Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting

Junqing Gong
Shanghai Jiao Tong University

Xiaolei Dong, Jie Chen, Zhenfu Cao
East China Normal University

ASIACRYPT 2016, Hanoi, Vietnam
Dec 7, 2016

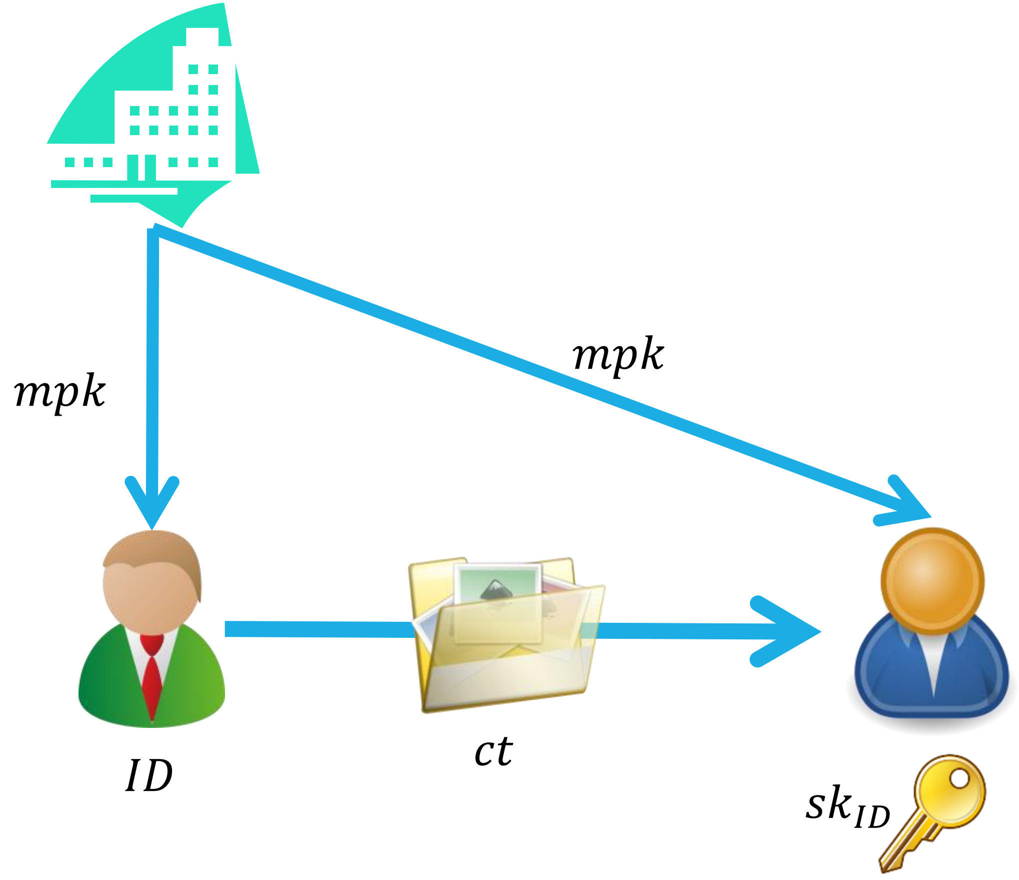
outline

- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

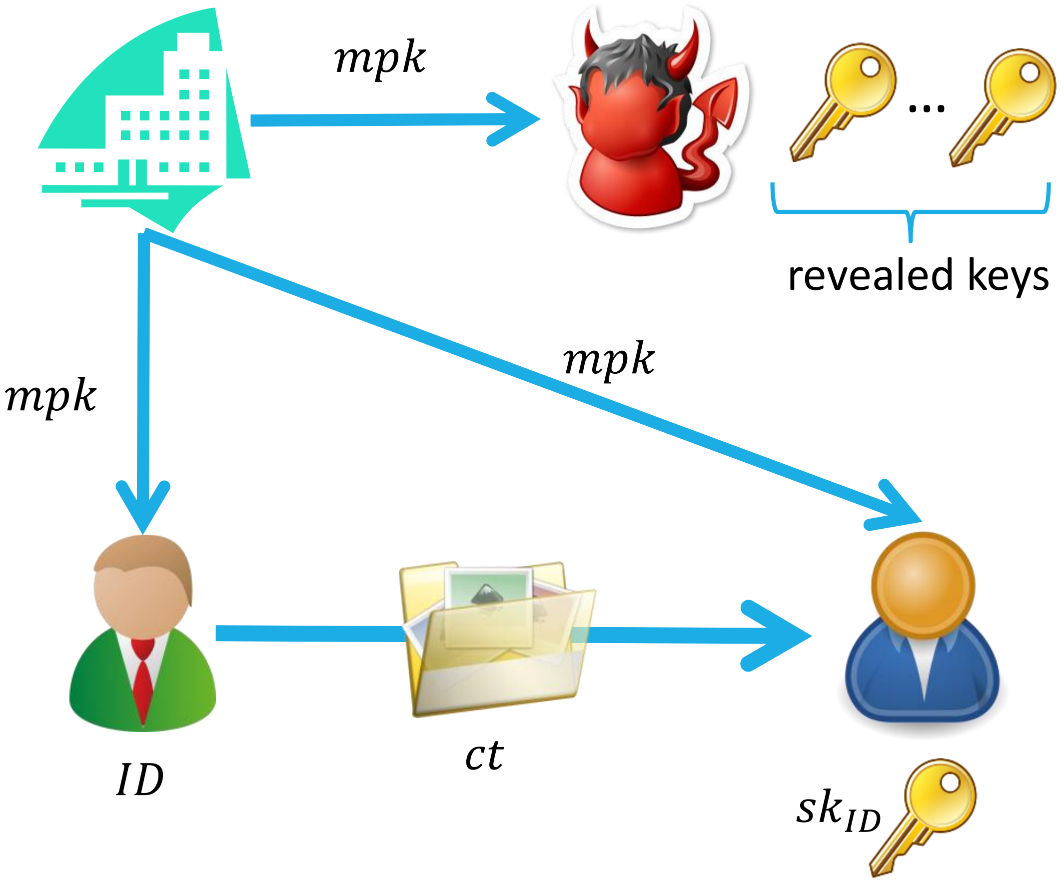
outline

- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

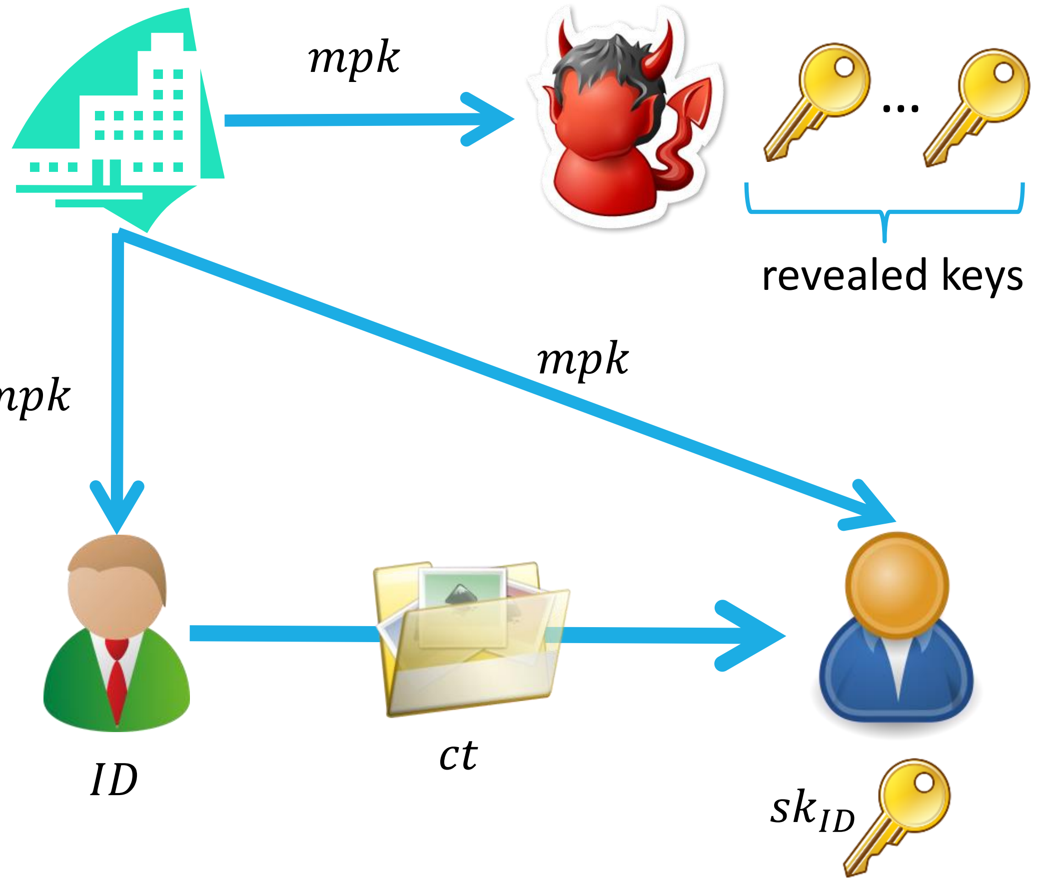
identity based encryption (IBE)

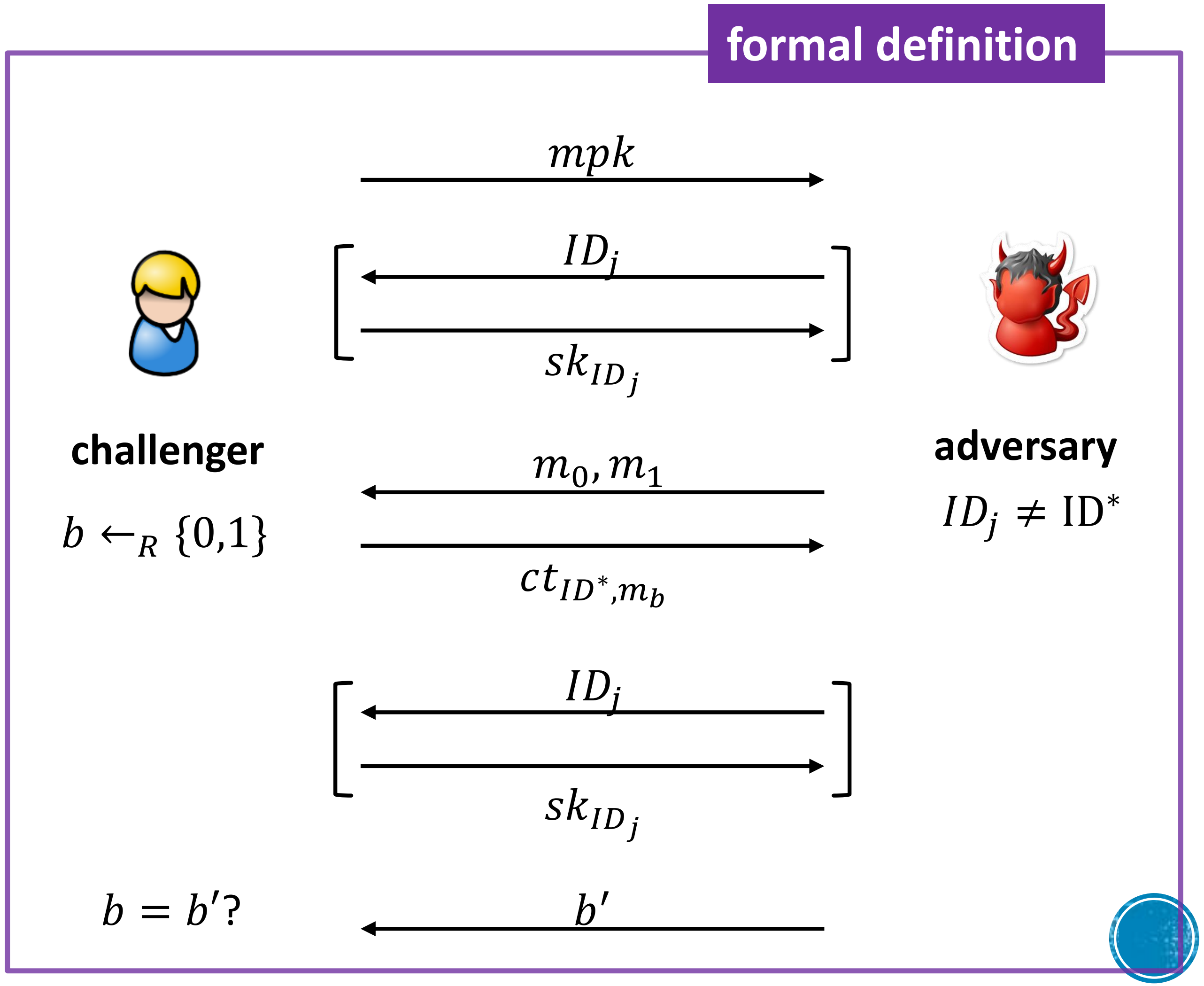


identity based encryption (IBE)

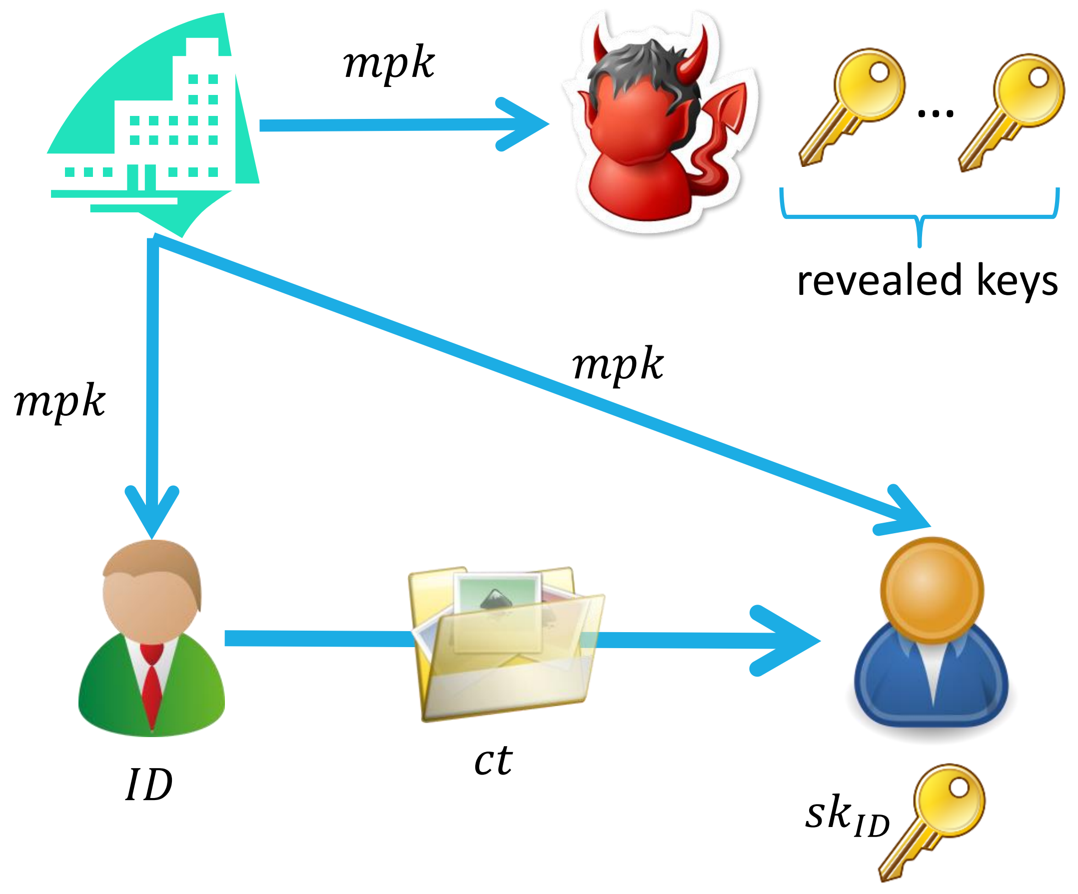


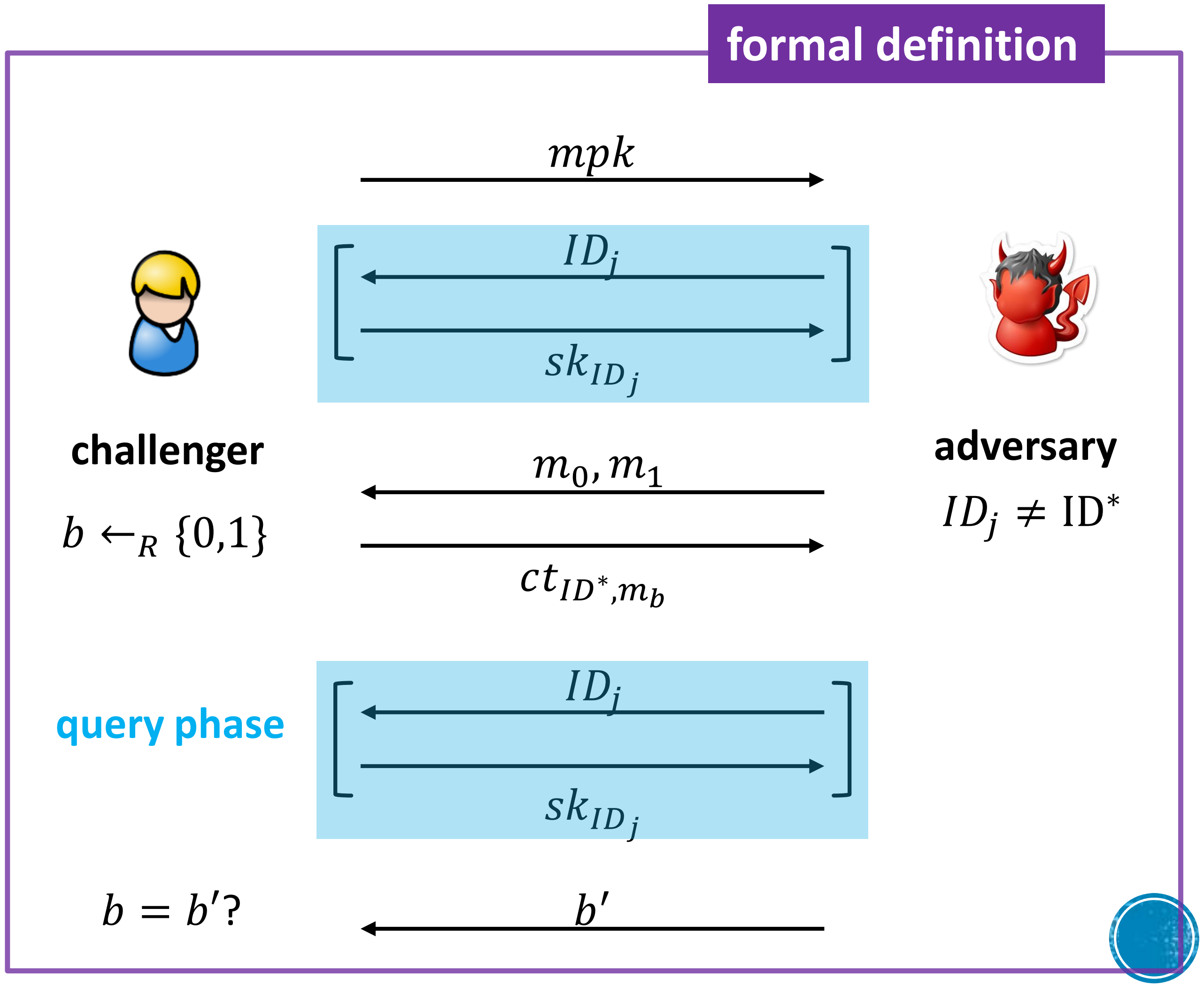
identity based encryption (IBE)



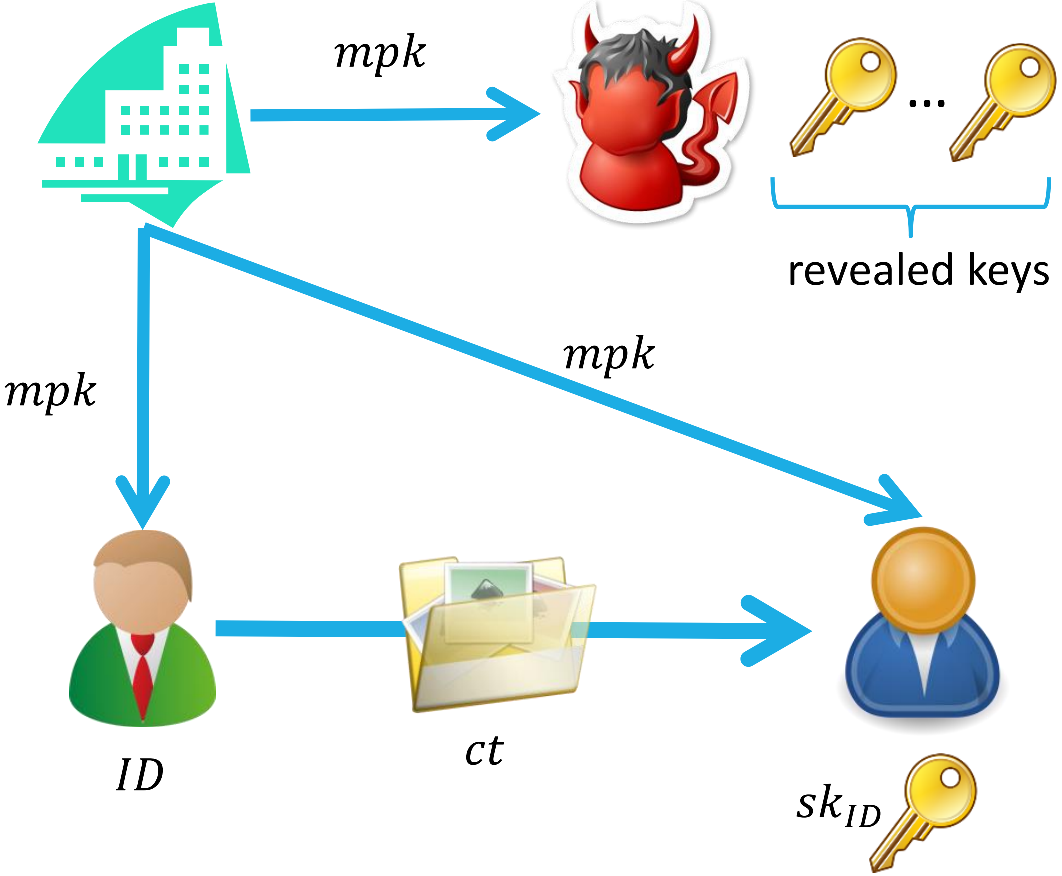


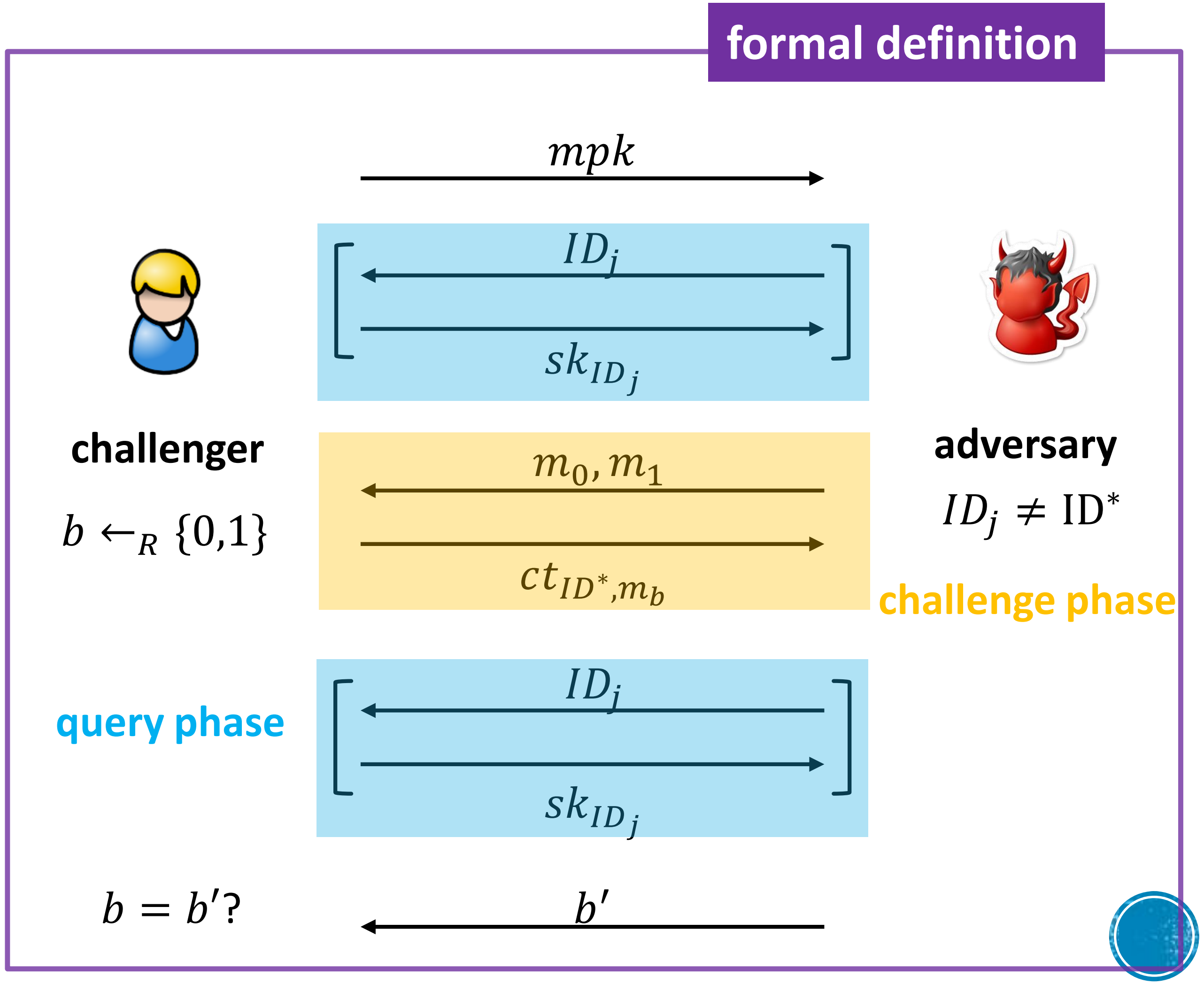
identity based encryption (IBE)





identity based encryption (IBE)





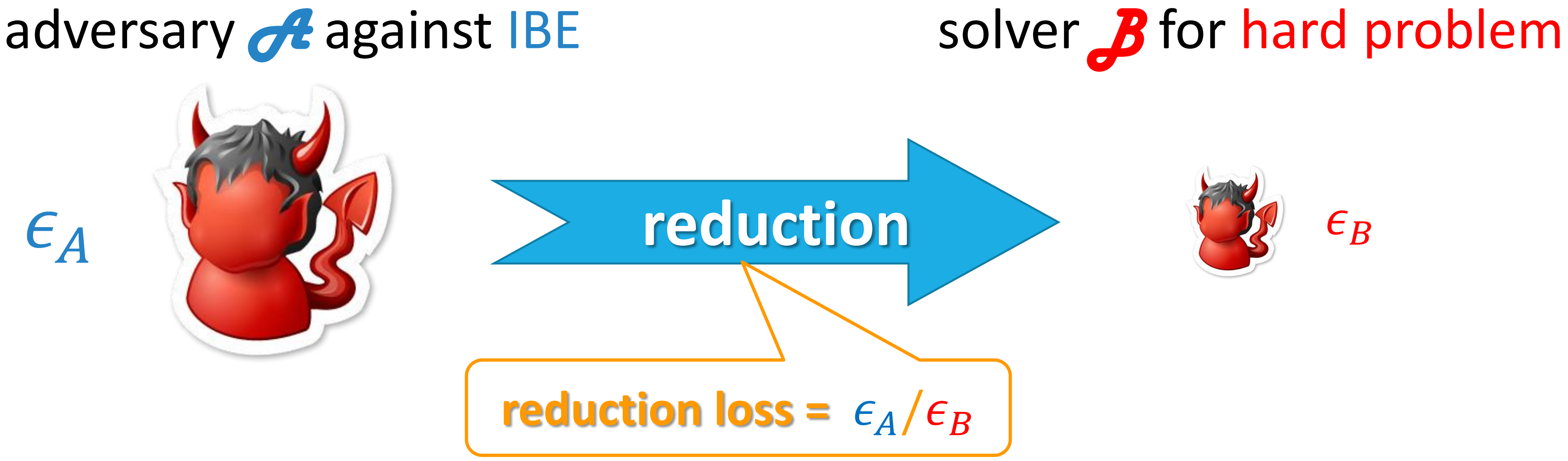
tight reduction

tight reduction

adversary $\mathcal{A}$ against IBE

solver $\mathcal{B}$ for hard problem

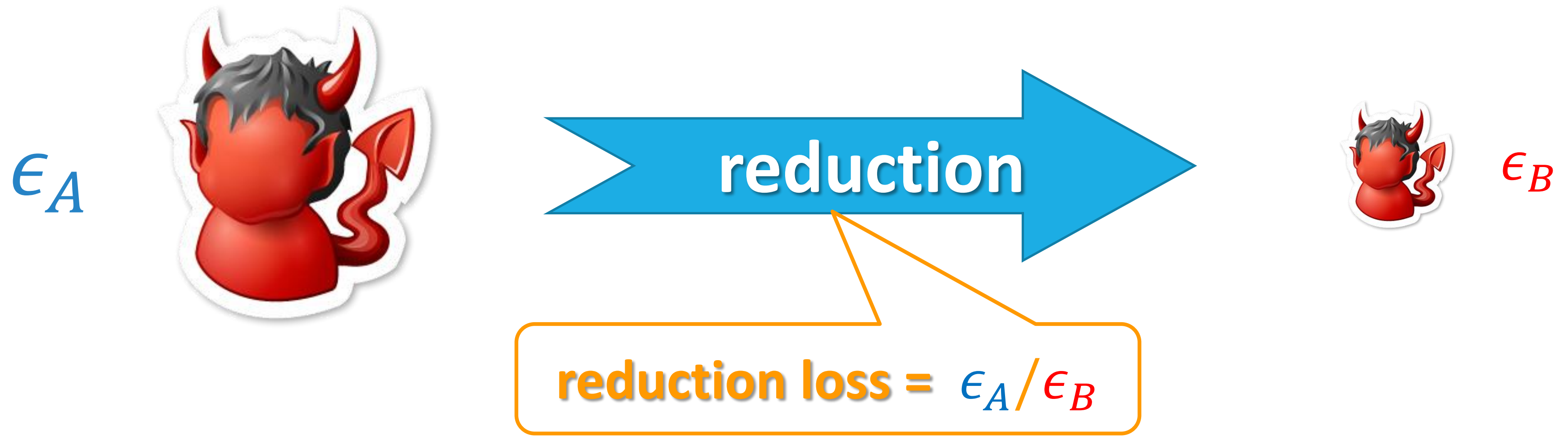
tight reduction



tight reduction

adversary $\mathcal{A}$ against IBE

solver $\mathcal{B}$ for hard problem



tighter reduction = smaller reduction loss

tight reduction

adversary $\mathcal{A}$ against IBE

solver $\mathcal{B}$ for hard problem

ϵ_A

reduction

ϵ_B

reduction loss = ϵ_A / ϵ_B

tighter reduction = smaller reduction loss

- better theoretical result
- more efficient implementation

multi-challenge setting

multi-challenge setting

multi-challenge setting

basic/single-challenge setting

+ multiple challenge queries: more than one challenge ct

+ multiple instances: multiple mpk

multi-challenge setting

multi-challenge setting

basic/single-challenge setting

+ multiple challenge queries: more than one challenge ct

+ multiple instances: multiple mpk

multi-challenge setting

multi-challenge setting

basic/single-challenge setting

+ multiple challenge queries: more than one challenge ct

+ multiple instances: multiple mpk

good news

single-challenge setting ⇒ multi-challenge setting

multi-challenge setting

multi-challenge setting

basic/single-challenge setting

+ multiple challenge queries: more than one challenge ct

+ multiple instances: multiple mpk

good news

single-challenge setting ⇒ multi-challenge setting

bad news

NOT tightness preserving

outline

- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	k-lin	2k + 2k
BKP14	no	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	3k + 3k
			stronger k-lin	2k + 2k

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
		composite & prime	k-lin	2k + 2k
BKP14	o	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	3k + 3k
			stronger k-lin	2k + 2k

more realistic

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
[illegible]	[illegible]	composite & prime	[illegible]	2k + 2k
BKP14	no	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	3k + 3k
			stronger k-lin	2k + 2k

more realistic

more efficient in general

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	k-lin	2k + 2k
BKP14	no	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	3k + 3k
			stronger k-lin	2k + 2k

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	k-lin	2k + 2k
BKP14	no	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	3k + 3k
			stronger k-lin	2k + 2k

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	k-lin	2k + 2k
BKP14	no	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	[illegible] + 3k
			stronger k-lin	2k + 2k

trade-off

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	k-lin	2k + 2k
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-li	+ 3k
			stronger k-lin	2k + 2k

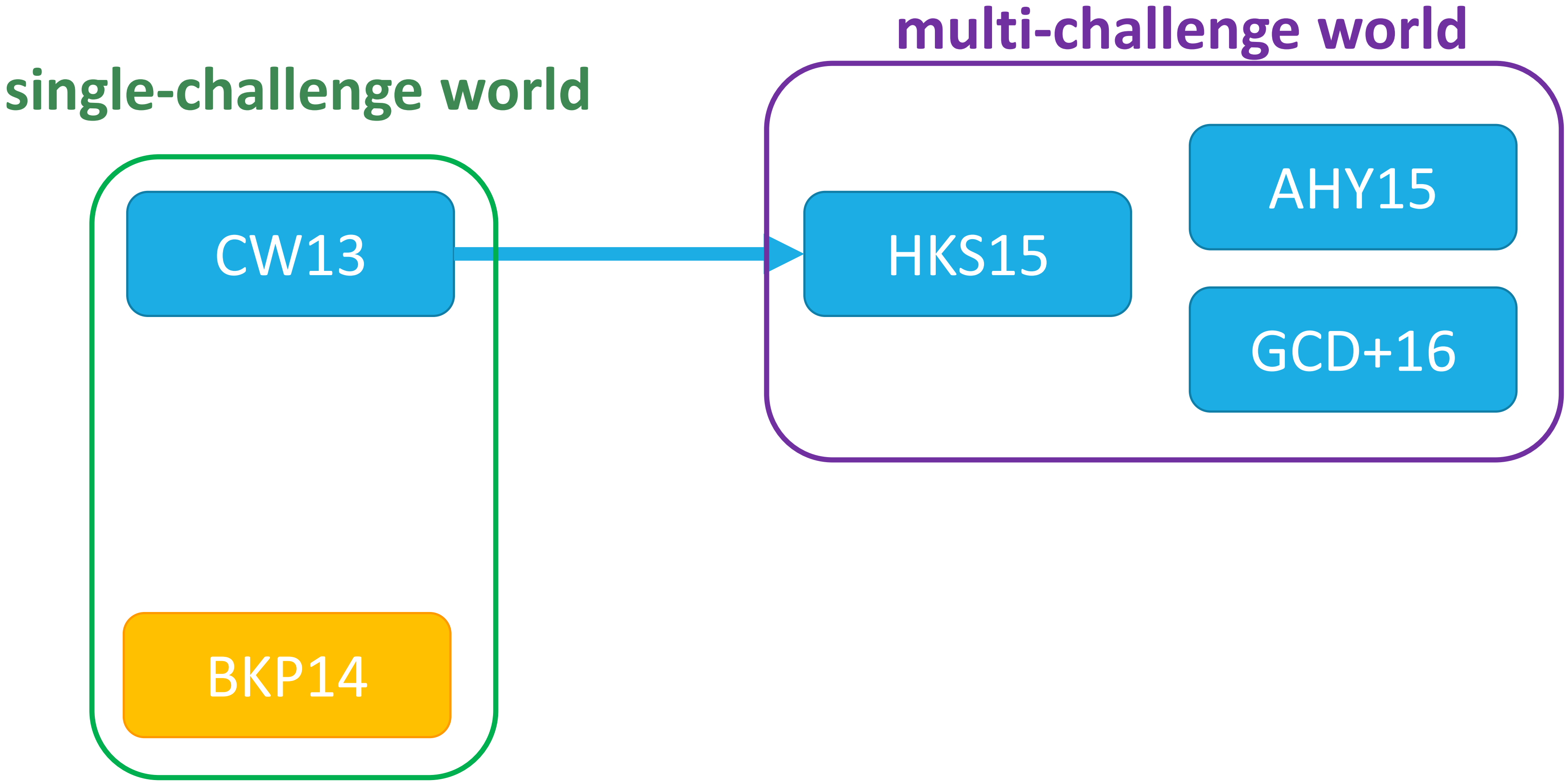
short ciphertext and weak/standard assumption simultaneously?

trade-off

outline

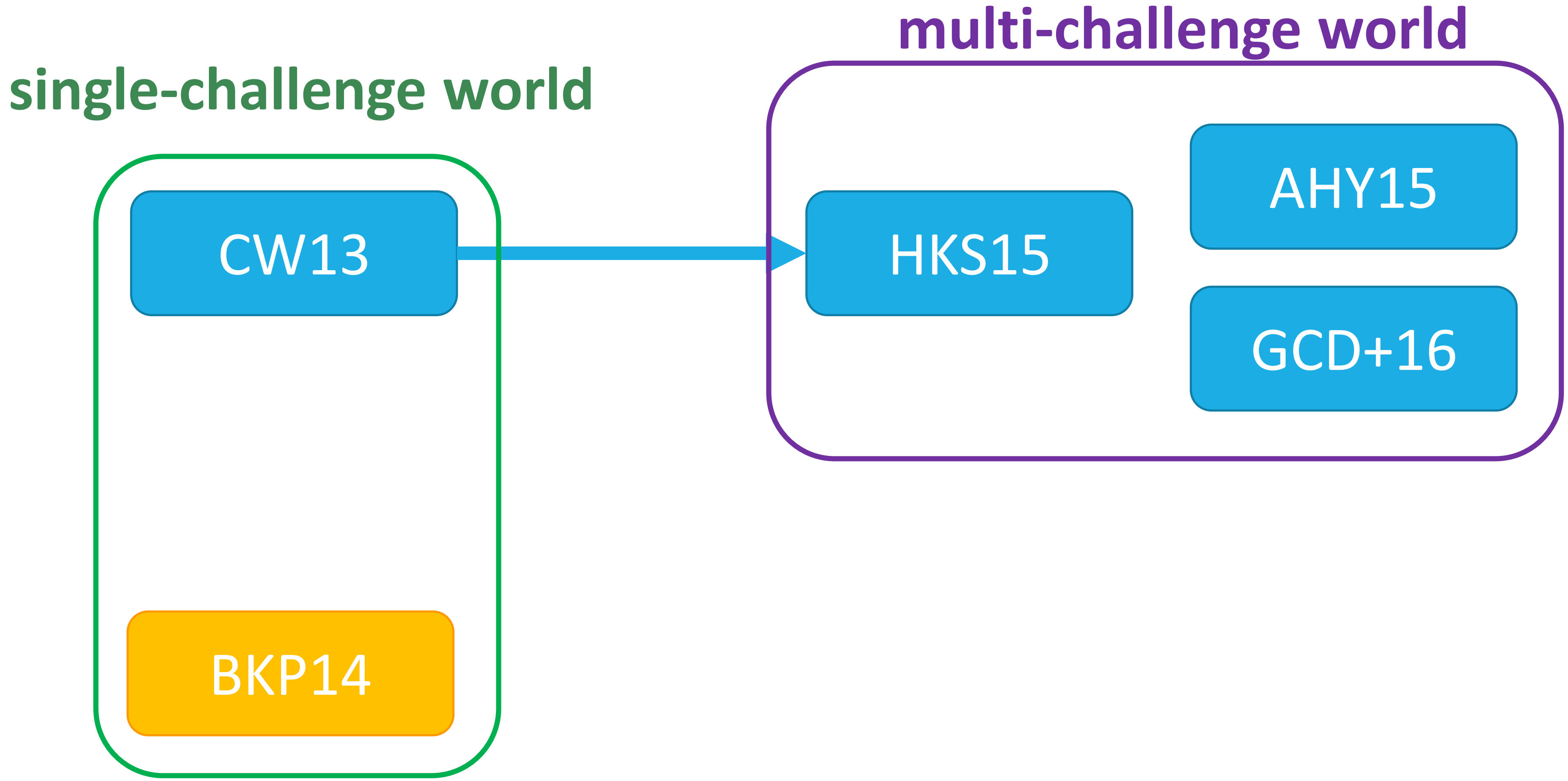
- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

big picture


multi-challenge world
single-challenge world
CW13
HKS15
AHY15
GCD+16
BKP14

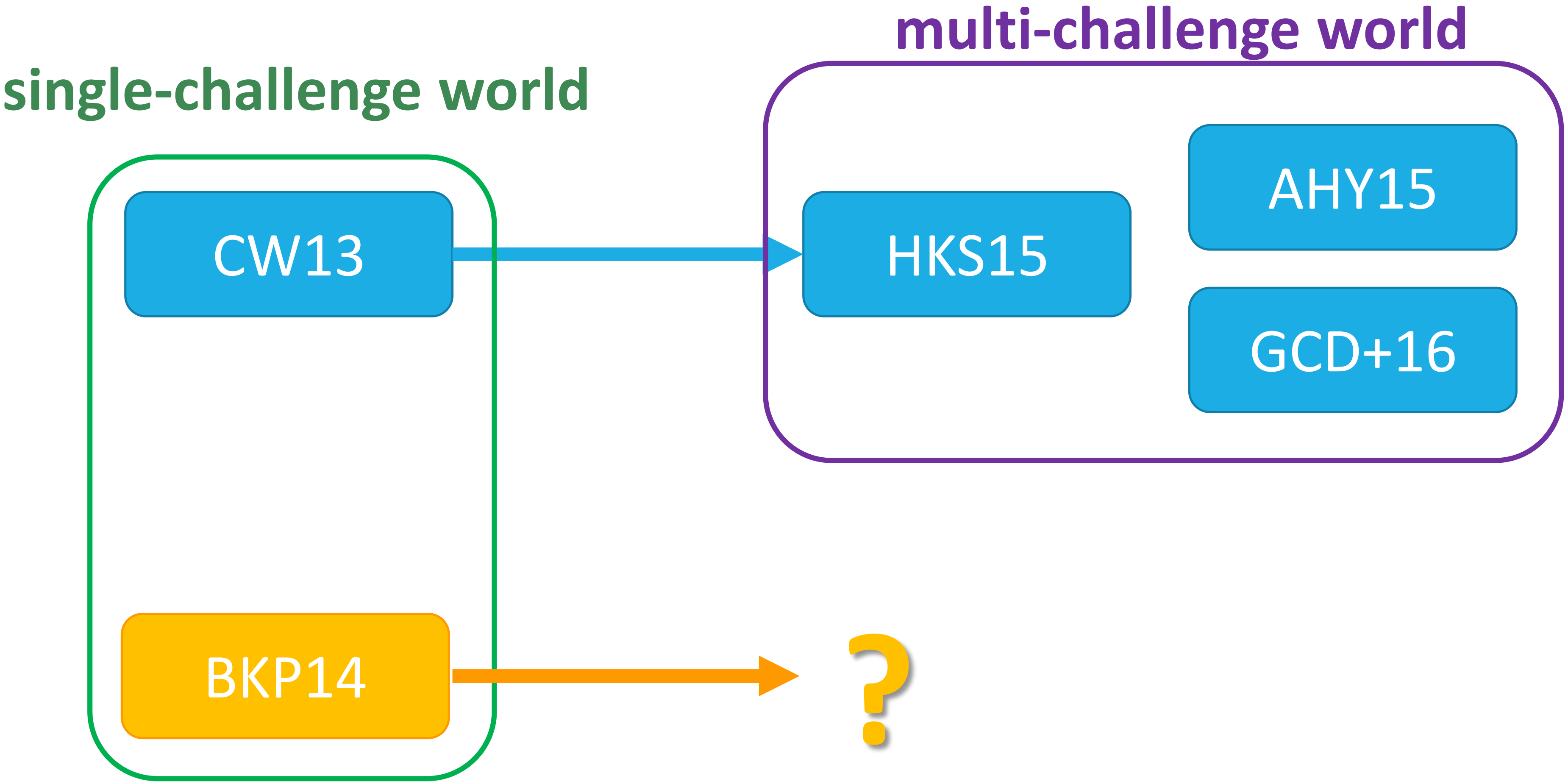
big picture

	assumption	ciphertext size
CW13	k-lin	2k + 2k
BKP14		k + (k+1) = 2k + 1



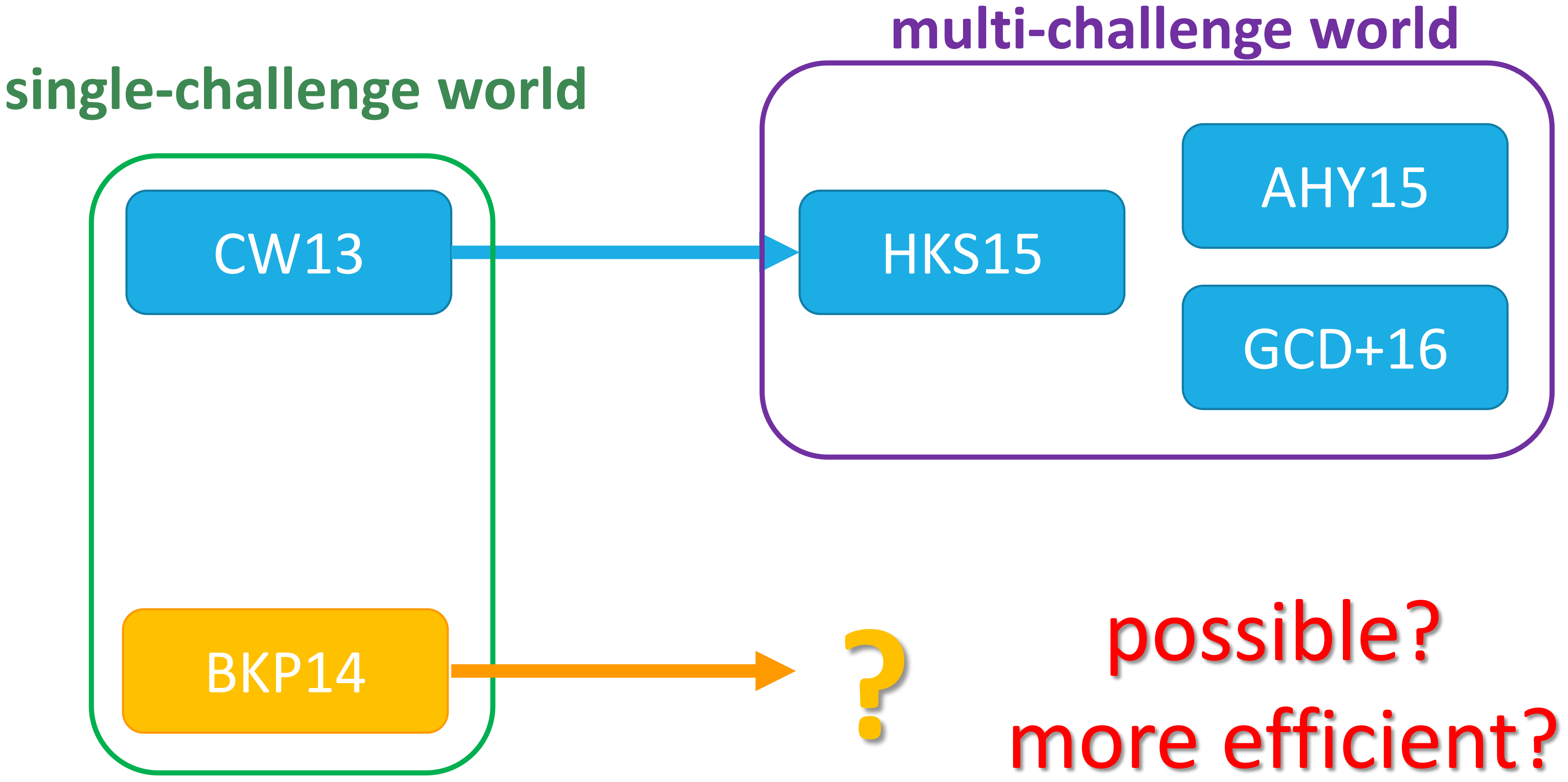
big picture

	assumption	ciphertext size
CW13	k-lin	2k + 2k
BKP14		k + (k+1) = 2k + 1



big picture

	assumption	ciphertext size
CW13	k-lin	2k + 2k
BKP14		k + (k+1) = 2k + 1



Blazy-Kiltz-Pan @ CRYPTO 14

affine MAC + Groth-Sahai proof = IBE

Blazy-Kiltz-Pan @ CRYPTO 14

IBE scheme

$$
\begin{aligned}
\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\
\mathrm{SK}_{\mathrm{ID}} &: [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2 \\
& \quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{Y}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top}\right]_2 \\
\mathrm{CT}_{\mathrm{ID}} &: [\mathbf{A}\mathbf{s}]_1, \quad \left[\textstyle\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]} \mathbf{s}\right]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}
\end{aligned}
$$

Blazy-Kiltz-Pan @ CRYPTO 14

IBE scheme

$$
\begin{aligned}
\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\
\mathrm{SK}_{\mathrm{ID}} &: [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2 \\
& \quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{Y}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top}\right]_2 \\
\mathrm{CT}_{\mathrm{ID}} &: [\mathbf{A}\mathbf{s}]_1, \quad \left[\textstyle\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]} \mathbf{s}\right]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}
\end{aligned}
$$

MAC tag for ID

Blazy-Kiltz-Pan @ CRYPTO 14

IBE scheme

commitment key

commitment to $\mathrm{SK}_{\mathrm{MAC}}$: $\mathbf{Z}_{i,b} = (\mathbf{Y}_{i,b}|\mathbf{x}_{i,b})\mathbf{A}$

$$\mathrm{MPK} : [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1$$

$$\mathrm{SK}_{\mathrm{ID}} : [\mathbf{k}_0]_2, \ [k_1]_2 = \left[\sum_{i=1}^n \mathbf{x}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + x\right]_2$$

$$[\mathbf{k}_2]_2 = \left[\sum_{i=1}^n \mathbf{Y}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + \mathbf{y}^\top\right]_2$$

$$\mathrm{CT}_{\mathrm{ID}} : [\mathbf{A}\mathbf{s}]_1, \quad \left[\sum_{i=1}^n \mathbf{Z}_{i,\mathrm{ID}[i]}\mathbf{s}\right]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}$$

MAC tag for ID

Blazy-Kiltz-Pan @ CRYPTO 14

IBE scheme

commitment key

commitment to SK_{MAC}: $\mathbf{Z}_{i,b} = (\mathbf{Y}_{i,b} | \mathbf{x}_{i,b})\mathbf{A}$

$$\begin{aligned} \text{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\ \text{SK}_{\text{ID}} &: [\mathbf{k}_0]_2, \; [k_1]_2 = \left[\textstyle\sum_{i=1}^n \mathbf{x}_{i,\text{ID}[i]}^\top \mathbf{k}_0 + x\right]_2 \\ & \quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^n \mathbf{Y}_{i,\text{ID}[i]}^\top \mathbf{k}_0 + \mathbf{y}^\top\right]_2 \\ \text{CT}_{\text{ID}} &: [\mathbf{As}]_1, \quad \left[\textstyle\sum_{i=1}^n \mathbf{Z}_{i,\text{ID}[i]}\mathbf{s}\right]_1, \quad [\mathbf{zs}]_T \cdot \text{M} \end{aligned}$$

MAC tag for ID

Groth-Sahai proof for correctness of the tag

Blazy-Kiltz-Pan @ CRYPTO 14

IBE scheme

they employ the dual system technique [Waters09], but

- normal and semi-functional space is **not** obvious
- **incompatible** with existing extension method

$$\begin{aligned}
\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\
\mathrm{SK}_{\mathrm{ID}} &: [\mathbf{k}_0]_2, \; [k_1]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2 \\
&\quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{Y}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top}\right]_2 \\
\mathrm{CT}_{\mathrm{ID}} &: [\mathbf{A}\mathbf{s}]_1, \quad \left[\textstyle\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]} \mathbf{s}\right]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}
\end{aligned}$$

outline

- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

clues in the proof

$$\mathrm{MPK} \; : \; [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1$$

$$\mathrm{SK}_{\mathrm{ID}} \; : \; [\mathbf{k}_0]_2, \; [k_1]_2 = \left[\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2$$

$$[\mathbf{k}_2]_2 = \left[\sum_{i=1}^{n} \mathbf{Y}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top}\right]_2$$

$$\mathrm{CT}_{\mathrm{ID}} \; : \; [\mathbf{A}\mathbf{s}]_1, \quad \left[\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]} \mathbf{s}\right]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}$$

clues in the proof

$$\text{MPK} : [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1$$

$$\text{SK}_{\text{ID}} : [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\sum_{i=1}^{n} \mathbf{x}_{i,\text{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2$$

$$[\mathbf{k}_2]_2 = \left[\sum_{i=1}^{n} \mathbf{Y}_{i,\text{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top}\right]_2$$

$$\text{CT}_{\text{ID}} : [\mathbf{A}\mathbf{s}]_1,\quad \left[\sum_{i=1}^{n} \mathbf{Z}_{i,\text{ID}[i]}\mathbf{s}\right]_1,\quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}$$

k-lin assumption

$$[\mathbf{A}\mathbf{s} + \boxed{h} \cdot \mathbf{e}_{k+1}]_1,\ \left[\sum_{i=1}^{n} \mathbf{Z}_{i,\text{ID}^*[i]}\mathbf{s} + \boxed{h \cdot \sum_{i=1}^{n} \mathbf{x}_{i,\text{ID}^*[i]}}\right]_1,\ [\mathbf{z}\mathbf{s} + \boxed{h \cdot x}]_T \cdot \mathrm{M}$$

clues in the proof

$$\mathrm{MPK}\ :\ [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1$$

$$\mathrm{SK_{ID}}\ :\ [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\textstyle\sum_{i=1}^n \mathbf{x}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + x\right]_2$$

$$[\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^n \mathbf{Y}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + \mathbf{y}^\top\right]_2$$

a simple substitution

$$\mathbf{k}_2 = \overline{\mathbf{A}}^* \cdot \left(\textstyle\sum_{i=1}^n \mathbf{Z}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + \mathbf{z}^\top - k_1 \underline{\mathbf{A}}^\top\right)$$

$$\mathrm{CT_{ID}}\ :\ [\mathbf{A}\mathbf{s}]_1,\quad \left[\textstyle\sum_{i=1}^n \mathbf{Z}_{i,\mathrm{ID}[i]}\mathbf{s}\right]_1,\quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}$$

k-lin assumption

$$[\mathbf{A}\mathbf{s} + \boxed{h} \cdot \mathbf{e}_{k+1}]_1,\ \left[\textstyle\sum_{i=1}^n \mathbf{Z}_{i,\mathrm{ID}^*[i]}\mathbf{s} + \boxed{h \cdot \textstyle\sum_{i=1}^n \mathbf{x}_{i,\mathrm{ID}^*[i]}}\right]_1,\ [\mathbf{z}\mathbf{s} + \boxed{h \cdot x}]_T \cdot \mathrm{M}$$

clues in the proof

$\mathrm{MPK} \; : \; [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1$

$\mathrm{SK}_{\mathrm{ID}} \; : \; [\mathbf{k}_0]_2, \; [k_1]_2 = \left[\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x \right]_2$

~~$[\mathbf{k}_2]_2 = \left[\sum_{i=1}^{n} \mathbf{X}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top} \right]_2$~~

a simple substitution

$$\mathbf{k}_2 = \overline{\mathbf{A}}^{*} \cdot \left(\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{z}^{\top} - k_1 \underline{\mathbf{A}}^{\top} \right)$$

$\mathrm{CT}_{\mathrm{ID}} \; :$ ~~$[\mathbf{As}]_1, \left[\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]} \mathbf{s} \right]_1, [\mathbf{zs}]_T \cdot \mathrm{M}$~~

k-lin assumption

$$[\mathbf{As} + \boxed{h} \cdot \mathbf{e}_{k+1}]_1, \; \left[\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}^*[i]} \mathbf{s} + \boxed{h \cdot \sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}^*[i]}} \right]_1, \; [\mathbf{zs} + \boxed{h \cdot x}]_T \cdot \mathrm{M}$$

clues in the proof

MPK : $[\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1$

$\mathrm{SK}_{\mathrm{ID}}$: $[\mathbf{k}_0]_2,\ [k_1]_2 = \left[\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2$

[redacted]

a simple substitution

$$\mathbf{k}_2 = \overline{\mathbf{A}}^* \cdot \left(\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{z}^{\top} - k_1 \underline{\mathbf{A}}^{\top}\right)$$

$\mathrm{CT}_{\mathrm{ID}}$: [redacted]

k-lin assumption

$$[\mathbf{A}\mathbf{s} + \boxed{h} \cdot \mathbf{e}_{k+1}]_1,\ \left[\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}^*[i]} \mathbf{s} + \boxed{h \cdot \sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}^*[i]}}\right]_1,\ [\mathbf{z}\mathbf{s} + \boxed{h \cdot x}]_T \cdot \mathrm{M}$$

Observation

- ✓ no $\mathbf{Y}_{i,b}$;
- ✓ $\mathbf{Z}_{i,b}$ are in the normal space;
- ✓ $\mathbf{x}_{i,b}$ are in the SF space.

transformation

$$
\begin{aligned}
\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\
\mathrm{SK}_{\mathrm{ID}} &: [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + x\right]_2 \\
&\quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{Y}_{i,\mathrm{ID}[i]}^{\top} \mathbf{k}_0 + \mathbf{y}^{\top}\right]_2 \\
\mathrm{CT}_{\mathrm{ID}} &: [\mathbf{A}\mathbf{s}]_1, \quad \left[\textstyle\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]} \mathbf{s}\right]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}
\end{aligned}
$$

Blazy-Kiltz-Pan IBE

transformation

$$\begin{aligned}
\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\
\mathrm{SK}_{\mathrm{ID}} &: [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\textstyle\sum_{i=1}^n \mathbf{x}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + x\right]_2 \\
&\quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^n \mathbf{Y}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + \mathbf{y}^\top\right]_2 \\
\mathrm{CT}_{\mathrm{ID}} &: [\mathbf{A}\mathbf{s}]_1,\quad \left[\textstyle\sum_{i=1}^n \mathbf{Z}_{i,\mathrm{ID}[i]}\mathbf{s}\right]_1,\quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}
\end{aligned}$$

Blazy-Kiltz-Pan IBE

2 define $\mathbf{Z}_{i,b} = \mathbf{W}_{i,b}\mathbf{A}$, $\mathbf{x}_{i,b} = \mathbf{W}_{i,b}\mathbf{e}_{k+1}$.

1 rewrite $\begin{bmatrix}\mathbf{k}_2 \\ k_1\end{bmatrix}_2 = \left[\sum_{i=1}^{n} (\mathbf{A}|\mathbf{e}_{k+1})^* \begin{pmatrix}\mathbf{Z}_{i,\mathrm{ID}[i]}^\top \\ \mathbf{x}_{i,\mathrm{ID}[i]}^\top\end{pmatrix} \mathbf{k}_0\right]_2$

transformation

$$\begin{aligned}\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 \\ \mathrm{SK_{ID}} &: [\mathbf{k}_0]_2,\ [k_1]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{x}_{i,\mathrm{ID}[i]}^{\top}\mathbf{k}_0 + x\right]_2 \\ &\quad [\mathbf{k}_2]_2 = \left[\textstyle\sum_{i=1}^{n} \mathbf{Y}_{i,\mathrm{ID}[i]}^{\top}\mathbf{k}_0 + \mathbf{y}^{\top}\right]_2 \\ \mathrm{CT_{ID}} &: [\mathbf{A}\mathbf{s}]_1,\ \left[\textstyle\sum_{i=1}^{n} \mathbf{Z}_{i,\mathrm{ID}[i]}\mathbf{s}\right]_1,\ [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M}\end{aligned}$$

Blazy-Kiltz-Pan IBE

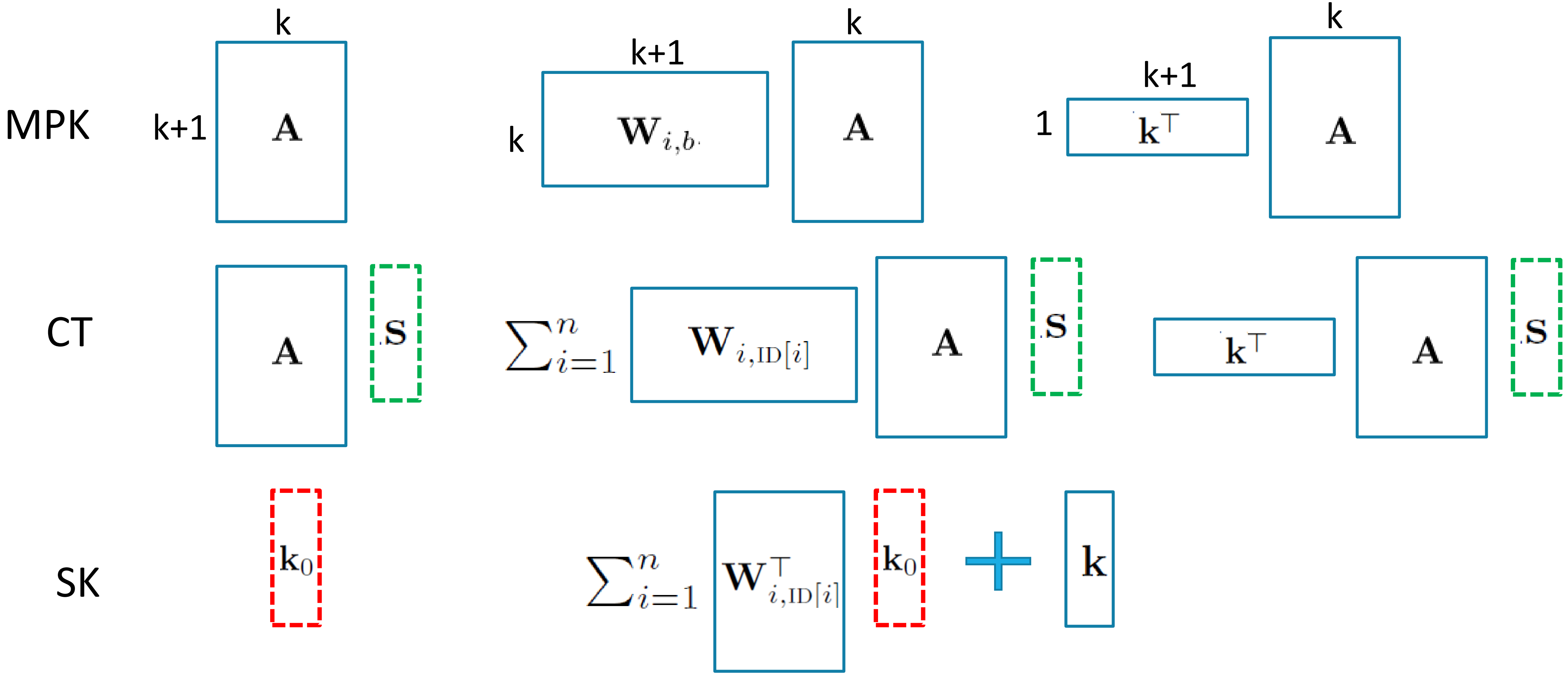
1 rewrite $\begin{bmatrix}\mathbf{k}_2 \\ k_1\end{bmatrix}_2 = \left[\sum_{i=1}^{n}(\mathbf{A}|\mathbf{e}_{k+1})^{*}\begin{pmatrix}\mathbf{Z}_{i,\mathrm{ID}[i]}^{\top} \\ \mathbf{x}_{i,\mathrm{ID}[i]}^{\top}\end{pmatrix}\mathbf{k}_0\right]_2$

2 define $\mathbf{Z}_{i,b} = \mathbf{W}_{i,b}\mathbf{A}$, $\mathbf{x}_{i,b} = \mathbf{W}_{i,b}\mathbf{e}_{k+1}$

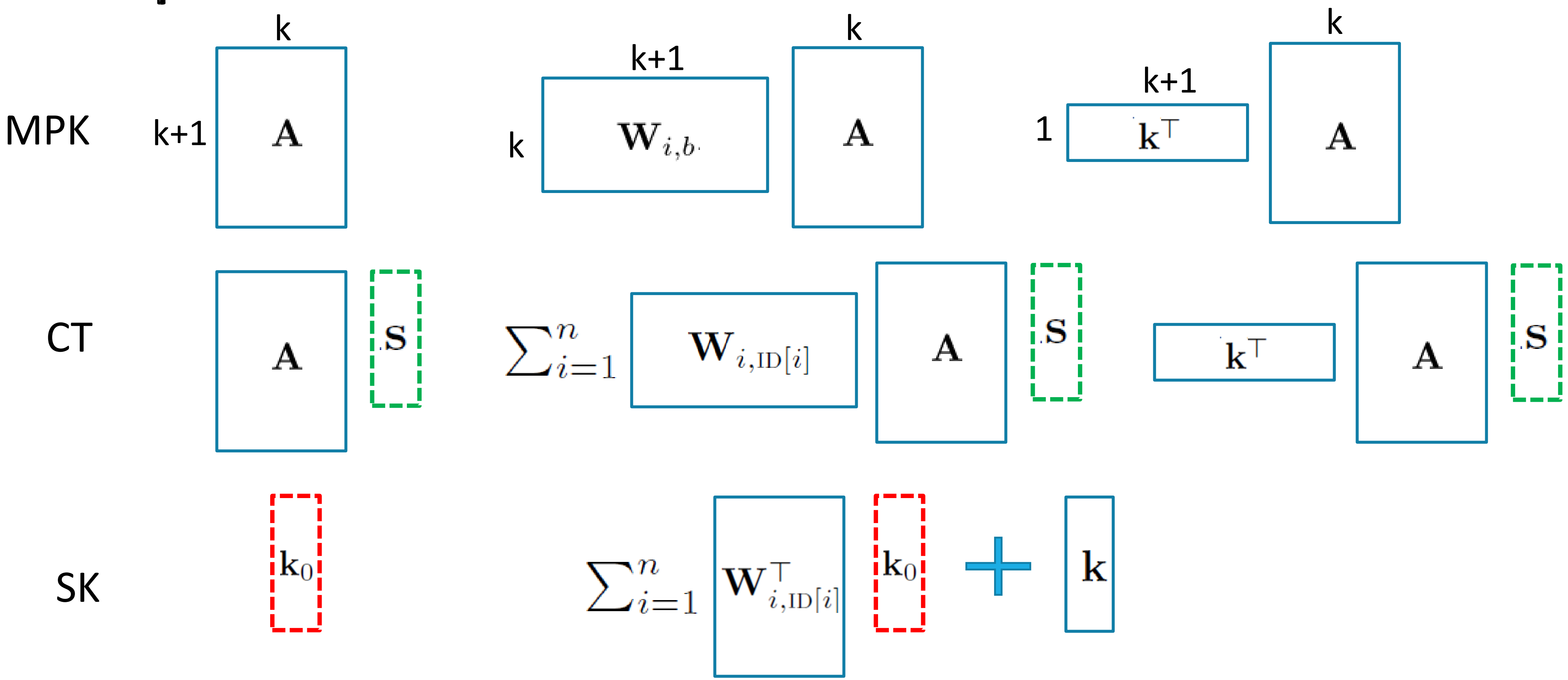
Our simplified version

$$\begin{aligned}\mathrm{MPK} &: [\mathbf{A}]_1, [\mathbf{W}_{1,0}\mathbf{A}]_1, [\mathbf{W}_{1,1}\mathbf{A}]_1, \ldots, [\mathbf{W}_{n,0}\mathbf{A}]_1, [\mathbf{W}_{n,1}\mathbf{A}]_1, [\mathbf{A}^{\top}\mathbf{k}]_T \\ \mathrm{CT_{ID}} &: [\mathbf{A}\mathbf{s}]_1, \left[\textstyle\sum_{i=1}^{n} \mathbf{W}_{i,\mathrm{ID}[i]}\mathbf{A}\mathbf{s}\right]_1, [\mathbf{s}^{\top}\mathbf{A}^{\top}\mathbf{k}]_T \cdot \mathrm{M} \\ \mathrm{SK_{ID}} &: [\mathbf{k}_0]_2, \left[\textstyle\sum_{i=1}^{n} \mathbf{W}_{i,\mathrm{ID}[i]}^{\top}\mathbf{k}_0 + \mathbf{k}\right]_2\end{aligned}$$

simplified BKP14



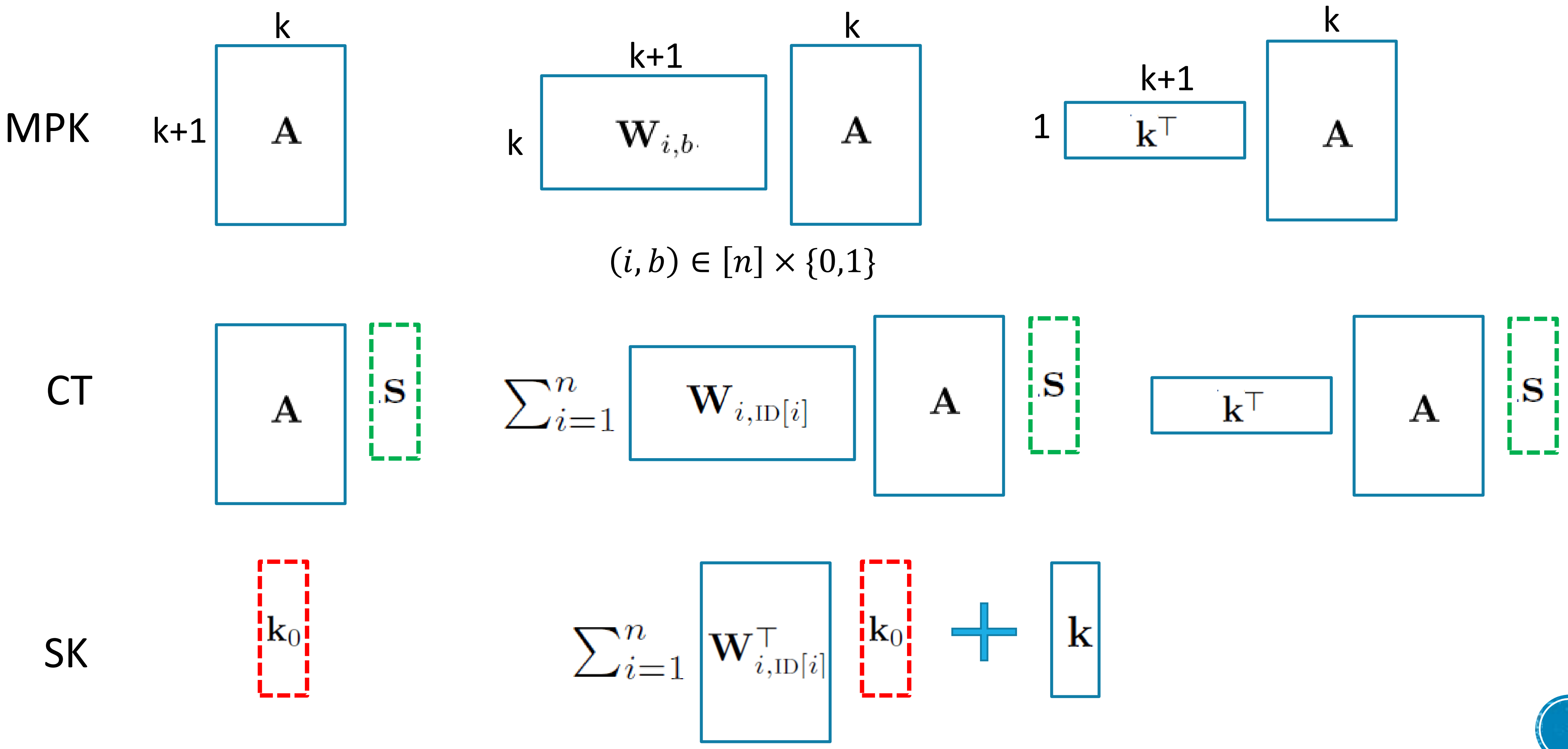
simplified BKP14 is similar to CGW15



[CGW15] *J. Chen, R. Gay, H. Wee.* Improved Dual System ABE in Prime-Order Groups via Predicate Encodings. EUROCRYPT 2015.

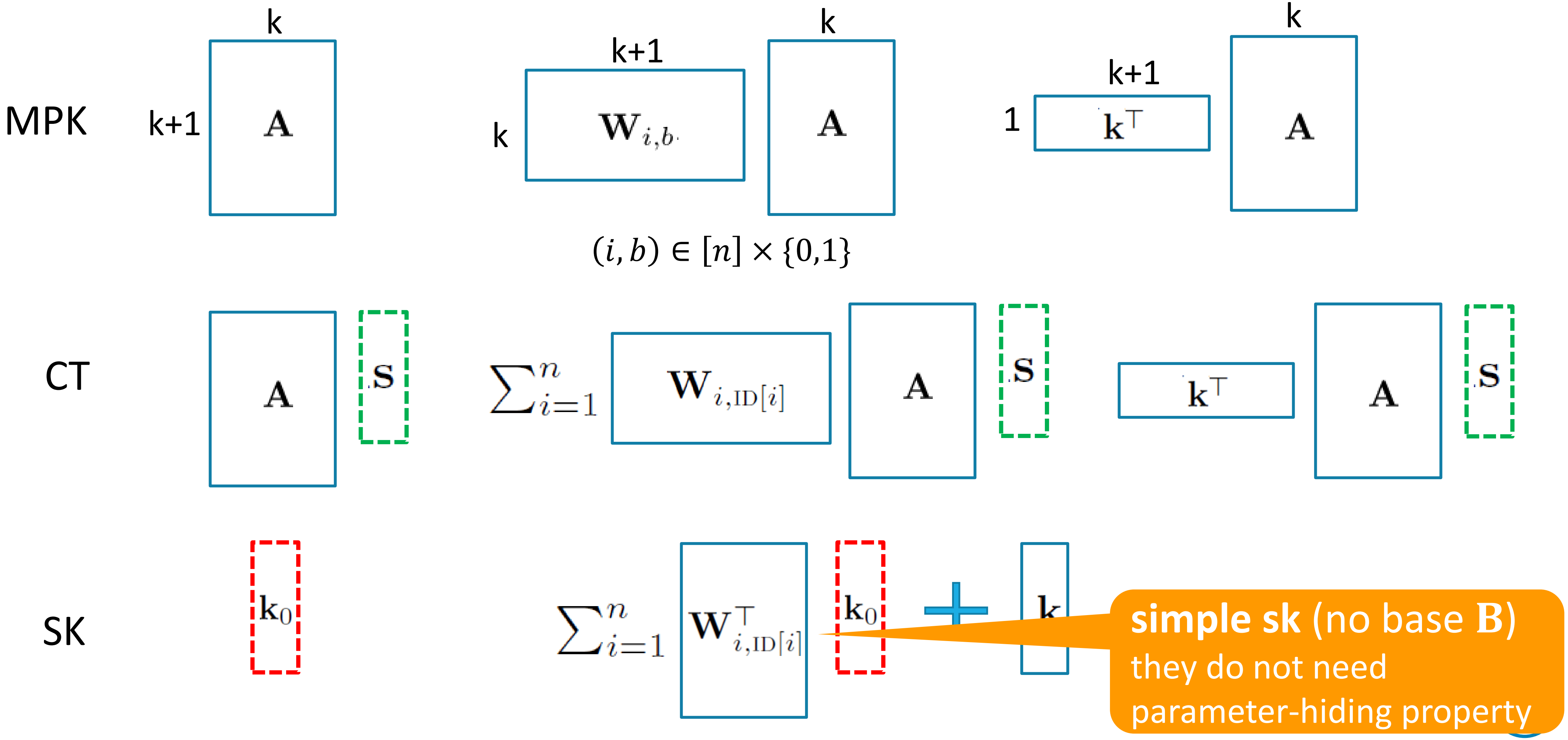
more than simplicity

why BKP14 is better than CW13?



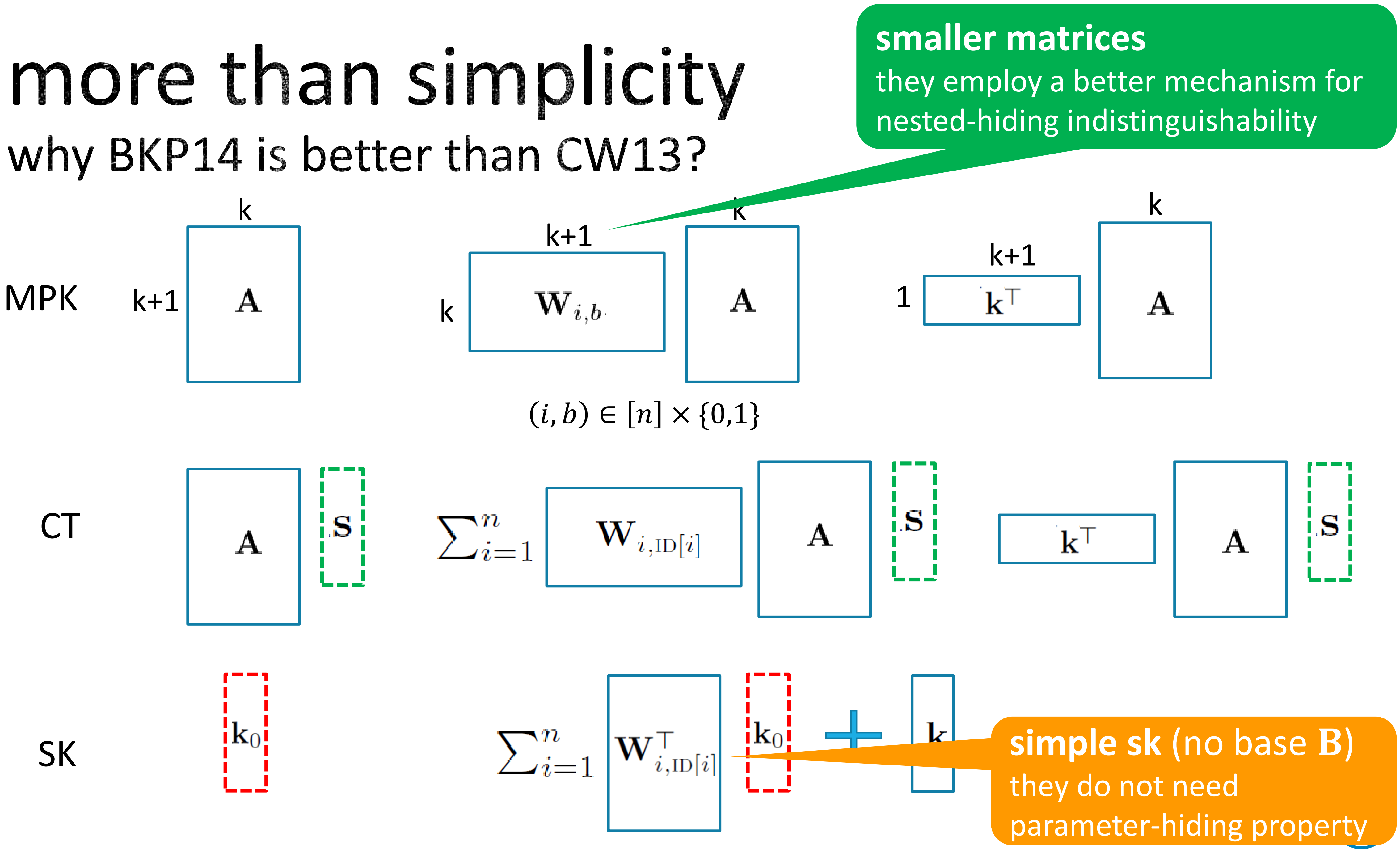
more than simplicity

why BKP14 is better than CW13?



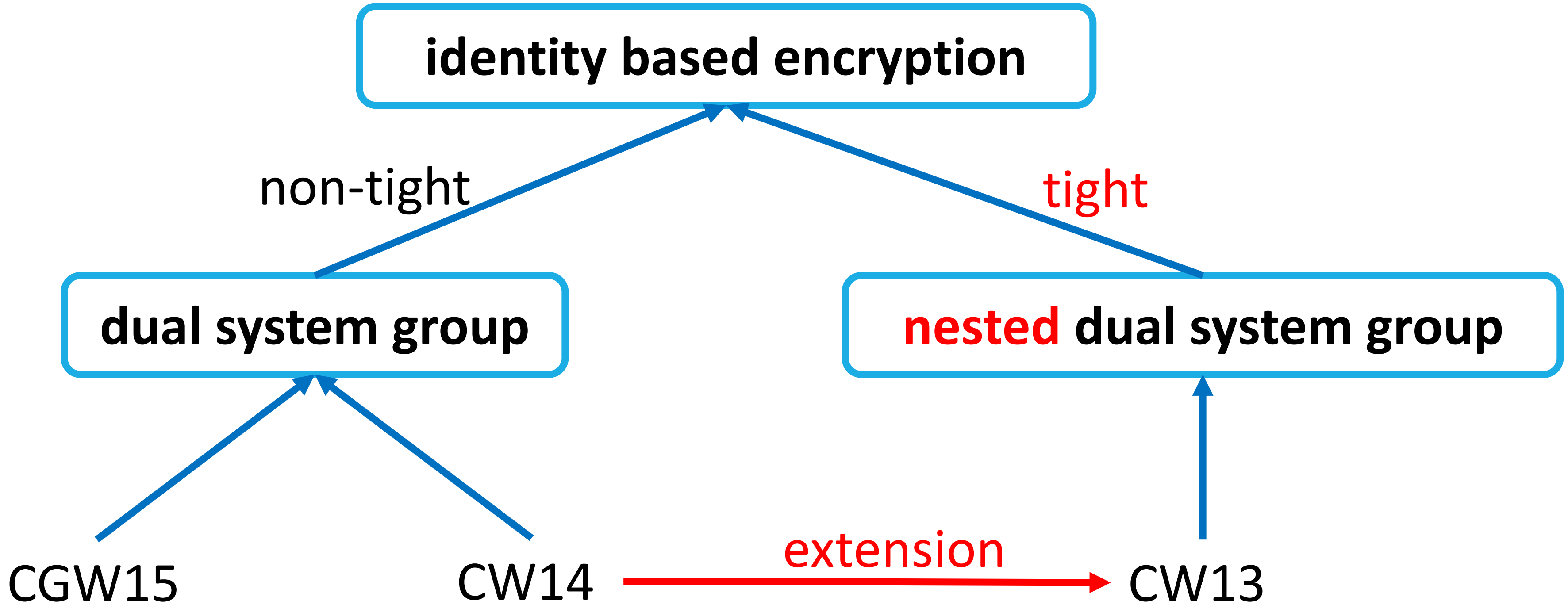
more than simplicity

why BKP14 is better than CW13?

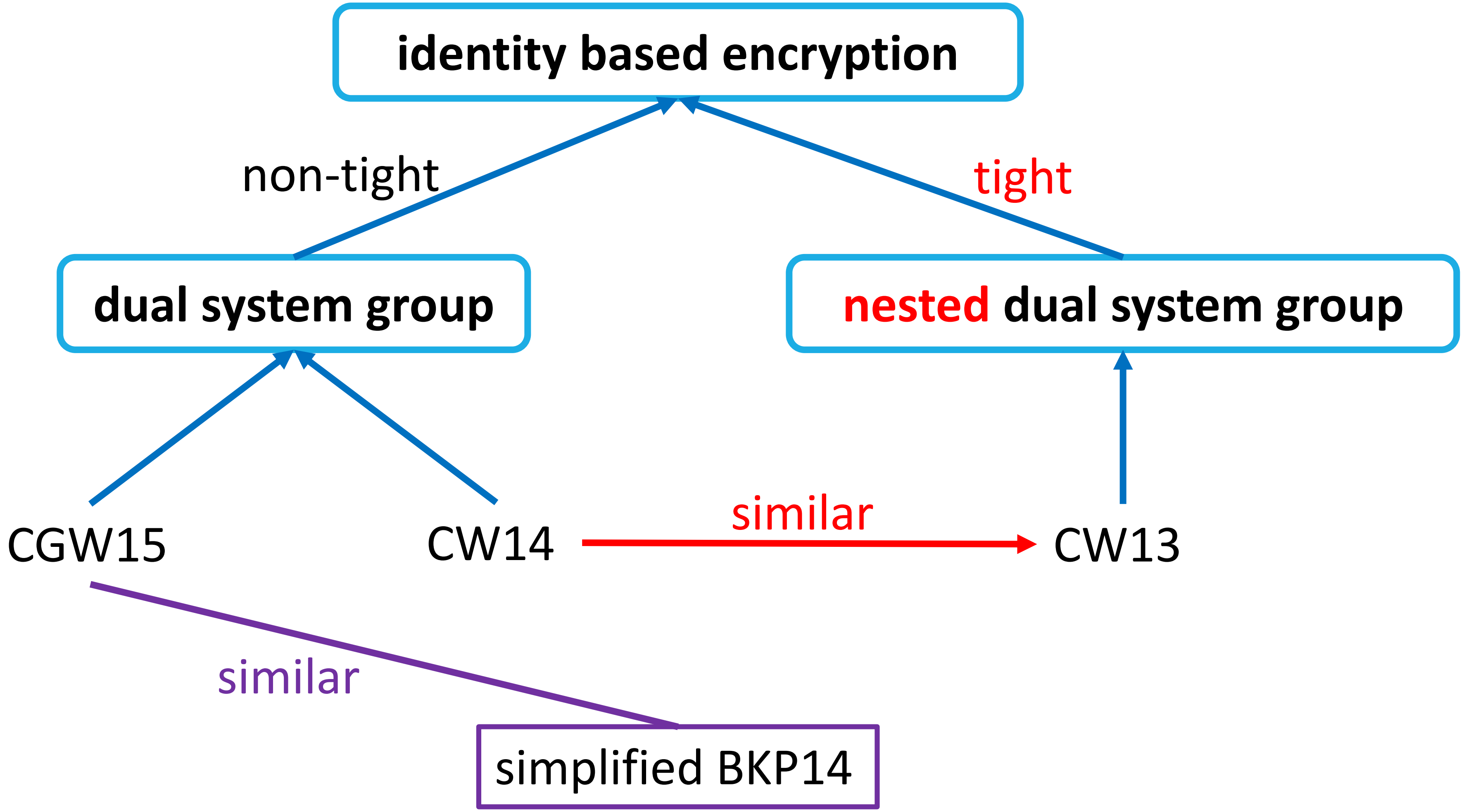


let’s be formal

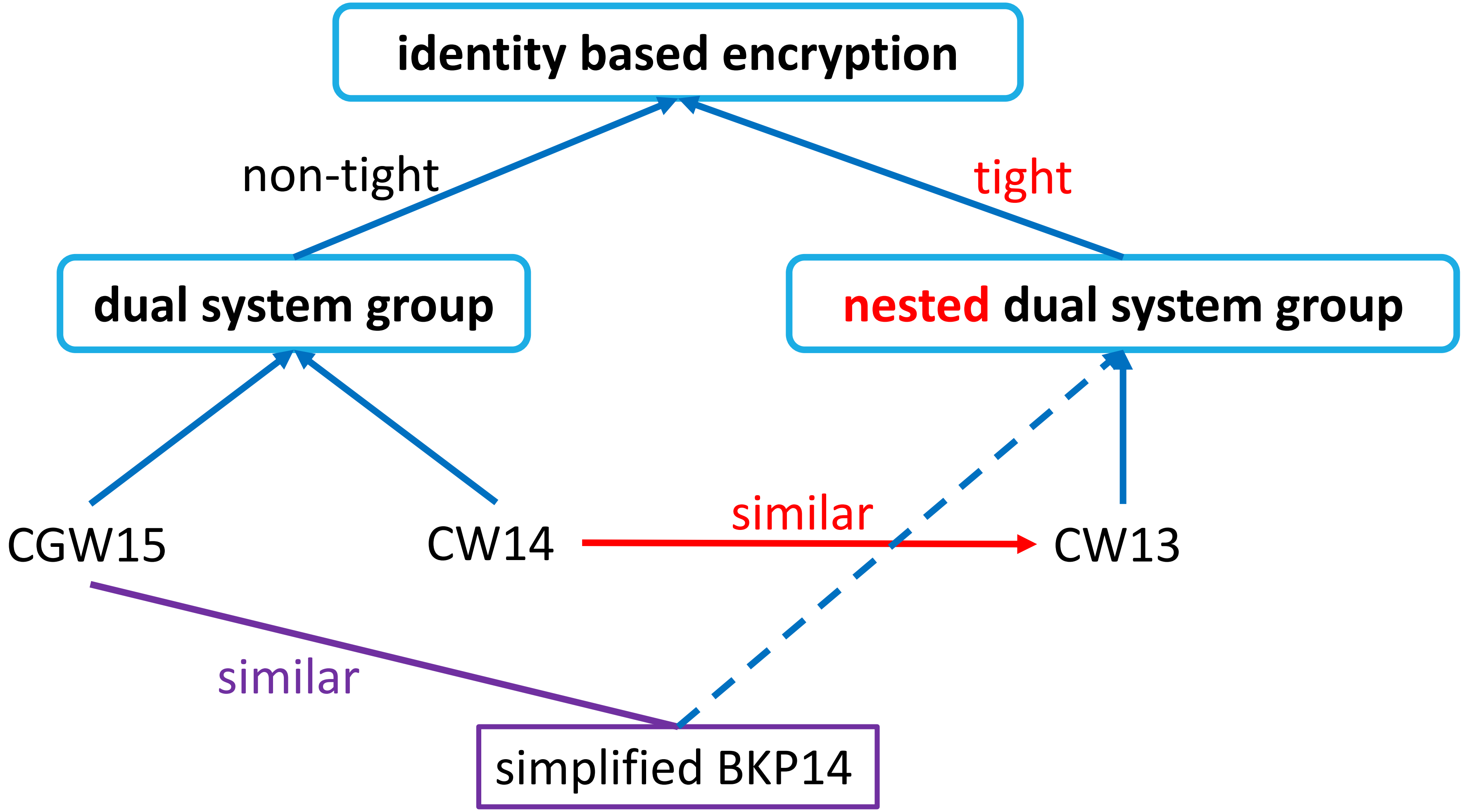
let's be formal



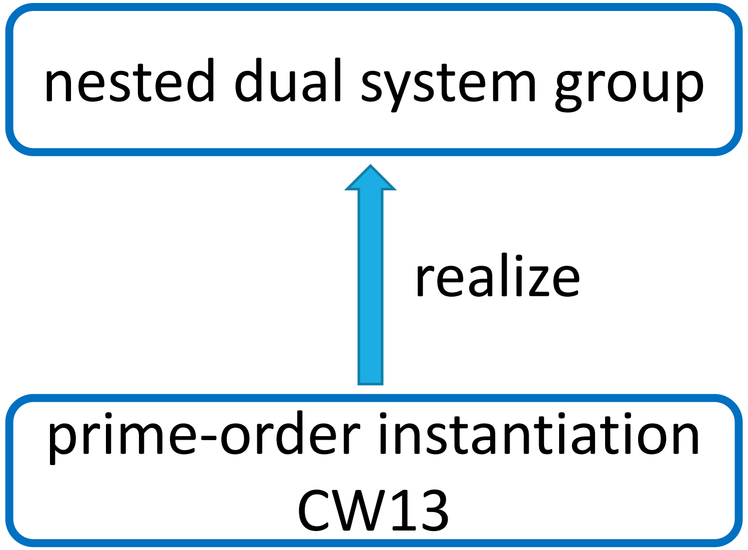
let's be formal



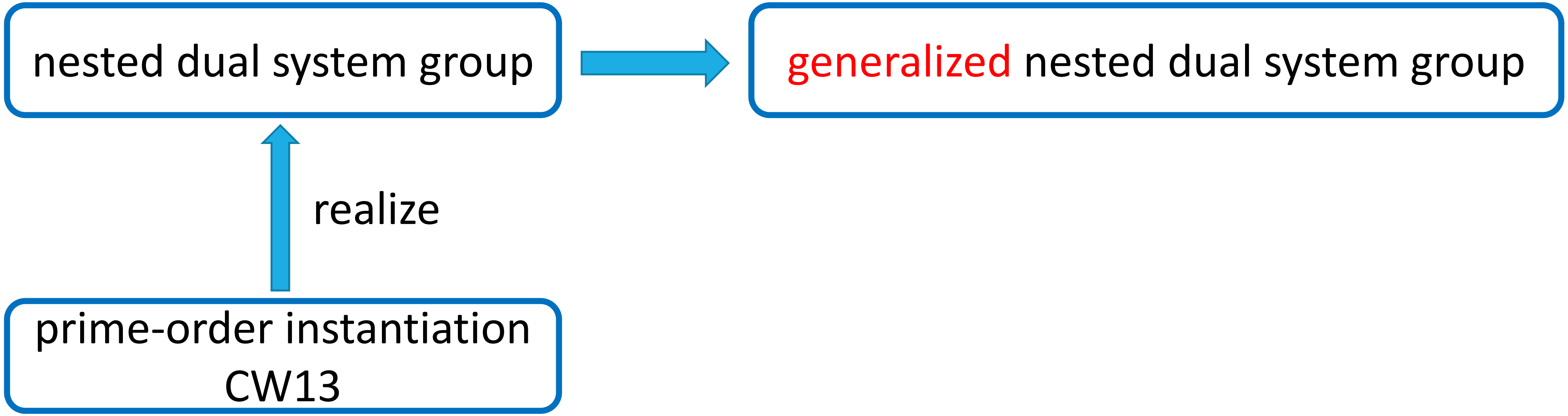
let's be formal



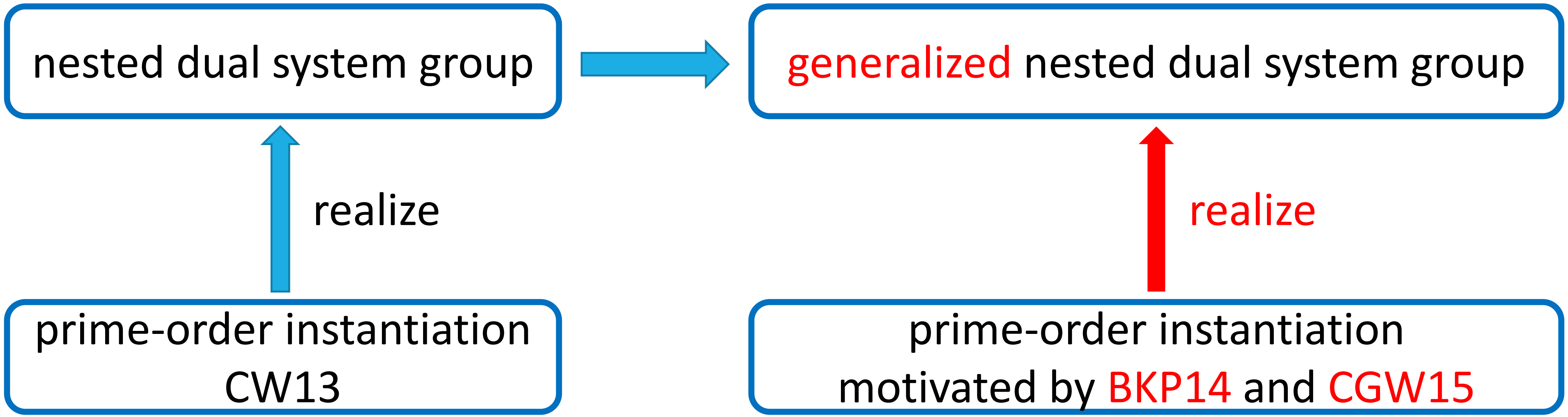
formal result



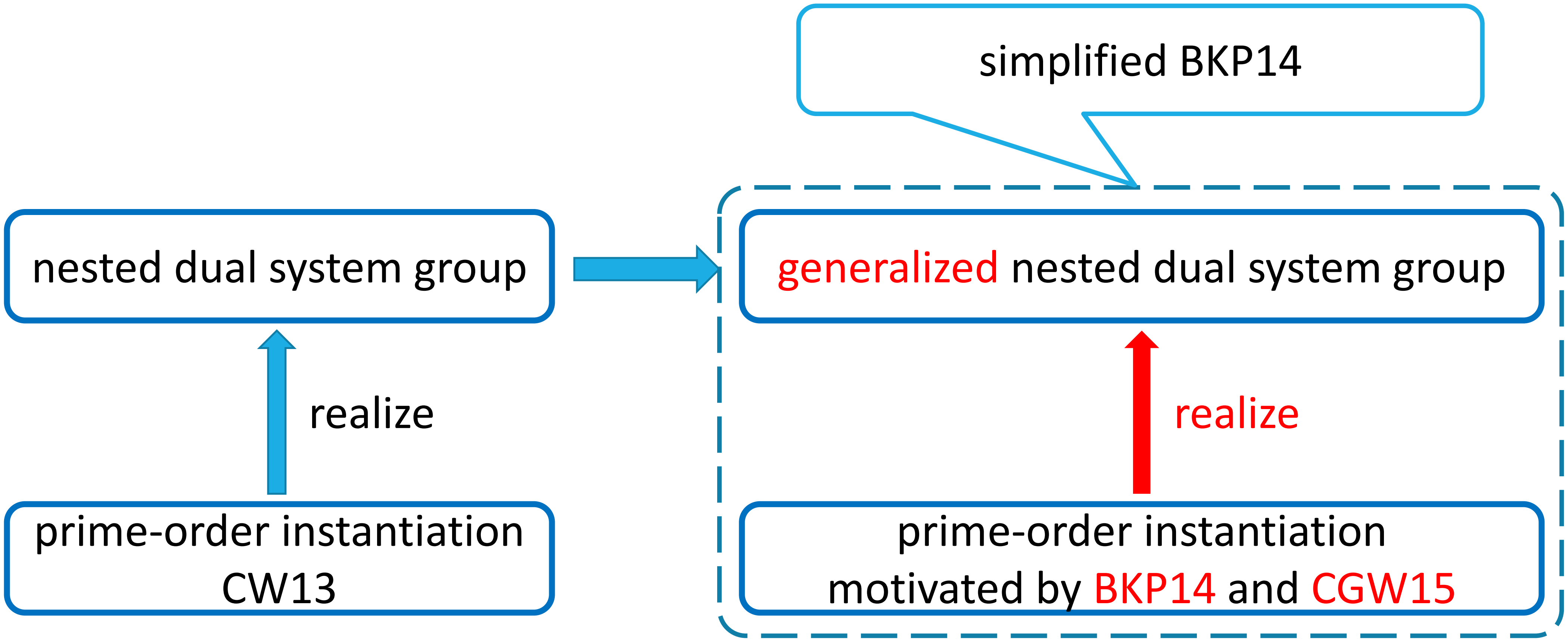
formal result



formal result



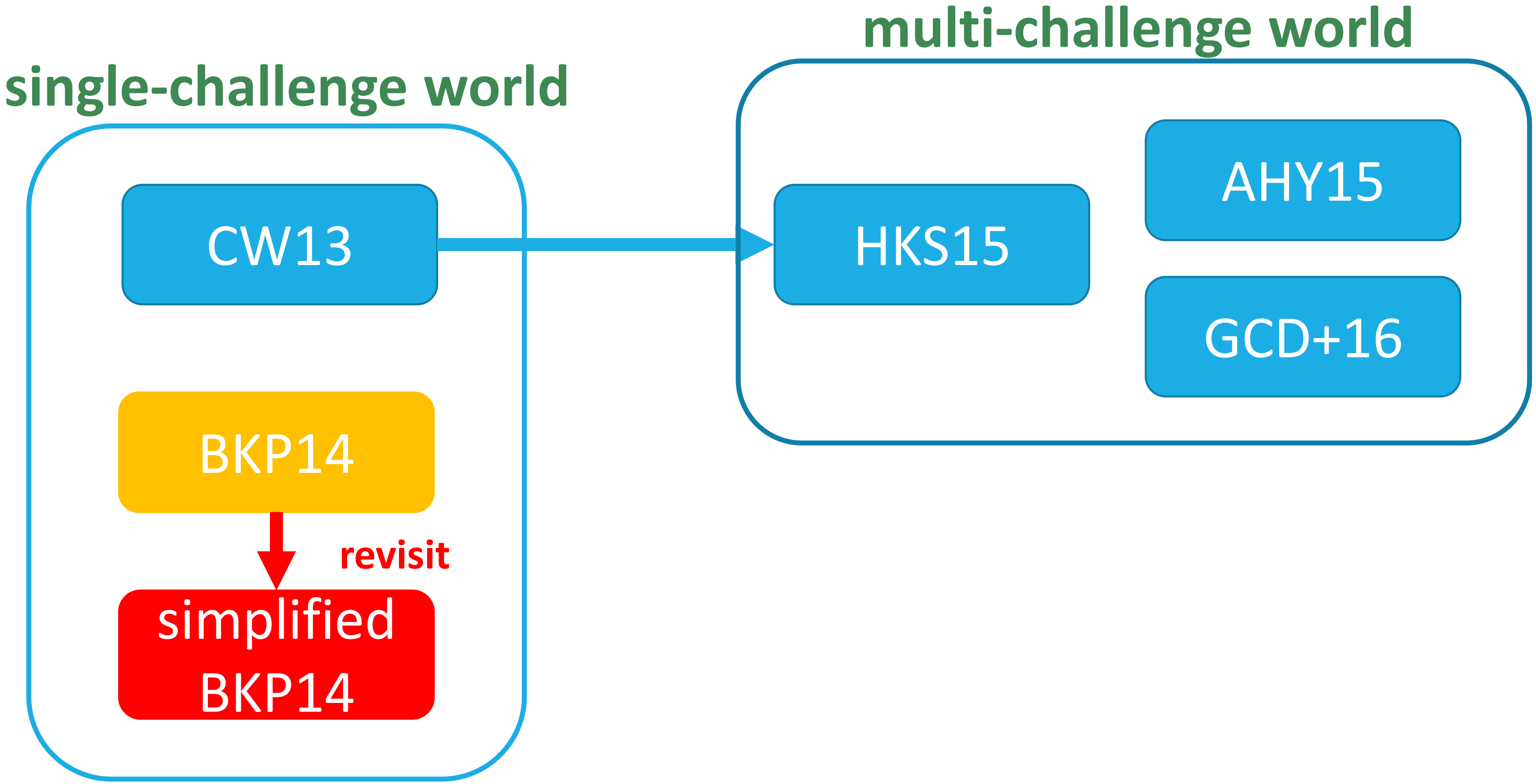
formal result



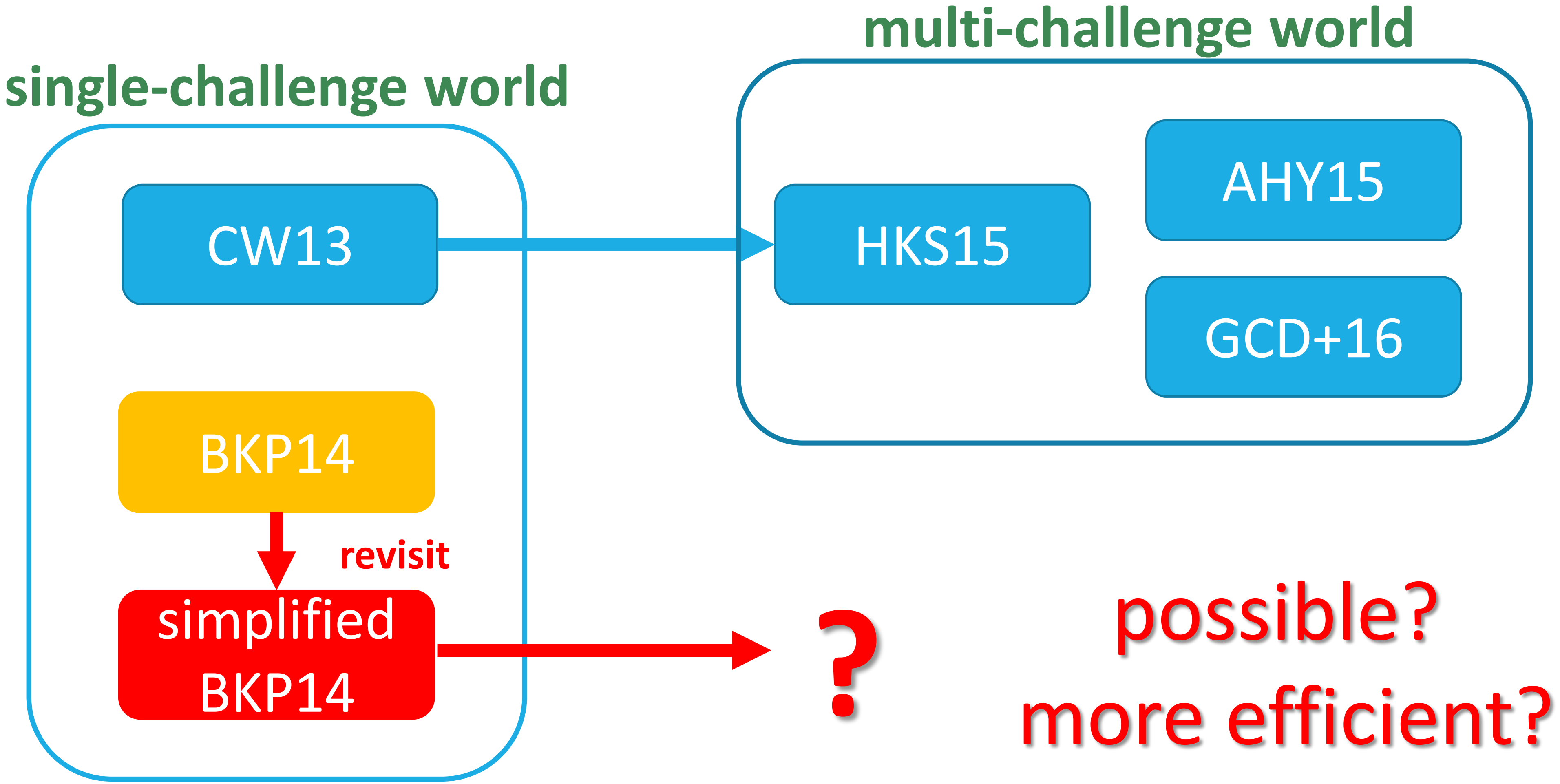
outline

- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

big picture

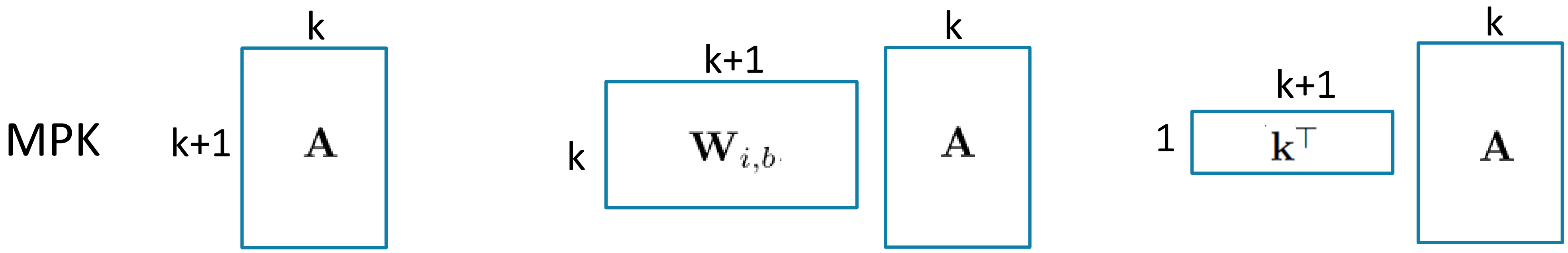

single-challenge world
CW13
BKP14
revisit
simplified BKP14
multi-challenge world
HKS15
AHY15
GCD+16

big picture



multi-challenge world
single-challenge world
CW13
HKS15
AHY15
GCD+16
BKP14
revisit
simplified BKP14
?
possible?
more efficient?

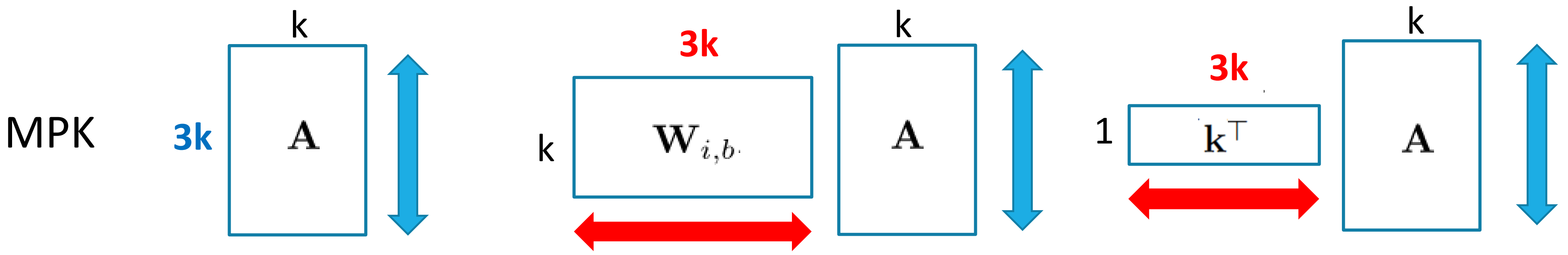
extension: [GCD+16]+[GHKW16]



[GCD+16] *J. Gong, J. Chen, X. Dong, Z. Cao, S. Tang.* Extended Nested Dual System Groups, Revisited. PKC 2016.

[GHKW16] *R. Gay, D. Hofheinz, E. Kiltz, H. Wee.* Tightly CCA-Secure Encryption without Pairings. EUROCRYPT 2016.

extension: [GCD+16]+[GHKW16]



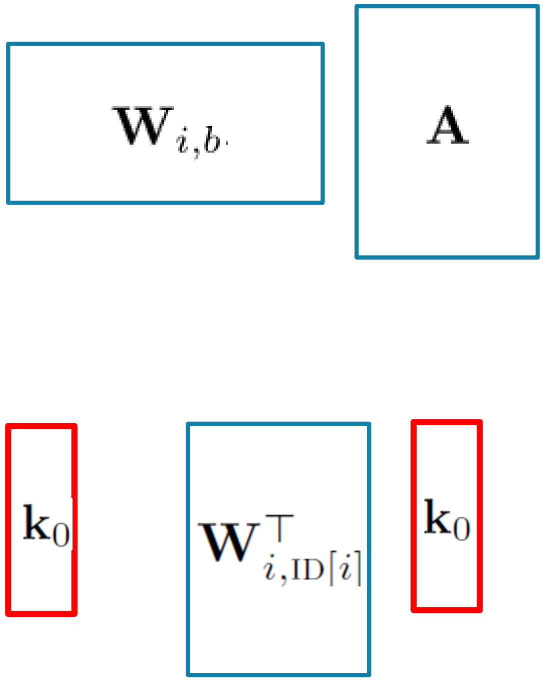
Dimension extension:

- base matrix $\mathbf{A}$: from (k+1)×k to 3k×k
- $\mathbf{W}$ and $\mathbf{k}$: from k×(k+1) to k×3k

[GCD+16] *J. Gong, J. Chen, X. Dong, Z. Cao, S. Tang.* Extended Nested Dual System Groups, Revisited. PKC 2016.

[GHKW16] *R. Gay, D. Hofheinz, E. Kiltz, H. Wee.* Tightly CCA-Secure Encryption without Pairings. EUROCRYPT 2016.

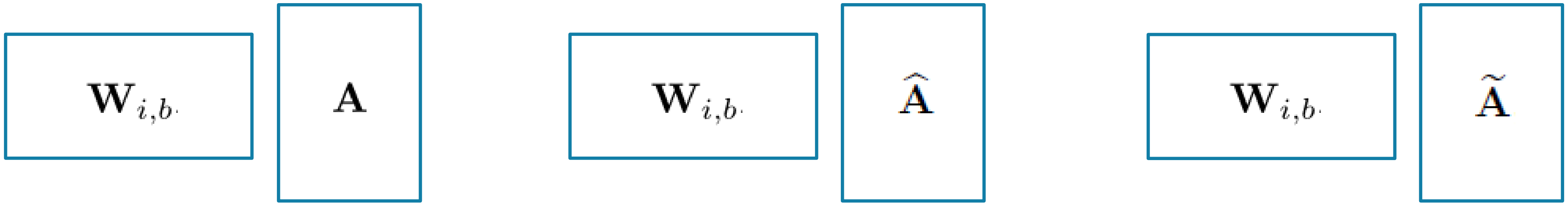
extension: [GCD+16]+[GHKW16]



[GCD+16] *J. Gong, J. Chen, X. Dong, Z. Cao, S. Tang.* Extended Nested Dual System Groups, Revisited. PKC 2016.

[GHKW16] *R. Gay, D. Hofheinz, E. Kiltz, H. Wee.* Tightly CCA-Secure Encryption without Pairings. EUROCRYPT 2016.

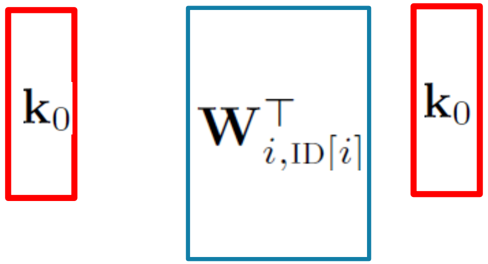
extension: [GCD+16]+[GHKW16]



normal space

∧-semi-functional space

~-semi-functional space

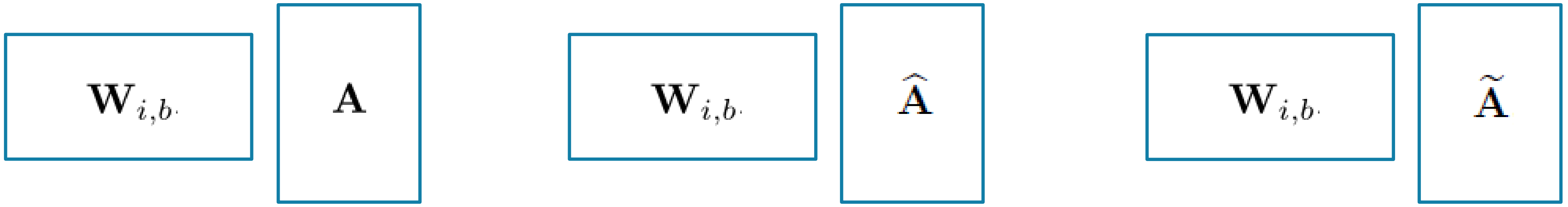


Define bases for three spaces:

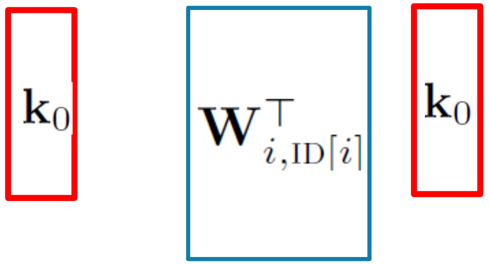
[GCD+16] *J. Gong, J. Chen, X. Dong, Z. Cao, S. Tang.* Extended Nested Dual System Groups, Revisited. PKC 2016.

[GHKW16] *R. Gay, D. Hofheinz, E. Kiltz, H. Wee.* Tightly CCA-Secure Encryption without Pairings. EUROCRYPT 2016.

extension: [GCD+16]+[GHKW16]



normal space ∧-semi-functional space ∼-semi-functional space



Define bases for three spaces:

- hide different parts of $\mathbf{W}$
- support nested-hiding using leftover entropy

[GCD+16] *J. Gong, J. Chen, X. Dong, Z. Cao, S. Tang.* Extended Nested Dual System Groups, Revisited. PKC 2016.

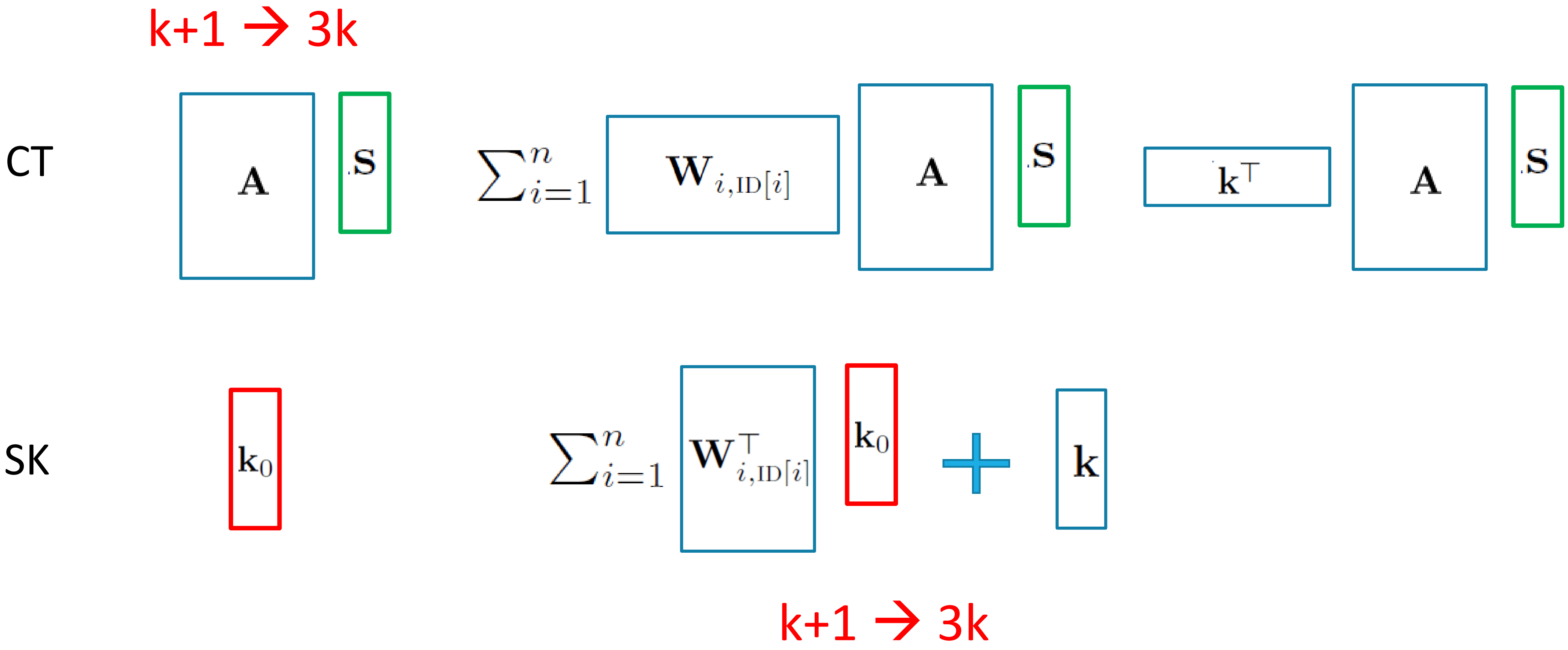
[GHKW16] *R. Gay, D. Hofheinz, E. Kiltz, H. Wee.* Tightly CCA-Secure Encryption without Pairings. EUROCRYPT 2016.

why shorter ciphertext?

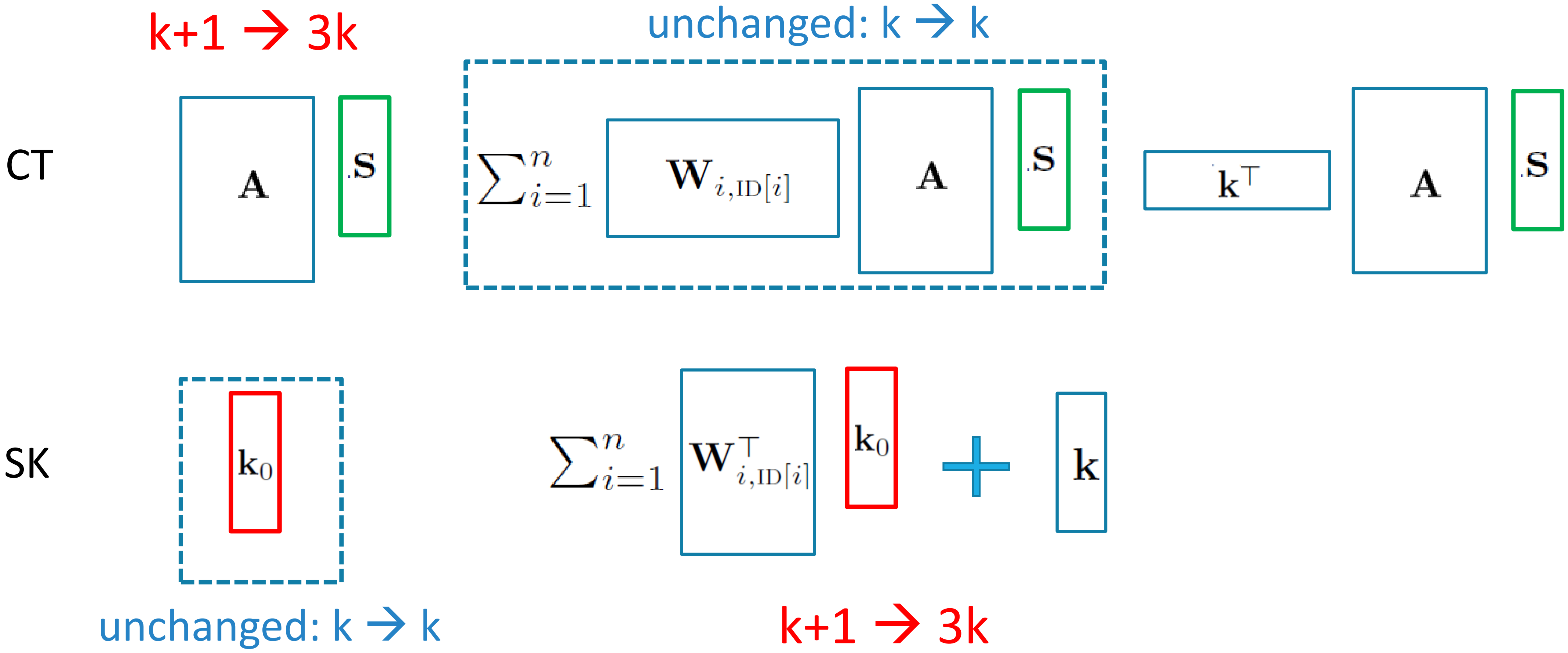
CT $\quad \mathbf{A}\mathbf{s} \qquad \sum_{i=1}^{n} \mathbf{W}_{i,\mathrm{ID}[i]} \mathbf{A}\mathbf{s} \qquad \mathbf{k}^\top \mathbf{A}\mathbf{s}$

SK $\quad \mathbf{k}_0 \qquad \sum_{i=1}^{n} \mathbf{W}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0 + \mathbf{k}$

why shorter ciphertext?



why shorter ciphertext?



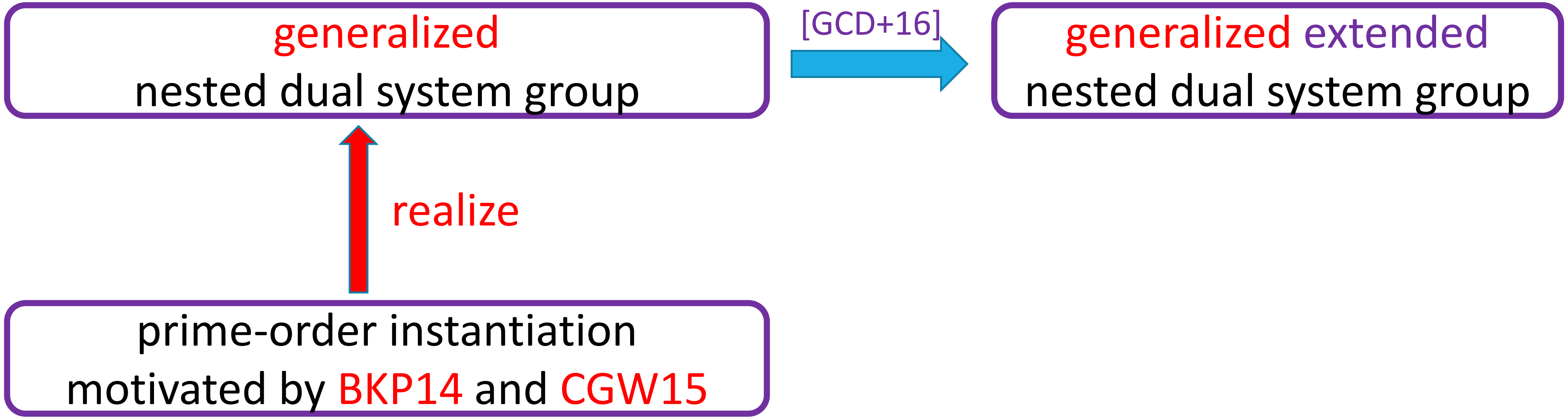
formal result

generalized
nested dual system group

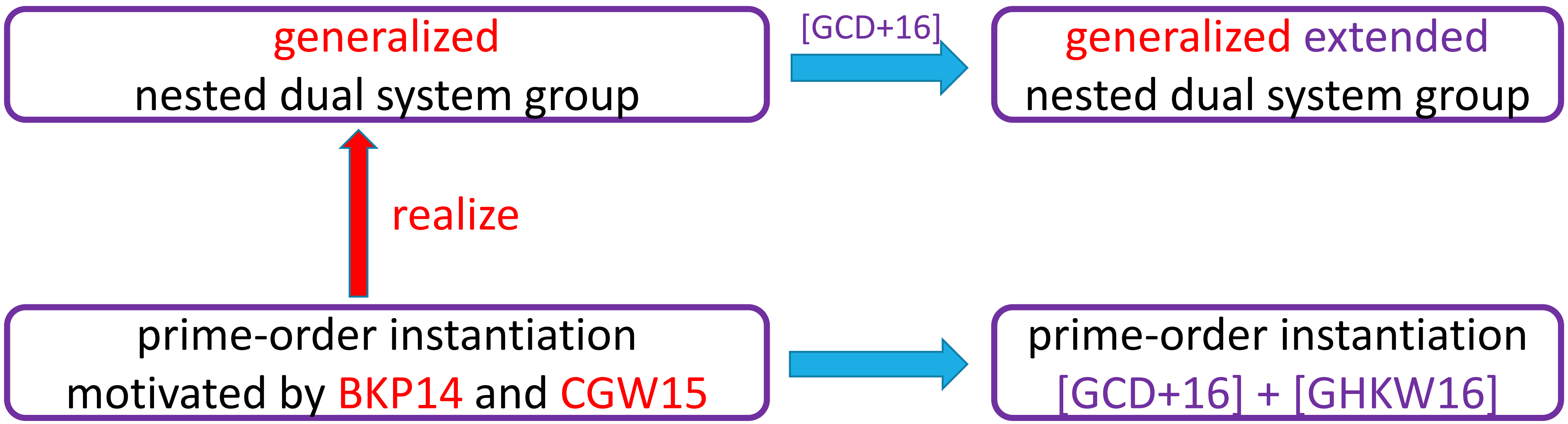
↑ realize

prime-order instantiation
motivated by BKP14 and CGW15

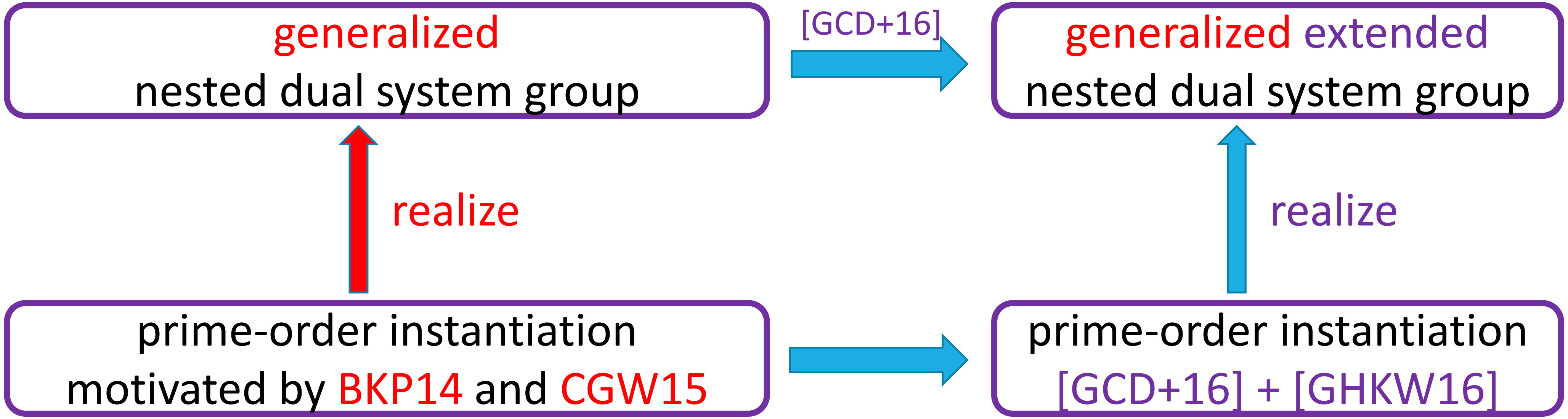
formal result



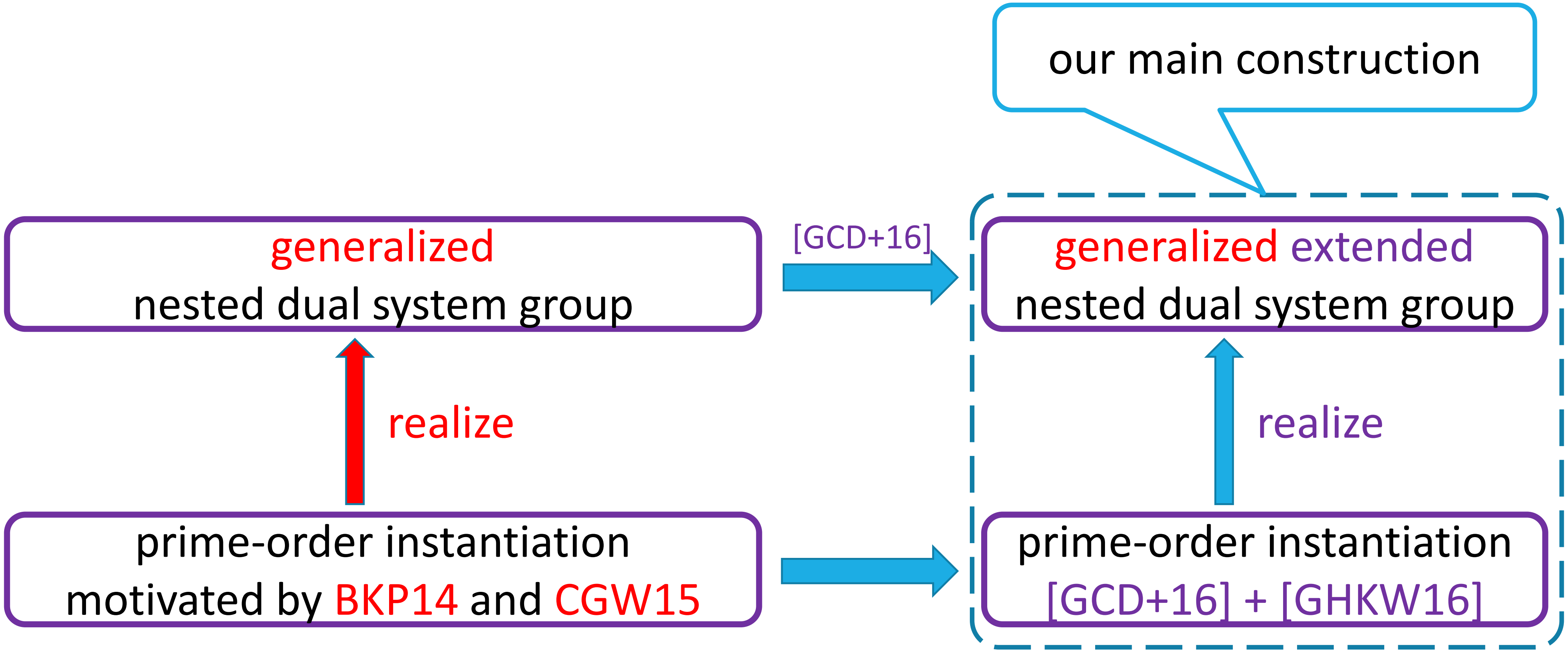
formal result



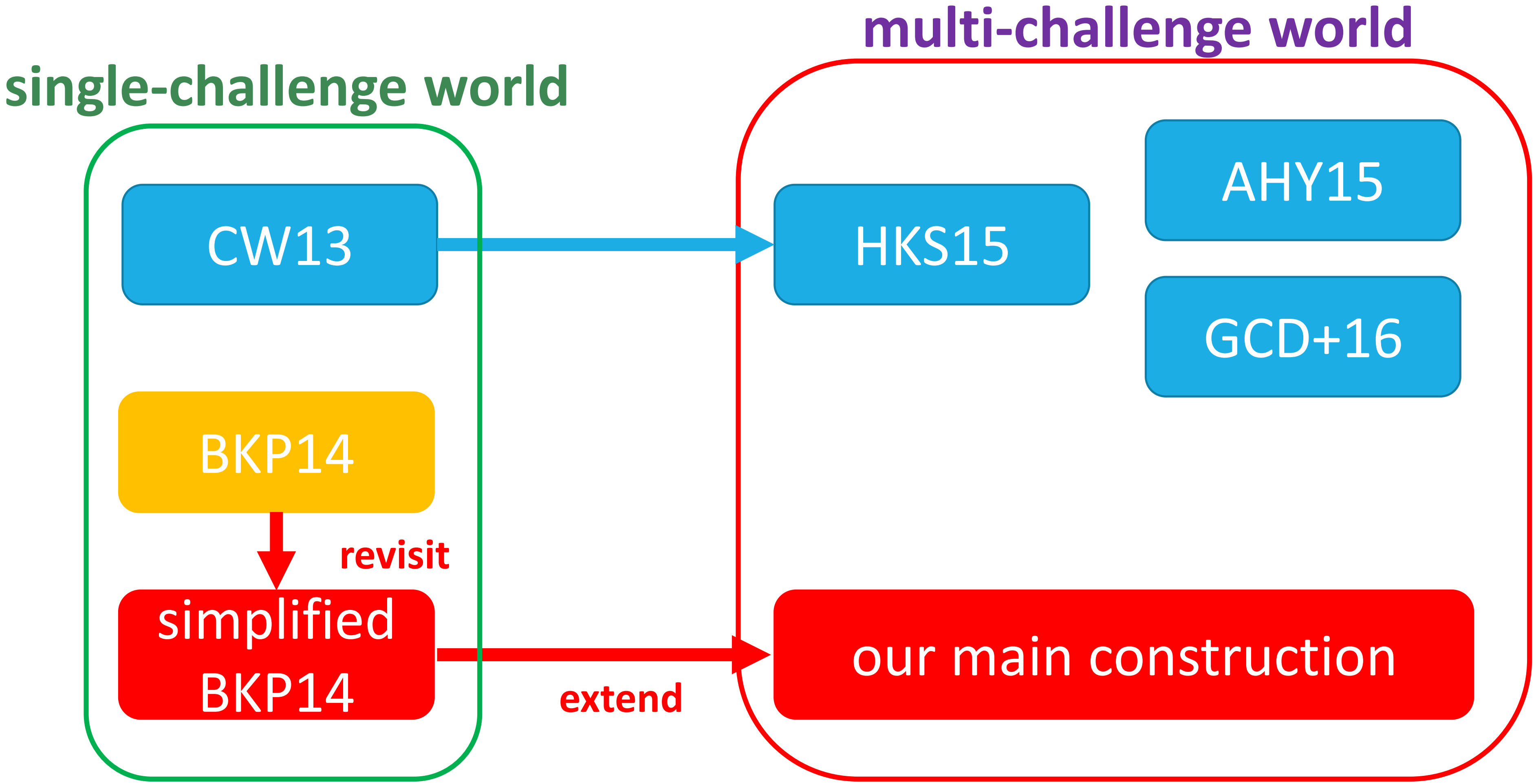
formal result



formal result



big picture


multi-challenge world
single-challenge world
CW13
HKS15
AHY15
GCD+16
BKP14
revisit
simplified BKP14
extend
our main construction

outline

- background
- motivation
- strategy
- technical result 1: revisiting Blazy-Kiltz-Pan IBE
- technical result 2: towards multi-challenge setting
- comparison

almost-tightly secure IBE

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	k-lin	2k + 2k
BKP14	no	prime	k-lin	k + (k+1)
HKS15	yes	composite	static	1 + 1
AHY15	yes	prime	stronger 2-lin	4 + 4 (k=2)
GCD+16	yes	prime	k-lin	3k + 3k
			stronger k-lin	2k + 2k
this work	yes	prime	k-lin	k+3k

concrete comparison

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	1-lin	4
BKP14	no	prime	1-lin	3
HKS15	yes	composite	static	2
AHY15	yes	prime	stronger 2-lin	8
GCD+16	yes	prime	1-lin	6
			stronger 2-lin	8
this work	yes	prime	1-lin	4

concrete comparison

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	1-lin	4
BKP14	no	prime	1-lin	3
HKS15	yes	composite	static	2
AHY15	yes	prime	stronger 2-lin	8
GCD+16	yes	prime	1-lin	6
			stronger 2-lin	8
this work	yes	prime	1-lin	4

concrete comparison

	multi-challenge	bilinear groups	assumption	ciphertext size
CW13	no	composite & prime	1-lin	4
BKP14	no	prime	1-lin	3
HKS15	yes	composite	static	2
AHY15	yes	prime	stronger 2-lin	8
GCD+16	yes	prime	1-lin	6
			stronger 2-lin	8
this work	yes	prime	1-lin	4

summary

1. revisit/simplify BKP14 IBE

   ✓ a new instantiation of (generalized) nested dual system group

   ✓ compare CW13 and BKP14 in a more clear way

2. extend simplified BKP14 to the multi-challenge setting

   ✓ achieve short ciphertexts (also high performance in other aspects) under standard assumption

   ✓ lead to the most efficient concrete construction

additional feature

✓ both of them are **weak** anonymous [AHY15]

✓ "weak" means each id has unique secret key

Thank you for your attention!

Any question?