Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding

Jie Chen

ECNU

Junqing Gong

ENS de Lyon

Hoeteck Wee

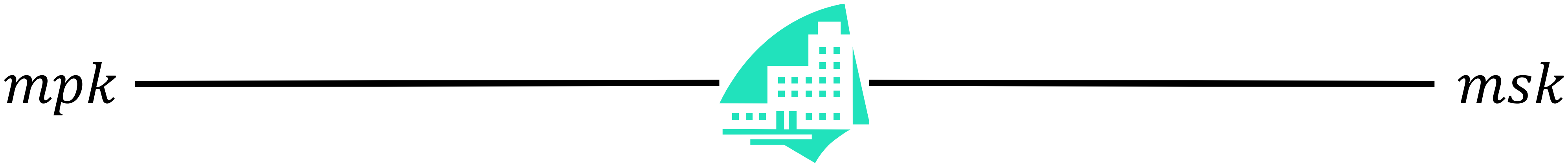
CNRS & ENS, PSL

attribute-based encryption (ABE)

[SW05, GPSW06]

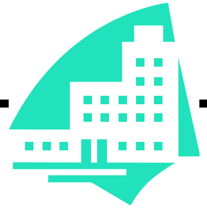
attribute-based encryption (ABE)

[SW05, GPSW06]



attribute-based encryption (ABE)

[SW05, GPSW06]

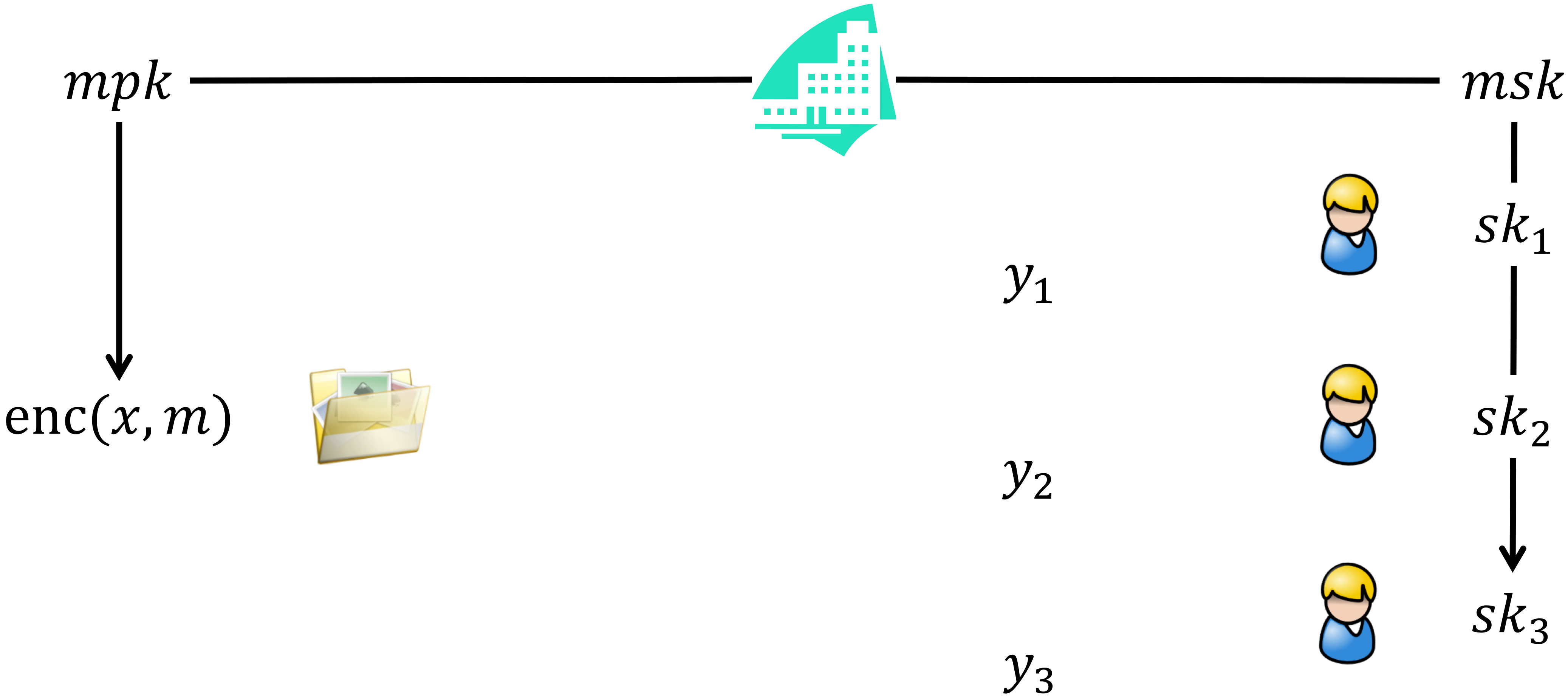
mpk  msk

$\downarrow$

$\mathrm{enc}(x, m)$ 

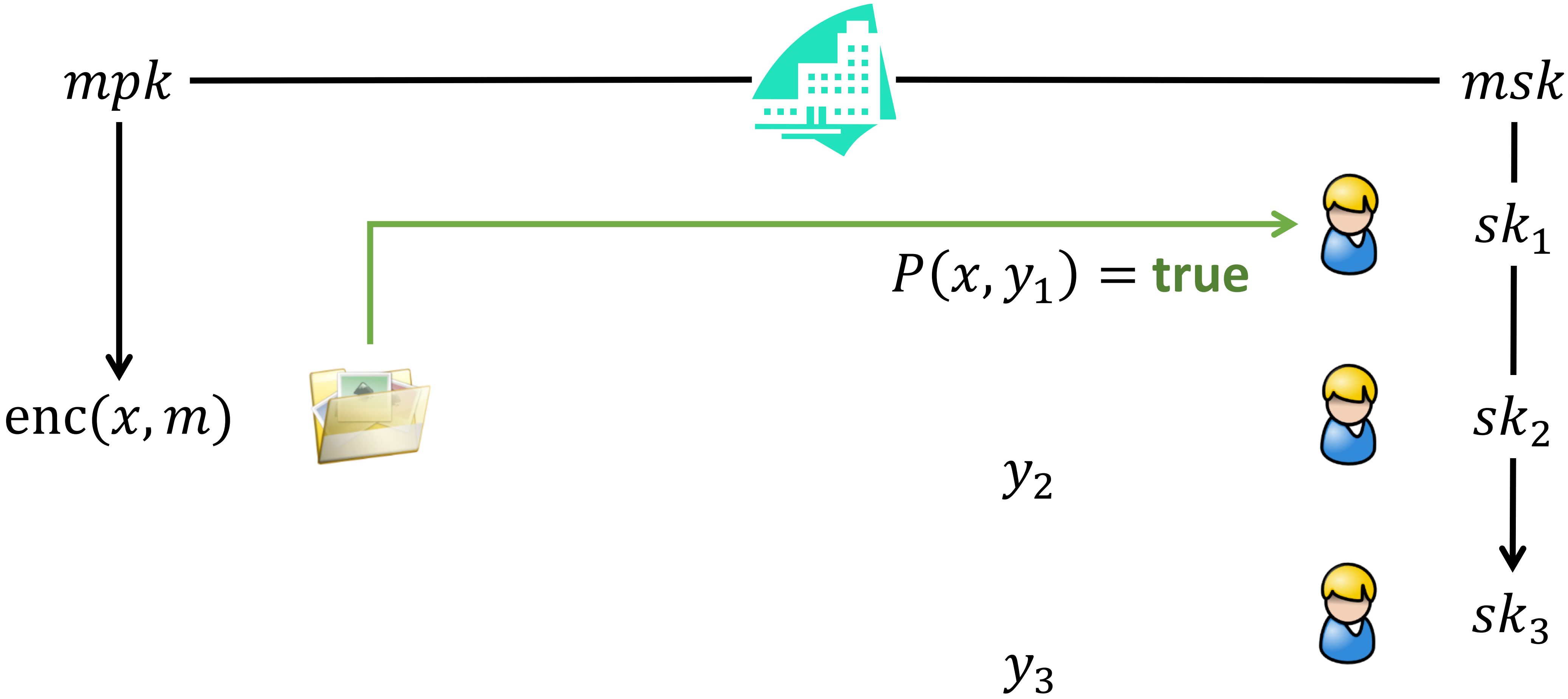
attribute-based encryption (ABE)

[SW05, GPSW06]



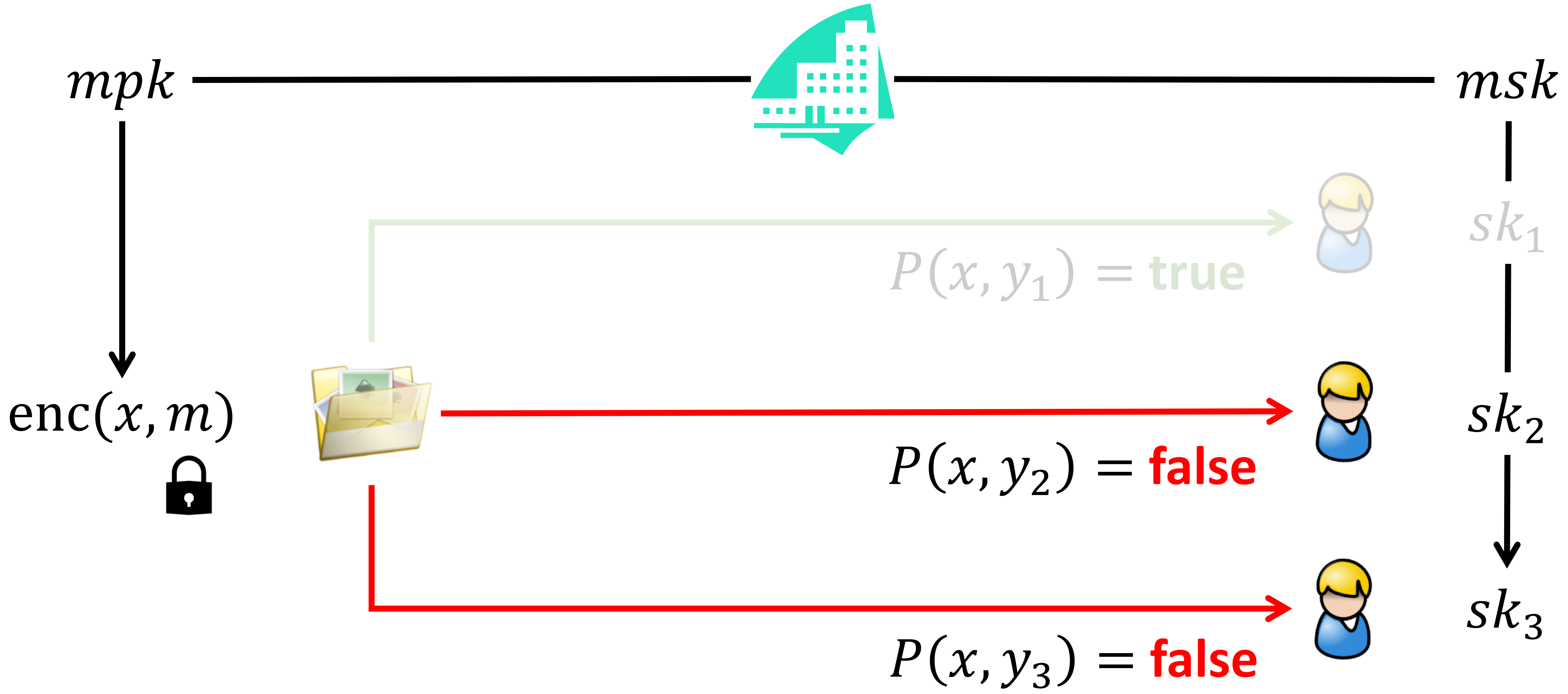
attribute-based encryption (ABE)

[SW05, GPSW06]



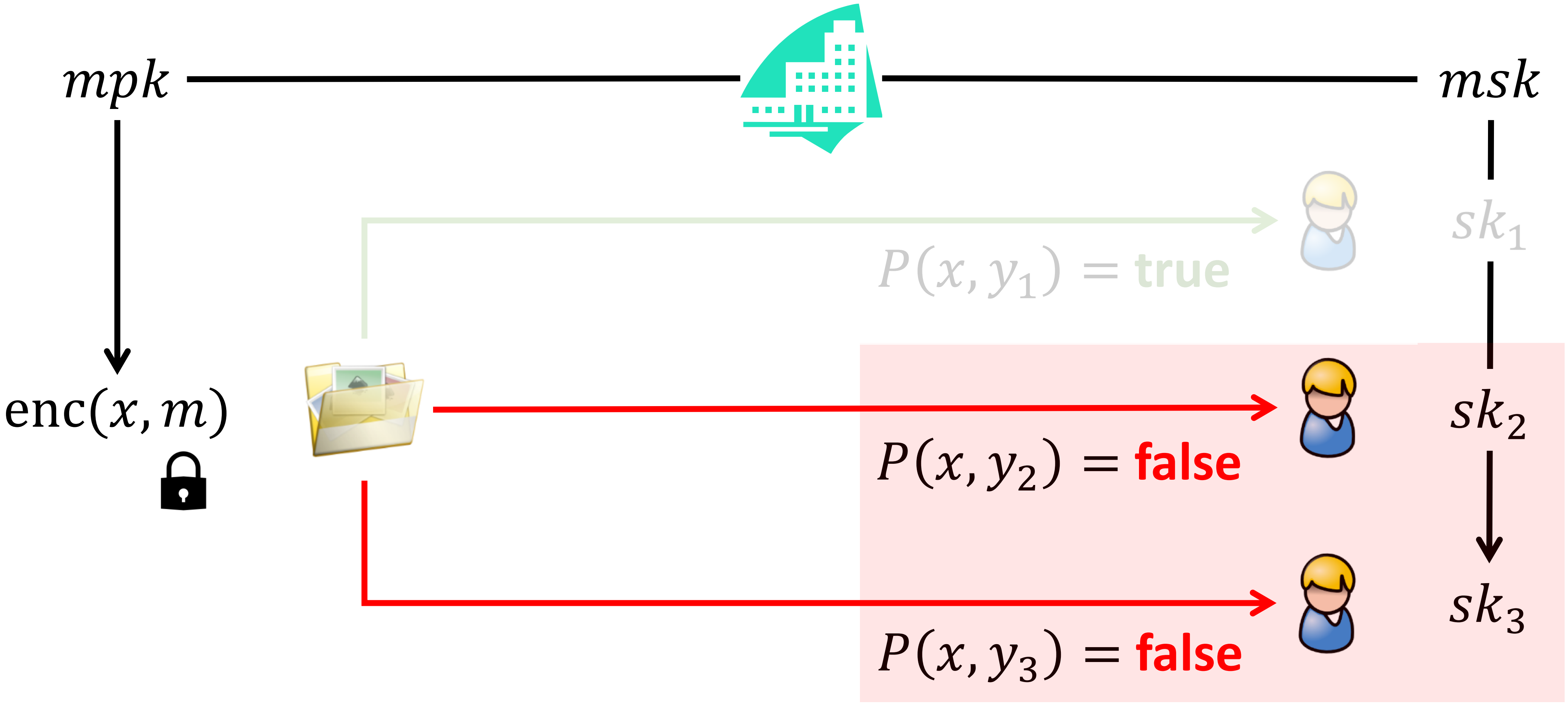
attribute-based encryption (ABE)

[SW05, GPSW06]



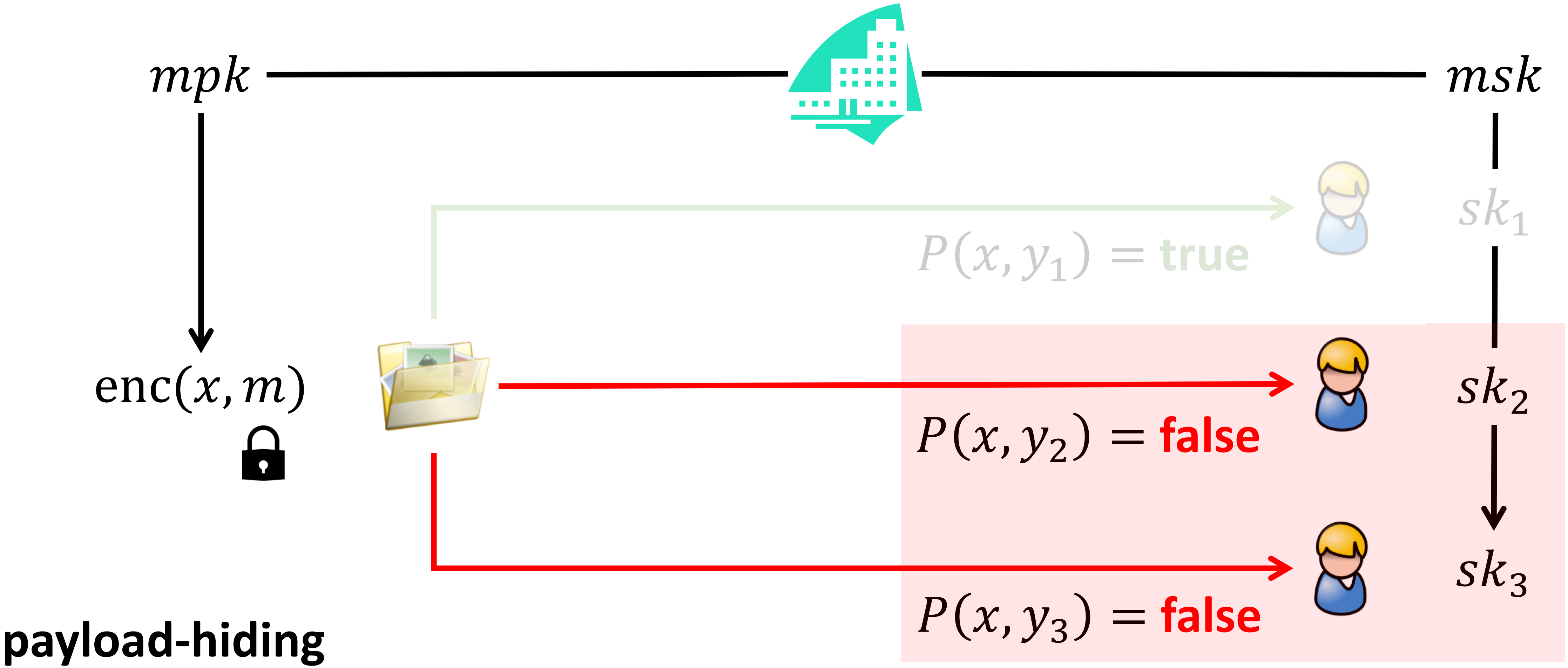
attribute-based encryption (ABE)

[SW05, GPSW06]



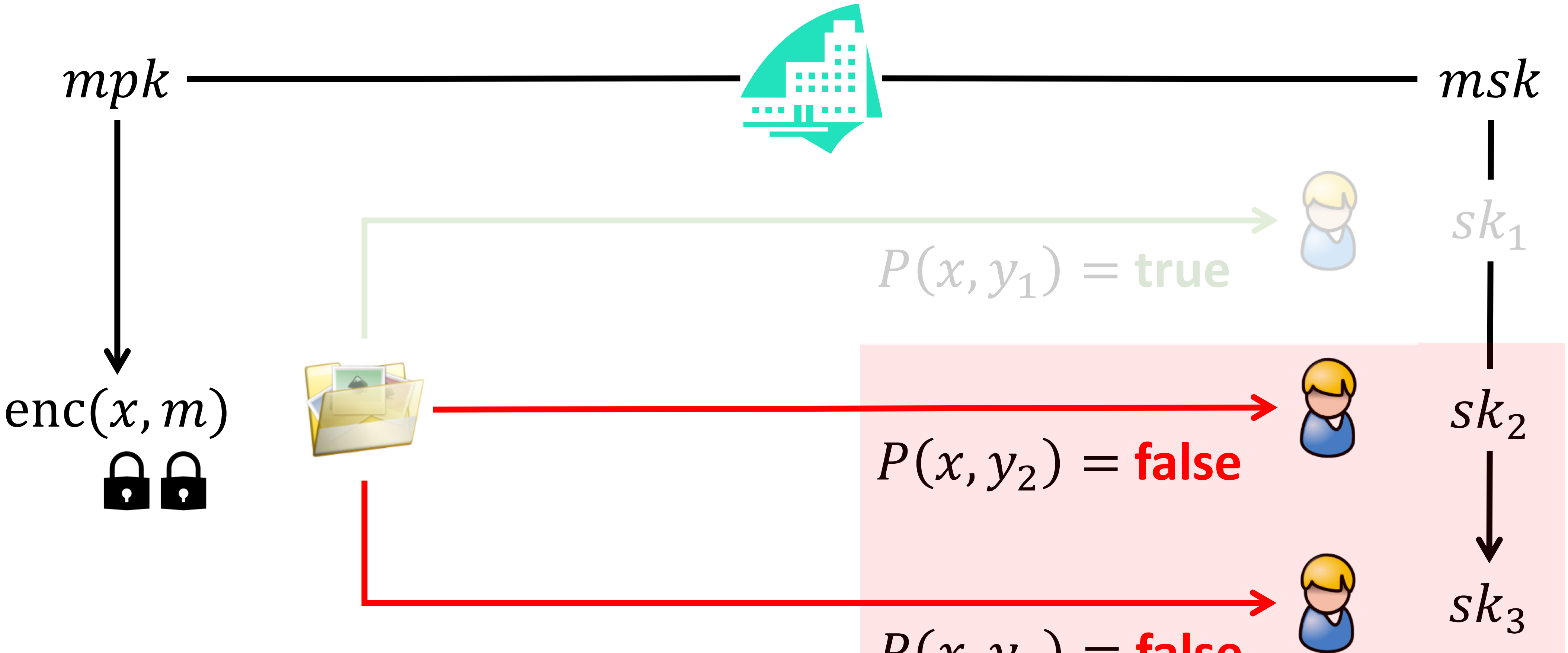
attribute-based encryption (ABE)

[SW05, GPSW06]



attribute-based encryption (ABE)

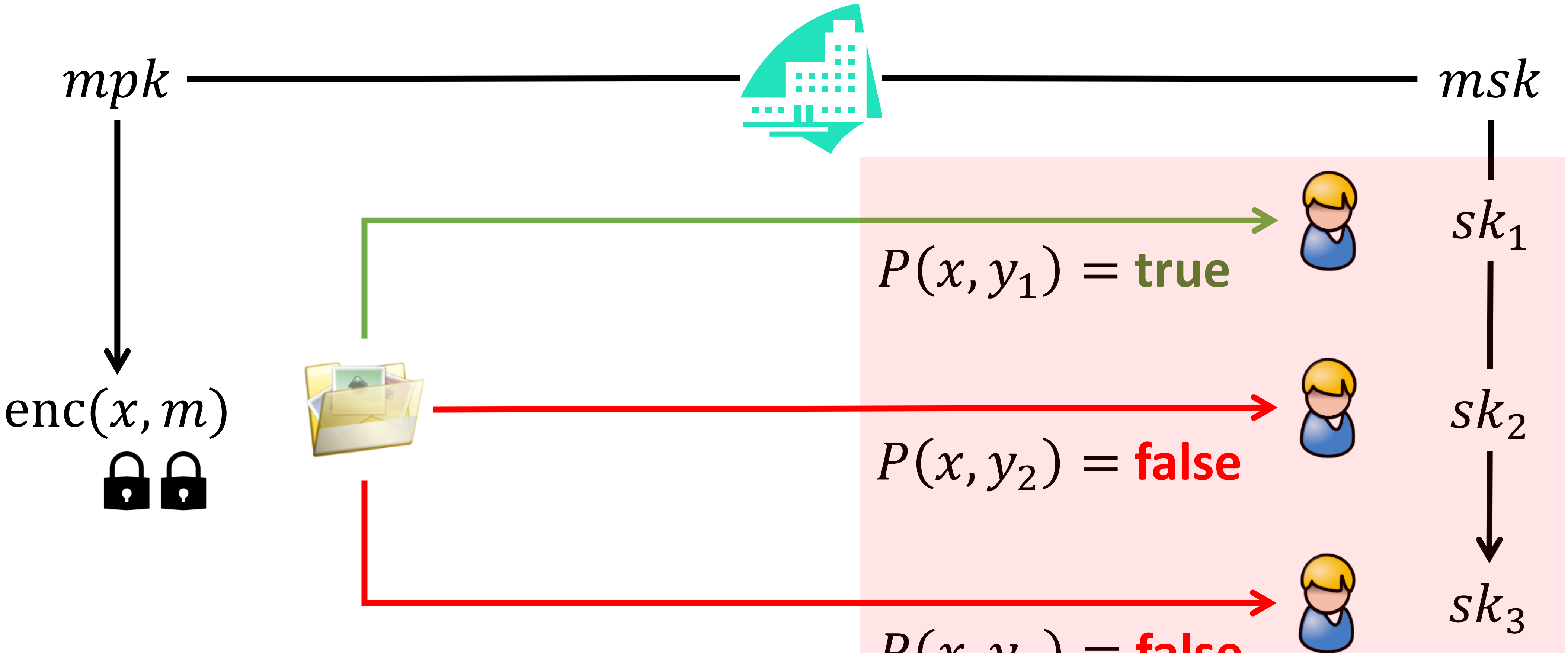
[SW05, GPSW06]



payload-hiding + attribute-hiding (weak)

attribute-based encryption (ABE)

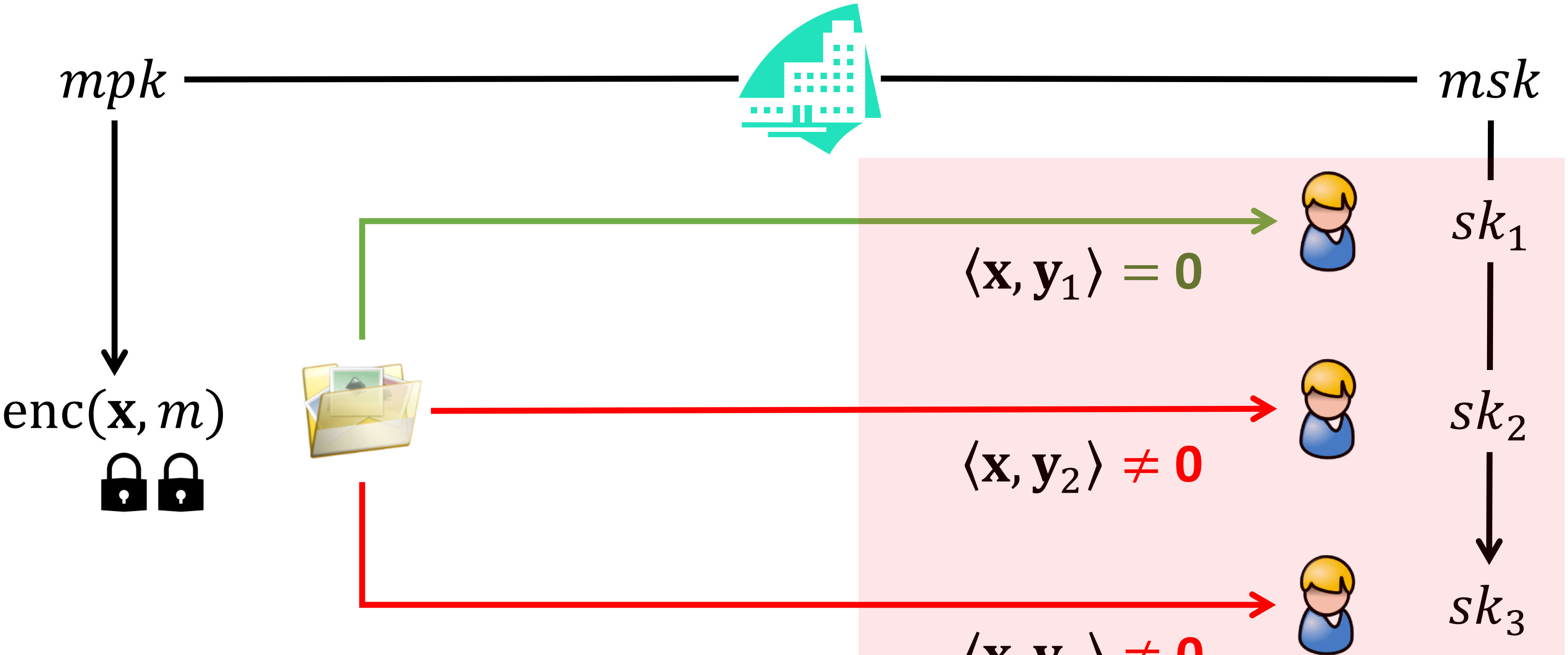
[SW05, GPSW06]



payload-hiding + attribute-hiding (full)

inner-product encryption (IPE)

[KSW08]



payload-hiding + attribute-hiding (full)

motivation

Boneh-Waters @ TCC'07

Katz-Sahai-Waters @ EC'08

Okamoto-Takashima @ EC'12

Okamoto-Takashima @ IEICE'13

Wee @ TCC'17

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

Okamoto-Takashima @ EC'12

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\|mpk\|$	$\|ct\|$	$\|sk\|$	assumption
Okamoto-Takashima @ EC'12				

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\lvert mpk \rvert$	$\lvert ct \rvert$	$\lvert sk \rvert$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\|mpk\|$	$\|ct\|$	$\|sk\|$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN
this work - basic	$10n + 16$	$5n + 3$	8	DLIN

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\|mpk\|$	$\|ct\|$	$\|sk\|$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN
this work - basic	$10n + 16$	$5n + 3$	8	DLIN

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\lvert mpk \rvert$	$\lvert ct \rvert$	$\lvert sk \rvert$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN
this work - basic	$10n + 16$	$5n + 3$	8	DLIN
	$3n + 5$	$3n + 2$	5	SXDH

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\lvert mpk \rvert$	$\lvert ct \rvert$	$\lvert sk \rvert$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN
this work - basic	$10n + 16$	$5n + 3$	8	DLIN
	$3n + 5$	$3n + 2$	5	SXDH

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\lvert mpk\rvert$	$\lvert ct\rvert$	$\lvert sk\rvert$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN
this work - basic	$10n + 16$	$5n + 3$	8	DLIN
	$3n + 5$	$3n + 2$	5	SXDH
this work - refined	$8n + 14$	$4n + 3$	7	XDLIN

motivation

We prefer a construction in **prime-order** groups with **adaptive security**.

scheme	$\|mpk\|$	$\|ct\|$	$\|sk\|$	assumption
Okamoto-Takashima @ EC'12	$12n + 16$	$5n + 1$	11	XDLIN
this work - basic	$10n + 16$	$5n + 3$	8	DLIN
	$3n + 5$	$3n + 2$	5	SXDH
this work - refined	$8n + 14$	$4n + 3$	7	XDLIN

strategy

Okamoto-Takashima @ EC’12

this work - basic

this work - refined

strategy

an AH IPE in comp-order groups

Okamoto-Takashima @ EC’12

this work - basic

this work - refined

strategy

an AH IPE in comp-order groups — comp-to-prime translator

Okamoto-Takashima @ EC'12

this work - basic

this work - refined

strategy

an AH IPE in comp-order groups — comp-to-prime translator

Okamoto-Takashima @ EC’12

this work - basic

[Gong-Chen-Dong-Cao-Tang @ PKC’16]

this work - refined

technique

an AH IPE in comp-order groups — comp-to-prime translator

Okamoto-Takashima @ EC’12

this work - basic

[Gong-Chen-Dong-Cao-Tang @ PKC’16]

this work - refined

an AH IPE in comp-order groups comp-to-prime translator

technique

technique

$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$

an AH IPE in comp-order groups comp-to-prime translator

technique

$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$

G

H

an AH IPE in comp-order groups   comp-to-prime translator

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

G $\qquad$ g^s

H $\qquad$ h^r

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e: G \times H \to G_T).$$

G	g^s	$=$	g_1^s	g_2^s
H	h^r	$=$	h_1^r	h_2^r
			p_1-subgroup	p_2-subgroup

an AH IPE in comp-order groups comp-to-prime translator

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

- orthogonal under e

$$G \qquad g^s = g_1^s \qquad g_2^s$$

$$H \qquad h^r = h_1^r \qquad h_2^r$$

p_1-subgroup p_2-subgroup

an AH IPE in comp-order groups comp-to-prime translator

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

$$\begin{array}{llll} G & g^s & = & g_1^s \quad g_2^s \\ H & h^r & = & h_1^r \quad h_2^r \end{array}$$

p_1-subgroup p_2-subgroup

- orthogonal under e
- non-degenerate under e

an AH IPE in comp-order groups comp-to-prime translator

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

G	g^s	$\equiv$	g_1^s	g_2^σ
H	h^r	$\equiv$	h_1^r	h_2^γ
			p_1-subgroup	p_2-subgroup

- orthogonal under e
- non-degenerate under e
- parameter-hiding

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

$ct_{\mathbf{x}}$ $\quad g^s = g_1^s \quad g_2^{\sigma}$

$sk_{\mathbf{y}}$ $\quad h^r = h_1^r \quad h_2^{\gamma}$

p_1-subgroup p_2-subgroup

- orthogonal under e
- non-degenerate under e
- parameter-hiding

an AH IPE in comp-order groups   comp-to-prime translator

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

$$ct_{\mathbf{x}} \quad g^s = \boxed{g_1^s} \ \boxed{g_2^{\sigma}}$$

$$sk_{\mathbf{y}} \quad h^r = \boxed{h_1^r} \ \boxed{h_2^{\gamma}}$$

p_1-subgroup p_2-subgroup

independence

- orthogonal under e
- non-degenerate under e
- parameter-hiding

an AH IPE in comp-order groups   comp-to-prime translator

technique

$$\mathcal{G} = (N = p_1 p_2,\ G,\ H,\ G_T,\ e: G \times H \to G_T).$$

$$ct_{\mathbf{x}} \quad g^s = \boxed{g_1^s} \; \boxed{g_2^s}$$

$$sk_{\mathbf{y}} \quad h^r = \boxed{h_1^r} \; \boxed{h_2^r}$$

p_1-subgroup p_2-subgroup

independence

- orthogonal under e
- non-degenerate under e
- parameter-hiding

technique

$$\mathcal{G} = (\, N = p_1 p_2,\ G,\ H,\ G_T,\ e\colon G \times H \to G_T).$$

$ct_{\mathbf{x}}$ $\quad g^s = \boxed{g_1^s} \approx \boxed{g_2^s}$

$sk_{\mathbf{y}}$ $\quad h^r = \boxed{h_1^r} \quad \boxed{h_2^r}$

p_1-subgroup p_2-subgroup

independence

- orthogonal under e
- non-degenerate under e
- parameter-hiding

connection

- subgroup-hiding

an AH IPE in **comp-order groups** comp-to-prime translator

technique

$$\mathcal{G} = (N = p_1 p_2,\ G,\ H,\ G_T,\ e: G \times H \to G_T).$$

$ct_{\mathbf{x}}$ $\quad g^s = g_1^s \approx g_2^s$

$sk_{\mathbf{y}}$ $\quad h^r = h_1^r \quad h_2^r$

p_1-subgroup p_2-subgroup

⚠ h_1^r and h_2^r cannot be given individually

independence

- orthogonal under e
- non-degenerate under e
- parameter-hiding

connection

- subgroup-hiding

an AH IPE in comp-order groups comp-to-prime translator

technique

$ct_{\mathbf{x}}$

$sk_{\mathbf{y}}$

an AH IPE in comp-order groups   comp-to-prime translator

technique

$mpk \quad g\ , g^{u}, g^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g^{s}, g^{s(\mathbf{w}+u\cdot\mathbf{x})}, e(g,h)^{\alpha s}\cdot m$

$sk_{\mathbf{y}} \quad h^{r}, h^{r\langle\mathbf{w},\mathbf{y}\rangle+\alpha}$

an AH IPE in comp-order groups comp-to-prime translator

technique

$mpk \quad g\ , g^u, g^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g^s, g^{s(\mathbf{w}+u\cdot\mathbf{x})}, e(g,h)^{\alpha s}\cdot m \longrightarrow$ *weakly* attribute-hiding IPE in prime-order bilinear group

[Chen-Gay-Wee @ EC'15]

$sk_{\mathbf{y}} \quad h^r, h^{r\langle\mathbf{w},\mathbf{y}\rangle+\alpha}$

an AH IPE in comp-order groups   comp-to-prime translator

technique

$mpk \quad g\ , g^{u}, g^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g^{s}, g^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}} \quad h^{r}, h^{r\langle\mathbf{w},\mathbf{y}\rangle}$

an AH IPE in comp-order groups   comp-to-prime translator   # technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct_{\mathbf{x}}$	$g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$			
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$			$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}\rangle}$

an AH IPE in comp-order groups   comp-to-prime translator   # technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$	$g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$			
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$			$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}\rangle}$

Goal : to prove $ct^*_{\mathbf{x}_b} \approx ct^*_{\mathbf{x}_0}$ if $\langle\mathbf{x}_0,\mathbf{y}\rangle \neq 0 \neq \langle\mathbf{x}_1,\mathbf{y}\rangle$ or

$\langle\mathbf{x}_0,\mathbf{y}\rangle = 0 = \langle\mathbf{x}_1,\mathbf{y}\rangle$

an AH IPE in comp-order groups   comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$			$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}\rangle}$

subgroup hiding: $g_1^s \approx g_2^s \cdot g_3^s \cdot g_4^s$

an AH IPE in comp-order groups comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}\rangle}$		

subgroup hiding: $h_4^r \approx h_2^r$

technique

an AH IPE in comp-order groups   comp-to-prime translator

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}\rangle}$		

parameter-hiding

technique

an AH IPE in comp-order groups

comp-to-prime translator

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\underline{\mathbf{w}+u\cdot\mathbf{x}_0})}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$	$h_2^r, h_2^{r\underline{\langle\mathbf{w},\mathbf{y}\rangle}}$		

parameter-hiding

+

statistical argument [Wee @ TCC’17]

an AH IPE in comp-order groups comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}\rangle}$		

an AH IPE in comp-order groups

comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$			$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$

technique

an AH IPE in comp-order groups   comp-to-prime translator

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$		$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$

technique

an AH IPE in comp-order groups   comp-to-prime translator

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$			$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$

an AH IPE in comp-order groups comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$			$h_4^r, h_4^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$

an AH IPE in comp-order groups comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$		$h_3^r, h_3^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$	

an AH IPE in comp-order groups   comp-to-prime translator   **technique**

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$		$h_3^r, h_3^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$	

an AH IPE in comp-order groups comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$		

an AH IPE in comp-order groups comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$		

an AH IPE in comp-order groups   comp-to-prime translator

technique

	p_1-subgroup	p_2-subgroup	p_3-subgroup	p_4-subgroup
mpk	$g_1, g_1^u, g_1^{\mathbf{w}}$			
$ct^*_{\mathbf{x}_b}$		$g_2^s, g_2^{s(\mathbf{w}+u\cdot\mathbf{x}_0)}$	$g_3^s, g_3^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$	$g_4^s, g_4^{s(\mathbf{w}+u\cdot\mathbf{x}_b)}$
$sk_{\mathbf{y}_1}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_1\rangle}$		
$sk_{\mathbf{y}_2}$	$h_1^r, h_1^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$	$h_2^r, h_2^{r\langle\mathbf{w},\mathbf{y}_2\rangle}$		

[Okamoto-Takashima @ EC'12]

an AH IPE in comp-order groups comp-to-prime translator

technique

$mpk \quad g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

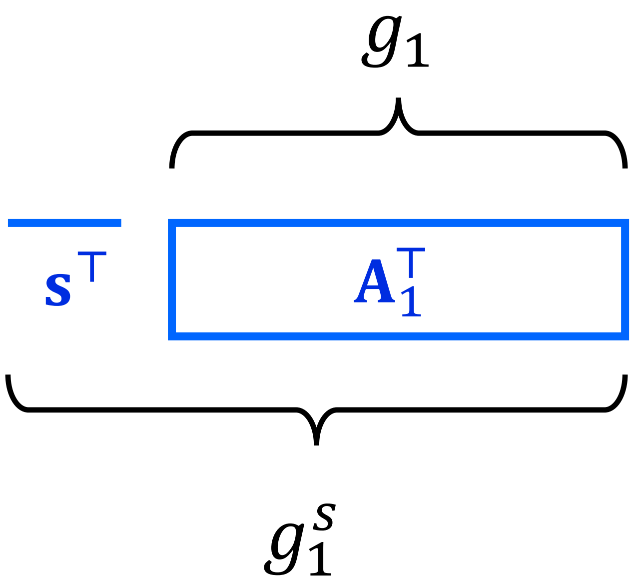
$sk_{\mathbf{y}} \quad h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$

an AH IPE in comp-order groups comp-to-prime translator **technique**

mpk $\quad g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $\quad g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}}$ $\quad h_{14}^r, h_{14}^{r\langle \mathbf{w},\mathbf{y}\rangle}$



technique

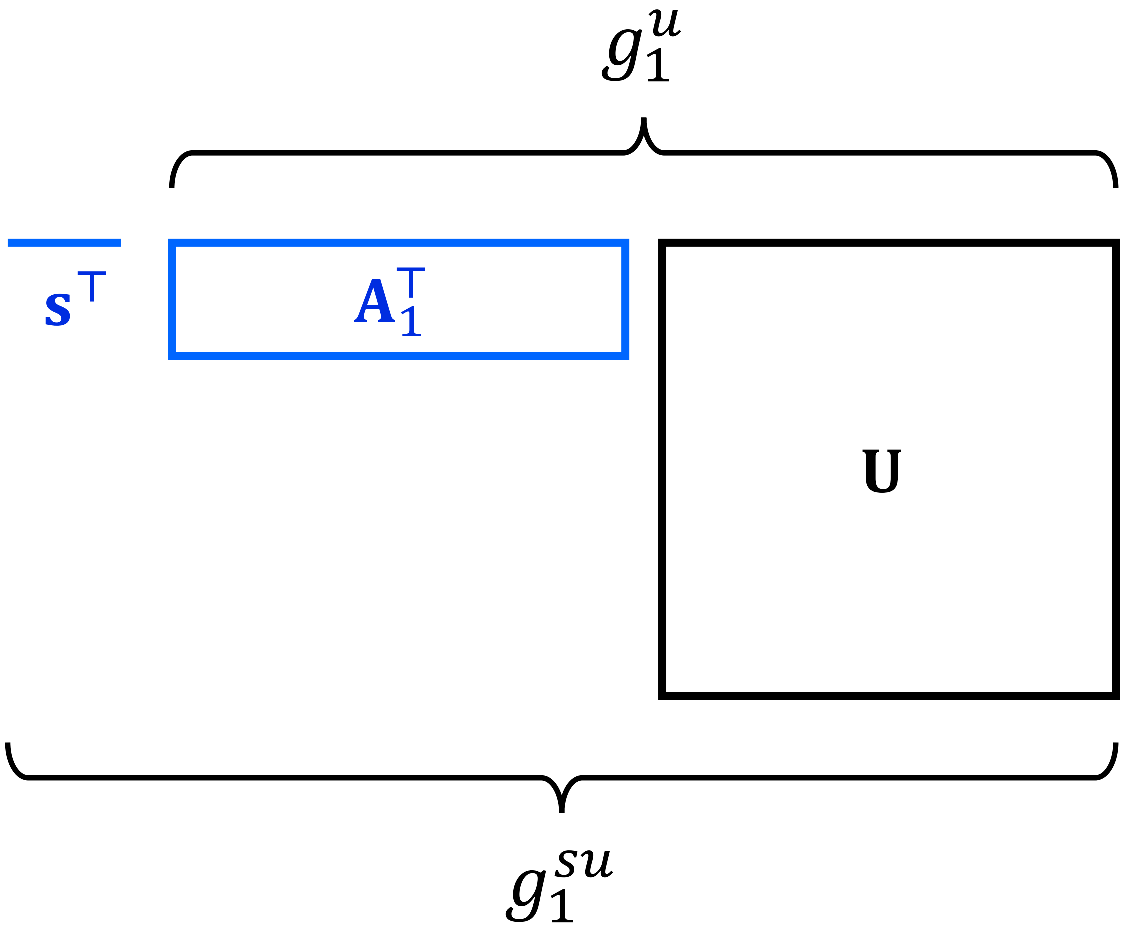
an AH IPE in comp-order groups

comp-to-prime translator

mpk $\quad g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $\quad g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}}$ $\quad h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



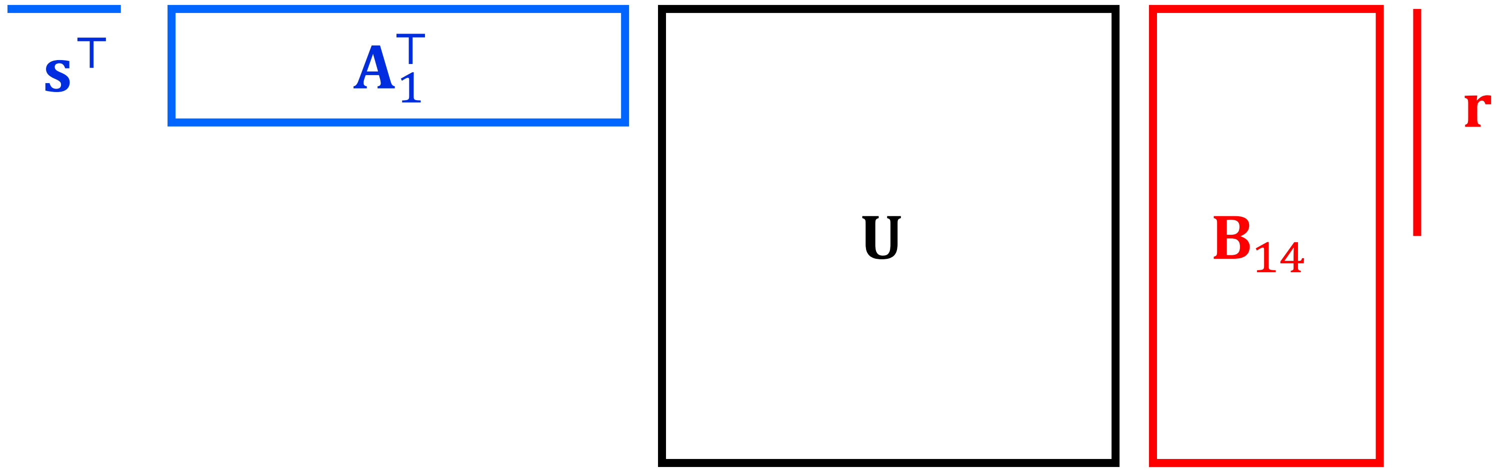
an AH IPE in comp-order groups   comp-to-prime translator

technique

$mpk \quad g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}} \quad h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



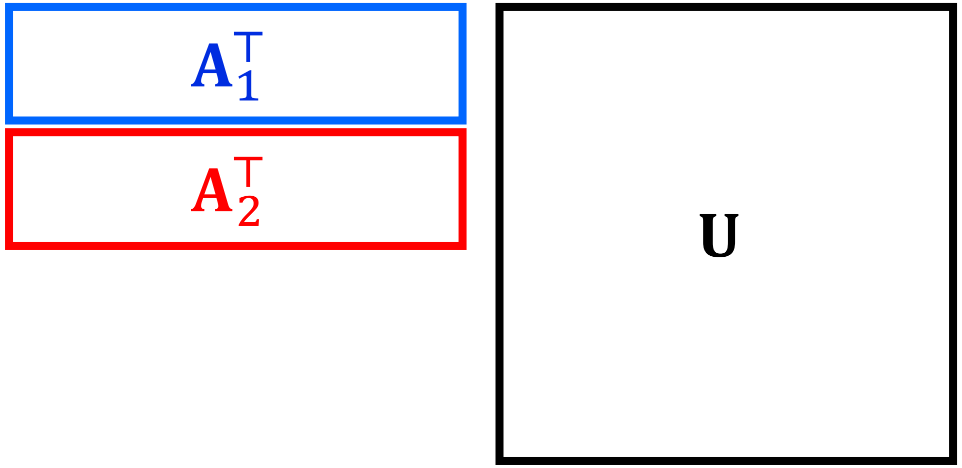
an AH IPE in comp-order groups   comp-to-prime translator

technique

$mpk \quad g_1, g_1^{u}, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g_1^{s}, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}} \quad h_{14}^{r}, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



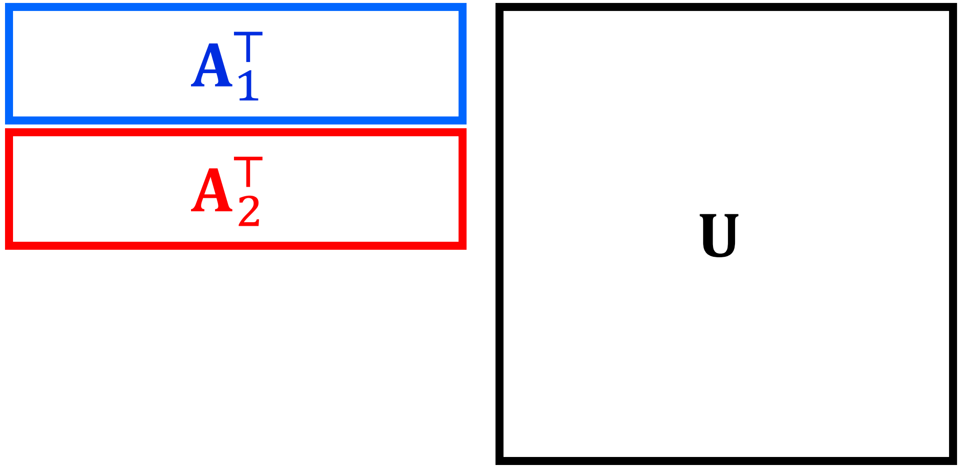
an AH IPE in comp-order groups   comp-to-prime translator

technique

mpk $g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}}$ $h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



subgroup hiding : $g_1^s \approx g_2^s$

↓

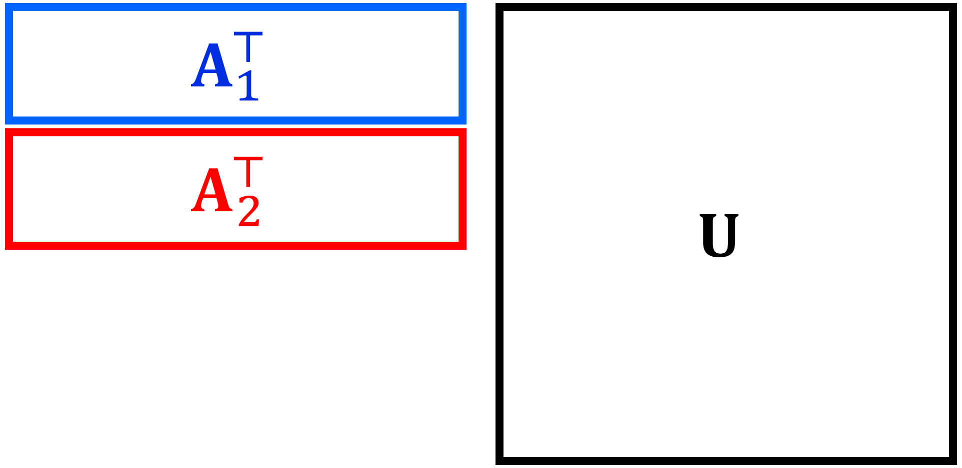
subspace hiding : $\mathrm{span}(\mathbf{A}_1) \approx \mathrm{span}(\mathbf{A}_2)$

technique

$mpk \quad g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}} \quad h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



k-Lin

subgroup hiding : $\quad g_1^s \approx g_2^s$

↓

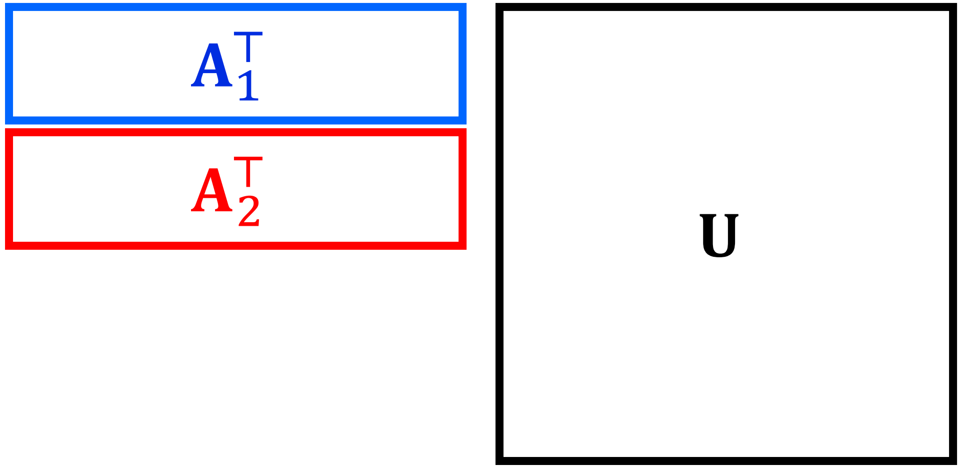
subspace hiding : $\quad \mathrm{span}(\mathbf{A}_1) \approx \mathrm{span}(\mathbf{A}_2)$

an AH IPE in comp-order groups   comp-to-prime translator   technique

$mpk \quad g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}} \quad g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}} \quad h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



k-Lin

an AH IPE in comp-order groups comp-to-prime translator

technique

mpk $g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}}$ $h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$

$\mathbf{A}_1^\top$

$\mathbf{A}_2^\top$

$\mathbf{U}$

k-Lin

$\mathbf{A}_1^\top\mathbf{U}$ and $\mathbf{A}_2^\top\mathbf{U}$ are independent

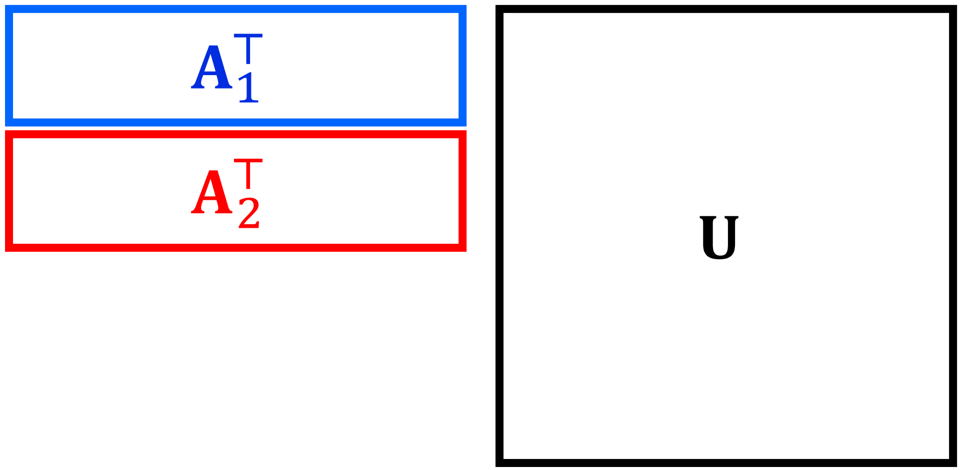
an AH IPE in comp-order groups   comp-to-prime translator

technique

mpk $\quad g_1, g_1^{u}, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $\quad g_1^{s}, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}}$ $\quad h_{14}^{r}, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$



k-Lin

parameter hiding : $\mathbf{A}_1^{\top}\mathbf{U}$ and $\mathbf{A}_2^{\top}\mathbf{U}$ are independent

technique

mpk $g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

$sk_{\mathbf{y}}$ $h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$

$\boxed{\mathbf{U}}$

k-Lin

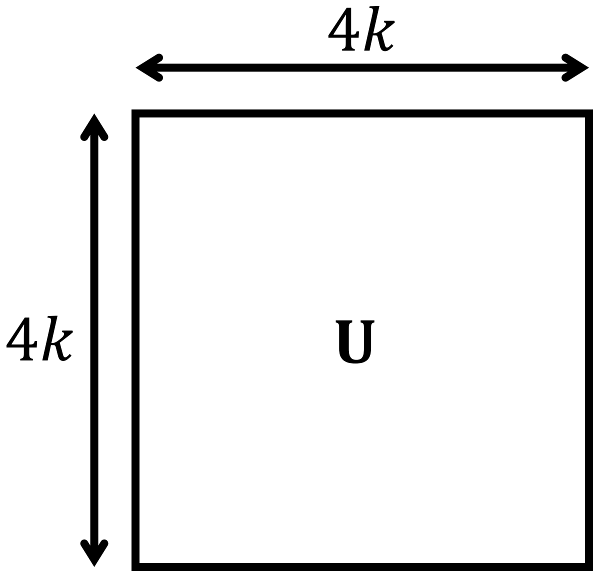
an AH IPE in comp-order groups   comp-to-prime translator

technique

mpk $g_1, g_1^u, g_1^{\mathbf{w}}$

$ct_{\mathbf{x}}$ $g_1^s, g_1^{s(\mathbf{w}+u\cdot\mathbf{x})}$

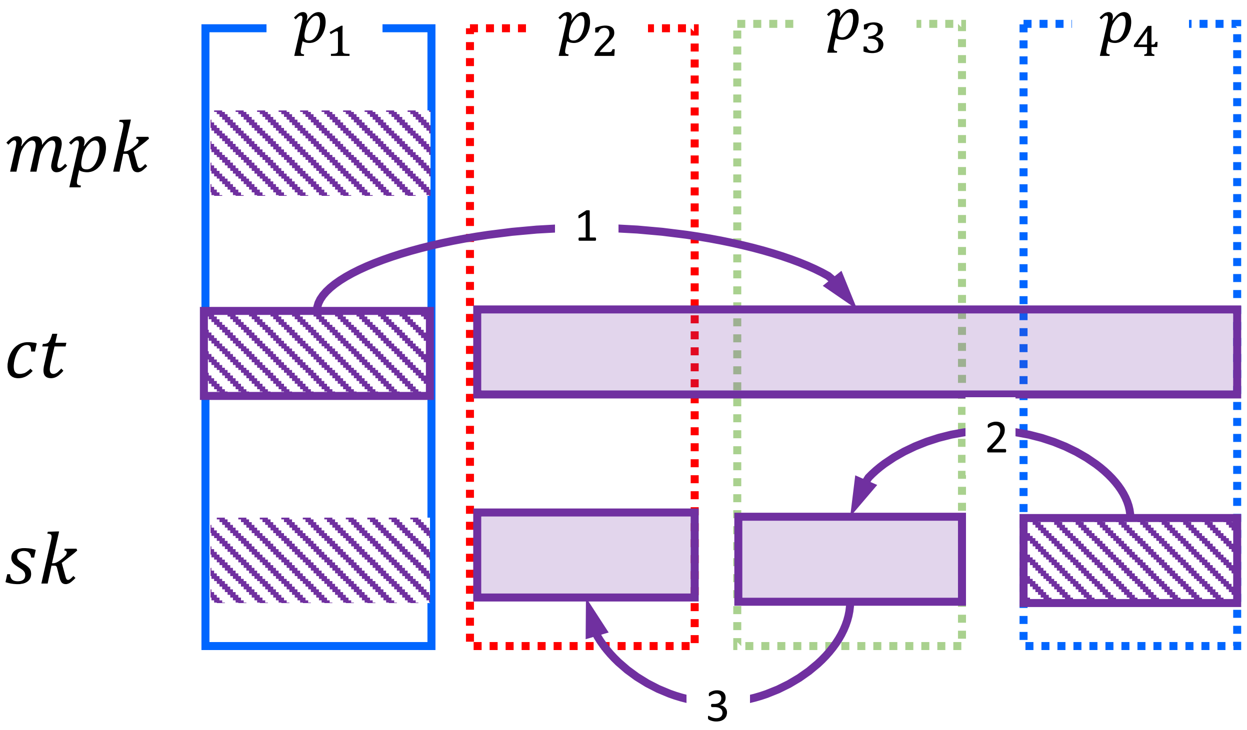
$sk_{\mathbf{y}}$ $h_{14}^r, h_{14}^{r\langle\mathbf{w},\mathbf{y}\rangle}$

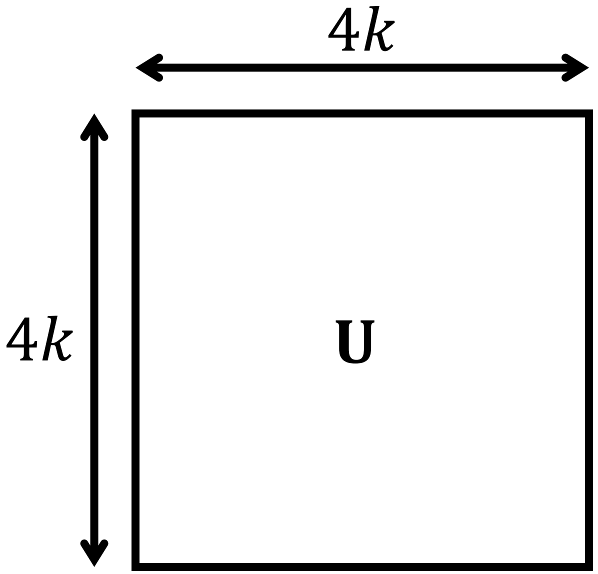


k-Lin

an AH IPE in comp-order groups   comp-to-prime translator

technique



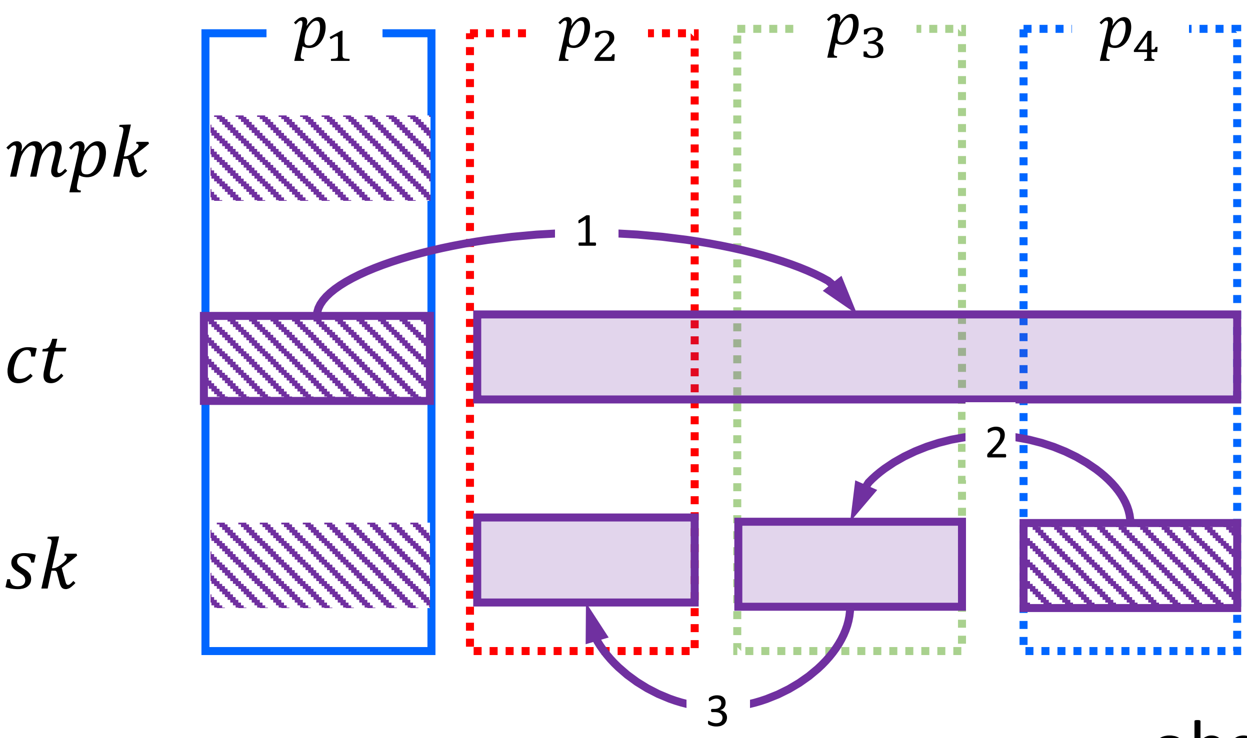


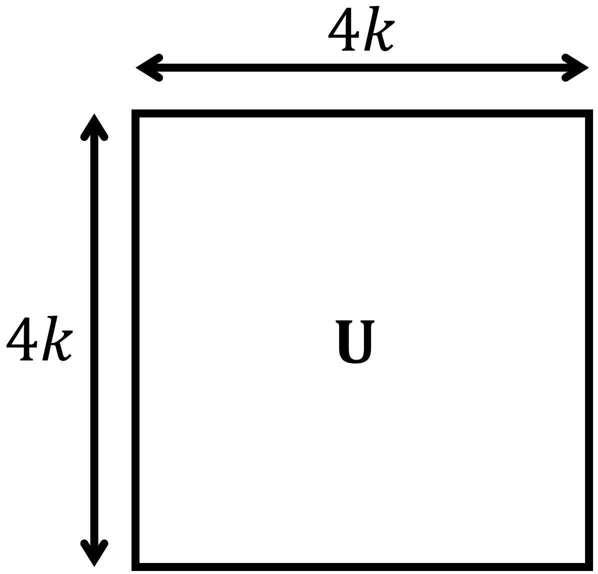
k-Lin

an AH IPE in comp-order groups

comp-to-prime translator

technique





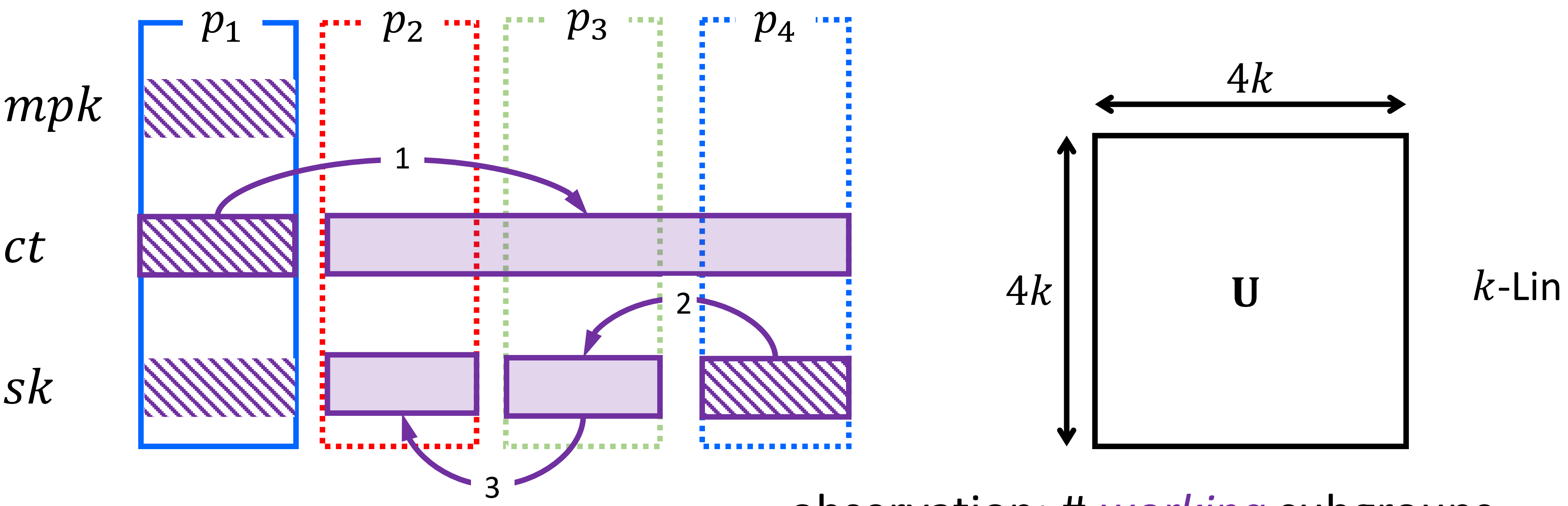
k-Lin

observation: # *working* subgroups

an AH IPE in comp-order groups

comp-to-prime translator

technique

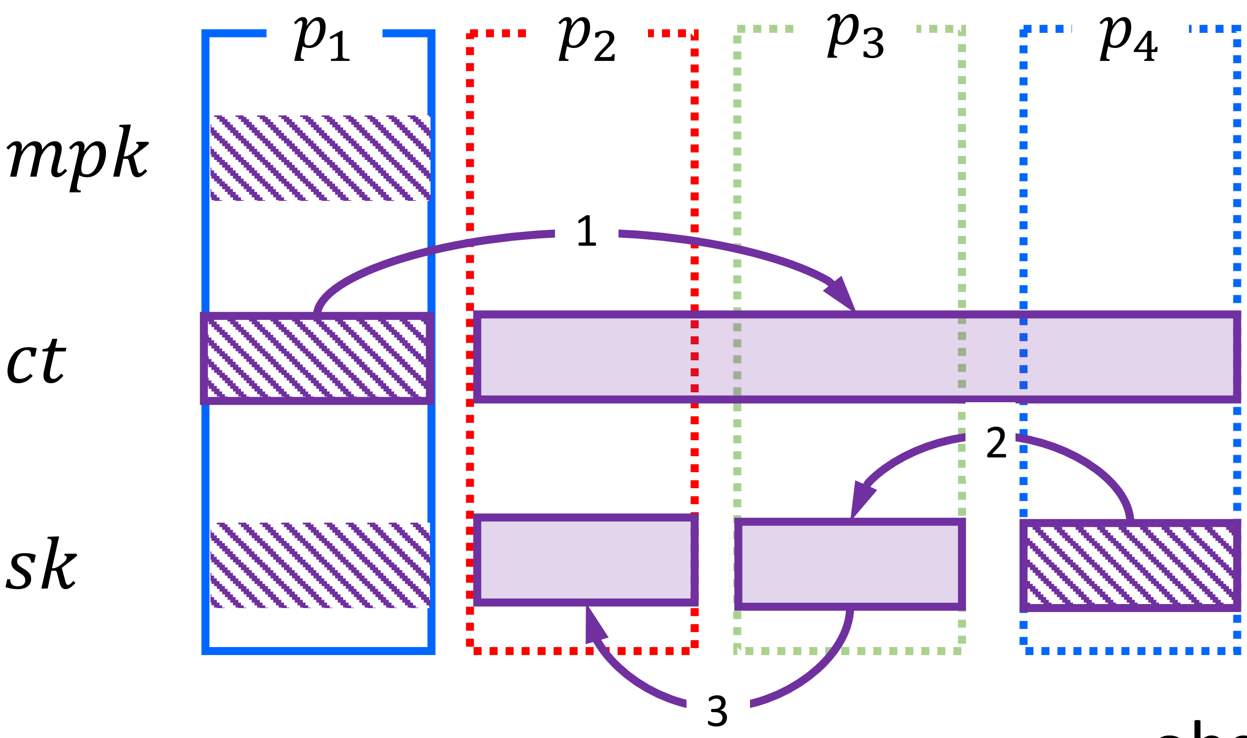


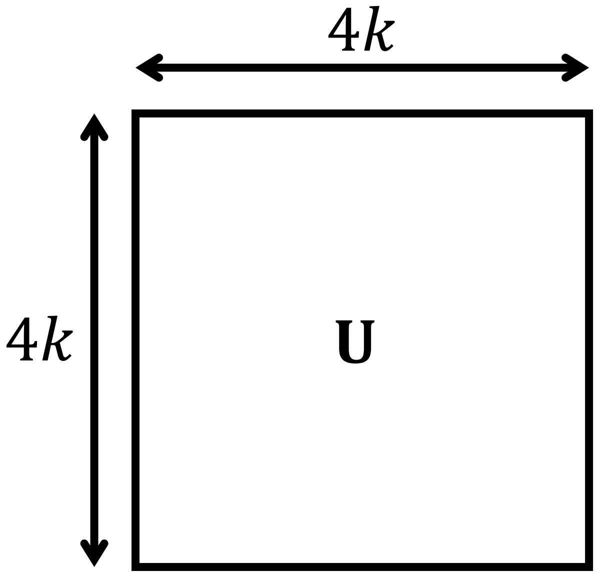
observation: # *working* subgroups

2 subgroups on ct (G_{p_1} & $G_{p_2p_3p_4}$) ;

an AH IPE in comp-order groups comp-to-prime translator

technique





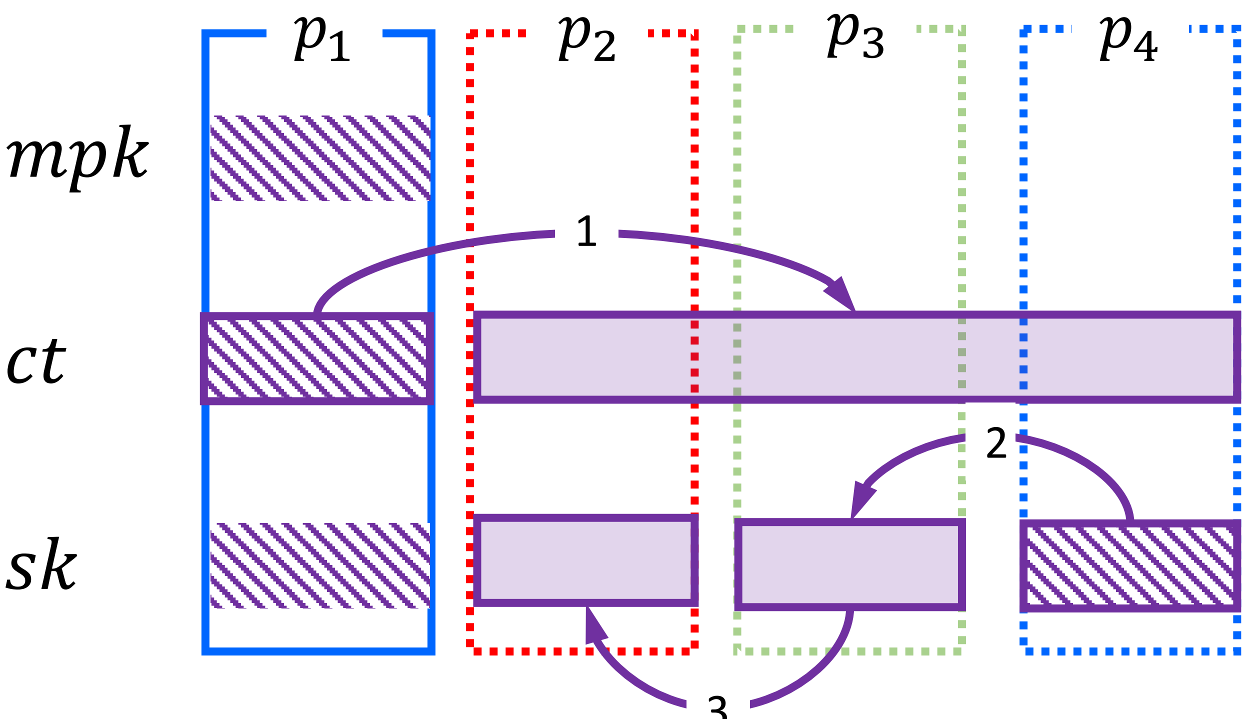
k-Lin

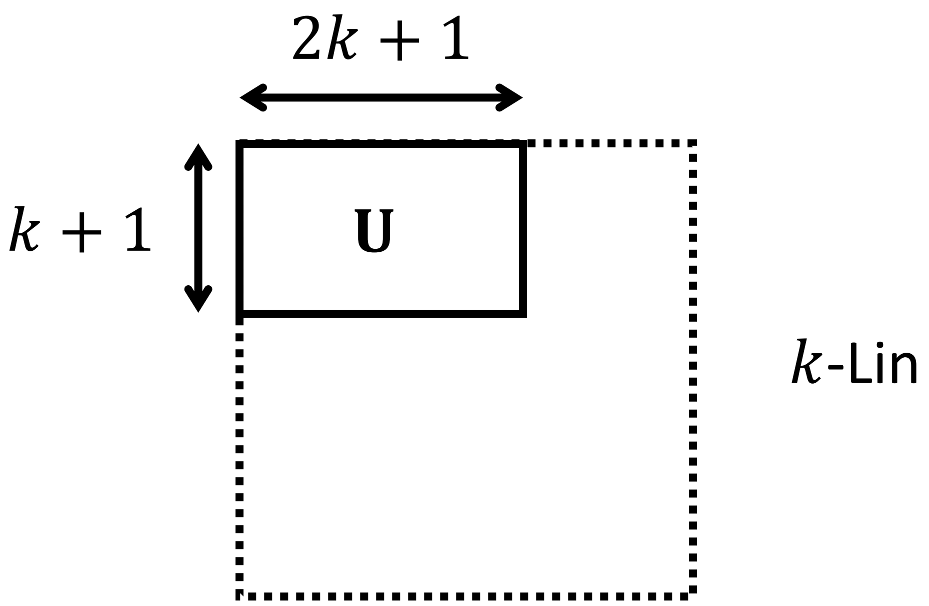
observation: # *working* subgroups

2 subgroups on ct (G_{p_1} & $G_{p_2p_3p_4}$) ; 3 subgroups on sk (H_{p_2}, H_{p_3} & H_{p_4})

an AH IPE in comp-order groups   comp-to-prime translator

technique





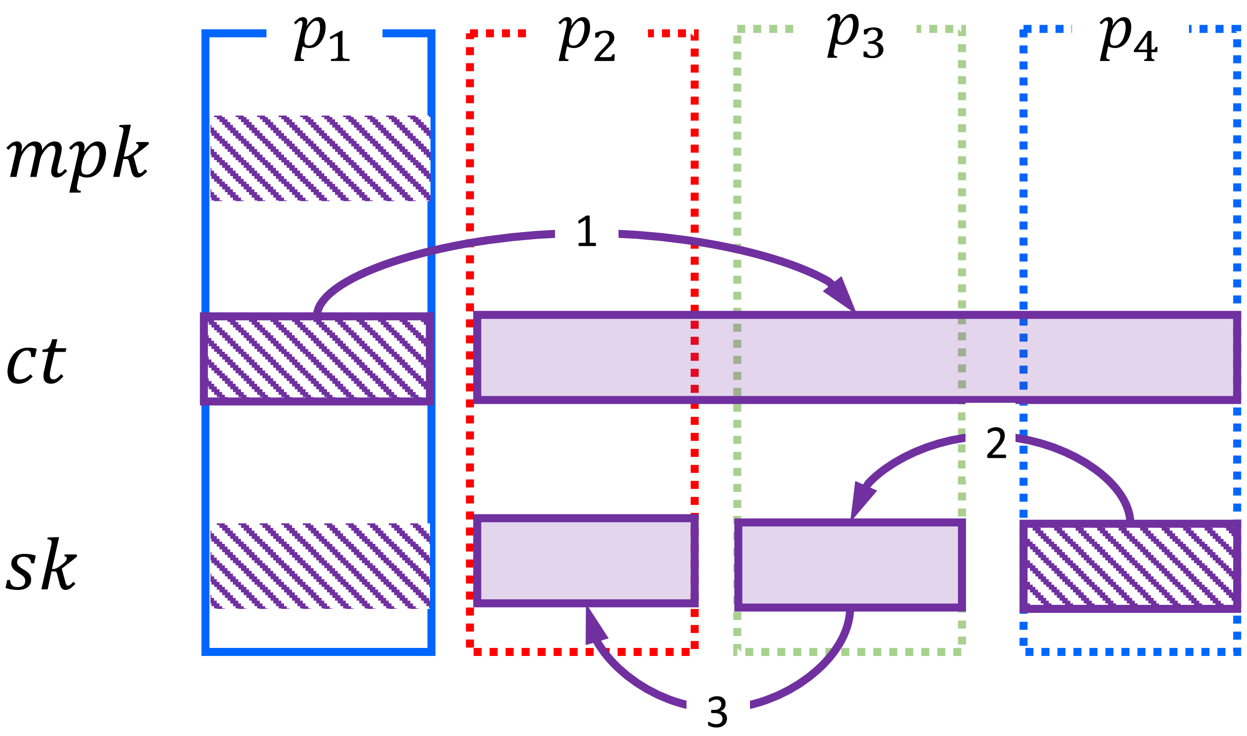
observation: # *working* subgroups

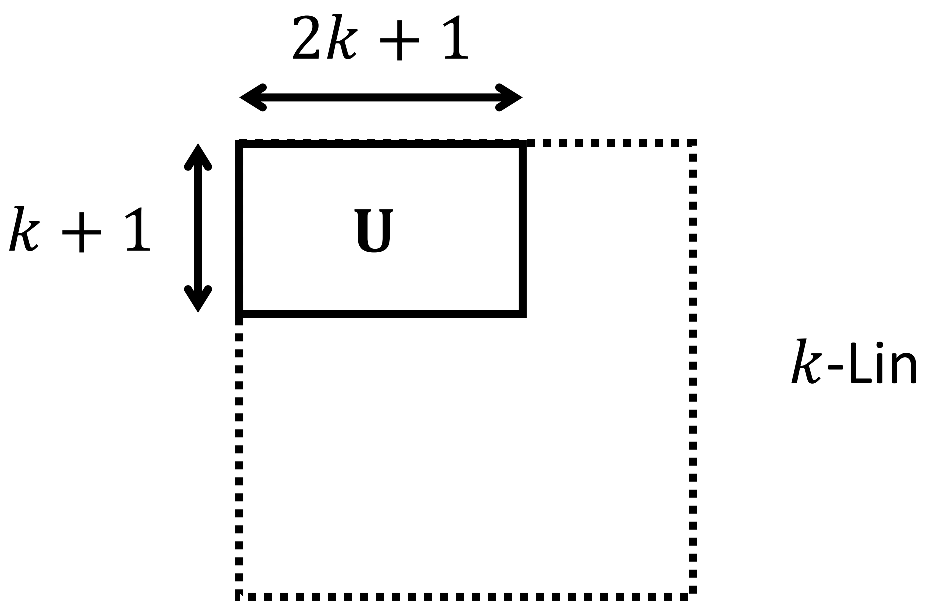
2 subgroups on ct (G_{p_1} & $G_{p_2p_3p_4}$) ; 3 subgroups on sk (H_{p_2}, H_{p_3} & H_{p_4})

an AH IPE in comp-order groups

comp-to-prime translator

technique



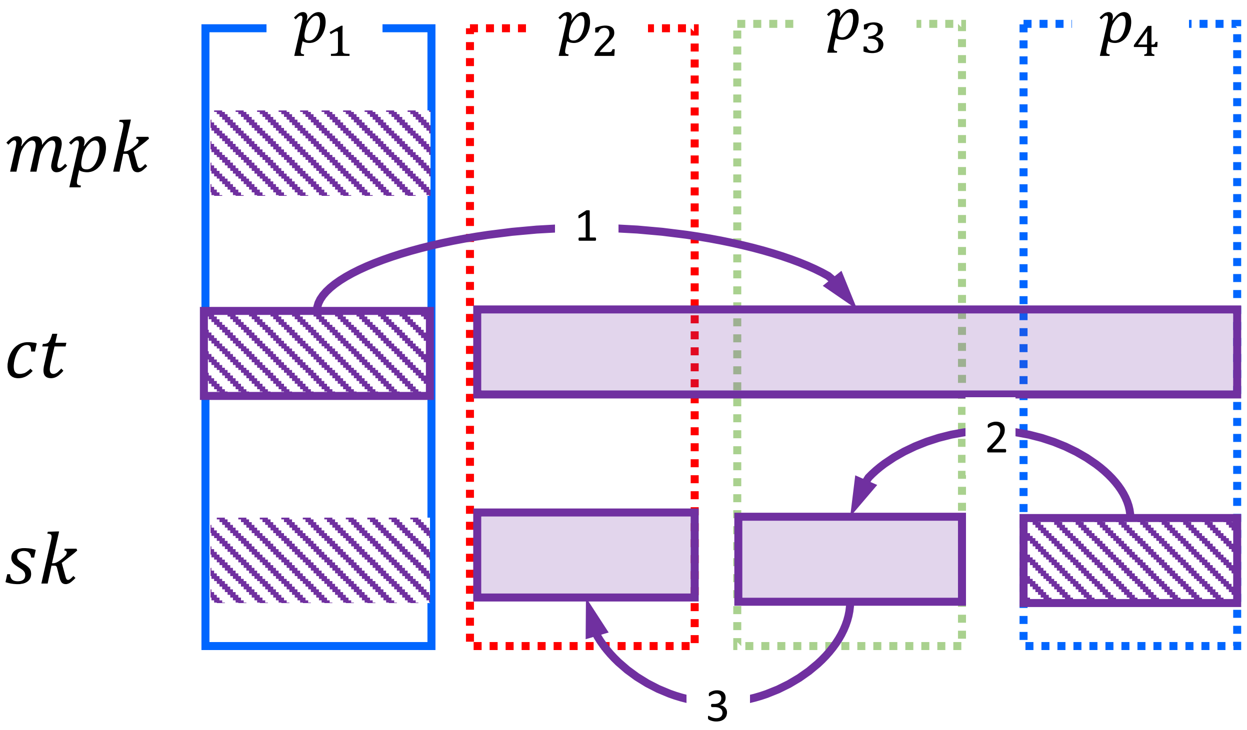


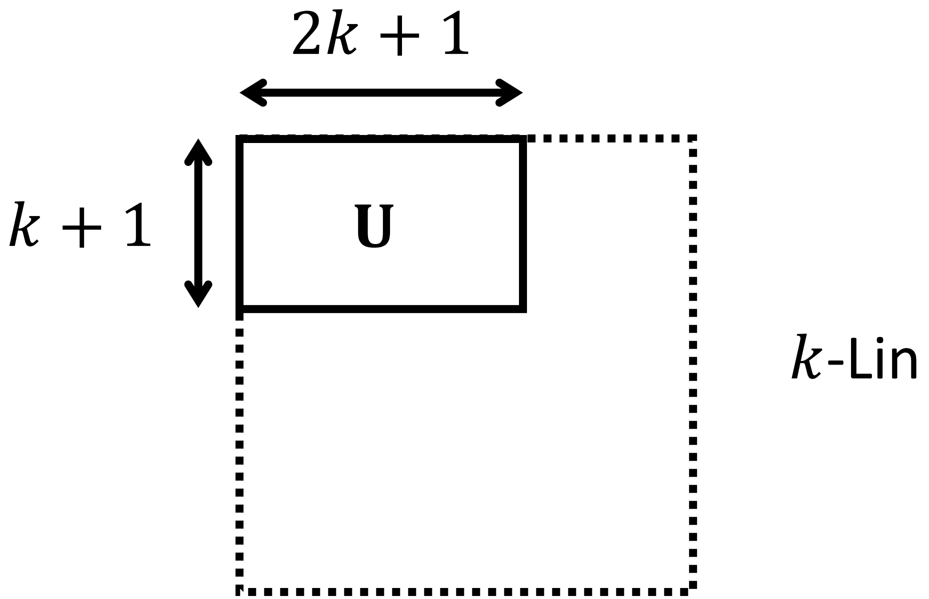
formal treatment

an AH IPE in comp-order groups

comp-to-prime translator

technique





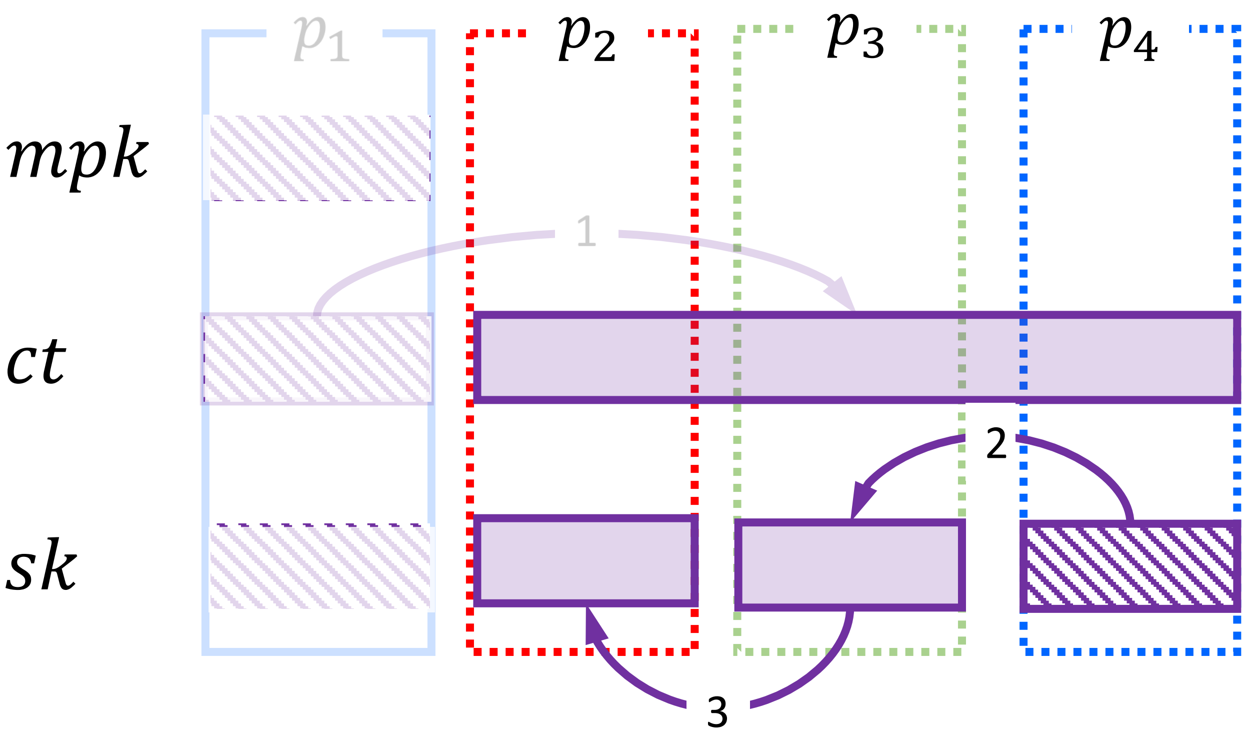
formal treatment

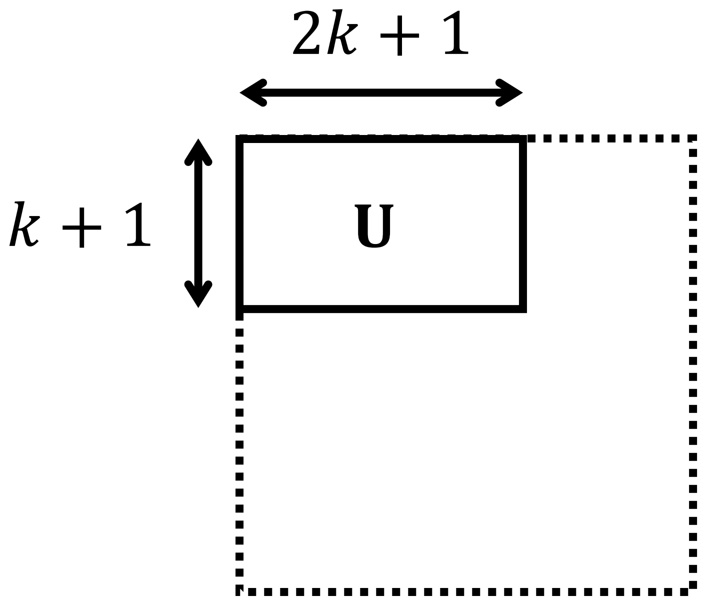
private-key IPE

an AH IPE in comp-order groups

comp-to-prime translator

technique





k-Lin

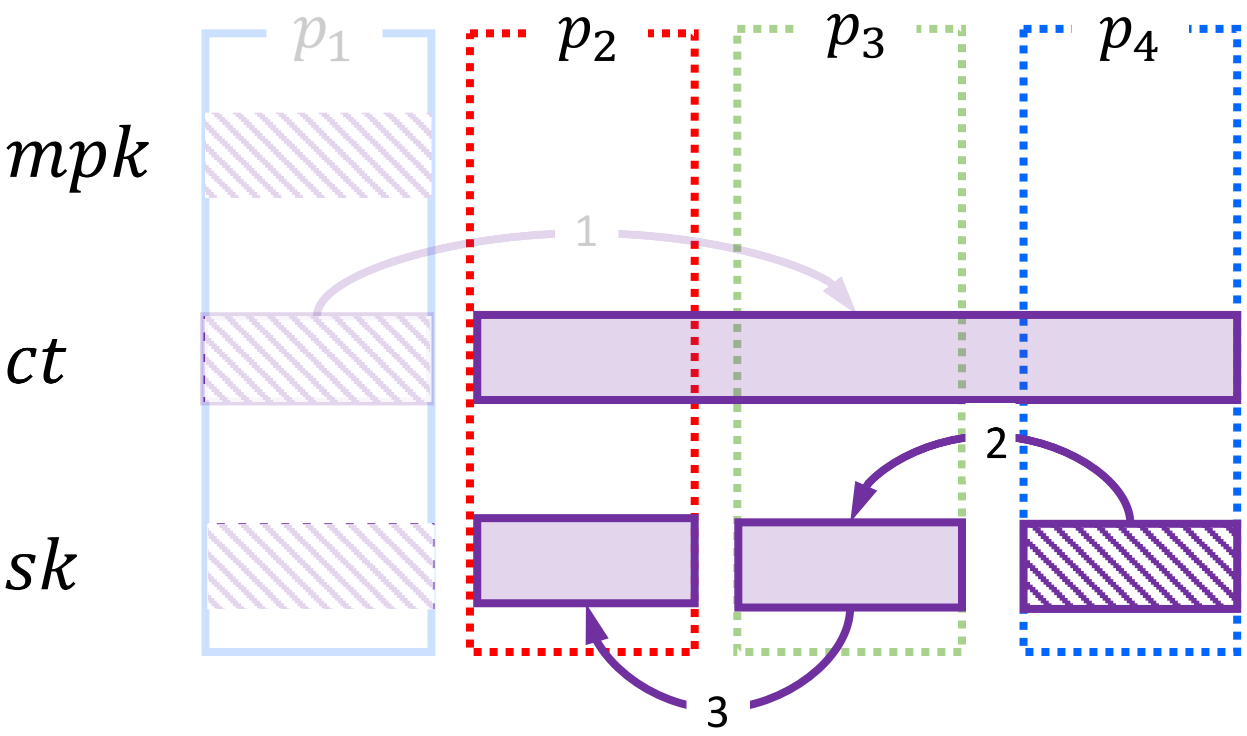
formal treatment

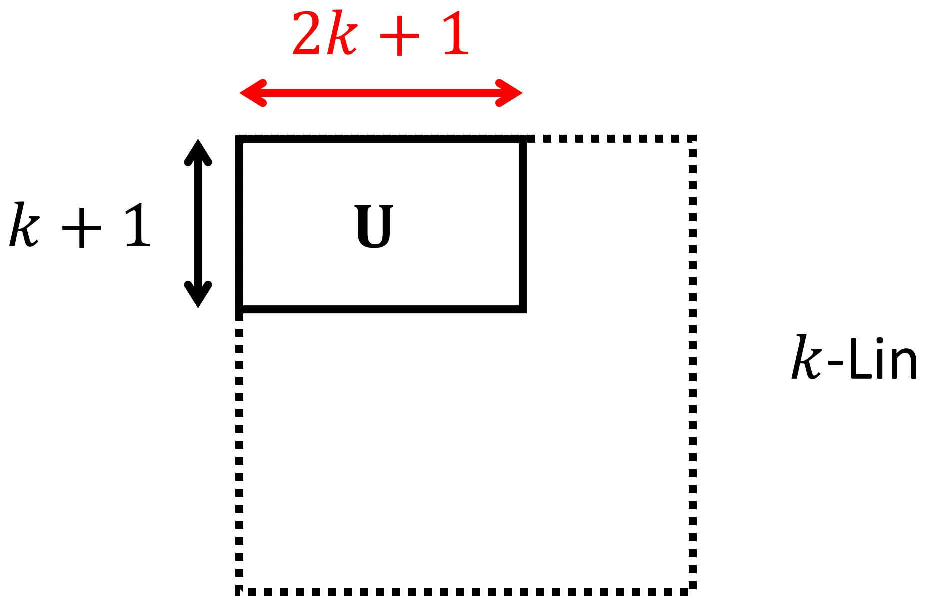
private-key IPE

an AH IPE in comp-order groups

comp-to-prime translator

technique





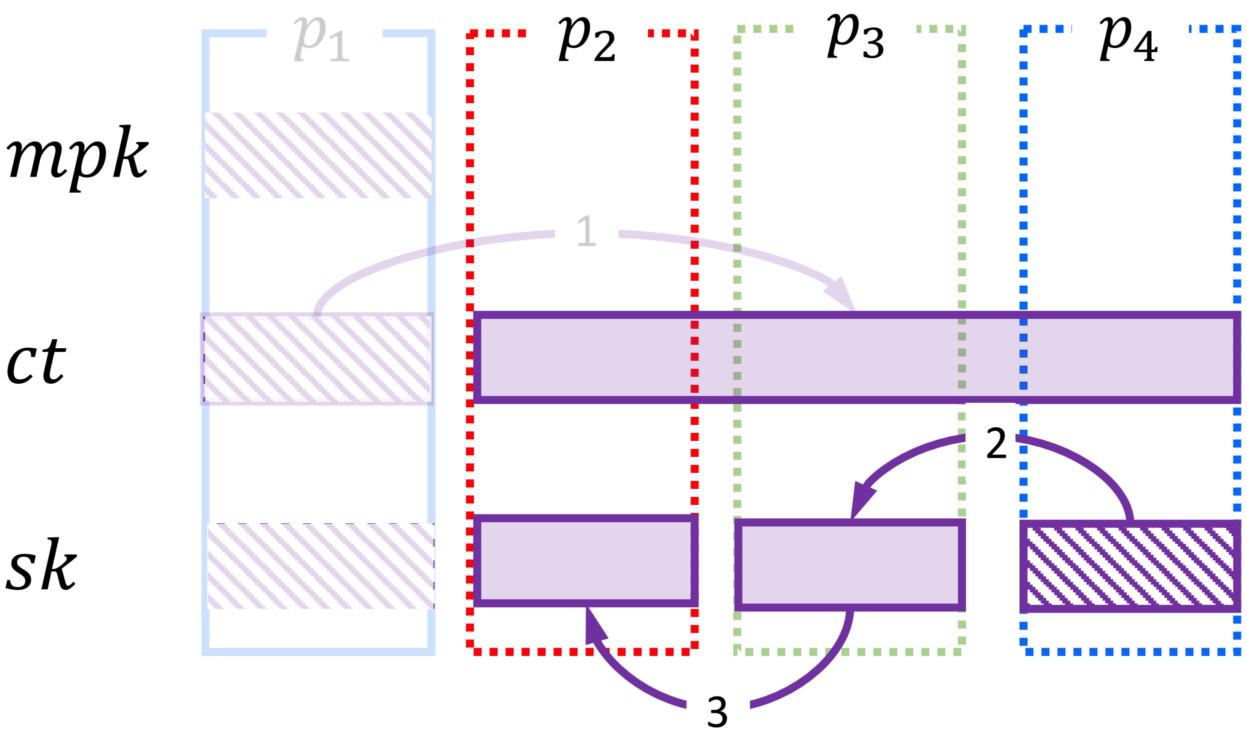
formal treatment

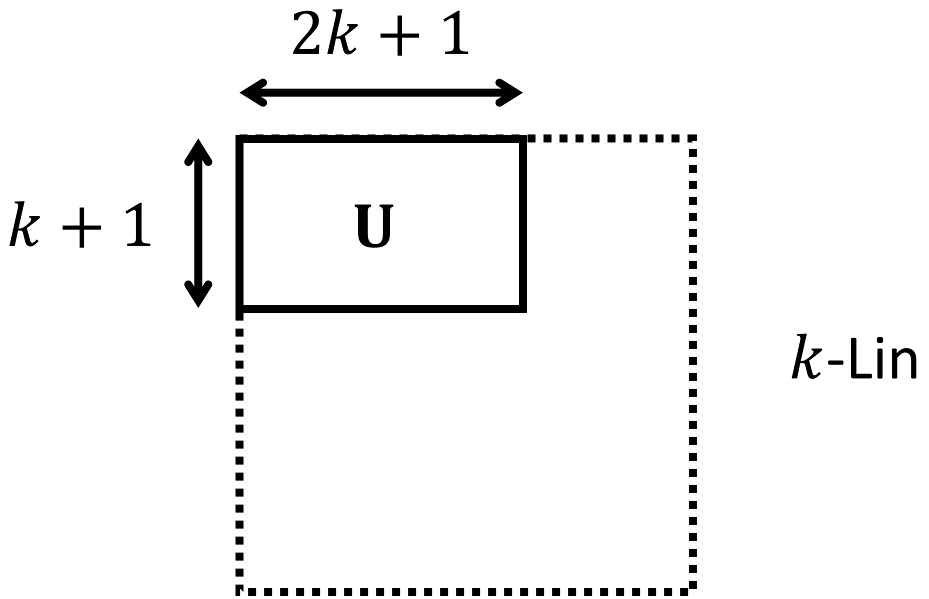
private-key IPE

[Chen-Gong-Kowalczyk-Wee @ EC'18]

an AH IPE in comp-order groups   comp-to-prime translator

technique



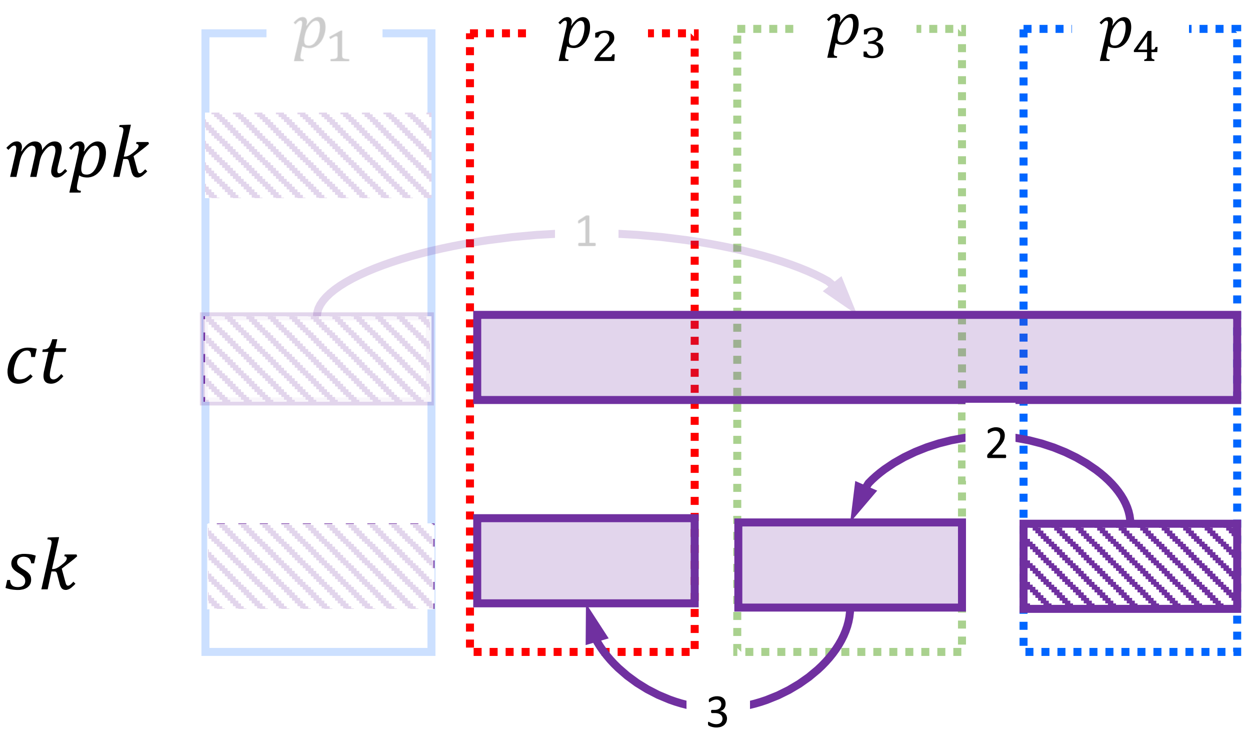


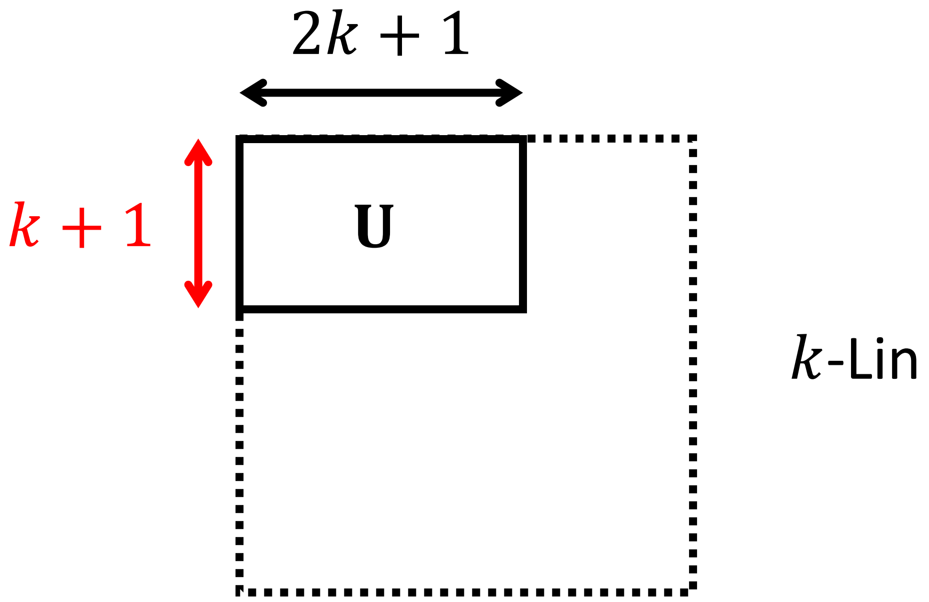
formal treatment

private-key IPE $\longrightarrow$ public-key IPE

[Chen-Gong-Kowalczyk-Wee @ EC'18]

an AH IPE in comp-order groups   comp-to-prime translator   technique





formal treatment

[Wee @ TCC'17]

private-key IPE $\longrightarrow$ public-key IPE

[Chen-Gong-Kowalczyk-Wee @ EC'18]

summary

our two IPE schemes

- adaptive secure + **fully** attribute-hiding
- k-Lin based IPE
  - shorter mpk and secret keys
  - but slightly larger ciphertexts
- XDLIN based IPE
  - shorter mpk, secret keys and ciphertexts