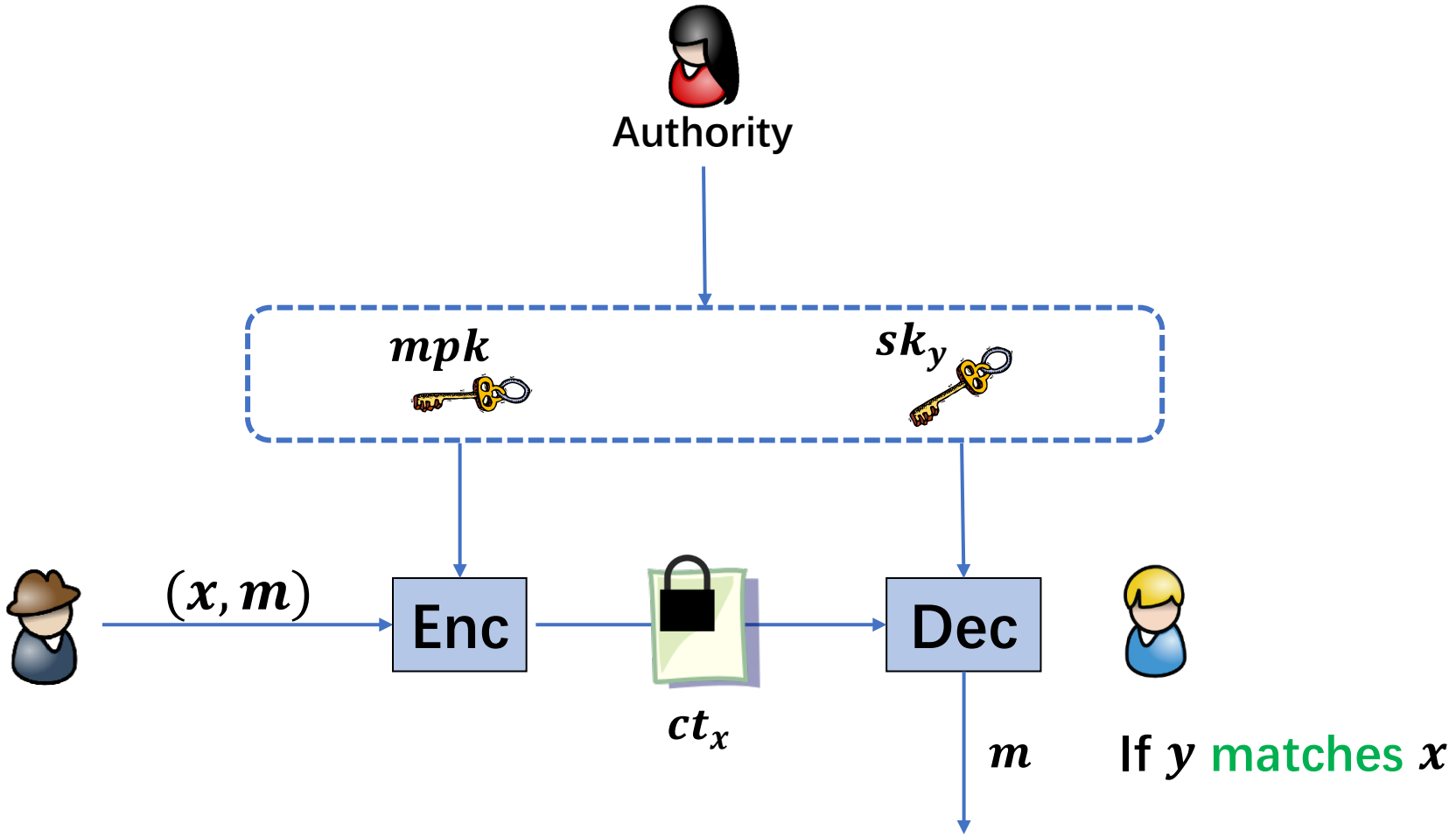
Improved Fully Adaptive Decentralized MA-ABE for NC1 from MDDH

Jie Chen	Qiaohan Chu	Ying Gao	Jianting Ning	Luping Wang
ECNU	ECNU	BUAA	FNU	SUST

Attribute-Based Encryption



decentralized MA-ABE

decentralized MA-ABE for NC1

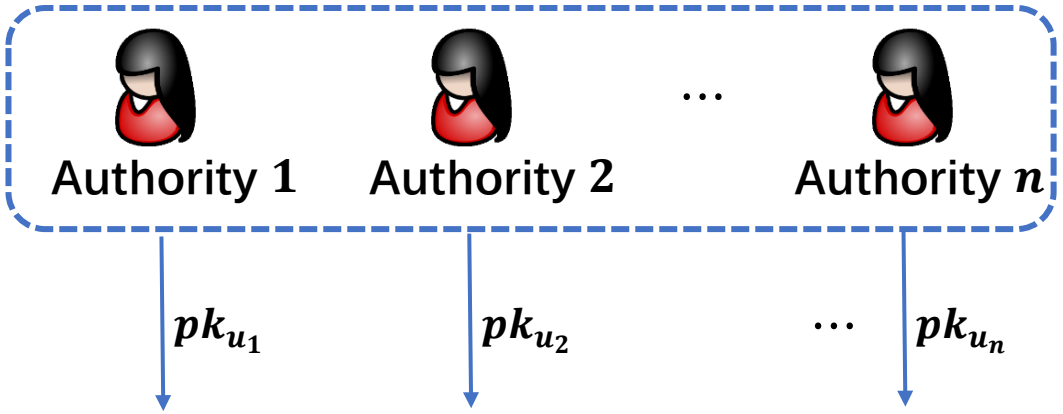
[LW11]

– [LW11] Allison B. Lewko, Brent Waters. Decentralized Attribute-Based Encryption. Eurocrypt 2011.

decentralized MA-ABE for NC1: GlobalSetup

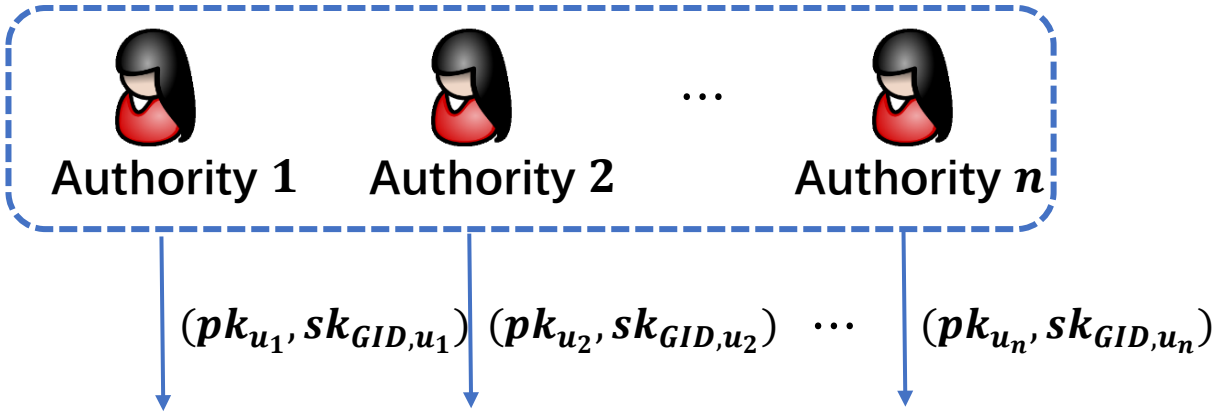
$$GP$$

decentralized MA-ABE for NC1: AuthSetup



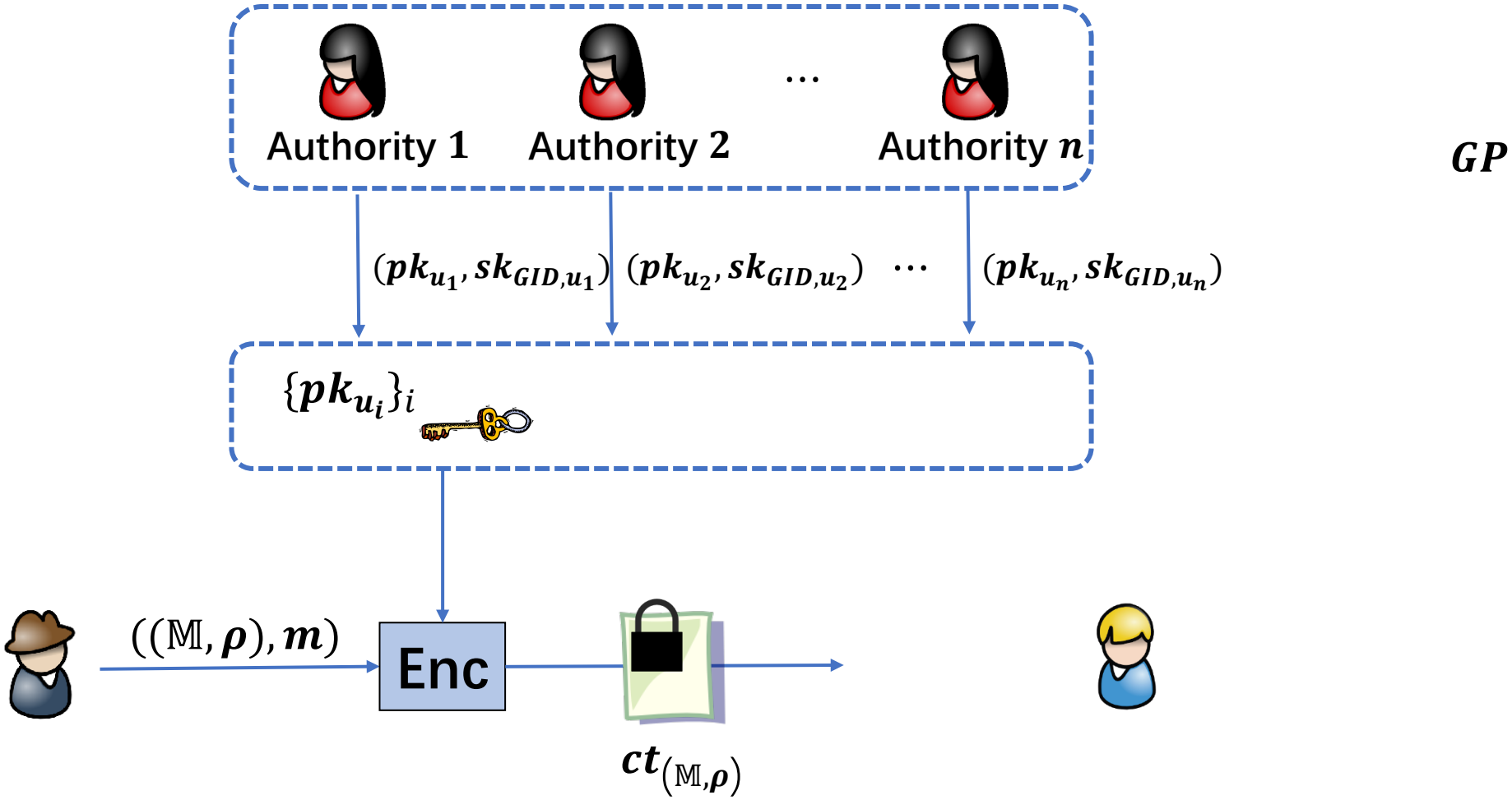
GP

decentralized MA-ABE for NC1: KeyGen

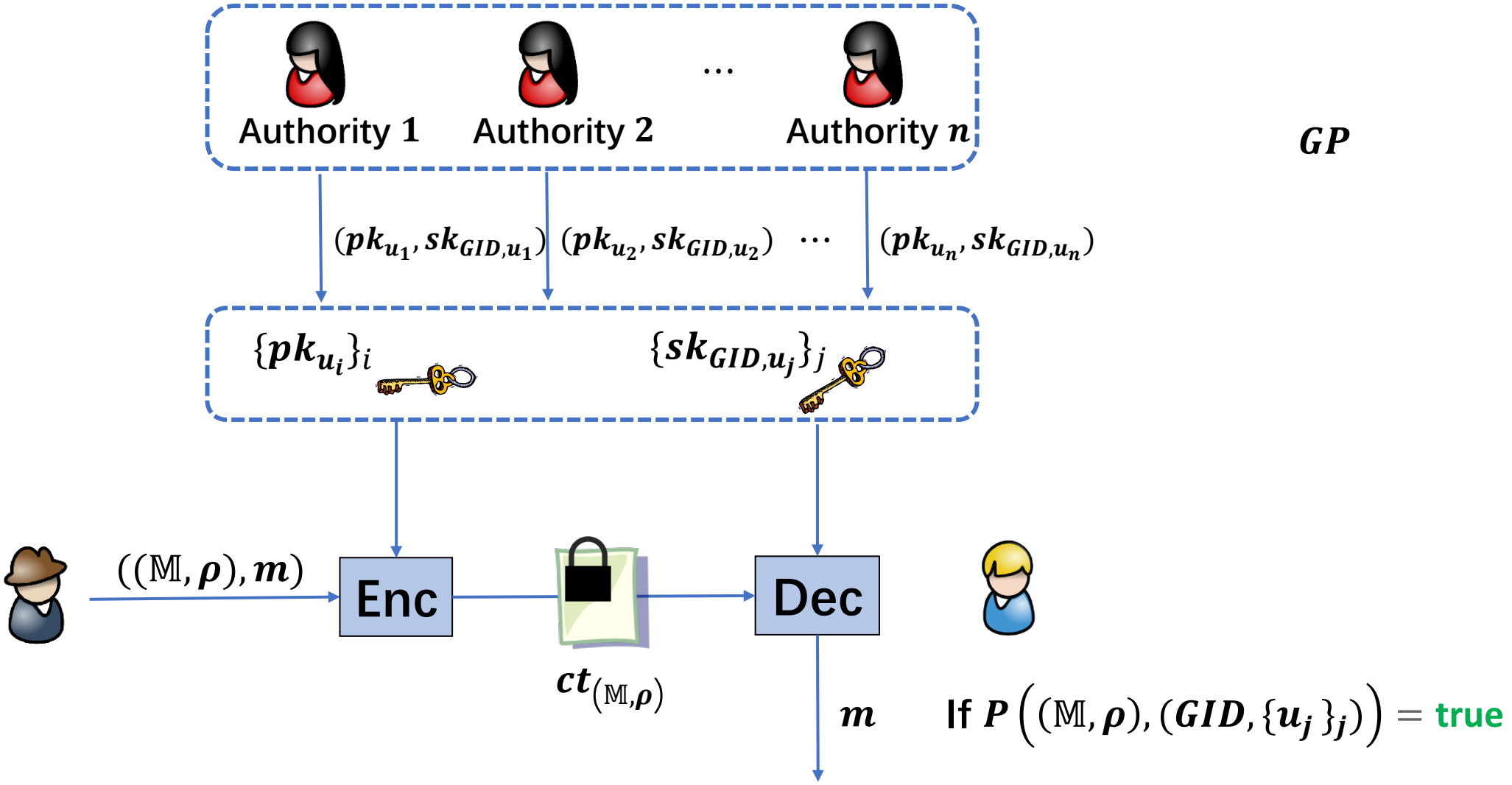


GP

decentralized MA-ABE for NC1: Enc

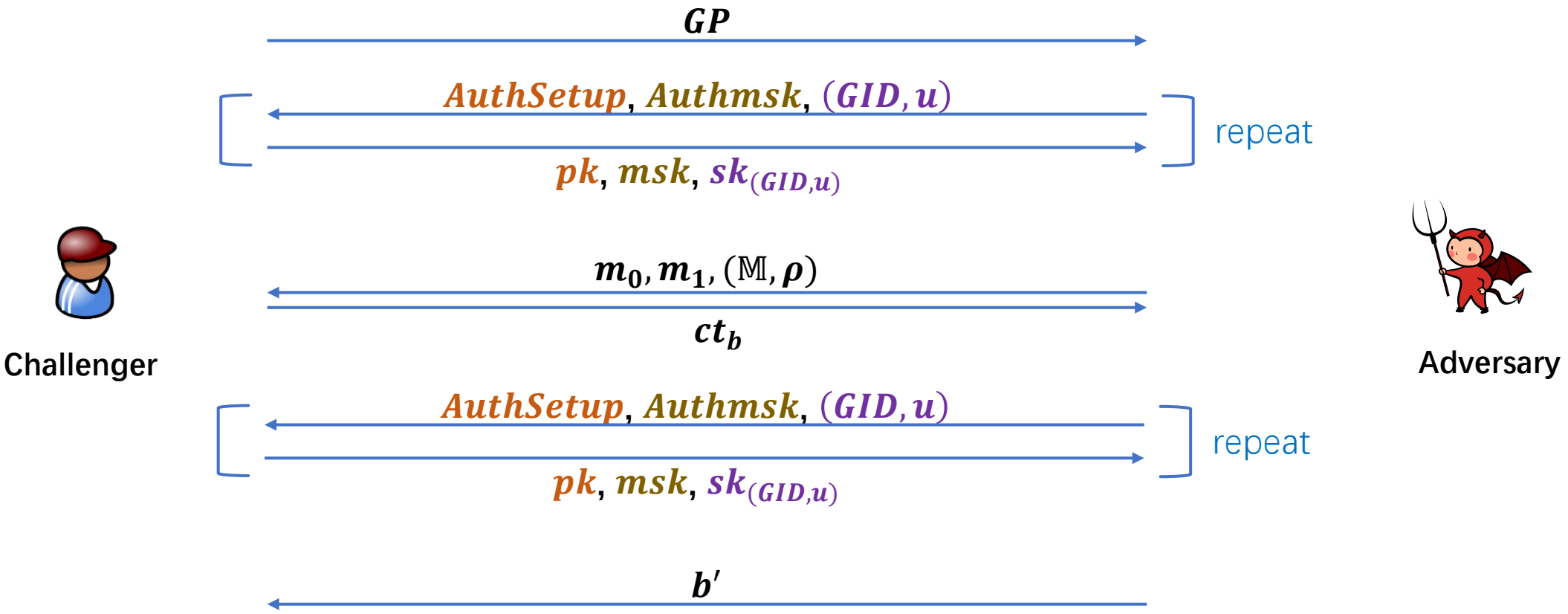


decentralized MA-ABE for NC1: Dec



decentralized MA-ABE for NC1: fully adaptive

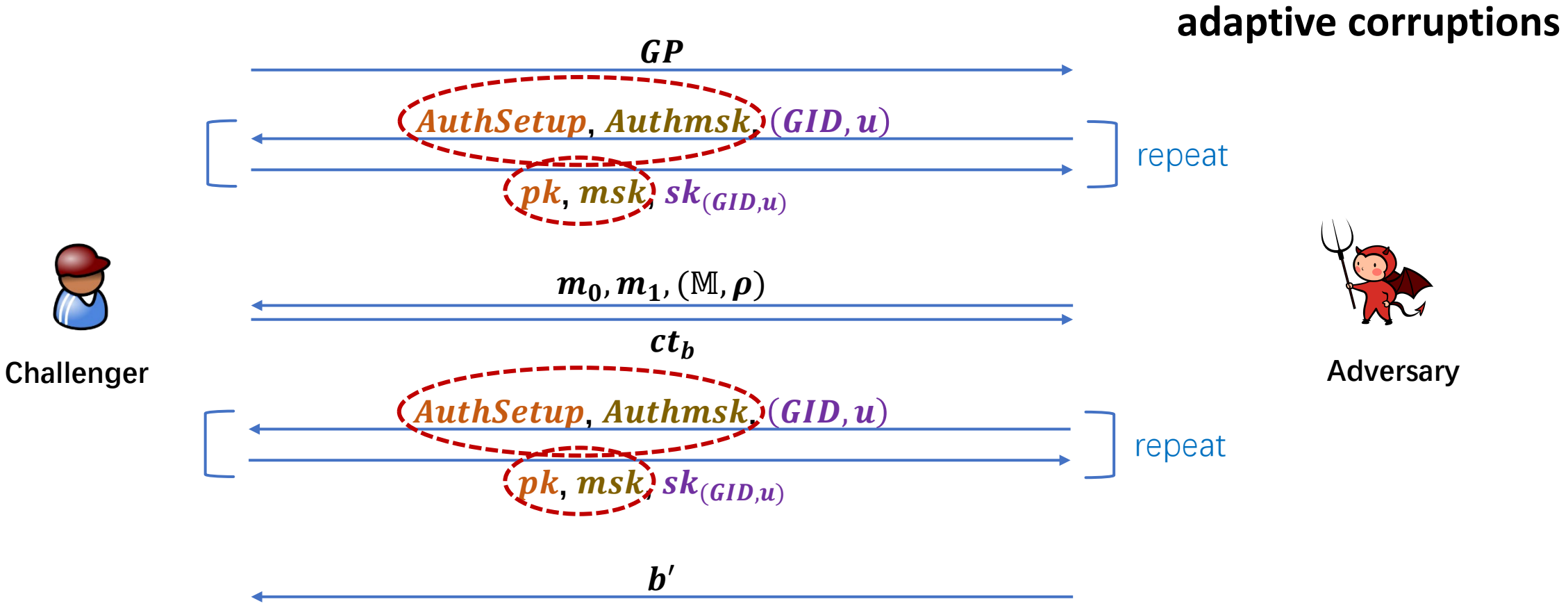
[DKW23]



– [DKW23] Pratish Datta, Ilan Komargodski, Brent Waters. Fully Adaptive Decentralized Multi-Authority ABE. Eurocrypt 2023.

decentralized MA-ABE for NC1: fully adaptive

[DKW23]



– [DKW23] Pratish Datta, Ilan Komargodski, Brent Waters. Fully Adaptive Decentralized Multi-Authority ABE. Eurocrypt 2023.

prime-order construction in [DKW23]

$\boldsymbol{\rho}$: injective

CT matrix: $\mathbf{A}_1^{\mathrm{T}} \in \mathbb{Z}_p^{k \times 3k}$

SK matrix: $\mathbf{B}_1 \in \mathbb{Z}_p^{3k \times k}$

bridge matrix: $\mathbf{W} \in \mathbb{Z}_p^{3k \times 3k}$

CT dimension

SK dimension

prime-order construction in [DKW23]

eliminate the one-use of attribute limitation and shrink the matrix?

$\boldsymbol{\rho}$: injective

CT matrix: $\mathbf{A}_1^{\mathrm{T}} \in \mathbb{Z}_p^{k \times 3k}$

SK matrix: $\mathbf{B}_1 \in \mathbb{Z}_p^{3k \times k}$

bridge matrix: $\mathbf{W} \in \mathbb{Z}_p^{3k \times 3k}$

CT dimension

SK dimension

prime-order construction in [DKW23]

eliminate the one-use of attribute limitation and shrink the matrix

$\boldsymbol{\rho}$: injective

CT matrix: $\mathbf{A}_1^{\mathrm{T}} \in \mathbb{Z}_p^{k \times 3k}$

SK matrix: $\mathbf{B}_1 \in \mathbb{Z}_p^{3k \times k}$

bridge matrix: $\mathbf{W} \in \mathbb{Z}_p^{3k \times 3k}$

○ CT dimension

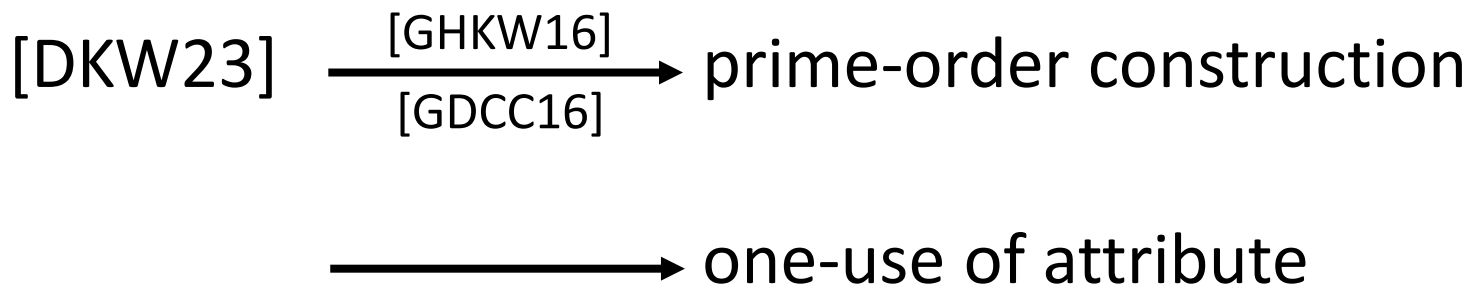
○ SK dimension

our contribution

one-use of attribute ⟶ many-use of attribute

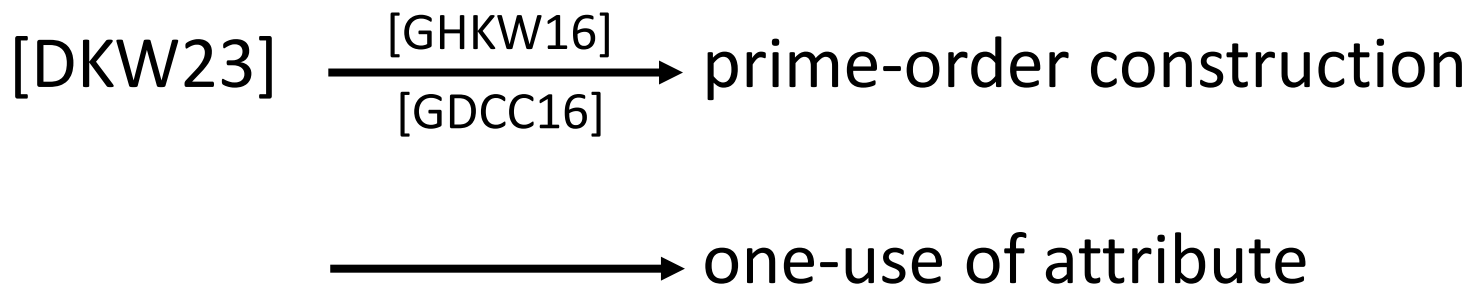
CT matrix: $3k$ ⟶ $2k + 1$

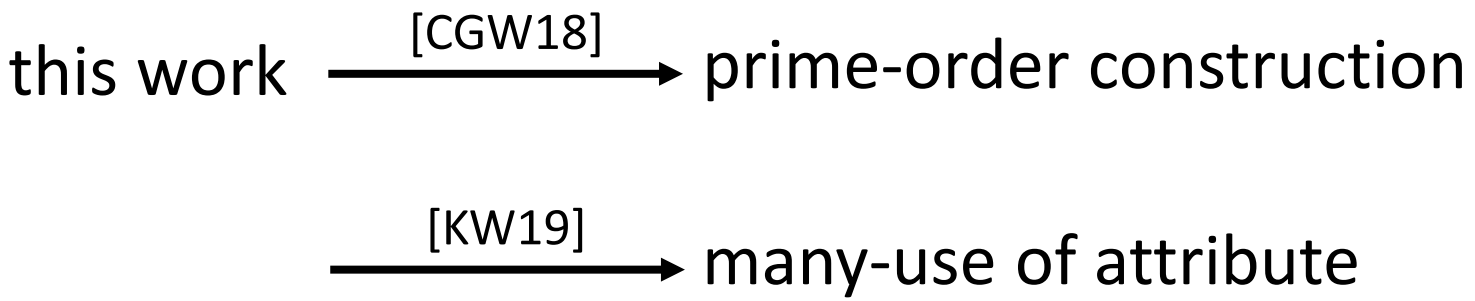
strategy



– [GHKW16] Romain Gay, Dennis Hofheinz, Eike Kiltz, Hoeteck Wee. Tightly CCA-Secure Encryption Without Pairings. Eurocrypt 2016.
– [GDCC16] Junqing Gong, Xiaolei Dong, Jie Chen, Zhenfu Cao. Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting. Asiacrypt 2016.

strategy





- [GHKW16] Romain Gay, Dennis Hofheinz, Eike Kiltz, Hoeteck Wee. Tightly CCA-Secure Encryption Without Pairings. Eurocrypt 2016.
- [GDCC16] Junqing Gong, Xiaolei Dong, Jie Chen, Zhenfu Cao. Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting. Asiacrypt 2016.
- [CGW18] Jie Chen, Junqing Gong, Hoeteck Wee. Improved Inner-Product Encryption with Adaptive Security and Full Attribute-Hiding. Asiacrypt 2018.
- [KW19] Lucas Kowalczyk, Hoeteck Wee. Compact Adaptively Secure ABE for NC1 from k-Lin. Eurocrypt 2019.

high-level: multi-authority & many-use

[KW19] ⟶ single authority (centralized) & many-use

[DKW23] ⟶ multi-authority (decentralized)

high-level: multi-authority & many-use

[KW19] ⟶ single authority (centralized) & many-use

[DKW23] —[KW19]→ multi-authority (decentralized) & many-use?

high-level: multi-authority & many-use

[KW19] ⟶ single authority (centralized) & many-use

[DKW23] —[KW19]⟶ multi-authority (decentralized) & many-use

high-level: multi-authority & many-use

[KW19] ⟶ single authority (centralized) & many-use

[DKW23] $\xrightarrow{\text{[KW19]}}$ multi-authority (decentralized) & many-use

$(3,3)$ subspaces ⟶ $3k \times 3k$

high-level: shorter parameters

[CGW18] ⟶ shorter parameters

high-level: shorter parameters

[CGW18] ⟶ shorter parameters

$(3,3)$ subspaces ⟶ $(k+2)\times 3k$

high-level: final

[DKW23] $\xrightarrow[\text{[CGW18]}]{\text{[KW19]}}$ multi-authority & many-use & shorter parameters?

high-level: final

[DKW23] $\xrightarrow[\text{[CGW18]}]{\text{[KW19]}}$ multi-authority & many-use & shorter parameters

$(3,3)$ subspaces $\longrightarrow$ $(2k+1) \times 3k$

technique: recap of the composite-order

CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
statistical	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
statistical	
	$p_{12} \longrightarrow p_{123}$
statistical	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
statistical	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
statistical	

technique: recap of the composite-order

CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
statistical	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
statistical	
	$p_{12} \longrightarrow p_{123}$
statistical	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
statistical	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
statistical	

one-use

technique: recap of the composite-order

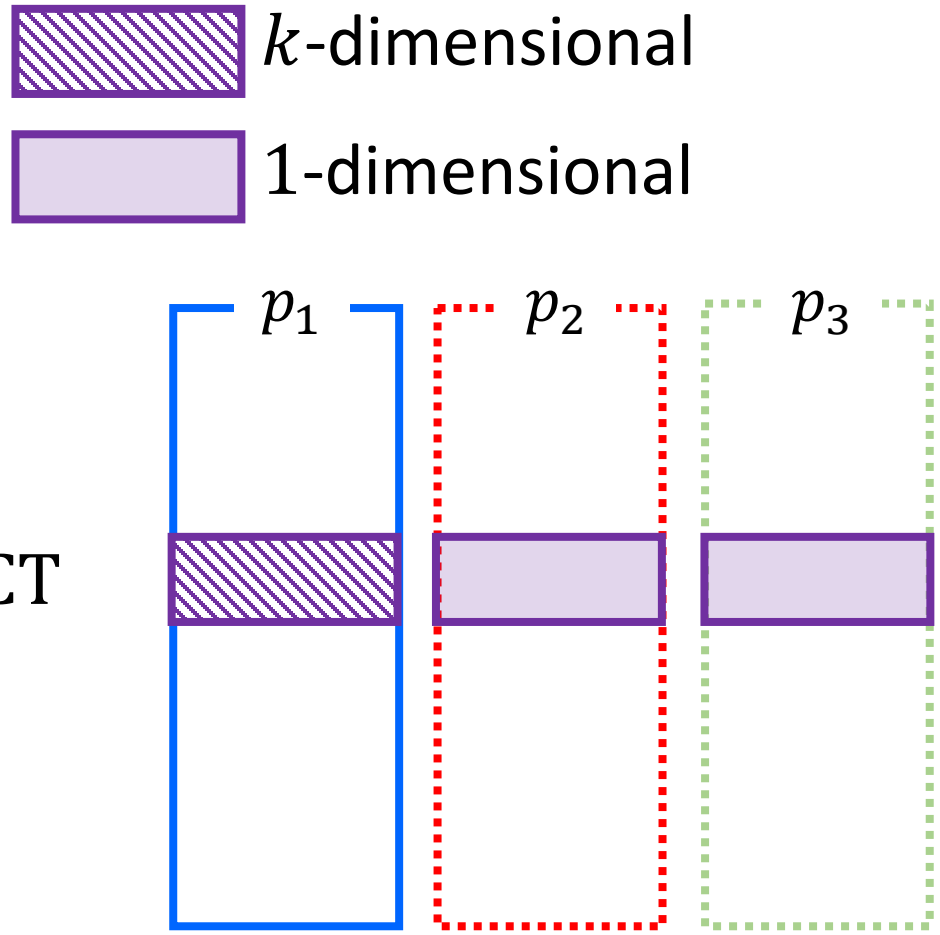
CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
computational	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
computational	
	$p_{12} \longrightarrow p_{123}$
computational	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
computational	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
computational	

many-use

1-dimensional

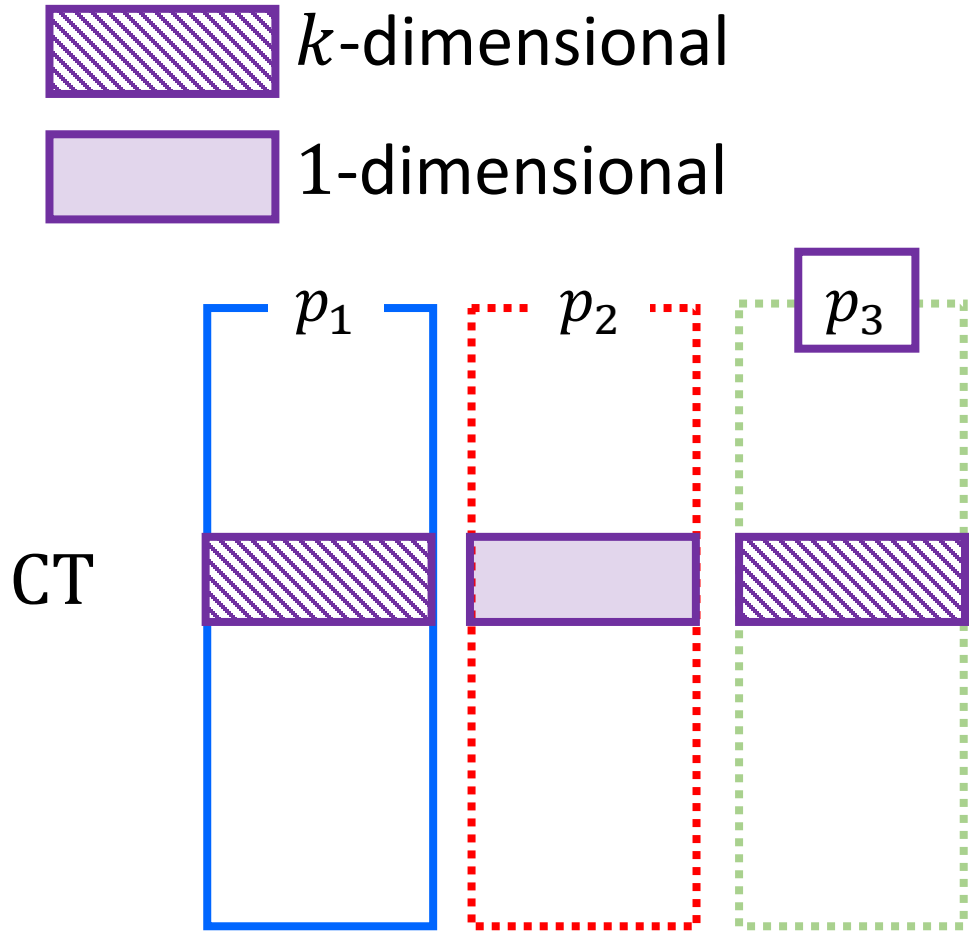
k-dimensional

technique: one-use-to-many-use



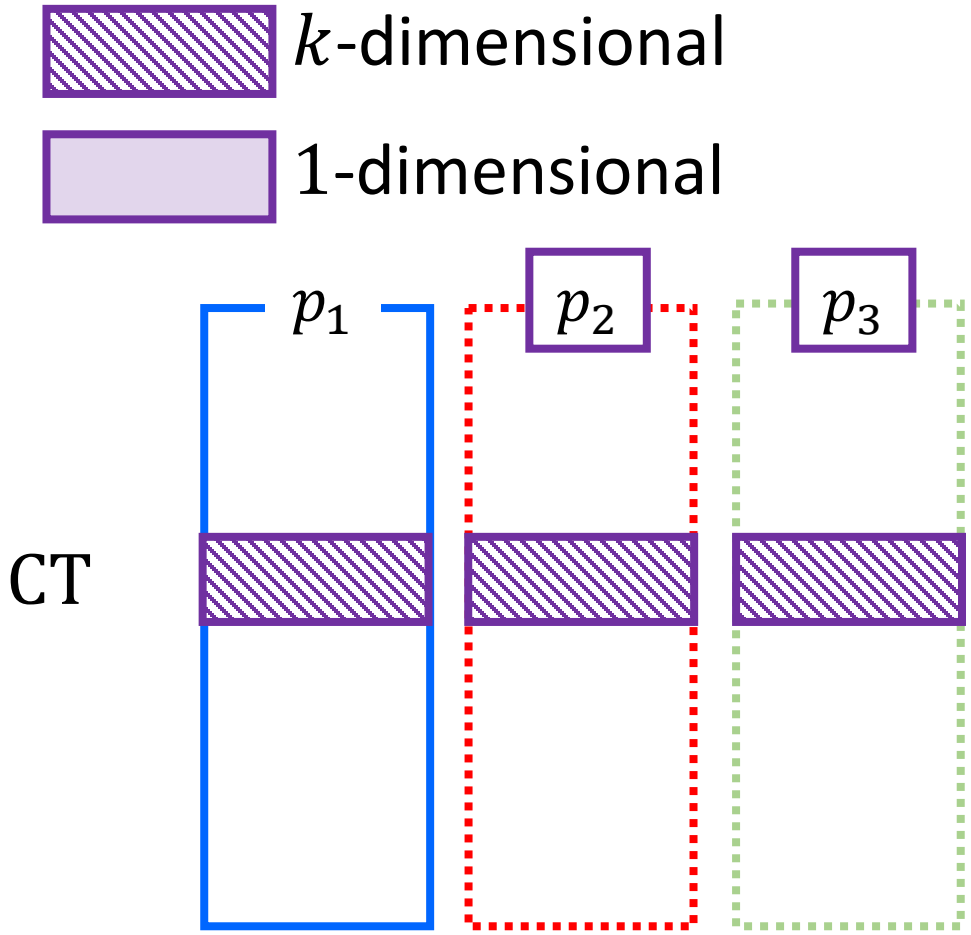
change the secrets in p_3 and p_2

technique: one-use-to-many-use



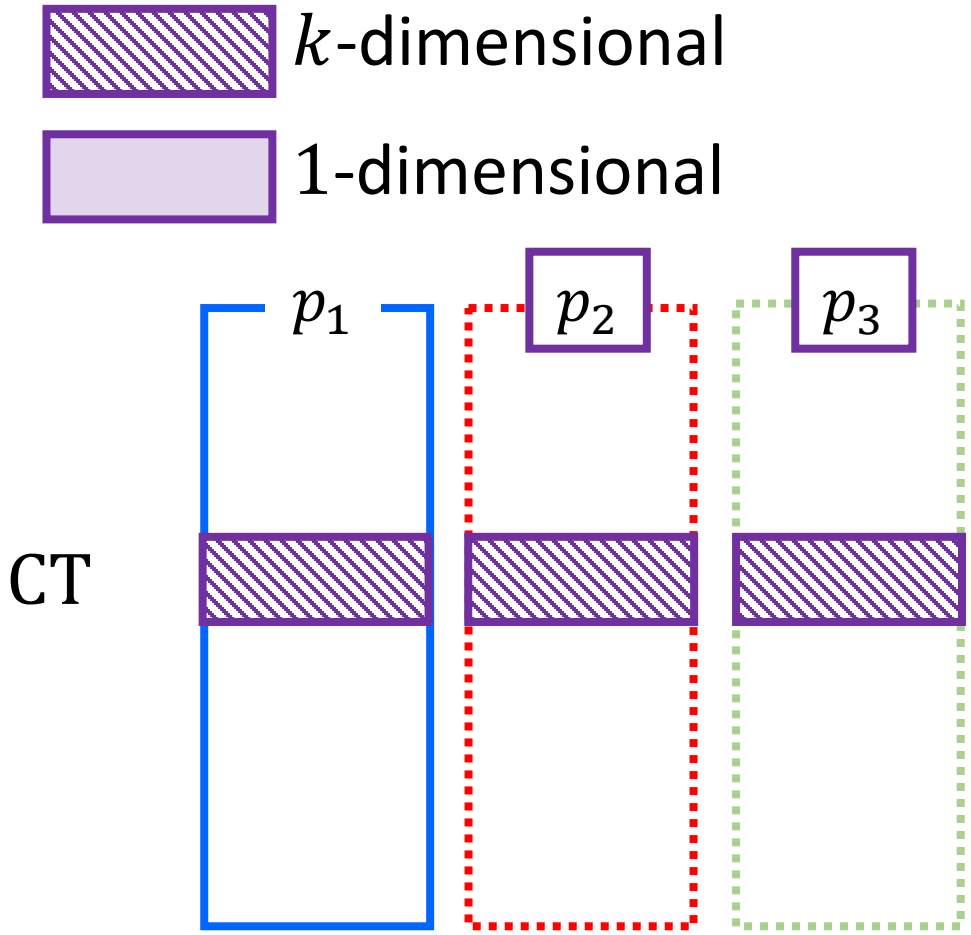
change the secrets in p_3 and p_2

technique: one-use-to-many-use

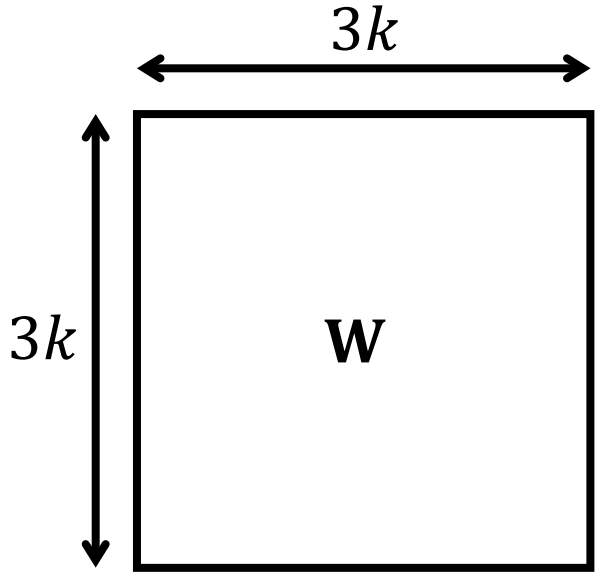


change the secrets in p_3 and p_2

technique: one-use-to-many-use



change the secrets in p_3 and p_2



$MDDH$

technique: recap of the composite-order

CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
~~statistical~~	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{12} \longrightarrow p_{123}$
~~statistical~~	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
~~statistical~~	

technique: recap of the composite-order

○ k-dimensional

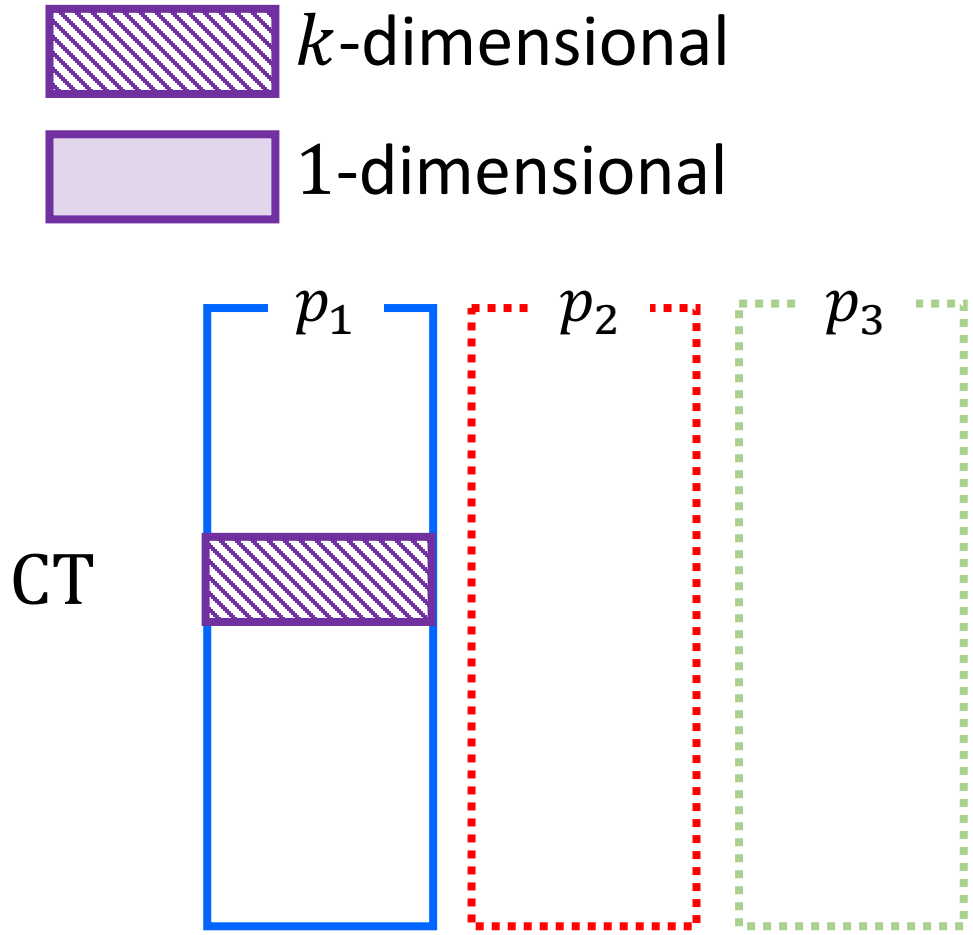
○ 1-dimensional

CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
~~statistical~~	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{12} \longrightarrow p_{123}$
~~statistical~~	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
~~statistical~~	

technique: recap of the composite-order

CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
~~statistical~~	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{12} \longrightarrow p_{123}$
~~statistical~~	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
~~statistical~~	

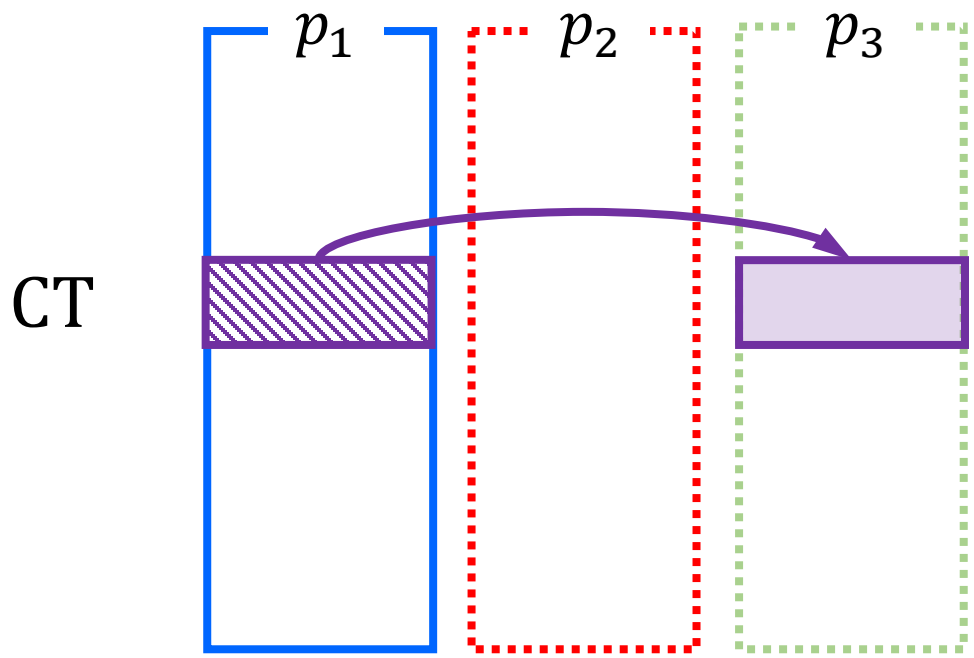
technique: composite-to-prime (CT)



technique: composite-to-prime (CT)

k-dimensional

1-dimensional

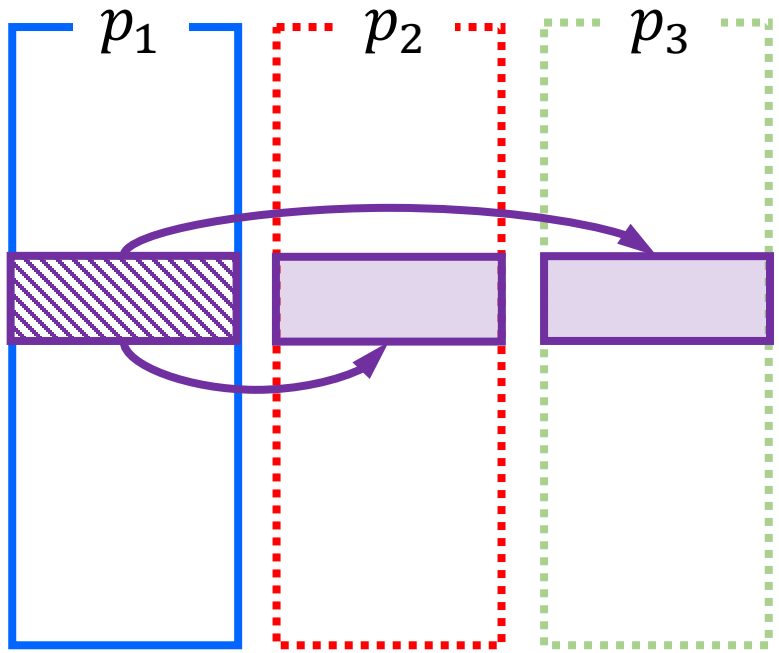


technique: composite-to-prime (CT)

k-dimensional

1-dimensional

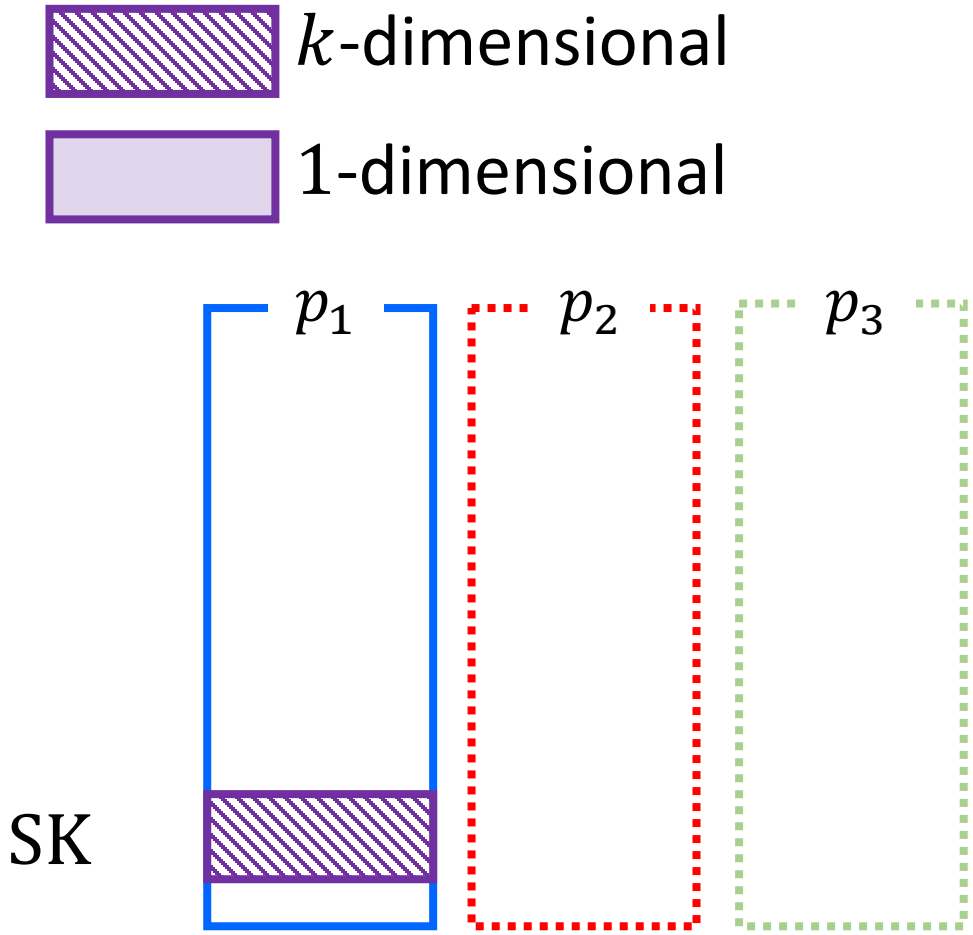
CT



technique: recap of the composite-order

CT	SK
	$p_{123} \longrightarrow p_1$
$p_1 \longrightarrow p_{13}$	
~~statistical~~	
$p_1 \longrightarrow p_{12}$	
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{12} \longrightarrow p_{123}$
~~statistical~~	
	$p_{12} \longrightarrow p_1$
	$p_1 \longrightarrow p_{12}$
~~statistical~~	
	$p_{13} \longrightarrow p_{123}$
	$p_{123} \longrightarrow p_{13}$
~~statistical~~	

technique: composite-to-prime (SK)

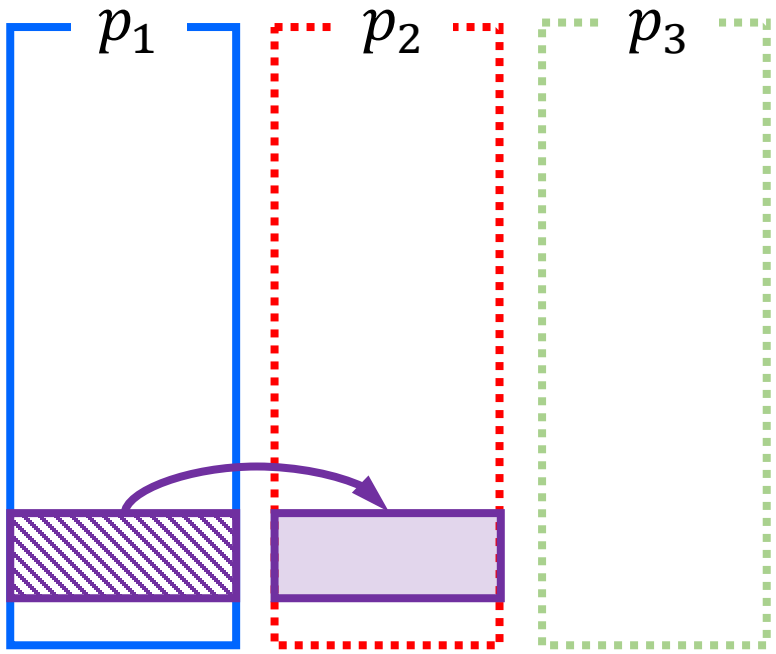


technique: composite-to-prime (SK)

k-dimensional

1-dimensional

SK

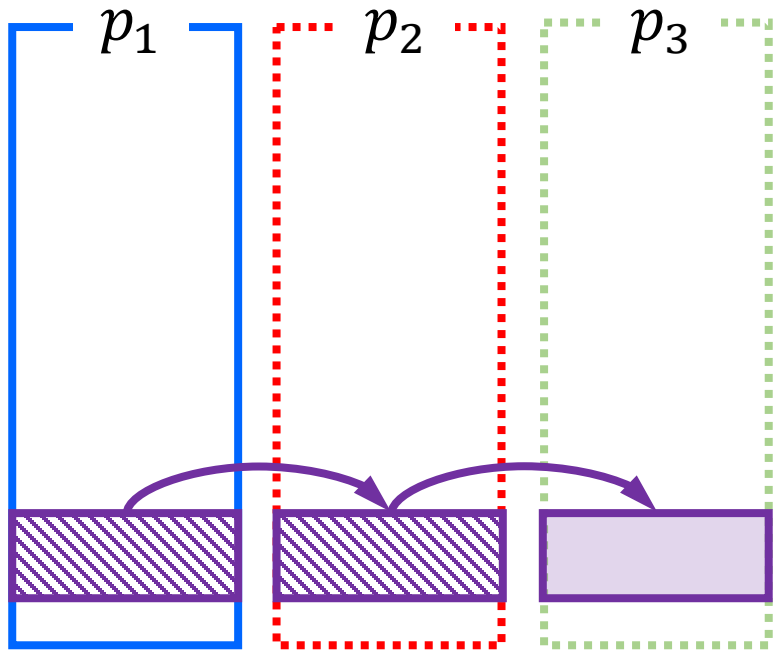


technique: composite-to-prime (SK)

k-dimensional

1-dimensional

SK

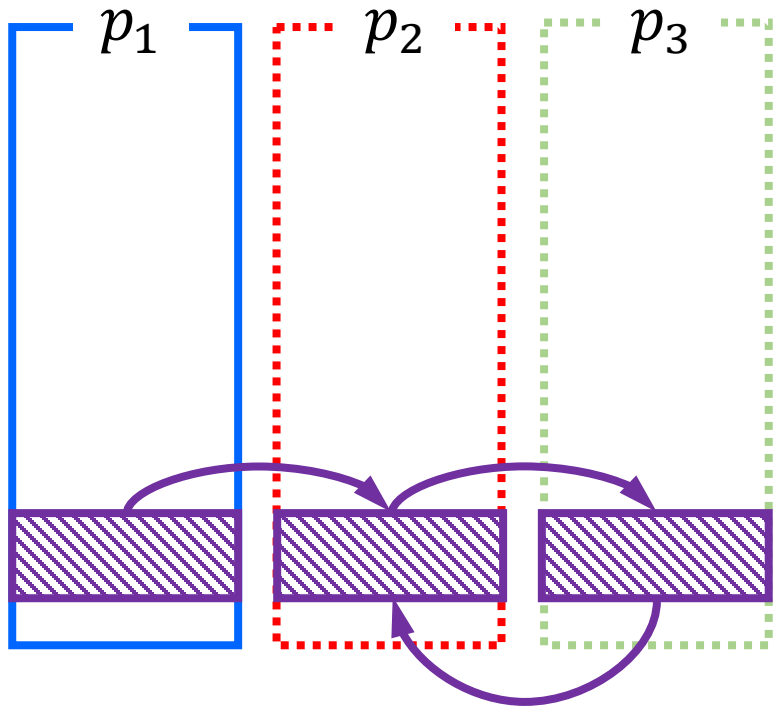


technique: composite-to-prime (SK)

k-dimensional

1-dimensional

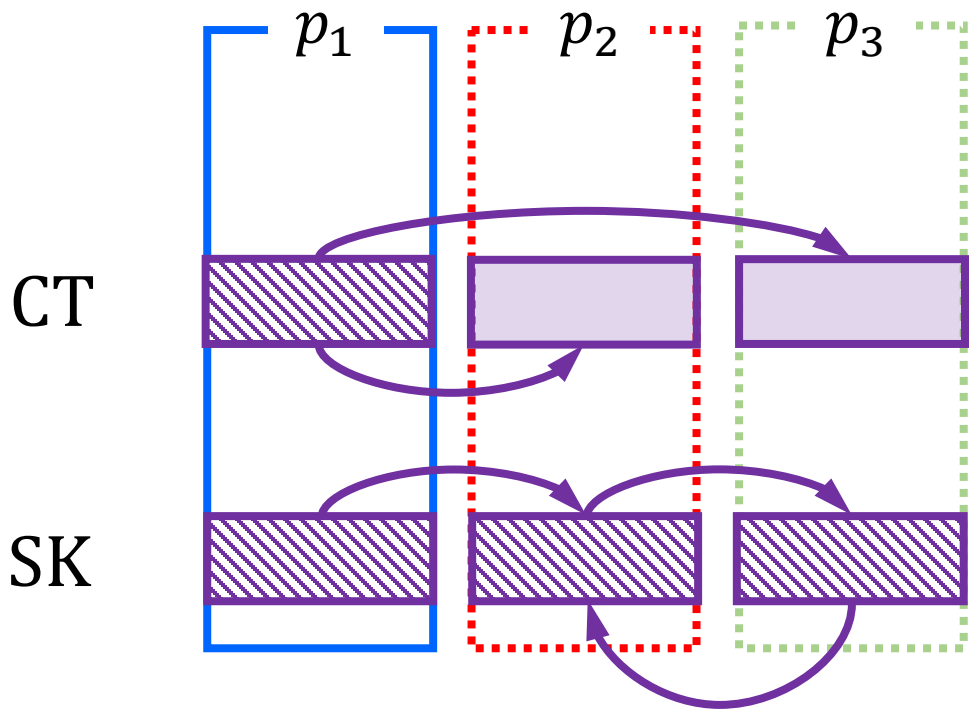
SK

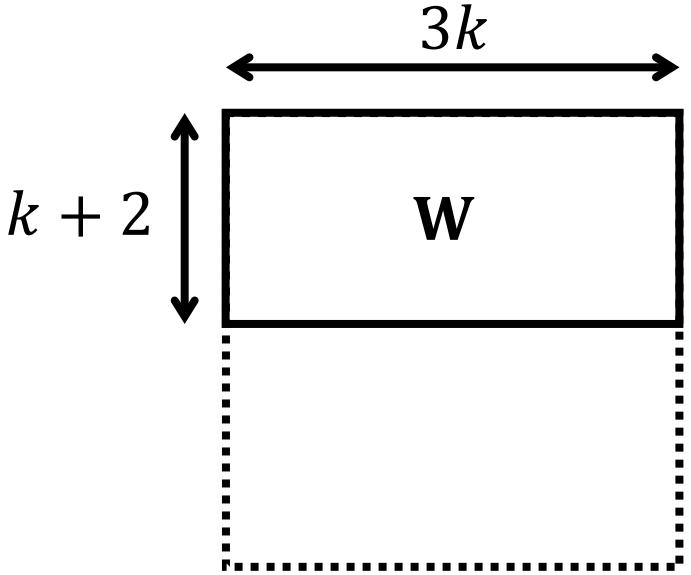


technique: composite-to-prime

k-dimensional

1-dimensional



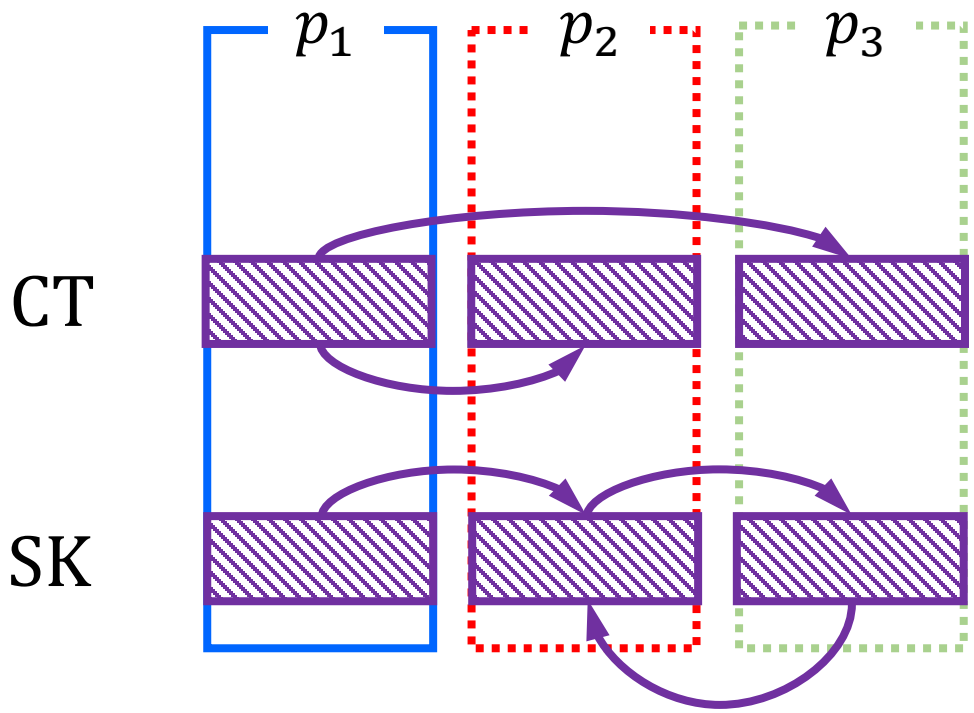


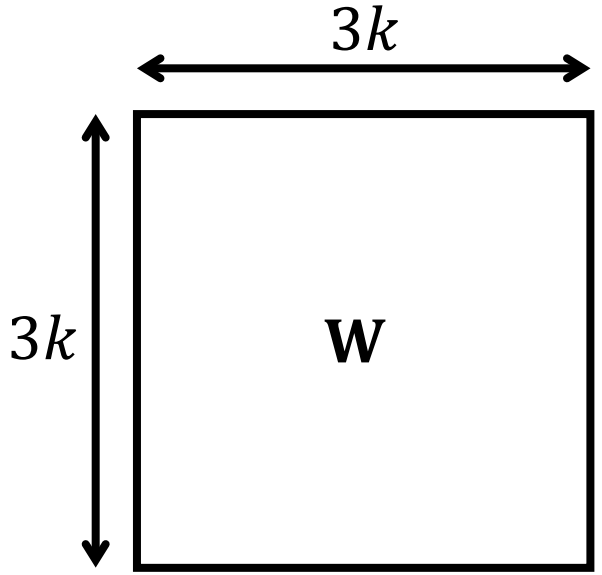
$MDDH$

technique: final

k-dimensional

1-dimensional





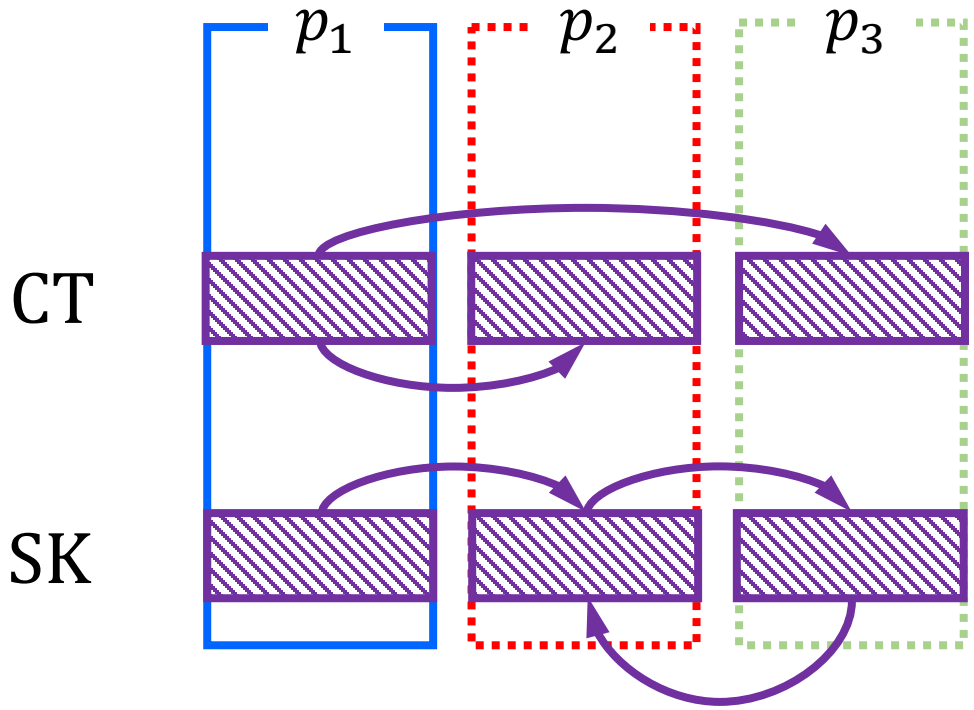
$MDDH$

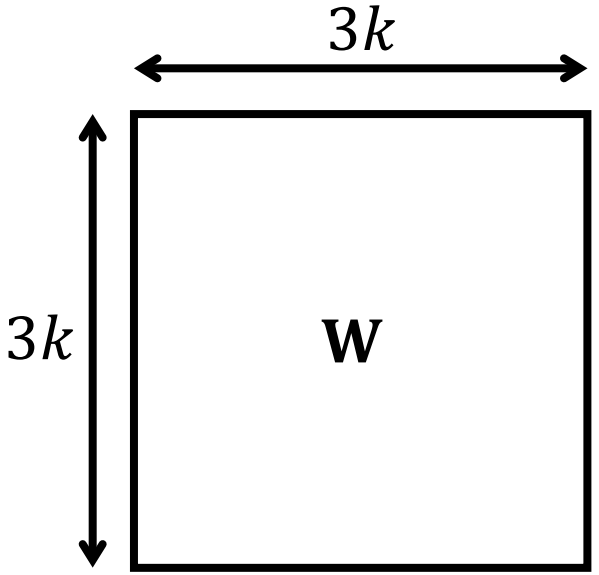
technique: final

k-dimensional

1-dimensional

~~shorter parameters~~



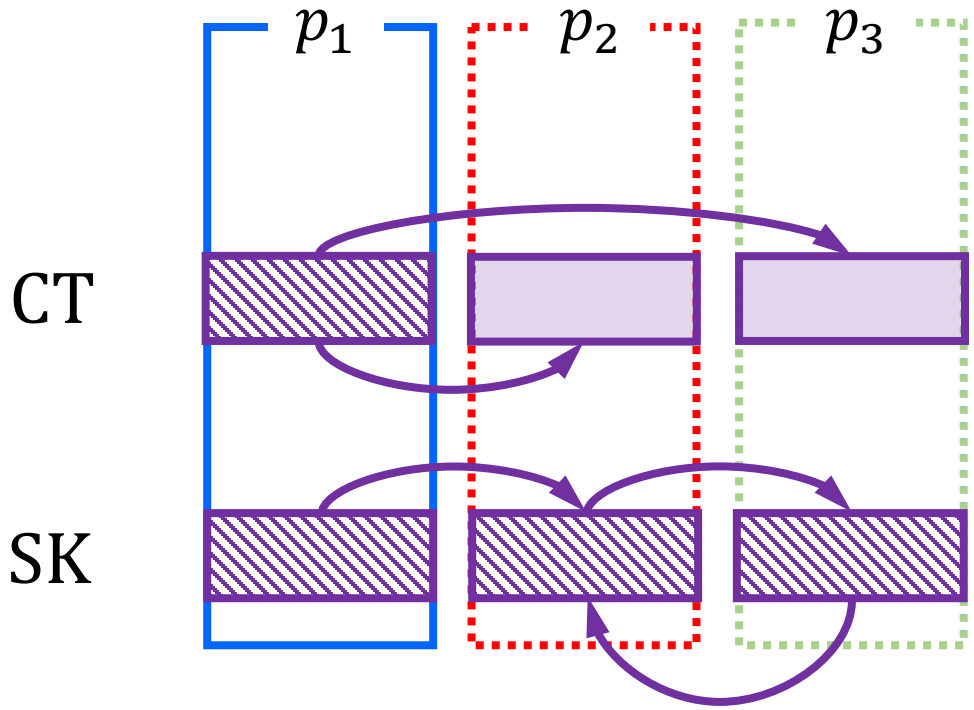


$MDDH$

technique: final

k-dimensional

1-dimensional

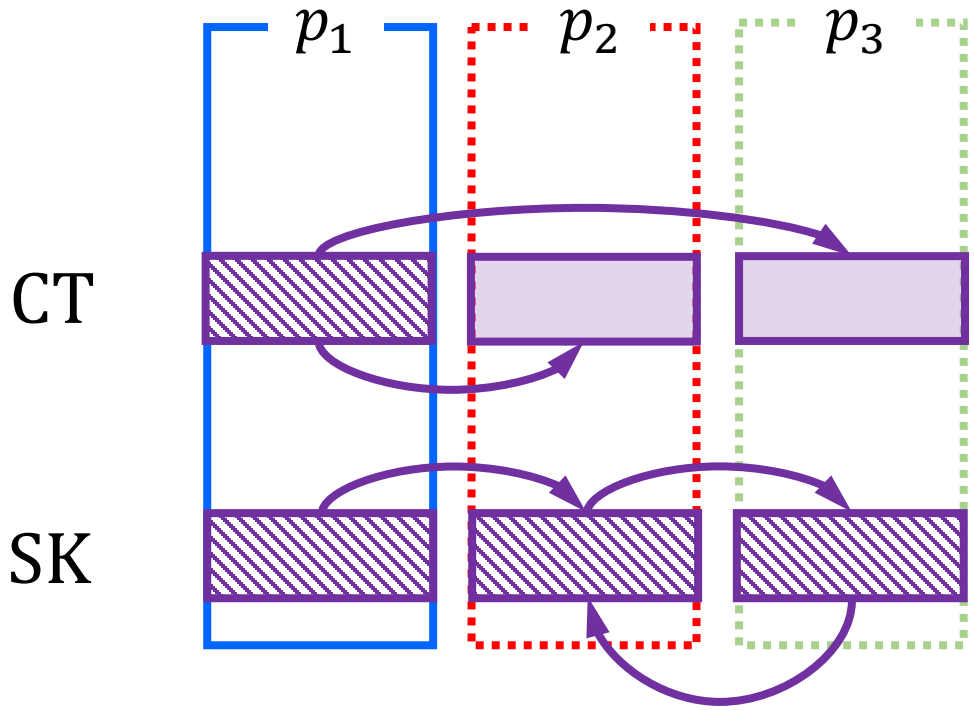


one k-dimensional

technique: final

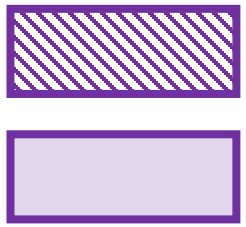
k-dimensional

1-dimensional



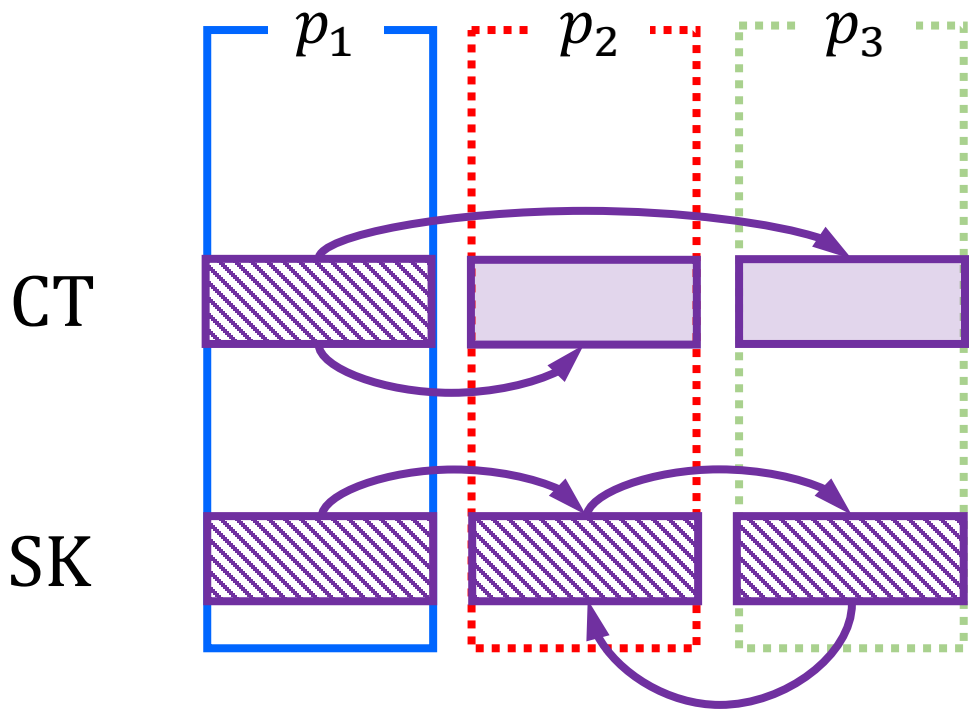
one k-dimensional ⟶ $2k + 1$

technique: final



k-dimensional

1-dimensional



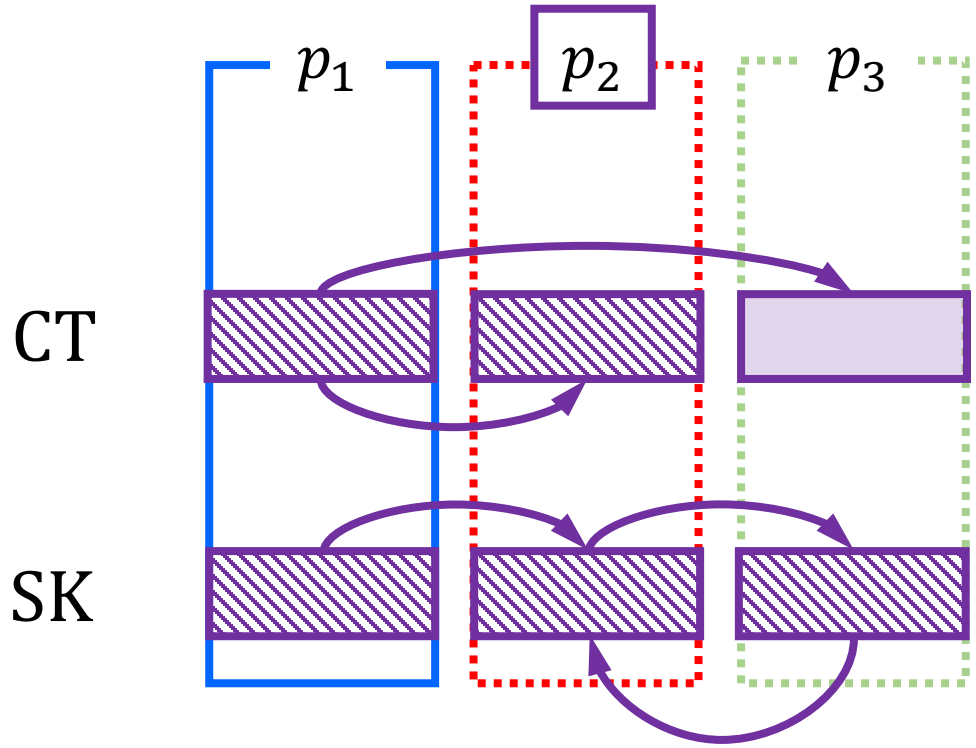
one k-dimensional ⟶ $2k + 1$

which subspace?

technique: final

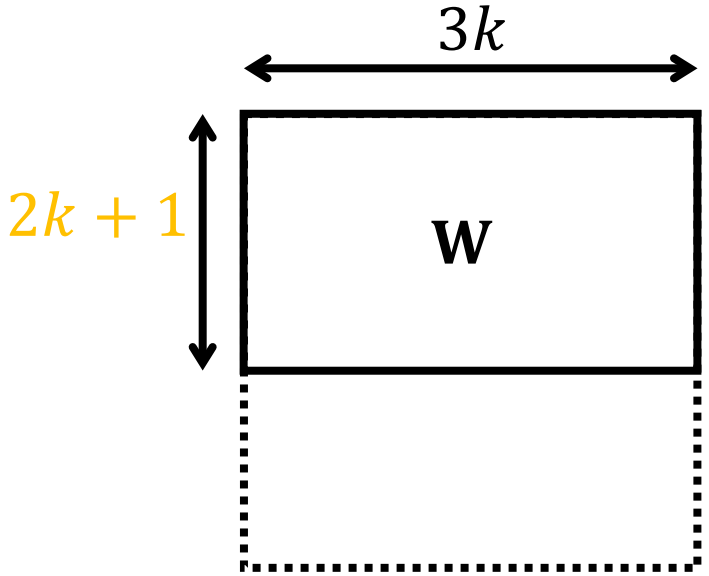
k-dimensional

1-dimensional



one k-dimensional

many-use?

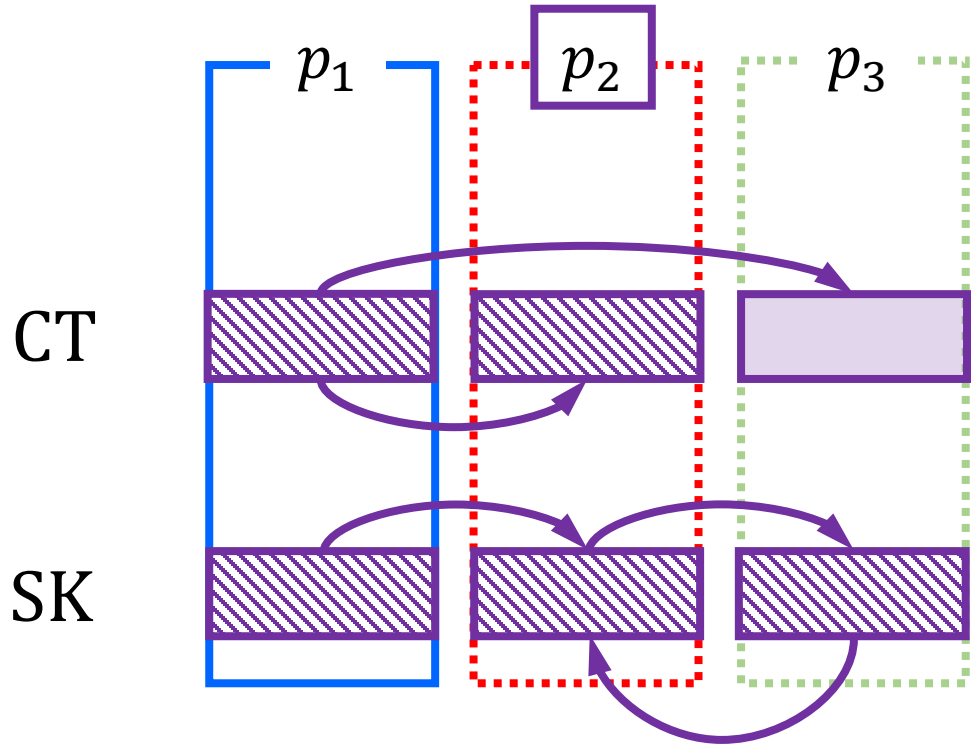


$MDDH$

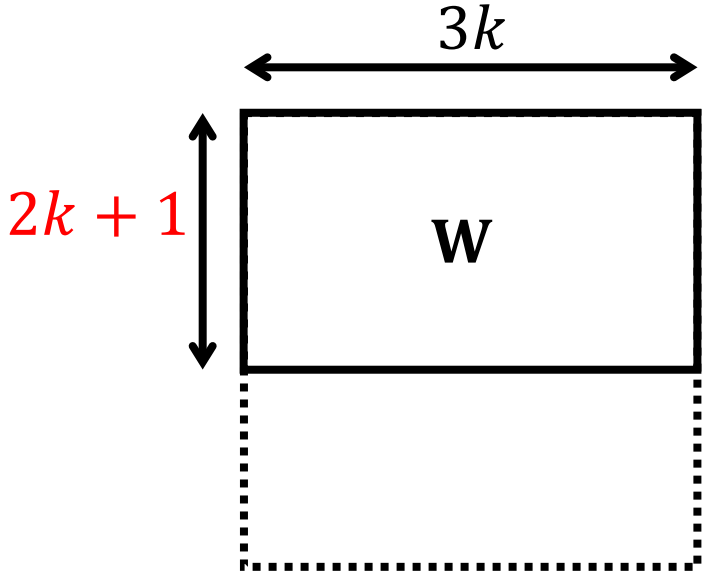
technique: final

k-dimensional

1-dimensional



one k-dimensional

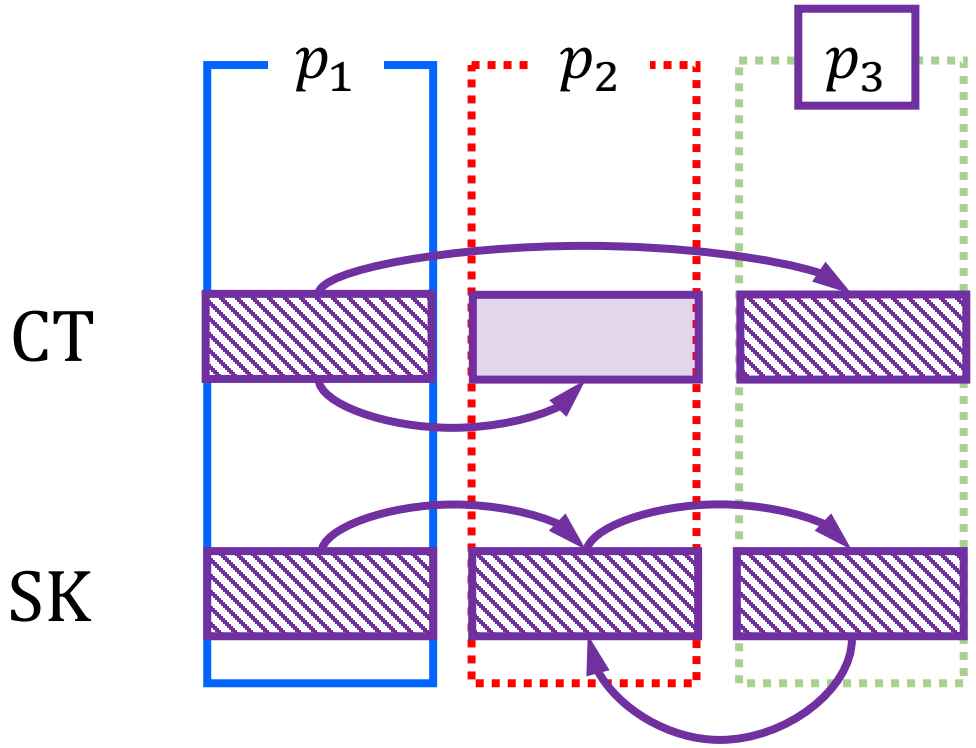


$MDDH$

technique: final

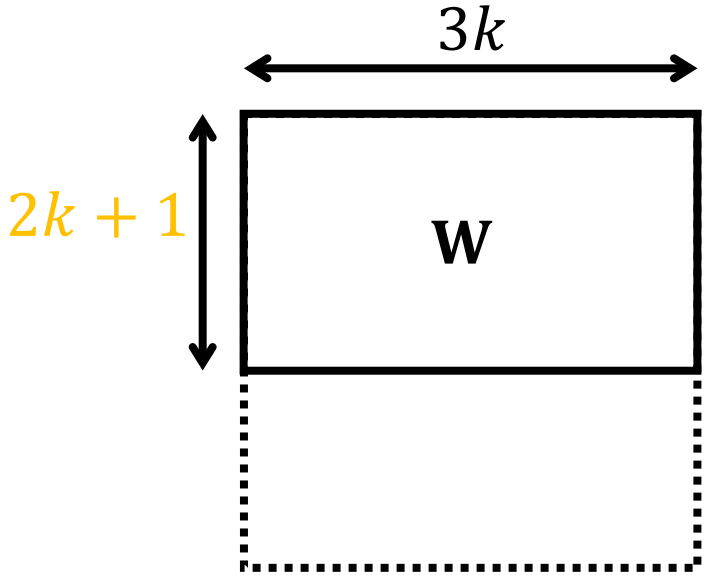
k-dimensional

1-dimensional



one k-dimensional

many-use?

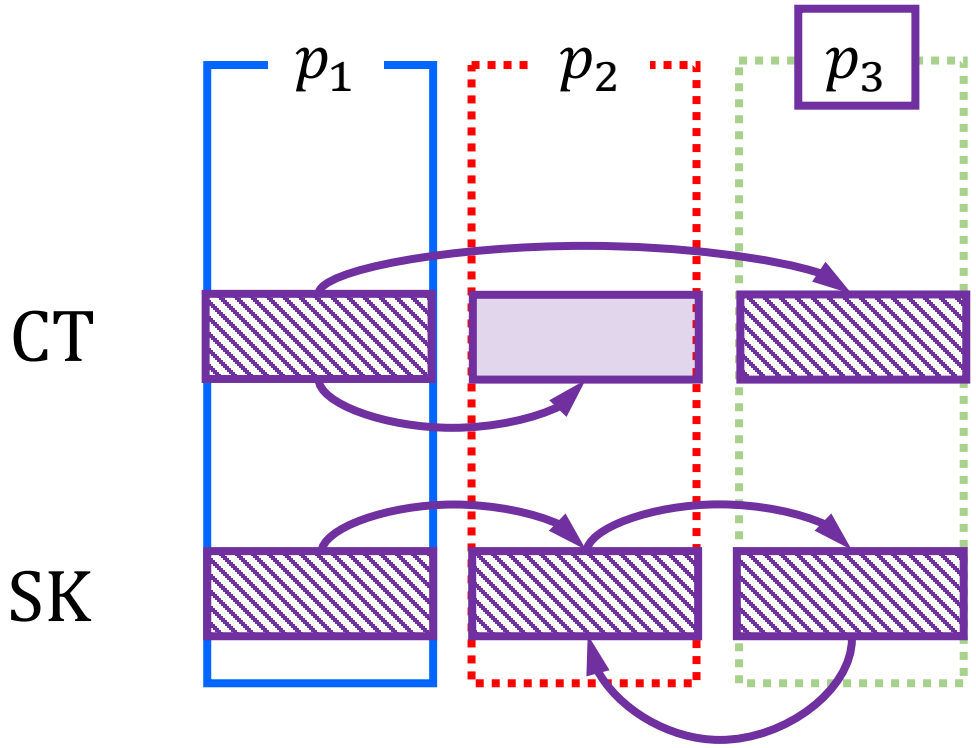


$MDDH$

technique: final

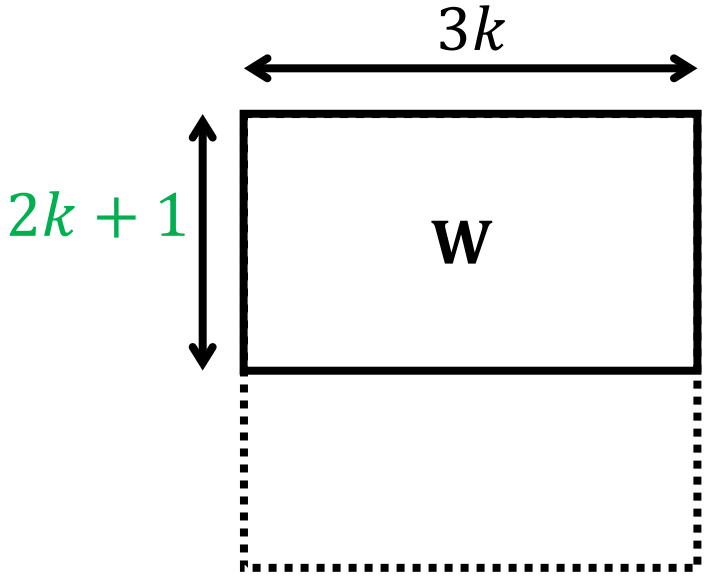
k-dimensional

1-dimensional



one k-dimensional

many-use



$MDDH$

summary

— our decentralized MA-ABE scheme for NC1 ——————————

fully adaptively secure

↓ many-use of attribute

↓ shorter parameters

summary

— our decentralized MA-ABE scheme for NC1 ——————————

fully adaptively secure

many-use of attribute

shorter parameters

remove the random oracle?

Thanks for your listening!