Decentralized Multi-Authority Attribute-Based Inner-Product FE: Large Universe and Unbounded

Pratish Datta
NTT Research

Tapas Pal
NTT SIL

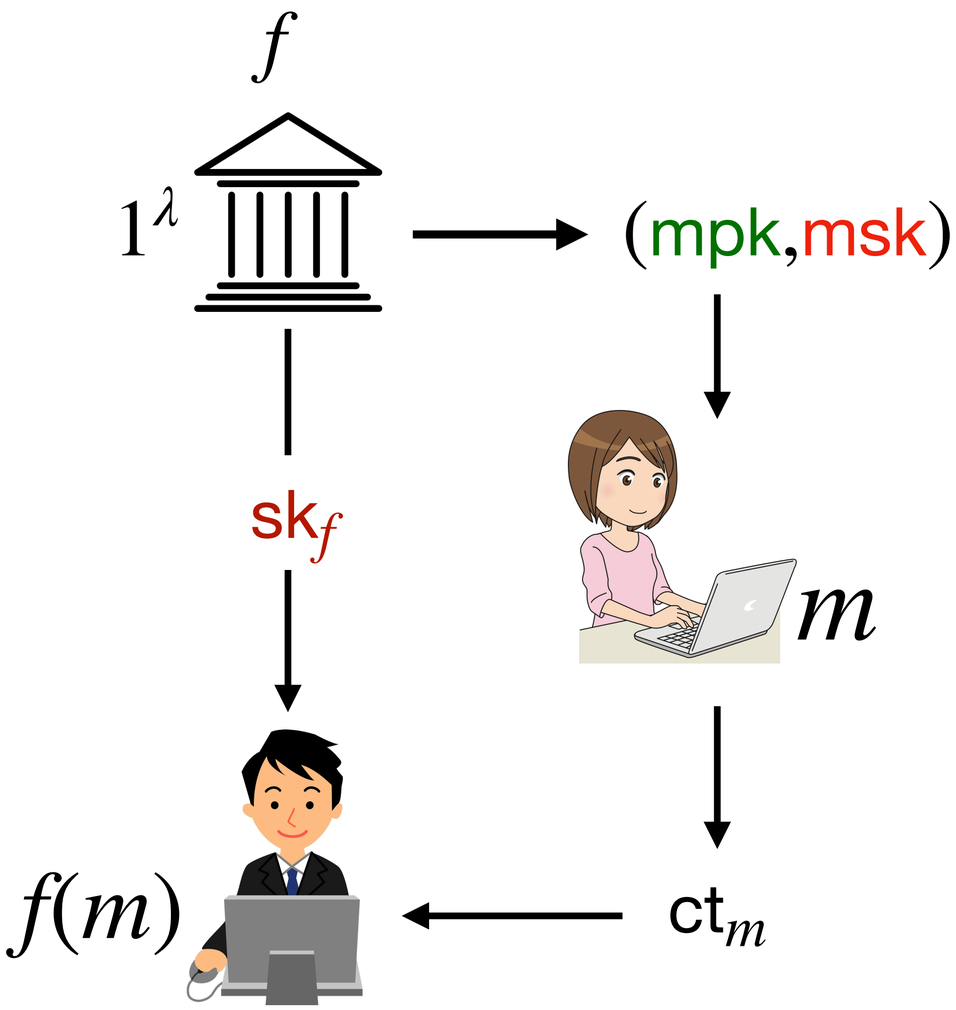
Functional Encryption [BSW11]

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

$\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{sk}_f$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_m) \to f(m)$



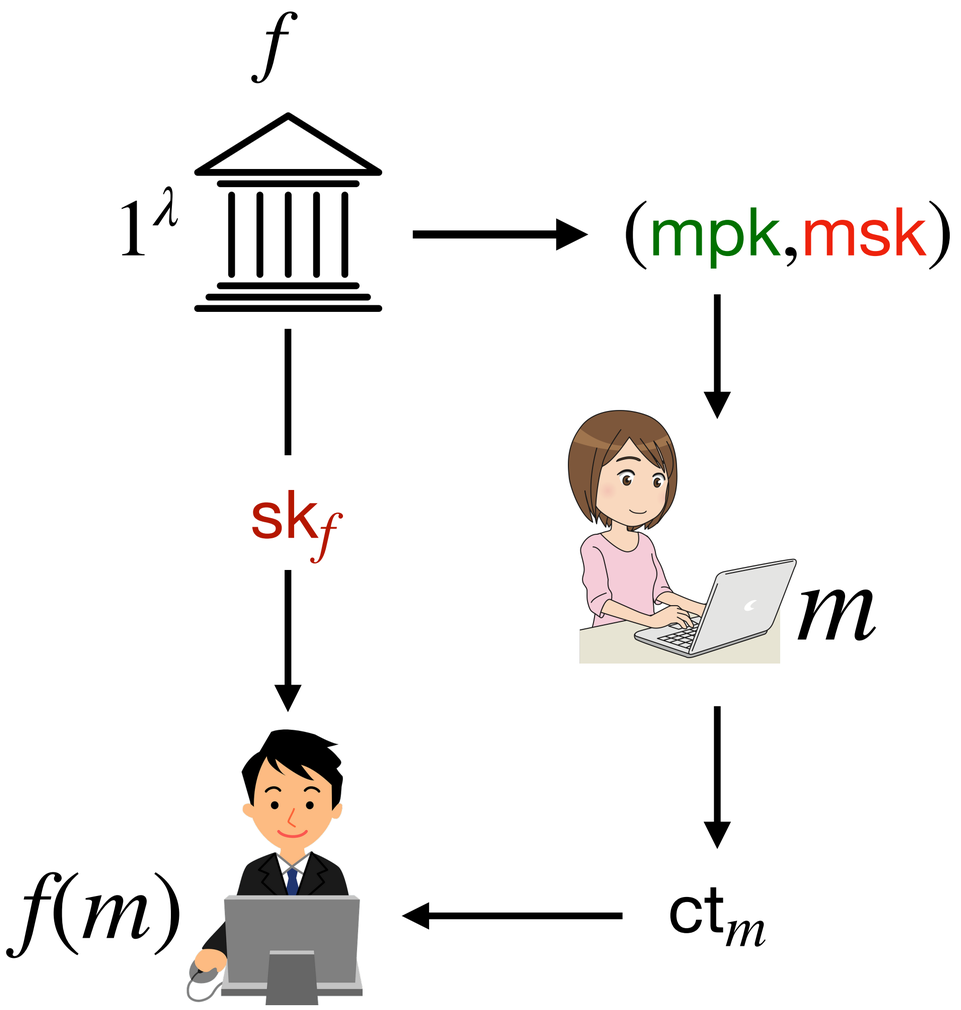
Functional Encryption: Security [BSW11]

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

$\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{sk}_f$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_m) \to f(m)$



Security: users learn *only* $f(m)$

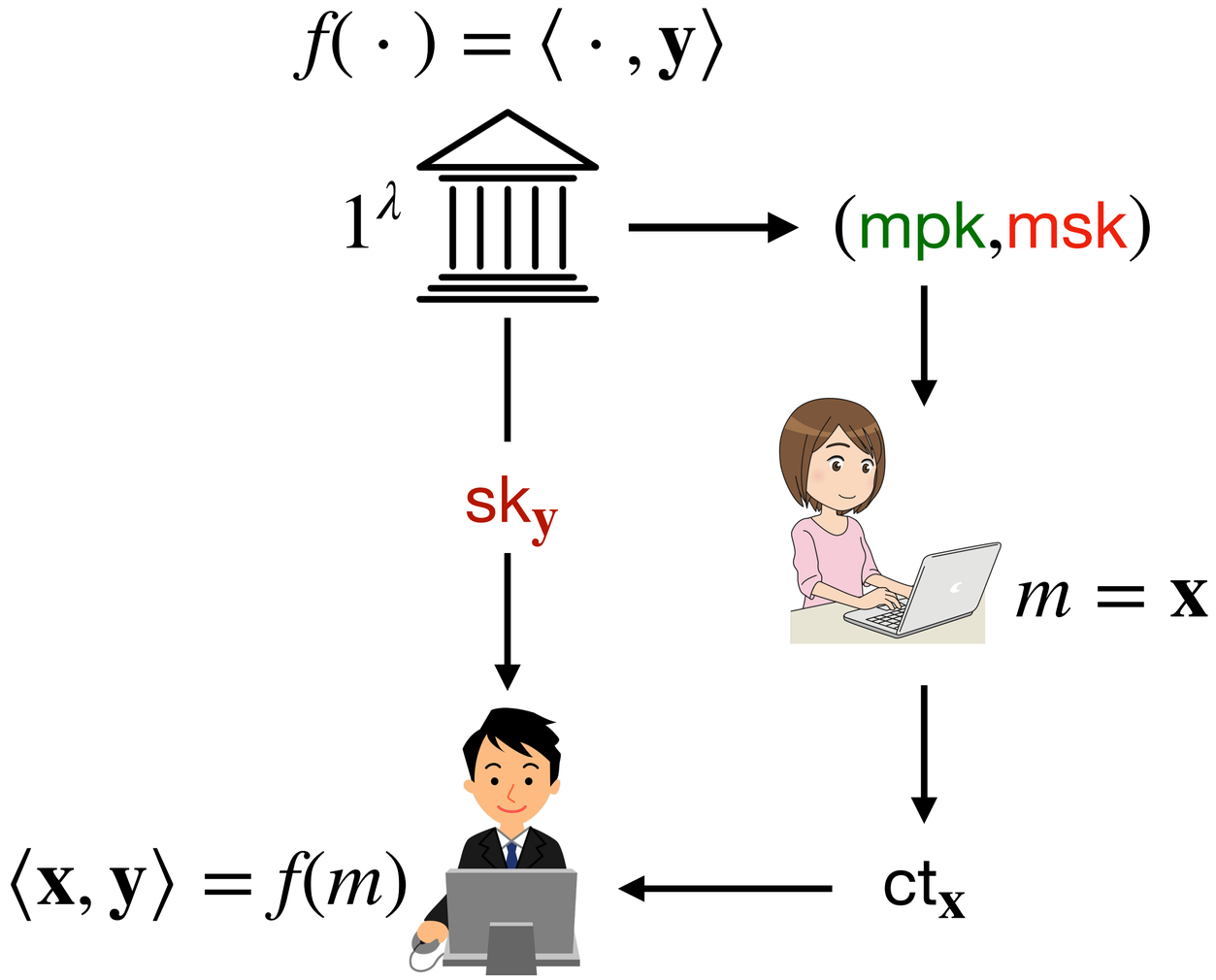
Inner Product Functional Encryption (IPFE) [ABDP15, ALS16]

Setup$(1^n) \to$ (mpk, msk)

KeyGen(msk, $\mathbf{y}$) $\to$ sk$_{\mathbf{y}}$

Enc(mpk, $\mathbf{x}$) $\to$ ct$_{\mathbf{x}}$

Dec(sk$_{\mathbf{y}}$, ct$_{\mathbf{x}}$) $\to \langle \mathbf{x}, \mathbf{y} \rangle$



Leakage of message in IPFE

Setup$(1^n) \rightarrow$ (mpk, msk)

KeyGen(msk, $\mathbf{y}$) $\rightarrow$ sk$_{\mathbf{y}}$

Enc(mpk, $\mathbf{x}$) $\rightarrow$ ct$_{\mathbf{x}}$

Dec(sk$_{\mathbf{y}}$, ct$_{\mathbf{x}}$) $\rightarrow \langle \mathbf{x}, \mathbf{y} \rangle$

- sk$_{\mathbf{y}}$ reveals $\langle \mathbf{x}, \mathbf{y} \rangle$
- release sufficient # sk$_{\mathbf{y}_i}$

$$\text{solve} \begin{pmatrix} \cdots & \mathbf{y}_1 & \cdots \\ & \vdots & \\ \cdots & \mathbf{y}_n & \cdots \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \langle \mathbf{x}, \mathbf{y}_1 \rangle \\ \vdots \\ \langle \mathbf{x}, \mathbf{y}_n \rangle \end{pmatrix} \text{ for } \mathbf{x}$$

- system is completely broken

Leakage of message in IPFE

Setup$(1^n) \rightarrow$ (mpk, msk)

KeyGen(msk, $\mathbf{y}$) $\rightarrow$ sk$_{\mathbf{y}}$

Enc(mpk, $\mathbf{x}$) $\rightarrow$ ct$_{\mathbf{x}}$

Dec(sk$_{\mathbf{y}}$, ct$_{\mathbf{x}}$) $\rightarrow \langle \mathbf{x}, \mathbf{y} \rangle$

- sk$_{\mathbf{y}}$ reveals $\langle \mathbf{x}, \mathbf{y} \rangle$
- release sufficient # sk$_{\mathbf{y}_i}$

$$\text{solve} \begin{pmatrix} \cdots & \mathbf{y}_1 & \cdots \\ & \vdots & \\ \cdots & \mathbf{y}_n & \cdots \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \langle \mathbf{x}, \mathbf{y}_1 \rangle \\ \vdots \\ \langle \mathbf{x}, \mathbf{y}_n \rangle \end{pmatrix} \text{ for } \mathbf{x}$$

- system is completely broken
- Cannot release sk$_{\mathbf{y}}$ for n L.I. $\mathbf{y}$ vectors

Leakage is high

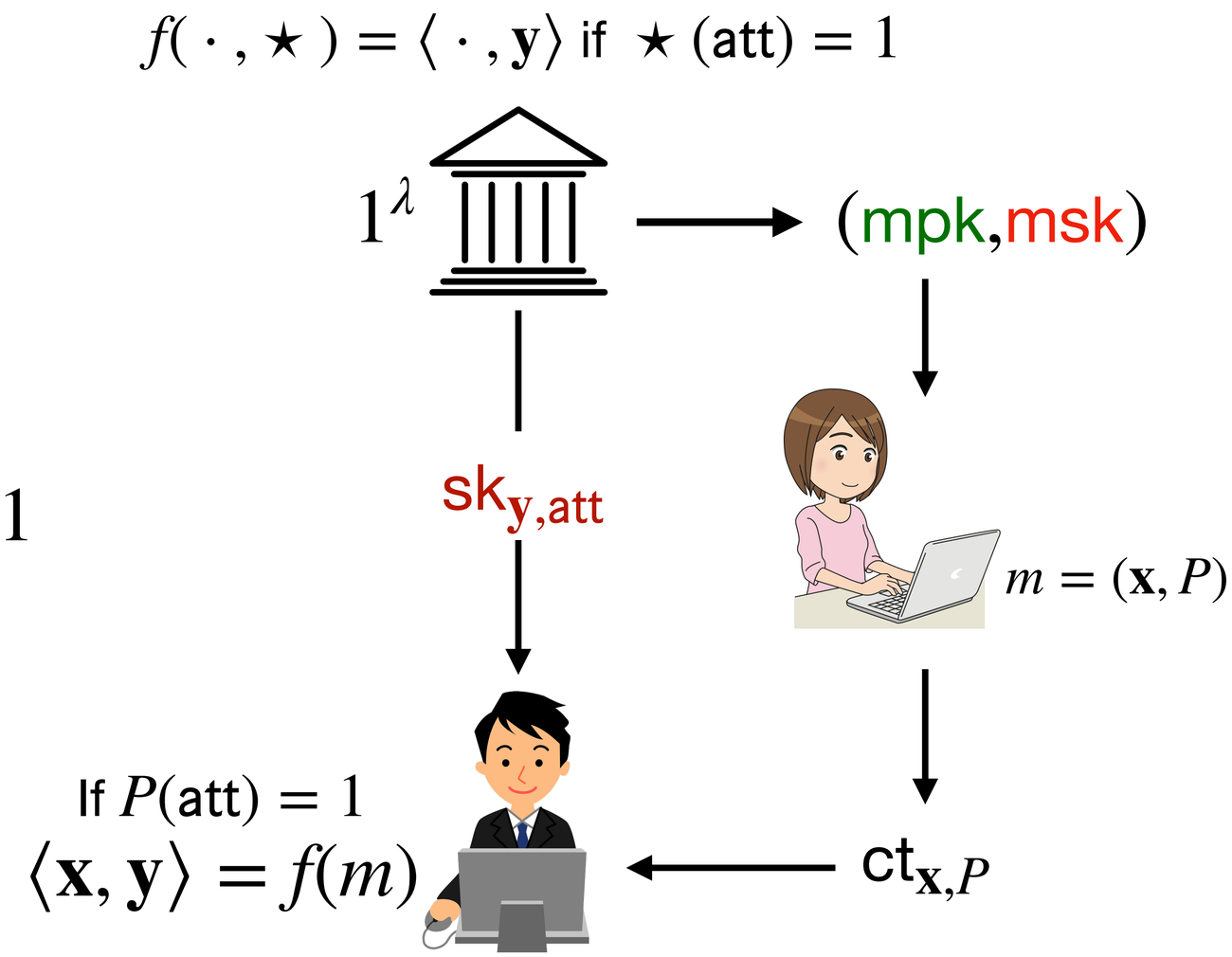
Attribute-Based IPFE (ABIPFE) [ACGU20]

Setup$(1^\lambda, 1^n) \to$ (mpk, msk)

KeyGen(msk, $\mathbf{y}$, att) $\to$ sk$_{\mathbf{y},\text{att}}$

Enc(mpk, $\mathbf{x}, P$) $\to$ ct$_{\mathbf{x},P}$

Dec(sk$_{\mathbf{y},\text{att}}$, ct$_{\mathbf{x},P}$) $\to \langle \mathbf{x}, \mathbf{y} \rangle$ if $P(\text{att}) = 1$



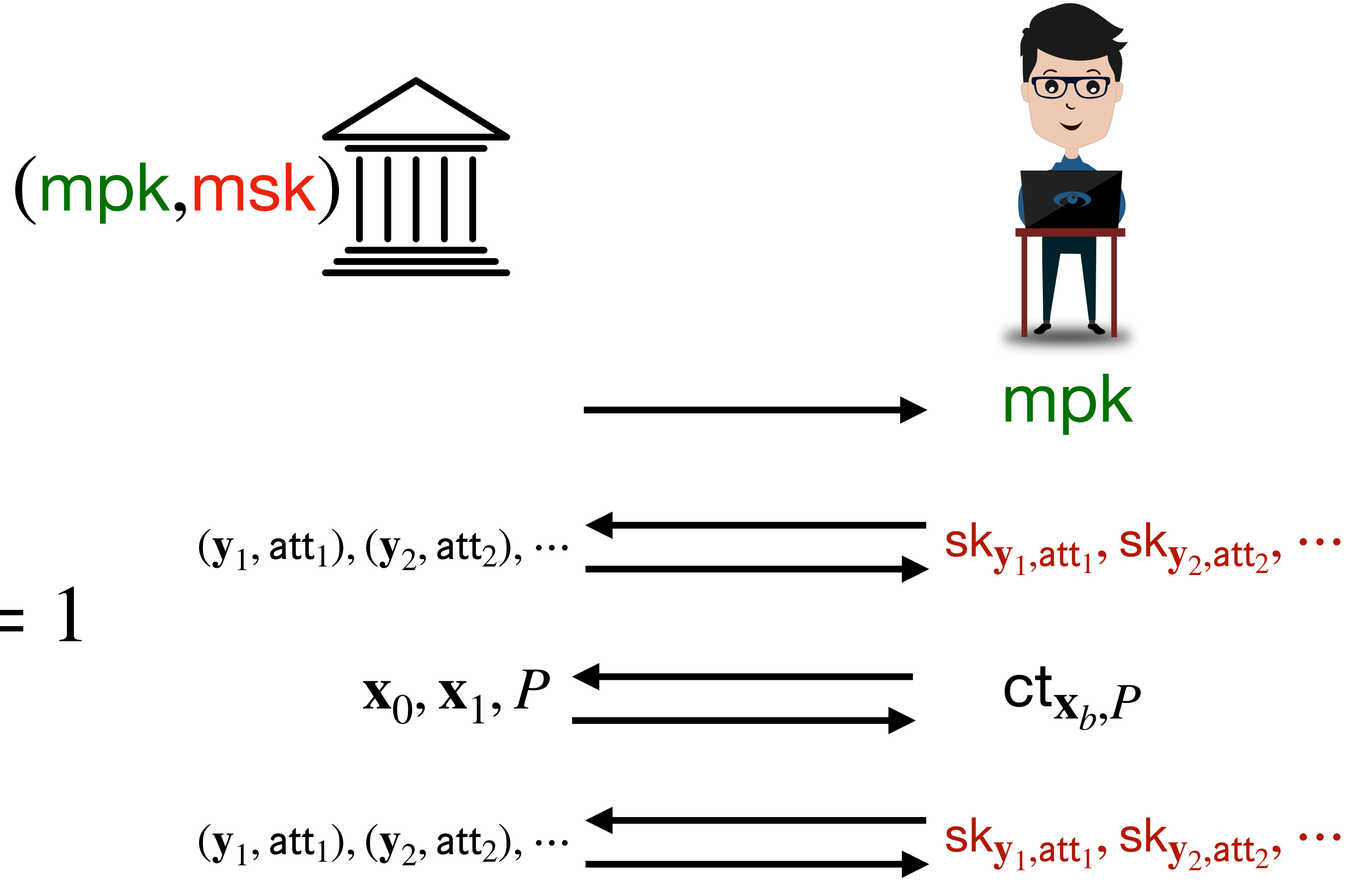
ABIPFE: IND-based Security [ACGU20]

Setup$(1^\lambda, 1^n) \rightarrow$ (mpk, msk)

KeyGen(msk, $\mathbf{y}$, att) $\rightarrow$ sk$_{\mathbf{y},\text{att}}$

Enc(mpk, $\mathbf{x}, P$) $\rightarrow$ ct$_{\mathbf{x},P}$

Dec(sk$_{\mathbf{y},\text{att}}$, ct$_{\mathbf{x},P}$) $\rightarrow \langle \mathbf{x}, \mathbf{y} \rangle$ if $P(\text{att}) = 1$



$\langle \mathbf{x}_0, \mathbf{y}_i \rangle = \langle \mathbf{x}_1, \mathbf{y}_i \rangle \ \forall i$ s.t. $P(\text{att}_i) = 1$

Security: cannot guess b

ABIPFE: IND-based Security [ACGU20]

Setup$(1^\lambda, 1^n) \rightarrow$ (mpk, msk)

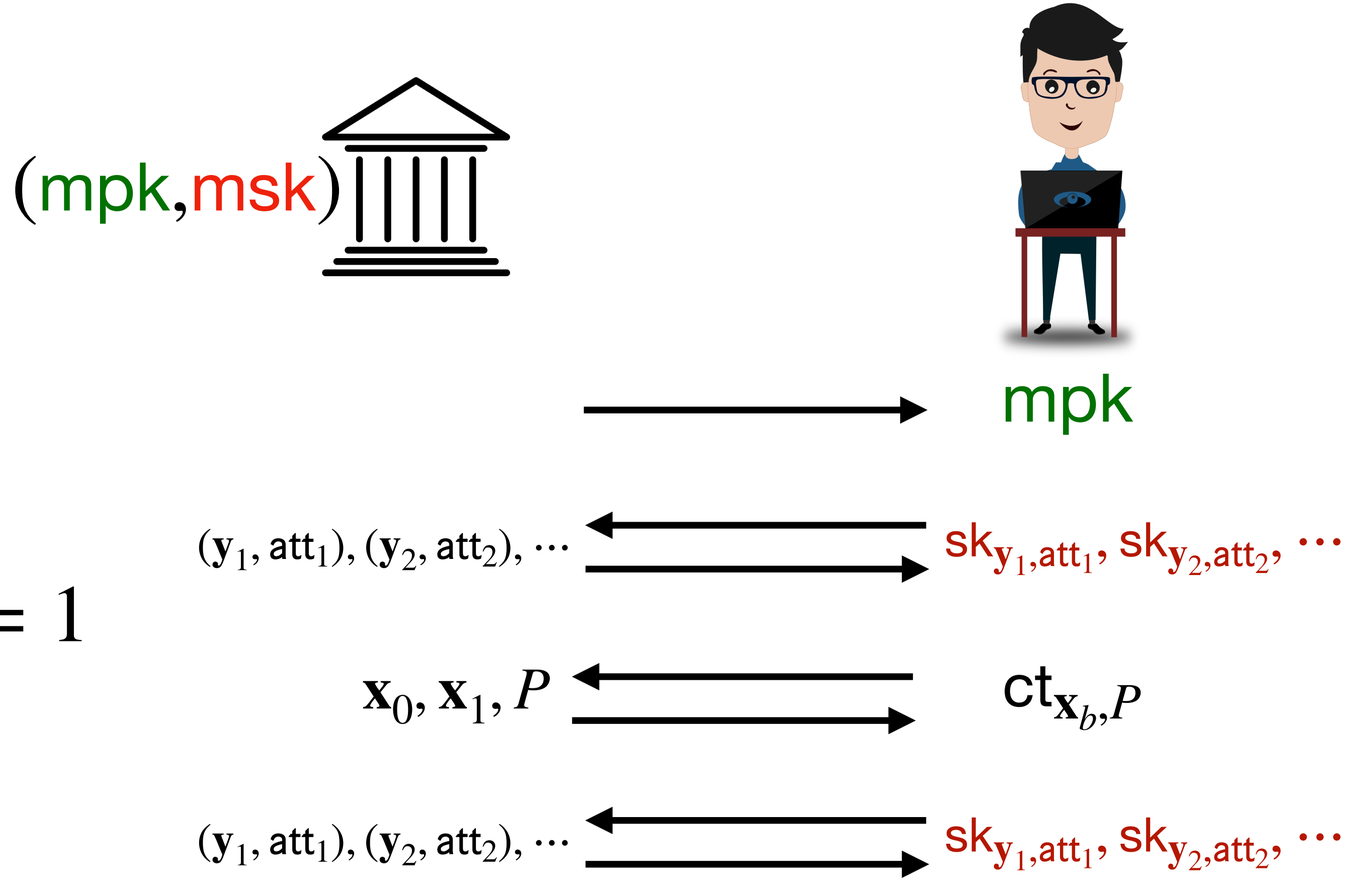
KeyGen(msk, $\mathbf{y}$, att) $\rightarrow$ sk$_{\mathbf{y},\text{att}}$

Enc(mpk, $\mathbf{x}, P$) $\rightarrow$ ct$_{\mathbf{x},P}$

Dec(sk$_{\mathbf{y},\text{att}}$, ct$_{\mathbf{x},P}$) $\rightarrow \langle \mathbf{x}, \mathbf{y} \rangle$ if $P(\text{att}) = 1$

- Can release sk$_{\mathbf{y}}$ for n L.I. $\mathbf{y}$ vectors unless these are associated to satisfying attributes.

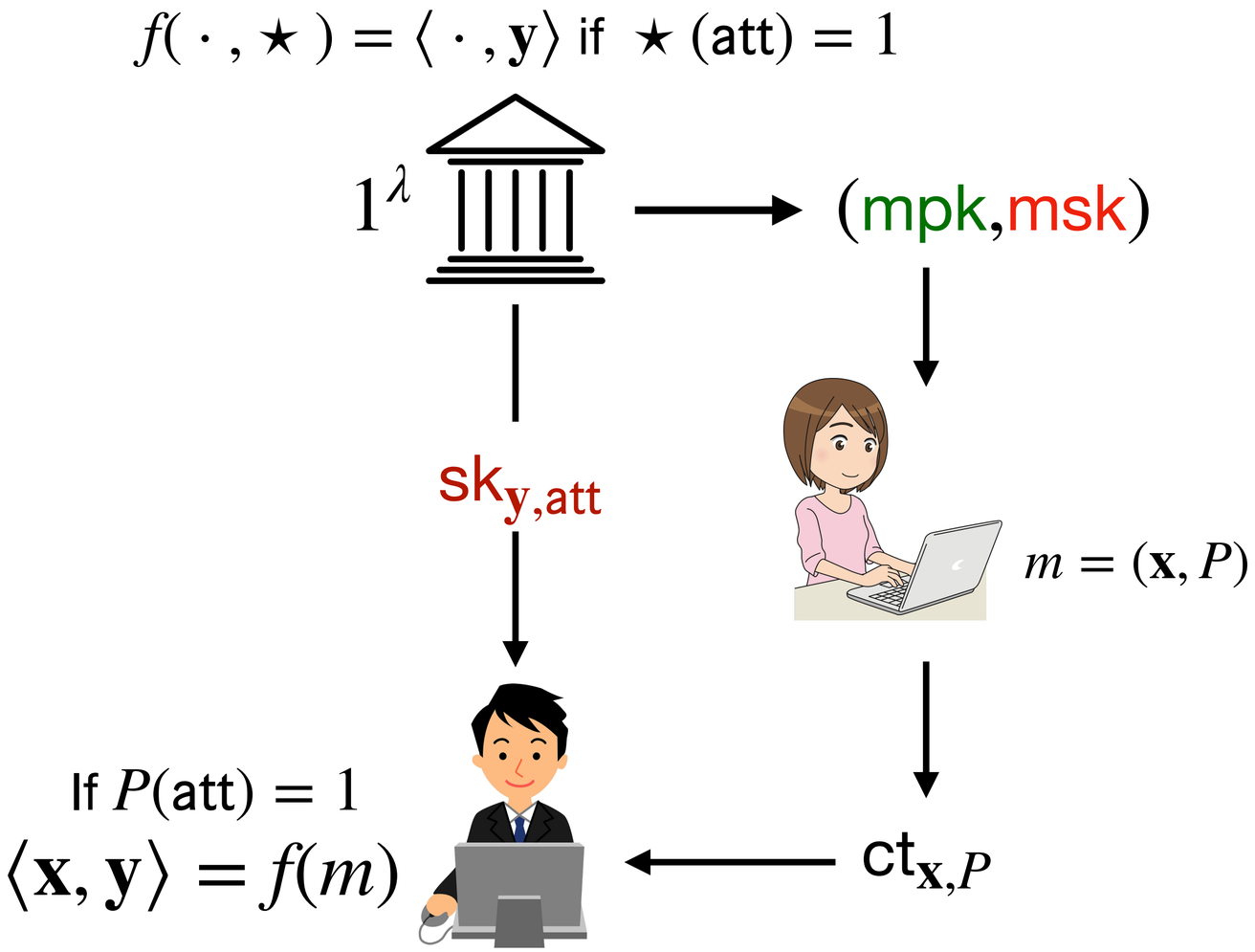
manage leakage by access control



$\langle \mathbf{x}_0, \mathbf{y}_i \rangle = \langle \mathbf{x}_1, \mathbf{y}_i \rangle \ \forall i$ s.t. $P(\text{att}_i) = 1$

Security: cannot guess b

Attribute-Based IPFE (ABIPFE): Application in IoMT



Attribute-Based IPFE (ABIPFE): Application in IoMT

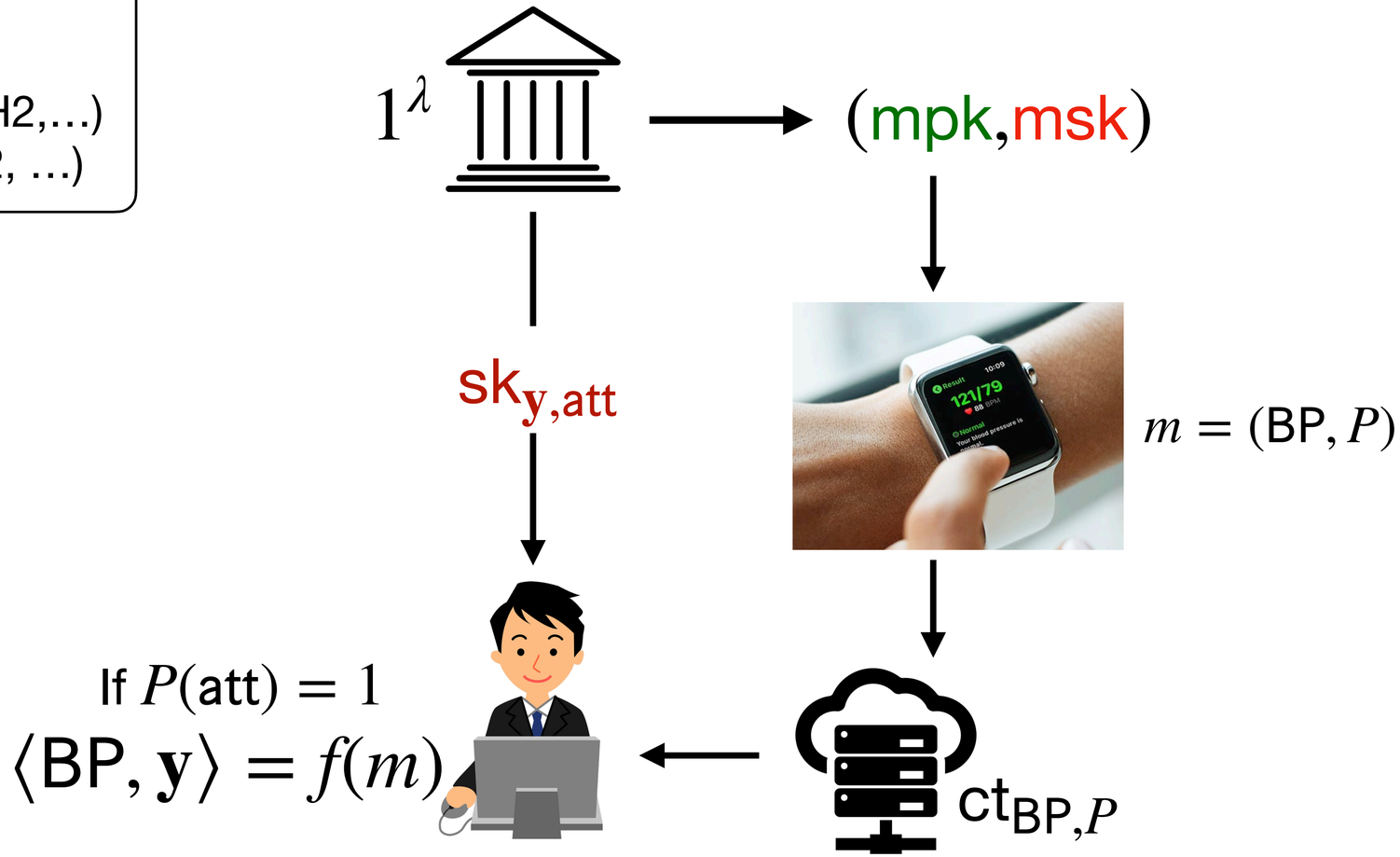
Data owner: IoMT device users

Data users:

- doctors of hospitals (H1, H2,…)
- researchers of labs (L1, L2, …)

att = {dept_H1/H2, section_L1/L2, …}

$f(\cdot, \star) = \langle \cdot, \mathbf{y} \rangle$ if $\star(\text{att}) = 1$



P: (doc@cardio_H1) ∧ (rs@drug_L2)

Attribute-Based IPFE (ABIPFE): Application in IoMT

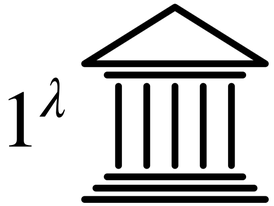
Data owner: IoMT device users

Data users:

- doctors of hospitals (H1, H2,…)
- researchers of labs (L1, L2, …)

att = {dept_H1/H2, section_L1/L2, …}

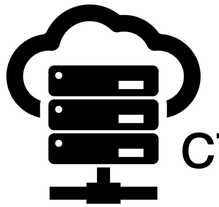
$f(\cdot, \star) = \langle \cdot, \mathbf{y} \rangle$ if $\star(\text{att}) = 1$



1^λ → (mpk,msk)

$\text{sk}_{\mathbf{y},\text{att}}$

$m = (\text{BP}, P)$



$\text{ct}_{\text{BP},P}$

If $P(\text{att}) = 1$

$\langle \text{BP}, \mathbf{y} \rangle = f(m)$

- all attributes are controlled by a *single* authority
- the security of the system depends on the *single* authority

P: (doc@cardio_H1) ∧ (rs@drug_L2)

Multi-Authority ABIPFE (MA-ABIPFE) [AGT21]

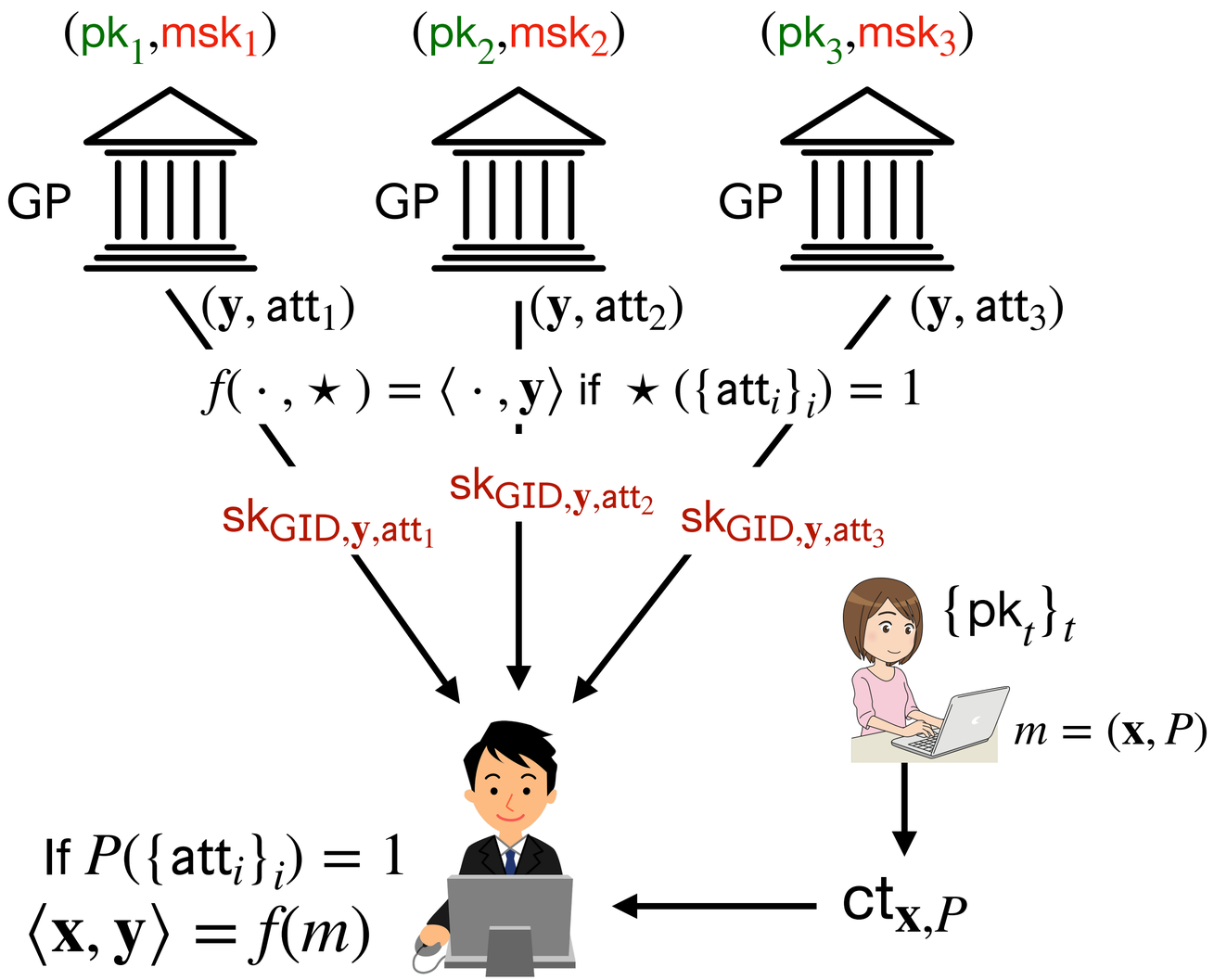
$\mathsf{GSetup}(1^\lambda) \to \mathsf{GP}$

$\mathsf{LSetup}(\mathsf{GP}, 1^n, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$

$\mathsf{KeyGen}(\mathsf{msk}_t, \mathsf{GID}, \mathbf{y}, \mathsf{att}) \to \mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}}$

$\mathsf{Enc}(\mathsf{GP}, \{\mathsf{pk}_t\}_t, \mathbf{x}, P) \to \mathsf{ct}_{\mathbf{x},P}$

$\mathsf{Dec}(\mathsf{GP}, \mathsf{GID}, \{\mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}_i}\}_i, \mathsf{ct}_{\mathbf{x},P}) \to \langle \mathbf{x}, \mathbf{y} \rangle$
if $P(\{\mathsf{att}_i\}_i) = 1$



Multi-Authority ABIPFE (MA-ABIPFE) [AGT21]

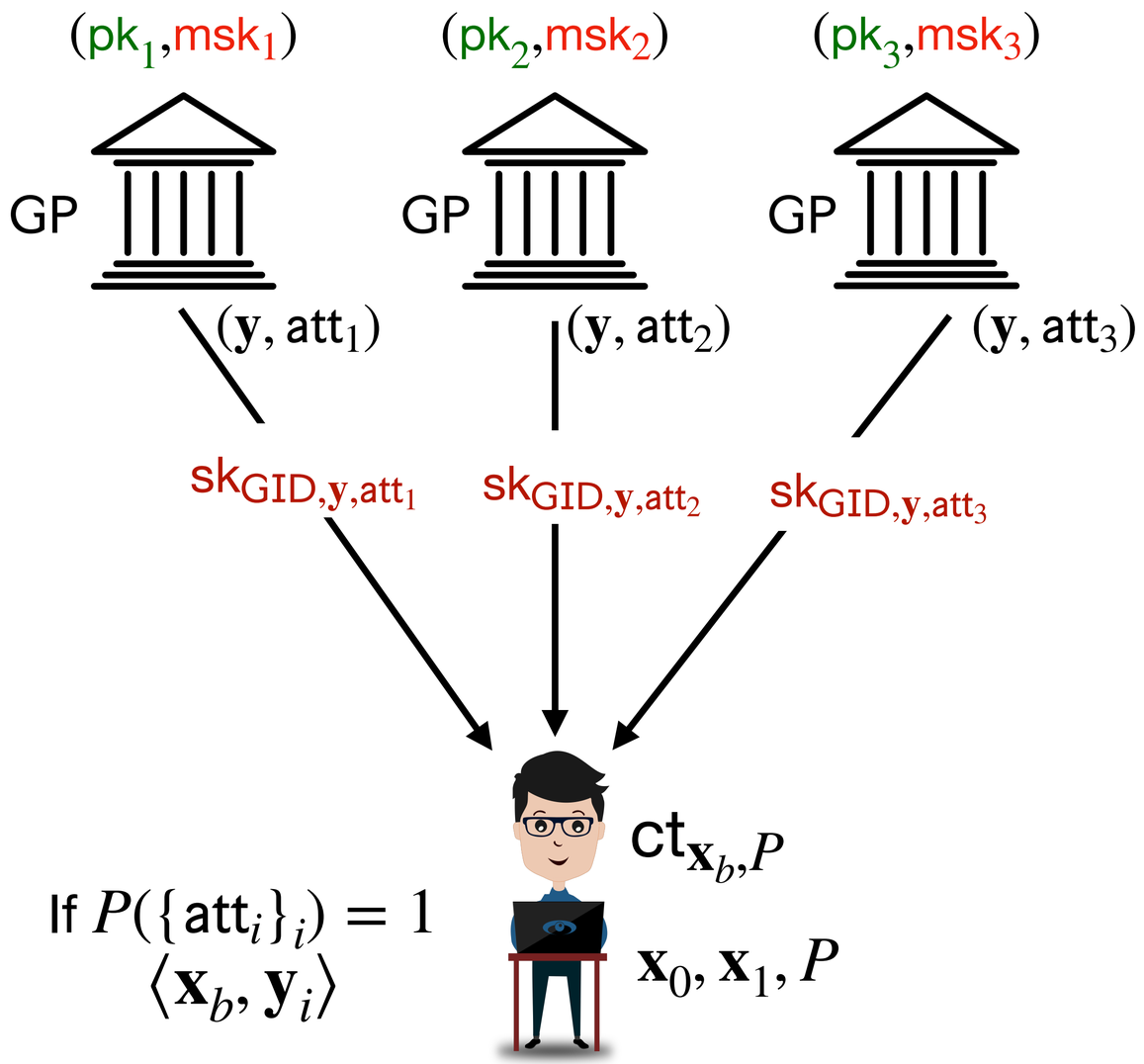
$\mathsf{GSetup}(1^\lambda) \to \mathsf{GP}$

$\mathsf{LSetup}(\mathsf{GP}, 1^n, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$

$\mathsf{KeyGen}(\mathsf{msk}_t, \mathsf{GID}, \mathbf{y}, \mathsf{att}) \to \mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}}$

$\mathsf{Enc}(\mathsf{GP}, \{\mathsf{pk}_t\}_t, \mathbf{x}, P) \to \mathsf{ct}_{\mathbf{x},P}$

$\mathsf{Dec}(\mathsf{GP}, \mathsf{GID}, \{\mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}_i}\}_i, \mathsf{ct}_{\mathbf{x},P}) \to \langle \mathbf{x}, \mathbf{y} \rangle$
if $P(\{\mathsf{att}_i\}_i) = 1$



Security: cannot guess b, given $\langle \mathbf{x}_0, \mathbf{y}_i \rangle = \langle \mathbf{x}_1, \mathbf{y}_i \rangle \ \forall i$ s.t. $P(\{\mathsf{att}_i\}_i) = 1$

Multi-Authority ABIPFE (MA-ABIPFE) [AGT21]

$\mathsf{GSetup}(1^\lambda) \to \mathsf{GP}$

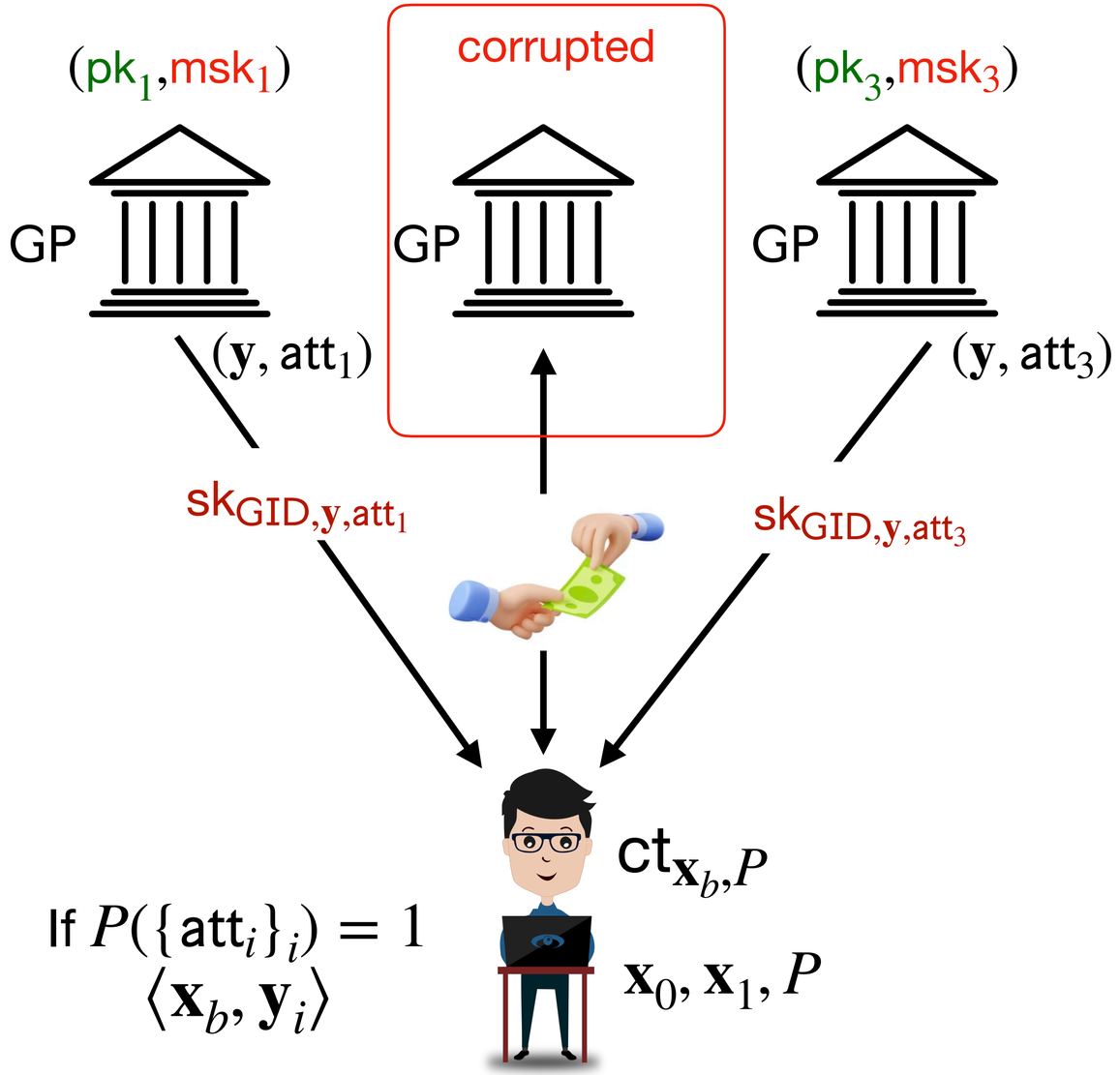
$\mathsf{LSetup}(\mathsf{GP}, 1^n, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$

$\mathsf{KeyGen}(\mathsf{msk}_t, \mathsf{GID}, \mathbf{y}, \mathsf{att}) \to \mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}}$

$\mathsf{Enc}(\mathsf{GP}, \{\mathsf{pk}_t\}_t, \mathbf{x}, P) \to \mathsf{ct}_{\mathbf{x},P}$

$\mathsf{Dec}(\mathsf{GP}, \mathsf{GID}, \{\mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}_i}\}_i, \mathsf{ct}_{\mathbf{x},P}) \to \langle \mathbf{x}, \mathbf{y} \rangle$
if $P(\{\mathsf{att}_i\}_i) = 1$

- authorities can be corrupted



Security: cannot guess b, given $\langle \mathbf{x}_0, \mathbf{y}_i \rangle = \langle \mathbf{x}_1, \mathbf{y}_i \rangle \ \forall i$ s.t. $P(\{\mathsf{att}_i\}_i) = 1$

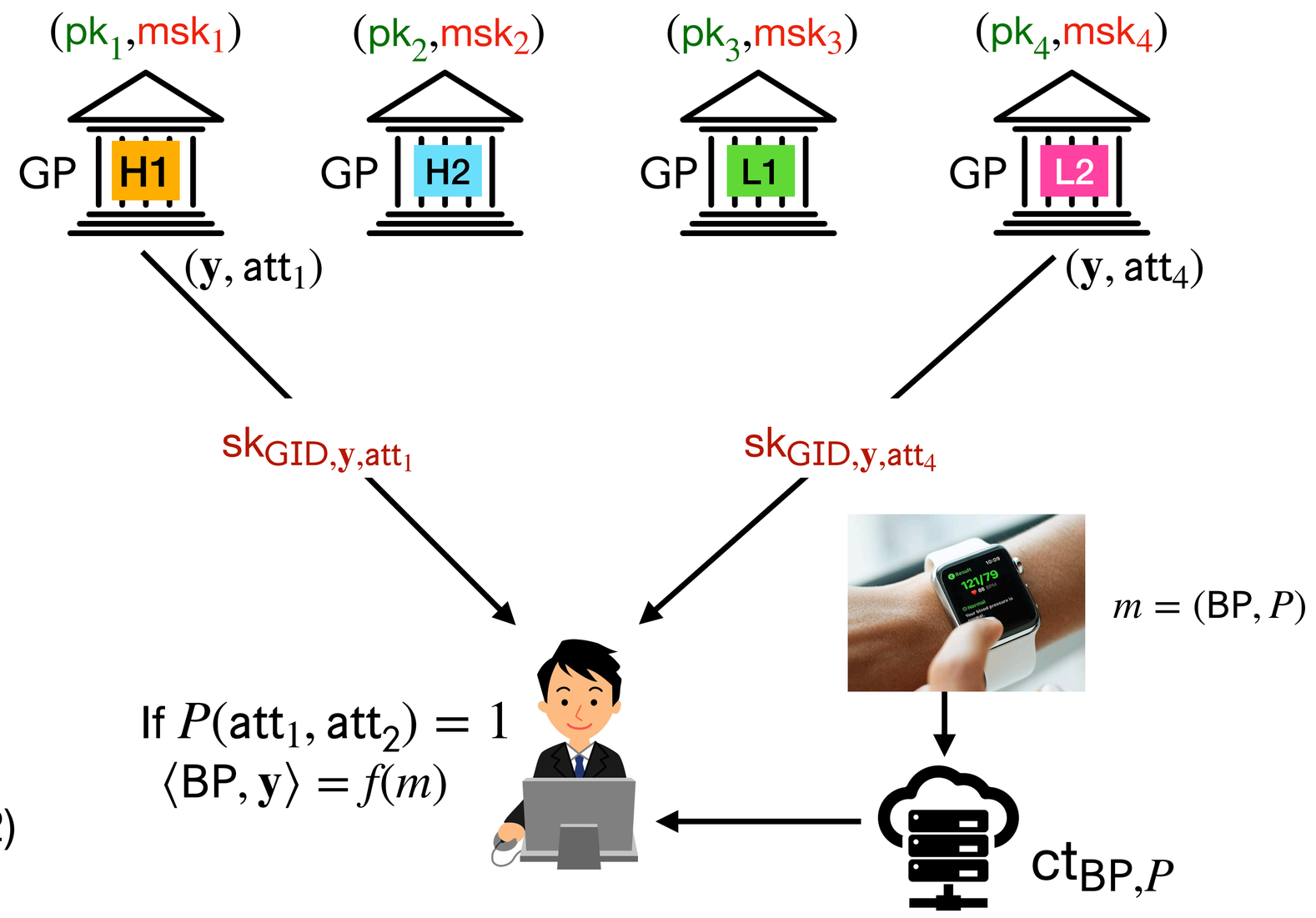
MA-ABIPFE: Application in IoMT

Data owner: IoMT device users

Data users:

- doctors of hospitals (H1, H2,…)
- researchers of labs (L1, L2, …)

att = {dept_H1/H2, section_L1/L2, …}



P: (doc@cardio_H1) ∧ (rs@drug_L2)

att_1 att_2

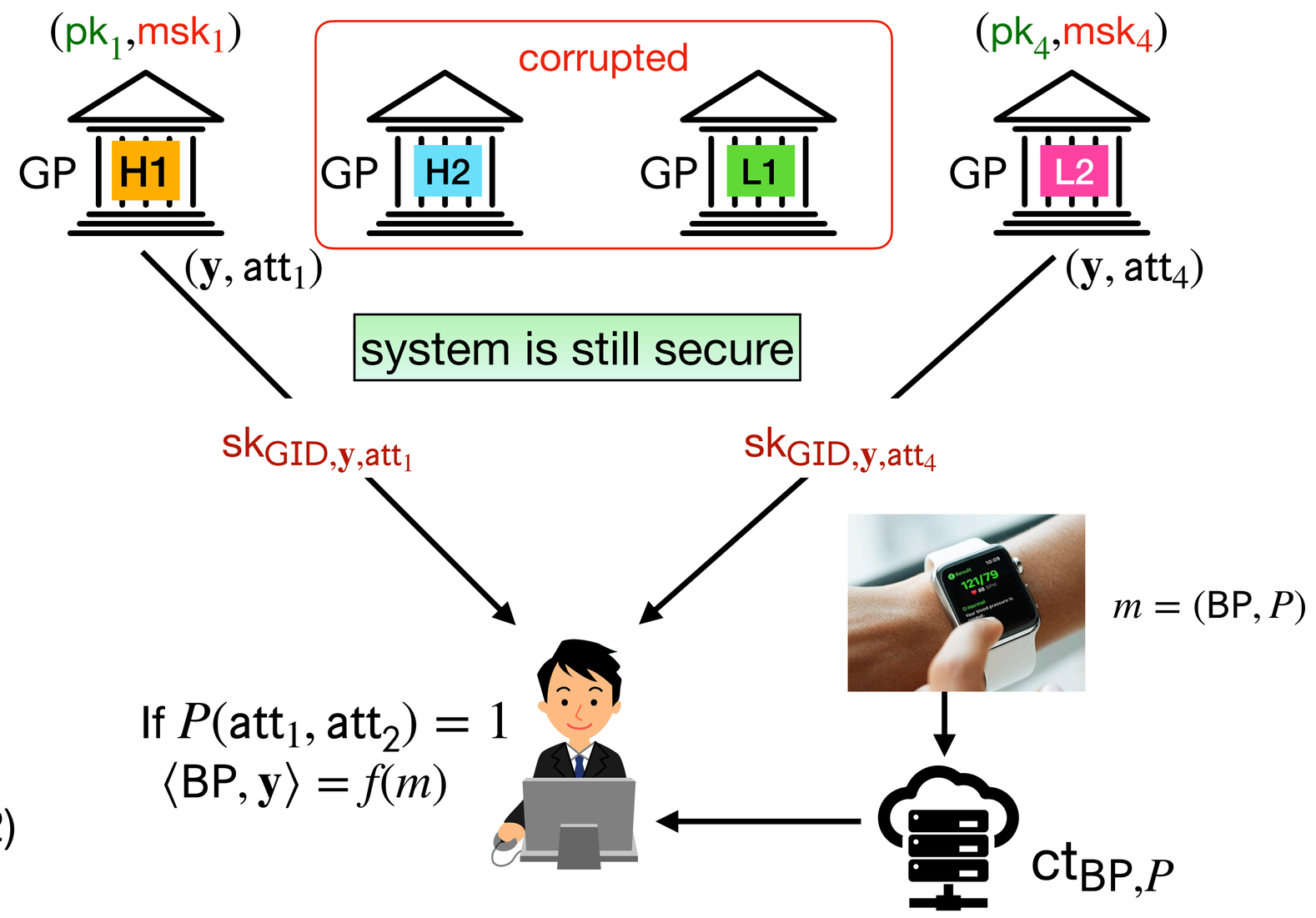
MA-ABIPFE: Application in IoMT

Data owner: IoMT device users

Data users:

- doctors of hospitals (H1, H2,…)
- researchers of labs (L1, L2, …)

att = {dept_H1/H2, section_L1/L2, …}



P: (doc@cardio_H1) ∧ (rs@drug_L2)

att_1 att_2

Limitations of MA-ABIPFE of AGT21: bounded vectors

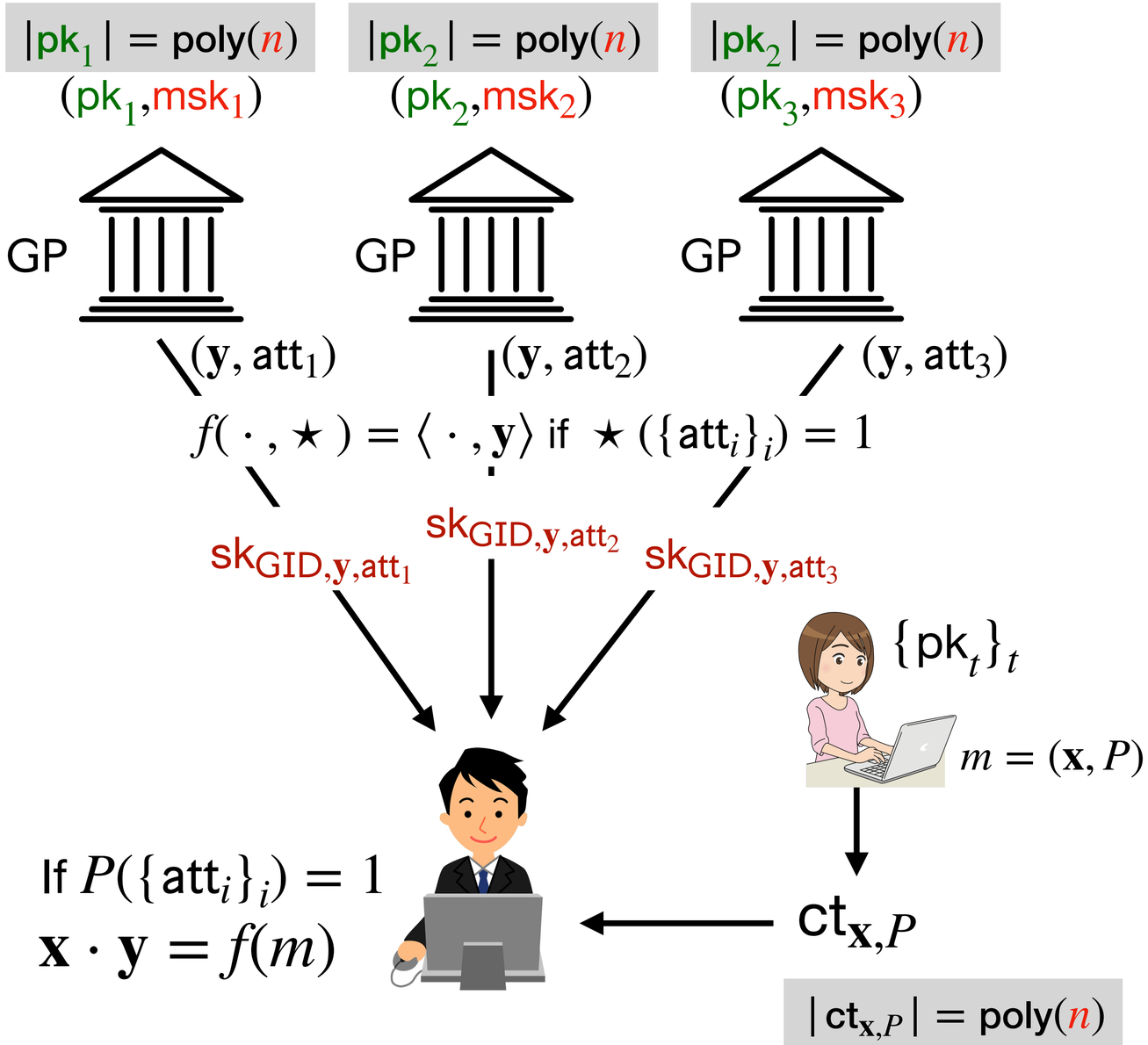
$\mathsf{GSetup}(1^\lambda) \to \mathsf{GP}$

$\mathsf{LSetup}(\mathsf{GP}, 1^n, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$

$\mathsf{KeyGen}(\mathsf{msk}_t, \mathsf{GID}, \mathbf{y}, \mathsf{att}) \to \mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}}$

$\mathsf{Enc}(\mathsf{GP}, \{\mathsf{pk}_t\}_t, \mathbf{x}, P) \to \mathsf{ct}_{\mathbf{x},P}$

- n is fixed for all authorities
- $|\mathsf{pk}_t| = \mathsf{poly}(n)$
- $|\mathsf{ct}_{\mathbf{x},P}| = \mathsf{poly}(n)$ even if $|\mathbf{x}| << n$



Limitations of MA-ABIPFE of AGT21: bounded attributes

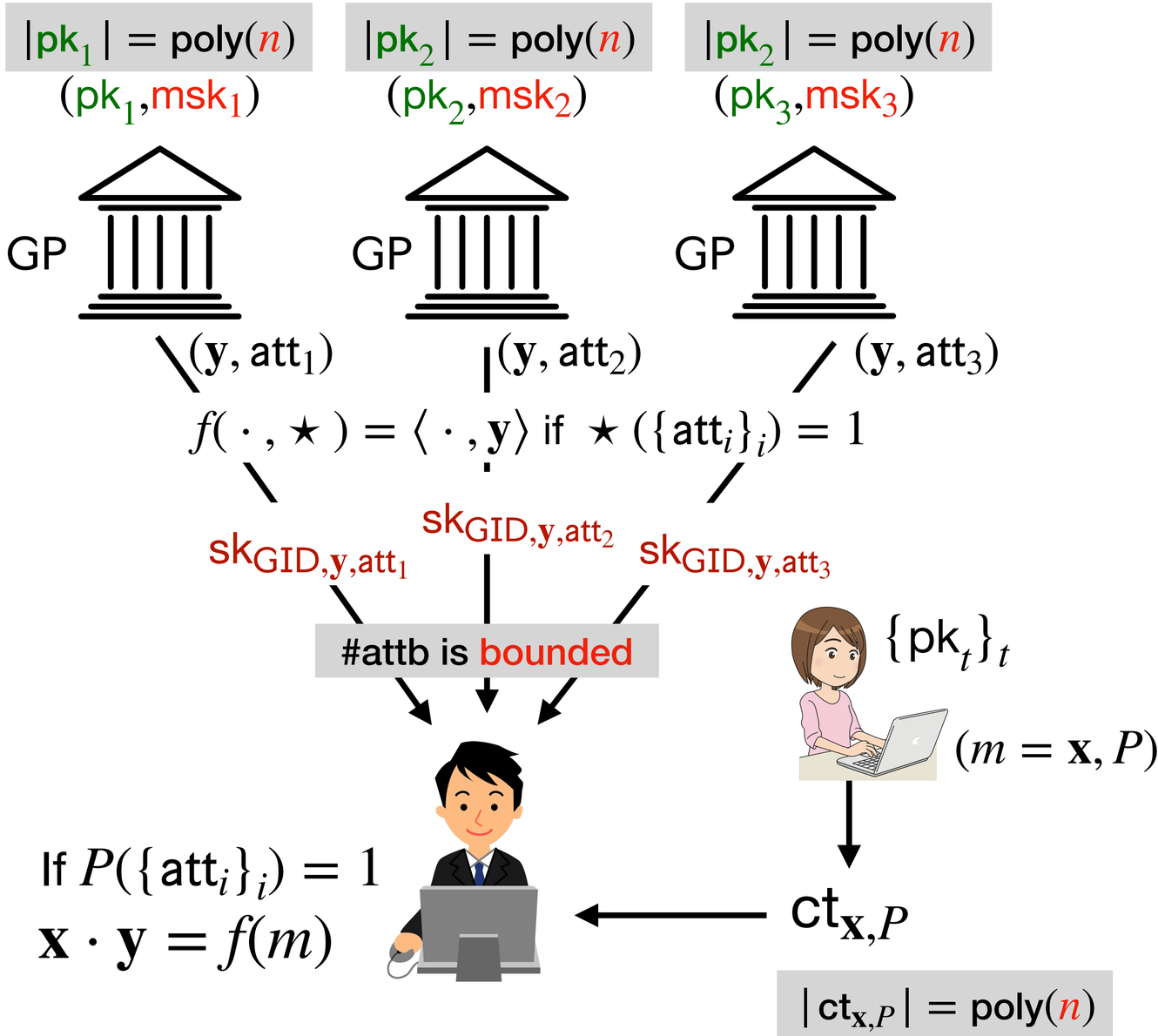
$\mathsf{GSetup}(1^\lambda) \to \mathsf{GP}$

$\mathsf{LSetup}(\mathsf{GP}, 1^n, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$

$\mathsf{KeyGen}(\mathsf{msk}_t, \mathsf{GID}, \mathbf{y}, \mathsf{att}) \to \mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}}$

$\mathsf{Enc}(\mathsf{GP}, \{\mathsf{pk}_t\}_t, \mathbf{x}, P) \to \mathsf{ct}_{\mathbf{x},P}$

- each auth controls a bounded #attb
- small universe



Limitations of MA-ABIPFE of AGT21: strong assumption/weak performance

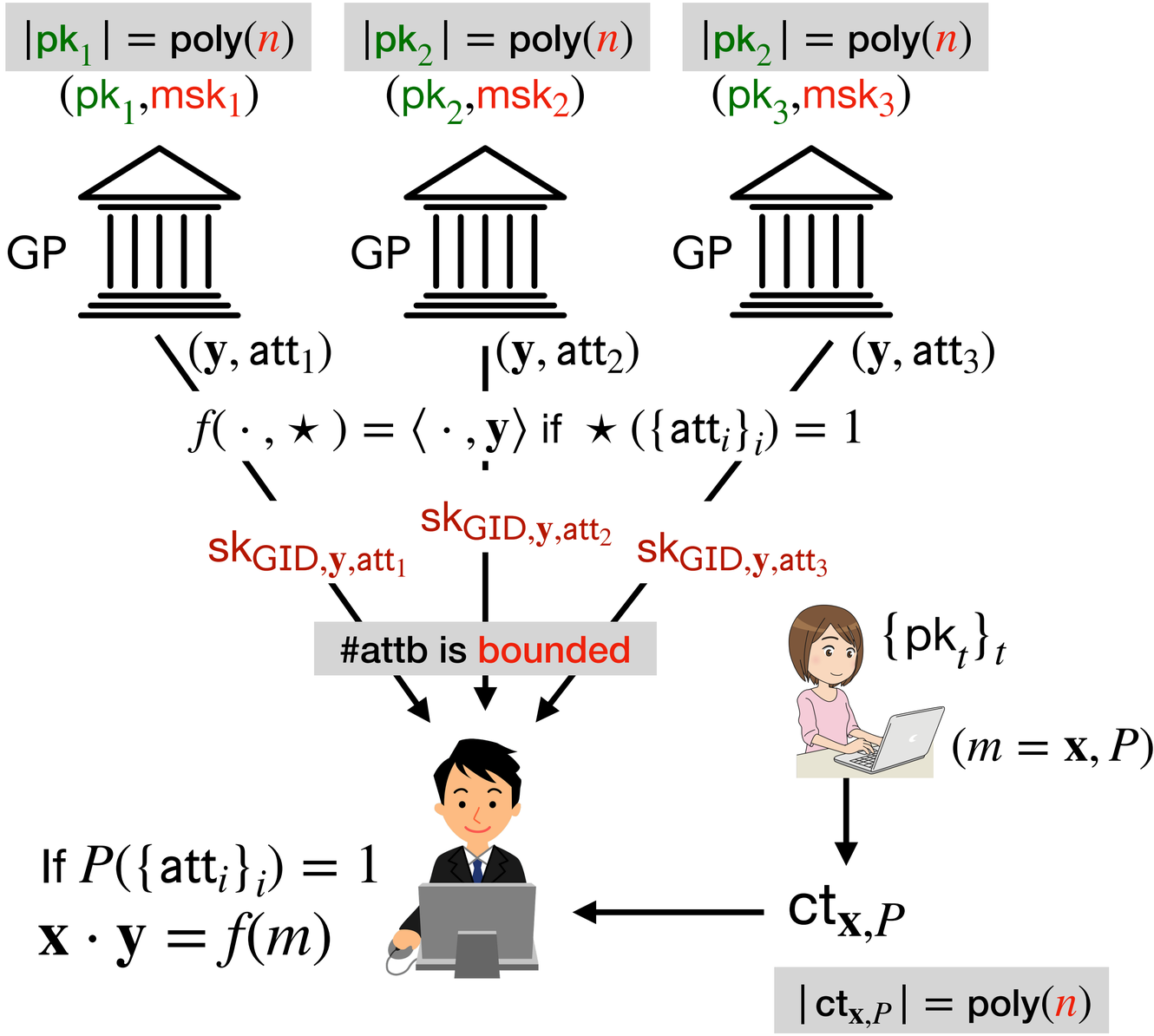
$\mathsf{GSetup}(1^\lambda) \to \mathsf{GP}$

$\mathsf{LSetup}(\mathsf{GP}, 1^n, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$

$\mathsf{KeyGen}(\mathsf{msk}_t, \mathsf{GID}, \mathbf{y}, \mathsf{att}) \to \mathsf{sk}_{\mathsf{GID},\mathbf{y},\mathsf{att}}$

$\mathsf{Enc}(\mathsf{GP}, \{\mathsf{pk}_t\}_t, \mathbf{x}, P) \to \mathsf{ct}_{\mathbf{x},P}$

- Built in composite order groups
- More than 2 hours for encryption
- About 5 days for decryption



Our results

We construct MA-ABIPFE where…

- unbounded length message/key vectors can be processed,

  $\mathsf{LSetup}(\mathsf{GP}, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$ $|\mathsf{pk}_t| = \mathsf{poly}(\lambda)$ $|\mathsf{ct}_{\mathbf{x},P}| = \mathsf{poly}(|\mathbf{x}|)$

- authorities are allowed to control arbitrary number of attributes
- attributes need not be enumerated at setup, i.e., large universe
- constructed in a prime-order pairing groups
- proven secure under target-group-based assumptions

Our results

We construct MA-ABIPFE where…

- unbounded length message/key vectors can be processed,

  $\mathsf{LSetup}(\mathsf{GP}, t) \to (\mathsf{pk}_t, \mathsf{msk}_t)$ $|\mathsf{pk}_t| = \mathsf{poly}(\lambda)$ $|\mathsf{ct}_{\mathbf{x},P}| = \mathsf{poly}(|\mathbf{x}|)$

- authorities are allowed to control arbitrary number of attributes
- attributes need not be enumerated at setup, i.e., large universe
- constructed in a prime-order pairing groups
- proven secure under target-group-based assumptions
- static security under DBDH-type assumption

Roadmap

[AGT21]	Our SMA-ABUIPFE	Our LMA-ABUIPFE
small-universe MA-ABIPFE	small-universe MA-ABUIPFE	large-universe MA-ABUIPFE
bounded-length vectors	unbounded-length vectors	unbounded-length vectors
composite-order group-based	prime-order group-based	prime-order group-based
source-group-based assump. e.g., subgroup decision assump.	target-group-based assump. e.g., DBDH	target-group-based assump. e.g., L-DBDH
selective security	static security	static security

Constructing SMA-ABUIPFE

An initial attempt combining techniques of [DKW21] and [DP19]

GP $= (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $s =$ max #AND gates in $P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

Constructing SMA-ABUIPFE

An initial attempt combining techniques of [DKW21] and [DP19]

GP $= (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s =$ max #AND gates in $P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

Constructing SMA-ABUIPFE

An initial attempt combining techniques of [DKW21] and [DP19]

GP $= (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s =$ max #AND gates in $P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k)^{u_{t,j} \cdot y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

vectorise using hash-and-exponentiation

Constructing SMA-ABUIPFE

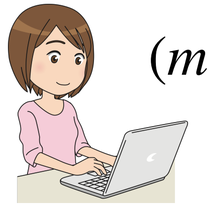
An initial attempt combining techniques of [DKW21] and [DP19]

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k)^{u_{t,j} \cdot y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

Constructing SMA-ABUIPFE

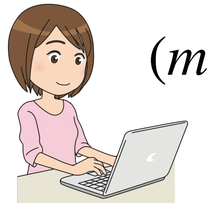
An initial attempt combining techniques of [DKW21] and [DP19]

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k)^{u_{t,j} \cdot y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$,
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{d}_{i,j}]_T$

$\mathsf{ct}_{\mathbf{x},P}$

vectorise using hash-and-pairing

$$[b_{i,k}]_T = e(r_i[a_{\rho(i)}]_1, \mathsf{H}_1(t \,\|\, k))$$

$$[d_{i,j,k}]_T = e(r_i[u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))$$

Constructing SMA-ABUIPFE

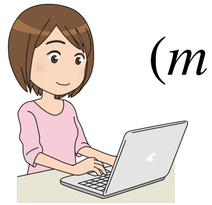
An initial attempt combining techniques of [DKW21] and [DP19]

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k)^{u_{t,j} \cdot y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$$\{w_i\}_{i \in I} \text{ s.t. } \sum_{i \in I} w_i \mathbf{M}_i = (1,0,\ldots,0)$$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$,
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{d}_{i,j}]_T$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \; \prod_{j=2}^{s} \prod_k e(C_{3,i,j,k} \cdot y_k, \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))}{e(C_{2,i}, \mathsf{sk}_{\mathsf{GID},\mathbf{y},t})} \right]^{w_i}$$

$$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \,\|\, k))$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))$$

Constructing SMA-ABUIPFE

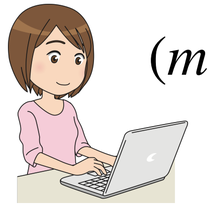
An initial attempt combining techniques of [DKW21] and [DP19]

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} \cdot y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1,0,\ldots,0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$,
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{d}_{i,j}]_T$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \quad \prod^{s} \quad \prod \quad e(C \quad \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))}{} \right]^{w_i}$$

not known to the encrypter

$[b_{i,k}]_T = e(r_i[a_{\rho(i)}]_1, \mathsf{H}_1(t \parallel k))$

$[d_{i,j,k}]_T = e(r_i[u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$

Constructing SMA-ABUIPFE

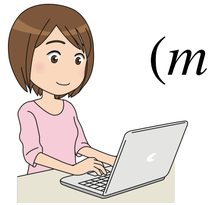
An initial attempt combining techniques of [DKW21] and [DP19]

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

not known to the encrypter

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \quad \prod_{j=2}^{s} \prod_k e(C_{3,i,j}, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))}{\quad} \right]^{w_i}$$

Constructing SMA-ABUIPFE

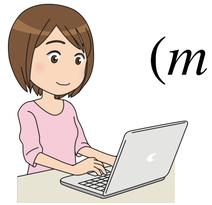
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

not known to the encrypter

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \prod_{j=2}^{s} \prod e(C_{3,i,j}, \mathbf{y}_j \cdot \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))}{\ldots} \right]^{w_i}$$

Constructing SMA-ABUIPFE

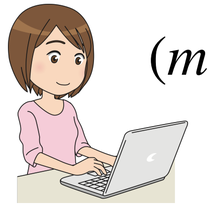
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)$$
$$= \mathsf{H}_2(j \parallel k) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)$$

Constructing SMA-ABUIPFE

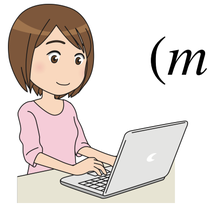
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)$$
$$= \mathsf{H}_2(j \parallel k) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)$$
$$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$$

Constructing SMA-ABUIPFE

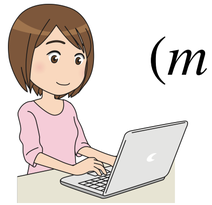
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)$$
$$= \mathsf{H}_2(j \parallel k) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)$$

$$[u_{t,j}]_1 \longrightarrow [u^{(3)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_3(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

Constructing SMA-ABUIPFE

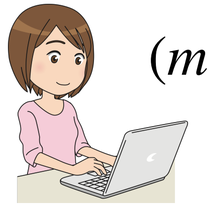
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k)^{u_{t,j} y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

$\mathsf{ct}_{\mathbf{x},P}$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$$

$$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$$

$$[u_{t,j}]_1 \longrightarrow [u^{(3)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_3(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

Constructing SMA-ABUIPFE

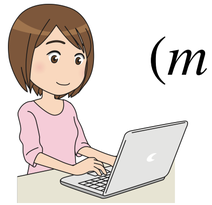
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j)^{\mathbf{u}_{t,j} \cdot \mathbf{y}} \in \mathbb{G}_2$$

$$= \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k}$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

$\mathsf{ct}_{\mathbf{x},P}$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$$

$$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$$

$$[u_{t,j}]_1 \longrightarrow [u^{(3)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_3(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

Constructing SMA-ABUIPFE

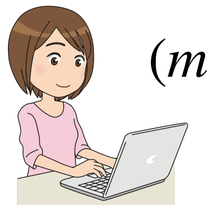
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1,0,\ldots,0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$

$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$

cannot simply replace H by H_2

$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$

$[u_{t,j}]_1 \longrightarrow [u^{(3)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_3(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$

Constructing SMA-ABUIPFE

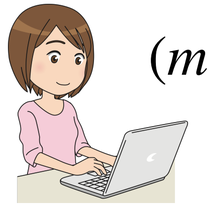
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1,0,\ldots,0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \ \prod_{j=2}^{s} \prod_k \boxed{e(C_{3,i,j,k} \cdot y_k, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))}}{e(C_{2,i}, \mathsf{sk}_{\mathsf{GID},\mathbf{y},t})} \right]^{w_i}$$

$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$

$[d_{i,j,k}]_T = e(r_i [u_{\rho(i),j}]_1, \mathsf{H}(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$

cannot simply replace H by H_2

Constructing SMA-ABUIPFE

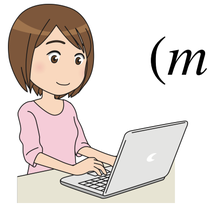
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1,0,\ldots,0)$

- $C_0 = [\mathbf{x}+\mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i[u_{\rho(i),j}]_1, \mathsf{H}(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$$

cannot simply replace H by H_2

$$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$$

$$e(C_{3,i,j} \cdot \mathbf{y}, \mathsf{H}_2(j \parallel k))$$

$$= e([M_{i,j}\mathbf{x}_j + r_i\mathbf{u}_{\rho(i),j}]_1 \cdot \mathbf{y}, \mathsf{H}_2(j \parallel k))$$

Constructing SMA-ABUIPFE

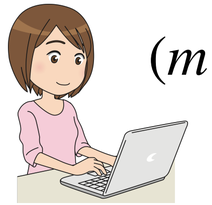
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1,0,\ldots,0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j} = [M_{i,j}\mathbf{x}_j + r_i\, \mathbf{u}_{\rho(i),j}]_T$

$$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$$

$$C_{3,i,j,k} = e([M_{i,j}x_{j,k}]_1, \mathsf{H}_2(j \parallel k)) \cdot [r_i\, u^{(2)}_{\rho(i),j,k}]_T$$

$$= [M_{i,j} \cdot \mathbf{x}_j + \mathbf{d}_{i,j}]_T$$

$$[d_{i,j,k}]_T = e(r_i[u_{\rho(i),j}]_1, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))$$

cannot simply replace H by H_2

Constructing SMA-ABUIPFE

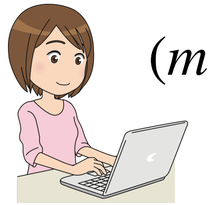
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1,0,\ldots,0)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \parallel k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$

$\mathsf{ct}_{\mathbf{x},P}$

$\mathsf{ct}_{\mathbf{x},P}$

$$[u_{t,j}]_1 \longrightarrow [u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \parallel k))$$

$$C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \parallel k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$$

$$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \parallel k))$$

Constructing SMA-ABUIPFE

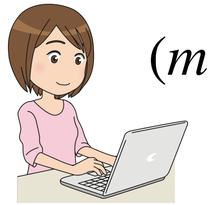
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

- $C_0 = [\mathbf{x}+\mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \parallel k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1,0,\ldots,0)$

$\mathsf{ct}_{\mathbf{x},P}$

w_i

$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \parallel k))$

$$[u_{t,j}]_1 \longrightarrow [u^{(3)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_3(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$$

How to handle $[u^{(3)}_{\rho(i),j,k}]_T$?

Constructing SMA-ABUIPFE

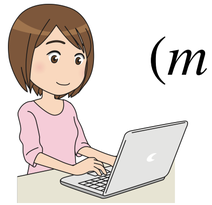
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_\mathbf{x}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_\mathbf{y}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_\mathbf{x}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_\mathbf{x}|}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \parallel k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\{w_i\}_{i \in I}$ s.t. $\sum w_i \mathbf{M}_i = (1, 0, \ldots, 0)$

$\mathsf{ct}_{\mathbf{x},P}$

$\mathsf{ct}_{\mathbf{x},P}$

$$[u_{t,j}]_1 \longrightarrow [u^{(3)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_3(\boxed{\mathsf{GID} \parallel \mathbf{y}} \parallel j \parallel k))$$

- $\mathbf{f} = (f_2, \ldots, f_s) \leftarrow \mathbb{Z}_p^{s-1}$
- $C_{4,i,j} = [M_{i,j} f_j \; + \; r_i u_{\rho(i),j}]_1$

$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \parallel k))$

Constructing SMA-ABUIPFE

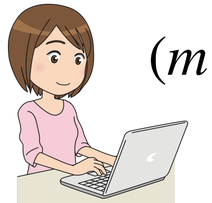
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$
- $\mathbf{f} = (f_2, \ldots, f_s) \leftarrow \mathbb{Z}_p^{s-1}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \parallel k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1,0,\ldots,0)$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \prod_{j=2}^{s} \prod_k e(C_{3,i,j,k} \cdot y_k, \mathsf{H}(\mathsf{GID} \parallel \mathbf{y} \parallel j \parallel k))}{e(C_{2,i}, \mathsf{sk}_{\mathsf{GID},\mathbf{y},t})} \right]^{w_i}$$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \parallel k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$
- $C_{4,i,j} = [M_{i,j} f_j + r_i u_{\rho(i),j}]_1$

$\mathsf{ct}_{\mathbf{x},P}$

$$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \parallel k))$$

Constructing SMA-ABUIPFE

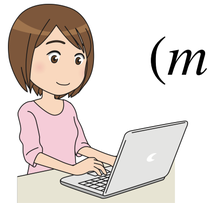
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$
- $\mathbf{f} = (f_2, \ldots, f_s) \leftarrow \mathbb{Z}_p^{s-1}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$\mathsf{ct}_{\mathbf{x},P}$

$$C_{3,i,j,k} \cdot y_k \cdot e(C_{4,i,j} \cdot y_k, \mathsf{H}_3(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))$$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \,\|\, k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$
- $C_{4,i,j} = [M_{i,j} f_j + r_i u_{\rho(i),j}]_1$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \prod_{j=2}^{s} \prod_k e(C_{3,i,j,k} \cdot y_k, \mathsf{H}(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))}{e(C_{2,i}, \mathsf{sk}_{\mathsf{GID},\mathbf{y},t})} \right]^{w_i}$$

$$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \,\|\, k))$$

Constructing SMA-ABUIPFE

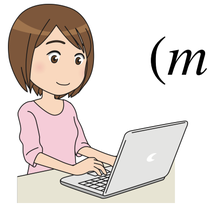
Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$
- $\mathbf{f} = (f_2, \ldots, f_s) \leftarrow \mathbb{Z}_p^{s-1}$

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$[u^{(3)}_{t,j,k}]_2 = \mathsf{H}_3(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k)^{u_{t,j}}$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \,\|\, k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$
- $C_{4,i,j} = [M_{i,j} f_j \; + \; r_i u_{\rho(i),j}]_1$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1,0,\ldots,0)$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \; \prod_{j=2}^{s} \prod_k C_{3,i,j,k} \cdot y_k \cdot e(C_{4,i,j} \cdot y_k, \mathsf{H}_3(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))}{e(C_{2,i}, \mathsf{sk}_{\mathsf{GID},\mathbf{y},t})} \right]^{w_i}$$

$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \,\|\, k))$

$[u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \,\|\, k))$

Constructing SMA-ABUIPFE

Our idea: SMA-ABUIPFE using "*hash-decomposition*" mechanism

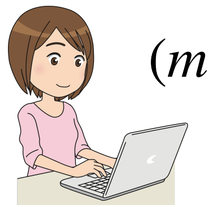
$\mathsf{GP} = (e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2)$ $\quad s = \text{max \#AND gates in } P = (\mathsf{M} \in \mathbb{Z}^{\ell \times s}, \rho)$ $\quad m = \mathbf{x} \in \mathbb{Z}^{|I_{\mathbf{x}}|}$ $\quad f = \mathbf{y} \in \mathbb{Z}^{|I_{\mathbf{y}}|}$

$|\mathsf{pk}_t| = \mathsf{poly}(\lambda, s)$

$\mathsf{pk}_t = ([a_t]_1, [u_{t,2}]_1, \ldots, [u_{t,s}]_1)$

$\mathsf{msk}_t = (a_t, u_{t,2}, \ldots, u_{t,s})$

$\{\mathsf{pk}_t\}_t$



$(m = \mathbf{x}, P = (\mathsf{M}, \rho))$

- $r_1, \ldots, r_\ell \leftarrow \mathbb{Z}_p$
- $\mathbf{V} = (\mathbf{z}, \mathbf{v}_2, \ldots, \mathbf{v}_s) \leftarrow \mathbb{Z}_p^{s \times |I_{\mathbf{x}}|}$
- $\mathbf{X} = (\mathbf{x}_2, \ldots, \mathbf{x}_s) \leftarrow \mathbb{Z}_p^{(s-1) \times |I_{\mathbf{x}}|}$
- $\mathbf{f} = (f_2, \ldots, f_s) \leftarrow \mathbb{Z}_p^{s-1}$

succinct

$$\mathsf{sk}_{\mathsf{GID},\mathbf{y},t} = \prod_k \mathsf{H}_1(t \,\|\, k)^{a_t y_k} \cdot \prod_{j=2}^{s} \prod_k \left([u^{(2)}_{t,j,k}]_2 \cdot [u^{(3)}_{t,j,k}]_2 \right)^{y_k} \in \mathbb{G}_2$$

$[u^{(3)}_{t,j,k}]_2 = \mathsf{H}_3(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k)^{u_{t,j}}$

$\{\mathsf{sk}_{\mathsf{GID},\mathbf{y},t}\}_t$

$|\mathsf{ct}_{\mathbf{x},P}| = \mathsf{poly}(|\mathbf{x}|, s)$

- $C_0 = [\mathbf{x} + \mathbf{z}]_T$
- $C_{1,i} = [\mathbf{M}_i \cdot \mathbf{V} + \mathbf{b}_i]_T, \quad C_{2,i} = [r_i]$
- $C_{3,i,j,k} = e([M_{i,j} x_{j,k}]_1, \mathsf{H}_2(j \,\|\, k)) \cdot [r_i \, u^{(2)}_{\rho(i),j,k}]_T$
- $C_{4,i,j} = [M_{i,j} f_j + r_i u_{\rho(i),j}]_1$

$\mathsf{ct}_{\mathbf{x},P}$

$\{w_i\}_{i \in I}$ s.t. $\sum_{i \in I} w_i \mathbf{M}_i = (1,0,\ldots,0)$

$\mathsf{ct}_{\mathbf{x},P}$

$$\mathbf{y} \cdot \mathbf{z} = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \mathbf{y} \prod_{j=2}^{s} \prod_k C_{3,i,j,k} \cdot y_k \cdot e(C_{4,i,j} \cdot y_k, \mathsf{H}_3(\mathsf{GID} \,\|\, \mathbf{y} \,\|\, j \,\|\, k))}{e(C_{2,i}, \mathsf{sk}_{\mathsf{GID},\mathbf{y},t})} \right]^{w_i}$$

$[b_{i,k}]_T = e(r_i [a_{\rho(i)}]_1, \mathsf{H}_1(t \,\|\, k))$

$[u^{(2)}_{t,j,k}]_T = e([u_{t,j}]_1, \mathsf{H}_2(j \,\|\, k))$

Conclusion

- Define and Construct **L**arge-universe **M**ulti-**A**uthority **ABUIPFE**
  - ✦ Constant size public-keys for each authority
  - ✦ Succinct secret-keys (only one group element)
  - ✦ Input-specific $|\mathsf{ct}| = \mathsf{poly}(|\mathbf{x}|, s)$
  - ✦ Each authority controls arbitrary number of attributes
  - ✦ Built using a prime-order pairing groups
  - ✦ Static security based on DBDH-type targer-group-based assumption

Conclusion

- Define and Construct **L**arge-universe **M**ulti-**A**uthority **ABUIPFE**
  - ✦ Constant size public-keys for each authority
  - ✦ Succinct secret-keys (only one group element)
  - ✦ Input-specific $|\mathsf{ct}| = \mathsf{poly}(|\mathbf{x}|, s)$
  - ✦ Each authority controls arbitrary number of attributes
  - ✦ Built using a prime-order pairing groups
  - ✦ Static security based on DBDH-type targer-group-based assumption

- Open problems in the area
  - ✦ Selective/adaptive security under target-group-based assumptions
  - ✦ Adaptive corruption from standard assumptions
  - ✦ MA-ABIPFE from PQ-assumptions

Thank you!