Improved Dual System ABE in Prime-Order Groups via Predicate Encodings

Jie Chen – East China Normal University, Shanghai

Romain Gay – ENS, Paris

Hoeteck Wee – ENS, Paris

Attribute-Based Encryption

//

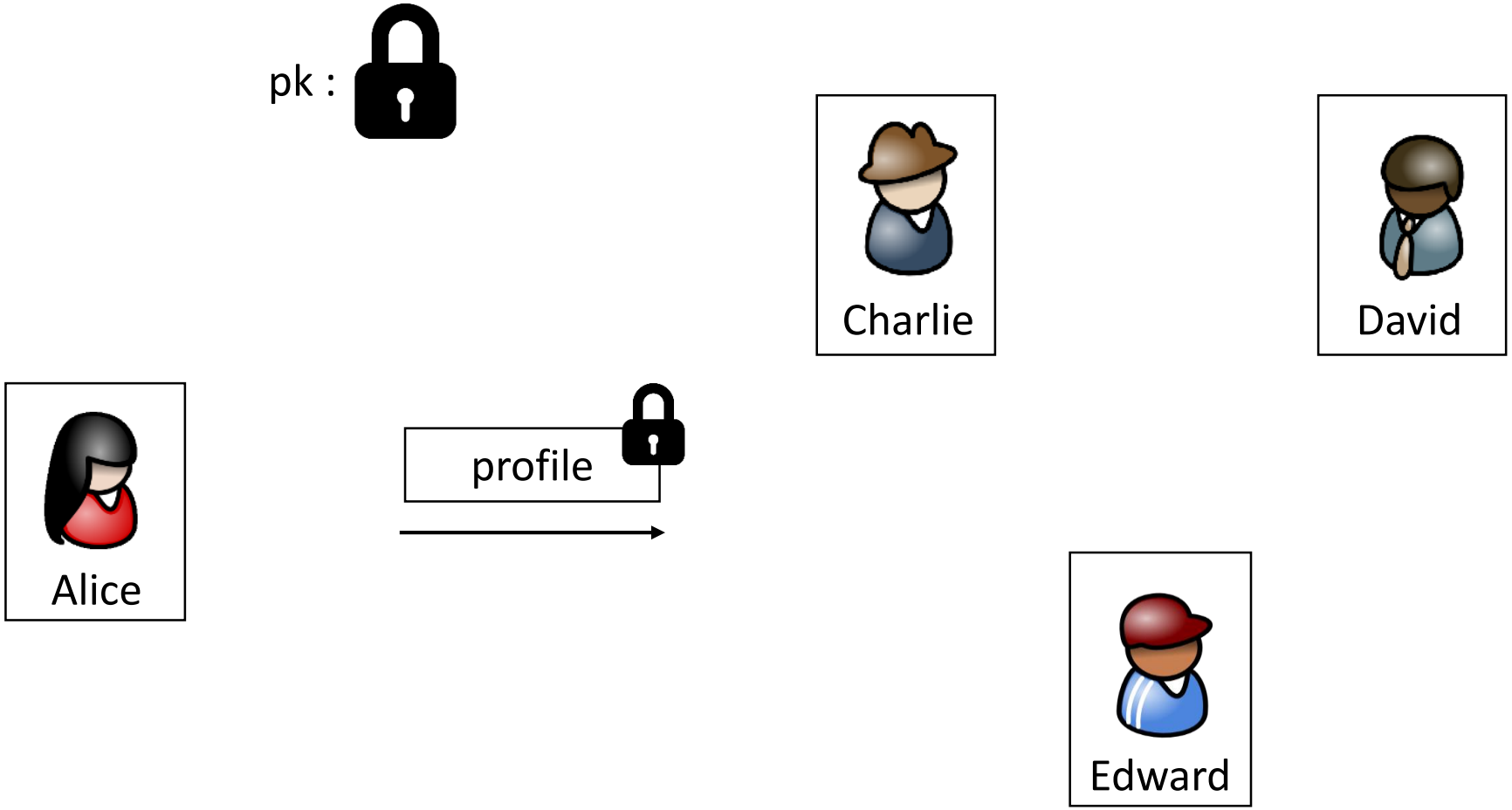
Improved Dual System ABE in Prime-Order Groups via Predicate Encodings

Jie Chen – East China Normal University, Shanghai

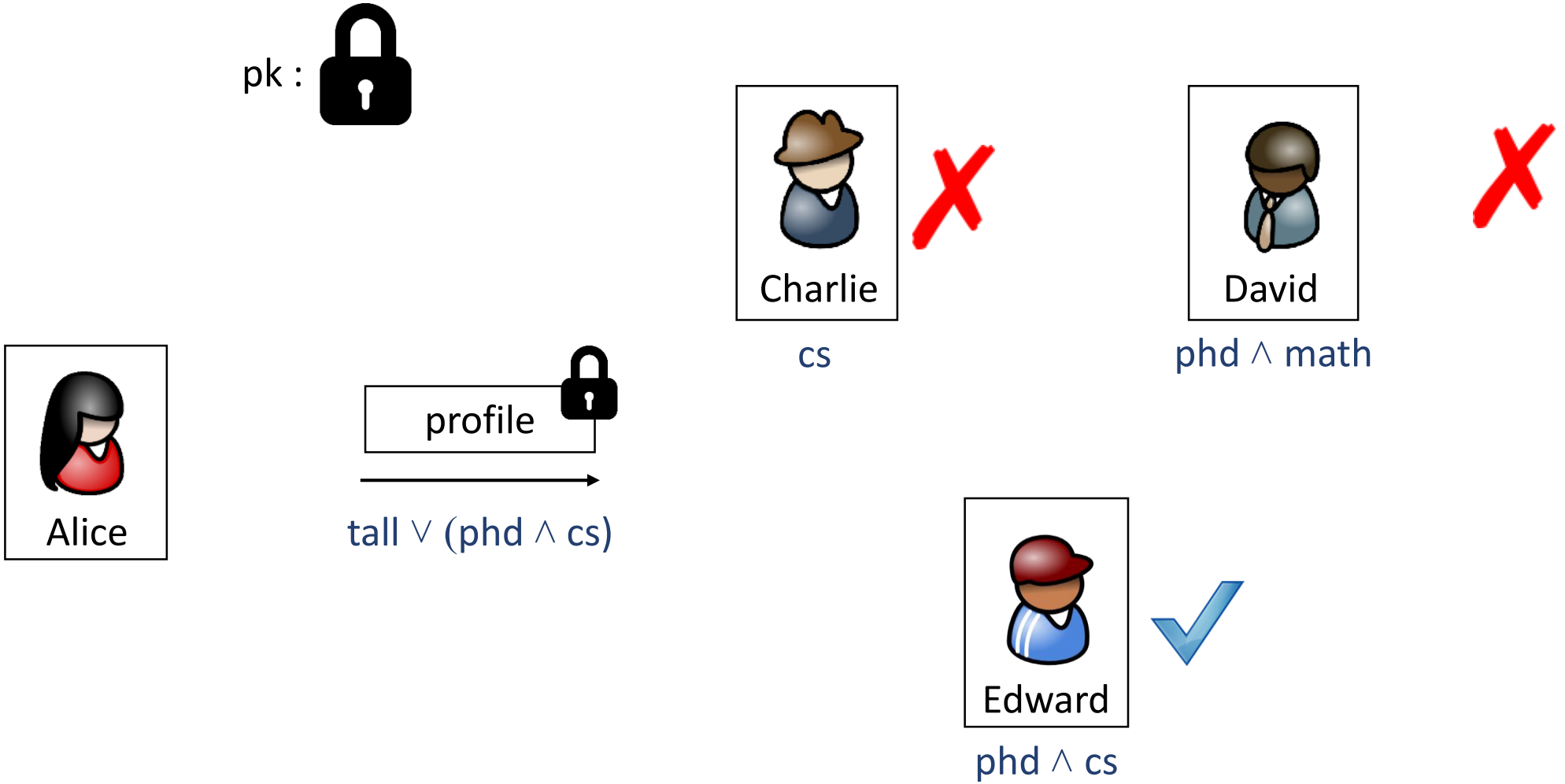
Romain Gay – ENS, Paris

Hoeteck Wee – ENS, Paris

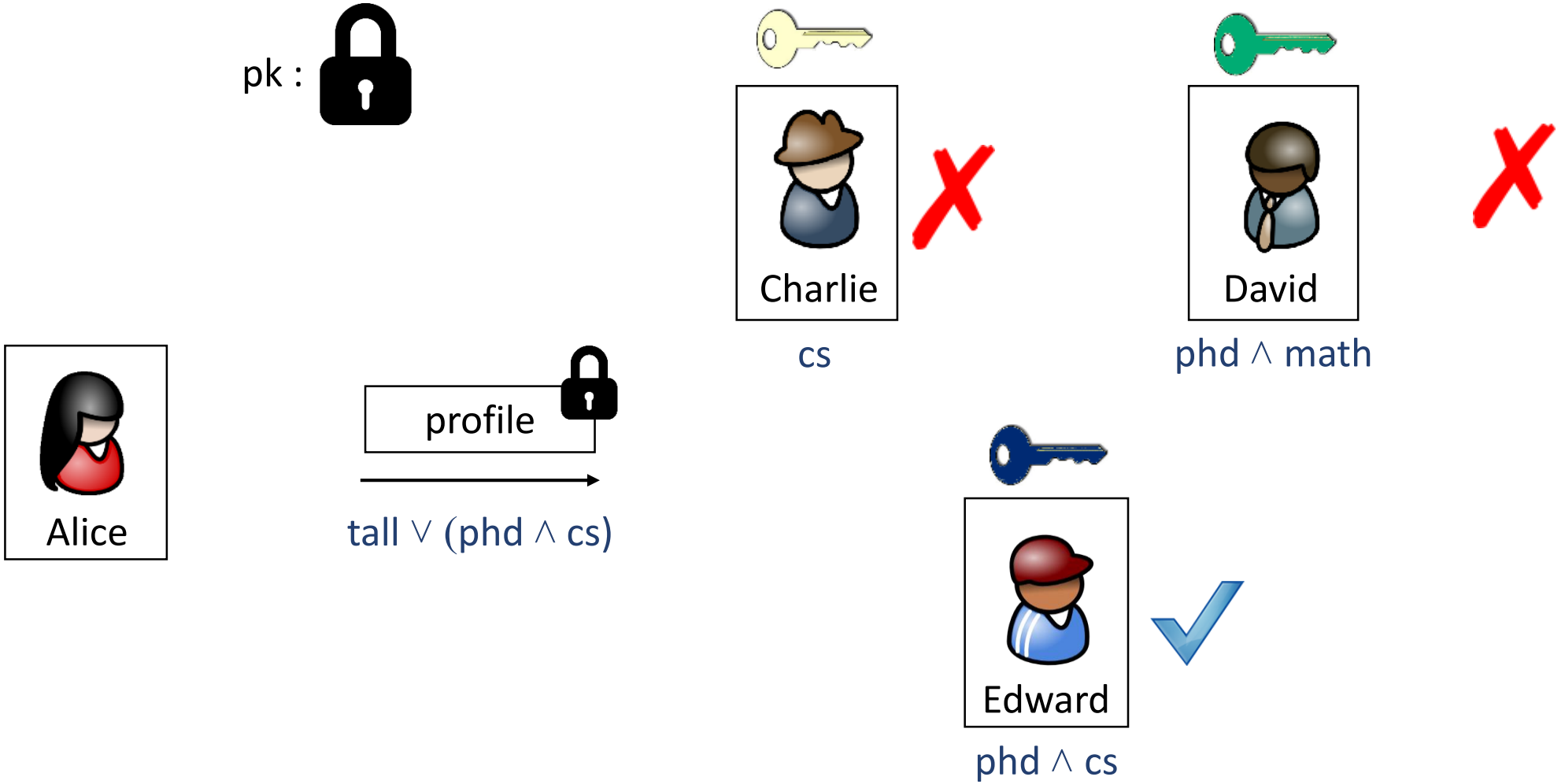
ABE [SW 05]: online dating



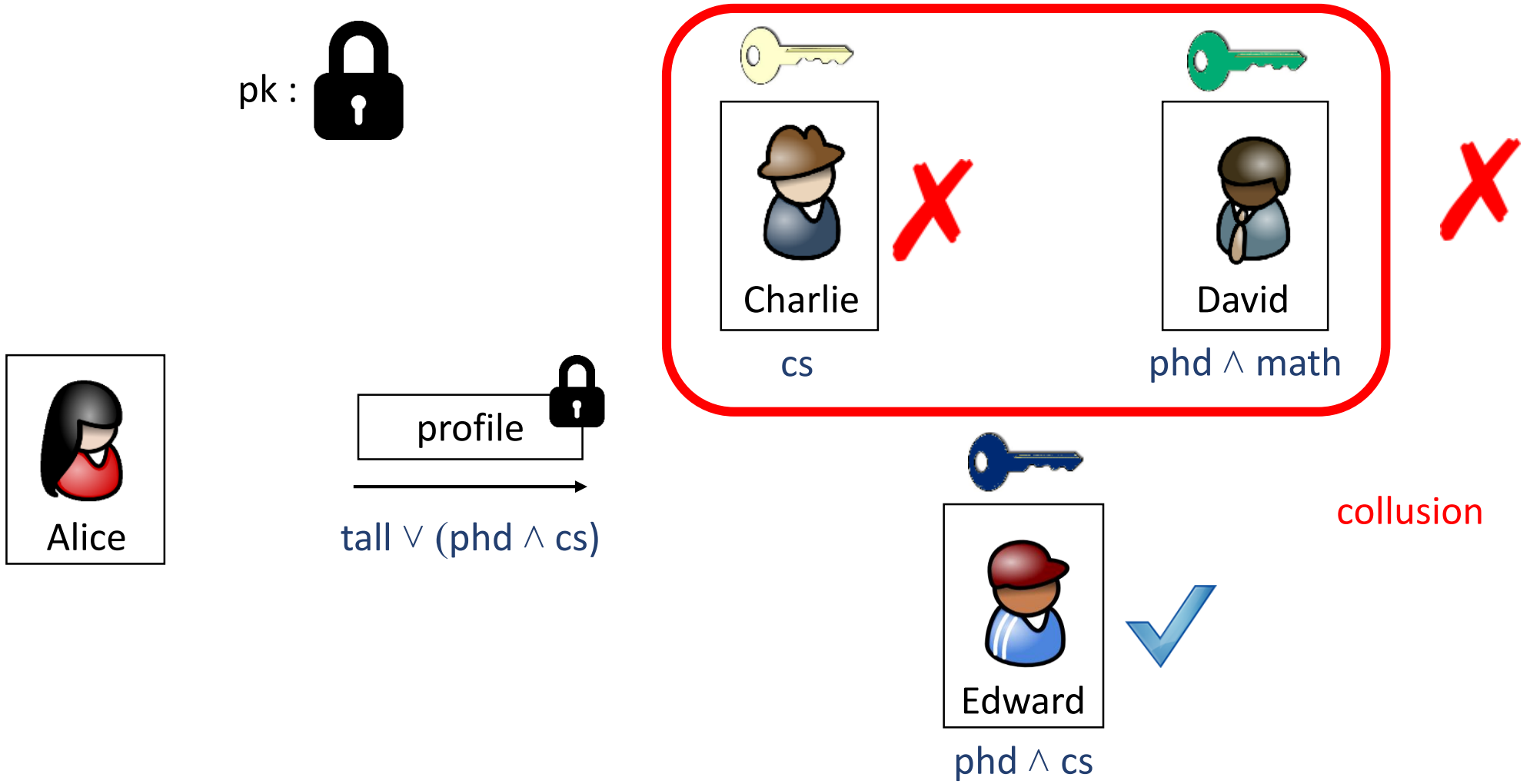
ABE [SW 05]: online dating



ABE [SW 05]: online dating

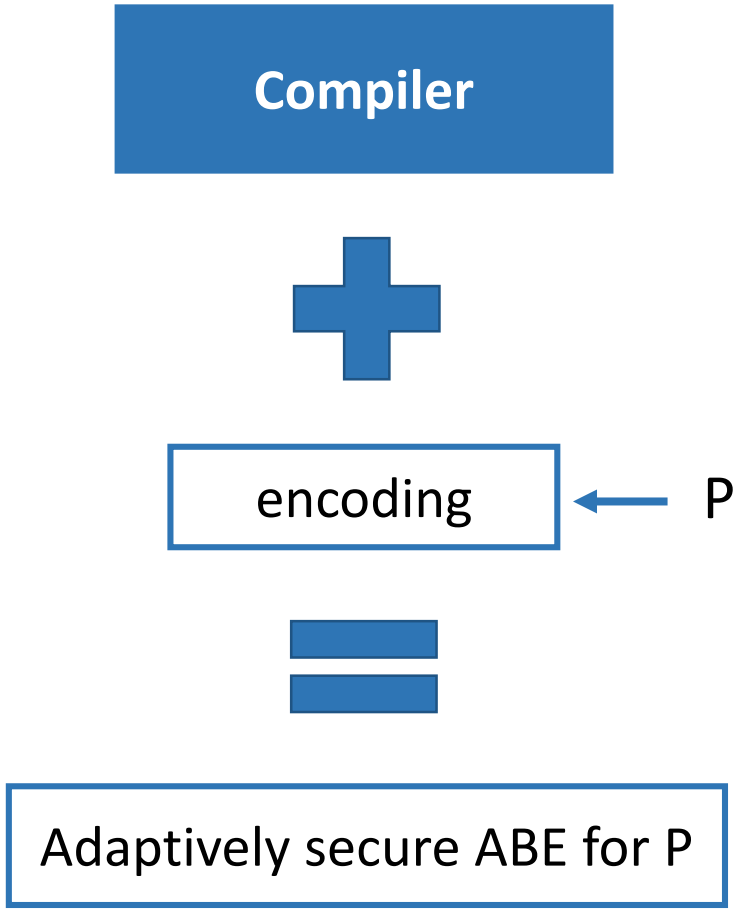


ABE [SW 05]: online dating



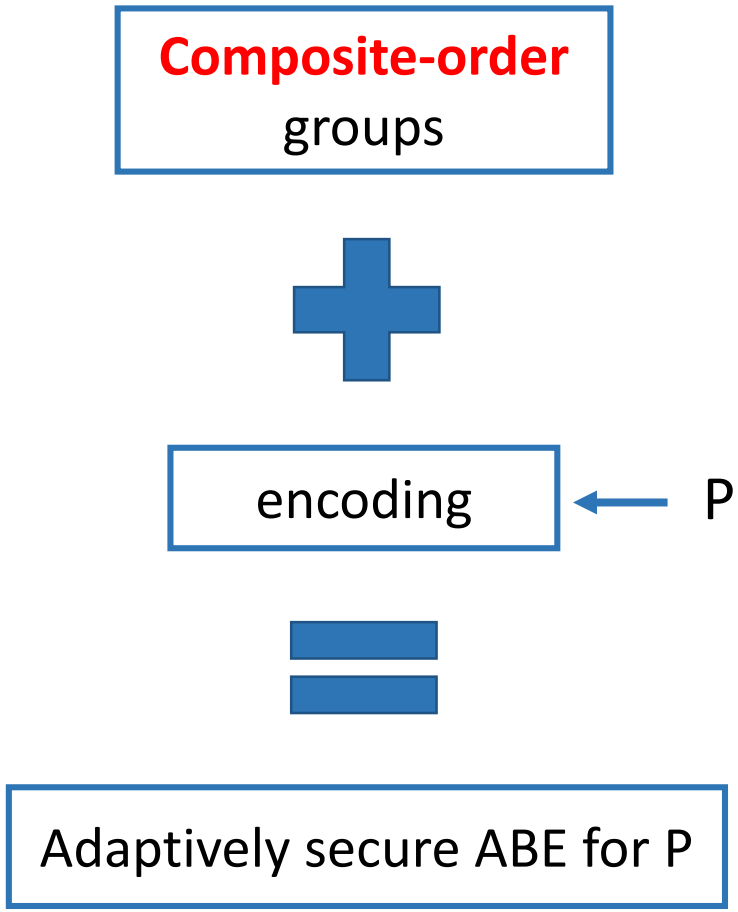
Modular framework for ABE

[Attrapadung 14, Wee 14]



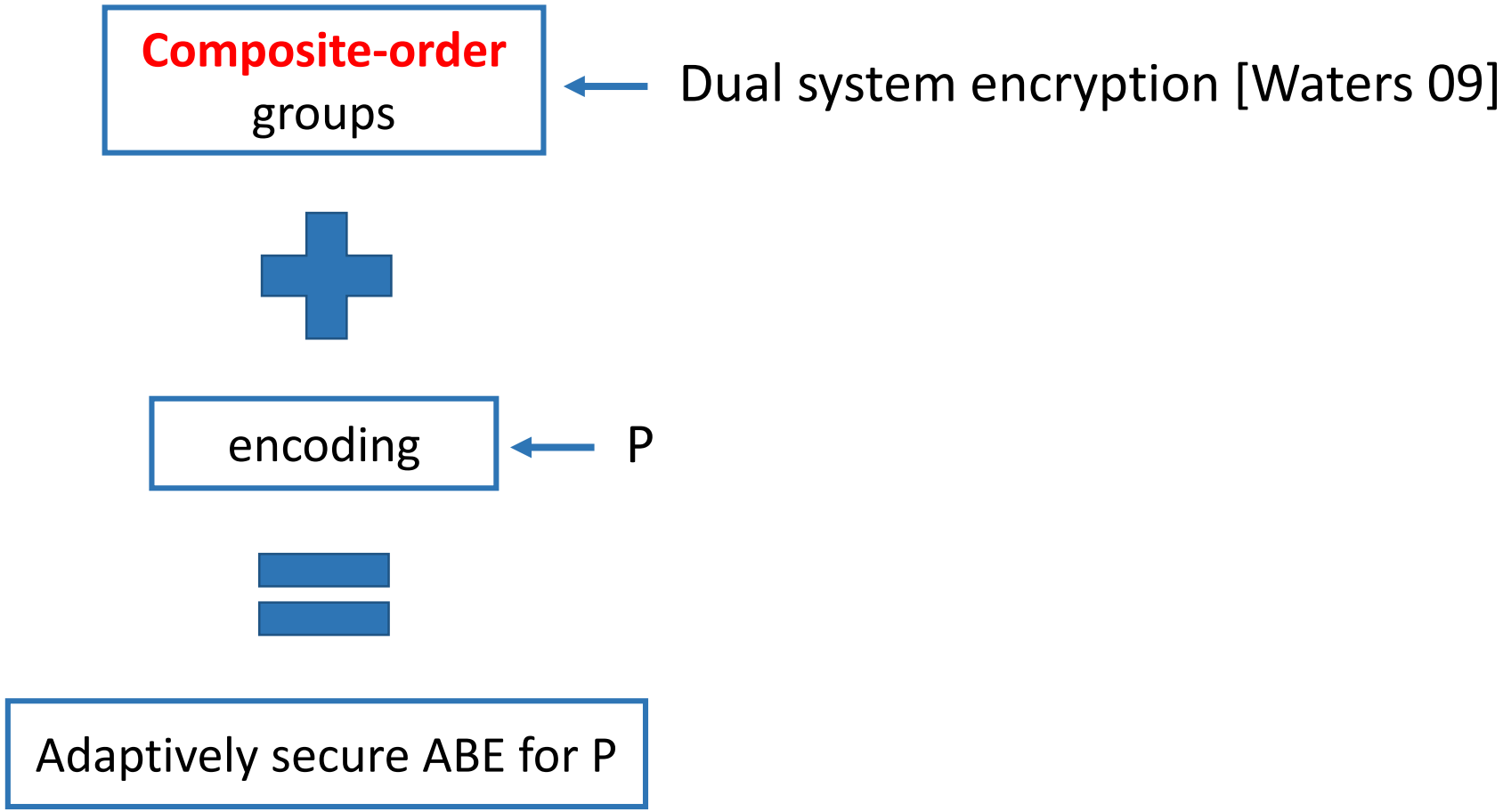
Modular framework for ABE

[Attrapadung 14, Wee 14]

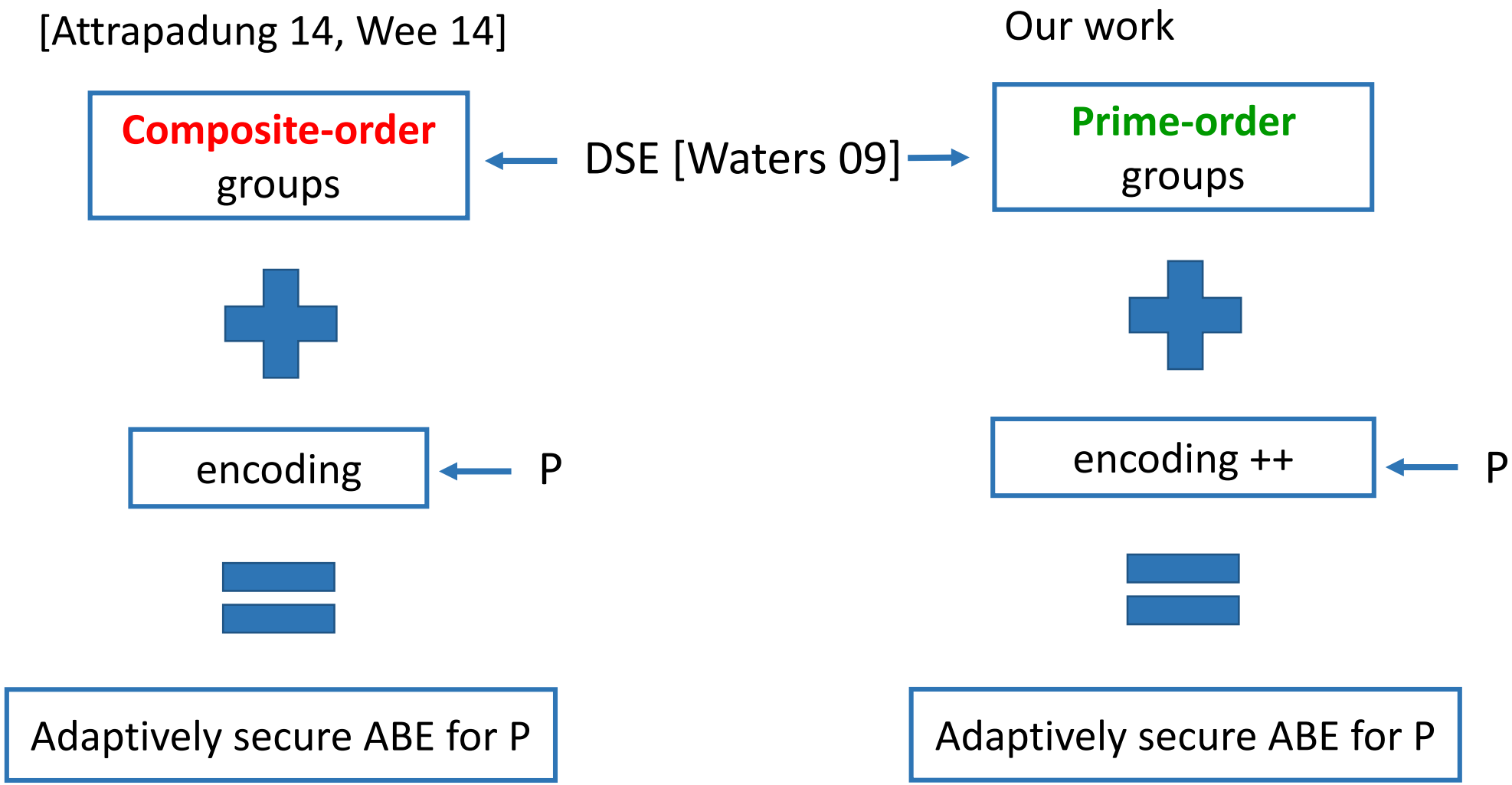


Modular framework for ABE

[Attrapadung 14, Wee 14]



Modular framework for ABE



Our contributions

1. New techniques for simulating composite-order groups

Our contributions

1. New techniques for simulating composite-order groups
2. New efficient ABEs

Our contributions

1. New techniques for simulating composite-order groups

2. New efficient ABEs

functionality	improvements
ABE for boolean formula	sk, ct 50% shorter

Our contributions

1. New techniques for simulating composite-order groups

2. New efficient ABEs

functionality	improvements
ABE for boolean formula	sk, ct 50% shorter
ABE for arithmetic formula	First adaptively secure scheme

Composite-order groups [BGN 05, LW 10]

p,q primes

e : $G = \boxed{G_p \times G_q}$

$\times$

$G = \boxed{G_p \times G_q}$

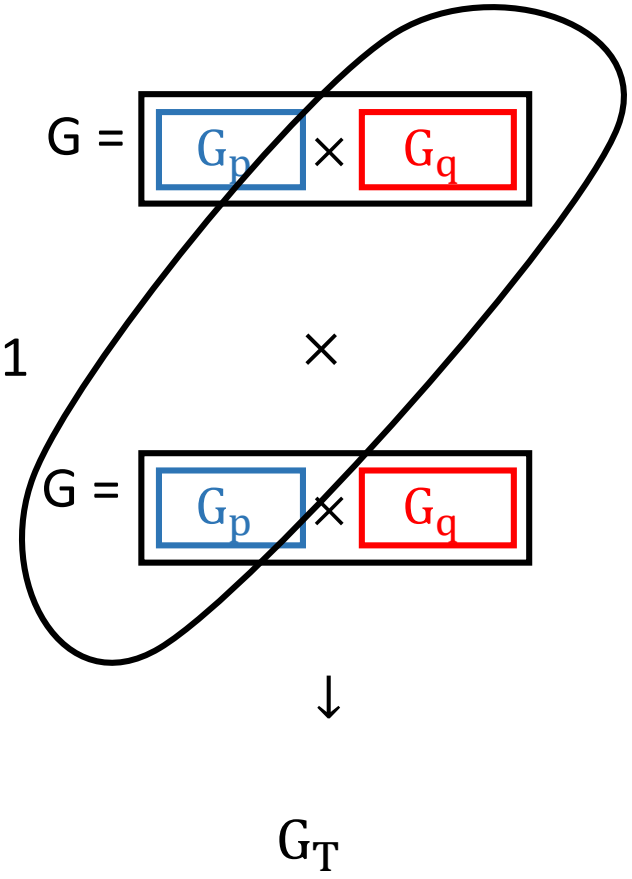
$\downarrow$

G_T

Composite-order groups [BGN 05, LW 10]

p,q primes

e :

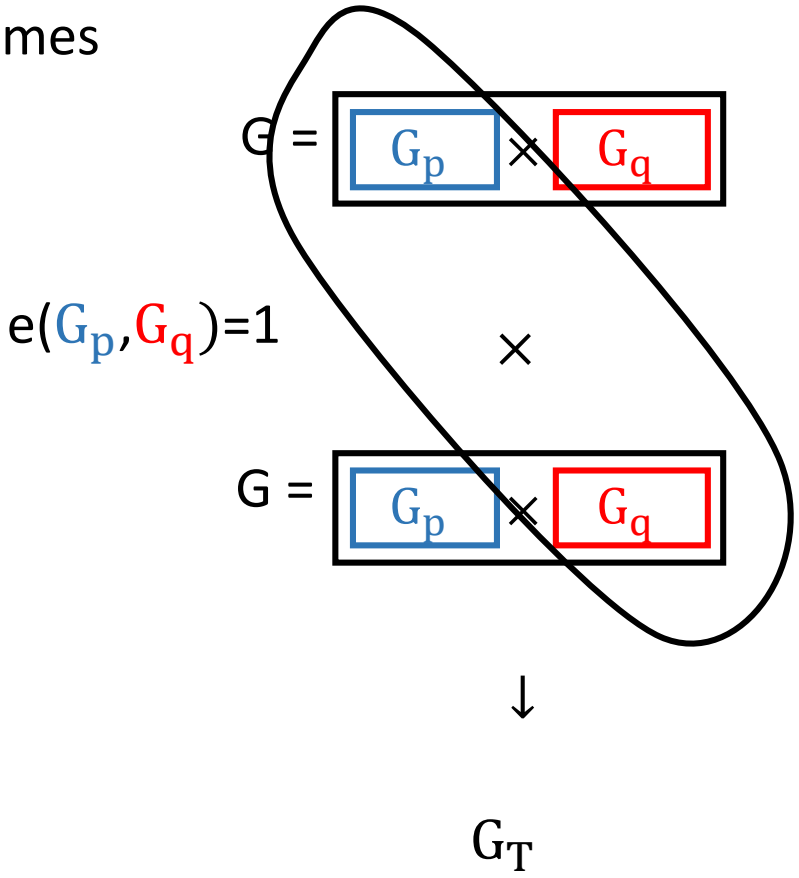


$e(G_q, G_p)=1$

Composite-order groups [BGN 05, LW 10]

p,q primes

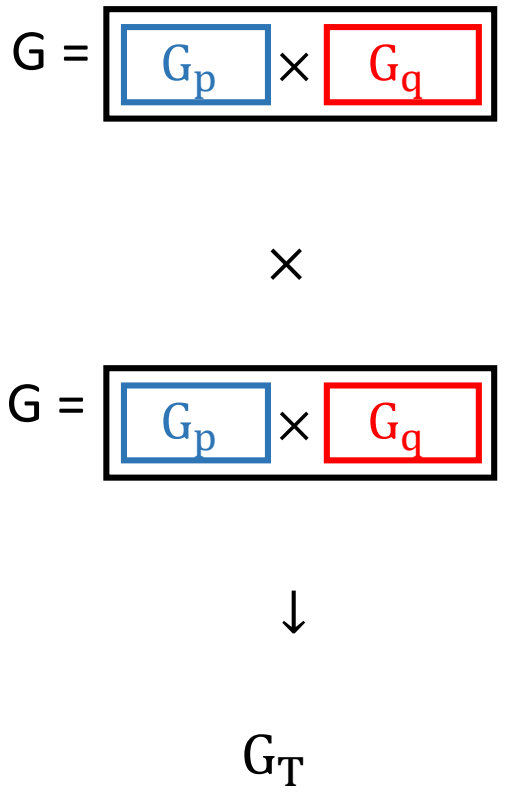
e :



Composite-order groups [BGN 05, LW 10]

p,q primes

e :



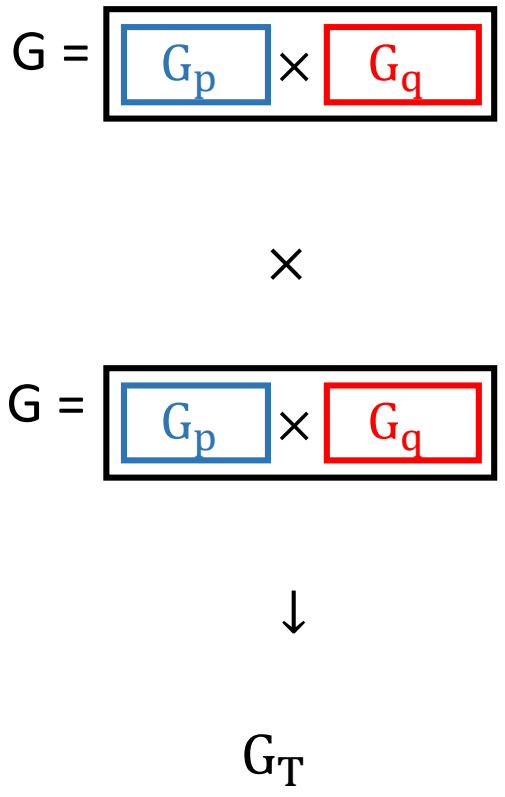
Subgroup Decision assumption:

$$\underset{\in G_p}{\text{random}} \approx_c \underset{\in G_p}{\text{random}} \cdot \underset{\in G_q}{\text{random}}$$

Composite-order groups [BGN 05, LW 10]

p,q primes

e :



Parameter hiding:

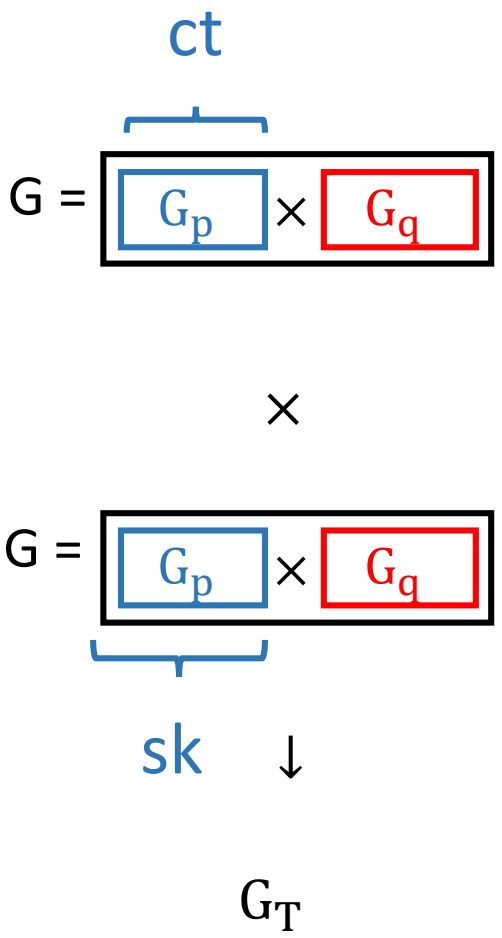
$G_p = \langle g_1 \rangle$, $G_q = \langle g_2 \rangle$

For all $w \leftarrow^R \mathbb{Z}_{pq}$
given $g_1^{\,w}$, $g_2^{\,w}$ is hidden

Composite-order groups [BGN 05, LW 10]

p,q primes

e :



Parameter hiding:

$G_p = \langle g_1 \rangle$, $G_q = \langle g_2 \rangle$

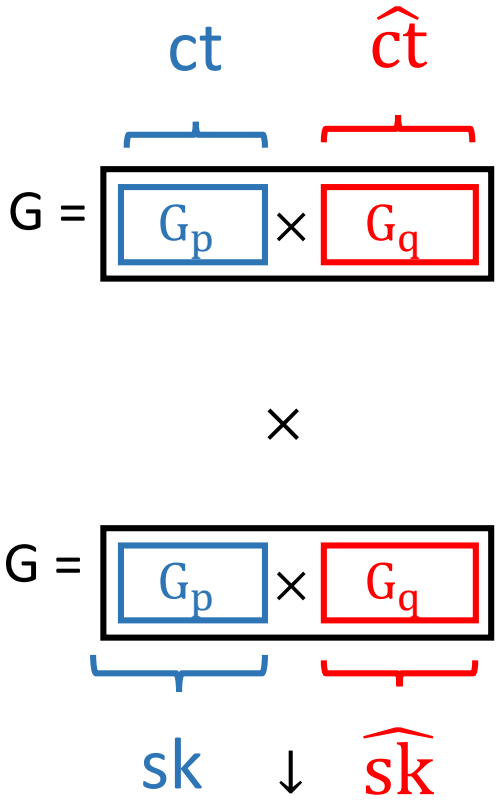
For all $w \leftarrow^R \mathbb{Z}_{pq}$

given $g_1^{\,w}$, $g_2^{\,w}$ is hidden

Composite-order groups [BGN 05, LW 10]

p,q primes

e :



Parameter hiding:

$G_p = < g_1 >$, $G_q = < g_2 >$

For all $w \leftarrow^R \mathbb{Z}_{pq}$

given $g_1^{\,w}$, $g_2^{\,w}$ is hidden

DSE [Waters 09]

Simulating composite-order groups

- [Freeman 10, MSF 10, Seo 12, HHHRR14] -> parameter hiding?
- DPVS: [OT 08, OT 09, Lewko 12, CLLWW 12] -> not compact
- [CW 13, BKP 14] -> not all predicate

Simulating composite-order groups

$G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, G_T of order p ,

$$e: G_1 \times G_2 \rightarrow G_T$$

$$e(g_1^x, g_2^y) = e(g_1, g_2)^{xy}$$

Simulating composite-order groups

$G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, G_T of order p ,

$$e: G_1 \times G_2 \rightarrow G_T$$

$$e([x]_1, [y]_2) = [xy]_T$$

Simulating composite-order groups

$G_1 = < g_1 >$, $G_2 = < g_2 >$, G_T of order p ,

$$e: G_1 \times G_2 \to G_T$$

$$e([x]_1, [y]_2) = [xy]_T$$

Matrix assumptions [EHKRV 13, MRV15]:

$$[A\vec{r}]_1 \approx_c [\vec{u}]_1$$

$A \in \mathbb{Z}_p^{(k+1)\times k}$, $\vec{r} \leftarrow^R \mathbb{Z}_p^{k}$ $\qquad$ $\vec{u} \leftarrow^R \mathbb{Z}_p^{(k+1)}$

Simulating composite-order groups

$G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, G_T of order p ,

$$e: G_1 \times G_2 \to G_T$$

$$e([x]_1, [y]_2) = [xy]_T$$

Matrix assumptions [EHKRV 13, MRV15]:

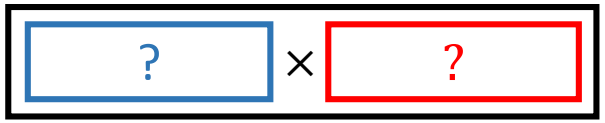
$$[A\vec{r}]_1 \approx_c [\vec{u}]_1$$

DDH: $A = \begin{pmatrix} 1 \\ a \end{pmatrix}$, $a \leftarrow^R \mathbb{Z}_p$

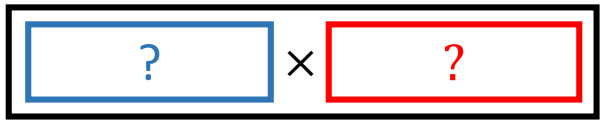
k-Lin: $A = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ a_1 & \cdots & a_k \end{pmatrix}$, $a_1, \ldots, a_k \leftarrow^R \mathbb{Z}_p$

Simulating composite-order groups

$e: G_1 \times G_2 \to G_T$ G_1, G_2 of order p

$\tilde{e}$: $G_1^{k+1} =$ 

×

$G_2^{k+1} =$ 

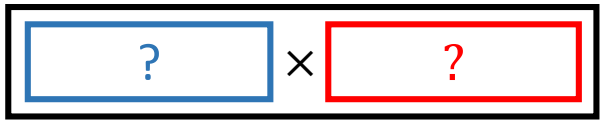
↓

G_T

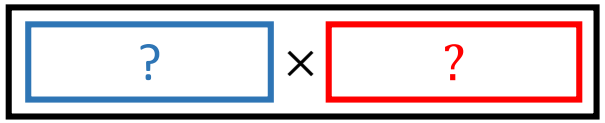
$\tilde{e}([\vec{x}]_1, [\vec{y}]_2) = [\vec{x}^T \vec{y}]_T$

Simulating composite-order groups

e: $G_1 \times G_2 \to G_T$ G_1, G_2 of order p

$\tilde{e}$: G_1^{k+1} = 

×

G_2^{k+1} = 

↓

G_T

$\tilde{e}([X]_1, [Y]_2) = [X^T Y]_T$

Simulating composite-order groups

e: $G_1 \times G_2 \to G_T$ $\quad G_1, G_2$ of order p

$\tilde{e}$: $\quad G_1^{k+1} = \boxed{< [A]_1 > \times ?}$

$\times$

$G_2^{k+1} = \boxed{< [B]_2 > \times ?}$

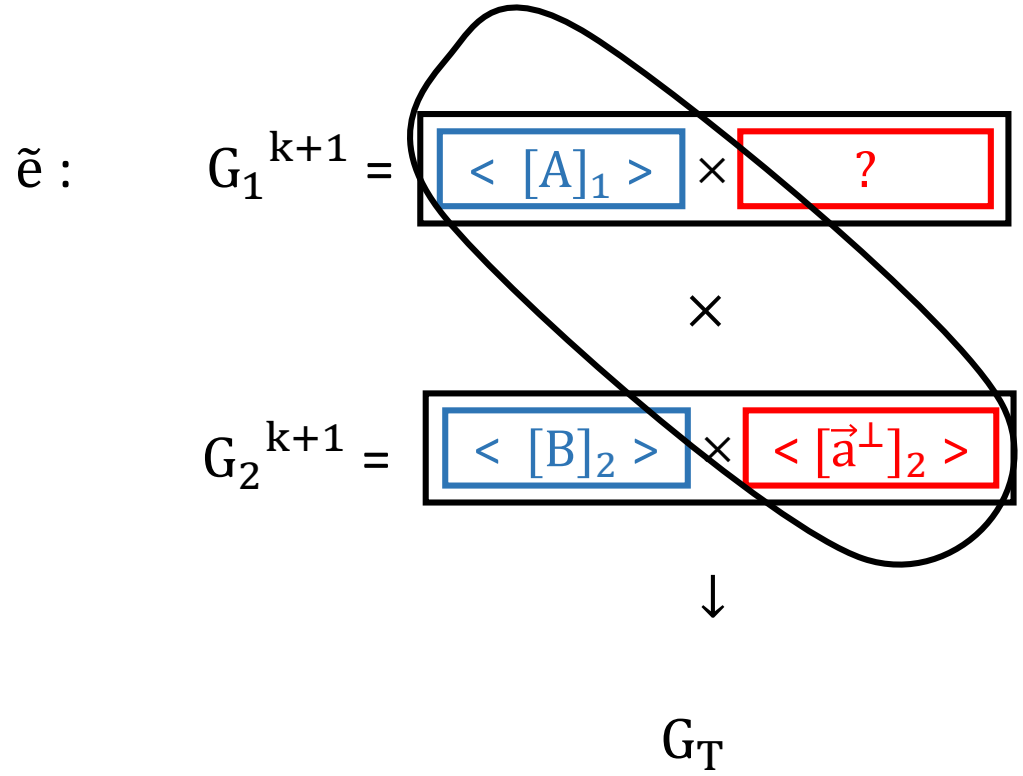
$\downarrow$

G_T

- $[A]_1, [B]_2 \leftarrow^R$ k-Lin

Simulating composite-order groups

$e: G_1 \times G_2 \rightarrow G_T$ G_1, G_2 of order p



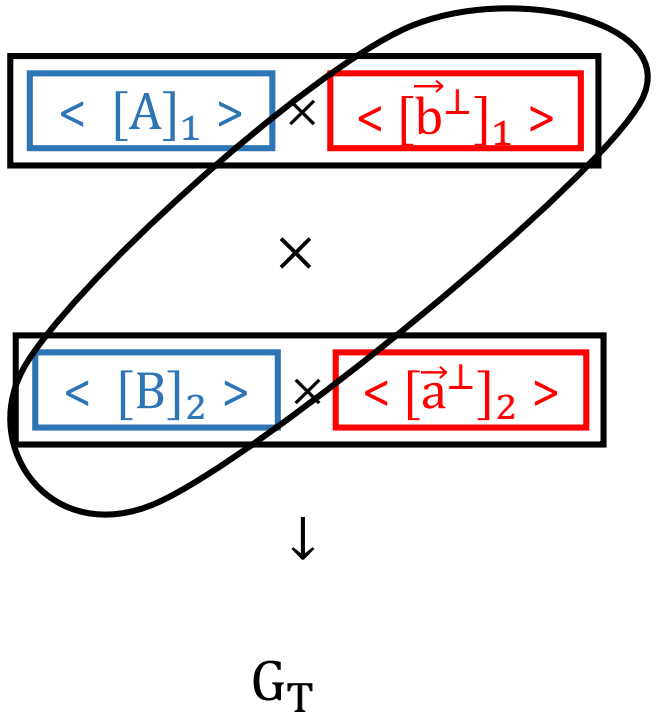
- $[A]_1, [B]_2 \leftarrow^R$ k-Lin
- $\vec{a}^{\perp} \leftarrow^R A^{\perp}$

$e([A]_1, [\vec{a}^{\perp}]_2)=1$

Simulating composite-order groups

$e: G_1 \times G_2 \rightarrow G_T$ G_1, G_2 of order p

$\tilde{e}$:



- $[A]_1, [B]_2 \leftarrow^R$ k-Lin
- $\vec{a}^{\perp} \leftarrow^R A^{\perp}$
- $\vec{b}^{\perp} \leftarrow^R B^{\perp}$

$e([\vec{b}^{\perp}]_1, [B]_2)=1$

Simulating composite-order groups

e: $G_1 \times G_2 \rightarrow G_T$ G_1, G_2 of order p

$\tilde{e}$: $G_1^{k+1} = \boxed{< [A]_1 > \times < [\vec{b}^{\perp}]_1 >}$

$\times$

$G_2^{k+1} = \boxed{< [B]_2 > \times < [\vec{a}^{\perp}]_2 >}$

$\downarrow$

G_T

- $[A]_1, [B]_2 \leftarrow^R$ k-Lin
- $\vec{a}^{\perp} \leftarrow^R A^{\perp}$
- $\vec{b}^{\perp} \leftarrow^R B^{\perp}$

Simulating composite-order groups

e: $G_1 \times G_2 \rightarrow G_T$ $\quad G_1, G_2$ of order p

$\tilde{e}$: $\quad {G_1}^{k+1} = \boxed{< [A]_1 > \times < [\vec{b}^{\perp}]_1 >}$

$\times$

${G_2}^{k+1} = \boxed{< [B]_2 > \times < [\vec{a}^{\perp}]_2 >}$

$\downarrow$

G_T

$[A]_1$, $[\vec{b}^{\perp}]_1$: basis of ${G_1}^{k+1}$

$[B]_2$, $[\vec{a}^{\perp}]_2$: basis of ${G_2}^{k+1}$

Simulating composite-order groups

e: $G_1 \times G_2 \rightarrow G_T$ G_1, G_2 of order p

$\tilde{e}$: $G_1^{k+1} = \boxed{< [A]_1 > \times < [\vec{b}^{\perp}]_1 >}$

$\times$

$G_2^{k+1} = \boxed{< [B]_2 > \times < [\vec{a}^{\perp}]_2 >}$

$\downarrow$

G_T

Subgroup membership:

$[A\vec{r}]_1 \approx_c [A\vec{r}]_1 \cdot [r'\vec{b}^{\perp}]_1$

Simulating composite-order groups

e: $G_1 \times G_2 \rightarrow G_T$ G_1, G_2 of order p

$\tilde{e}$: $G_1^{k+1} = \boxed{< [A]_1 > \times < [\vec{b}^{\perp}]_1 >}$

$\times$

$G_2^{k+1} = \boxed{< [B]_2 > \times < [\vec{a}^{\perp}]_2 >}$

$\downarrow$

G_T

Subgroup membership:

$[A\vec{r}]_1 \approx_c [A\vec{r}]_1 \cdot [r'\vec{b}^{\perp}]_1 = [\vec{u}]_1$

k-Lin in G_1

Simulating composite-order groups

$e: G_1 \times G_2 \to G_T$ G_1, G_2 of order p

$\tilde{e}$:

$$G_1^{k+1} = \boxed{< [A]_1 > \times < [\vec{b}^{\perp}]_1 >}$$

$$\times$$

$$G_2^{k+1} = \boxed{< [B]_2 > \times < [\vec{a}^{\perp}]_2 >}$$

$$\downarrow$$

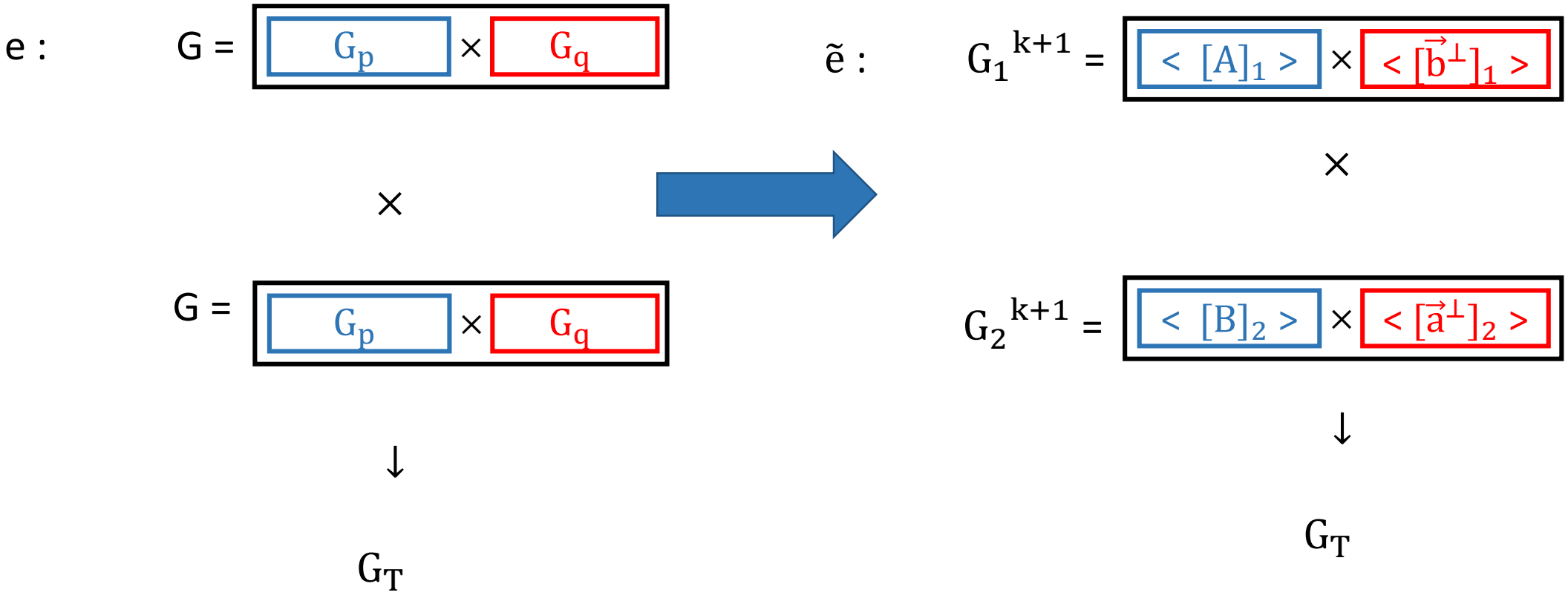
$$G_T$$

Subgroup membership:

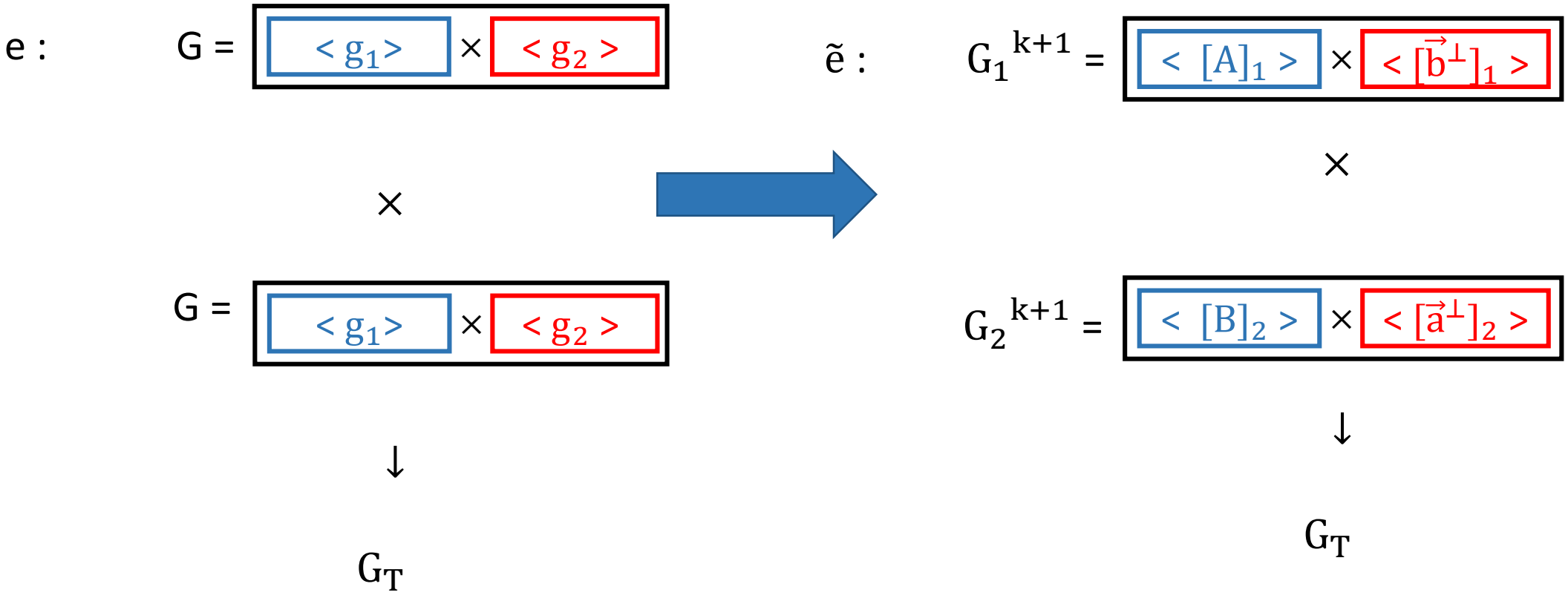
$$[B\vec{s}]_2 \approx_c [B\vec{s}]_2 \cdot [s'\vec{a}^{\perp}]_2 = [\vec{u}]_2$$

k-Lin in G_2

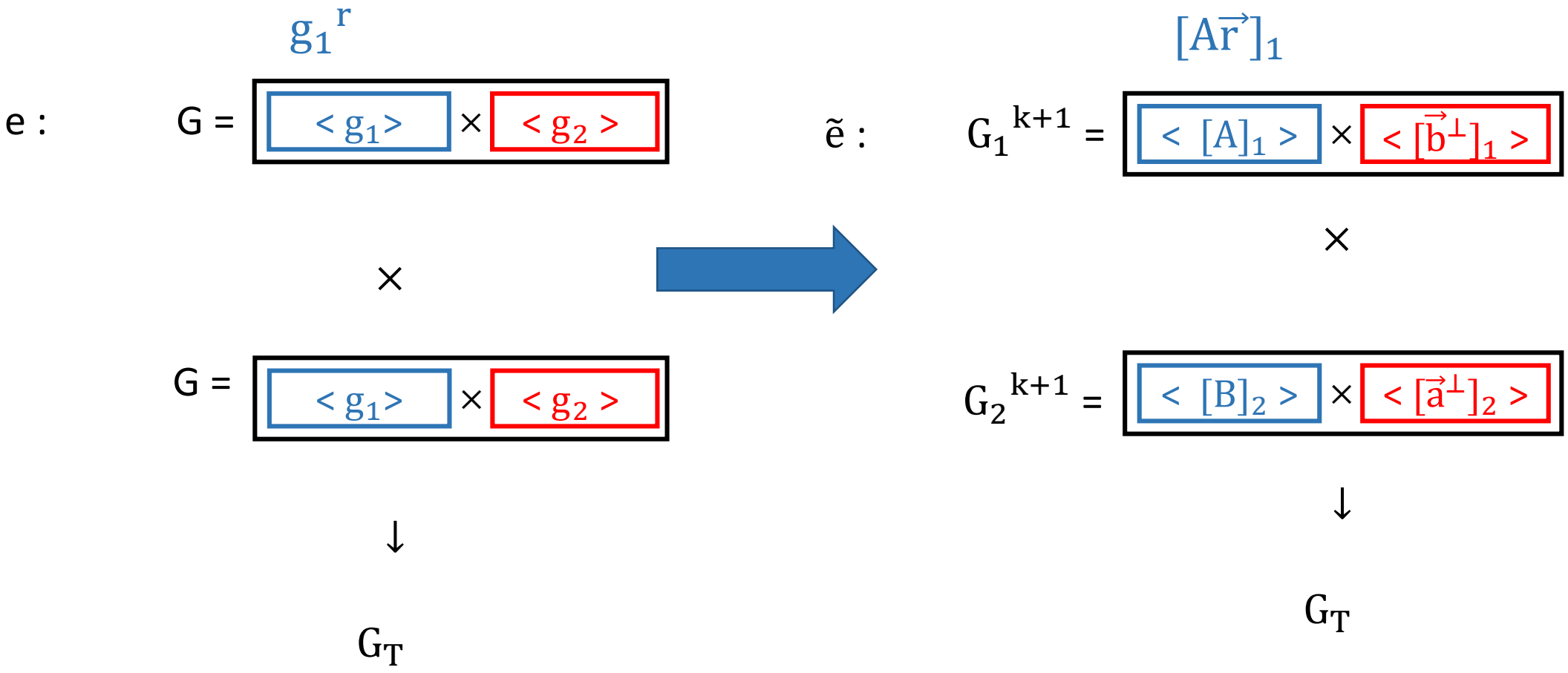
Simulating composite-order groups



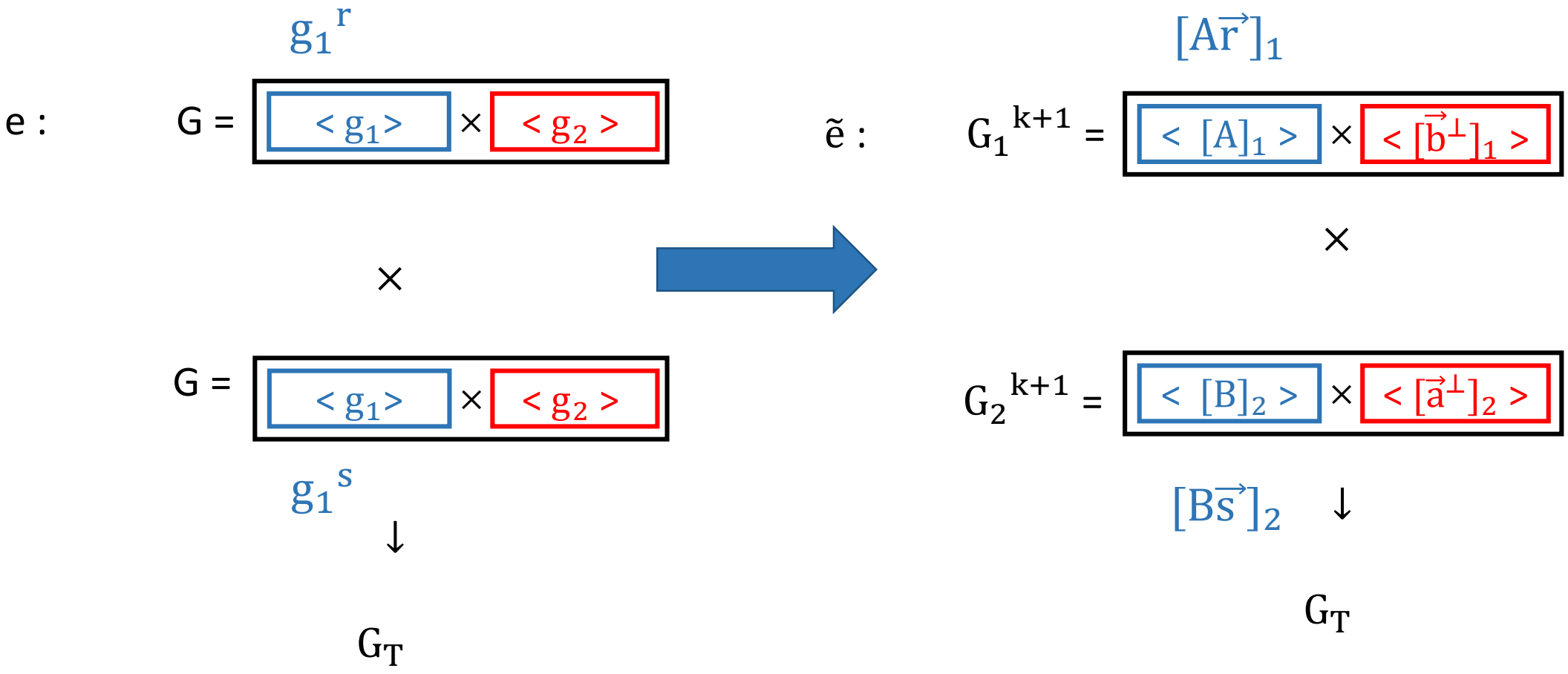
Simulating composite-order groups



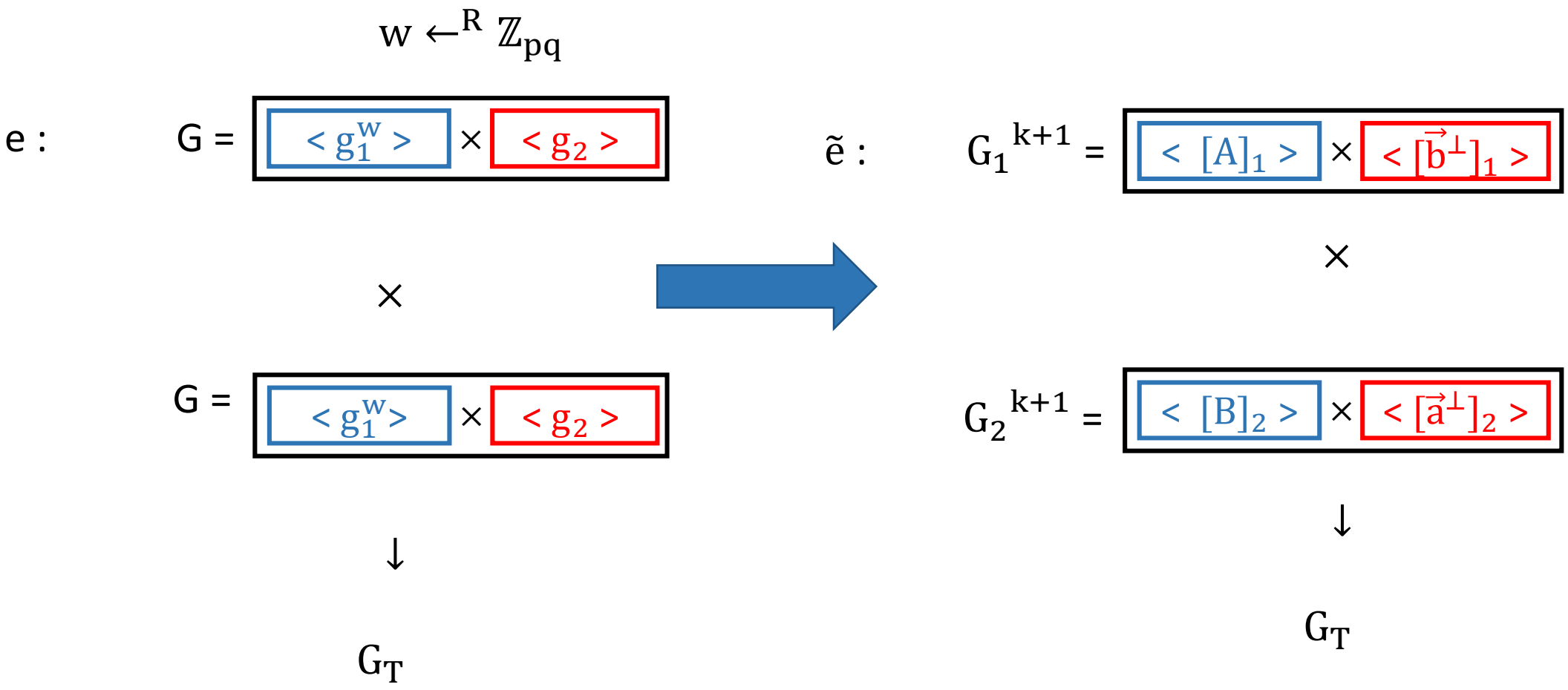
Simulating composite-order groups



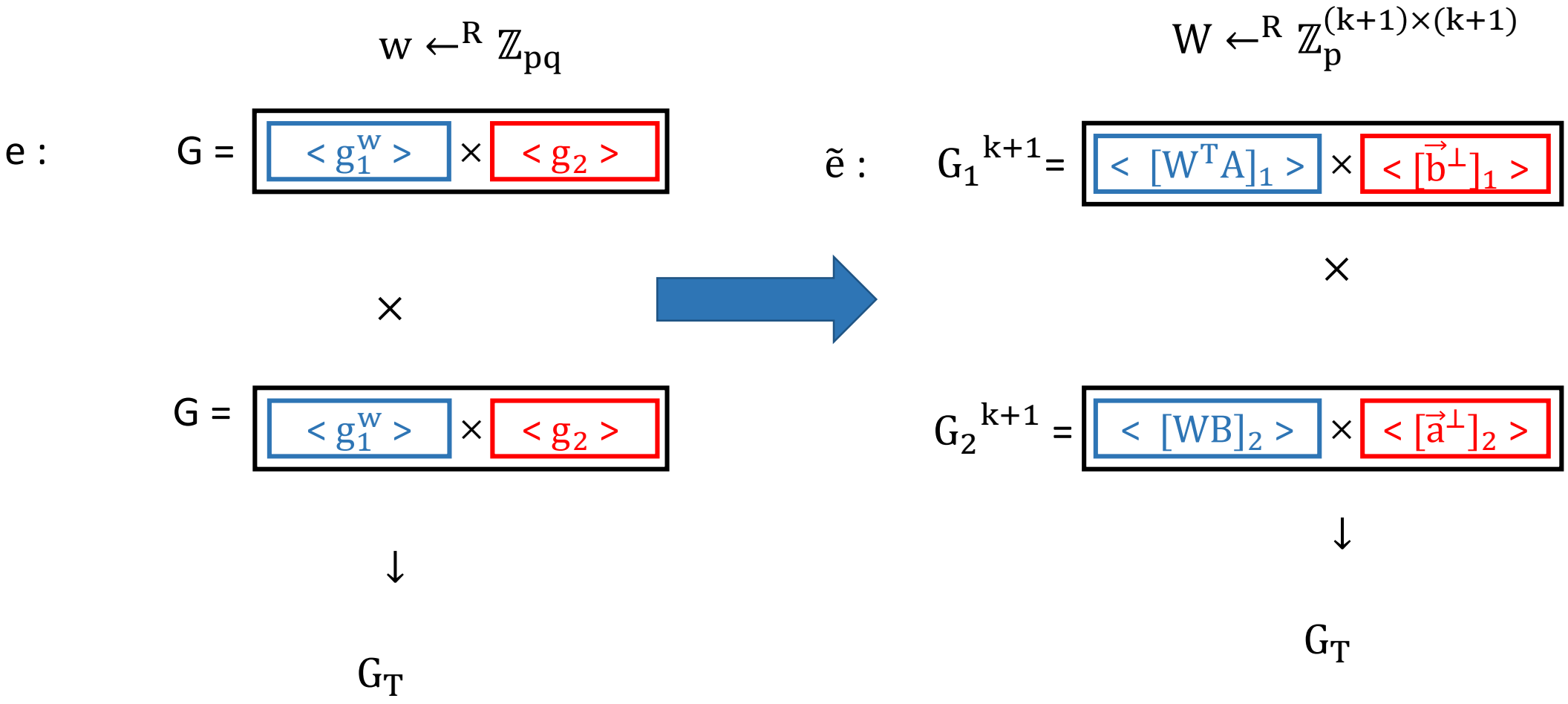
Simulating composite-order groups



Simulating composite-order groups



Simulating composite-order groups



Simulating composite-order groups

Parameter hiding:

$w \leftarrow^R \mathbb{Z}_{pq}$

$W \leftarrow^R \mathbb{Z}_p^{(k+1)\times(k+1)}$

Given $g_1{}^w$, $g_2{}^w$ is hidden

Given $[A^T W]_1$ and $[WB]_2$ $(\vec{a}^{\perp})^T W \vec{b}^{\perp}$ is hidden

Simulating composite-order groups

$$w \rightarrow W \in \mathbb{Z}_p^{(k+1)\times(k+1)}$$

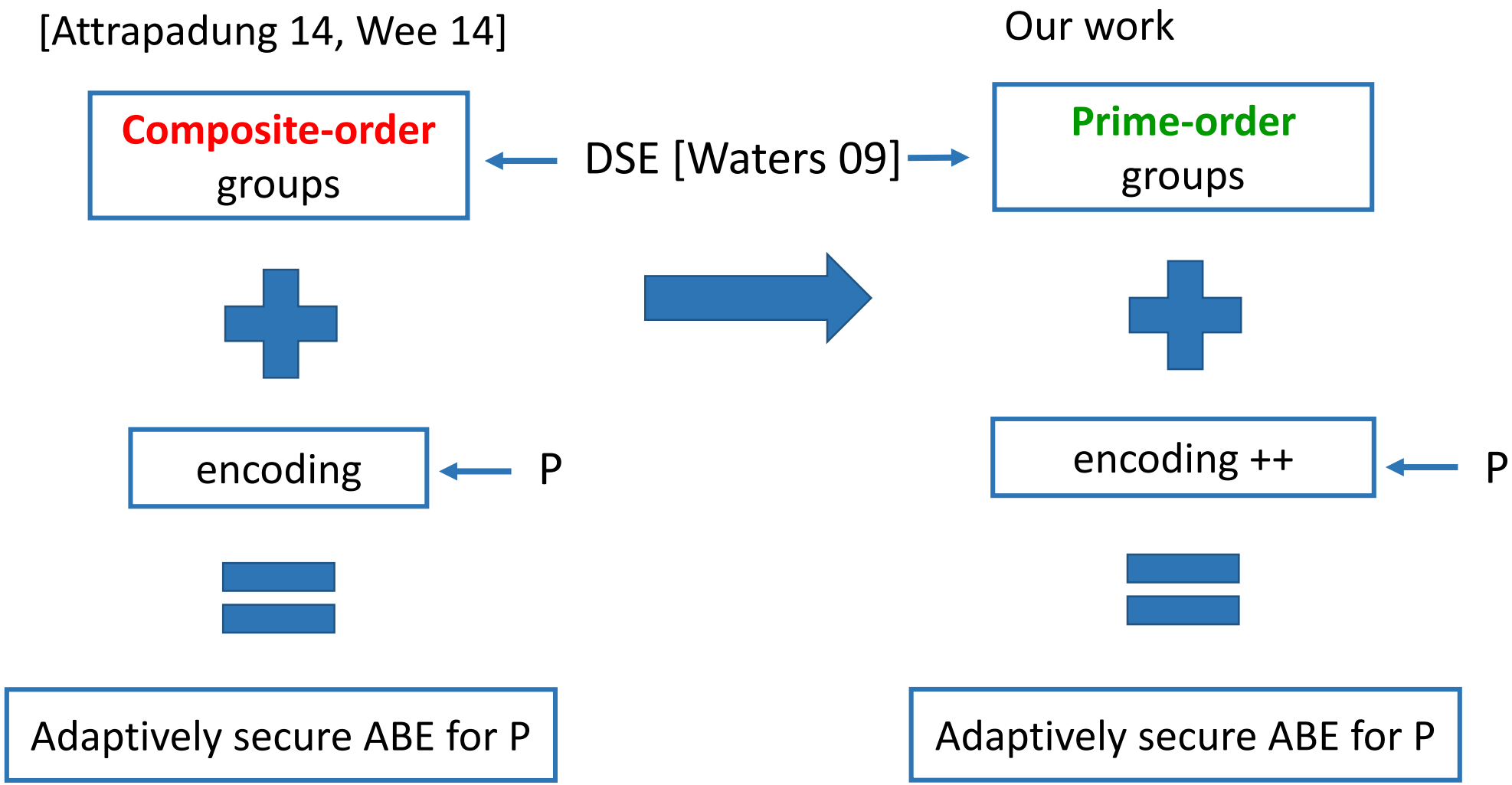
$$s \rightarrow \vec{s} \in \mathbb{Z}_p^k$$
$$g_1{}^s \rightarrow [A\vec{s}]_1$$
$$g_1{}^{ws} \rightarrow [W^T A\vec{s}]_1$$

ct

$$r \rightarrow \vec{r} \in \mathbb{Z}_p^k$$
$$g_1{}^r \rightarrow [B\vec{r}]_2$$
$$g_1{}^{wr} \rightarrow [WB\vec{r}]_2$$

sk

Modular framework for ABE



Conclusion

New efficient ABEs for boolean formula of size n:

reference	(static) assumption	|sk| , |ct|
[A14, W14]	Composite-order	|sk| , |ct| = n + O(1) g.e.

Conclusion

New efficient ABEs for boolean formula of size n:

reference	(static) assumption	|sk| , |ct|
[A14, W14]	Composite-order	|sk| , |ct| = n + O(1) g.e.
[Lewko 12, CLL+ 12]	k-Lin	|sk| , |ct| = O((k+1)(n + O(1))) g.e.

Conclusion

New efficient ABEs for boolean formula of size n:

reference	(static) assumption	|sk| , |ct|
[A14, W14]	Composite-order	|sk| , |ct| = n + O(1) g.e.
[Lewko 12, CLL+ 12]	k-Lin	|sk| , |ct| = O((k+1)(n + O(1))) g.e.
[our work]	k-Lin	|sk| , |ct| = (k+1)(n + O(1)) g.e.

Conclusion

New efficient ABEs for boolean formula of size n:

reference	(static) assumption	|sk| , |ct|
[A14, W14]	Composite-order	|sk| , |ct| = n + O(1) g.e.
[Lewko 12, CLL+ 12]	k-Lin	|sk| , |ct| = O((k+1)(n + O(1))) g.e.
[our work]	k-Lin	|sk| , |ct| = (k+1)(n + O(1)) g.e.
Open problem	k-Lin	|sk| , |ct| = n + k + O(1) ? g.e.

Thank you!

Questions?

Encoding ++

$$\mathsf{mpk} := \left(g_1,\ g_1^{\mathbf{w}},\ e(g_1, g_1)^{\alpha} \right)$$

$$\mathsf{sk}_y := \left(g_1^{r},\ g_1^{\mathsf{kE}(y,\alpha)+r\cdot\mathsf{rE}(y,\mathbf{w})} \right)$$

$$\mathsf{ct}_x := \left(g_1^{s},\ g_1^{s\cdot\mathsf{sE}(x,\mathbf{w})},\ e(g_1, g_1)^{\alpha s}\cdot m \right)$$

Encoding ++

$$\mathsf{mpk} := \left(g_1,\ g_1^{\mathbf{w}},\ e(g_1, g_1)^{\alpha} \right)$$

$$\mathsf{sk}_y := \left(g_1^{r},\ g_1^{\mathsf{kE}(y,\alpha)+r\cdot\mathsf{rE}(y,\mathbf{w})} \right)$$

$$\mathsf{ct}_x := \left(g_1^{s},\ g_1^{s\cdot\mathsf{sE}(x,\mathbf{w})},\ e(g_1, g_1)^{\alpha s}\cdot m \right)$$

Hiding: $\mathrm{P}(x, y) = 0 \ \Rightarrow (\ \mathrm{kE}(y, \alpha) + \mathrm{rE}(y, \mathbf{w})\ , \mathrm{sE}(x, \mathbf{w})\ ) \perp \alpha$

Encoding ++

$$\mathsf{mpk} := \left(g_1,\ g_1^{\mathbf{w}},\ e(g_1, g_1)^{\alpha} \right)$$

$$\mathsf{sk}_y := \left(g_1^{r},\ g_1^{\mathsf{kE}(y,\alpha)+r\cdot\mathsf{rE}(y,\mathbf{w})} \right)$$

$$\mathsf{ct}_x := \left(g_1^{s},\ g_1^{s\cdot\mathsf{sE}(x,\mathbf{w})},\ e(g_1, g_1)^{\alpha s}\cdot m \right)$$

Hiding: $\mathrm{P}(x, y) = 0 \ \Rightarrow (\ \mathrm{kE}(y, \alpha) + \mathrm{rE}(y, \mathbf{w})\ , \mathrm{sE}(x, \mathbf{w})\ ) \perp \alpha$

Decryption: $L_{xy}\left(\mathsf{kE}(y, \alpha) + r \cdot \mathsf{rE}(y, \mathbf{w}),\ r \cdot \mathsf{sE}(x, \mathbf{w}) \right) = \alpha$

« Pairwise associative » property:

For all $s, r, w_1, w_2 \in \mathbb{Z}_{pq}$: $e({g_1}^{w_1 s}, {g_1}^{w_2 r}) = e({g_1}^{w_2 s}, {g_1}^{w_1 r})$

$$(A^T W_1)(W_2 B) \neq (A^T W_2)(W_1 B)$$

« Pairwise associative » property:

For all $s, r, w_1, w_2 \in \mathbb{Z}_{pq}$: $e(g_1{}^{w_1 s}, g_1{}^{w_2 r}) = e(g_1{}^{w_2 s}, g_1{}^{w_1 r})$

$$(A^T W_1)(W_2 B) \neq (A^T W_2)(W_1 B)$$

« Associative » property:

For all $s, r, w \in \mathbb{Z}_{pq}$: $e(g_1{}^{s}, g_1{}^{wr}) = e(g_1{}^{sw}, g_1{}^{r})$

$$(A^T W)B = A^T(WB)$$

An example: IBE

- $\mathrm{Enc}(M,x\,;\vec{r}) =$

$$[A\vec{r}]_1 \quad , \quad [(W_1{}^{T}x + W_2{}^{T})A\,\vec{r}]_1 \quad , \quad M\cdot[\mathrm{Enc.key}]_T$$

- $\mathrm{KeyGen}(\overrightarrow{msk}, y\,;\vec{s}) =$

$$[\overrightarrow{msk} + (W_1 y + W_2)B\vec{s}]_2 \quad , \quad [B\vec{s}]_2$$

An example: IBE

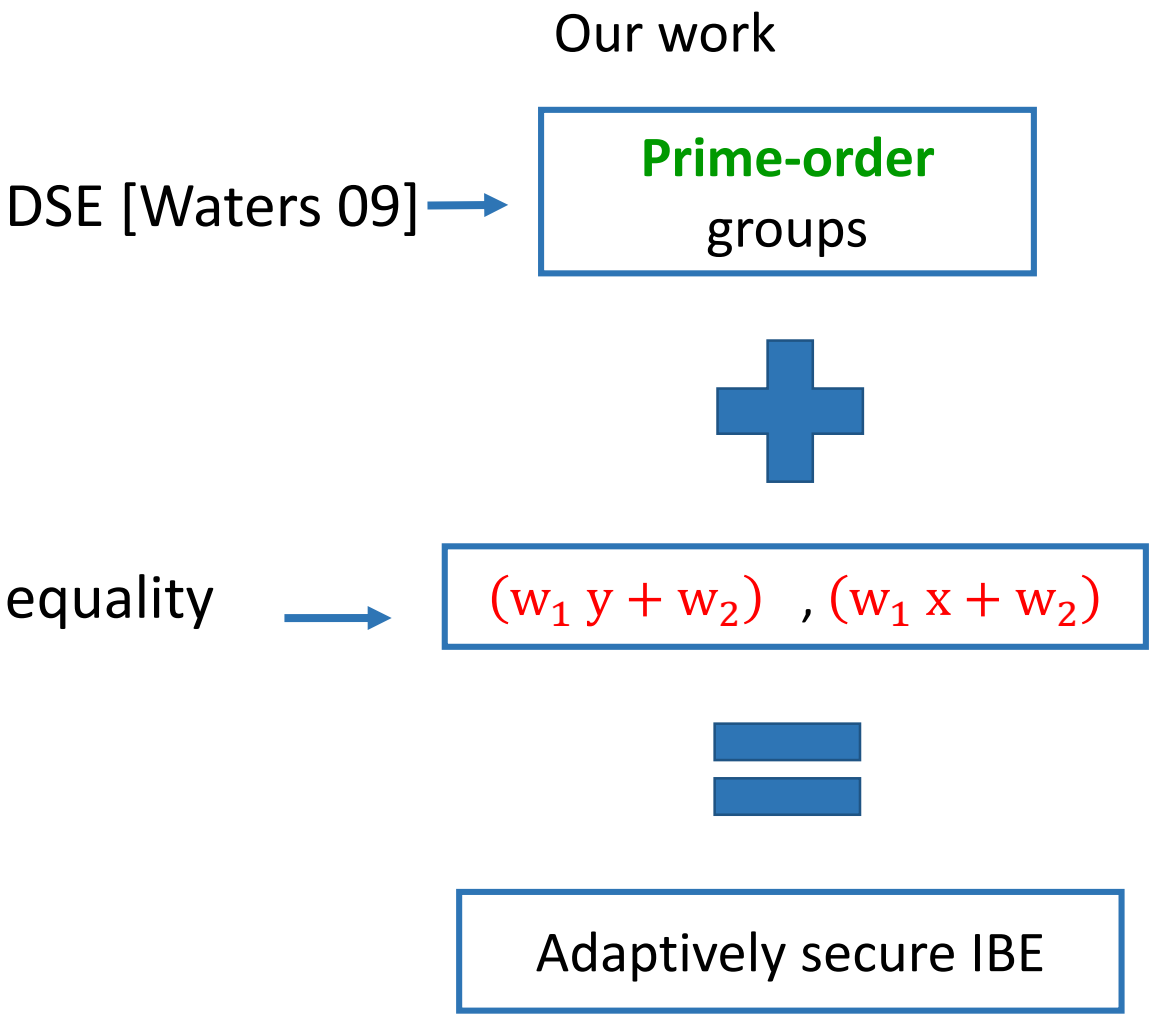
- $\mathrm{Enc}(M,x\,;\vec{r}) =$

$$[A\vec{r}]_1 \quad , \quad [(W_1{}^{T}x + W_2{}^{T})A\,\vec{r}]_1 \quad , \quad M\cdot[\mathrm{Enc.\,key}]_T$$

- $\mathrm{KeyGen}(\overrightarrow{msk}, y\,;\vec{s}) =$

$$[\overrightarrow{msk} + (W_1 y + W_2)B\vec{s}]_2 \quad , \quad [B\vec{s}]_2$$

An example: IBE [LW 10]



An example: IBE [LW 10]

- $\mathrm{Enc}(M,x\,;r) =$

$$g_1^{\,r}\ ,$$
$$g_1^{\,(w_1 x+w_2)r}\ ,$$
$$M\cdot [\mathrm{Enc.key}]_T$$

- $\mathrm{Enc}(M,x\,;\vec{r}) =$

$$[A\vec{r}]_1\ ,$$
$$[(W_1^{\,T}x + W_2^{\,T})A\,\vec{r}]_1\ ,$$
$$M\cdot [\mathrm{Enc.key}]_T$$

- $\mathrm{KeyGen}(\mathrm{msk}, y\,; s) =$

$$g_1^{\,\mathrm{msk} + (w_1 y+w_2)s}\ ,$$
$$g_1^{\,r}$$

- $\mathrm{KeyGen}(\overrightarrow{\mathrm{msk}}, y\,; \vec{s}) =$

$$[\overrightarrow{\mathrm{msk}} + (W_1 y + W_2)B\vec{s}]_2,$$
$$[B\vec{s}]_2$$

An example: IBE [LW 10]

- $\mathrm{Enc}(M,x\,;r) =$

$$g_1^{\,r}\ ,$$
$$g_1^{\,(w_1 x+w_2)r}\ ,$$
$$M\cdot [\mathrm{Enc.key}]_T$$

- $\mathrm{Enc}(M,x\,;\vec{r}) =$

$$[A\vec{r}]_1\ ,$$
$$[(W_1^{\,T}x + W_2^{\,T})A\,\vec{r}]_1\ ,$$
$$M\cdot [\mathrm{Enc.key}]_T$$

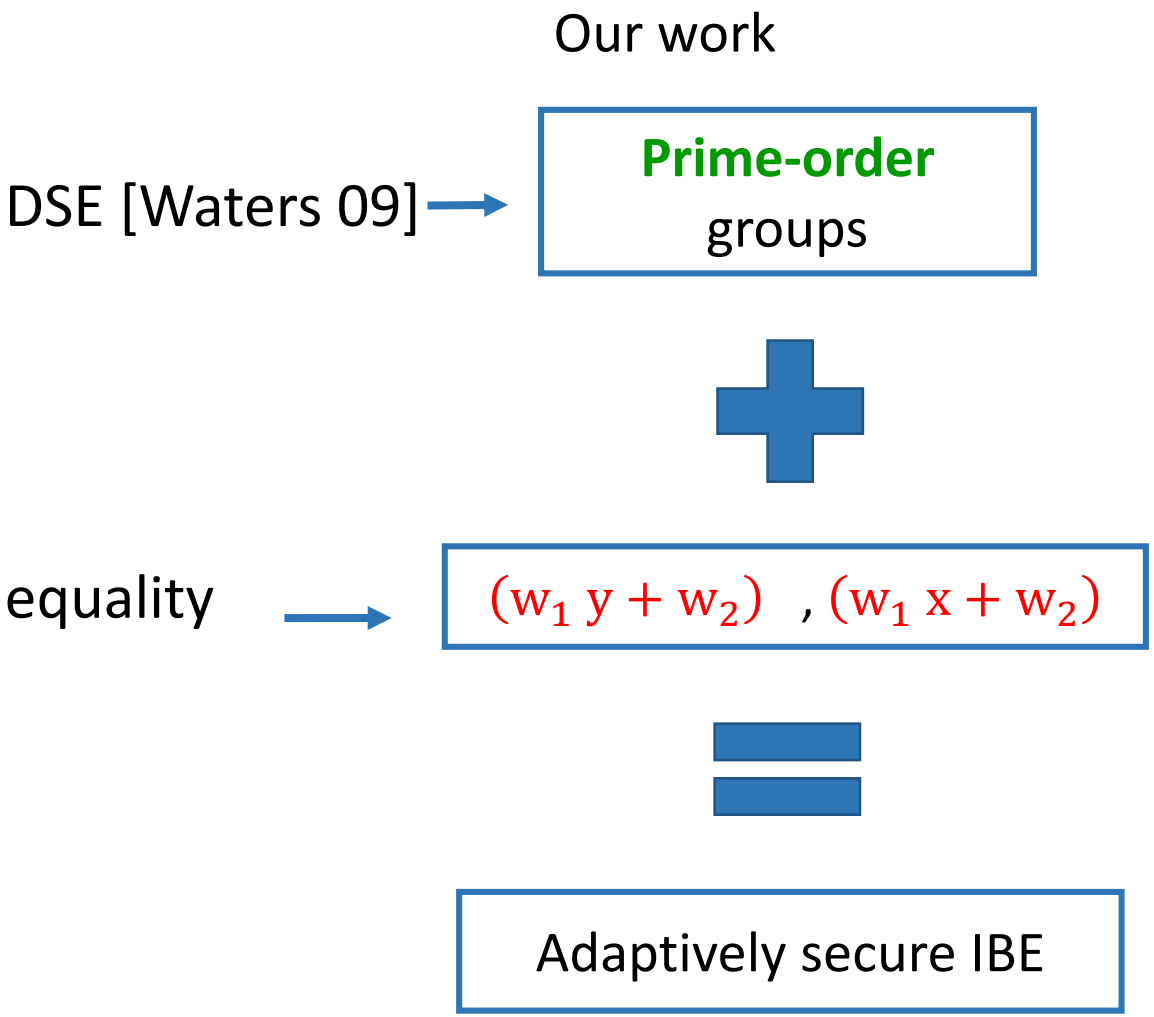
- $\mathrm{KeyGen}(\mathrm{msk}, y\,; s) =$

$$g_1^{\,\mathrm{msk} + (w_1 y+w_2)s}\ ,$$
$$g_1^{\,r}$$

- $\mathrm{KeyGen}(\overrightarrow{\mathrm{msk}}, y\,; \vec{s}) =$

$$[\overrightarrow{\mathrm{msk}} + (W_1 y + W_2)B\vec{s}]_2,$$
$$[B\vec{s}]_2$$

An example: IBE [LW 10]



ABE: adaptive security

Challenger

$b \leftarrow^{R} \{0,1\}$

$b' =^{?} b$

pk

y

sk_y

repeat

m_0, m_1, x

$Enc_{pk}(x, m_b)$

y

sk_y

repeat

b'

Adversary

P(x,y)=0 for all y