Multi-Client Attribute-Based Unbounded Inner Product Functional Encryption, and More

Subhranil Dutta
Aikaterini Mitrokotsa
Jenit Tomy

University of St. Gallen

Tapas Pal

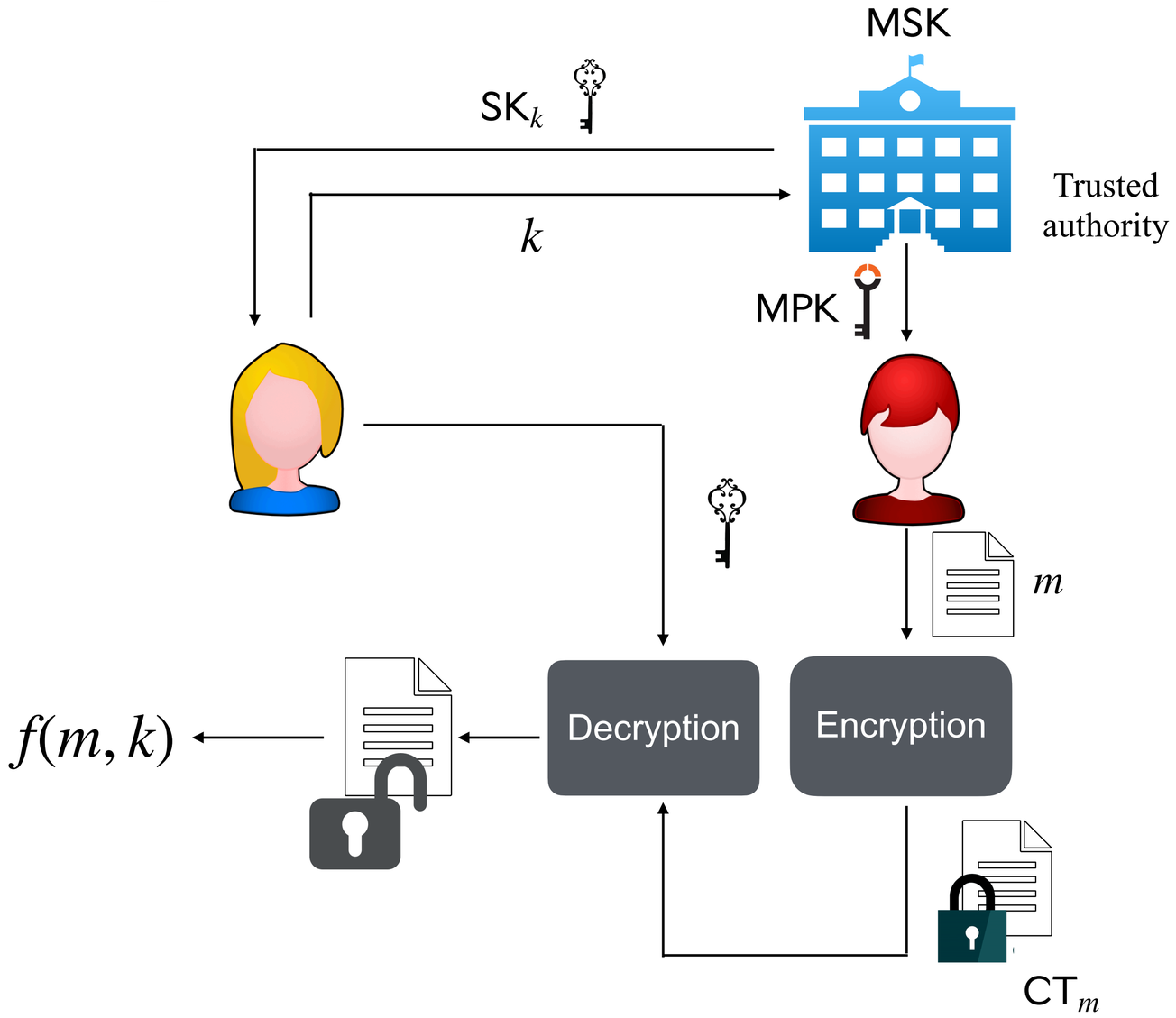
KIT, KASTEL SRL

Karlsruher Institut für Technologie

Functional Encryption (FE) [BSW11]

Functionality $f : \mathscr{M} \times \mathscr{K} \rightarrow \Sigma \cup \{ \perp \}$

Message space: $\mathscr{M}$; Key space: $\mathscr{K}$

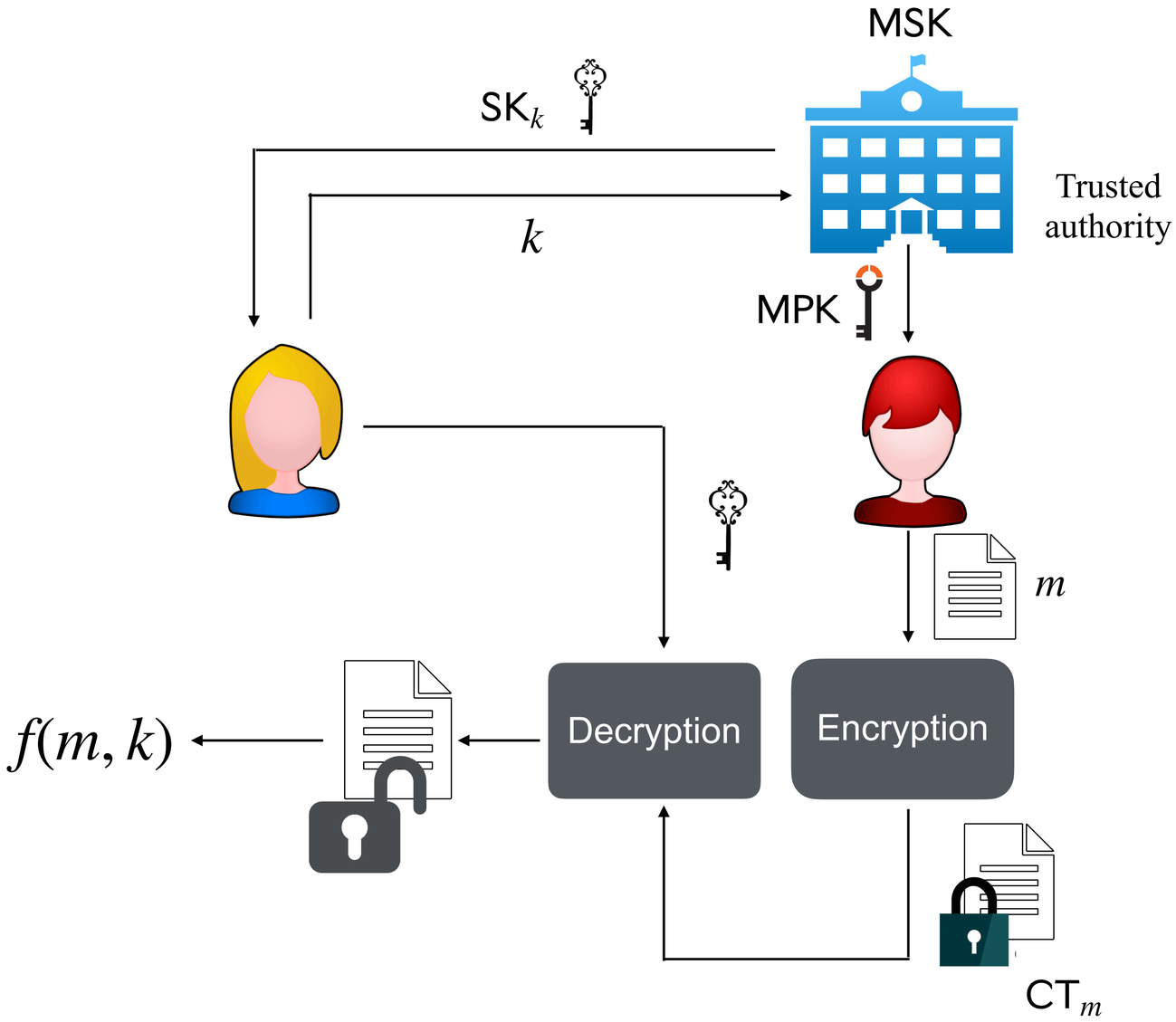


Functional Encryption (FE) [BSW11]

Functionality $f : \mathcal{M} \times \mathcal{K} \to \Sigma \cup \{ \perp \}$

Message space: $\mathcal{M}$; Key space: $\mathcal{K}$

- Setup$(1^\lambda) \to$ (MPK, MSK)
- KeyGen(MSK, k) $\to$ SK$_k$
- Enc(MPK, m) $\to$ CT$_m$
- Dec(SK$_k$, CT$_m$) $\to f(m, k)$

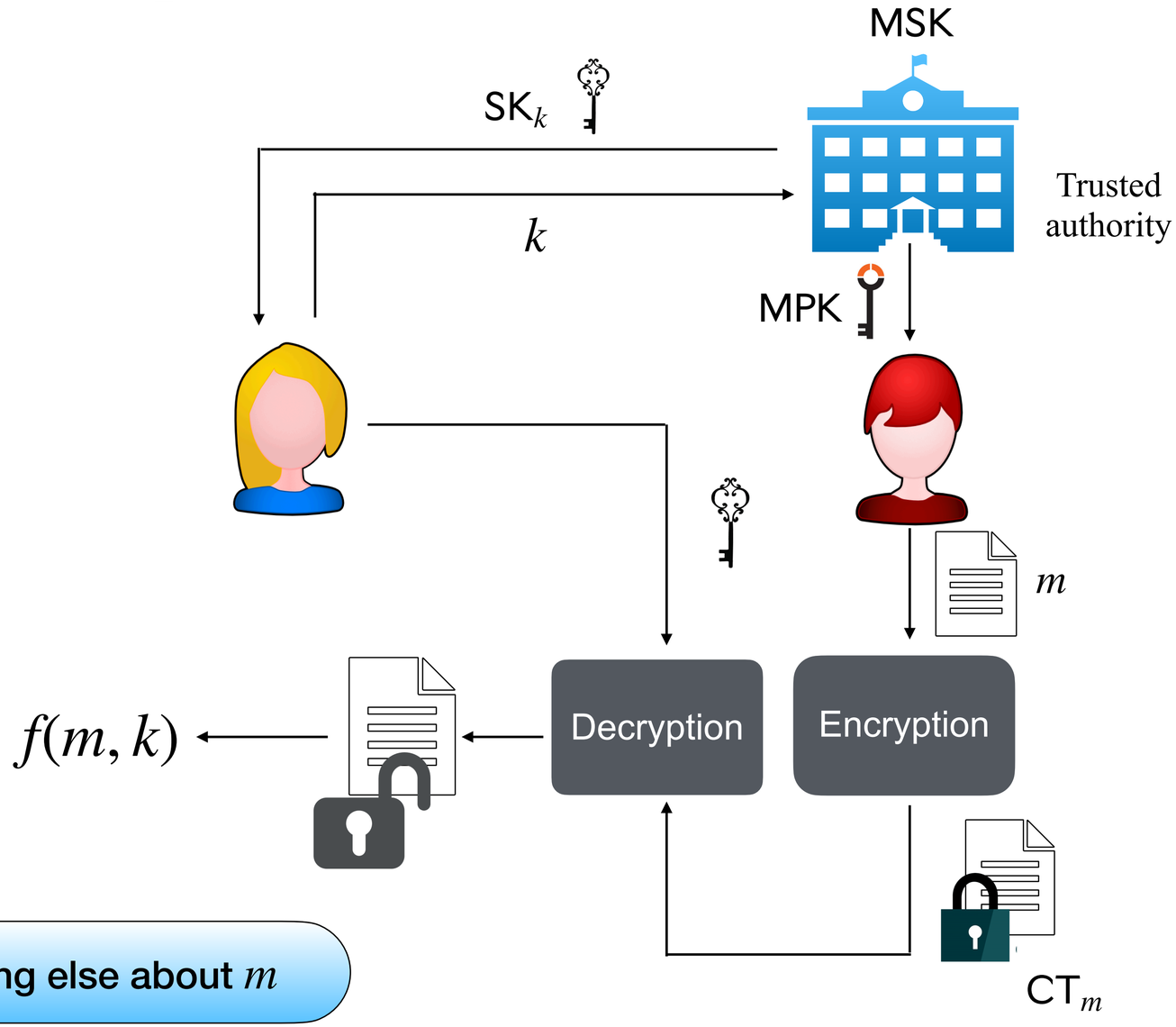


Functional Encryption (FE) [BSW11]

Functionality $f : \mathcal{M} \times \mathcal{K} \to \Sigma \cup \{ \perp \}$

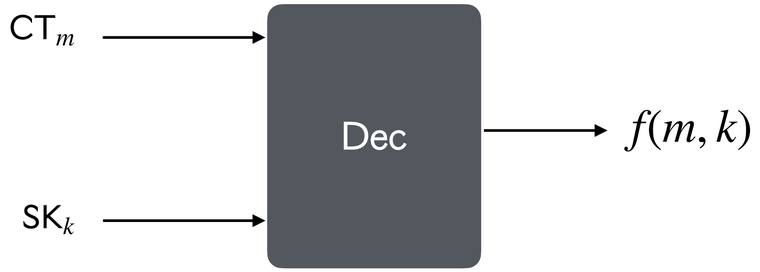
Message space: $\mathcal{M}$; Key space: $\mathcal{K}$

- Setup$(1^\lambda) \to$ (MPK, MSK)
- KeyGen(MSK, k) $\to$ SK$_k$
- Enc(MPK, m) $\to$ CT$_m$
- Dec(SK$_k$, CT$_m$) $\to f(m, k)$



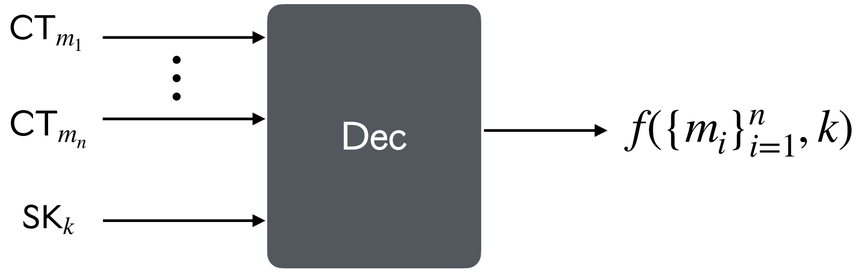
Security : CT$_m$ and SK$_k$ only leaks $f(m, k)$ and nothing else about m

FE with Multiple users



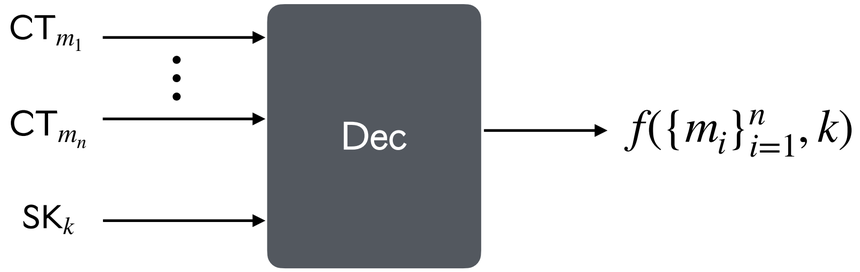
FE with Multiple users

- Multiple ciphertexts



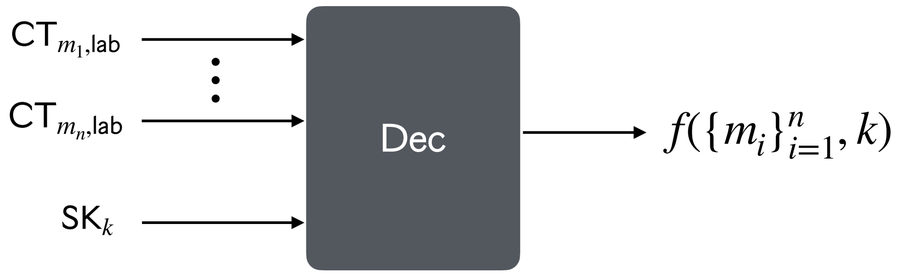
FE with Multiple users

- Multiple ciphertexts
    - Multi-input FE (MI-FE) [AGR+17]

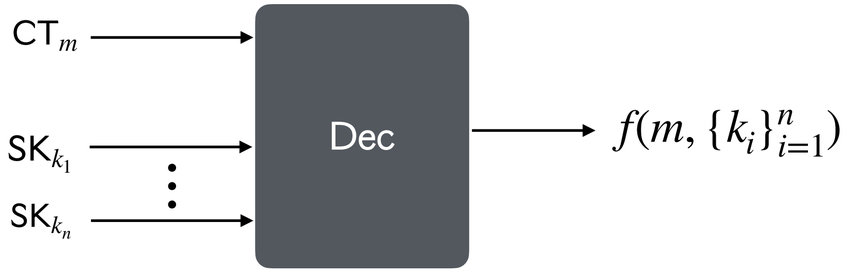


FE with Multiple users

- Multiple ciphertexts
  - Multi-client FE (MC-FE) [ABG19]

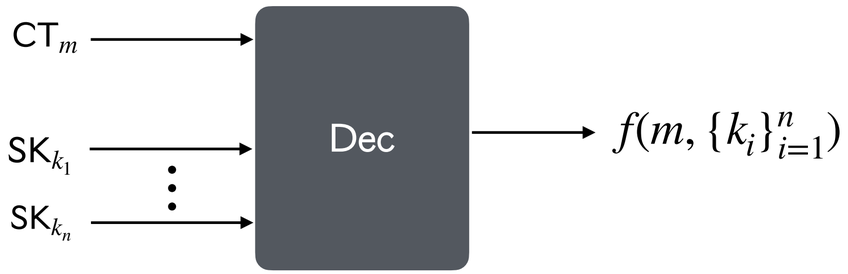


FE with Multiple users



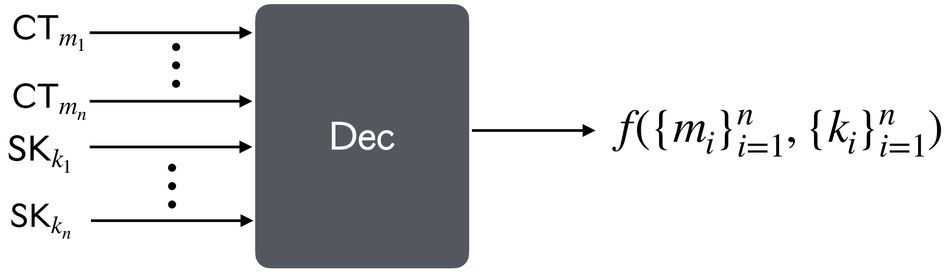
- Multiple secret keys

FE with Multiple users



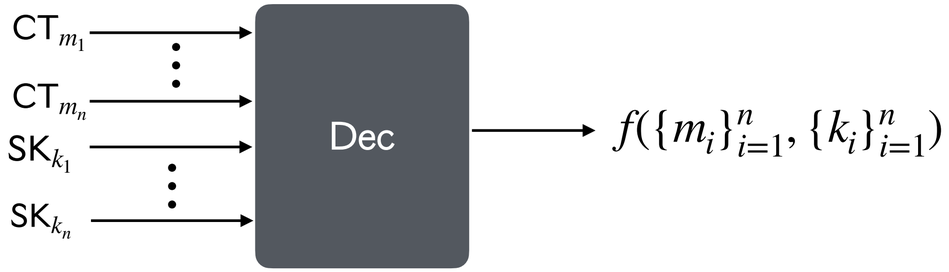
- Multiple secret keys
    - Multi-authority FE (MA-FE) [AGT21a,DP23]

FE with Multiple users



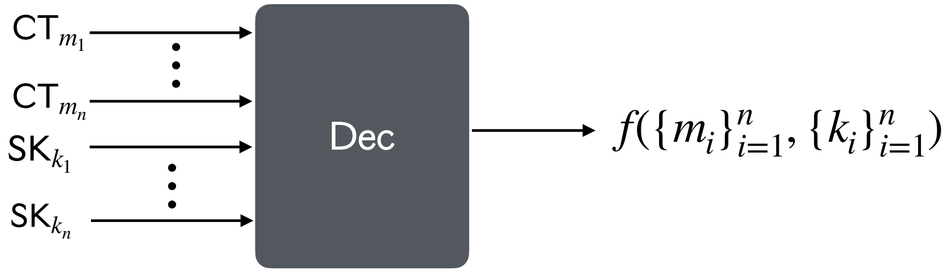
- Both Multiple ciphertexts and secret keys

FE with Multiple users



- Both Multiple ciphertexts and secret keys
    - Decentralized multi-client FE (DMC-FE) [CDG+18]

FE with Multiple users



- Both Multiple ciphertexts and secret keys
    - Dynamic decentralized FE (DD-FE) [CDG+20]

Multi-user FE for Various Function Classes

Functionalities	Related Work	Data and Functions	Output

Multi-user FE for Various Function Classes

Functionalities	Related Work	Data and Functions	Output
Linear	[AGR+17, ACF+18, DOT18, CDG+18, ABG19, ABK+19, ABM+20, CDG+20, AGT21a, DP23, FFM+23, NPP23, NPR24, ….]	• $m_i = \mathbf{x}_i \in \mathbb{Z}_p^m$ • $k_i = \mathbf{y}_i \in \mathbb{Z}_p^m$	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \langle \mathbf{x}_i, \mathbf{y}_i \rangle$

Multi-user FE for Various Function Classes

Functionalities	Related Work	Data and Functions	Output
Linear	[AGR+17, ACF+18, DOT18, CDG+18, ABG19, ABK+19, ABM+20, CDG+20, AGT21a, DP23, FFM+23, NPP23, NPR24, ….]	• $m_i = \mathbf{x}_i \in \mathbb{Z}_p^m$ • $k_i = \mathbf{y}_i \in \mathbb{Z}_p^m$	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \langle \mathbf{x}_i, \mathbf{y}_i \rangle$
Quadratic	[AGT21b, AGT22]	• $m_i = (\mathbf{x}_i, \mathbf{x}_i) \in \mathbb{Z}_p^m \times \mathbb{Z}_p^m$ • $k_i = \mathbf{F}_i \in \mathbb{Z}_p^{m\times m}$	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \mathbf{x}_i^\top \mathbf{F}_i \mathbf{x}_i$

Multi-user FE for Various Function Classes

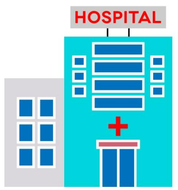
Functionalities	Related Work	Data and Functions	Output
Linear	[AGR+17, ACF+18, DOT18, CDG+18, ABG19, ABK+19, ABM+20, CDG+20, AGT21a, DP23, FFM+23, NPP23, NPR24, ….]	• $m_i = \mathbf{x}_i \in \mathbb{Z}_p^m$ • $k_i = \mathbf{y}_i \in \mathbb{Z}_p^m$	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \langle \mathbf{x}_i, \mathbf{y}_i \rangle$
Quadratic	[AGT21b, AGT22]	• $m_i = (\mathbf{x}_i, \mathbf{x}_i) \in \mathbb{Z}_p^m \times \mathbb{Z}_p^m$ • $k_i = \mathbf{F}_i \in \mathbb{Z}_p^{m\times m}$	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \mathbf{x}_i^\top \mathbf{F}_i \mathbf{x}_i$
Attribute weighted sum	[ATY23]	• $m_i = (\mathbf{x}_i, \mathbf{z}_i) \in \mathbb{Z}_p^m \times \mathbb{Z}_p^m$ • $k_i = g_i \in$ ABP	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \langle g_i(\mathbf{x}_i), \mathbf{z}_i \rangle$

Multi-user FE for Various Function Classes

Functionalities	Related Work	Data and Functions	Output
Linear	[AGR+17, ACF+18, DOT18, CDG+18, ABG19, ABK+19, ABM+20, CDG+20, AGT21a, DP23, FFM+23, NPP23, NPR24, ….]	• $m_i = \mathbf{x}_i \in \mathbb{Z}_p^m$ • $k_i = \mathbf{y}_i \in \mathbb{Z}_p^m$	$f(\{m_i\}_{i=1}^n, \{k_i\}_{i=1}^n) = \sum_{i\in[n]} \langle \mathbf{x}_i, \mathbf{y}_i \rangle$
Quadratic	[AGT21b, AGT22]		
Attribute weighted sum	[ATY23]		

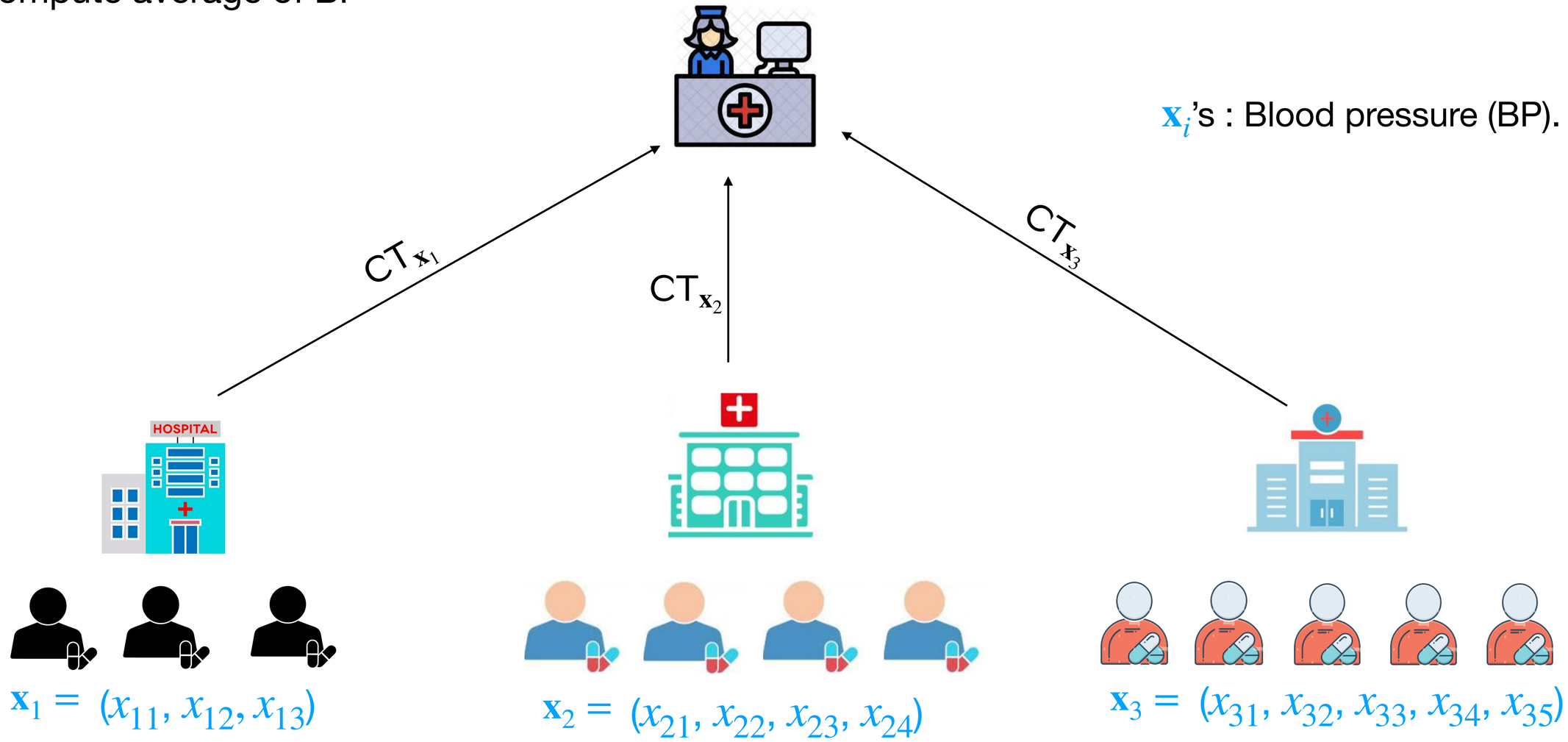
Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP



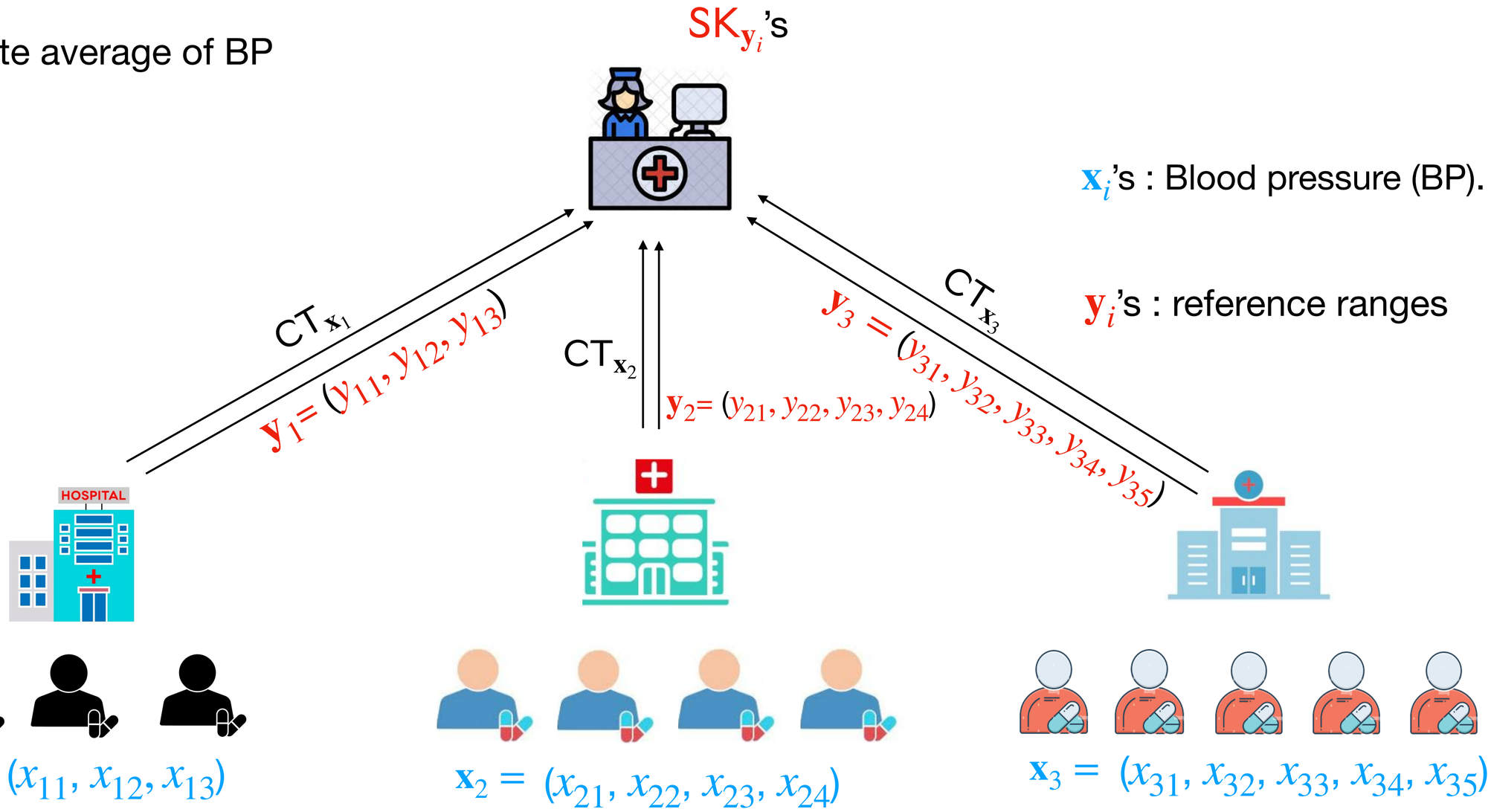
Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP



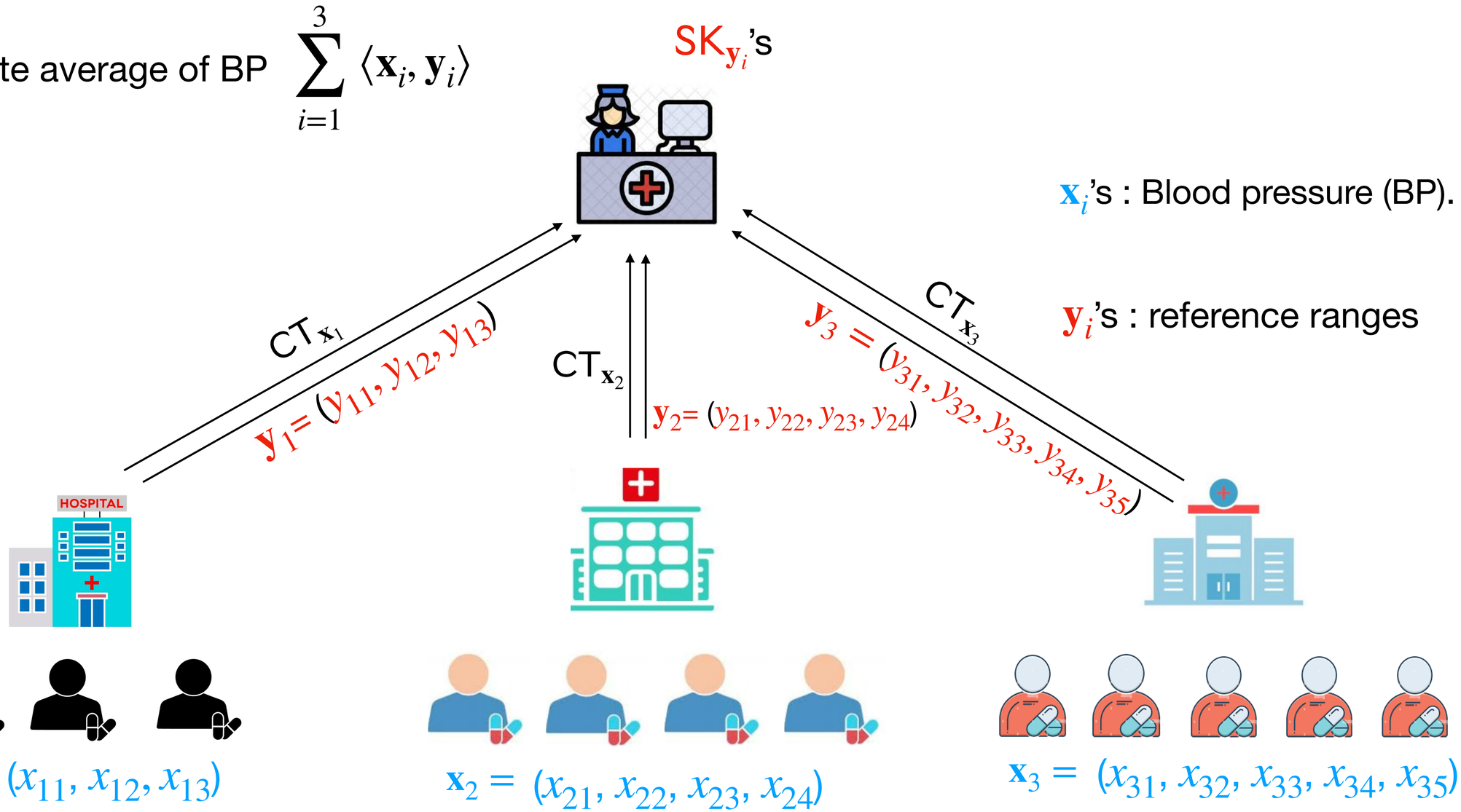
Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP



Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP $\sum_{i=1}^{3} \langle \mathbf{x}_i, \mathbf{y}_i \rangle$

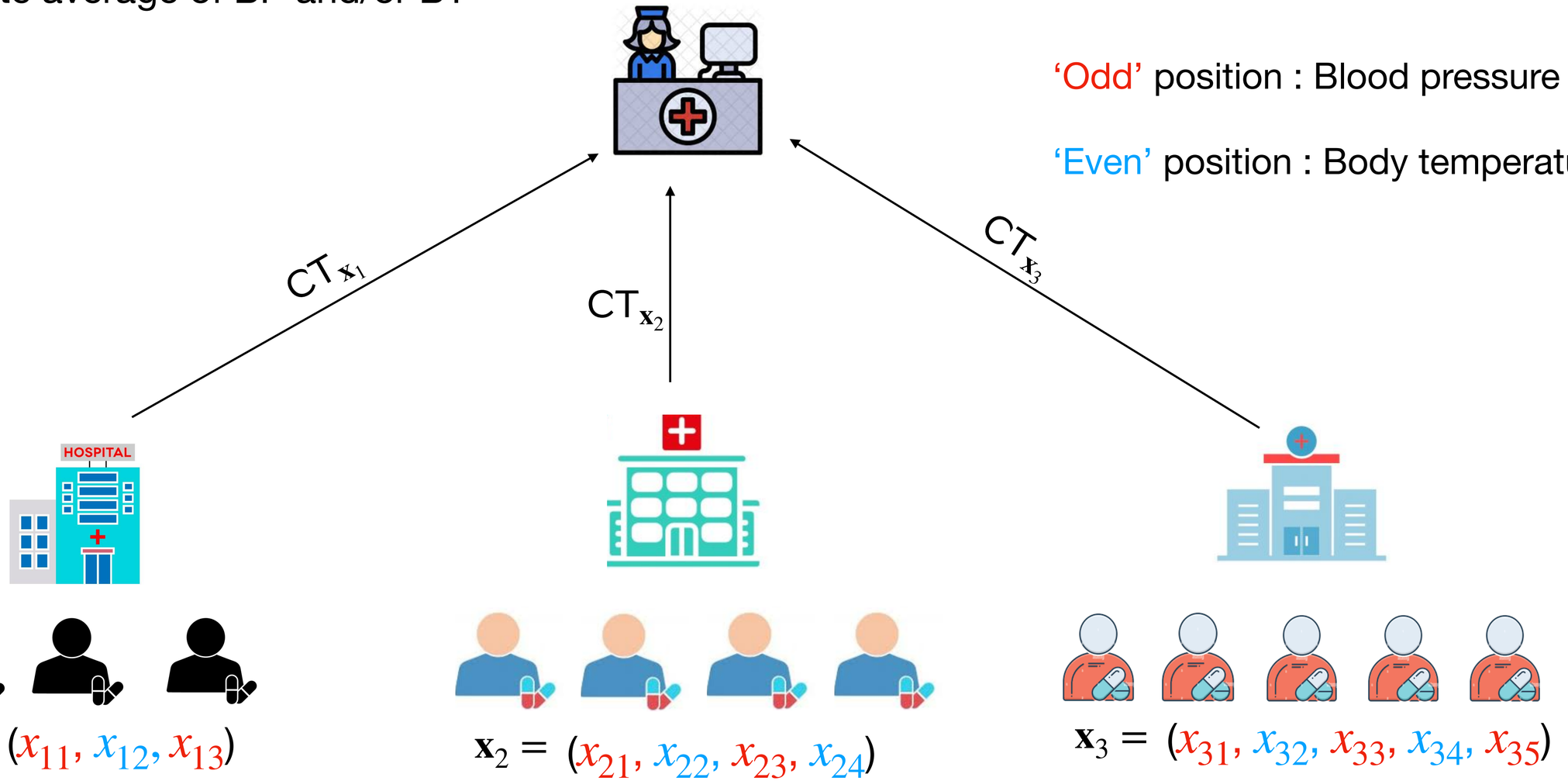


$\mathbf{x}_i$'s : Blood pressure (BP).

$\mathbf{y}_i$'s : reference ranges

Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP and/or BT

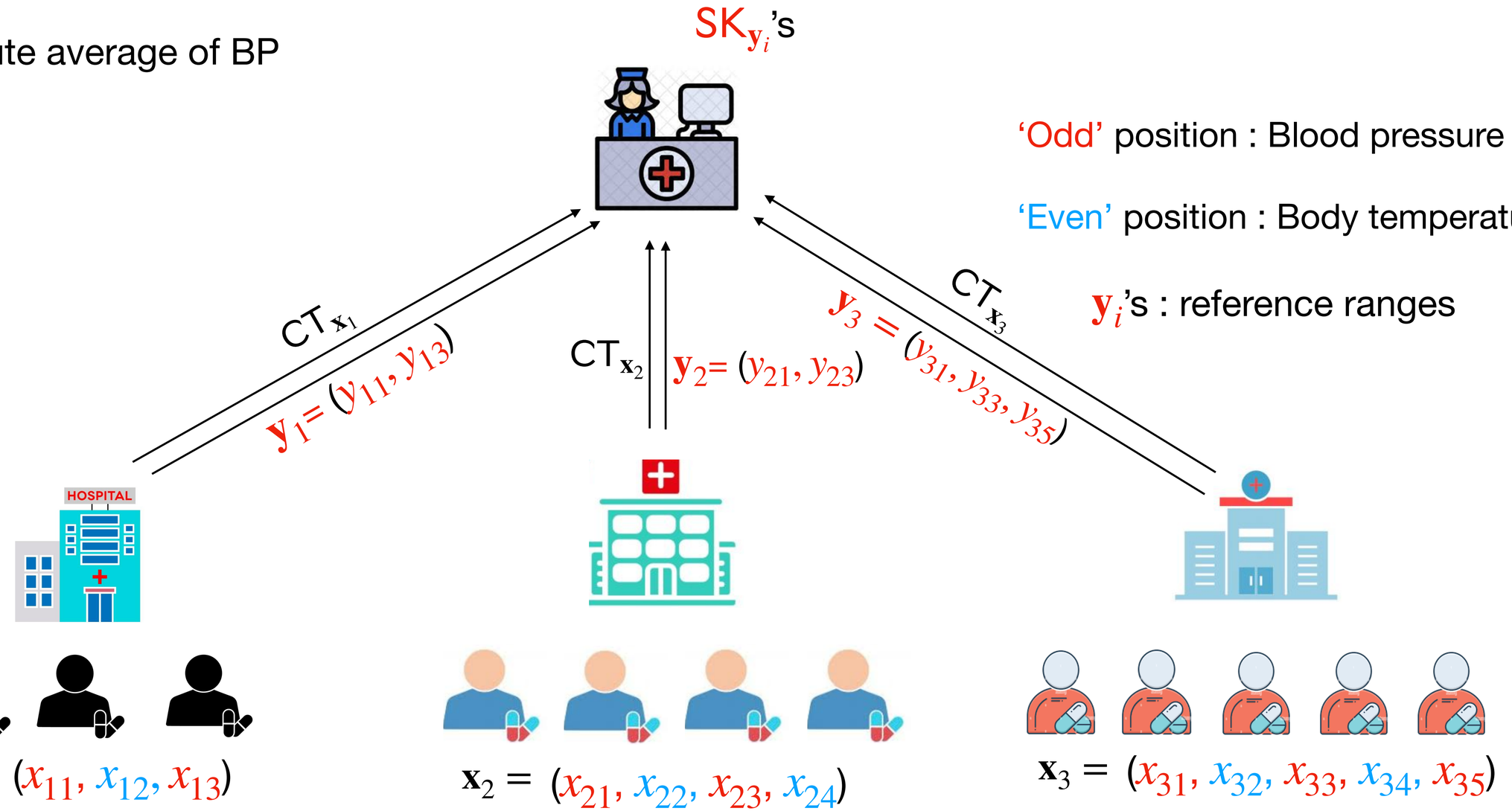


'Odd' position : Blood pressure (BP).

'Even' position : Body temperature (BT).

Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP



'Odd' position : Blood pressure (BP).

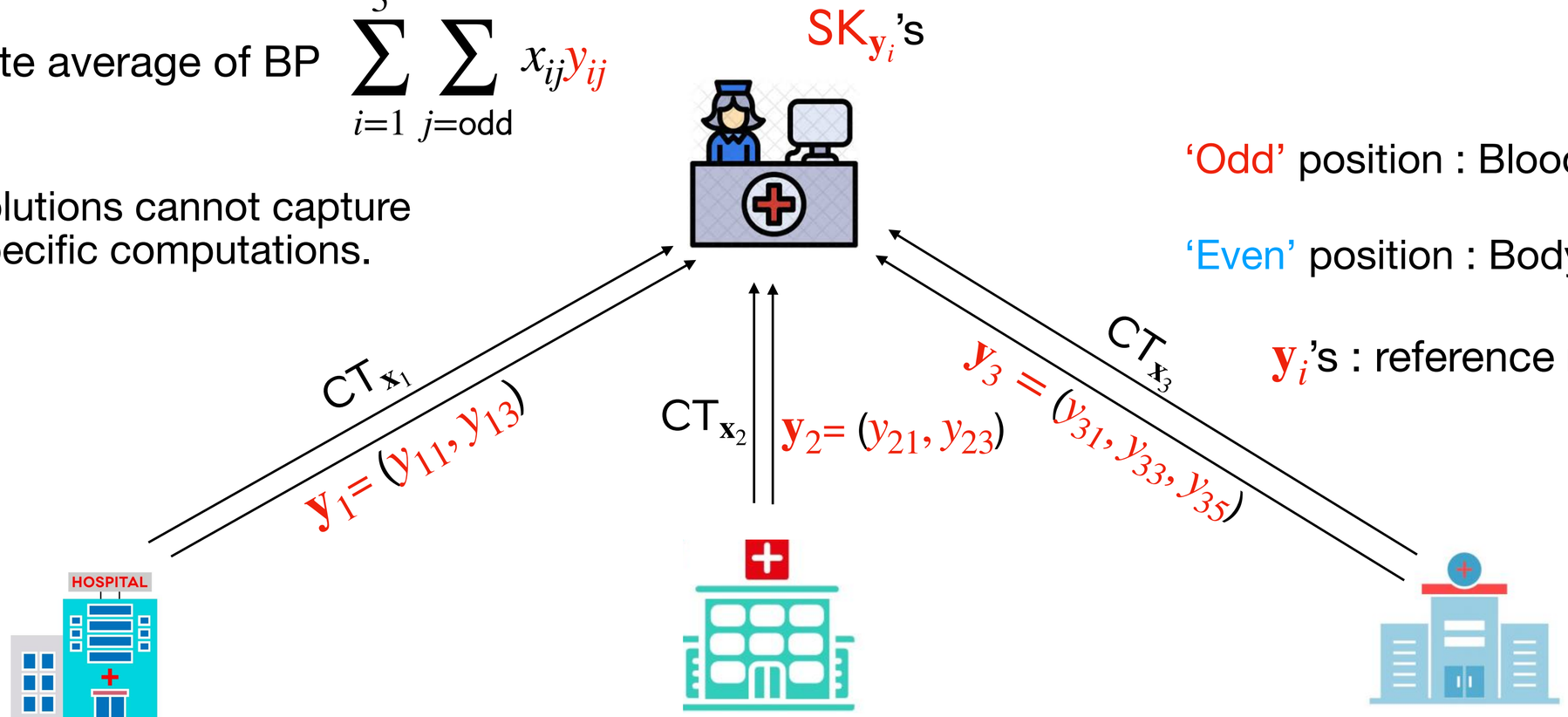
'Even' position : Body temperature (BT).

$\mathbf{y}_i$'s : reference ranges

Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP $\sum_{i=1}^{3} \sum_{j=\text{odd}} x_{ij} y_{ij}$

- Existing solutions cannot capture index-specific computations.



'Odd' position : Blood pressure (BP).

'Even' position : Body temperature (BT).

$\mathbf{y}_i$'s : reference ranges

$\mathbf{x}_1 = (x_{11}, x_{12}, x_{13})$

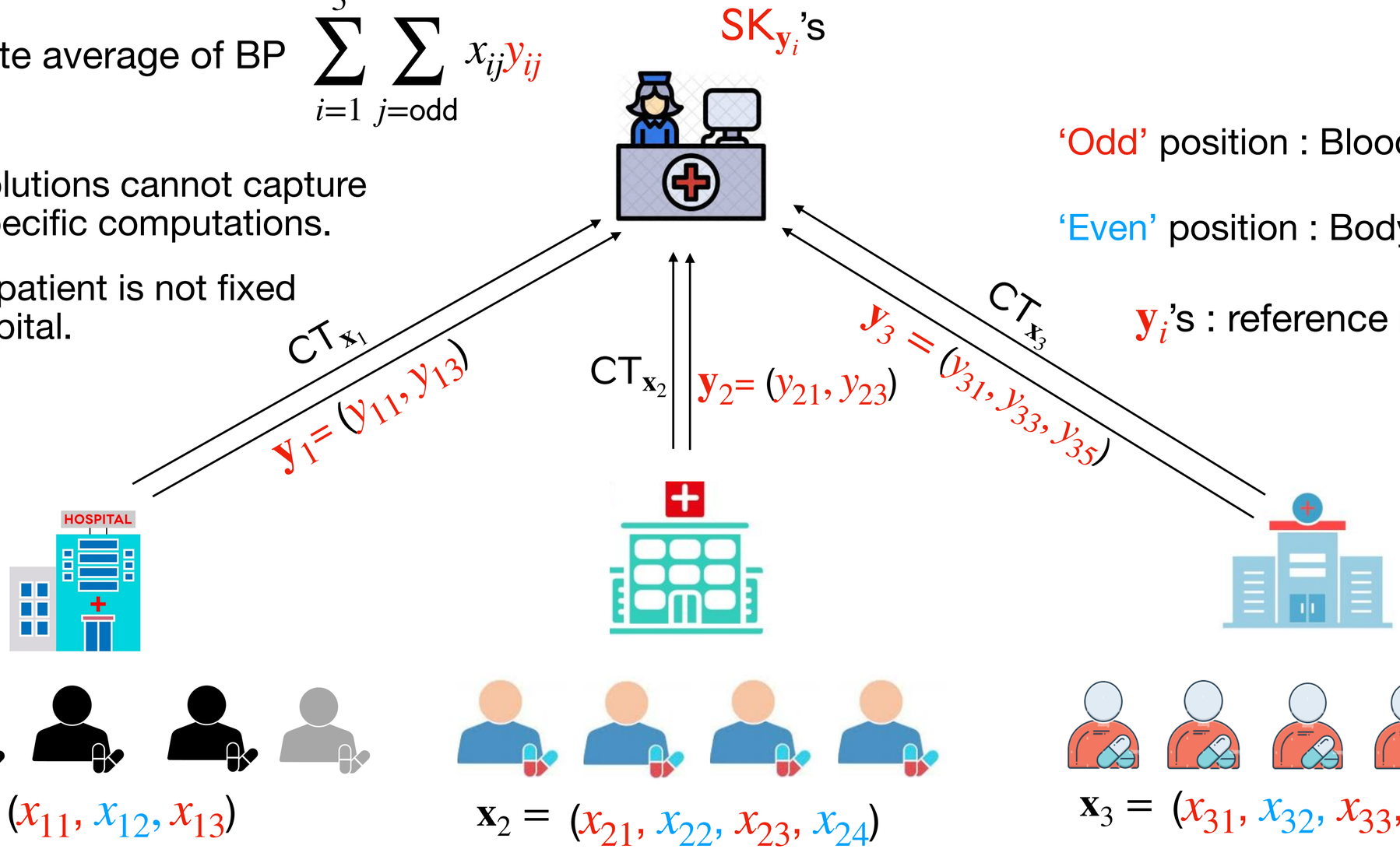
$\mathbf{x}_2 = (x_{21}, x_{22}, x_{23}, x_{24})$

$\mathbf{x}_3 = (x_{31}, x_{32}, x_{33}, x_{34}, x_{35})$

Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP $\sum_{i=1}^{3} \sum_{j=\text{odd}} x_{ij} y_{ij}$

- Existing solutions cannot capture index-specific computations.
- Number of patient is not fixed for any hospital.



'Odd' position : Blood pressure (BP).

'Even' position : Body temperature (BT).

$\mathbf{y}_i$'s : reference ranges

Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP

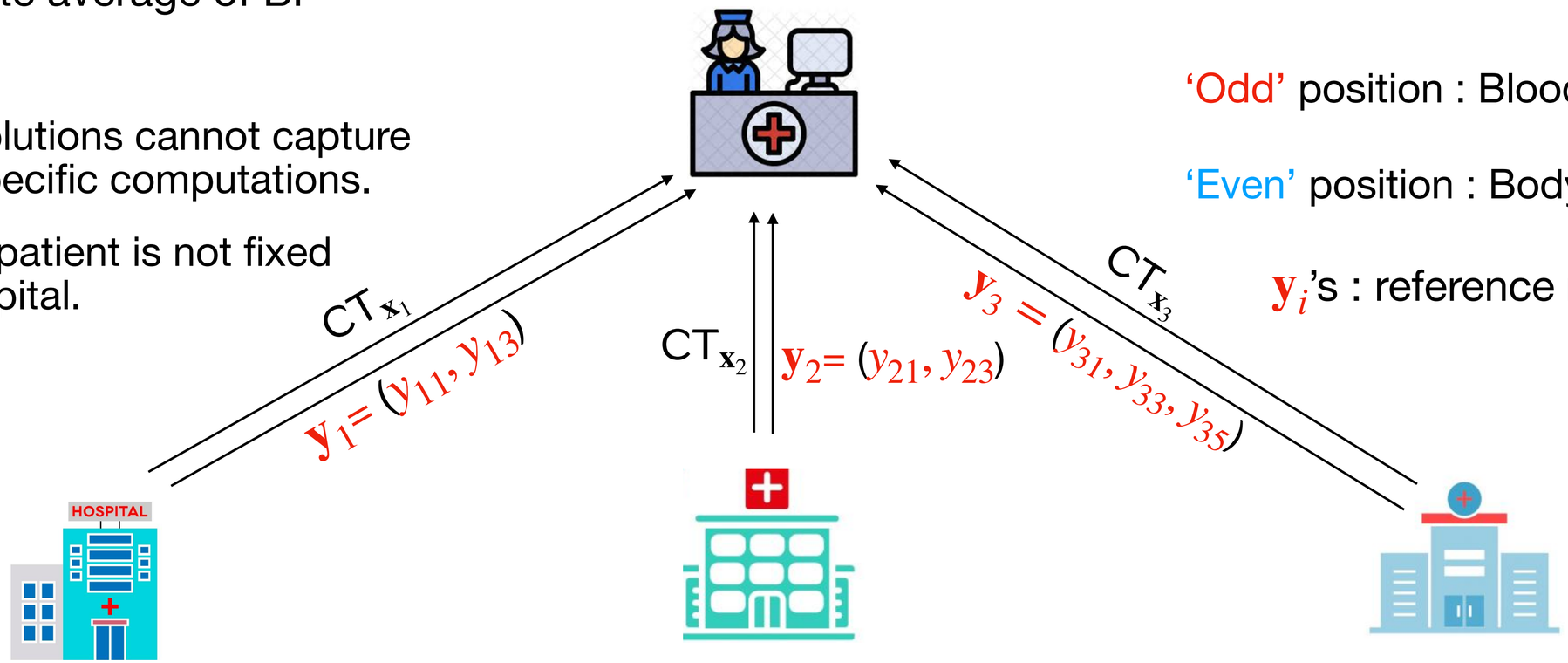
- Existing solutions cannot capture index-specific computations.
- Number of patient is not fixed for any hospital.

$SK_{\mathbf{y}_i}$'s P : 1000< Location_id < 2000

'Odd' position : Blood pressure (BP).

'Even' position : Body temperature (BT).

$\mathbf{y}_i$'s : reference ranges



$\mathbf{x}_1 = (x_{11}, x_{12}, x_{13})$

att: Location_id: 1105

$\mathbf{x}_2 = (x_{21}, x_{22}, x_{23}, x_{24})$

att: Location_id: 1004

$\mathbf{x}_3 = (x_{31}, x_{32}, x_{33}, x_{34}, x_{35})$

att: Location_id: 2004

Application of Linear Functionality in Multi-user Settings

Goal: Compute average of BP $\sum_{i=1}^{2} \sum_{j=\text{odd}} x_{ij} y_{ij}$

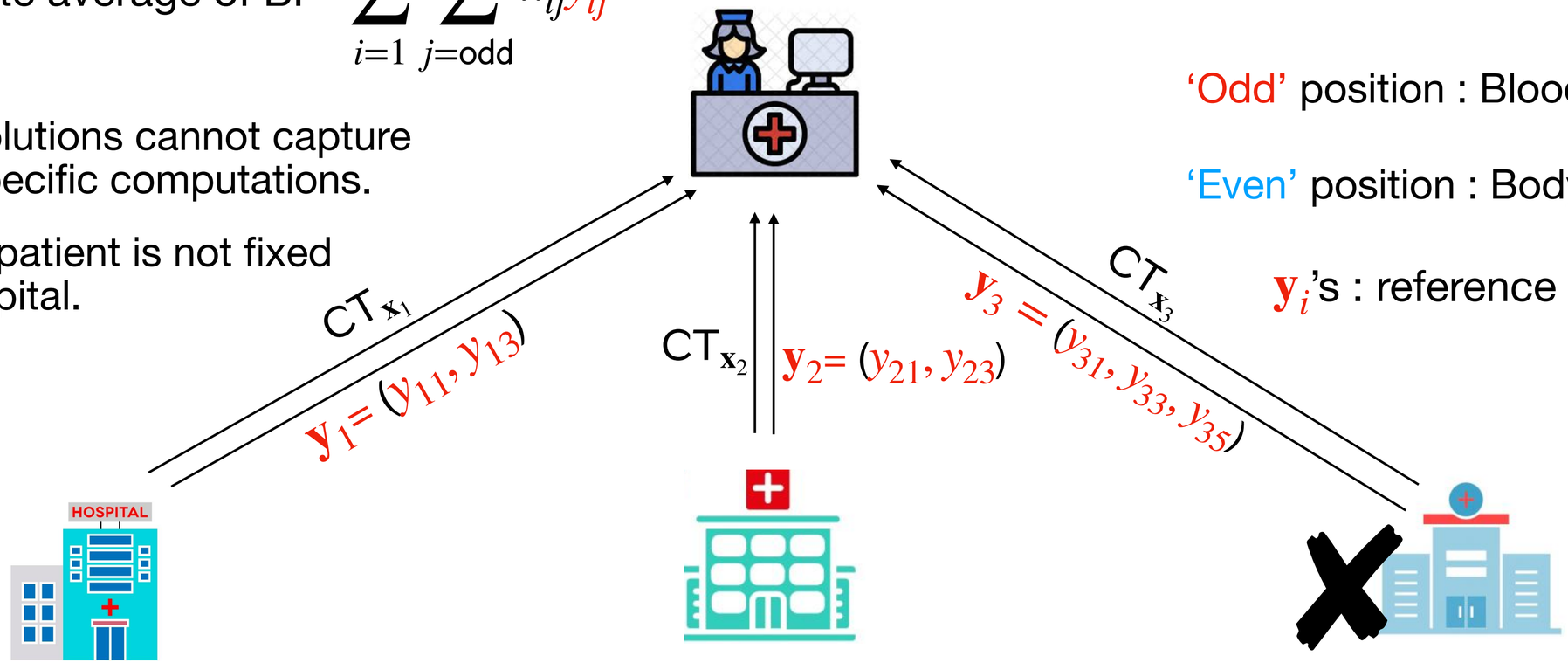
$SK_{\mathbf{y}_i}$'s P : 1000< Location_id < 2000

- Existing solutions cannot capture index-specific computations.
- Number of patient is not fixed for any hospital.

'Odd' position : Blood pressure (BP).

'Even' position : Body temperature (BT).

$\mathbf{y}_i$'s : reference ranges



$\mathbf{x}_1 = (x_{11}, x_{12}, x_{13})$

att: Location_id: 1105

$\mathbf{x}_2 = (x_{21}, x_{22}, x_{23}, x_{24})$

att: Location_id: 1004

$\mathbf{x}_3 = (x_{31}, x_{32}, x_{33}, x_{34}, x_{35})$

att: Location_id: 2004

Previous works in Multi-user FE

Works	Primitives	Parties	Input length	Fun. length	Acc Con.	Label	Corr.	Assumption
[CDG+18]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH
	DMC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	SXDH
[ABG19]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH, LWE, DCR
[CDG+20]	DD-IPFE	Unbounded	Bounded	Bounded	N/A	Yes	Yes	DDH

Previous works in Multi-user FE

Works	Primitives	Parties	Input length	Fun. length	Acc Con.	Label	Corr.	Assumption
[CDG+18]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH
	DMC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	SXDH
[ABG19]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH, LWE, DCR
[CDG+20]	DD-IPFE	Unbounded	Bounded	Bounded	N/A	Yes	Yes	DDH
[NPP22]	MC-AB-IPFE	n	Bounded	Bounded	LSSS	OT	Yes	SXDH

Previous works in Multi-user FE

Works	Primitives	Parties	Input length	Fun. length	Acc Con.	Label	Corr.	Assumption
[CDG+18]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH
	DMC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	SXDH
[ABG19]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH, LWE, DCR
[CDG+20]	DD-IPFE	Unbounded	Bounded	Bounded	N/A	Yes	Yes	DDH
[NPP22]	MC-AB-IPFE	n	Bounded	Bounded	LSSS	OT	Yes	SXDH
[ATY23]	MC-FE for AWS	n	Unbounded	Bounded	N/A	Yes	Yes	MDDH
	MI-AB-FE for AWS	n	Unbounded	Bounded	ABP	Yes	Yes	MDDH
	DD-FE for AWS	Unbounded	Unbounded	Bounded	N/A	Yes	Yes	MDDH

Previous works in Multi-user FE

Works	Primitives	Parties	Input length	Fun. length	Acc Con.	Label	Corr.	Assumption
[CDG+18]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH
	DMC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	SXDH
[ABG19]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH, LWE, DCR
[CDG+20]	DD-IPFE	Unbounded	Bounded	Bounded	N/A	Yes	Yes	DDH
[NPP22]	MC-AB-IPFE	n	Bounded	Bounded	LSSS	OT	Yes	SXDH
[ATY23]	MC-FE for AWS	n	Unbounded	Bounded	N/A	Yes	Yes	MDDH
	MI-AB-FE for AWS	n	Unbounded	Bounded	ABP	Yes	Yes	MDDH
	DD-FE for AWS	Unbounded	Unbounded	Bounded	N/A	Yes	Yes	MDDH

Previous works in Multi-user FE

Works	Primitives	Parties	Input length	Fun. length	Acc Con.	Label	Corr.	Assumption
[CDG+18]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH
	DMC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	SXDH
[ABG19]	MC-IPFE	n	Bounded	Bounded	N/A	Yes	Yes	DDH, LWE, DCR
[CDG+20]	DD-IPFE	Unbounded	Bounded	Bounded	N/A	Yes	Yes	DDH
[NPP22]	MC-AB-IPFE	n	Bounded	Bounded	LSSS	OT	Yes	SXDH
[ATY23]	MC-FE for AWS	n	Unbounded	Bounded	N/A	Yes	Yes	MDDH
	MI-AB-FE for AWS	n	Unbounded	Bounded	ABP	Yes	Yes	MDDH
	DD-FE for AWS	Unbounded	Unbounded	Bounded	N/A	Yes	Yes	MDDH

Our Results

Primitives	Parties	Input length	Fun. length	Acc Con.	Label	Corr.	Assumption
MC-AB-UIPFE	n	Unbounded	Unbounded	LSSS	OT	Yes	MDDH
MI-AB-UIPFE	n	Unbounded	Unbounded	LSSS	N/A	Yes	MDDH
DD-UIPFE	Unbounded	Unbounded	Unbounded	N/A	Yes	Yes	MDDH

Our Functionalities

$|\mathbf{x}_k| : \ell_k$; $I_{\mathbf{y}_k}$: index set of $\mathbf{y}_k$; $\mathbb{A}$: access structure; S_k : set of attributes; L : label; k : client indicies .

MC-AB-UIPFE: $$f\left(\{\mathsf{S}_k, L_k, \mathbf{x}_k, \ell_k\}_{k=1}^n, \{\mathbb{A}, (\mathbf{y}_k, I_{\mathbf{y}_k})\}_{k=1}^n\right) = \begin{cases} \sum_{k\in[n]} \sum_{i\in I_{\mathbf{y}_k}} x_{k,i} y_{k,i} & \text{if } (I_{\mathbf{y}_k} \subseteq [\ell_k]) \wedge (\mathbb{A}(\mathsf{S}_k) = 1) \wedge (L_k = L),\ \forall k \in [n] \\ \perp & \text{otherwise} \end{cases}$$

MI-AB-UIPFE: $$f\left(\{\mathsf{S}_k, \mathbf{x}_k, \ell_k\}_{k=1}^n, \{\mathbb{A}, (\mathbf{y}_k, I_{\mathbf{y}_k})\}_{k=1}^n\right) = \begin{cases} \sum_{k\in[n]} \sum_{i\in I_{\mathbf{y}_k}} x_{k,i} y_{k,i} & \text{if } (I_{\mathbf{y}_k} \subseteq [\ell_k]) \wedge (\mathbb{A}(\mathsf{S}_k) = 1),\ \forall k \in [n] \\ \perp & \text{otherwise} \end{cases}$$

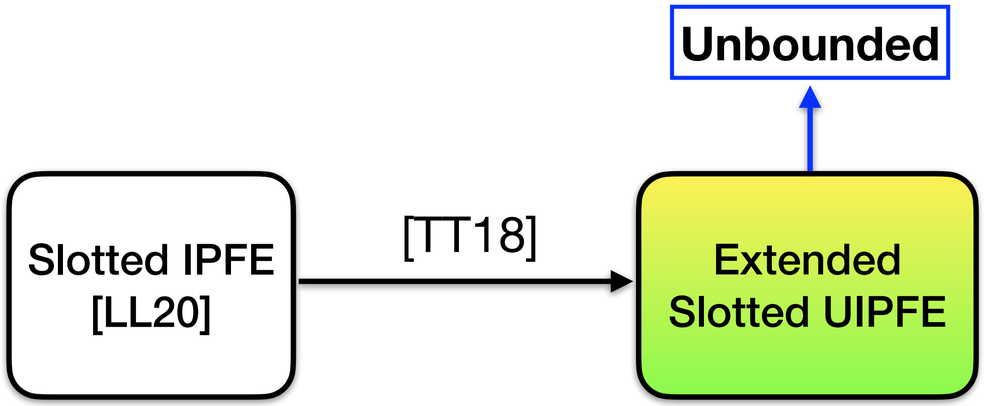
DD-UIPFE: $$f\left(\{L_k, \mathbf{x}_k, \ell_k\}_{k\in\mathcal{U}_{k,msg}}, \{(\mathbf{y}_k, I_{\mathbf{y}_k})\}_{k\in\mathcal{U}_{k,key}}\right) = \begin{cases} \sum_{k\in\mathcal{U}} \sum_{i\in I_{\mathbf{y}_k}} x_{k,i} y_{k,i} & \text{if } (\mathcal{U} = \mathcal{U}_{k,msg} = \mathcal{U}_{k,key}) \wedge (I_{\mathbf{y}_k} \subseteq [\ell_k]) \wedge (L_k = L),\ \forall k \in \mathcal{U} \\ \perp & \text{otherwise} \end{cases}$$

- Access control for MC-AB-UIPFE and MI-AB-UIPFE using Linear Secret Sharing Schemes (LSSS).
- Unbounded size of input and function with permissive setting.

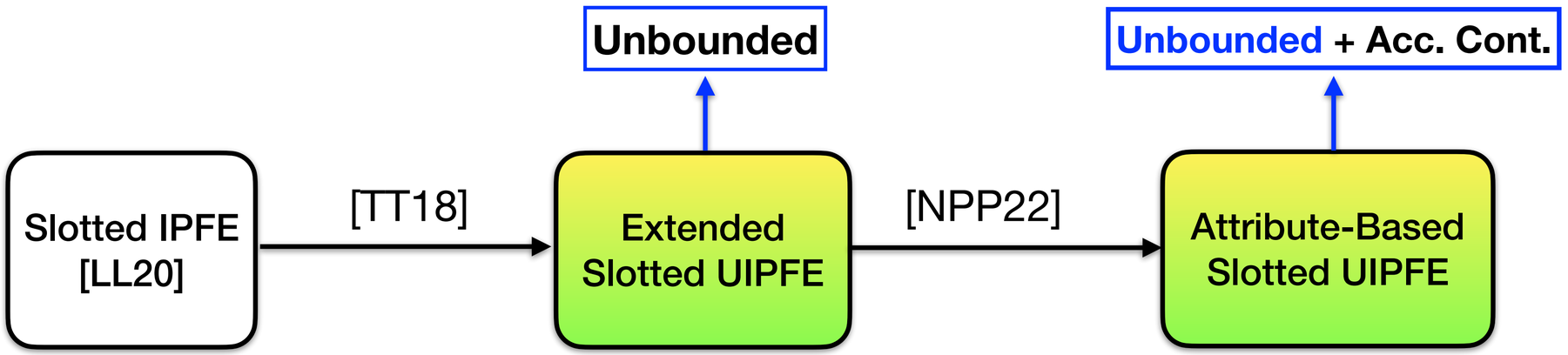
Technical Steps Towards MC-AB-UIPFE

Slotted IPFE
[LL20]

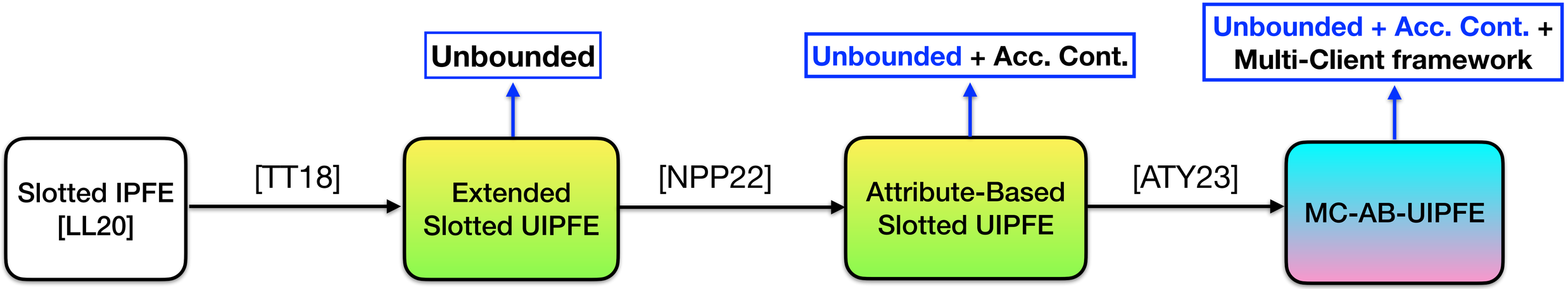
Technical Steps Towards MC-AB-UIPFE



Technical Steps Towards MC-AB-UIPFE



Technical Steps Towards MC-AB-UIPFE



Slotted IPFE (sIPFE) [LL20]

Pairing group $\mathsf{G} = (p, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot, \cdot))$; $[\mathbf{a}]_\iota = g_\iota^{\mathbf{a}}$

Slotted IPFE (sIPFE) [LL20]

Pairing group $\mathsf{G} = (p, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot, \cdot))$; $[\mathbf{a}]_\iota = g_\iota^{\mathbf{a}}$

- $\mathsf{Setup}(1^\lambda, \mathcal{S}_{\mathsf{pub}}, \mathcal{S}_{\mathsf{priv}}) \to (\mathsf{MPK}, \mathsf{MSK})$
- $\mathsf{KeyGen}(\mathsf{MSK}, [\mathbf{y}]_2) \to \mathsf{SK}_{\mathbf{y}}, \quad \mathbf{y} = (\mathbf{y}_{\mathsf{pub}}, \mathbf{y}_{\mathsf{priv}})$
- $\mathsf{SlotEnc}(\mathsf{MPK}, [\mathbf{x}_{\mathsf{pub}}]_1) \to \mathsf{CT}_{\mathbf{x}}^{\mathsf{slot}}$
- $\mathsf{Enc}(\mathsf{MSK}, [(\mathbf{x}_{\mathsf{pub}}, \mathbf{x}_{\mathsf{priv}})]_1) \to \mathsf{CT}_{\mathbf{x}}^{\mathsf{norm}}, \quad \mathbf{x} = (\mathbf{x}_{\mathsf{pub}}, \mathbf{x}_{\mathsf{priv}})$
- $\mathsf{Dec}(\mathsf{SK}_{\mathbf{y}}, \mathsf{CT}_{\mathbf{x}}) \to [\langle \mathbf{x}, \mathbf{y} \rangle]_T$

Slotted IPFE (sIPFE) [LL20]

Pairing group $\mathsf{G} = (p, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot, \cdot))$; $[\mathbf{a}]_\iota = g_\iota^{\mathbf{a}}$

- $\mathsf{Setup}(1^\lambda, \mathcal{S}_{\mathsf{pub}}, \mathcal{S}_{\mathsf{priv}}) \to (\mathsf{MPK}, \mathsf{MSK})$
- $\mathsf{KeyGen}(\mathsf{MSK}, [\mathbf{y}]_2) \to \mathsf{SK}_{\mathbf{y}}, \quad \mathbf{y} = (\mathbf{y}_{\mathsf{pub}}, \mathbf{y}_{\mathsf{priv}})$
- $\mathsf{SlotEnc}(\mathsf{MPK}, [\mathbf{x}_{\mathsf{pub}}]_1) \to \mathsf{CT}^{\mathsf{slot}}_{\mathbf{x}}$
- $\mathsf{Enc}(\mathsf{MSK}, [(\mathbf{x}_{\mathsf{pub}}, \mathbf{x}_{\mathsf{priv}})]_1) \to \mathsf{CT}^{\mathsf{norm}}_{\mathbf{x}}, \quad \mathbf{x} = (\mathbf{x}_{\mathsf{pub}}, \mathbf{x}_{\mathsf{priv}})$
- $\mathsf{Dec}(\mathsf{SK}_{\mathbf{y}}, \mathsf{CT}_{\mathbf{x}}) \to [\langle \mathbf{x}, \mathbf{y} \rangle]_T$

Slot mode Correctness

$\mathsf{SlotEnc}(\mathsf{MPK}, [\mathbf{x}]_1) \approx_c \mathsf{Enc}(\mathsf{MSK}, [(\mathbf{x}_{\mathsf{pub}} \,||\, \mathbf{0})]_1)$

Slotted IPFE (sIPFE) [LL20]

Pairing group $\mathsf{G} = (p, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(\cdot, \cdot))$; $[\mathbf{a}]_\iota = g_\iota^{\mathbf{a}}$

- $\mathsf{Setup}(1^\lambda, \mathcal{S}_{\mathsf{pub}}, \mathcal{S}_{\mathsf{priv}}) \to (\mathsf{MPK}, \mathsf{MSK})$
- $\mathsf{KeyGen}(\mathsf{MSK}, [\mathbf{y}]_2) \to \mathsf{SK}_{\mathbf{y}}, \quad \mathbf{y} = (\mathbf{y}_{\mathsf{pub}}, \mathbf{y}_{\mathsf{priv}})$
- $\mathsf{SlotEnc}(\mathsf{MPK}, [\mathbf{x}_{\mathsf{pub}}]_1) \to \mathsf{CT}_{\mathbf{x}}^{\mathsf{slot}}$
- $\mathsf{Enc}(\mathsf{MSK}, [(\mathbf{x}_{\mathsf{pub}}, \mathbf{x}_{\mathsf{priv}})]_1) \to \mathsf{CT}_{\mathbf{x}}^{\mathsf{norm}}, \quad \mathbf{x} = (\mathbf{x}_{\mathsf{pub}}, \mathbf{x}_{\mathsf{priv}})$
- $\mathsf{Dec}(\mathsf{SK}_{\mathbf{y}}, \mathsf{CT}_{\mathbf{x}}) \to [\langle \mathbf{x}, \mathbf{y} \rangle]_T$

Slot mode Correctness

$\mathsf{SlotEnc}(\mathsf{MPK}, [\mathbf{x}]_1) \approx_c \mathsf{Enc}(\mathsf{MSK}, [(\mathbf{x}_{\mathsf{pub}} \,||\, \mathbf{0})]_1)$

Function-hiding Security

For all queried $\mathbf{x}_\kappa^{(\beta)} = (\mathbf{x}_{\kappa,\mathsf{pub}}^{(\beta)}, \mathbf{x}_{\kappa,\mathsf{priv}}^{(\beta)})$,

$\mathbf{y}_\ell^{(\beta)} = (\mathbf{y}_{\ell,\mathsf{pub}}, \mathbf{y}_{\ell,\mathsf{priv}}^{(\beta)})$ by the adversary,

$$[\langle \mathbf{x}_\kappa^{(0)}, \mathbf{y}_\ell^{(0)} \rangle]_T = [\langle \mathbf{x}_\kappa^{(1)}, \mathbf{y}_\ell^{(1)} \rangle]_T$$

Unbounded IPFE [TT18] using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE

Unbounded IPFE [TT18] using sIPFE

sIPFE = (iS, iKG, iSE, iE, iD)

[TT18] from sIPFE

$\mathsf{SK}_{\mathbf{y}}$: { iKG([($i\sigma_i$, σ_i, y_i, r_i)]$_2$) }$_{i \in I_{\mathbf{y}}}$

$$\sum r_i = 0$$

Unbounded IPFE [TT18] using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE

Index encoding

$\mathsf{SK}_{\mathbf{y}} : \{\ \mathsf{iKG}([(\ i\sigma_i,\ \sigma_i,\ y_i,\ r_i\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$

$$\sum r_i = 0$$

Unbounded IPFE [TT18] using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE

Index encoding

$\mathsf{SK}_{\mathbf{y}} : \{\ \mathsf{iKG}([(\ i\sigma_i,\ \sigma_i,\ y_i,\ r_i\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$

$$\sum r_i = 0$$

$\mathsf{CT}_{\mathbf{x}} : \{\ \mathsf{iSE}([(\ \pi_i,\ -i\pi_i,\ x_i,\ \alpha\ )]_1)\ \}_{i \in [\ell]}$

Index encoding

Unbounded IPFE [TT18] using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE

Index encoding

$$\mathsf{SK}_{\mathbf{y}} : \{\ \mathsf{iKG}([(\ i\sigma_i,\ \sigma_i,\ y_i,\ r_i\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$$

$$\sum r_i = 0$$

$$\mathsf{CT}_{\mathbf{x}} : \{\ \mathsf{iSE}([(\ \pi_i,\ -i\pi_i,\ x_i,\ \alpha\ )]_1)\ \}_{i \in [\ell]}$$

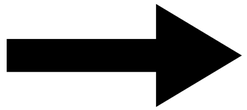
Index encoding

$$[\langle \mathbf{x}, \mathbf{y} \rangle_p]_T \leftarrow \{\ \mathsf{iD}(\mathsf{iSK}_i, \mathsf{iCT}_i)\ \}_{i \in I_{\mathbf{y}}}$$

Extended slotted UIPFE (esUIPFE) using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE



Our esUIPFE

$\mathsf{SK}_{\mathbf{y}} : \{\ \mathsf{iKG}([(\ i\sigma_i,\ \sigma_i,\ \ y_i,\ r_i\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$

$$\sum r_i = 0$$

$\mathsf{CT}_{\mathbf{x}} : \{\ \mathsf{iSE}([(\ \pi_i,\ \ -i\pi_i,\ \ x_i,\ \alpha\ )]_1)\ \}_{i \in [\ell]}$

$[\langle \mathbf{x}, \mathbf{y} \rangle_p]_T \leftarrow \{\ \mathsf{iD}(\mathsf{iSK}_i, \mathsf{iCT}_i)\ \}_{i \in I_{\mathbf{y}}}$

Extended slotted UIPFE (esUIPFE) using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE

$\mathsf{SK}_{\mathbf{y}} : \{ \mathsf{iKG}([(i\sigma_i, \sigma_i, y_i, r_i)]_2) \}_{i \in I_{\mathbf{y}}}$

$$\sum r_i = 0$$

$\mathsf{CT}_{\mathbf{x}} : \{ \mathsf{iSE}([(\pi_i, -i\pi_i, x_i, \alpha)]_1) \}_{i \in [\ell]}$

$[\langle \mathbf{x}, \mathbf{y} \rangle_p]_T \leftarrow \{ \mathsf{iD}(\mathsf{iSK}_i, \mathsf{iCT}_i) \}_{i \in I_{\mathbf{y}}}$

Our esUIPFE

Unboundedness | Extended

$\mathsf{SK}_{\mathbf{y}} : \{ \mathsf{iKG}([(i\sigma_i, \sigma_i, y_{\mathsf{upub},i}, r_i, \mathbf{y}_{\mathsf{bpub},i}, \mathbf{y}_{\mathsf{priv},i})]_2) \}_{i \in I_{\mathbf{y}}}$

Bounded Pub. Slot | Bounded Priv. Slot

$$\sum r_i = 0; \ \sum \mathbf{y}_{\mathsf{bpub},i} = \mathbf{y}_{\mathsf{bpub}}; \ \sum \mathbf{y}_{\mathsf{priv},i} = \mathbf{y}_{\mathsf{priv}}$$

$\mathsf{CT}_{\mathbf{x}}^{\mathsf{slot}} : \{ \mathsf{iSE}([(\pi_i, -i\pi_i, x_{\mathsf{upub},i}, \alpha, \mathbf{x}_{\mathsf{bpub}})]_1) \}_{i \in [\ell]}$

$\mathsf{CT}_{\mathbf{x}}^{\mathsf{norm}} : \{ \mathsf{iE}([(\pi_i, -i\pi_i, x_{\mathsf{upub},i}, \alpha, \mathbf{x}_{\mathsf{bpub}}, \mathbf{x}_{\mathsf{priv}})]_1) \}_{i \in [\ell]}$

Extended slotted UIPFE (esUIPFE) using sIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

[TT18] from sIPFE

$\mathsf{SK}_{\mathbf{y}} : \{ \mathsf{iKG}([(i\sigma_i, \sigma_i, y_i, r_i)]_2) \}_{i \in I_{\mathbf{y}}}$

$$\sum r_i = 0$$

$\mathsf{CT}_{\mathbf{x}} : \{ \mathsf{iSE}([(\pi_i, -i\pi_i, x_i, \alpha)]_1) \}_{i \in [\ell]}$

$[\langle \mathbf{x}, \mathbf{y} \rangle_p]_T \leftarrow \{ \mathsf{iD}(\mathsf{iSK}_i, \mathsf{iCT}_i) \}_{i \in I_{\mathbf{y}}}$

Our esUIPFE

Unboundedness — Extended

$\mathsf{SK}_{\mathbf{y}} : \{ \mathsf{iKG}([(i\sigma_i, \sigma_i, y_{\mathsf{upub},i}, r_i, \mathbf{y}_{\mathsf{bpub},i}, \mathbf{y}_{\mathsf{priv},i})]_2) \}_{i \in I_{\mathbf{y}}}$

Bounded Pub. Slot — Bounded Priv. Slot

$$\sum r_i = 0; \ \sum \mathbf{y}_{\mathsf{bpub},i} = \mathbf{y}_{\mathsf{bpub}}; \ \sum \mathbf{y}_{\mathsf{priv},i} = \mathbf{y}_{\mathsf{priv}}$$

$\mathsf{CT}_{\mathbf{x}}^{\mathsf{slot}} : \{ \mathsf{iSE}([(\pi_i, -i\pi_i, x_{\mathsf{upub},i}, \alpha, \mathbf{x}_{\mathsf{bpub}})]_1) \}_{i \in [\ell]}$

$\mathsf{CT}_{\mathbf{x}}^{\mathsf{norm}} : \{ \mathsf{iE}([(\pi_i, -i\pi_i, x_{\mathsf{upub},i}, \alpha, \mathbf{x}_{\mathsf{bpub}}, \mathbf{x}_{\mathsf{priv}})]_1) \}_{i \in [\ell]}$

$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{ \mathsf{iD}(\mathsf{iSK}_i, \mathsf{iCT}_i) \}_{i \in I_{\mathbf{y}}}$

Extended Computation

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

Our esUIPFE

$\mathsf{eSK}_{\mathbf{y}} : \{\ \mathsf{eKG}([(\ \mathbf{y}_{\mathsf{upub}},\ \mathbf{y}_{\mathsf{bpub}},\ \mathbf{y}_{\mathsf{priv},i}\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$

Unbounded Pub. Slot

Bounded Pub. Slot

Bounded Priv. Slot

$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{slot}} : \{\ \mathsf{eSE}([(\ \mathbf{x}_{\mathsf{upub}},\ \mathbf{x}_{\mathsf{bpub}}\ )]_1)\ \}_{i \in [\ell]}$

$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{norm}} : \{\ \mathsf{eE}([(\ \mathbf{x}_{\mathsf{upub}},\ \mathbf{x}_{\mathsf{bpub}},\ \mathbf{x}_{\mathsf{priv}}\ )]_1)\ \}_{i \in [\ell]}$

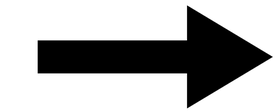
$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{\ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}})\ \}_{i \in I_{\mathbf{y}}}$

Extended Computation

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

Our esUIPFE



$\mathsf{esUIPFE} = (\mathsf{eS}, \mathsf{eKG}, \mathsf{eSE}, \mathsf{eE}, \mathsf{eD})$

Our AB-sUIPFE

$$\mathsf{eSK}_{\mathbf{y}} : \{\ \mathsf{eKG}([(\ \mathbf{y}_{\mathsf{upub},}\ \mathbf{y}_{\mathsf{bpub},}\ \mathbf{y}_{\mathsf{priv},i}\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$$

Unbounded Pub. Slot

Bounded Pub. Slot

Bounded Priv. Slot

$$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{slot}} : \{\ \mathsf{eSE}([(\ \mathbf{x}_{\mathsf{upub},}\ \mathbf{x}_{\mathsf{bpub}}\ )]_1)\ \}_{i \in [\ell]}$$

$$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{norm}} : \{\ \mathsf{eE}([(\ \mathbf{x}_{\mathsf{upub},}\ \mathbf{x}_{\mathsf{bpub},}\ \mathbf{x}_{\mathsf{priv}}\ )]_1)\ \}_{i \in [\ell]}$$

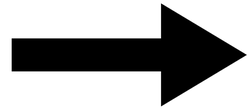
$$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{\ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}})\ \}_{i \in I_{\mathbf{y}}}$$

Extended Computation

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

sIPFE = (iS, iKG, iSE, iE, iD)

Our esUIPFE



esUIPFE = (eS, eKG, eSE, eE, eD)

Our AB-sUIPFE

LSSS Access structure: $\mathbb{A}$; attribute set: S

$\mathsf{eSK}_{\mathbf{y}} : \{\ \mathsf{eKG}([(\ \mathbf{y}_{\mathsf{upub},} \ \mathbf{y}_{\mathsf{bpub},} \ \mathbf{y}_{\mathsf{priv},i}\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$

Unbounded Pub. Slot

Bounded Pub. Slot

Bounded Priv. Slot

$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{slot}} : \{\ \mathsf{eSE}([(\ \mathbf{x}_{\mathsf{upub},} \ \mathbf{x}_{\mathsf{bpub}}\ )]_1)\ \}_{i \in [\ell]}$

$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{norm}} : \{\ \mathsf{eE}([(\ \mathbf{x}_{\mathsf{upub},} \ \mathbf{x}_{\mathsf{bpub},} \ \mathbf{x}_{\mathsf{priv}}\ )]_1)\ \}_{i \in [\ell]}$

$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{\ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}})\ \}_{i \in I_{\mathbf{y}}}$

Extended Computation

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

sIPFE = (iS, iKG, iSE, iE, iD)

Our esUIPFE

esUIPFE = (eS, eKG, eSE, eE, eD)

Our AB-sUIPFE

$\mathsf{eSK}_{\mathbf{y}} : \{ \mathsf{eKG}([(\mathbf{y}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{priv},i})]_2) \}_{i \in I_{\mathbf{y}}}$

Unbounded Pub. Slot

Bounded Pub. Slot

Bounded Priv. Slot

$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{slot}} : \{ \mathsf{eSE}([(\mathbf{x}_{\mathsf{upub}}, \mathbf{x}_{\mathsf{bpub}})]_1) \}_{i \in [\ell]}$

$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{norm}} : \{ \mathsf{eE}([(\mathbf{x}_{\mathsf{upub}}, \mathbf{x}_{\mathsf{bpub}}, \mathbf{x}_{\mathsf{priv}})]_1) \}_{i \in [\ell]}$

$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}}) \}_{i \in I_{\mathbf{y}}}$

Extended Computation

LSSS Access structure: $\mathbb{A}$; attribute set: S

- Sample $a_0 \leftarrow \$$; $(a_j)_{j \in \mathsf{List\text{-}Att}(\mathbb{A})} \leftarrow \Lambda_{a_0}(\mathbb{A})$
- $\mathbb{A}(\mathsf{S}) = 1$, compute reconstruction vector $\mathbf{c} = (c_j)_j$:

$$a_0 = \sum_{j \in \mathsf{S}} c_j a_j$$

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

$\mathsf{sIPFE} = (\mathsf{iS}, \mathsf{iKG}, \mathsf{iSE}, \mathsf{iE}, \mathsf{iD})$

Our esUIPFE

$\mathsf{esUIPFE} = (\mathsf{eS}, \mathsf{eKG}, \mathsf{eSE}, \mathsf{eE}, \mathsf{eD})$

Our AB-sUIPFE

$$a_0 = \sum_{j \in S} c_j a_j$$

$$\mathsf{eSK}_{\mathbf{y}} : \{\ \mathsf{eKG}([(\ \mathbf{y}_{\mathsf{upub},} \ \ \mathbf{y}_{\mathsf{bpub},} \ \ \mathbf{y}_{\mathsf{priv},i}\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$$

Unbounded Pub. Slot

Bounded Pub. Slot

Bounded Priv. Slot

$$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{slot}} : \{\ \mathsf{eSE}([(\ \mathbf{x}_{\mathsf{upub},} \ \ \mathbf{x}_{\mathsf{bpub}}\ )]_1)\ \}_{i \in [\ell]}$$

$$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{norm}} : \{\ \mathsf{eE}([(\ \mathbf{x}_{\mathsf{upub},} \ \ \mathbf{x}_{\mathsf{bpub},} \ \ \mathbf{x}_{\mathsf{priv}}\ )]_1)\ \}_{i \in [\ell]}$$

$$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{\ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}})\ \}_{i \in I_{\mathbf{y}}}$$

Extended Computation

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

sIPFE = (iS, iKG, iSE, iE, iD)

Our esUIPFE

esUIPFE = (eS, eKG, eSE, eE, eD)

Our AB-sUIPFE

$$a_0 = \sum_{j \in S} c_j a_j$$

$$\mathsf{eSK}_{\mathbf{y}} : \{\ \mathsf{eKG}([(\ \mathbf{y}_{\mathsf{upub}},\ \mathbf{y}_{\mathsf{bpub}},\ \mathbf{y}_{\mathsf{priv},i}\ )]_2)\ \}_{i \in I_{\mathbf{y}}}$$

Unbounded Pub. Slot — Bounded Pub. Slot — Bounded Priv. Slot

$$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{slot}} : \{\ \mathsf{eSE}([(\ \mathbf{x}_{\mathsf{upub}},\ \mathbf{x}_{\mathsf{bpub}}\ )]_1)\ \}_{i \in [\ell]}$$

$$\mathsf{eCT}_{\mathbf{x}}^{\mathsf{norm}} : \{\ \mathsf{eE}([(\ \mathbf{x}_{\mathsf{upub}},\ \mathbf{x}_{\mathsf{bpub}},\ \mathbf{x}_{\mathsf{priv}}\ )]_1)\ \}_{i \in [\ell]}$$

$$\mathsf{SK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{iKG}([(\ j\sigma_j,\ \sigma_j,\ a_j \cdot z\ )]_2)\ \}_{j \in \mathsf{List\text{-}Att}(\mathbb{A})}$$
$$\{\ \mathsf{eKG}([(\ \mathbf{y},\ a_0 \cdot z,\ \mathbf{y}_{\mathsf{priv}}\ )]_2)\ \}$$

Acc. Cont. — Function Hiding

$$\mathsf{CT}_{\mathsf{S},\mathbf{x}}^{\mathsf{slot}} : \{\ \mathsf{iSE}([(\ \pi_j,\ -j\pi_j,\ \psi\ )]_1)\ \}_{j \in S}$$
$$\{\ \mathsf{eSE}([(\ \mathbf{x},\ \psi\ )]_1)\ \}$$

$$\mathsf{CT}_{\mathsf{S},\mathbf{x}}^{\mathsf{norm}} : \{\ \mathsf{iSE}([(\ \pi_j,\ -j\pi_j,\ \psi\ )]_1)\ \}_{j \in S}$$
$$\{\ \mathsf{eE}([(\ \mathbf{x},\ \psi,\ \mathbf{x}_{\mathsf{priv}}\ )]_1)\ \}$$

$$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{\ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}})\ \}_{i \in I_{\mathbf{y}}}$$

Extended Computation

Attribute-Based sUIPFE (AB-sUIPFE) using esUIPFE

sIPFE = (iS, iKG, iSE, iE, iD)

Our esUIPFE

esUIPFE = (eS, eKG, eSE, eE, eD)

Our AB-sUIPFE

$$a_0 = \sum_{j \in S} c_j a_j$$

$\mathsf{eSK}_{\mathbf{y}} : \{ \mathsf{eKG}([(\mathbf{y}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{priv},i})]_2) \}_{i \in I_{\mathbf{y}}}$

Unbounded Pub. Slot — Bounded Pub. Slot — Bounded Priv. Slot

$\mathsf{eCT}^{\mathsf{slot}}_{\mathbf{x}} : \{ \mathsf{eSE}([(\mathbf{x}_{\mathsf{upub}}, \mathbf{x}_{\mathsf{bpub}})]_1) \}_{i \in [\ell]}$

$\mathsf{eCT}^{\mathsf{norm}}_{\mathbf{x}} : \{ \mathsf{eE}([(\mathbf{x}_{\mathsf{upub}}, \mathbf{x}_{\mathsf{bpub}}, \mathbf{x}_{\mathsf{priv}})]_1) \}_{i \in [\ell]}$

$\mathsf{SK}_{\mathbb{A},\mathbf{y}} : \{ \mathsf{iKG}([(j\sigma_j, \sigma_j, a_j \cdot z)]_2) \}_{j \in \mathsf{List\text{-}Att}(\mathbb{A})}$
$\{ \mathsf{eKG}([(\mathbf{y}, a_0 \cdot z, \mathbf{y}_{\mathsf{priv}})]_2) \}$

Acc. Cont. — Function Hiding

$\mathsf{CT}^{\mathsf{slot}}_{\mathsf{S},\mathbf{x}} : \{ \mathsf{iSE}([(\pi_j, -j\pi_j, \psi)]_1) \}_{j \in S}$
$\{ \mathsf{eSE}([(\mathbf{x}, \psi)]_1) \}$

$\mathsf{CT}^{\mathsf{norm}}_{\mathsf{S},\mathbf{x}} : \{ \mathsf{iSE}([(\pi_j, -j\pi_j, \psi)]_1) \}_{j \in S}$
$\{ \mathsf{eE}([(\mathbf{x}, \psi, \mathbf{x}_{\mathsf{priv}})]_1) \}$

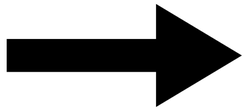
$[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{bpub}}, \mathbf{y}_{\mathsf{bpub}} \rangle + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \{ \mathsf{eD}(\mathsf{eSK}_{\mathbf{y}}, \mathsf{eCT}_{\mathbf{y}}) \}_{i \in I_{\mathbf{y}}}$

Extended Computation

If $\mathbb{A}(S) = 1$, $[\langle \mathbf{x}, \mathbf{y} \rangle_p + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \mathsf{eD}(\mathsf{eSK}, \mathsf{eCT})$;
$\{ \mathsf{iD}(\mathsf{iSK}_j, \mathsf{iCT}_j) \}_{j \in S}$

Multi-Client Extension via AB-sUIPFE

Our AB-sUIPFE



Our MC-AB-UIPFE

$\mathsf{aSK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\ \mathbf{y}_{\mathsf{upub}},\ \mathbf{y}_{\mathsf{priv}}\ )]_2,\ \mathbb{A})\ \}$

Unbounded Pub. Slot

Bounded Function Hiding Priv. Slot

$\mathsf{aCT}^{\mathsf{slot}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aSE}([(\ \mathbf{x}_{\mathsf{upub}}\ )]_1,\ \ \mathsf{S})\ \}$

$\mathsf{aCT}^{\mathsf{norm}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aE}([(\ \mathbf{x}_{\mathsf{upub}},\ \ \mathbf{x}_{\mathsf{priv}}\ )]_1,\ \ \mathsf{S})\ \}$

If $\mathbb{A}(\mathsf{S}) = 1$,

$[\langle \mathbf{x}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{upub}} \rangle_p + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \mathsf{aD}(\mathsf{aSK}_{\mathbb{A},\mathbf{y}}, \mathsf{aCT}_{\mathsf{S},\mathbf{x}})$

Multi-Client Extension via AB-sUIPFE

Our AB-sUIPFE

$\mathsf{aSK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\mathbf{y}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{priv}})]_2, \mathbb{A})\ \}$

Unbounded Pub. Slot

Bounded Function Hiding Priv. Slot

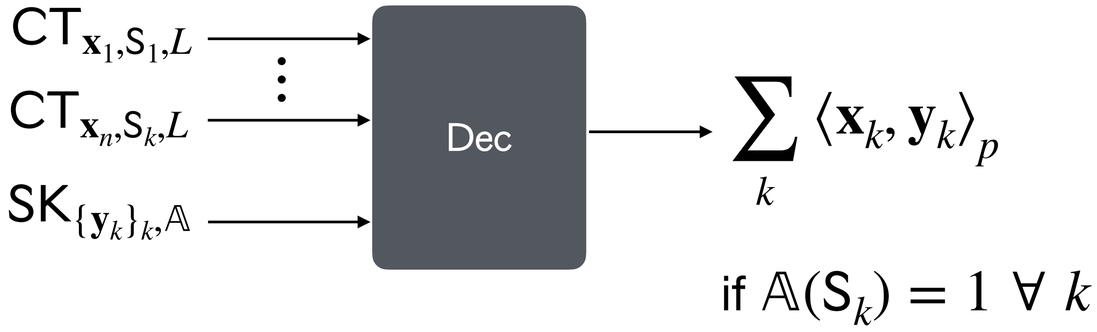
$\mathsf{aCT}^{\mathsf{slot}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aSE}([(\mathbf{x}_{\mathsf{upub}})]_1, \mathsf{S})\ \}$

$\mathsf{aCT}^{\mathsf{norm}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aE}([(\mathbf{x}_{\mathsf{upub}}, \mathbf{x}_{\mathsf{priv}})]_1, \mathsf{S})\ \}$

If $\mathbb{A}(\mathsf{S}) = 1$,

$[\langle \mathbf{x}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{upub}} \rangle_p + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \mathsf{aD}(\mathsf{aSK}_{\mathbb{A},\mathbf{y}}, \mathsf{aCT}_{\mathsf{S},\mathbf{x}})$

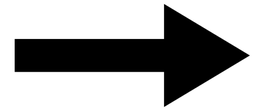
Our MC-AB-UIPFE



Multi-Client Extension via AB-sUIPFE

$\mathsf{AB\text{-}sUIPFE} = (\mathsf{aS}, \mathsf{aKG}, \mathsf{aSE}, \mathsf{aE}, \mathsf{aD})$

Our AB-sUIPFE



Our MC-AB-UIPFE

$\mathsf{aSK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\ \mathbf{y}_{\mathsf{upub}},\ \mathbf{y}_{\mathsf{priv}}\ )]_2,\ \mathbb{A})\ \}$

Unbounded Pub. Slot

Bounded Function Hiding Priv. Slot

$\mathsf{aCT}^{\mathsf{slot}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aSE}([(\ \mathbf{x}_{\mathsf{upub}}\ )]_1,\ \ \mathsf{S})\ \}$

$\mathsf{aCT}^{\mathsf{norm}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aE}([(\ \mathbf{x}_{\mathsf{upub}},\ \ \mathbf{x}_{\mathsf{priv}}\ )]_1,\ \ \mathsf{S})\ \}$

If $\mathbb{A}(\mathsf{S}) = 1$,

$[\langle \mathbf{x}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{upub}} \rangle_p + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \mathsf{aD}(\mathsf{aSK}_{\mathbb{A},\mathbf{y}}, \mathsf{aCT}_{\mathsf{S},\mathbf{x}})$

Multi-Client Extension via AB-sUIPFE

$\mathsf{AB\text{-}sUIPFE} = (\mathsf{aS}, \mathsf{aKG}, \mathsf{aSE}, \mathsf{aE}, \mathsf{aD})$

Our AB-sUIPFE

$\mathsf{aSK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\ \mathbf{y}_{\mathsf{upub}},\ \mathbf{y}_{\mathsf{priv}}\ )]_2,\ \mathbb{A})\ \}$

Unbounded Pub. Slot

Bounded Function Hiding Priv. Slot

$\mathsf{aCT}^{\mathsf{slot}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aSE}([(\ \mathbf{x}_{\mathsf{upub}}\ )]_1,\ \mathsf{S})\ \}$

$\mathsf{aCT}^{\mathsf{norm}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aE}([(\ \mathbf{x}_{\mathsf{upub}},\ \mathbf{x}_{\mathsf{priv}}\ )]_1,\ \mathsf{S})\ \}$

If $\mathbb{A}(\mathsf{S}) = 1$,

$[\langle \mathbf{x}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{upub}} \rangle_p + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \mathsf{aD}(\mathsf{aSK}_{\mathbb{A},\mathbf{y}}, \mathsf{aCT}_{\mathsf{S},\mathbf{x}})$

Our MC-AB-UIPFE

$\mathsf{SK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\ \mathbf{y}_k,\ \alpha,\ 0\ )]_2,\ \mathbb{A})\}_k$

Unbounded

$\mathsf{CT}_{\mathsf{S}_k,\mathbf{x}_k} : \{\mathsf{aE}([(\ \mathbf{x}_k,\ \mathbf{s}_k,\ 0\ )]_1),\ \mathsf{S}_k\}$

Unbounded

$$\mathbf{s}_k = \sum_{k \neq k'} (-1)^{k<k'} \mathsf{PRF}^{\mathsf{seed}_{k,k'}}(L)$$

Secret share of 0 over k

Multi-Client Extension via AB-sUIPFE

$\mathsf{AB\text{-}sUIPFE} = (\mathsf{aS}, \mathsf{aKG}, \mathsf{aSE}, \mathsf{aE}, \mathsf{aD})$

Our AB-sUIPFE

$\mathsf{aSK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\ \mathbf{y}_{\mathsf{upub}},\ \mathbf{y}_{\mathsf{priv}}\ )]_2,\ \mathbb{A})\ \}$

Unbounded Pub. Slot

Bounded Function Hiding Priv. Slot

$\mathsf{aCT}^{\mathsf{slot}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aSE}([(\ \mathbf{x}_{\mathsf{upub}}\ )]_1,\ \mathsf{S})\ \}$

$\mathsf{aCT}^{\mathsf{norm}}_{\mathsf{S},\mathbf{x}} : \{\ \mathsf{aE}([(\ \mathbf{x}_{\mathsf{upub}},\ \mathbf{x}_{\mathsf{priv}}\ )]_1,\ \mathsf{S})\ \}$

If $\mathbb{A}(\mathsf{S}) = 1$,

$[\langle \mathbf{x}_{\mathsf{upub}}, \mathbf{y}_{\mathsf{upub}} \rangle_p + \langle \mathbf{x}_{\mathsf{priv}}, \mathbf{y}_{\mathsf{priv}} \rangle]_T \leftarrow \mathsf{aD}(\mathsf{aSK}_{\mathbb{A},\mathbf{y}}, \mathsf{aCT}_{\mathsf{S},\mathbf{x}})$

Our MC-AB-UIPFE

$\mathsf{SK}_{\mathbb{A},\mathbf{y}} : \{\ \mathsf{aKG}([(\ \mathbf{y}_k,\ \alpha,\ 0\ )]_2,\ \mathbb{A})\}_k$

Unbounded

$\mathsf{CT}_{\mathsf{S}_k,\mathbf{x}_k} : \{\mathsf{aE}([(\ \mathbf{x}_k,\ \mathbf{s}_k,\ 0\ )]_1),\ \mathsf{S}_k\}$

Unbounded

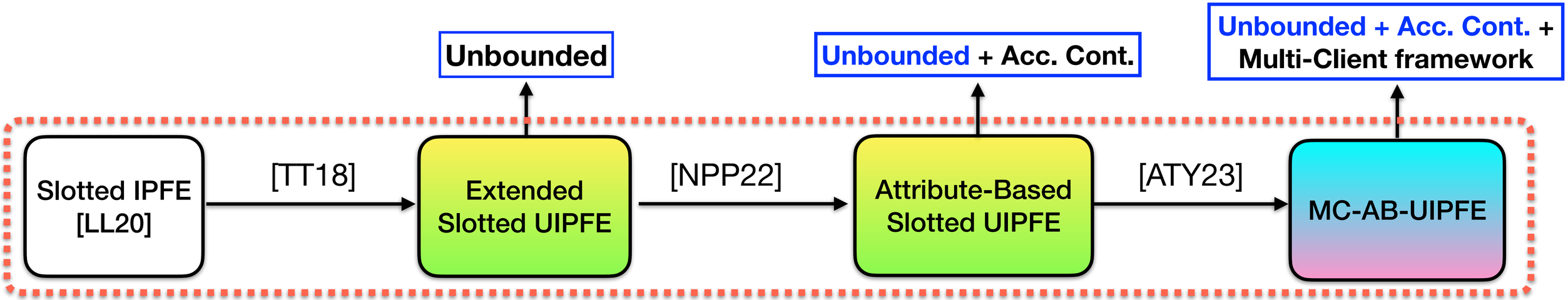
$\mathbf{s}_k = \sum_{k \neq k'} (-1)^{k<k'} \mathsf{PRF}^{\mathsf{seed}_{k,k'}}(L)$

Secret share of 0 over k

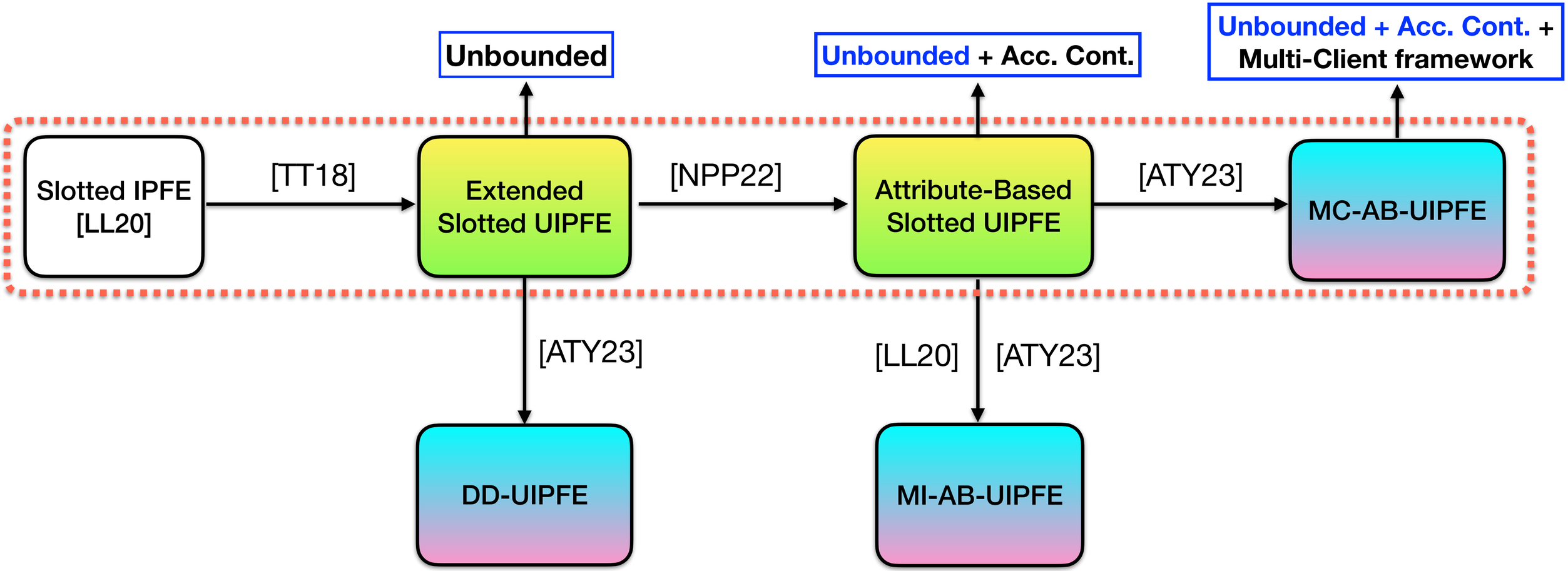
$\forall\ k,\ \mathbb{A}(\mathsf{S}_k) = 1,$

$$\left[\sum_k \langle \mathbf{x}_k, \mathbf{y}_k \rangle_p\right]_T \leftarrow \{\ \mathsf{aD}(\mathsf{aSK}_{\mathbb{A},\mathbf{y}_k}, \mathsf{aCT}_{\mathsf{S}_k,\mathbf{x}_k})\ \}_k$$

Technical Steps Towards MC-AB-UIPFE



Technical Steps Towards MC-AB-UIPFE



Technical Steps Towards MC-AB-UIPFE

Conclusion

- Formalize the notion of ‘**unboundedness**’ in MC-AB-UIPFE, MI-AB-UIPFE and DD-UIPFE.
- Realizing access control via **LSSS access structure** in MC-AB-UIPFE, MI-AB-UIPFE.
- A generic compiler from sIPFE to MC-AB-UIPFE.

Conclusion

- Formalize the notion of '**unboundedness**' in MC-AB-UIPFE, MI-AB-UIPFE and DD-UIPFE.
- Realizing access control via **LSSS access structure** in MC-AB-UIPFE, MI-AB-UIPFE.
- A generic compiler from sIPFE to MC-AB-UIPFE.

Open Problems:

- Upgrade the security of MC-AB-UIPFE from one-time label to multi-label scenarios.
- Adding access control feature in DD-UIPFE.

Thank You

For Your Attention!

Any Questions

Full version : https://ia.cr/2025/423