Registered Attribute-Based Signature

Yijian Zhang Jun Zhao Ziqi Zhu Junqing Gong Jie Chen

East China Normal University

Shanghai Qi Zhi Institute

Attribute-Based Signature

m: message

x: policy

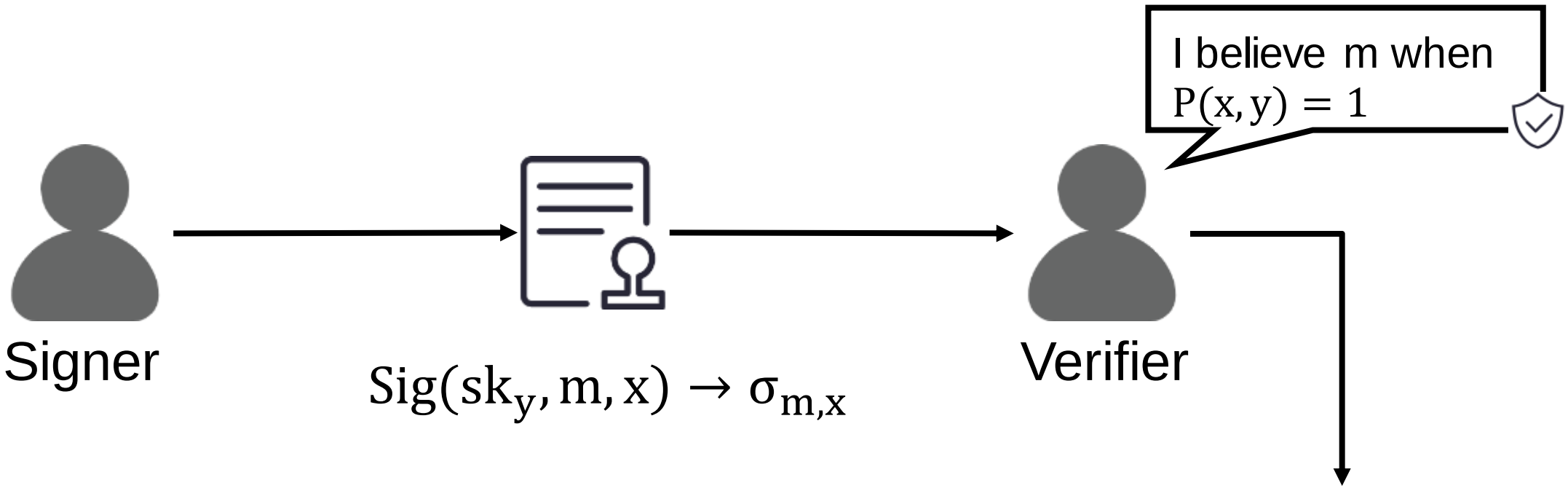
y: attribute

Attribute-Based Signature

m: message

x: policy

y: attribute

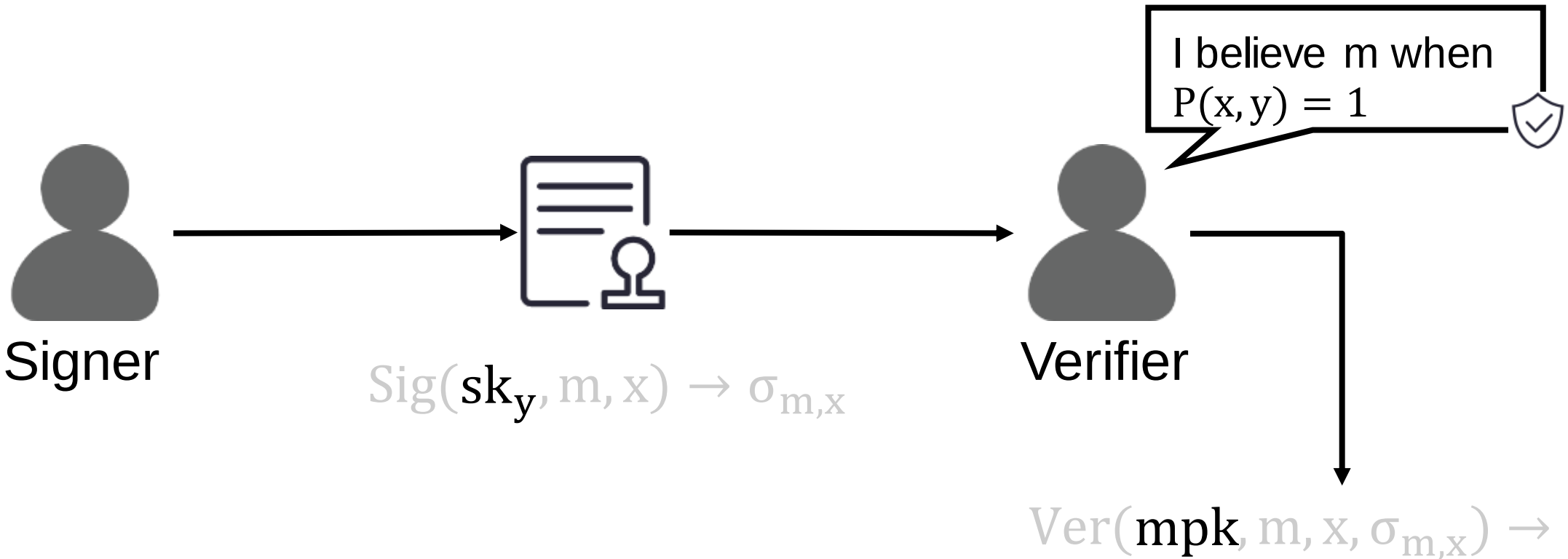


Attribute-Based Signature

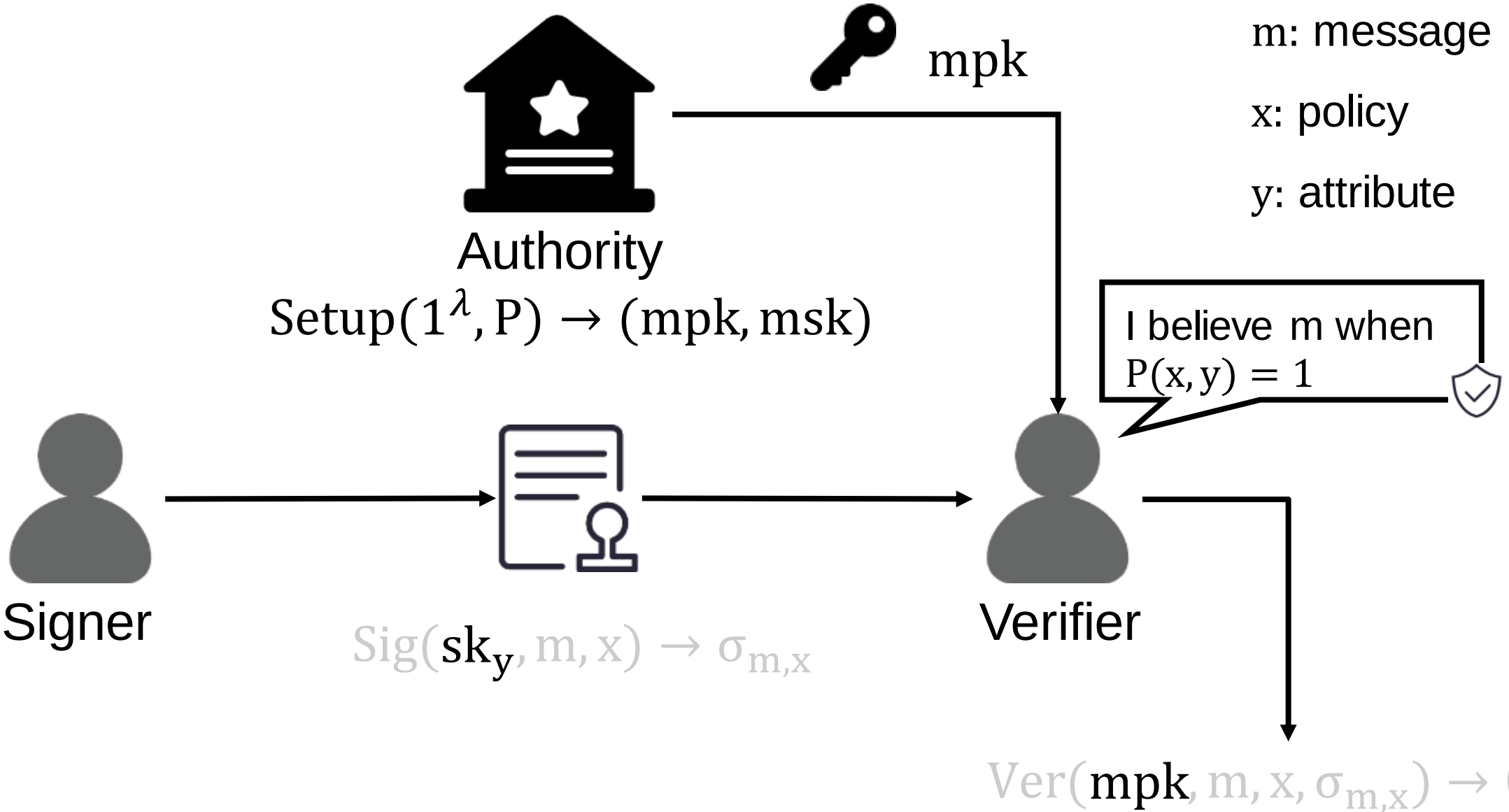
m: message

x: policy

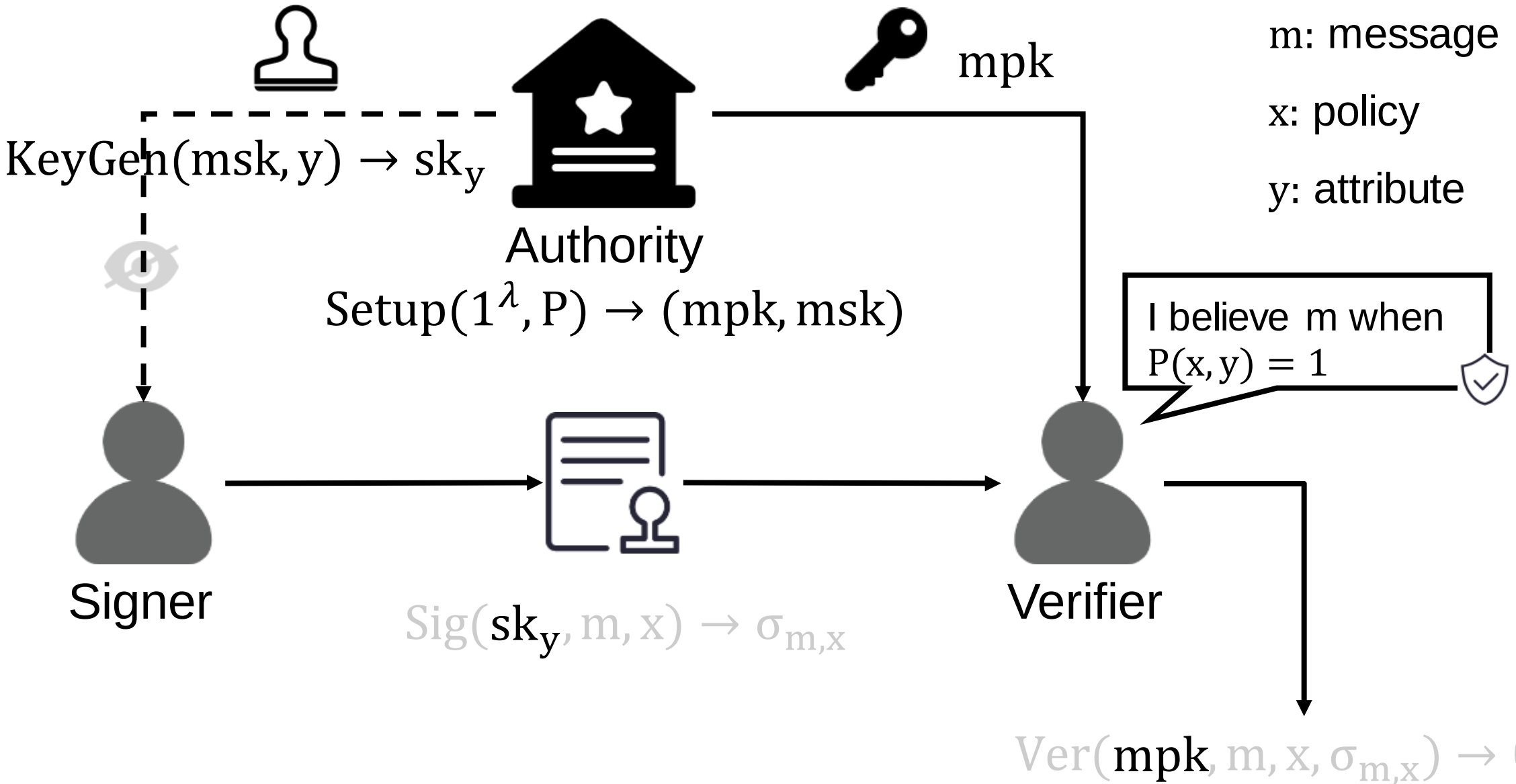
y: attribute



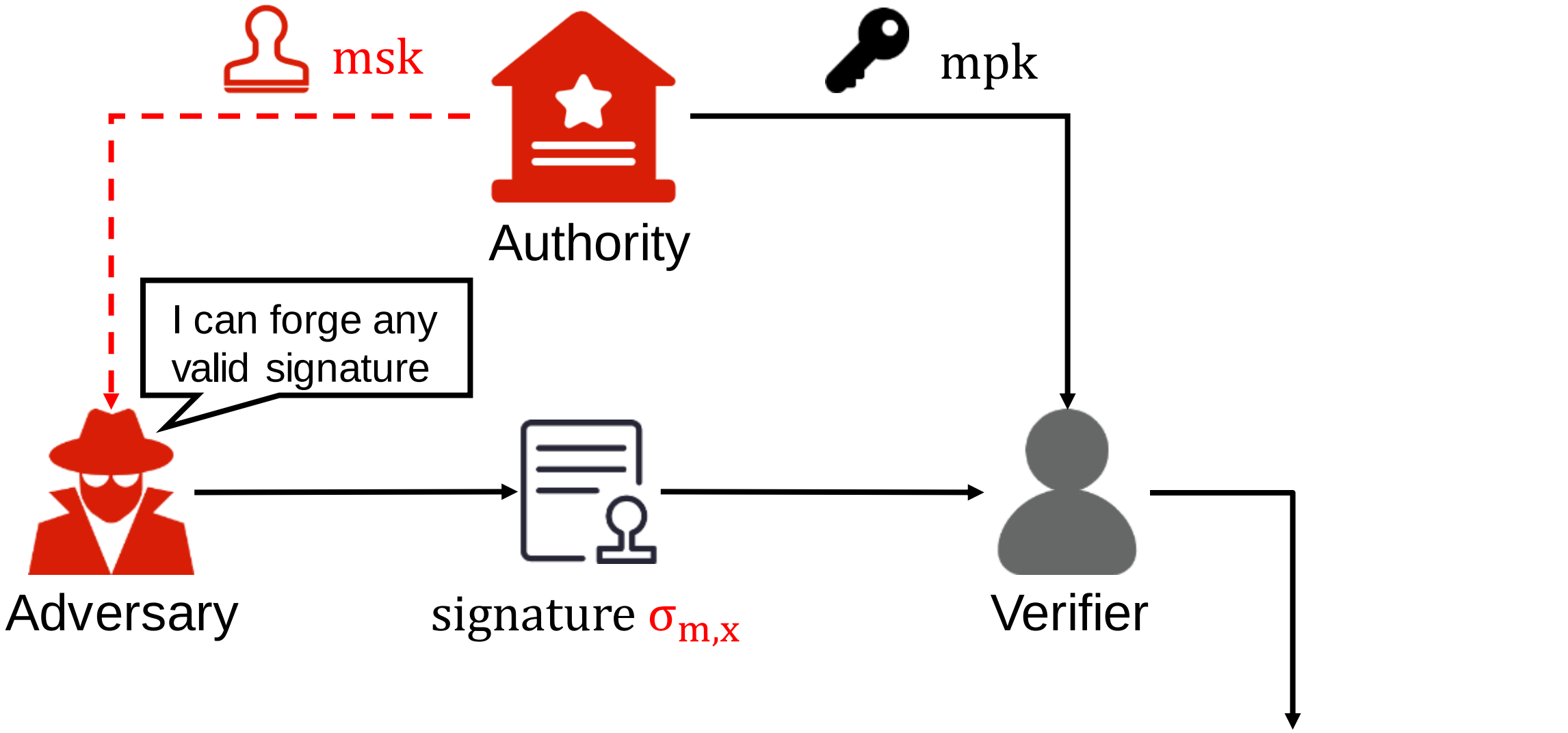
Attribute-Based Signature



Attribute-Based Signature



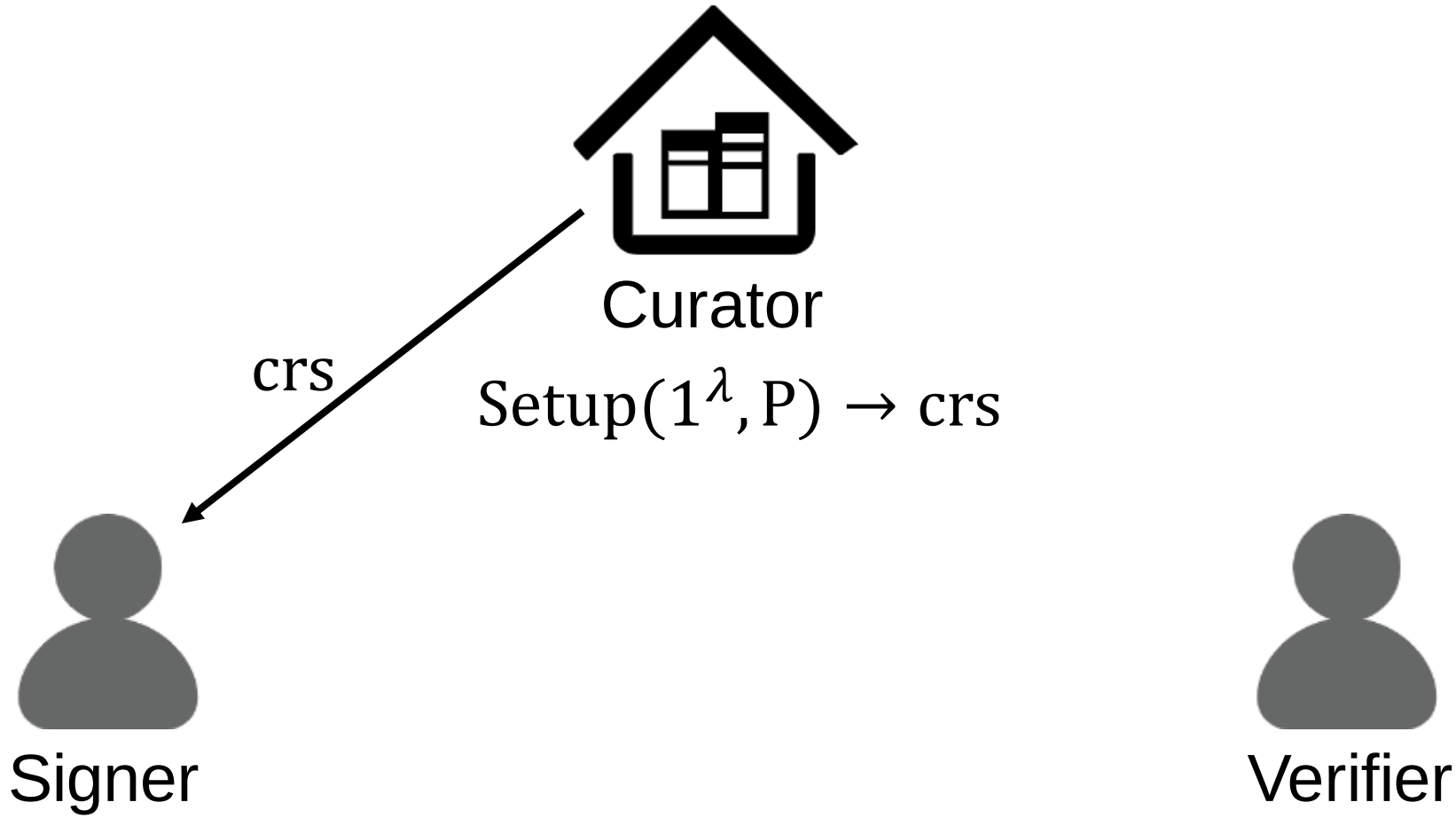
Motivation: Key-Escrow Problem



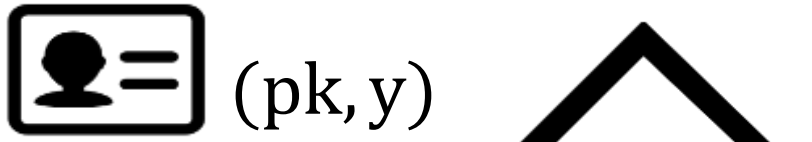
This Work: Registered ABS

	ABS	Decentralized ABS	Registered ABS
Reference	[OT11]	[OT13]	This work
Key-escrow	✗	⊗	✓
Standard model	✓	✗	✓
Assumption	DLIN	DLIN	k-Lin

Registered ABS

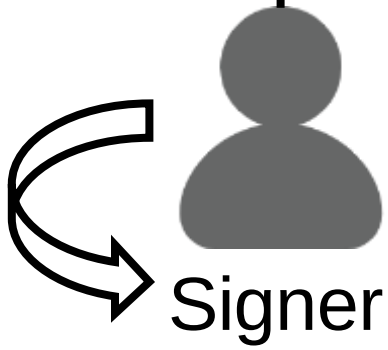


Registered ABS



$(\mathrm{pk}, \mathrm{y})$

Curator

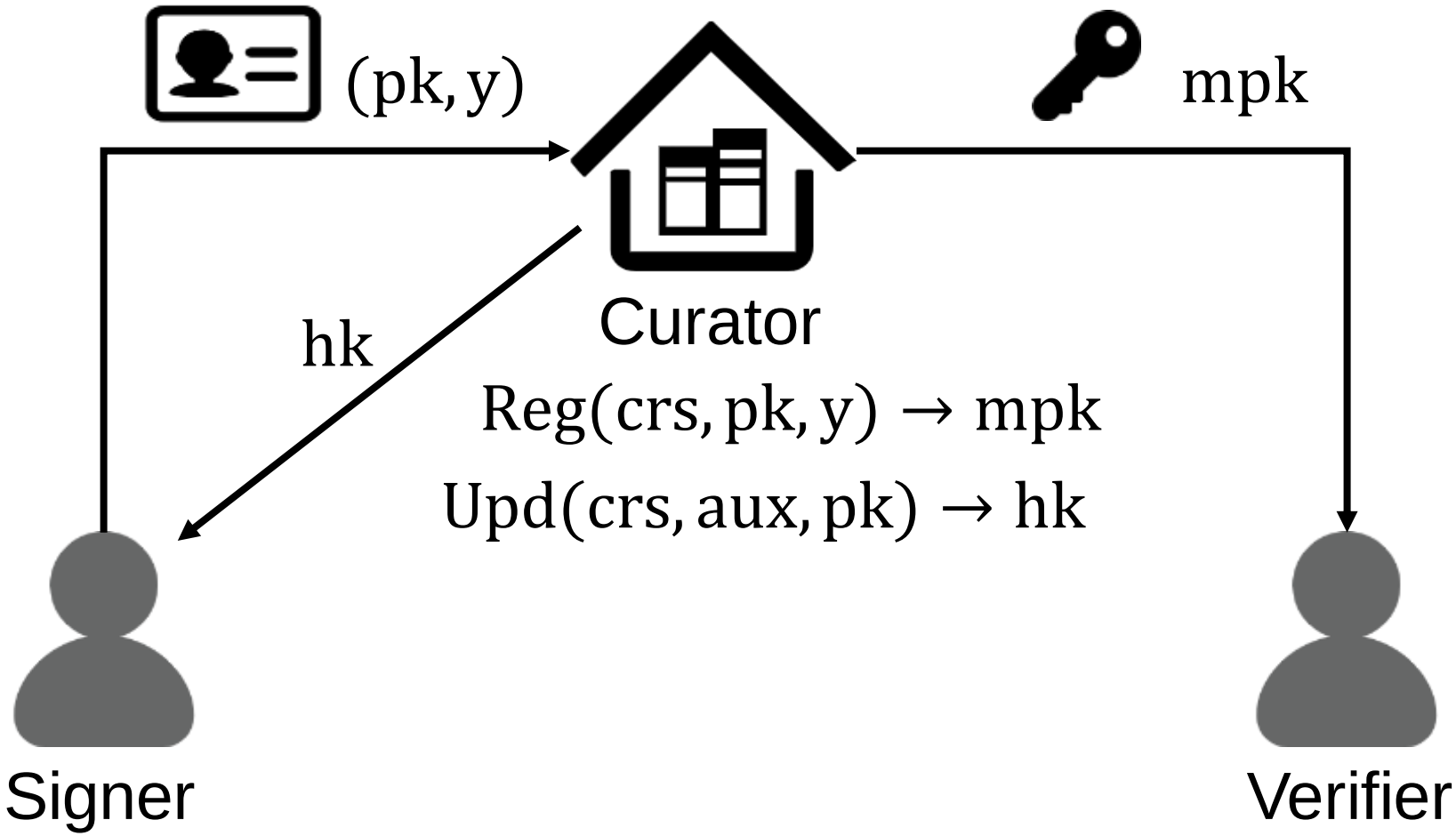


Signer

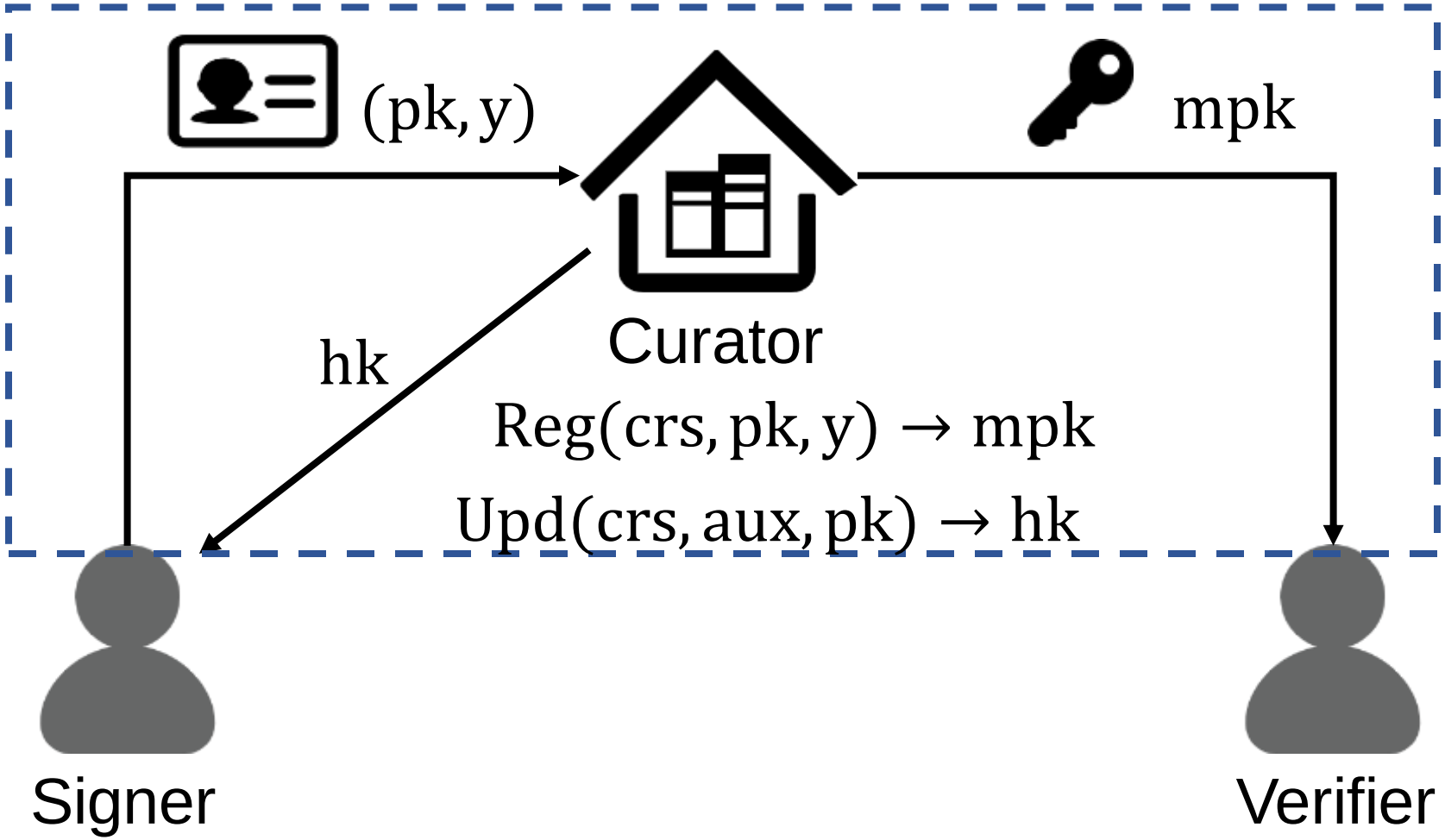
Verifier

$\mathrm{Gen}(\mathrm{crs}, \mathrm{aux}) \rightarrow (\mathrm{pk}, \mathrm{sk})$

Registered ABS

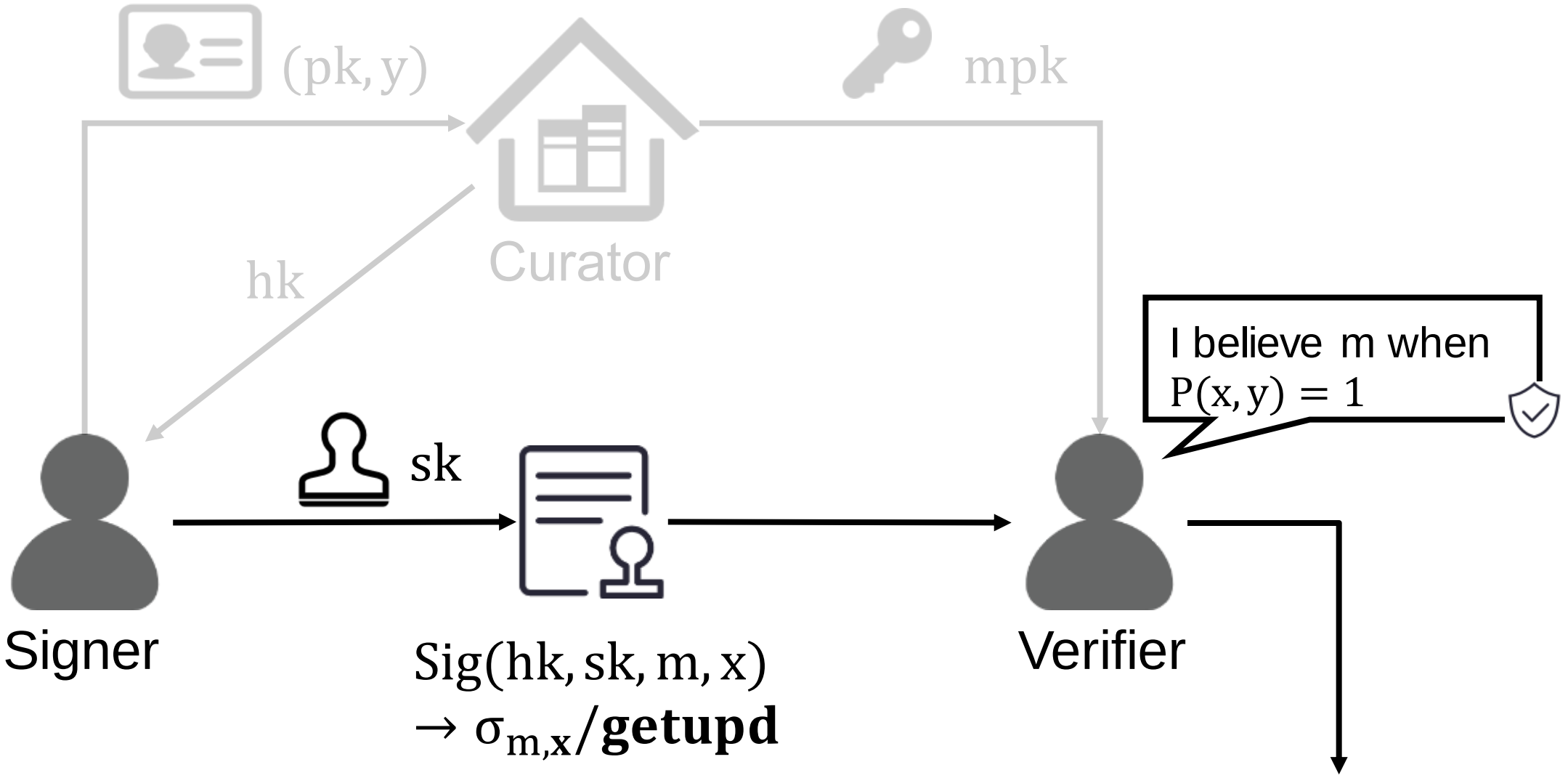


Registered ABS



Fully transparent
No secret stored

Registered ABS



Unforgeability

Challenger

crs

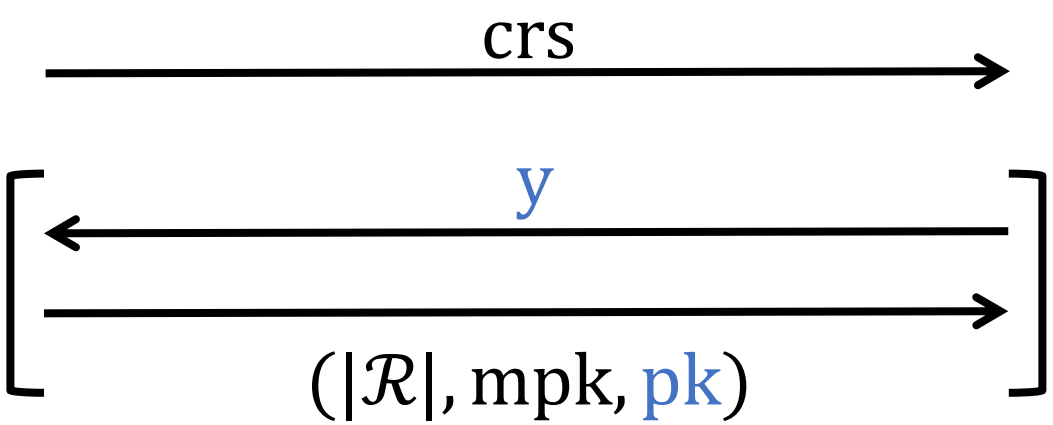
Adversary

$\mathrm{Setup}(1^{\lambda}, \mathrm{P}) \rightarrow \mathrm{crs}$

Unforgeability

Challenger

Adversary



Repeat

ORegHK(y):

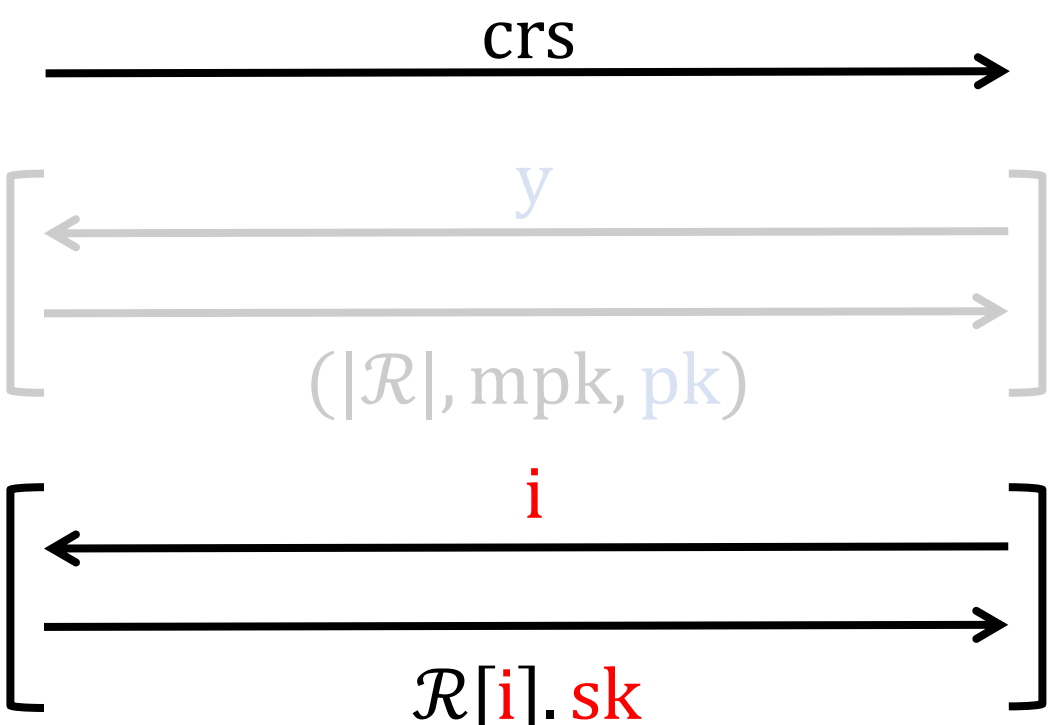
- $(pk, sk) \leftarrow Gen(crs, aux)$;
- Update $mpk \leftarrow Reg(crs, pk, y)$;
- Record (pk, sk) into $\mathcal{R}$:

1	2	…	$\lvert\mathcal{R}\rvert$
(pk, sk)	(pk, sk)	…	(pk, sk)

Unforgeability

Challenger

Adversary



ORegHK(y)

OCor(i):

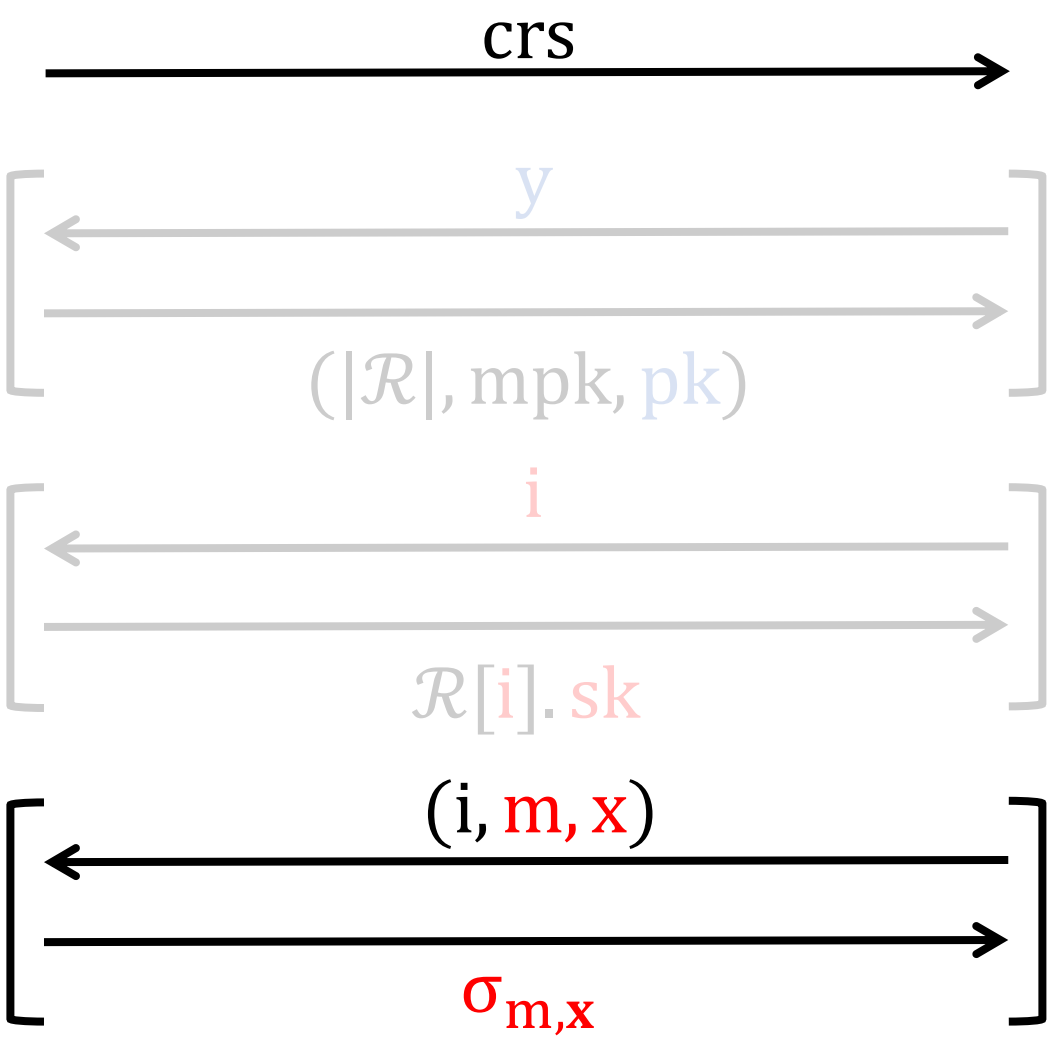
- Find $\mathcal{R}[i]$:

…	i	…
…	(pk, sk)	…

Unforgeability

Challenger

Adversary



ORegHK(y)

OCor(i)

OSig(i, m, x):

- Run hk ← Upd(crs, ℛ[i].pk)
- Run $\sigma_{m,x}$ ← Sig(hk, ℛ[i].sk, x, m)

Unforgeability

Challenger

crs →

Adversary

$\mathrm{ORegHK}(y)$

$\mathrm{OCor}(i)$

$(i^*, m^*, x^*, \sigma^*)$ ←

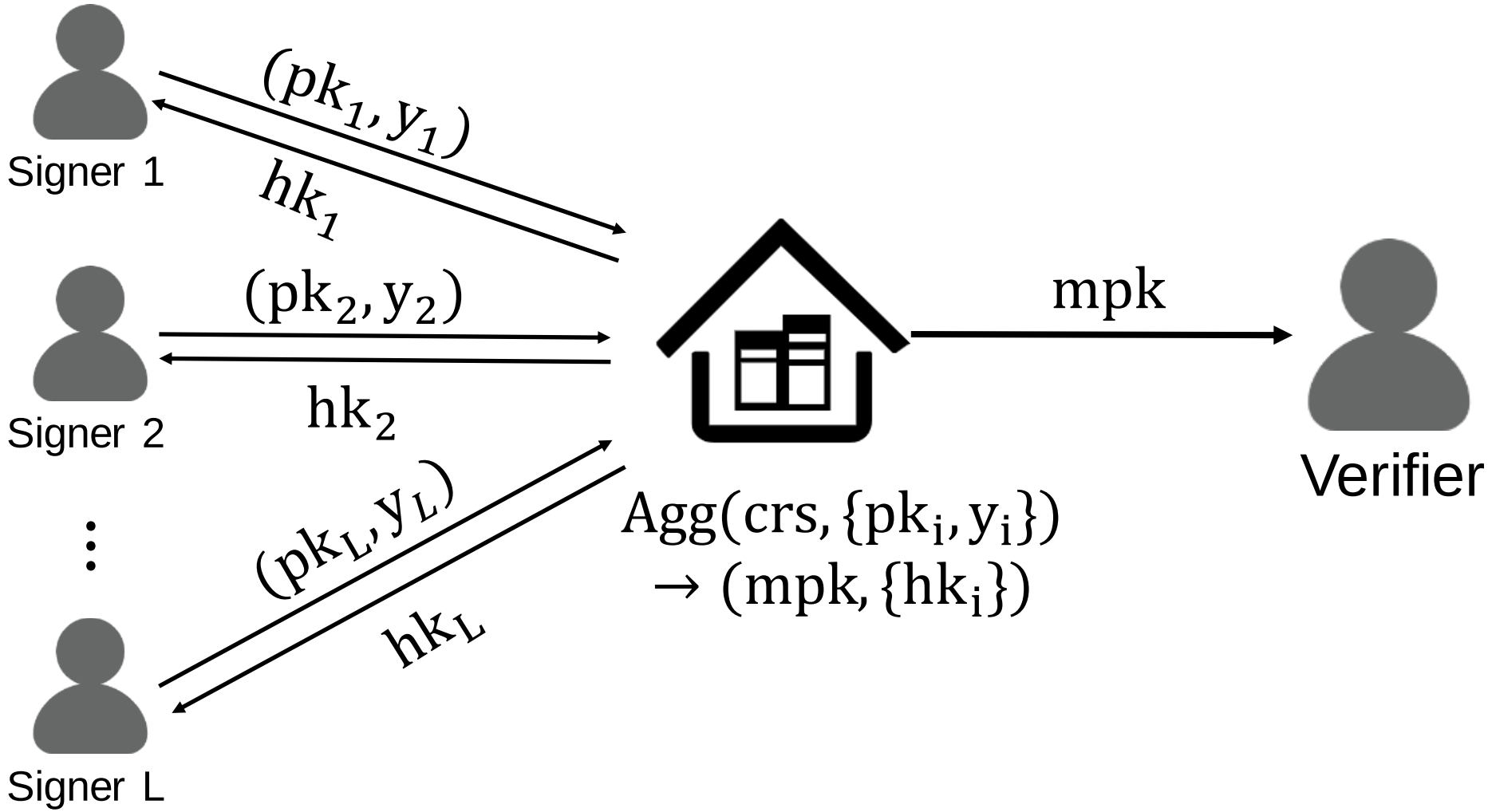
$\mathrm{OSig}(i, m, x)$

Forgery Phase:

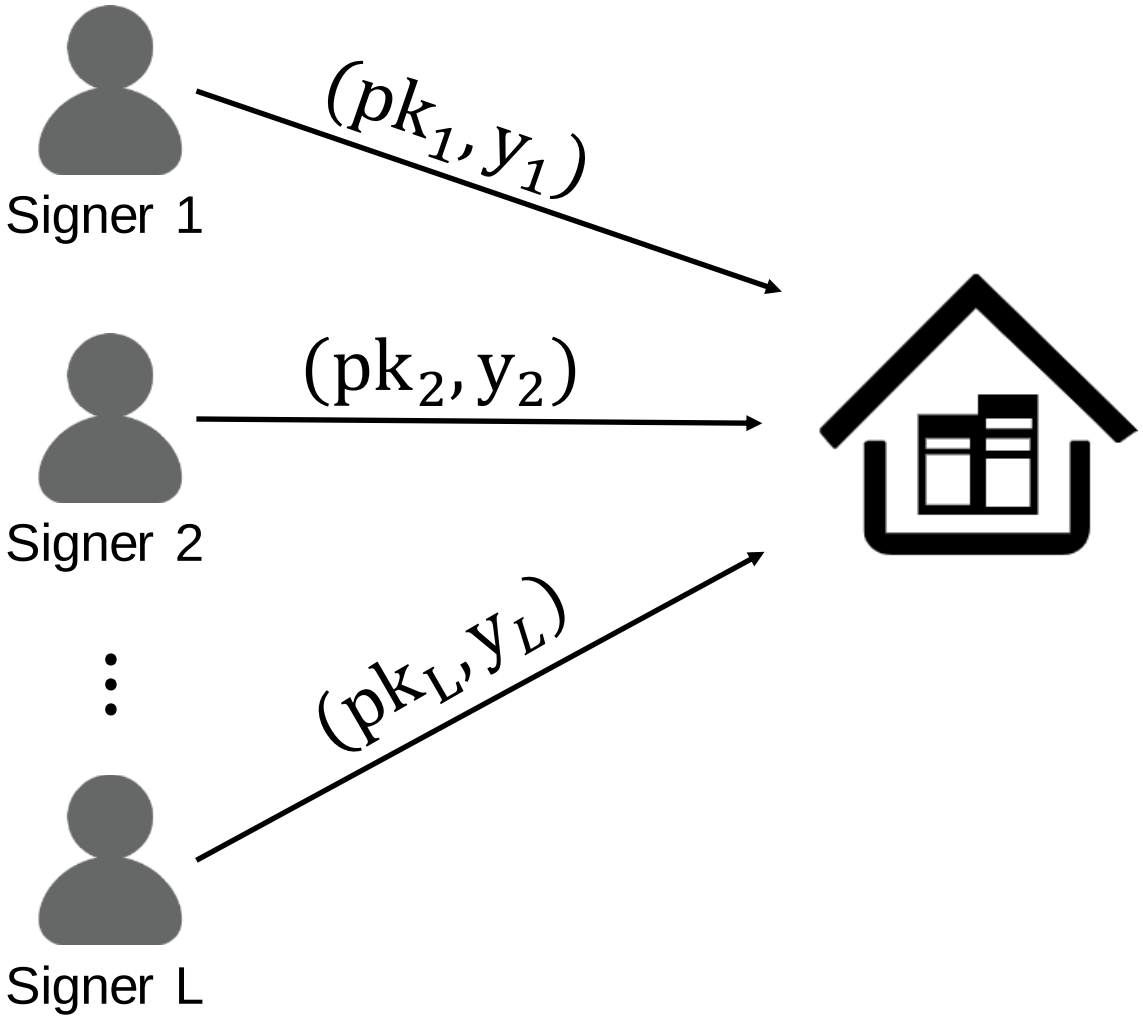
- $\mathcal{R}[i^*]$ is not empty
- $P(x^*, y_i) = 0$ for all $\mathrm{OCor}(i)$
- No query to $\mathrm{OSig}(i^*, m^*, x^*)$
- σ^* is valid

⟹ Successfully Forge!

Building Block: Slotted Registered ABS



Building Block: Slotted Registered ABS



Slotted Registered ABS

register at once

static

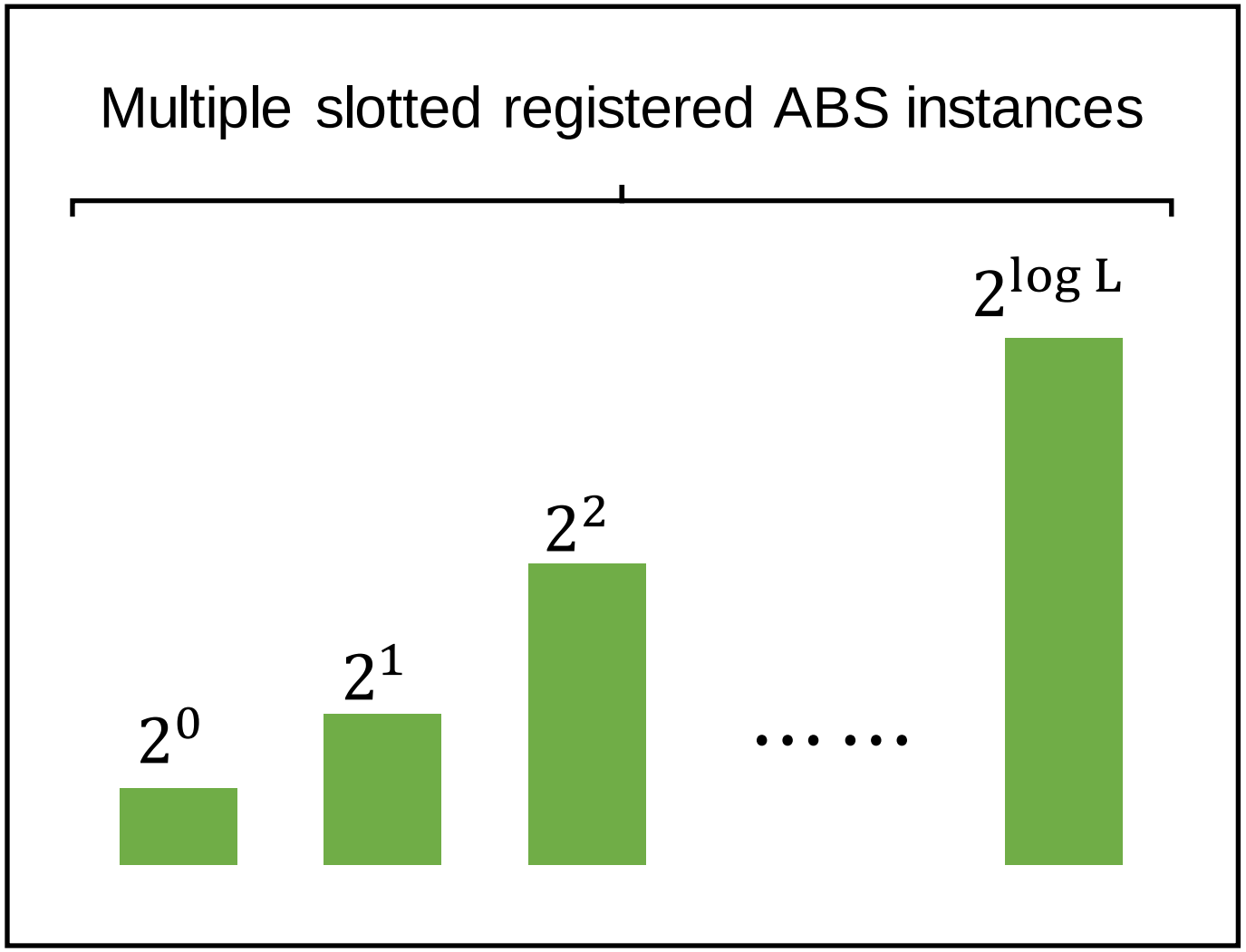
vs

Registered ABS

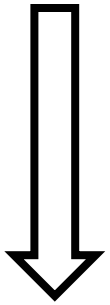
register dynamically

updatable

Construct Registered ABS

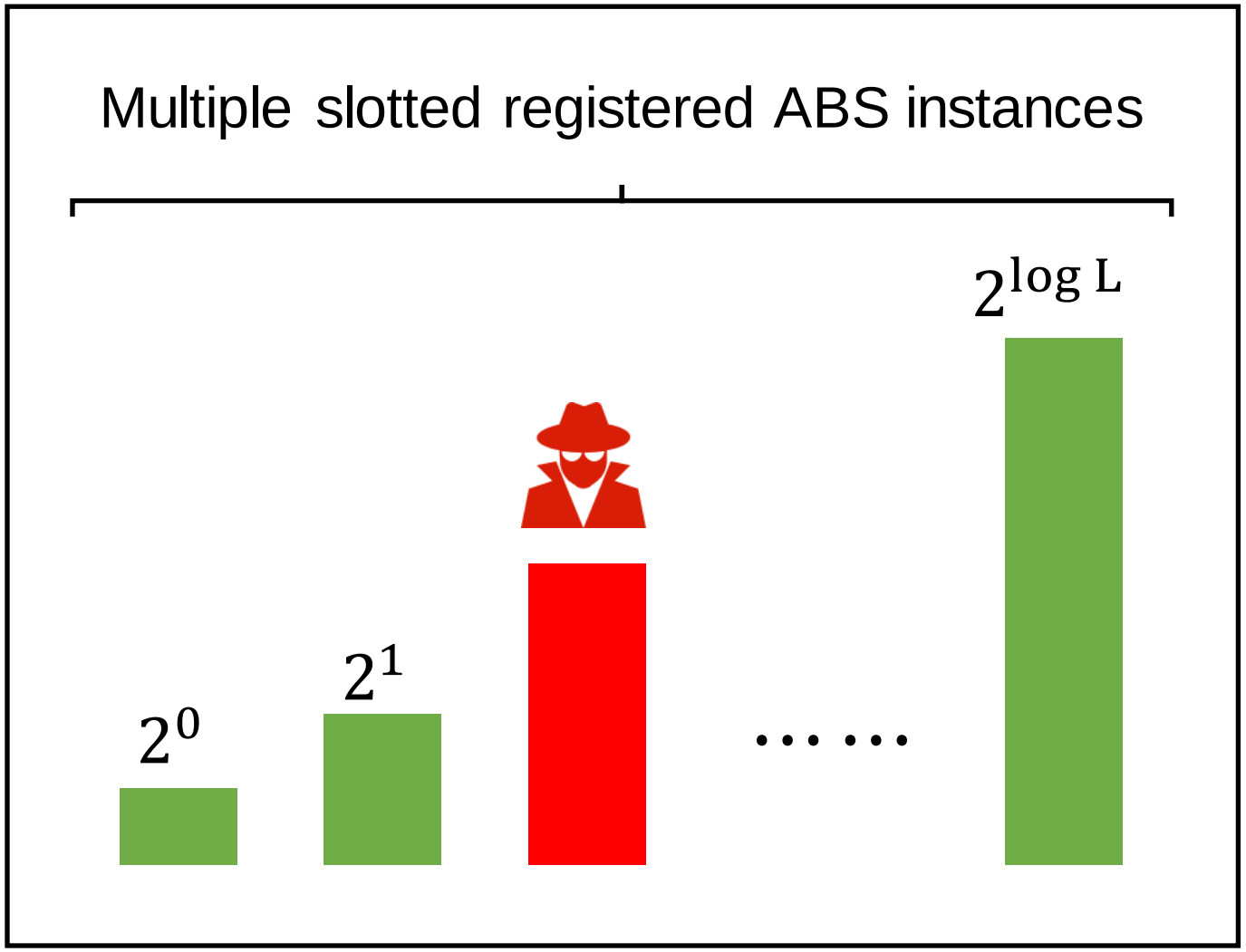


Slotted Registered ABS



Registered ABS

Construct Registered ABS



Slotted Registered ABS
(Unforgeability)

Registered ABS
(Unforgeability)

Construct Slotted Registered ABS

Inspired by [OT13], we start from slotted registered attribute-based encryption (ABE) based on bilinear groups [ZCGQ23]

Slotted Registered ABE $\Longrightarrow$ Slotted Registered ABS

Construct Slotted Registered ABS

Inspired by [OT13], we start from slotted registered attribute-based encryption (ABE) based on bilinear groups [ZCGQ23]

Slotted Registered ABE $\Longrightarrow$ **Slotted Registered ABS**

$(\mathrm{crs}, \mathrm{mpk})$ $(\mathrm{crs}, \mathrm{mpk})$

$(\mathrm{sk}_i, \mathrm{hk}_i)$ $(\mathrm{sk}_i, \mathrm{hk}_i)$

$\mathrm{Sig}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{m}, \mathrm{x}) \to \sigma_{\mathrm{m,x}}$

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

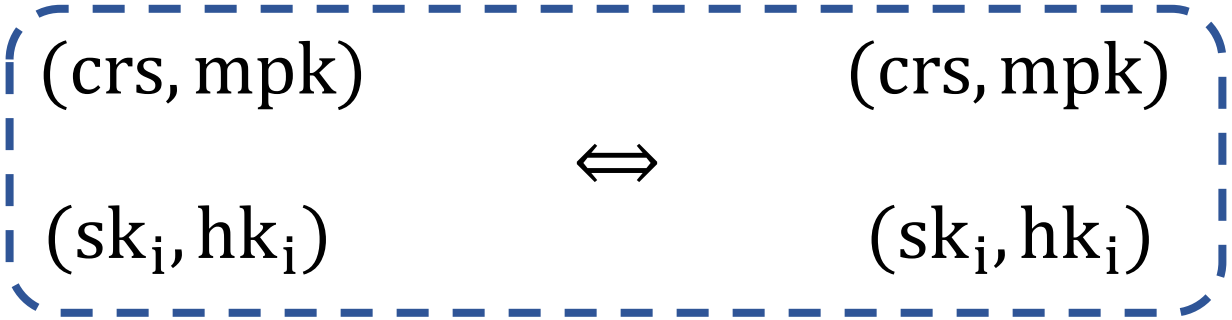
$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{ct}_{\mathrm{m,x}}) \to \mathrm{m}$

$\mathrm{Ver}(\mathrm{mpk}, \mathrm{m}, \mathrm{x}, \sigma_{\mathrm{m,x}}) \to 0/1$

Construct Slotted Registered ABS

Inspired by [OT13], we start from slotted registered attribute-based encryption (ABE) based on bilinear groups [ZCGQ23]

Slotted Registered ABE $\Longrightarrow$ **Slotted Registered ABS**



Registration

$$\mathrm{Sig}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{m}, \mathrm{x}) \to \sigma_{\mathrm{m,x}}$$

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

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{ct}_{\mathrm{m,x}}) \to \mathrm{m}$$

$$\mathrm{Ver}(\mathrm{mpk}, \mathrm{m}, \mathrm{x}, \sigma_{\mathrm{m,x}}) \to 0/1$$

Construct Slotted Registered ABS

Inspired by [OT13], we start from slotted registered attribute-based encryption (ABE) based on bilinear groups [ZCGQ23]

Slotted Registered ABE $\Longrightarrow$ **Slotted Registered ABS**

$(\mathrm{crs}, \mathrm{mpk})$

$(\mathrm{sk}_i, \mathrm{hk}_i)$

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

$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{ct}_{\mathrm{m,x}}) \to \mathrm{m}$

$(\mathrm{crs}, \mathrm{mpk})$

$(\mathrm{sk}_i, \mathrm{hk}_i)$

$\Downarrow$

$\mathrm{Sig}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{m}, \mathrm{x}) \to \sigma_{\mathrm{m,x}}$

Delegate

$\mathrm{Ver}(\mathrm{mpk}, \mathrm{m}, \mathrm{x}, \sigma_{\mathrm{m,x}}) \to 0/1$

Construct Slotted Registered ABS

Inspired by [OT13], we start from slotted registered attribute-based encryption (ABE) based on bilinear groups [ZCGQ23]

Slotted Registered ABE $\Rightarrow$ **Slotted Registered ABS**

$(\mathrm{crs}, \mathrm{mpk})$ $(\mathrm{crs}, \mathrm{mpk})$

$(\mathrm{sk}_i, \mathrm{hk}_i)$ $(\mathrm{sk}_i, \mathrm{hk}_i)$

$\Downarrow$

$\mathrm{Sig}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{m}, \mathrm{x}) \to \sigma_{\mathrm{m,x}}$

Verification Text

$v_{i,m,x}$

$\mathrm{Enc}(\mathrm{mpk}, \mathrm{m}, \mathrm{x}) \to \cancel{\mathrm{ct}_{\mathrm{m,x}}}$

$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{hk}_i, \mathrm{ct}_{\mathrm{m,x}}) \to \mathrm{m}$

$\Rightarrow \quad \mathrm{Ver}(\mathrm{mpk}, \mathrm{m}, \mathrm{x}, \sigma_{\mathrm{m,x}}) \to 0/1$

Construct Slotted Registered ABS

Inspired by [OT13], we start from slotted registered attribute-based encryption (ABE) based on bilinear groups [ZCGQ23]

Slotted Registered ABE $\Rightarrow$ **Slotted Registered ABS**

$(\mathrm{crs}, \mathrm{mpk})$ $(\mathrm{crs}, \mathrm{mpk})$

$(\mathrm{sk}_i, \mathrm{hk}_i)$ $(\mathrm{sk}_i, \mathrm{hk}_i)$

$\Downarrow$

$\mathrm{Sig}(\mathrm{sk}_i, \mathrm{hk}_i, m, x) \to \sigma_{m,x}$

Decryption

When $P(x, y) = 1$, recover m?

Verification Text

$\nu_{i,m,x}$

$\mathrm{Enc}(\mathrm{mpk}, m, x) \to \cancel{\mathrm{ct}_{m,x}}$

$\sigma_{i,m,x}$ $\nu_{i,m,x}$

$\mathrm{Dec}(\cancel{\mathrm{sk}_i}, \cancel{\mathrm{hk}_i}, \cancel{\mathrm{ct}_{m,x}}) \to m$

$\Rightarrow$ $\mathrm{Ver}(\mathrm{mpk}, m, x, \sigma_{m,x}) \to 0/1$

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

$$hk_i: [r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2,$$
$$[r_i \textstyle\sum_{j \neq i} \mathbf{w}_j]_2, [r_i, r_i \alpha_i + \alpha]_2$$

$$mpk: [\sum_j ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_1, [\sum_j \mathbf{w}_j]_1, [\alpha]_T$$

Construct Slotted Registered ABS

Predicate Encoding: $\exists\ \mathrm{M}_{x,y} = \begin{pmatrix} \mathbf{a}_y & \mathbf{0} \\ \mathbf{K}_y & \mathbf{C}_x \end{pmatrix}$ and $\mathbf{d}_{x,y}$:

- ***α*-reconstruction:** $\mathrm{P}(x,y) = 1 \Rightarrow \mathrm{M}_{x,y}\mathbf{d}_{x,y}^{T} = (1,0,\ldots,0)^{T}$;
- ***α*-privacy:** $\mathrm{P}(x,y) = 0 \Rightarrow \{x, y, \alpha, (\alpha||\mathbf{w})\mathrm{M}_{x,y}\} \approx_s \{x, y, \alpha, (0||\mathbf{w})\mathrm{M}_{x,y}\}$.

$$\mathrm{hk}_i: [r_i \sum_{j\neq i}((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j\mathbf{K}_{y_j})]_2,$$
$$[r_i \textstyle\sum_{j\neq i}\mathbf{w}_j]_2, [r_i, r_i\alpha_i + \alpha]_2$$

$$\mathrm{mpk}: [\sum_j((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j\mathbf{K}_{y_j})]_1, [\sum_j \mathbf{w}_j]_1, [\alpha]_T$$

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

$$hk_i: [r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2,$$
$$[r_i \textstyle\sum_{j \neq i} \mathbf{w}_j]_2, [r_i, r_i\alpha_i + \alpha]_2$$

$+ u_i$

$$[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2,$$
$$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2, [r_i, r_i\alpha_i + r_i u_i + \alpha]_2$$

$$mpk: [\sum_j ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_1, [\sum_j \mathbf{w}_j]_1, [\alpha]_T$$

Verification Text

$$v_{i^*,m^*,x^*}: [s, s \sum_j ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_1,$$
$$[s \sum_j \mathbf{w}_j \mathbf{C}_{x^*}]_1, [\alpha s]_T$$

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

Verify signature from slot i:

$$\sigma_{i,m,x}: [r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2,$$
$$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2, [r_i, r_i\alpha_i + r_i u_i + \alpha]_2$$

$$\nu_{i^*,m^*,x^*}: [s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1,$$
$$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1, [\alpha s]_T$$

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

$\sigma_{i,m,x}$: $[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2$,

$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2$, $[r_i, r_i\alpha_i + r_i u_i + \alpha]_2$

ν_{i^*,m^*,x^*}: $[s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1$,

$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1, [\alpha s]_T$

Verify signature from slot i:

1. Cancel cross terms for $j \neq i$ via pairing

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

$$\sigma_{i,m,x}: [r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2,$$
$$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2, [r_i, r_i\alpha_i + r_i u_i + \alpha]_2$$

$$\nu_{i^*,m^*,x^*}: [s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1,$$
$$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1, [\alpha s]_T$$

Verify signature from slot i:

1. Cancel cross terms for $j \neq i$ via pairing
2. Check $P(x, y_i) = 1$ via ***α*-reconstruction**

➢ ***α*-reconstruction:** $P(x, y) = 1 \Rightarrow M_{x,y}\mathbf{d}_{x,y}^T = (1,0,\ldots,0)^T$.

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

$\sigma_{i,m,x}$: $[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2$,

$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2, [r_i, r_i\alpha_i + r_i u_i + \alpha s]_T$

ν_{i^*,m^*,x^*}: $[s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1$,

$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1, [\alpha s]_T$

Verify signature from slot i:

1. Cancel cross terms for $j \neq i$ via pairing
2. Check $P(x, y_i) = 1$ via ***α*-reconstruction**
3. Cancel (α_i, u_i) and check

$[\alpha s]_T = [\alpha s]_T$?

Construct Slotted Registered ABS

sk_i: u_i
Secrets: α_i, α

$\sigma_{i,m,x}$: $[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2$,

$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2$, $[r_i \alpha_i + r_i u_i + \alpha]_2$

ν_{i^*,m^*,x^*}: $[s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1$,

$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1$, $[\alpha s]_T$

Verify signature from slot i:

1. Cancel cross terms for $j \neq i$ via pairing
2. Check $P(x, y_i) = 1$ via ***α*-reconstruction**
3. Cancel (α_i, u_i) and check

$$[\alpha s]_T = [\alpha s]_T \ ?$$

Problem:
u_i is completely leaked, anyone can acquire it!

Construct Slotted Registered ABS

sk_i: u_i, c_i, d_i
Secrets: α_i, α

$\sigma_{i,m,x}$: $[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2$,

$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2$,

$[r_i, t, t(c_i + \mathrm{Hash}(i, m, x) \cdot d_i) + r_i u_i + r_i \alpha_i + \alpha]_2$

ν_{i^*,m^*,x^*}: $[s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1$,

$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1$,

$[s(c_i + \mathrm{Hash}(i, m^*, x^*) \cdot d_i)]_1$ $[\alpha s]_T$

Verify signature from slot i:

1. Cancel cross terms for $j \neq i$ via pairing
2. Check $P(x, y_i) = 1$ via ***α*-reconstruction**
3. Cancel (α_i, u_i) and check

$$[\alpha s]_T = [\alpha s]_T \ ?$$

Solution:
sample new randomness t and use $(c_i + \mathrm{Hash} \cdot d_i)$ to hide u_i

Security Proof

sk_i: u_i, c_i, d_i
Secrets: α_i, α

$\sigma_{i,m,x}$: $[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2$,

$[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2$,

$[r_i, t, t(c_i + Hash(i, m, x) \cdot d_i) + r_i u_i + r_i \alpha_i + \boxed{\alpha}]_2$

ν_{i^*,m^*,x^*}: $[s, s \sum_j ((\alpha_i + u_i)\mathbf{a}_{y_i} + \mathbf{w}_i \mathbf{K}_{y_i})]_1$,

$[s \sum_j (\mathbf{w}_i \mathbf{C}_{x^*})]_1$,

$[s(c_i + Hash(i, m^*, x^*) \cdot d_i)]_1$, $\boxed{[\alpha s]_T}$

Verify signature from slot i:

1. Cancel cross terms for $j \neq i$ via pairing
2. Check $P(x, y_i) = 1$ via ***α*-reconstruction**
3. Cancel (α_i, u_i) and check

$$\boxed{[random]_T = [\alpha s]_T \ ?}$$

⇩

Invalid forged signature

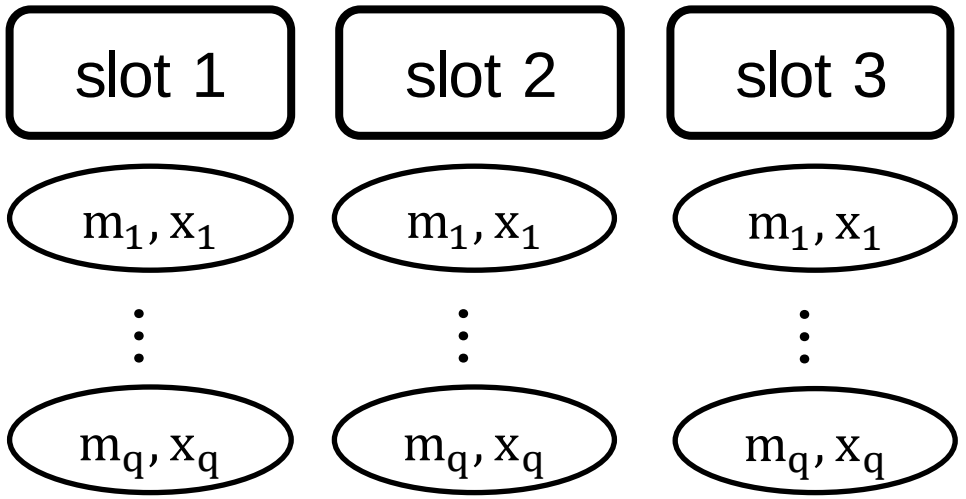
Security Proof

sk_i: u_i, c_i, d_i
Secrets: α_i, α

$$\sigma_{i,m,x}: \left[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})\right]_2, \left[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x\right]_2,$$
$$[t, r_i, t(c_i + \mathrm{Hash}(i, m, x) \cdot d_i) + r_i u_i + r_i \alpha_i + \alpha]_2$$

$$\nu_{i^*,m^*,x^*}: \left[s, s \sum_j ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})\right]_1, [\alpha s]_T,$$
$$\left[s \sum_j \mathbf{w}_j \mathbf{C}_x\right]_1, \left[s \sum_j (c_i + \mathrm{Hash}(i^*, m^*, x^*) \cdot d_i)\right]_1$$

Honest Case



$P(x^*, y_i) = 1$ and allow signature queries on $(i, m, x) \neq (i^*, m^*, x^*)$

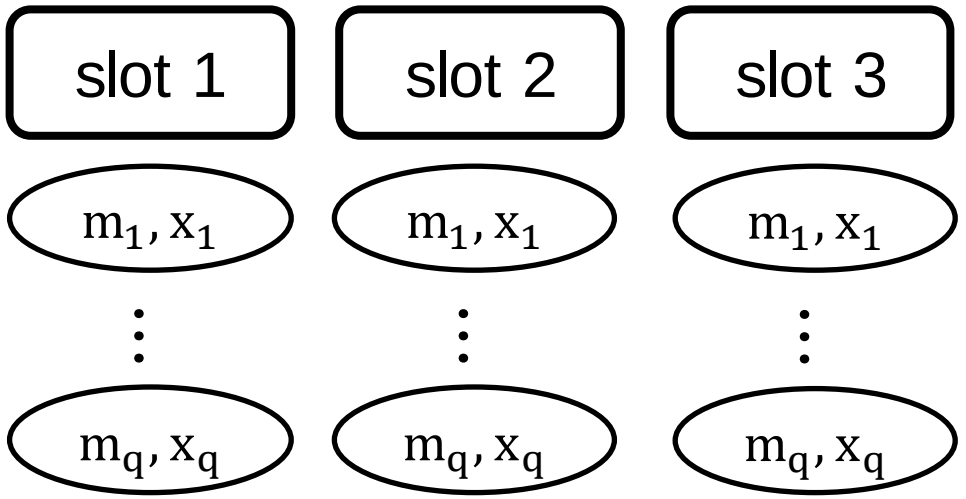
Security Proof

sk_i: u_i, c_i, d_i
Secrets: α_i, α

$$\sigma_{i,m,x}: \left[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})\right]_2, \left[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x\right]_2,$$
$$[t, r_i, t(c_i + \mathrm{Hash}(i, m, x) \cdot d_i) + r_i u_i + r_i \alpha_i + \alpha]_2$$

$$\nu_{i^*,m^*,x^*}: \left[s, s \sum_j ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})\right]_1, [\alpha s]_T,$$
$$\left[s \sum_j \mathbf{w}_j \mathbf{C}_x\right]_1, \left[s \sum_j (c_i + \mathrm{Hash}(i^*, m^*, x^*) \cdot d_i)\right]_1$$

Honest Case



Adversary don't know u_i and $(c_i + \mathrm{Hash}(i, m, x) \cdot d_i)$ hide extra u_i so that α_i can hide α

Security Proof

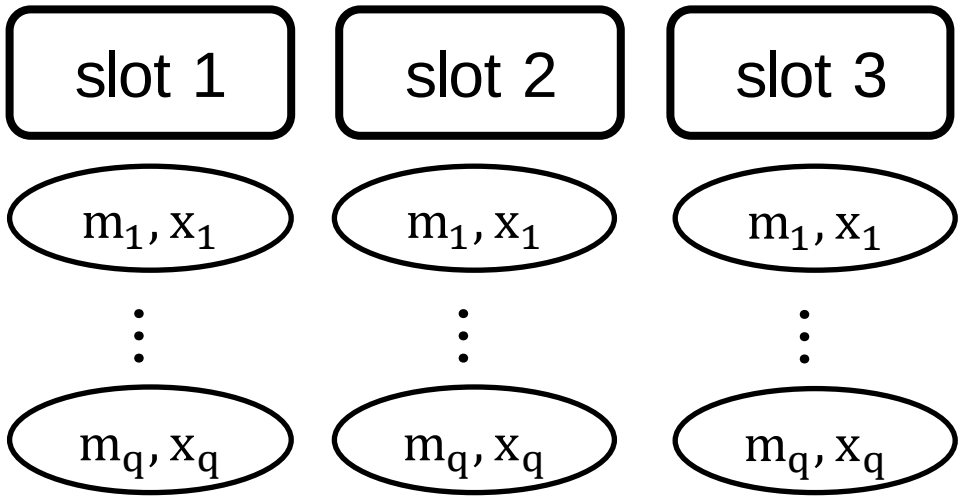
sk_i: u_i, c_i, d_i
Secrets: α_i, α

$$\sigma_{i,m,x}: [r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2, [r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2,$$
$$[t, r_i, t(c_i + \mathrm{Hash}(i,m,x) \cdot d_i) + r_i u_i + \boxed{r_i \alpha_i + \alpha}]_2$$

Random

$$\nu_{i^*,m^*,x^*}: [s, s \sum_j (\boxed{(\alpha_j + u_j)}\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_1, [\alpha s]_T,$$
$$[s \sum_j \mathbf{w}_j \mathbf{C}_x]_1, [s \sum_j (c_i + \mathrm{Hash}(i^*, m^*, x^*) \cdot d_i)]_1$$

Honest Case



Adversary don't know u_i and $(c_i + \mathrm{Hash}(i,m,x) \cdot d_i)$ hide extra u_i so that α_i can hide α

Security Proof

sk_i: u_i, c_i, d_i
Secrets: α_i, α

$$\sigma_{i,m,x}: \left[r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})\right]_2, \left[r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x\right]_2,$$
$$[t, r_i, t(c_i + \mathrm{Hash}(i, m, x) \cdot d_i) + r_i u_i + r_i \alpha_i + \alpha]_2$$

$$\nu_{i^*,m^*,x^*}: \left[s, s \sum_j ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})\right]_1, [\alpha s]_T,$$
$$\left[s \sum_j \mathbf{w}_j \mathbf{C}_x\right]_1, \left[s \sum_j (c_i + \mathrm{Hash}(i^*, m^*, x^*) \cdot d_i)\right]_1$$

Corrupt Case

slot 1 | slot 2 | slot 3

$P(x^*, y_i) = 0$ and adversary has known u_i, c_i, d_i

Security Proof

sk_i: u_i, c_i, d_i
Secrets: α_i, α

Corrupt Case

slot 1 | slot 2 | slot 3

$$\sigma_{i,m,x}: [r_i \sum_{j \neq i} ((\alpha_j + u_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_2, [r_i \sum_{j \neq i} \mathbf{w}_j \mathbf{C}_x]_2,$$
$$[t, r_i, t(c_i + \mathrm{Hash}(i,m,x) \cdot d_i) + r_i u_i + \boxed{r_i \alpha_i + \alpha}]_2$$

Random

hide extra α_i when $P(x^*, y_j) = 0$

$$\nu_{i^*,m^*,x^*}: [s, s \sum_j (\boxed{0 + u_j})\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})]_1, [\alpha s]_T,$$
$$[s \sum_j \mathbf{w}_j \mathbf{C}_x]_1, [s \sum_j (c_i + \mathrm{Hash}(i^*, m^*, x^*) \cdot d_i)]_1$$

➢ ***α*-privacy:** $P(x,y) = 0 \Rightarrow \{x, y, \alpha, (\alpha || \mathbf{w}) M_{x,y}\} \approx_s \{x, y, \alpha, (0 || \mathbf{w}) M_{x,y}\}.$

Open Problems

- More expressive predicates such as finite state automata and circuits;
- Signer Anonymity;
- LWE-based construction;

.....

Thank You!