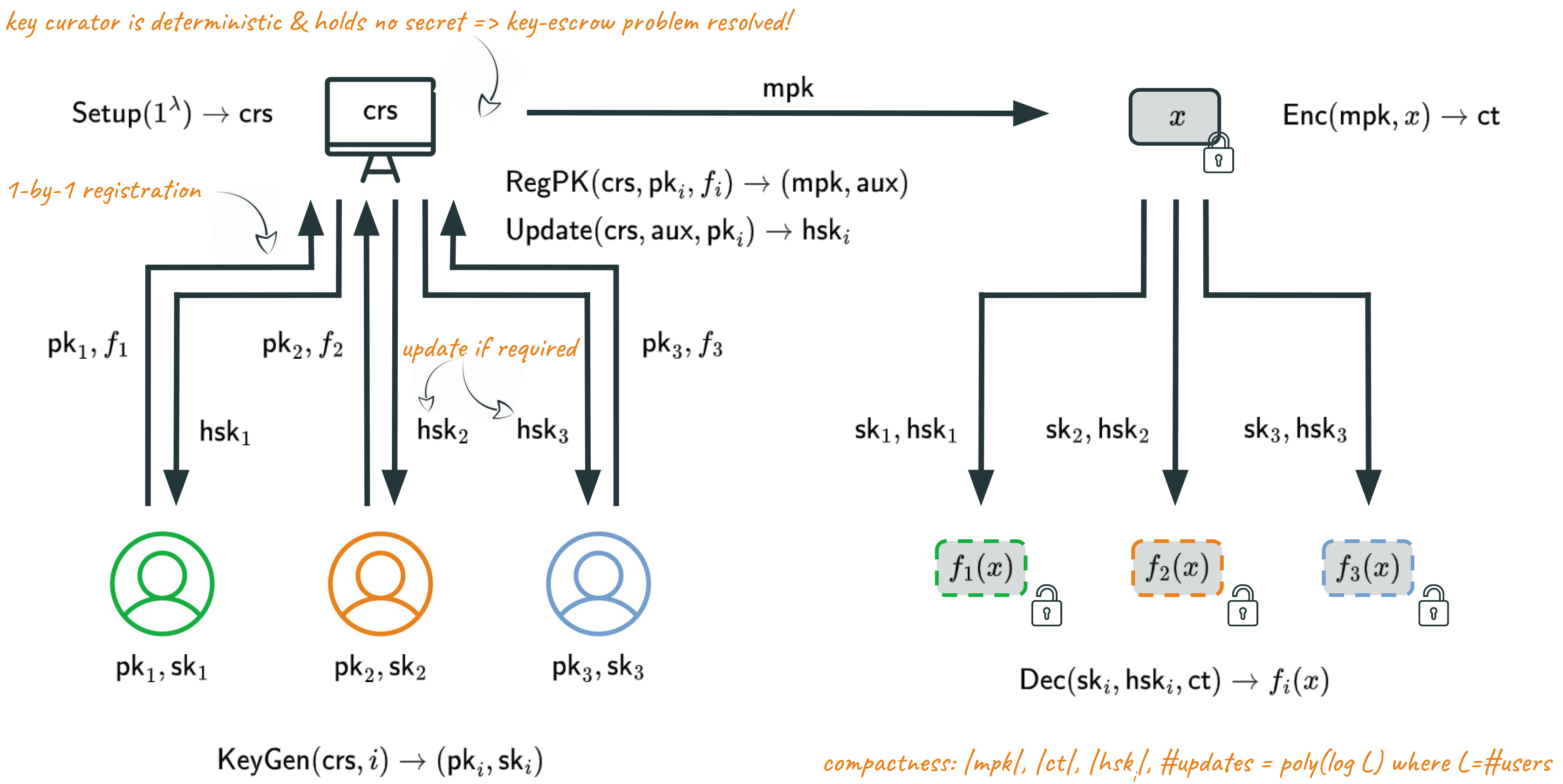


compactness: |mpk|, |ct|, |hsk$_i$| = poly(log L) where L=#users

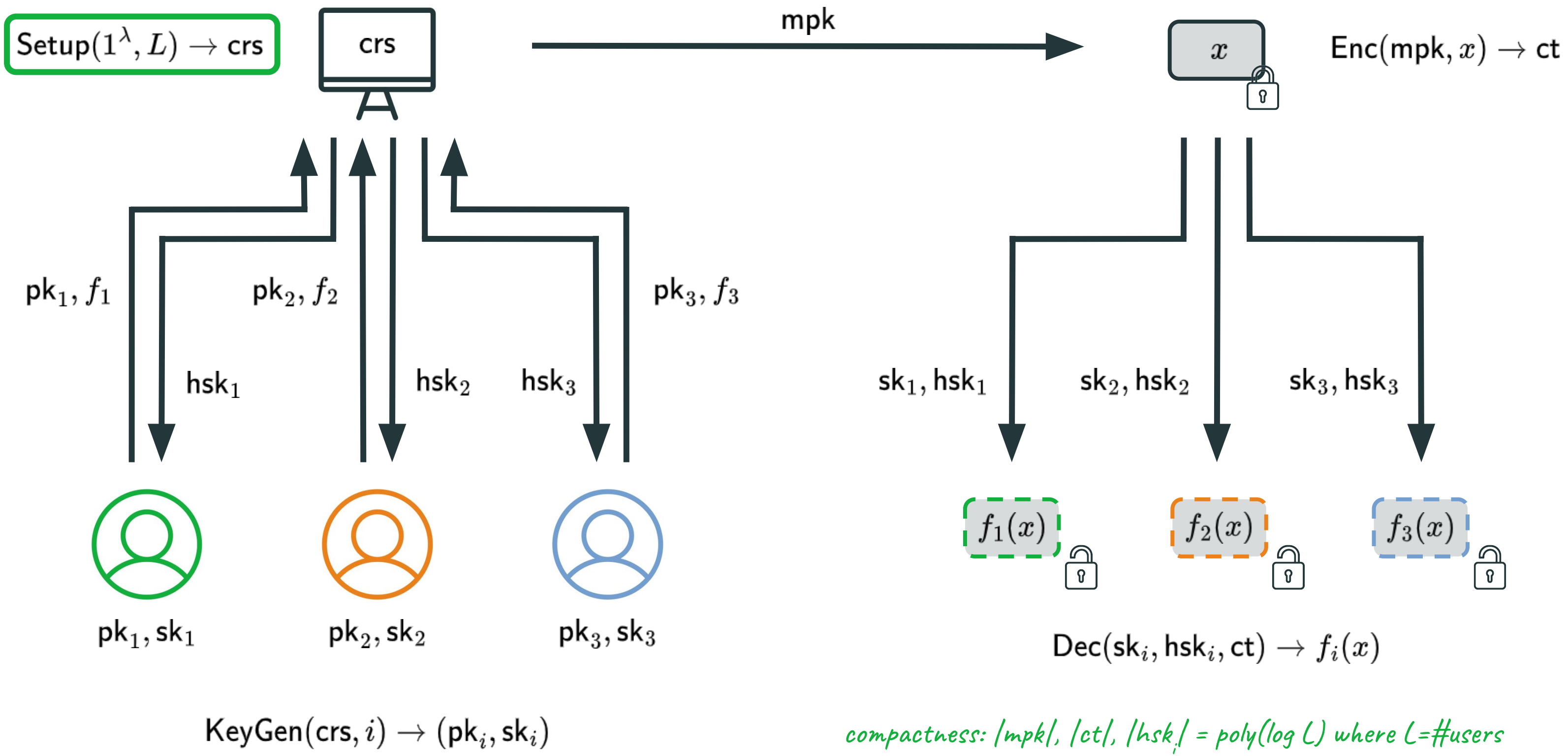
Registered Functional Encryption (RFE) [AC:FFM+23]



Registered Functional Encryption (RFE) [AC:FFM+23]

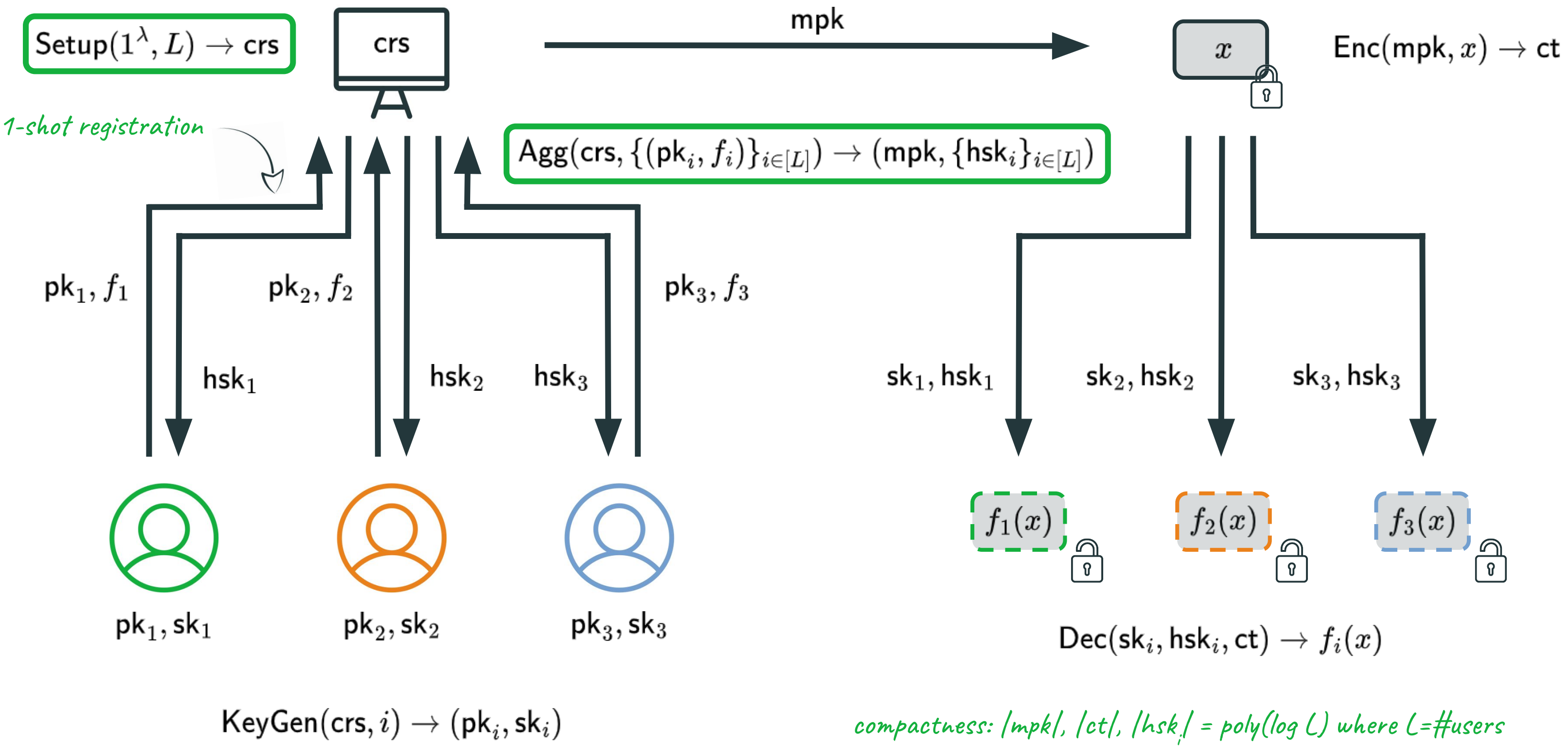


Slotted Registered Functional Encryption (sRFE)

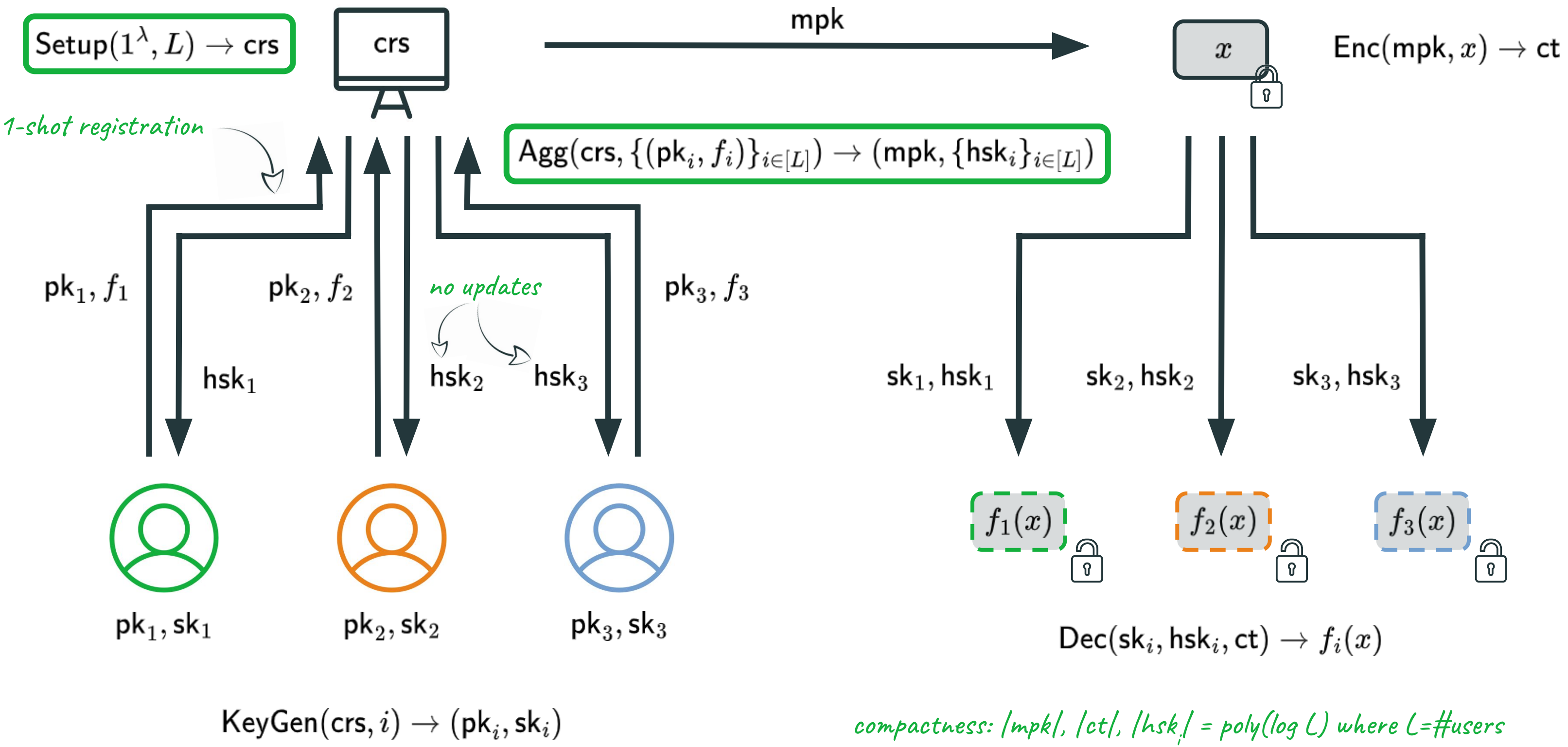


compactness: |mpk|, |ct|, |hsk$_i$| = poly(log L) where L=#users

Slotted Registered Functional Encryption (sRFE)

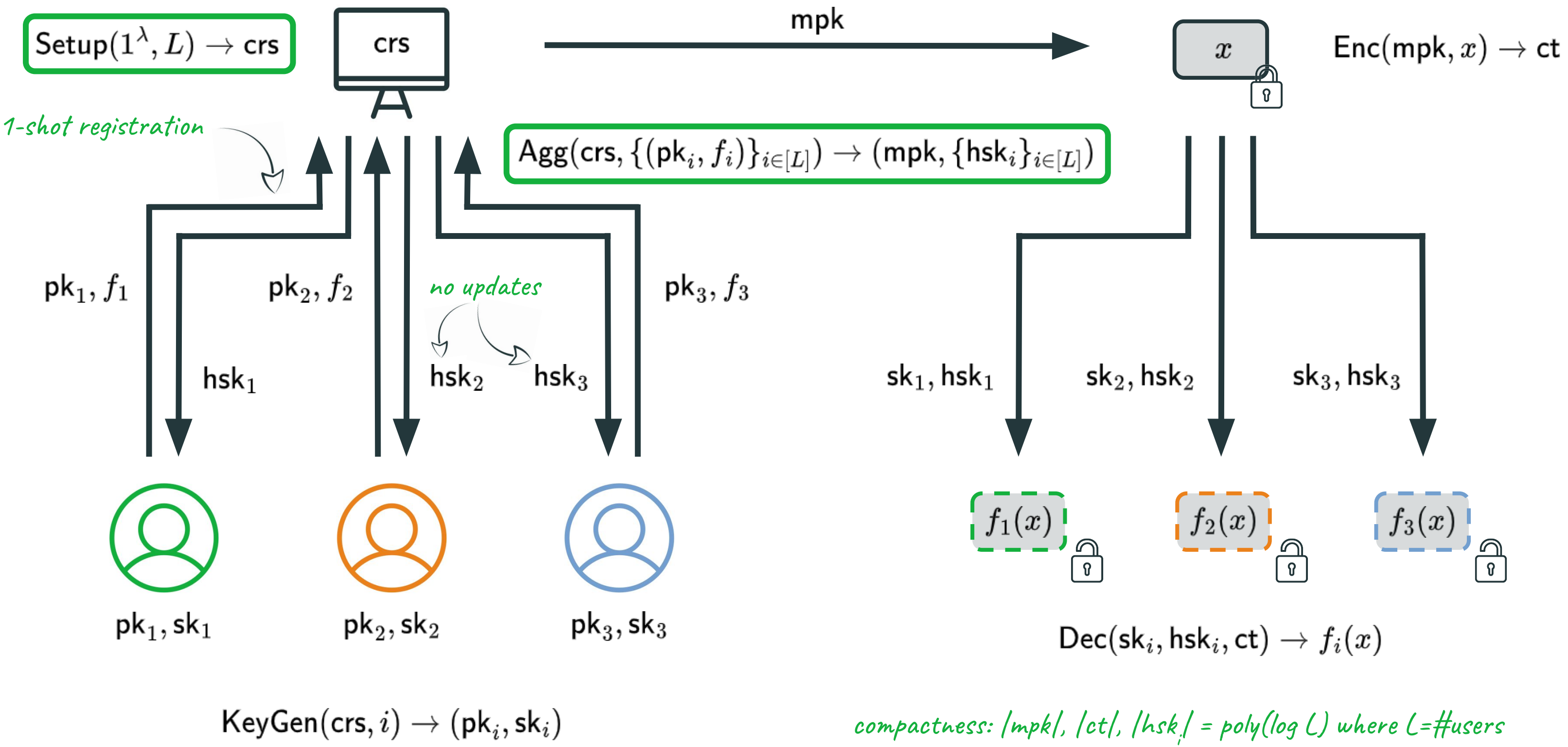


Slotted Registered Functional Encryption (sRFE)

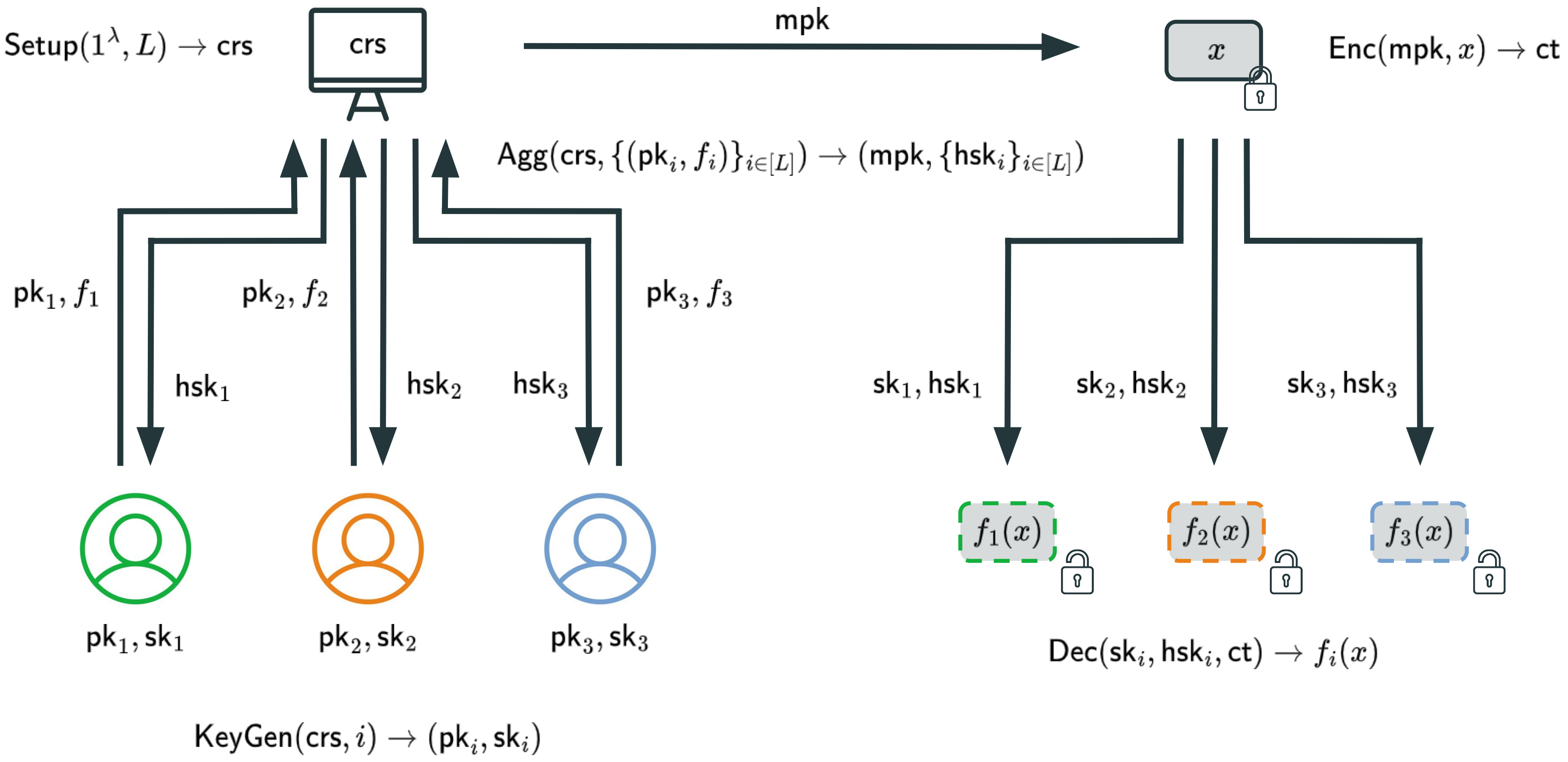


Slotted Registered Functional Encryption (sRFE)

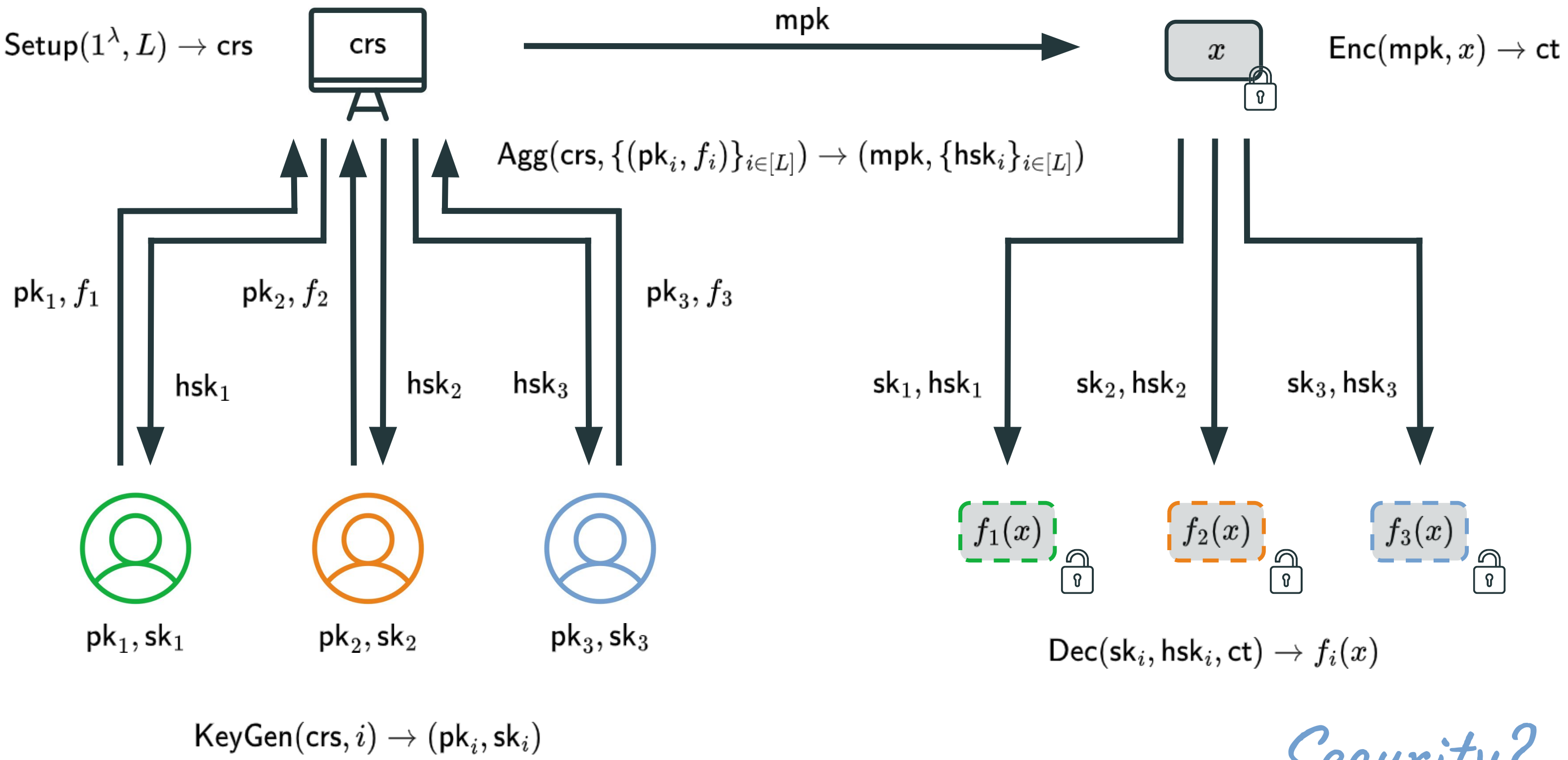
[HLWW23]: sRFE => RFE ("powers-of-two compiler")



Slotted Registered Functional Encryption (sRFE)

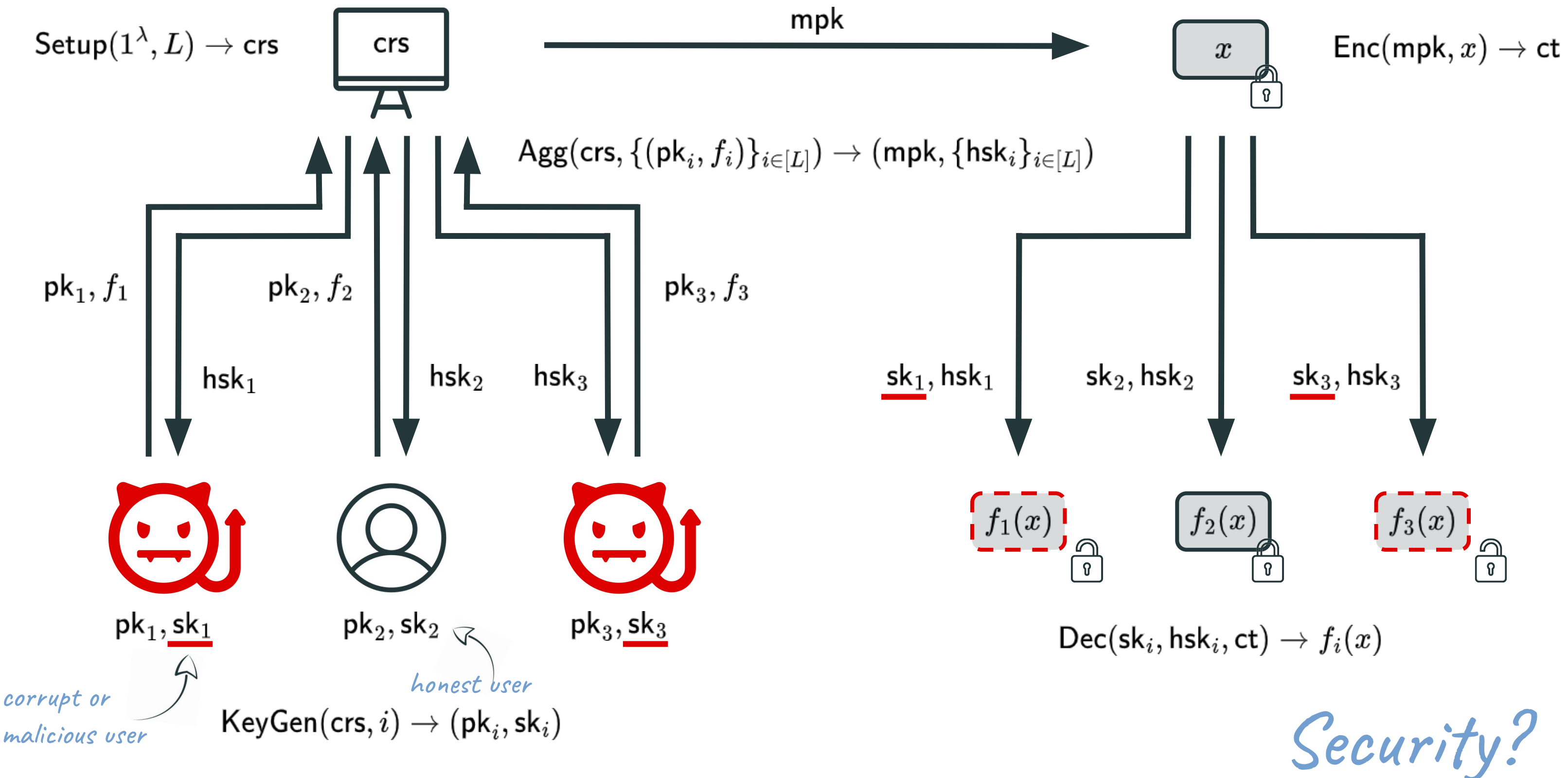


Slotted Registered Functional Encryption (sRFE)

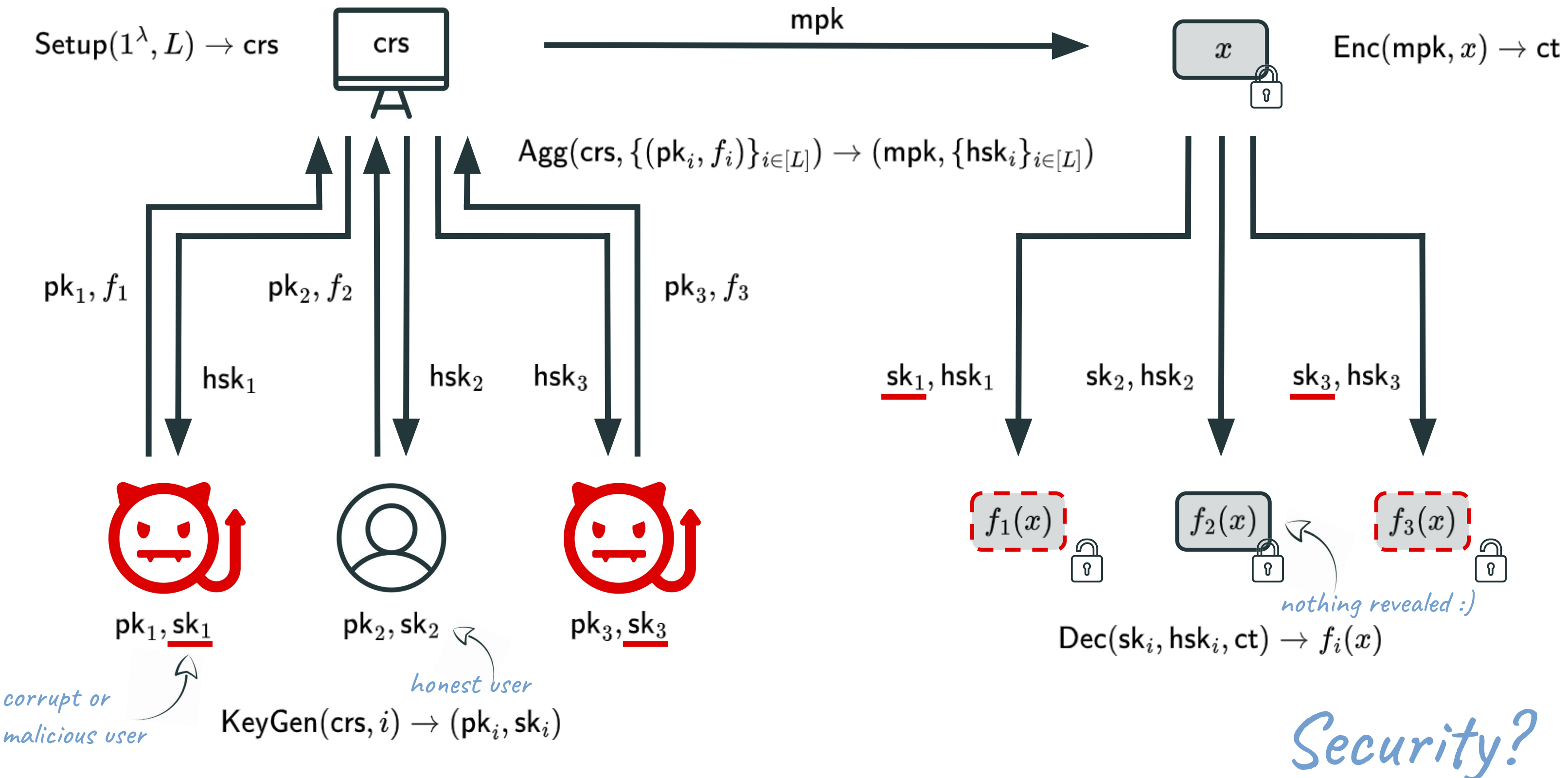


Security?

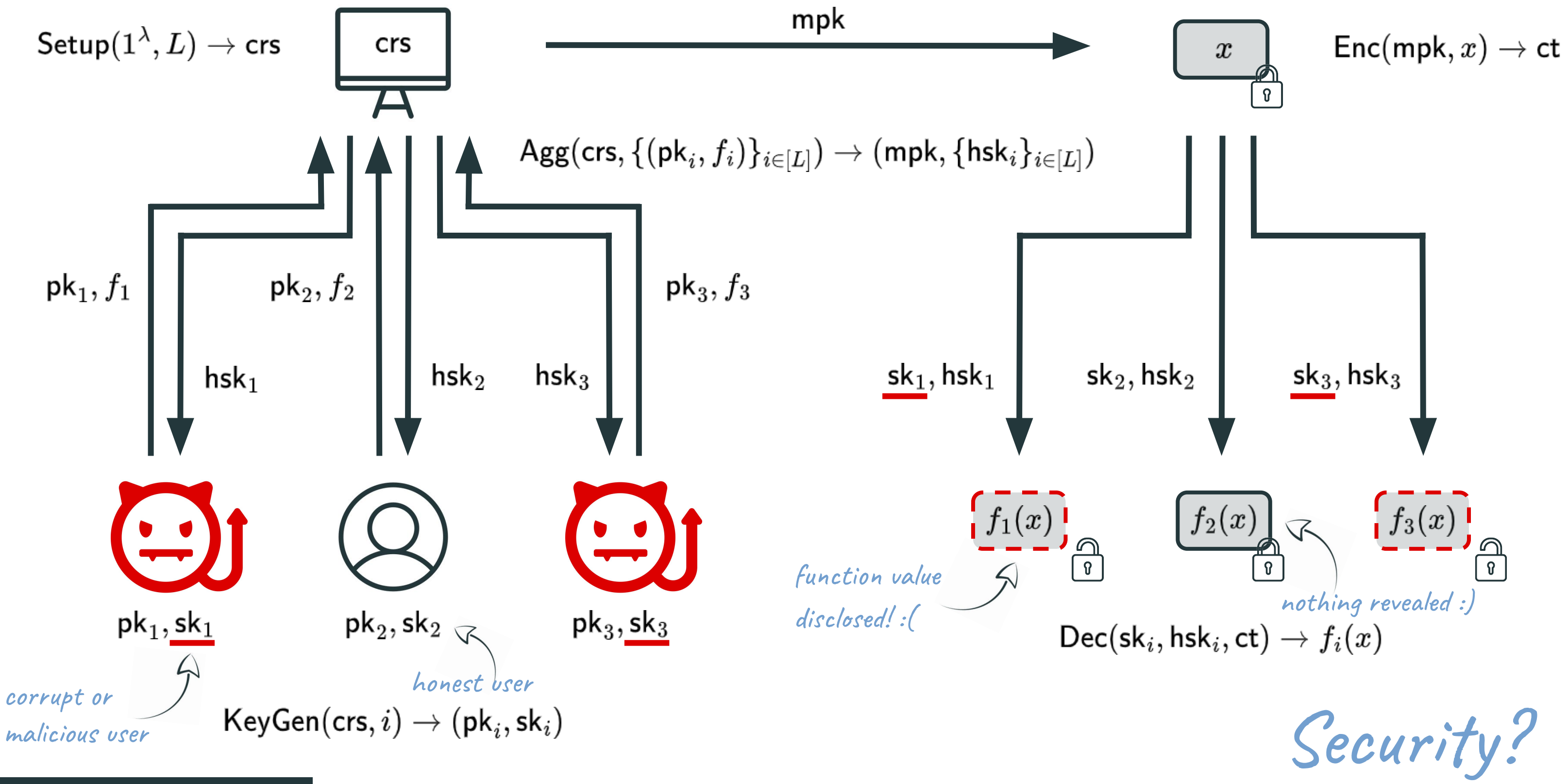
Slotted Registered Functional Encryption (sRFE)



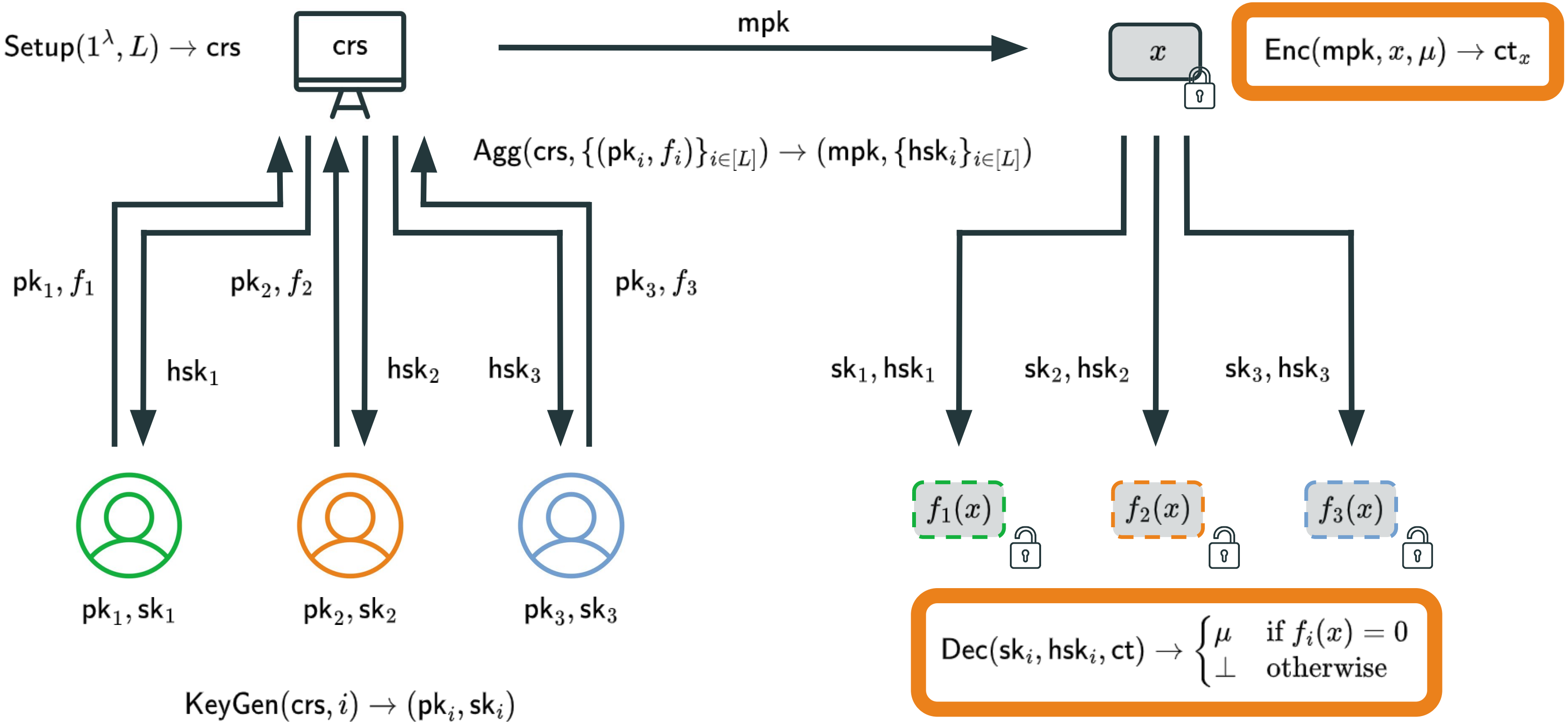
Slotted Registered Functional Encryption (sRFE)



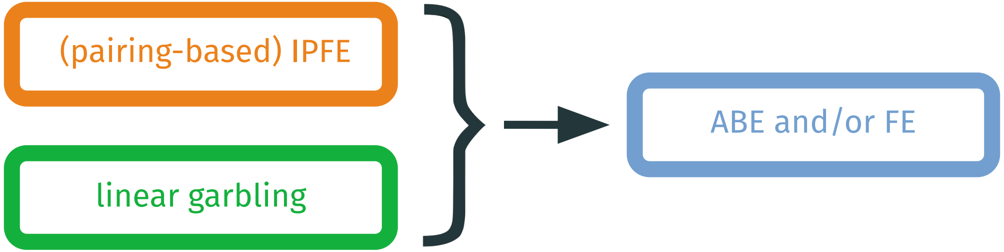
Slotted Registered Functional Encryption (sRFE)



Special Case: Registered ABE



Framework for *Non-Registered* ABE



Framework for *Non-Registered* ABE

(pairing-based) IPFE

linear garbling

$\rightarrow$ ABE and/or FE

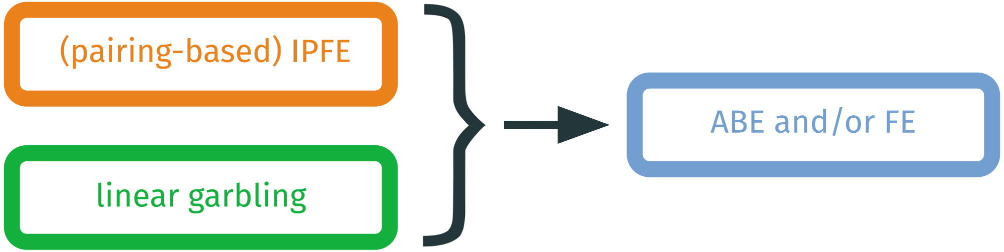
Inner-Product Functional Encryption

$\mathbf{u}$ ict($[\mathbf{u}]_1$)

$\mathbf{v}$ isk($[\mathbf{v}]_2$)

$\rightarrow [\mathbf{u}^\top \mathbf{v}]_t$

Framework for *Non-Registered* ABE



Arithmetic Key Garbling Scheme [EC:LL20]

2-step garbling procedure:

1. given f and secret inputs σ_0, σ_1, output *linear* label functions $L_1(X), \ldots, L_m(X)$ represented by their coefficient vectors $\mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$
2. given public input $\mathbf{x}$, output label vector $\boldsymbol{\ell} = \mathbf{x} \cdot \mathbf{L} = (L_1(\mathbf{x}), \ldots, L_m(\mathbf{x}))$

evaluation: given $f, \mathbf{x}, \boldsymbol{\ell}$, output $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

simulation: given $f, \mathbf{x}, d$, output $\tilde{\ell} \approx \ell$

Framework for *Non-Registered* ABE

$\mathsf{ct}_{\mathbf{x}}$ $\quad \mu \quad \mathbf{x} \quad$ $\mathsf{ict}([(\mu, s, s \cdot \mathbf{x})]_1)$

sk_f $\quad f \quad$ $\mathsf{isk}([(1, \sigma_0, \mathbf{0})]_2), \{\mathsf{isk}([(0, \mathbf{L}[j])]_2)\}_{j \in [m]}$

$$\longrightarrow [\mu + s \cdot \sigma_0]_t, \underline{\{[\mathbf{x} \cdot s \cdot \mathbf{L}[j]]_t\}_{j \in [m]}}$$

Eval(...) -> f(x) · sσ₁ + sσ₀

Inner-Product Functional Encryption

$\mathbf{u}$ $\quad \mathsf{ict}([\mathbf{u}]_1)$

$\mathbf{v}$ $\quad \mathsf{isk}([\mathbf{v}]_2)$

$$\longrightarrow [\mathbf{u}^\top \mathbf{v}]_t$$

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \ell := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

$\mathsf{Sim}(f, \mathbf{x}, d) \to \tilde{\ell}$ s.t. $\tilde{\ell} \approx \ell$

Linearity:

- *labels linear in (1) σ's, r, and (2) x*
- *evaluation linear in labels*

Framework for *Non-Registered* ABE

Security
1. security of IPFE
2. DDH
3. security of AKGS

$\mathsf{ct}_{\mathbf{x}}$ $\boxed{\mu}$ $\mathbf{x}$ $\quad \mathsf{ict}([(\mu, s, s \cdot \mathbf{x})]_1)$

sk_f f $\quad \mathsf{isk}([(1, \sigma_0, \mathbf{0})]_2), \{\mathsf{isk}([(0, \mathbf{L}[j])]_2)\}_{j \in [m]}$

$\longrightarrow [\mu + s \cdot \sigma_0]_t, \underline{\{[\mathbf{x} \cdot s \cdot \mathbf{L}[j]]_t\}_{j \in [m]}}$

Eval(...) -> f(x) · sσ₁ + sσ₀

Inner-Product Functional Encryption

$\boxed{\mathbf{u}}$ $\quad \mathsf{ict}([\mathbf{u}]_1)$

$\mathbf{v}$ $\quad \mathsf{isk}([\mathbf{v}]_2)$

$\longrightarrow [\mathbf{u}^\top \mathbf{v}]_t$

Arithmetic Key Garbling Scheme [EC:LL20]

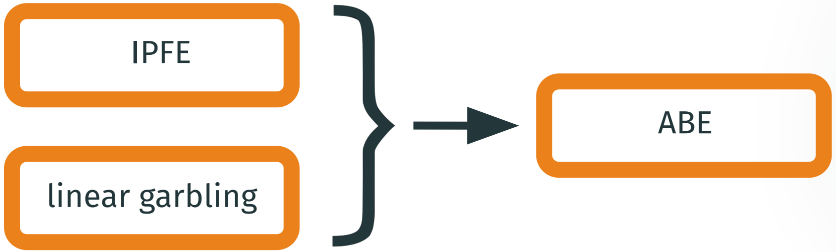
$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \ell := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

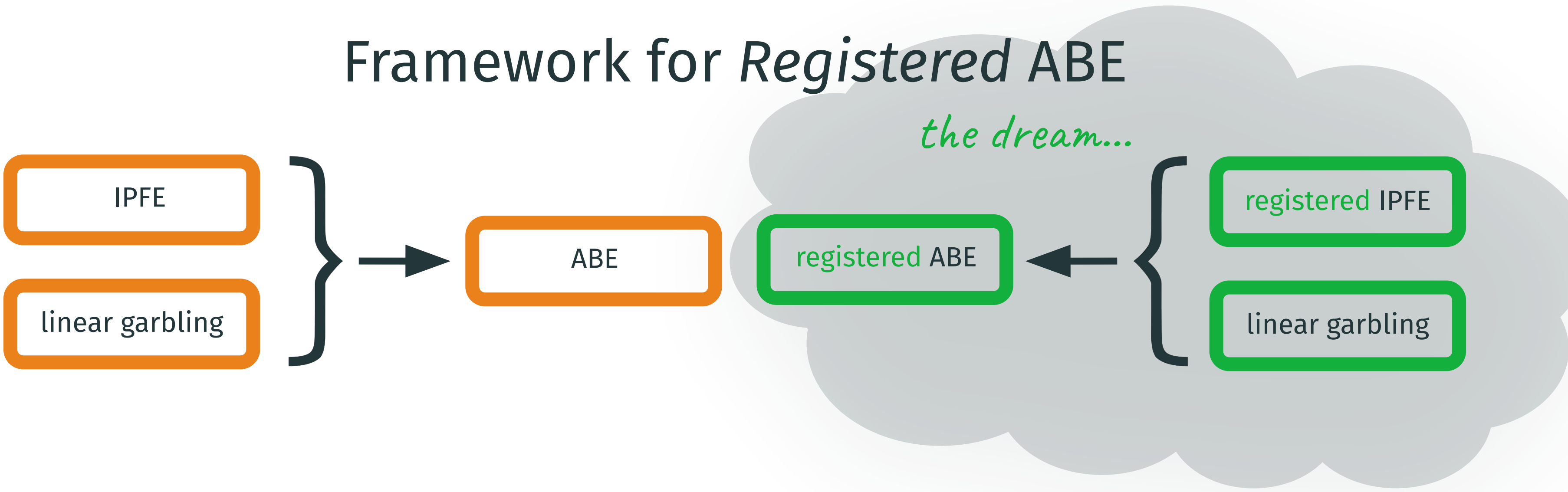
$\mathsf{Sim}(f, \mathbf{x}, d) \to \tilde{\ell}$ s.t. $\tilde{\ell} \approx \ell$

Linearity:
- *labels linear in (1) σ's, r, and (2) x*
- *evaluation linear in labels*

Framework for *Registered* ABE



Framework for *Registered* ABE



Framework for *Registered* ABE

Challenges in the registered setting.

(1) Registered IPFE supporting registration of **vectors over group** unknown

Framework for *Registered* ABE

Challenges in the registered setting.

(1) Registered IPFE supporting registration of **vectors over group** unknown

(2) Sampling of **user-specific** randomness

- key generation performed by (potentially **malicious**) users
- aggregation is **deterministic**
- encryption time is polylogarithmic in number of users (**compactness**)

Framework for *Registered* ABE

Challenges in the registered setting.

(1) Registered IPFE supporting registration of **vectors over group** unknown

(2) Sampling of **user-specific** randomness

- key generation performed by (potentially **malicious**) users
- aggregation is **deterministic**
- encryption time is polylogarithmic in number of users (**compactness**)

Linearity to the rescue. $\mathbf{L} = (\sigma_0, \sigma_1, \mathbf{r}) \cdot \widehat{\mathbf{L}}$ -> **offline/online** phase

RFE for Pre-IP (Batch Variant)

- setup: given matrices $\{[\mathbf{P}_i]_2\}_{i \in [L]}$, output **crs**

RFE for Pre-IP (Batch Variant)

- setup: given matrices $\{[\mathbf{P}_i]_2\}_{i\in[L]}$, output crs
- user key generation: output $(\mathsf{pk}, \mathsf{sk})$
- aggregation: given crs and public key-matrix tuples $\{(\mathsf{pk}_i, \mathbf{V}_i)\}_{i\in[L]}$, output mpk and $\{\mathsf{hsk}_i\}_{i\in[L]}$
- encryption: given mpk and a matrix $[\mathbf{U}]_1$, output ct

RFE for Pre-IP (Batch Variant)

- setup: given matrices $\{[\mathbf{P}_i]_2\}_{i\in[L]}$, output crs
- user key generation: output $(\mathsf{pk}, \mathsf{sk})$
- aggregation: given crs and public key-matrix tuples $\{(\mathsf{pk}_i, \mathbf{V}_i)\}_{i\in[L]}$, output mpk and $\{\mathsf{hsk}_i\}_{i\in[L]}$
- encryption: given mpk and a matrix $[\mathbf{U}]_1$, output ct
- decryption: given $\mathsf{sk}_i, \mathsf{hsk}_i$ and ct, output $[\mathbf{D}]_t = [\mathbf{U}\mathbf{P}_i\mathbf{V}_i]_t$

RFE for Pre-IP (Batch Variant)

- setup: given matrices $\{[\mathbf{P}_i]_2\}_{i\in[L]}$, output crs
- user key generation: output $(\mathsf{pk}, \mathsf{sk})$
- aggregation: given crs and public key-matrix tuples $\{(\mathsf{pk}_i, \mathbf{V}_i)\}_{i\in[L]}$, output mpk and $\{\mathsf{hsk}_i\}_{i\in[L]}$
- encryption: given mpk and a matrix $[\mathbf{U}]_1$, output ct
- decryption: given $\mathsf{sk}_i, \mathsf{hsk}_i$ and ct, output $[\mathbf{D}]_\mathsf{t} = [\mathbf{U}\mathbf{P}_i\mathbf{V}_i]_\mathsf{t}$

Theorem. Assuming bilateral MDDH on pairings, there exists a SIM-secure RFE scheme for Pre-IP.

Proof. (see the paper, based on IND-secure RFE for IP of [EC:ZLZ+24])

How to pick the matrices?

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \boldsymbol{\ell} := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Labels are

- linear in secret input and randomness
- linear in public input

$$\boxed{\boldsymbol{\ell} = \big(\mathbf{x} \otimes (\sigma_0, \sigma_1, \mathbf{r})\big) \cdot \widehat{\mathbf{L}}}$$

How to pick the matrices?

$$[\mathbf{u}]_1 = \left[(\mu, s, \mathbf{x} \otimes s)\right]_1 \qquad [\mathbf{P}_i]_2 = \left[\begin{pmatrix} 1 & \\ \sigma_{i,0} & \\ & \mathbf{I}_{|\mathbf{x}|} \otimes (\sigma_{i,0}, \sigma_{i,1}, \mathbf{r}_i) \end{pmatrix}\right]_2 \qquad \mathbf{V}_i = \begin{pmatrix} 1 & \\ & \widehat{\mathbf{L}}_i \end{pmatrix}$$

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \boldsymbol{\ell} := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Labels are

- linear in secret input and randomness
- linear in public input

$$\boxed{\boldsymbol{\ell} = \left(\mathbf{x} \otimes (\sigma_0, \sigma_1, \mathbf{r})\right) \cdot \widehat{\mathbf{L}}}$$

How to pick the matrices?

$$[\mathbf{u}]_1 = \left[(\mu, s, \mathbf{x} \otimes s)\right]_1 \qquad [\mathbf{P}_i]_2 = \left[\begin{pmatrix} 1 & \\ \sigma_{i,0} & \\ & \mathbf{I}_{|\mathbf{x}|} \otimes (\sigma_{i,0}, \sigma_{i,1}, \mathbf{r}_i) \end{pmatrix}\right]_2 \qquad \mathbf{V}_i = \begin{pmatrix} 1 & \\ & \widehat{\mathbf{L}}_i \end{pmatrix}$$

Correctness. *RIPFE decryption yields* $[\mathbf{d}_i]_t = [\mathbf{u}\mathbf{P}_i\mathbf{V}_i]_t = \left[\left(\mu + s\sigma_{i,0}, \underline{(\mathbf{x} \otimes (s\sigma_{i,0}, s\sigma_{i,1}, s\mathbf{r}_i)) \cdot \widehat{\mathbf{L}}_i}\right)\right]_t$

Eval(...) -> $f_i(x) \cdot s\sigma_{i,1} + s\sigma_{i,0}$

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \ell := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Labels are

- linear in secret input and randomness
- linear in public input

$$\boxed{\ell = (\mathbf{x} \otimes (\sigma_0, \sigma_1, \mathbf{r})) \cdot \widehat{\mathbf{L}}}$$

How to pick the matrices?

$$[\mathbf{u}]_1 = \left[(\mu, s, \mathbf{x} \otimes s)\right]_1 \qquad [\mathbf{P}_i]_2 = \left[\begin{pmatrix} 1 & \\ \sigma_{i,0} & \\ & \mathbf{I}_{|\mathbf{x}|} \otimes (\sigma_{i,0}, \sigma_{i,1}, \mathbf{r}_i) \end{pmatrix}\right]_2 \qquad \mathbf{V}_i = \begin{pmatrix} 1 & \\ & \widehat{\mathbf{L}}_i \end{pmatrix}$$

Security. *RIPFE leakage is* $[\mathbf{d}_i]_{\mathsf{t}_{1,2}} = [\mathbf{u}\mathbf{P}_i\mathbf{V}_i]_{\mathsf{t}_{1,2}} = \left[\left(\mu + s\overset{\$}{\sigma}_{i,0}, \underline{(\mathbf{x} \otimes (s\overset{\$}{\sigma}_{i,0}, s\overset{\$}{\sigma}_{i,1}, s\overset{\$}{\mathbf{r}}_i)) \cdot \widehat{\mathbf{L}}_i}\right)\right]_{\mathsf{t}_{1,2}}$

indistinguishable from Sim(f, x, d <-$)

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \boldsymbol{\ell} := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Labels are

- linear in secret input and randomness
- linear in public input

$$\boxed{\boldsymbol{\ell} = (\mathbf{x} \otimes (\sigma_0, \sigma_1, \mathbf{r})) \cdot \widehat{\mathbf{L}}}$$

How to pick the matrices?

$$[\mathbf{u}]_1 = \left[(\mu, s, \mathbf{x} \otimes s)\right]_1$$

$$[\mathbf{P}_i]_2 = \left[\begin{pmatrix} 1 & \\ \sigma_{i,0} & \\ & \mathbf{I}_{|\mathbf{x}|} \otimes (\sigma_{i,0}, \sigma_{i,1}, \mathbf{r}_i) \end{pmatrix}\right]_2$$

$$\mathbf{V}_i = \begin{pmatrix} 1 & \\ & \widehat{\mathbf{L}}_i \end{pmatrix}$$

What about Turing machines?

Problem: shape of L and r depends on input length, runtime and space -> only known during encryption :(

$$[\mathbf{d}_i]_{\mathrm{t}} = [\mathbf{u}\mathbf{P}_i\mathbf{V}_i]_{\mathrm{t}} = \left[\left(\mu + s\sigma_{i,0}, (\mathbf{x} \otimes (s\sigma_{i,0}, s\sigma_{i,1}, s\mathbf{r}_i)) \cdot \widehat{\mathbf{L}}_i\right)\right]_{\mathrm{t}}$$

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \boldsymbol{\ell} := \mathbf{x} \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Labels are

- linear in secret input and randomness
- linear in public input

$$\boldsymbol{\ell} = (\mathbf{x} \otimes (\sigma_0, \sigma_1, \mathbf{r})) \cdot \widehat{\mathbf{L}}$$

Arithmetization of TM Computations

- consider TM $M = (Q, \mathbf{y}_{\mathsf{acc}}, \delta)$ and denote by (N, S, T) the input length, space and runtime

Arithmetization of TM Computations

- consider TM $M = (Q, \mathbf{y}_{\mathsf{acc}}, \delta)$ and denote by (N, S, T) the input length, space and runtime
- set of internal configurations $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$ with initial configuration $\boldsymbol{c}_0 = (\mathbf{1}, \mathbf{1}, \mathbf{0}_S, \mathbf{1})$

  (input tape head, working tape head, working tape, state)

Arithmetization of TM Computations

- consider TM $M = (Q, \mathbf{y}_{\mathsf{acc}}, \delta)$ and denote by (N, S, T) the input length, space and runtime
- set of internal configurations $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$ with initial configuration $\boldsymbol{c}_0 = (\mathbf{1}, \mathbf{1}, \mathbf{0}_S, \mathbf{1})$

  (input tape head, working tape head, working tape, state)
- define transition matrix $\mathbf{T}(\mathbf{x}) \in \mathbb{Z}_p^{\mathcal{C} \times \mathcal{C}}$ as

$$\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } c \to_M c' \\ 0 & \text{otherwise} \end{cases}$$

c' = (k', j', w', q') c = (k, j, w, q)

Arithmetization of TM Computations

- consider TM $M = (Q, \mathbf{y}_{\mathsf{acc}}, \delta)$ and denote by (N, S, T) the input length, space and runtime
- set of internal configurations $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$ with initial configuration $\boldsymbol{c}_0 = (\mathbf{1}, \mathbf{1}, \mathbf{0}_S, \mathbf{1})$

  (input tape head, working tape head, working tape, state)

- define transition matrix $\mathbf{T}(\mathbf{x}) \in \mathbb{Z}_p^{\mathcal{C} \times \mathcal{C}}$ as

$$\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } c \to_M c' \\ 0 & \text{otherwise} \end{cases}$$

$c' = (k', j', w', q')$ $\qquad$ $c = (k, j, w, q)$

- we have $\mathbf{T}(\mathbf{x}) \cdot \mathbf{e}_c^\top = \mathbf{e}_{c'}^\top$

Arithmetization of TM Computations

- consider TM $M = (Q, \mathbf{y}_{\mathsf{acc}}, \delta)$ and denote by (N, S, T) the input length, space and runtime
- set of internal configurations $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$ with initial configuration $c_0 = (1, 1, \mathbf{0}_S, 1)$

  (input tape head, working tape head, working tape, state)
- define transition matrix $\mathbf{T}(\mathbf{x}) \in \mathbb{Z}_p^{\mathcal{C} \times \mathcal{C}}$ as

$$\mathbf{T}(\mathbf{x})[\underbrace{c'}_{c' = (k', j', w', q')}, \underbrace{c}_{c = (k, j, w, q)}] = \begin{cases} 1 & \text{if } c \to_M c' \\ 0 & \text{otherwise} \end{cases}$$

- we have $\mathbf{T}(\mathbf{x}) \cdot \mathbf{e}_c^\top = \mathbf{e}_{c'}^\top$ and more general

$$\boxed{M|_{N,S,T}(\mathbf{x}) = (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \cdot (\mathbf{T}(\mathbf{x}))^T \cdot \mathbf{e}_{c_0}^\top}$$

Arithmetization of TM Computations

- consider TM $M = (Q, \mathbf{y}_{\mathsf{acc}}, \delta)$ and denote by (N, S, T) the input length, space and runtime
- set of internal configurations $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$ with initial configuration $c_0 = (1, 1, \mathbf{0}_S, 1)$

  (input tape head, working tape head, working tape, state)
- define transition matrix $\mathbf{T}(\mathbf{x}) \in \mathbb{Z}_p^{\mathcal{C} \times \mathcal{C}}$ as

$$\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } c \to_M c' \\ 0 & \text{otherwise} \end{cases}$$

c' = (k', j', w', q') *c = (k, j, w, q)*

- we have $\mathbf{T}(\mathbf{x}) \cdot \mathbf{e}_c^\top = \mathbf{e}_{c'}^\top$ and more general

$$\boxed{M|_{N,S,T}(\mathbf{x}) = (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \cdot (\mathbf{T}(\mathbf{x}))^T \cdot \mathbf{e}_{c_0}^\top}$$

*... so we only need to garble **matrix multiplication***

Arithmetic Key Garbling for Logspace TMs [EC:LL20]

- garbling: sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$$\begin{aligned} L_{\mathsf{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \\ L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) \\ L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \end{aligned}$$

Arithmetic Key Garbling for Logspace TMs [EC:LL20]

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$$
\begin{aligned}
L_{\mathsf{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \\
L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) \\
L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})
\end{aligned}
$$

- **evaluation:** given labels $\ell_{\mathsf{init}} := L_{\mathsf{init}}(\mathbf{x})$, $\{\boldsymbol{\ell}_t := L_t(\mathbf{x})\}_{t \in [T+1]}$, output

$$
\ell_{\mathsf{init}} + \sum_{t \in [T+1]} \boldsymbol{\ell}_t \cdot \mathbf{T}(\mathbf{x})^{t-1} \cdot \mathbf{e}_{c_0}^\top
$$

Arithmetic Key Garbling for Logspace TMs [EC:LL20]

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$$
\begin{aligned}
L_{\mathsf{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \\
L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) \\
L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot \big(\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}\big)
\end{aligned}
$$

- **evaluation:** given labels $\ell_{\mathsf{init}} := L_{\mathsf{init}}(\mathbf{x}),\ \{\boldsymbol{\ell}_t := L_t(\mathbf{x})\}_{t \in [T+1]}$, output

$$
\ell_{\mathsf{init}} + \sum_{t \in [T+1]} \boldsymbol{\ell}_t \cdot \mathbf{T}(\mathbf{x})^{t-1} \cdot \mathbf{e}_{c_0}^\top = \sigma_0 + \sigma_1 (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \cdot \mathbf{T}(\mathbf{x})^T \cdot \mathbf{e}_{c_0}^\top
$$

telescoping sum

Arithmetic Key Garbling for Logspace TMs [EC:LL20]

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$$\begin{aligned} L_{\mathsf{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \\ L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) \\ L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot \left(\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}\right) \end{aligned}$$

- **evaluation:** given labels $\ell_{\mathsf{init}} := L_{\mathsf{init}}(\mathbf{x})$, $\{\boldsymbol{\ell}_t := L_t(\mathbf{x})\}_{t \in [T+1]}$, output

$$\ell_{\mathsf{init}} + \sum_{t \in [T+1]} \boldsymbol{\ell}_t \cdot \mathbf{T}(\mathbf{x})^{t-1} \cdot \mathbf{e}_{c_0}^\top = \sigma_0 + \sigma_1 (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \cdot \mathbf{T}(\mathbf{x})^T \cdot \mathbf{e}_{c_0}^\top = \sigma_0 + \sigma_1 \cdot M|_{N,S,T}(\mathbf{x})$$

telescoping sum

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\text{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\text{acc}})$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\text{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^{\top}$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\text{acc}})$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_{\text{init}}(\mathbf{x}) = s \cdot \sigma_0 + (\mathbf{r}_{\mathsf{x},0} \otimes \mathbf{r}_{\mathsf{f}})[1, 1, \mathbf{0}_S, 1]$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0, 1\}^S \times [Q]$

$$
\begin{aligned}
L_{\mathsf{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \\
L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) \\
L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})
\end{aligned}
$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$
L_{\mathsf{init}}(\mathbf{x}) = s \cdot \sigma_0 + (\mathbf{r}_{\mathsf{x},0} \otimes \mathbf{r}_{\mathsf{f}})[1, 1, \mathbf{0}_S, 1] = s \cdot \sigma_0 + \mathbf{r}_{\mathsf{x},0}[1, 1, \mathbf{0}_S] \cdot \mathbf{r}_{\mathsf{f}}[1]
$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_{\mathsf{init}}(\mathbf{x}) = s \cdot \sigma_0 + (\mathbf{r}_{\mathsf{x},0} \otimes \mathbf{r}_{\mathsf{f}})[1, 1, \mathbf{0}_S, 1] = \overbrace{s \cdot \sigma_0 + \mathbf{r}_{\mathsf{x},0}[1, 1, \mathbf{0}_S]}^{u} \cdot \underbrace{\mathbf{r}_{\mathsf{f}}[1]}_{P_i}$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})$$

✔

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

u

$$L_{\mathsf{init}}(\mathbf{x}) = s \cdot \sigma_0 + (\mathbf{r}_{\mathsf{x},0} \otimes \mathbf{r}_{\mathsf{f}})[1,1,\mathbf{0}_S,1] = s \cdot \sigma_0 + \mathbf{r}_{\mathsf{x},0}[1,1,\mathbf{0}_S] \cdot \mathbf{r}_{\mathsf{f}}[1]$$

P_i

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\text{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\text{acc}})$$

✔

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_{T+1}[\underbrace{k, j, \mathbf{w}}_{=:\,\underline{c}}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},T} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + s \cdot \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\text{acc}})[\underline{c}, q]$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})$$

✔

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_{T+1}[\underbrace{k, j, \mathbf{w}}_{=: \underline{c}}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},T} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + s \cdot \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})[\underline{c}, q] = -\mathbf{r}_{\mathsf{x},T}[\underline{c}] \cdot \mathbf{r}_{\mathsf{f}}[q] + s \cdot \sigma_1 \cdot \mathbf{y}_{\mathsf{acc}}[q]$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})$$

✔

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_{T+1}[\underbrace{k, j, \mathbf{w}}_{=:\underline{c}}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},T} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + s \cdot \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})[\underline{c}, q] = -\mathbf{r}_{\mathsf{x},T}[\underline{c}] \cdot \mathbf{r}_{\mathsf{f}}[q] + s \cdot \sigma_1 \cdot \mathbf{y}_{\mathsf{acc}}[q]$$

u V_i P_i

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$
\begin{aligned}
L_{\mathsf{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \\
L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) \\
L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})
\end{aligned}
$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$u \qquad V_i$

$$
L_{T+1}[\underbrace{k, j, \mathbf{w}}_{=:\, \underline{c}}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},T} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + s \cdot \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})[\underline{c}, q] = -\mathbf{r}_{\mathsf{x},T}[\underline{c}] \cdot \mathbf{r}_{\mathsf{f}}[q] + s \cdot \sigma_1 \cdot \mathbf{y}_{\mathsf{acc}}[q]
$$

P_i

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \quad ✔$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \quad ✔$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_t[\underline{c}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},t-1} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + \big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q]$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \dots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top \quad ✔$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}}) \quad ✔$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_t[\underline{c}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},t-1} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + \big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q] = -\mathbf{r}_{\mathsf{x},t-1}[\underline{c}] \cdot \mathbf{r}_{\mathsf{f}}[q] + \big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q]$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

  $\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$L_{\mathsf{init}}(\mathbf{x}) = \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top$$
$$L_t(\mathbf{x}) = -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x})$$
$$L_{T+1}(\mathbf{x}) = -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\mathsf{acc}})$$

✔ ✔

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_t[\underline{c}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},t-1} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + \big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q] = -\overset{u}{\mathbf{r}_{\mathsf{x},t-1}[\underline{c}]} \cdot \underset{P_i}{\mathbf{r}_{\mathsf{f}}[q]} + \big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q]$$

Decomposition of the Labels

- **garbling:** sample $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_T \leftarrow_\$ \mathbb{Z}_p^{\mathcal{C}}$ and output label functions

$\mathcal{C} = [N] \times [S] \times \{0,1\}^S \times [Q]$

$$\begin{aligned} L_{\text{init}}(\mathbf{x}) &= \sigma_0 + \mathbf{r}_0 \cdot \mathbf{e}_{c_0}^\top & ✔ \\ L_t(\mathbf{x}) &= -\mathbf{r}_{t-1} + \mathbf{r}_t \cdot \mathbf{T}(\mathbf{x}) & ✘ \\ L_{T+1}(\mathbf{x}) &= -\mathbf{r}_T + \sigma_1 \cdot (\mathbf{1} \otimes \mathbf{y}_{\text{acc}}) & ✔ \end{aligned}$$

- **idea:** set $\mathbf{r}_t = \mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}$ where $\mathbf{r}_{\mathsf{x},t} \leftarrow_\$ \mathbb{Z}_p^{[N]\times[S]\times\{0,1\}^S}$ and $\mathbf{r}_{\mathsf{f}} \leftarrow_\$ \mathbb{Z}_p^{[Q]}$
- **decomposition of the labels:**

$$L_t[\underline{c}, q](\mathbf{x}) = -(\mathbf{r}_{\mathsf{x},t-1} \otimes \mathbf{r}_{\mathsf{f}})[\underline{c}, q] + \big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q] = -\overset{u}{\mathbf{r}_{\mathsf{x},t-1}[\underline{c}]} \cdot \underset{P_i}{\mathbf{r}_{\mathsf{f}}[q]} + \underbrace{\big((\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})\big)[\underline{c}, q]}_{?}$$

Block Structure of Transition Matrix

- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k' - k, j' - j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

$c' = (k', j', w', q')$ $c = (k, j, w, q)$

Block Structure of Transition Matrix

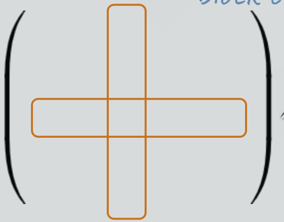
- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k' - k, j' - j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

  $c' = (k', j', w', q')$ $\qquad$ $c = (k, j, w, q)$

- consider Q x Q blocks $\mathbf{T}(\mathbf{x})[(\underbrace{k', j', \mathbf{w}'}_{\underline{c}'}, \_), (\underbrace{k, j, \mathbf{w}}_{\underline{c}}, \_)]$

block column $(\underline{c} = (k, j, w), \_)$

block row $(\underline{c}' = (k', j', w'), \_)$

$\mathbf{T}(\mathbf{x}) =$ 

Block Structure of Transition Matrix

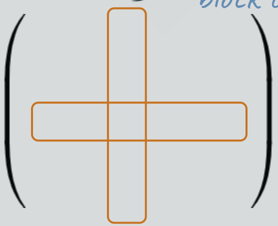
- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k' - k, j' - j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

  $c' = (k', j', w', q')$ $c = (k, j, w, q)$

- consider *Q* x *Q* blocks $\mathbf{T}(\mathbf{x})[\underbrace{(k', j', \mathbf{w}'}_{\underline{c}'}, \_), \underbrace{(k, j, \mathbf{w}}_{\underline{c}}, \_)]$

  -> either zero matrix

$\mathbf{T}(\mathbf{x}) =$



block column $(\underline{c} = (k, j, w), \_)$

block row $(\underline{c}' = (k', j', w'), \_)$

Block Structure of Transition Matrix

- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k' - k, j' - j),\ \ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

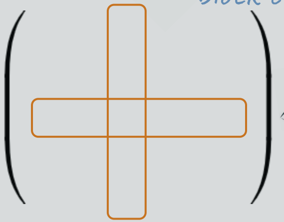
  $c' = (k', j', w', q')$ $c = (k, j, w, q)$

- consider Q x Q blocks $\mathbf{T}(\mathbf{x})[(\underbrace{k', j', \mathbf{w}'}_{\underline{c}'}, \_), (\underbrace{k, j, \mathbf{w}}_{\underline{c}}, \_)]$

  -> either zero matrix
  -> or "**transition block**" in $\mathcal{B} = \left\{ \mathbf{B}_{x,w,w',\Delta k,\Delta j} \middle| x, w, w' \in \{0,1\},\ \Delta k, \Delta j \in \{0, \pm 1\} \right\}$

block column ($\underline{c}=(k, j, w), \_$)

block row ($\underline{c}'=(k', j', w'), \_$)

$\mathbf{T}(\mathbf{x}) =$ 

Block Structure of Transition Matrix

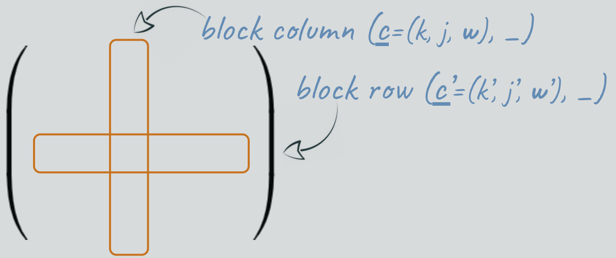
- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k'-k, j'-j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

  $c' = (k', j', w', q')$ $\quad$ $c = (k, j, w, q)$

- consider Q x Q blocks $\mathbf{T}(\mathbf{x})[(\underbrace{k', j', \mathbf{w}'}_{\underline{c}'}, \_), (\underbrace{k, j, \mathbf{w}}_{\underline{c}}, \_)]$

  -> either zero matrix
  -> or "**transition block**" in $\mathcal{B} = \left\{ \mathbf{B}_{x,w,w',\Delta k,\Delta j} \middle| x, w, w' \in \{0,1\},\ \Delta k, \Delta j \in \{0, \pm 1\} \right\}$

- **observation:** each $\mathbf{B}_{x,w,w',\Delta k,\Delta j}$ appears at most once per "block column"

$\mathbf{T}(\mathbf{x}) =$ 

Block Structure of Transition Matrix

- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k'-k, j'-j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

  $c' = (k', j', w', q')$ $c = (k, j, w, q)$

- consider Q x Q blocks $\mathbf{T}(\mathbf{x})[\underbrace{(k', j', \mathbf{w}'}_{\underline{c'}}, \_), \underbrace{(k, j, \mathbf{w}}_{\underline{c}}, \_)]$

  -> either zero matrix
  -> or "**transition block**" in $\mathcal{B} = \{\mathbf{B}_{x,w,w',\Delta k,\Delta j} \mid x, w, w' \in \{0,1\},\ \Delta k, \Delta j \in \{0, \pm 1\}\}$

- **observation:** each $\mathbf{B}_{x,w,w',\Delta k,\Delta j}$ appears at most once per "block column"

decomposition of the last term:

$$(\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})[(\_, \_), (\underline{c}, q)]$$

Block Structure of Transition Matrix

- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k'-k, j'-j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

  $c' = (k', j', w', q')$ $c = (k, j, w, q)$

- consider Q x Q blocks $\mathbf{T}(\mathbf{x})[\underbrace{(k', j', \mathbf{w}'}_{\underline{c'}}, \_), \underbrace{(k, j, \mathbf{w}}_{\underline{c}}, \_)]$

  -> either zero matrix
  -> or "**transition block**" in $\mathcal{B} = \{\mathbf{B}_{x,w,w',\Delta k,\Delta j} \,|\, x, w, w' \in \{0,1\},\ \Delta k, \Delta j \in \{0, \pm 1\}\}$

- **observation:** each $\mathbf{B}_{x,w,w',\Delta k,\Delta j}$ appears at most once per "block column", position independent of $\mathbf{x}$

decomposition of the last term:

$$(\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})[(\_, \_), (\underline{c}, q)] = \sum_{w', \Delta k, \Delta j} \mathbf{r}_{\mathsf{x},t}[c'] \cdot \mathbf{r}_{\mathsf{f}}[q] \cdot \mathbf{B}_{\mathbf{x}[k], \mathbf{w}[j], w', \Delta k, \Delta j}$$

Block Structure of Transition Matrix

- transition matrix $\mathbf{T}(\mathbf{x})[c', c] = \begin{cases} 1 & \text{if } \delta(q, \mathbf{x}[k], \mathbf{w}[j]) = (q', \mathbf{w}'[j], k'-k, j'-j),\ \mathbf{w}[\neq j] = \mathbf{w}'[\neq j] \\ 0 & \text{otherwise} \end{cases}$

  $c' = (k', j', w', q')$ $c = (k, j, w, q)$

- consider Q x Q blocks $\mathbf{T}(\mathbf{x})[(\underbrace{k', j', \mathbf{w}'}_{c'}, \_), (\underbrace{k, j, \mathbf{w}}_{c}, \_)]$

  -> either zero matrix
  -> or "**transition block**" in $\mathcal{B} = \{\mathbf{B}_{x,w,w',\Delta k,\Delta j} \mid x, w, w' \in \{0,1\},\ \Delta k, \Delta j \in \{0, \pm 1\}\}$

- **observation:** each $\mathbf{B}_{x,w,w',\Delta k,\Delta j}$ appears at most once per "block column", position independent of $\mathbf{x}$

decomposition of the last term:

$$(\mathbf{r}_{\mathsf{x},t} \otimes \mathbf{r}_{\mathsf{f}}) \cdot \mathbf{T}(\mathbf{x})[(\_, \_), (\underline{c}, q)] = \sum_{w', \Delta k, \Delta j} \overbrace{\mathbf{r}_{\mathsf{x},t}[c']}^{u} \cdot \underbrace{\mathbf{r}_{\mathsf{f}}[q]}_{P_i} \cdot \overbrace{\mathbf{B}_{\mathbf{x}[k], \mathbf{w}[j], w', \Delta k, \Delta j}}^{V_i}$$

Generalization to RFE

- so far, we used $\boldsymbol{\sigma_0}$ as a pad for (a fixed message) $\boldsymbol{\mu}$ and $\boldsymbol{\sigma_1}$ as a masking term

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \ell := (1, \mathbf{x}) \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Generalization to RFE

- so far, we used $\boldsymbol{\sigma_0}$ as a pad for (a fixed message) $\boldsymbol{\mu}$ and $\boldsymbol{\sigma_1}$ as a masking term
- more general, we can
  - encode data in $\boldsymbol{\sigma_1}$
    -> attribute-weighted sums functionalities

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \ell := (1, \mathbf{x}) \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Generalization to RFE

- so far, we used $\boldsymbol{\sigma_0}$ as a pad for (a fixed message) $\boldsymbol{\mu}$ and $\boldsymbol{\sigma_1}$ as a masking term
- more general, we can
  - encode data in $\boldsymbol{\sigma_1}$
    -> attribute-weighted sums functionalities
  - use $\boldsymbol{\sigma_0}$ as pad for any other (independently computed) RFE functionality
    -> attribute-based functionalities (AB-AWS, AB-QF)

Arithmetic Key Garbling Scheme [EC:LL20]

$\mathsf{Garble}(f, \sigma_0, \sigma_1; \mathbf{r}) \to \mathbf{L} = (\mathbf{L}[1], \ldots, \mathbf{L}[m])$

$\mathsf{Eval}(f, \mathbf{x}, \ell := (1, \mathbf{x}) \cdot \mathbf{L}) \to d$ s.t. $d = \sigma_1 f(\mathbf{x}) + \sigma_0$

Conclusion

- classical FE provides security against malicious user but needs to trust authority
- registered FE circumvents the need for trusted authority

Conclusion

- **classical FE** provides security against malicious user but needs to trust authority
- **registered FE** circumvents the need for trusted authority

- **this work:** adapt modular framework from classical to registered setting to obtain
  - RABE for **logspace TMs**
  - RFE for **AB-AWS** and **AB-QF**

Conclusion

- **classical FE** provides security against malicious user but needs to trust authority
- **registered FE** circumvents the need for trusted authority

- **this work:** adapt modular framework from classical to registered setting to obtain
  - RABE for **logspace TMs**
  - RFE for **AB-AWS** and **AB-QF**

- **on-going work:**
  - realize framework from lattices (evasive RFE for Pre-IP + noisy linear garbling scheme)

Conclusion

- **classical FE** provides security against malicious user but needs to trust authority
- **registered FE** circumvents the need for trusted authority

- **this work:** adapt modular framework from classical to registered setting to obtain
  - RABE for **logspace TMs**
  - RFE for **AB-AWS** and **AB-QF**

- **on-going work:**
  - realize framework from lattices (evasive RFE for Pre-IP + noisy linear garbling scheme)

- **open problems:**
  - (pairings) adaptive security, compression of CRS
  - (lattices) weaker, falsifiable assumptions

Conclusion

- **classical FE** provides security against malicious user but needs to trust authority
- **registered FE** circumvents the need for trusted authority

- **this work:** adapt modular framework from classical to registered setting to obtain
  - RABE for **logspace TMs**
  - RFE for **AB-AWS** and **AB-QF**

- **on-going work:**
  - realize framework from lattices (evasive RFE for Pre-IP + noisy linear garbling scheme)

- **open problems:**
  - (pairings) adaptive security, compression of CRS
  - (lattices) weaker, falsifiable assumptions

Thank you!!! :)