

Multi-Client Attribute-Based and Predicate Encryption from Standard Assumptions

David Pointcheval^{1,2}

Robert Schädlich²

December 5, 2024

¹ Cosmian, Paris, France

² DIENS, École normale supérieure, PSL University, CNRS, Inria, Paris, France

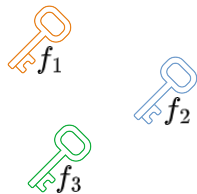


Attribute-Based Encryption (ABE) [SW05]

$\text{Enc}(\text{mpk}, x, \mu) \rightarrow \text{ct}_x$



$\text{KeyGen}(\text{msk}, f) \rightarrow \text{dk}_f$

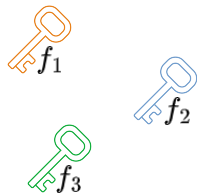


Attribute-Based Encryption (ABE) [SW05]

$\text{Enc}(\text{mpk}, x, \mu) \rightarrow \text{ct}_x$



$\text{KeyGen}(\text{msk}, f) \rightarrow \text{dk}_f$



$\text{Dec}(\text{dk}_{f_i}, \text{ct}_x)$



if some $f_i(x) = 1$



if all $f_i(x) = 0$

Attribute-Based Encryption (ABE) [SW05]

attribute-based encryption: **public** input
predicate encryption: **private** input

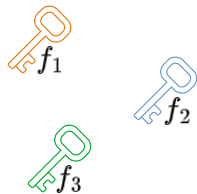
↓

$$\text{Enc}(\text{mpk}, x, \mu) \rightarrow \text{ct}_x$$



$$\text{KeyGen}(\text{msk}, f) \rightarrow \text{dk}_f$$

↑
public input



$$\text{Dec}(\text{dk}_{f_i}, \text{ct}_x)$$

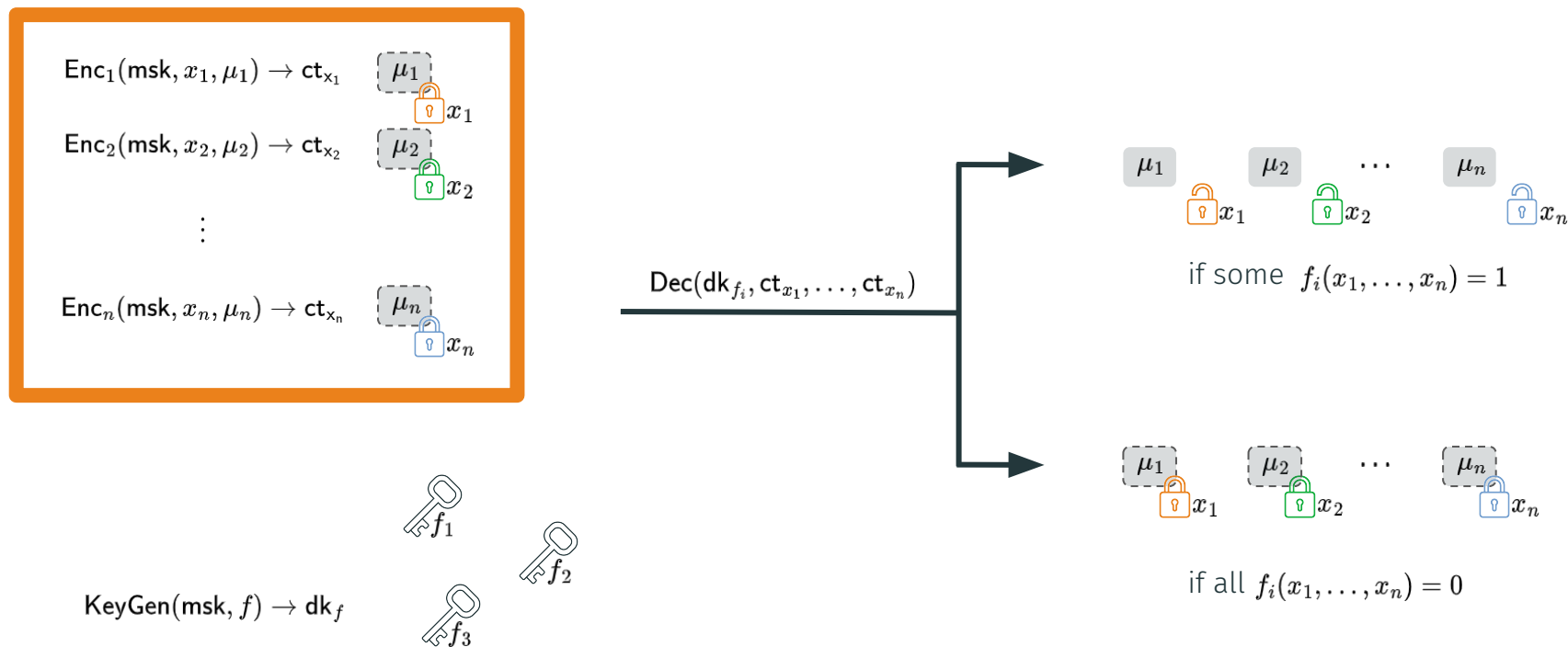


if some $f_i(x) = 1$



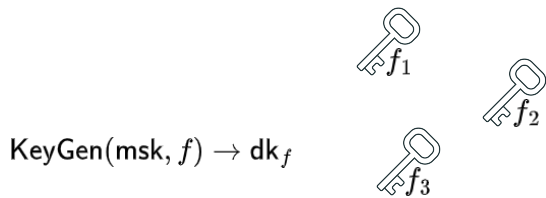
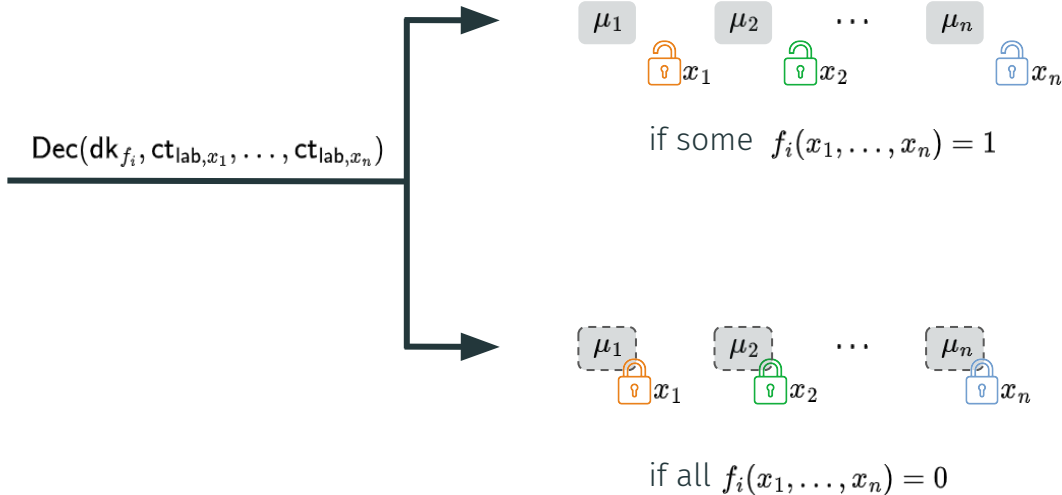
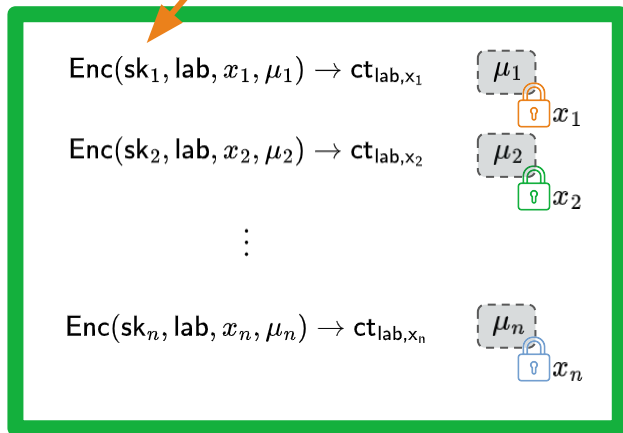
if all $f_i(x) = 0$

Multi-Input Attribute-Based Encryption (MI-ABE) [BJK⁺18]



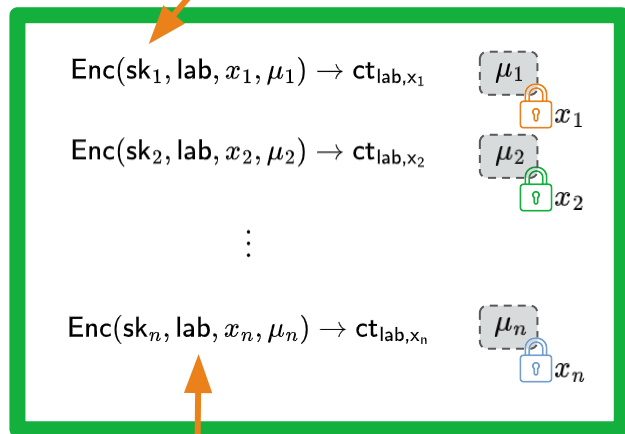
Multi-Client Attribute-Based Encryption (MC-ABE)

1st new feature:
separation & corruption of secret keys



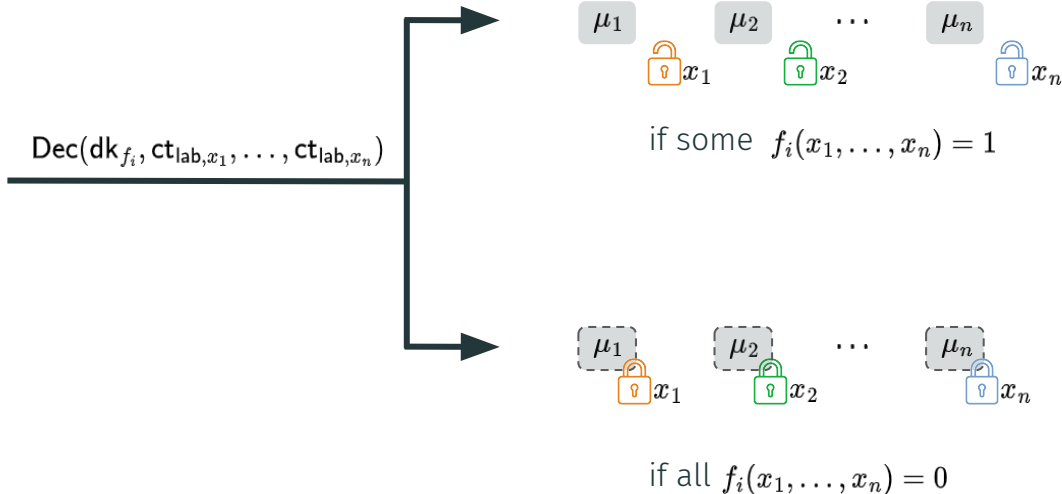
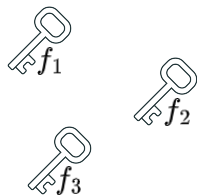
Multi-Client Attribute-Based Encryption (MC-ABE)

1st new feature:
separation & corruption of secret keys



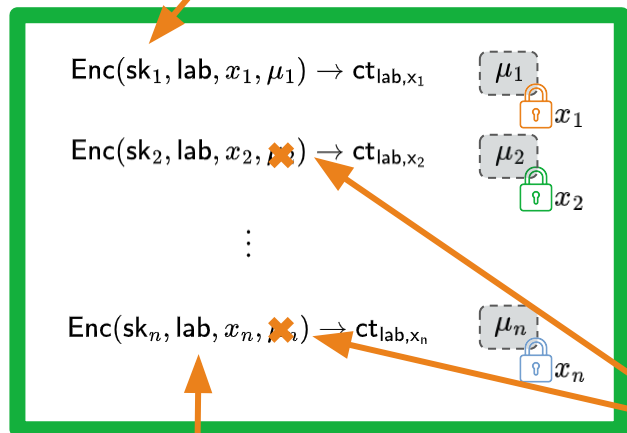
2nd new feature:
encryption w.r.t. labels

$\text{KeyGen}(\text{msk}, f) \rightarrow \text{dk}_f$



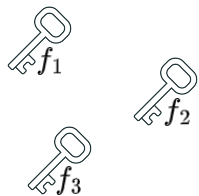
Multi-Client Attribute-Based Encryption (MC-ABE)

1st new feature:
separation & corruption of secret keys



2nd new feature:
encryption w.r.t. labels

$\text{KeyGen}(\text{msk}, f) \rightarrow \text{dk}_f$



$\text{Dec}(\text{dk}_{f_i}, \text{ct}_{\text{lab}, x_1}, \dots, \text{ct}_{\text{lab}, x_n})$

w.l.o.g., only 1st client
encrypts message



if some $f_i(x_1, \dots, x_n) = 1$




if all $f_i(x_1, \dots, x_n) = 0$

Existing MI-ABE

Work	Policy Class	Assumption	Remarks
[C:AYY22]	NC ¹	KOALA	--- only arity 2
[C:ARYY23]	P	Evasive LWE, Tensor LWE	

Existing MI-ABE

Work	Policy Class	Assumption	Remarks
[C:AYY22]	NC ¹	KOALA	--- only arity 2
[C:ARYY23]	P	Evasive LWE, Tensor LWE	
[EC:FFMV23]	Conjunctions of P	LWE	+++ supports corruptions --- no collusions
[C:ATY23]	Conjunctions of NC ¹	MDDH	



$$f(x_1, \dots, x_n) = f_1(x_1) \wedge \dots \wedge f_n(x_n)$$

Existing MI-ABE

Work	Policy Class	Assumption	Remarks
[C:AYY22]	NC ¹	KOALA	only arity 2
[C:ARYY23]	P	Evasive LWE, Tensor LWE	
[EC:FFMV23]	Conjunctions of P	LWE	+++ supports ...
[C:ATY23]	Conjunctions of NC ¹		

↑

$$f(x_1, \dots, x_n) = f_1(x_1) \wedge \dots \wedge f_n(x_n)$$

Is it possible to build MC-ABE
(or even MI-ABE) from standard
assumptions for global policies?

Existing MI-ABE

Work	Policy Class	Assumption	Remarks
[C:AYY22]	NC ¹	KOALA	only arity 2
[C:ARYY23]	P	Evasive LWE, Tensor LWE	
[EC:FFMV23]	Conjunctions of P	LWE	+++ supports ...
[C:ATY23]	Conjunctions of NC ¹		

↑

$$f(x_1, \dots, x_n) = f_1(x_1) \wedge \dots \wedge f_n(x_n)$$

Is it possible to build MC-ABE
(or even MI-ABE) from standard
assumptions for global policies?

YES!

but ...

Contributions (MC-ABE)

Note: MI-ABE for polynomial arity and NC^1 policies \Rightarrow Witness Encryption for NP

Contributions (MC-ABE)

Note: MI-ABE for polynomial arity and NC^1 policies \Rightarrow Witness Encryption for NP

We consider settings that circumvent this implication.

1) Weaker Policies (\leadsto cannot verify NP relation)

- MC-ABE for NC^0 policies
- MC-ABE for constant-threshold policies

Contributions (MC-ABE)

Note: MI-ABE for polynomial arity and NC^1 policies \Rightarrow Witness Encryption for NP

We consider settings that circumvent this implication.

- 1) **Weaker Policies (\leadsto cannot verify NP relation)**
 - MC-ABE for NC^0 policies
 - MC-ABE for constant-threshold policies
- 2) **Short Inputs (\leadsto WE with exp-size ciphertexts)**
 - MC-ABE for NC^1 for parameters s.t. $|x_1| + \dots + |x_n| = O(\log \lambda)$

Contributions (MC-ABE)

Note: MI-ABE for polynomial arity and NC^1 policies \Rightarrow Witness Encryption for NP

We consider settings that circumvent this implication.

- 1) **Weaker Policies (\leadsto cannot verify NP relation)**
 - MC-ABE for NC^0 policies
 - MC-ABE for constant-threshold policies
- 2) **Short Inputs (\leadsto WE with exp-size ciphertexts)**
 - MC-ABE for NC^1 for parameters s.t. $|x_1| + \dots + |x_n| = O(\log \lambda)$
- 3) **Weaker Security Model (\leadsto MC-ABE with OT labels \nRightarrow MI-ABE)**
 - MC-ABE for NC^1 under one-time label restriction

Contributions (MC-PE)

What does already exist?

- 1) **Direct Construction of MI-PE ([EC:FFMV23])**
 - conjunctions of bounded-depth circuits
 - (poly arity and no corruptions) or (constant arity and corruptions)
 - no collusions!
- 2) **Generic Compiler MI-ABE + Lockable Obfuscation \Rightarrow MI-PE ([C:AYY22])**
 - only arity 2 (or constant arity and weak security)
 - no corruptions

Contributions (MC-PE)

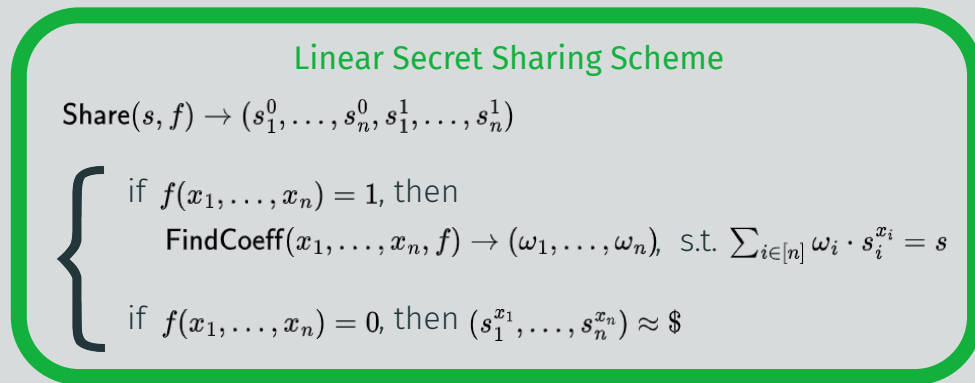
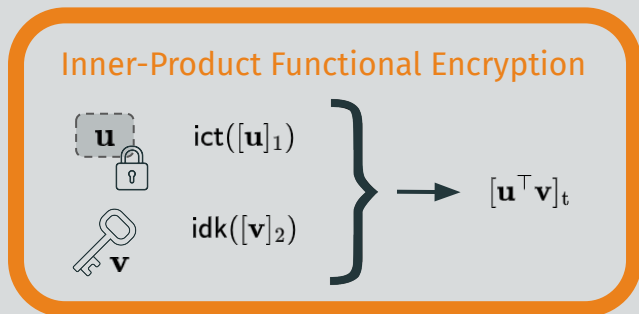
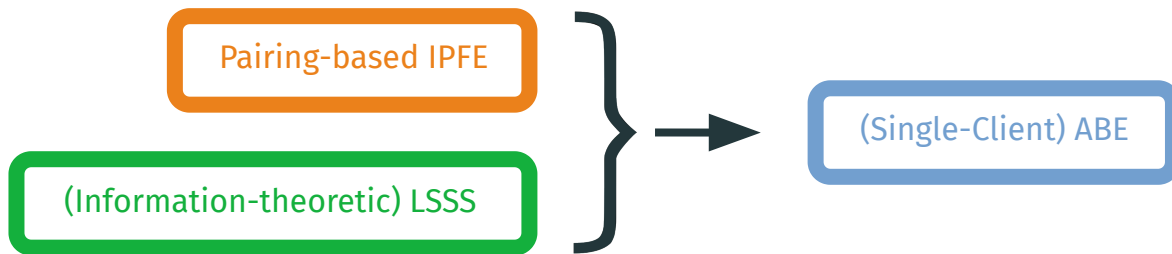
What does already exist?

- 1) **Direct Construction of MI-PE ([EC:FFMV23])**
 - conjunctions of bounded-depth circuits
 - (poly arity and no corruptions) or (constant arity and corruptions)
 - no collusions!
- 2) **Generic Compiler MI-ABE + Lockable Obfuscation \Rightarrow MI-PE ([C:AYY22])**
 - only arity 2 (or constant arity and weak security)
 - no corruptions

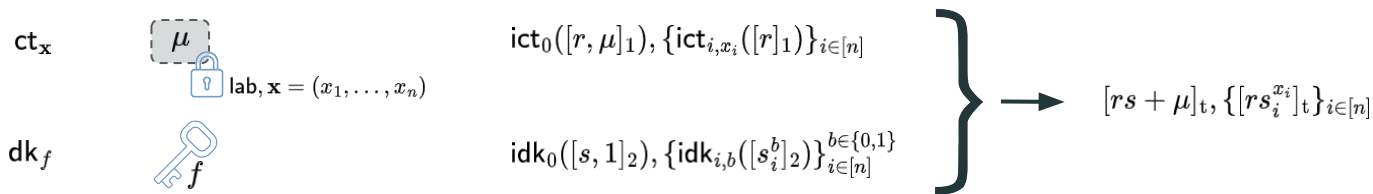
This Work — A New Generic Compiler

Constant-Arity MC-ABE + Lockable Obfuscation \Rightarrow Constant-Arity MC-PE

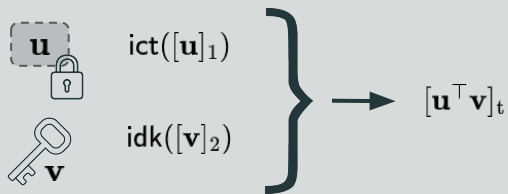
Framework for Pairing-based KP-ABE



Framework for Pairing-based KP-ABE



Inner-Product Functional Encryption

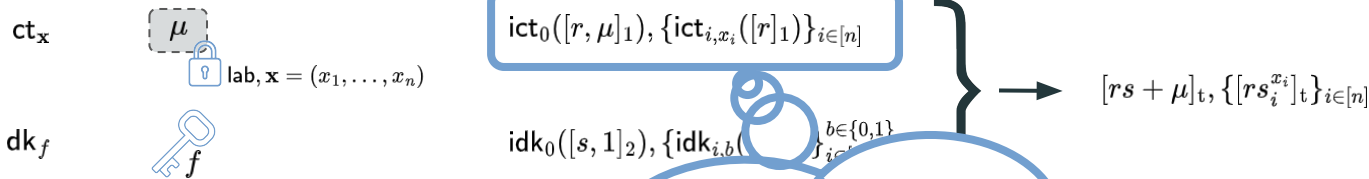


Linear Secret Sharing Scheme

$\text{Share}(s, f) \rightarrow (s_1^0, \dots, s_n^0, s_1^1, \dots, s_n^1)$

$\left\{ \begin{array}{l} \text{if } f(x_1, \dots, x_n) = 1, \text{ then} \\ \quad \text{FindCoeff}(x_1, \dots, x_n, f) \rightarrow (\omega_1, \dots, \omega_n), \text{ s.t. } \sum_{i \in [n]} \omega_i \cdot s_i^{x_i} = s \\ \text{if } f(x_1, \dots, x_n) = 0, \text{ then } (s_1^{x_1}, \dots, s_n^{x_n}) \approx \$ \end{array} \right.$

Framework for Pairing-based KP-ABE



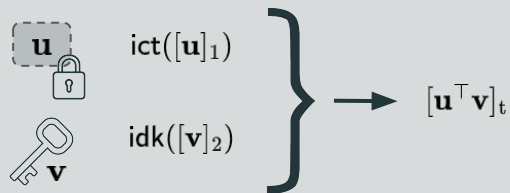
How to distribute this?

... using random oracles,
i.e., $[r]_1 = H(\text{lab})$?

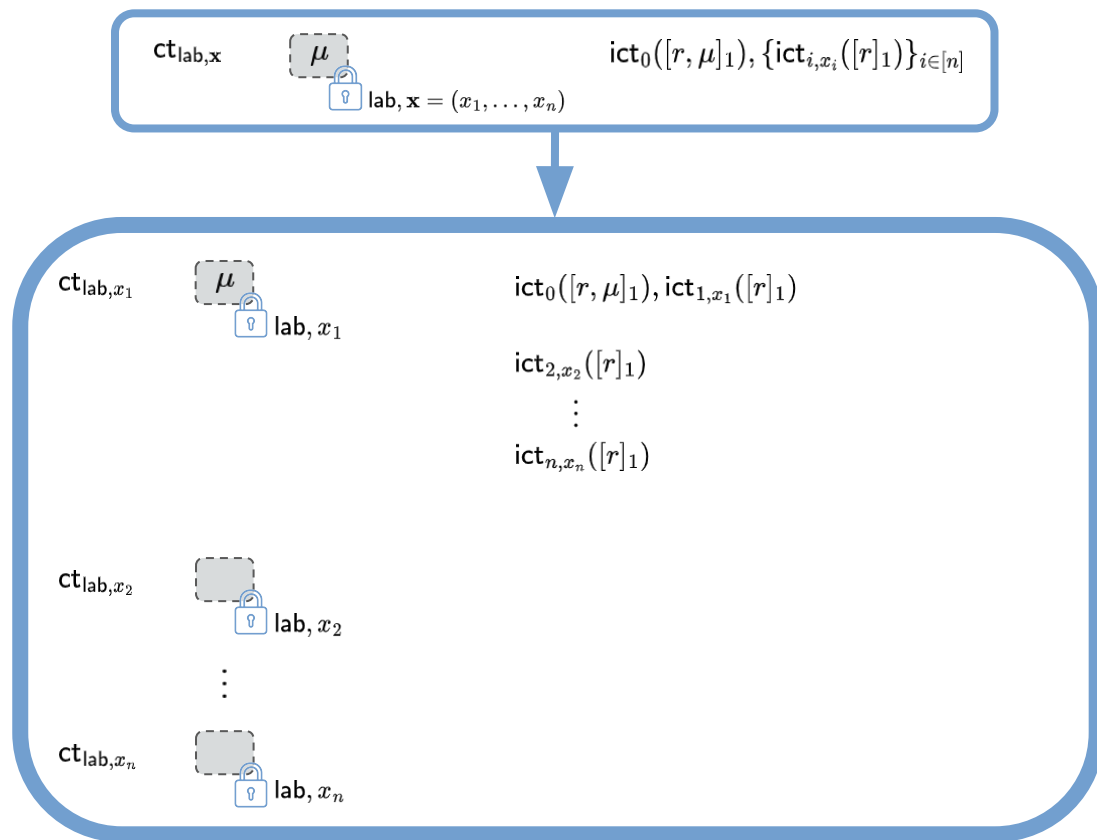
\leadsto only one-time labels :(

$\left\{ \begin{array}{l} \text{if } f(x_1, \dots, x_n) = 1, \text{ then} \\ \quad \text{FindCoeff}(x_1, \dots, x_n, f) \rightarrow (\omega_1, \dots, \omega_n), \text{ s.t. } \sum_{i \in [n]} \omega_i \cdot s_i^{x_i} = s \\ \text{if } f(x_1, \dots, x_n) = 0, \text{ then } (s_1^{x_1}, \dots, s_n^{x_n}) \approx \$ \end{array} \right.$

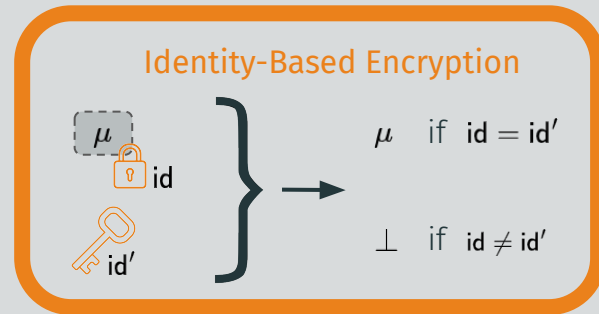
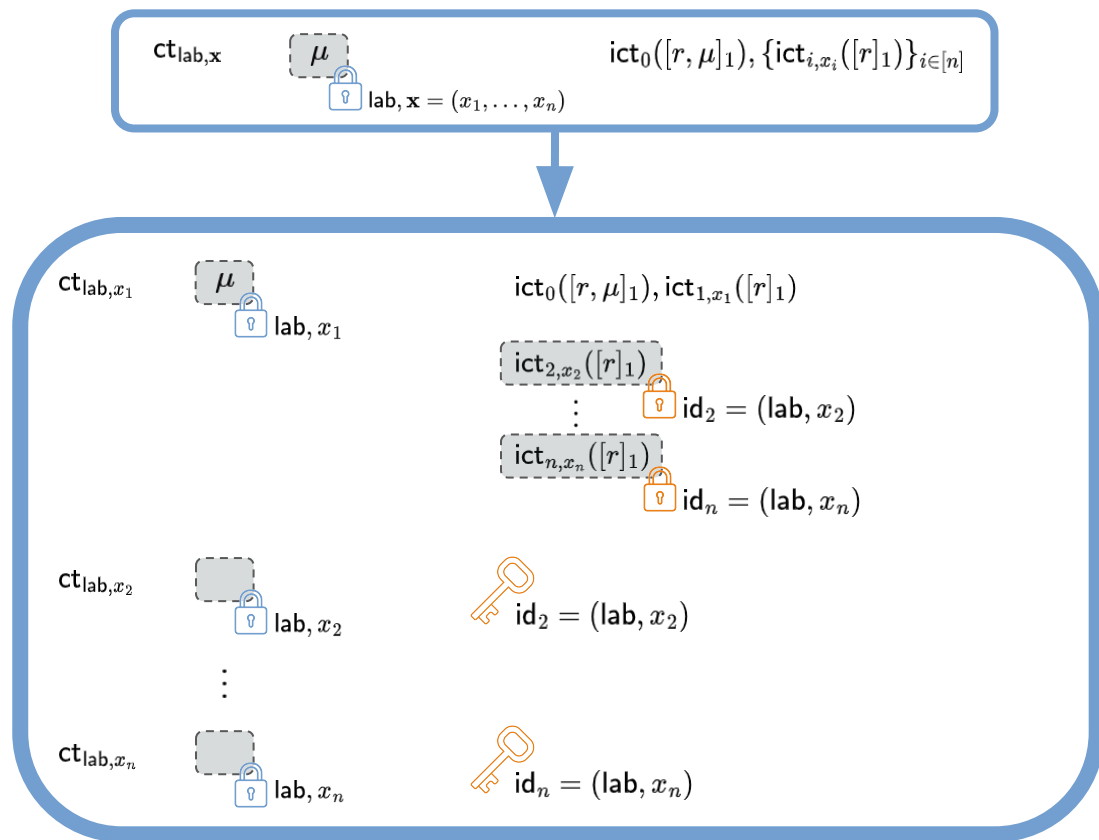
Inner-Product Functional Encryption



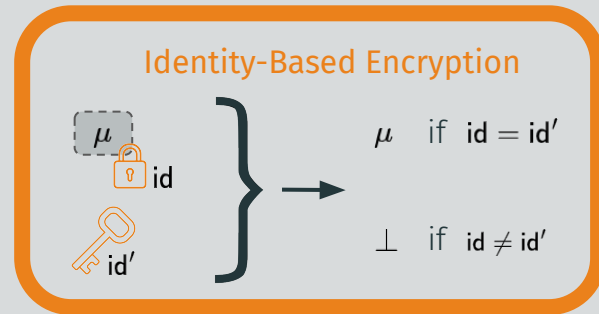
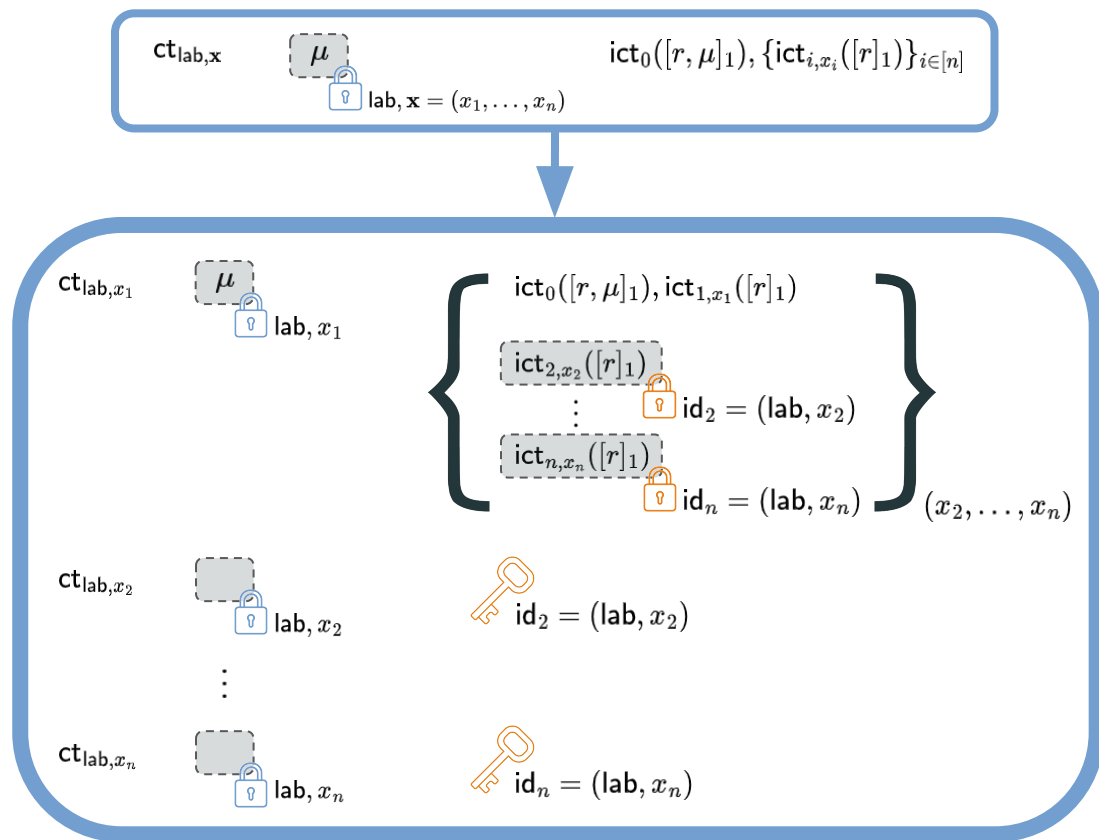
Distributed Encryption



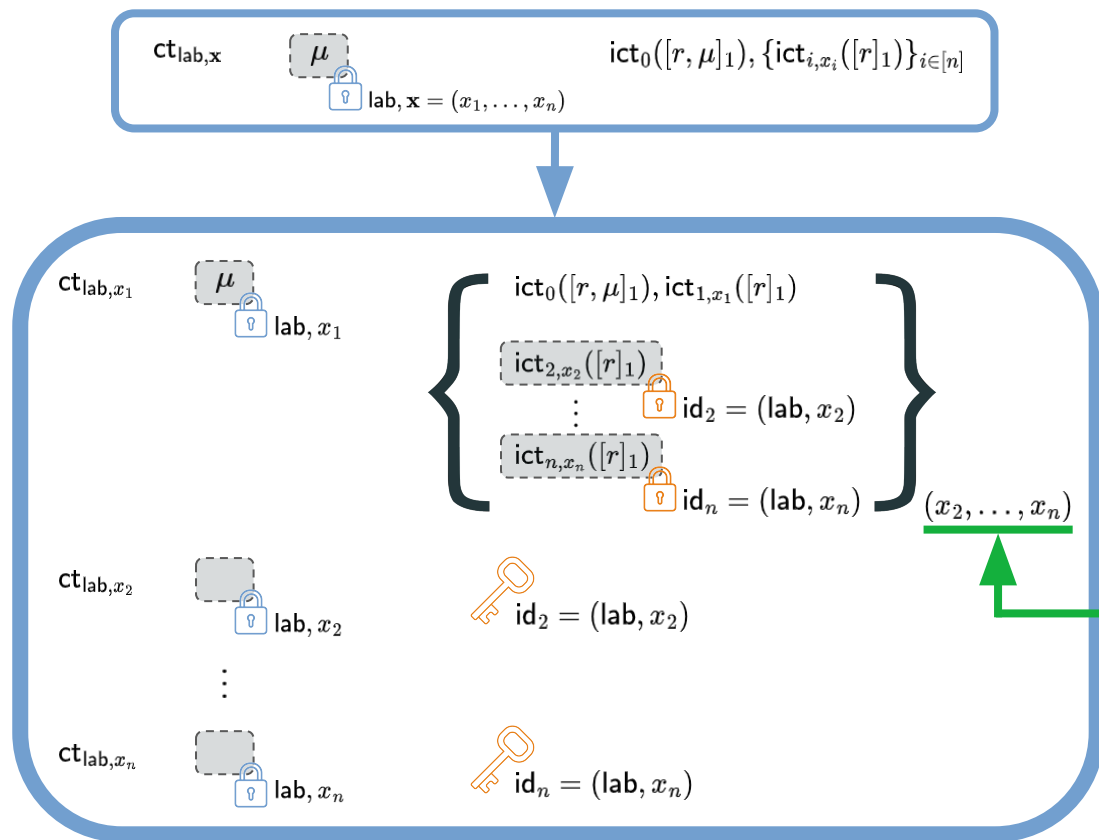
Distributed Encryption



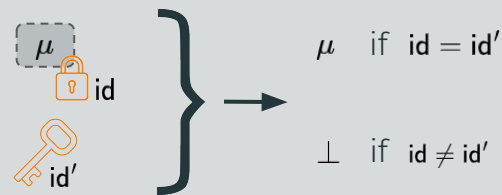
Distributed Encryption



Distributed Encryption



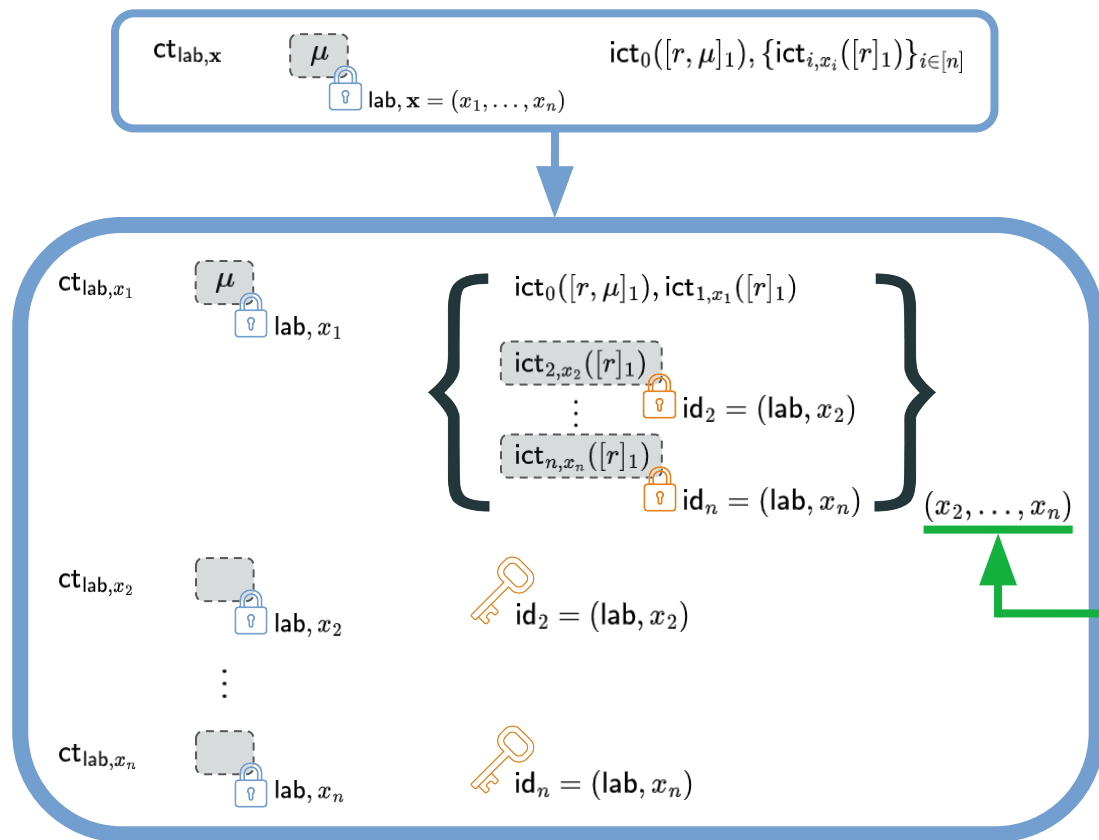
Identity-Based Encryption



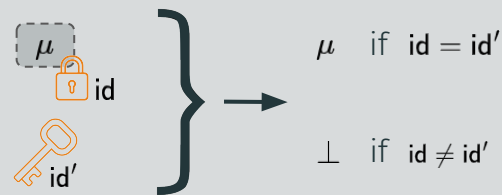
Which $(x_2, \dots, x_n) \in \{0, 1\}^{n-1}$ do we need?

- all \rightarrow NC¹ policies for $O(\log \lambda)$ inputs

Distributed Encryption



Identity-Based Encryption



Which $(x_2, \dots, x_n) \in \{0, 1\}^{n-1}$ do we need?

- all \rightarrow NC^1 policies for $O(\log \lambda)$ inputs
- constant-size subsets \rightarrow NC^0 policies and constant-threshold policies

From MC-ABE to MC-PE using [Lockable Obfuscation]

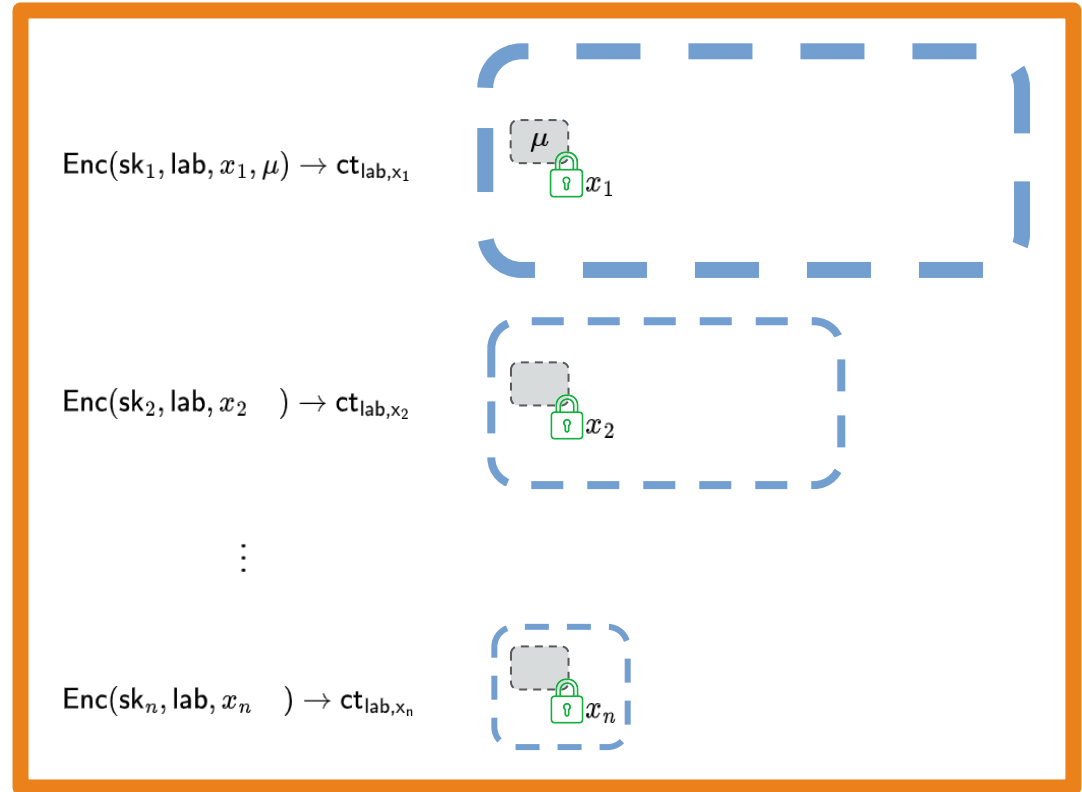
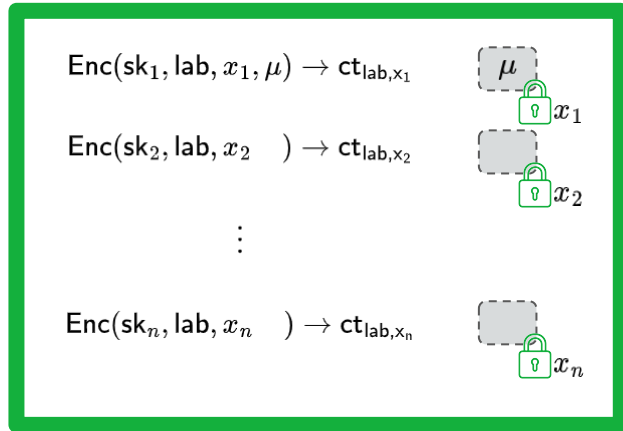
$$\text{Enc}(\text{sk}_1, \text{lab}, x_1, \mu) \rightarrow \text{ct}_{\text{lab}, x_1}$$



$$\text{Enc}(\text{sk}_1, \text{lab}, x_1, \mu) \rightarrow \text{ct}_{\text{lab}, x_1}$$

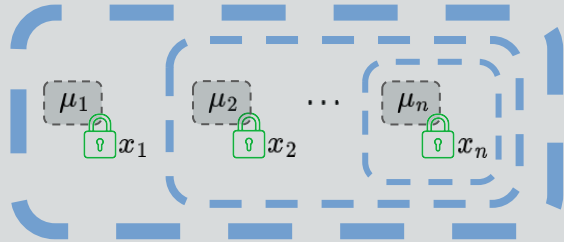


From MC-ABE to MC-PE using [Lockable Obfuscation]



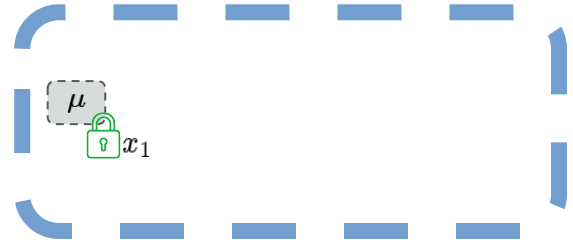
From MC-ABE to MC-PE using [Lockable Obfuscation]

“Communication” between the obfuscated circuits?

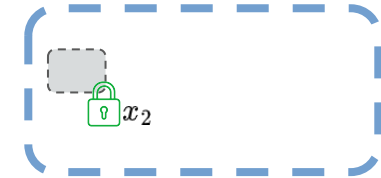


nested evaluation checks
global authorization

$$\text{Enc}(\text{sk}_1, \text{lab}, x_1, \mu) \rightarrow \text{ct}_{\text{lab}, x_1}$$



$$\text{Enc}(\text{sk}_2, \text{lab}, x_2) \rightarrow \text{ct}_{\text{lab}, x_2}$$



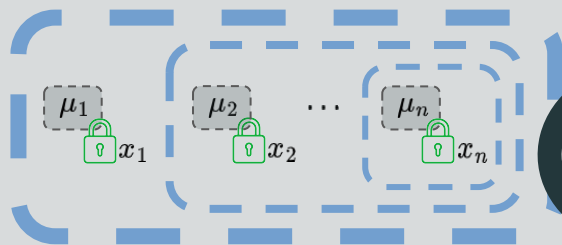
\vdots

$$\text{Enc}(\text{sk}_n, \text{lab}, x_n) \rightarrow \text{ct}_{\text{lab}, x_n}$$



From MC-ABE to MC-PE using [Lockable Obfuscation]

“Communication” between the obfuscated circuits?



nested evaluation checks
global authorization

Security against corruptions?

- use n independent MC-ABE instances with rotated slots
- nested recursion to check **global** authorization in **each slot**

$\text{Enc}(\text{sk}_1, \text{lab}, \dots, \text{ct})$

μ

x_n

Conclusion

- definition of MC-ABE and MC-PE
- construction of MC-ABE for global policies from SXDH
- generic compiler for constant-arity MC-ABE \Rightarrow constant-arity MC-PE from LWE
- previous to this work, these results were unknown even for MI-ABE

Conclusion

- definition of MC-ABE and MC-PE
- construction of MC-ABE for global policies from SXDH
- generic compiler for constant-arity MC-ABE \Rightarrow constant-arity MC-PE from LWE
- previous to this work, these results were unknown even for MI-ABE

Thank you for your attention!



ia.cr/2024/1945