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

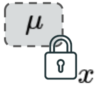
David Pointcheval[1,2] **Robert Schädlich**[2]

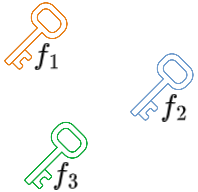
December 5, 2024

[1] Cosmian, Paris, France
[2] DIENS, École normale supérieure, PSL University, CNRS, Inria, Paris, France

Attribute-Based Encryption (ABE) [SW05]

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



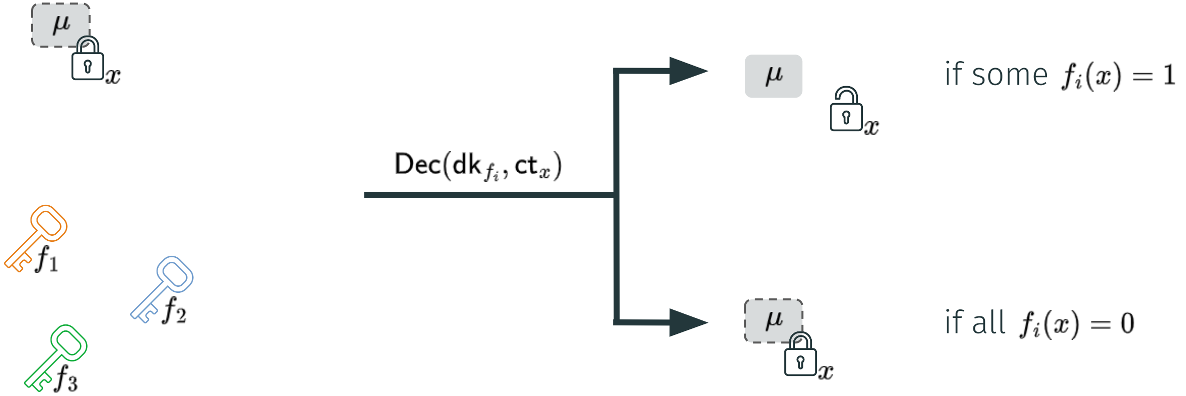


$\mathsf{KeyGen}(\mathsf{msk}, f) \rightarrow \mathsf{dk}_f$

Attribute-Based Encryption (ABE) [SW05]

$\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x$

$\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{dk}_f$



Attribute-Based Encryption (ABE) [SW05]

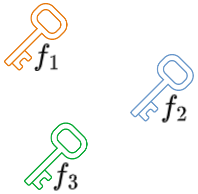
attribute-based encryption: **public** input
predicate encryption: **private** input

$\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x$

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

μ if some $f_i(x) = 1$

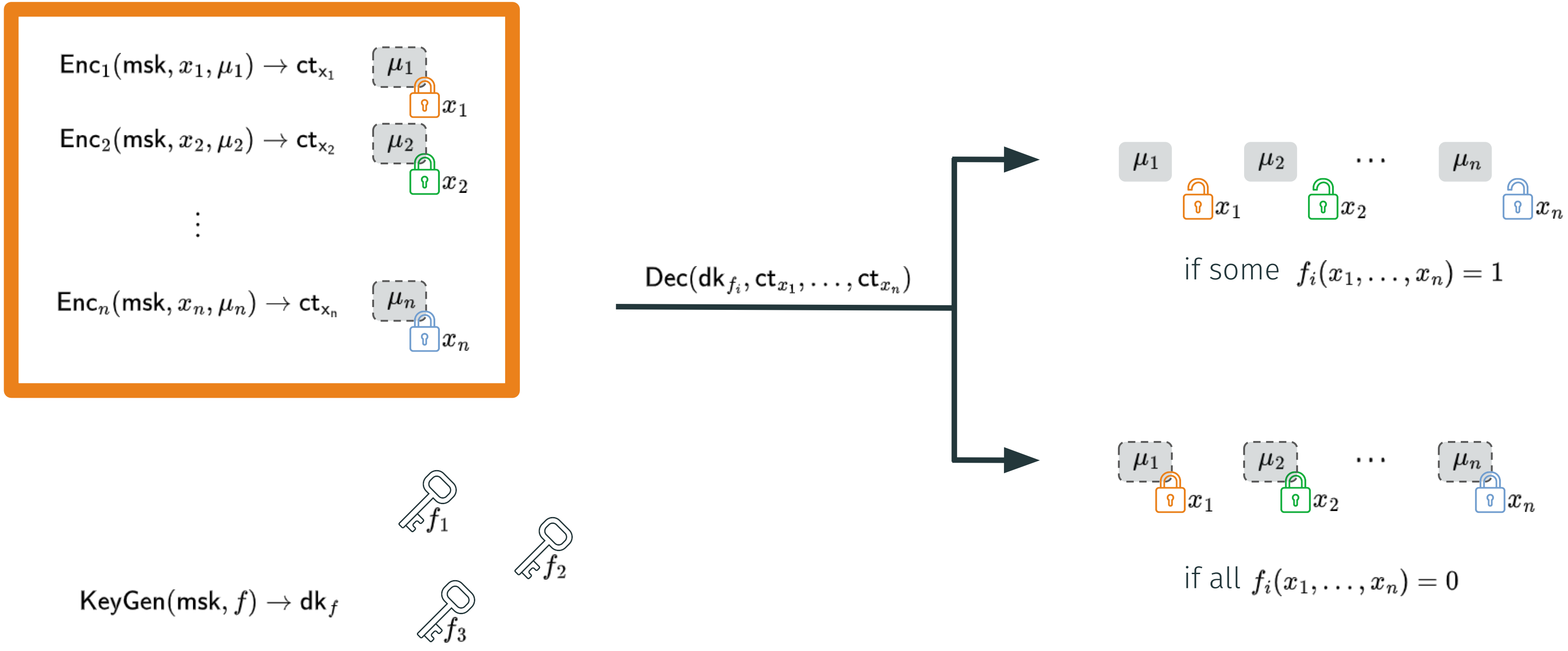
if all $f_i(x) = 0$



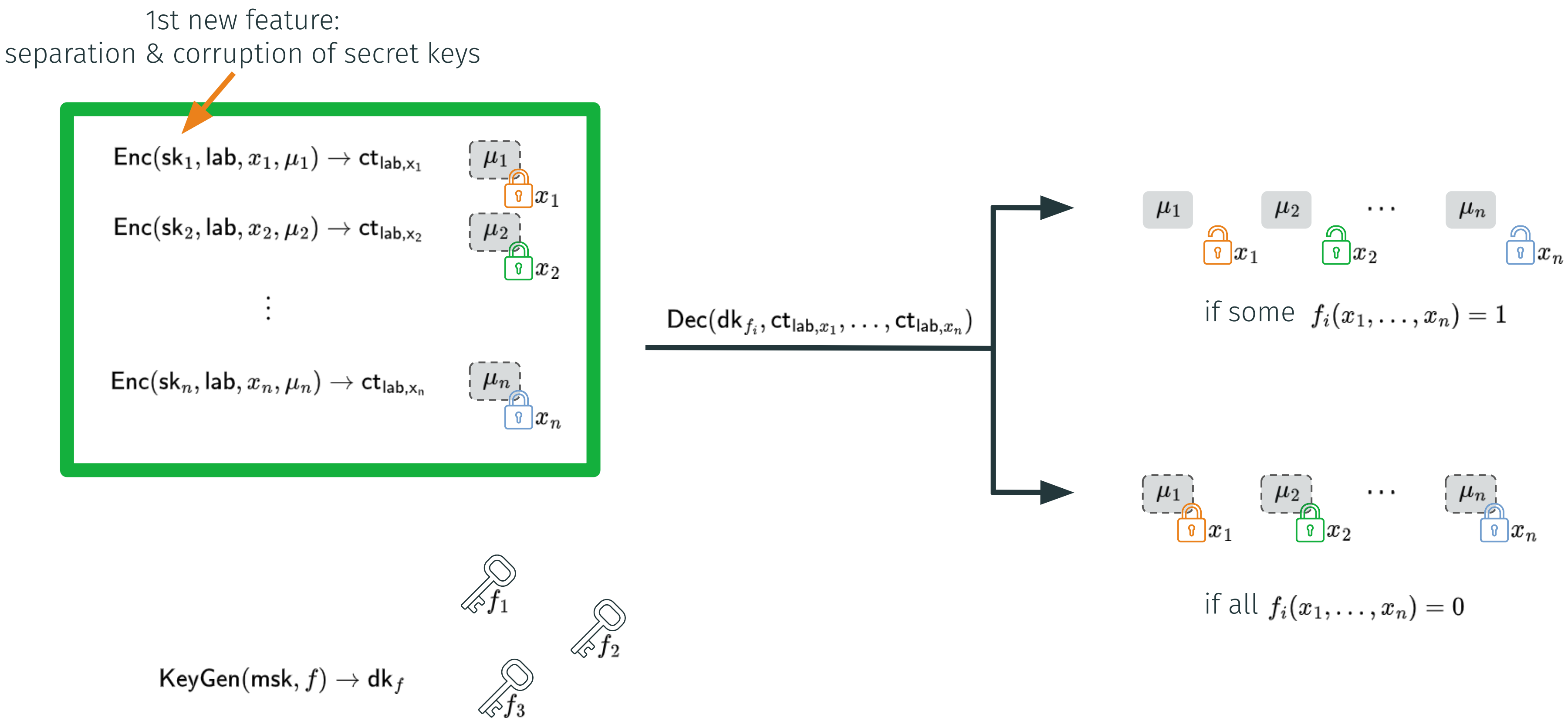
$\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{dk}_f$

public input

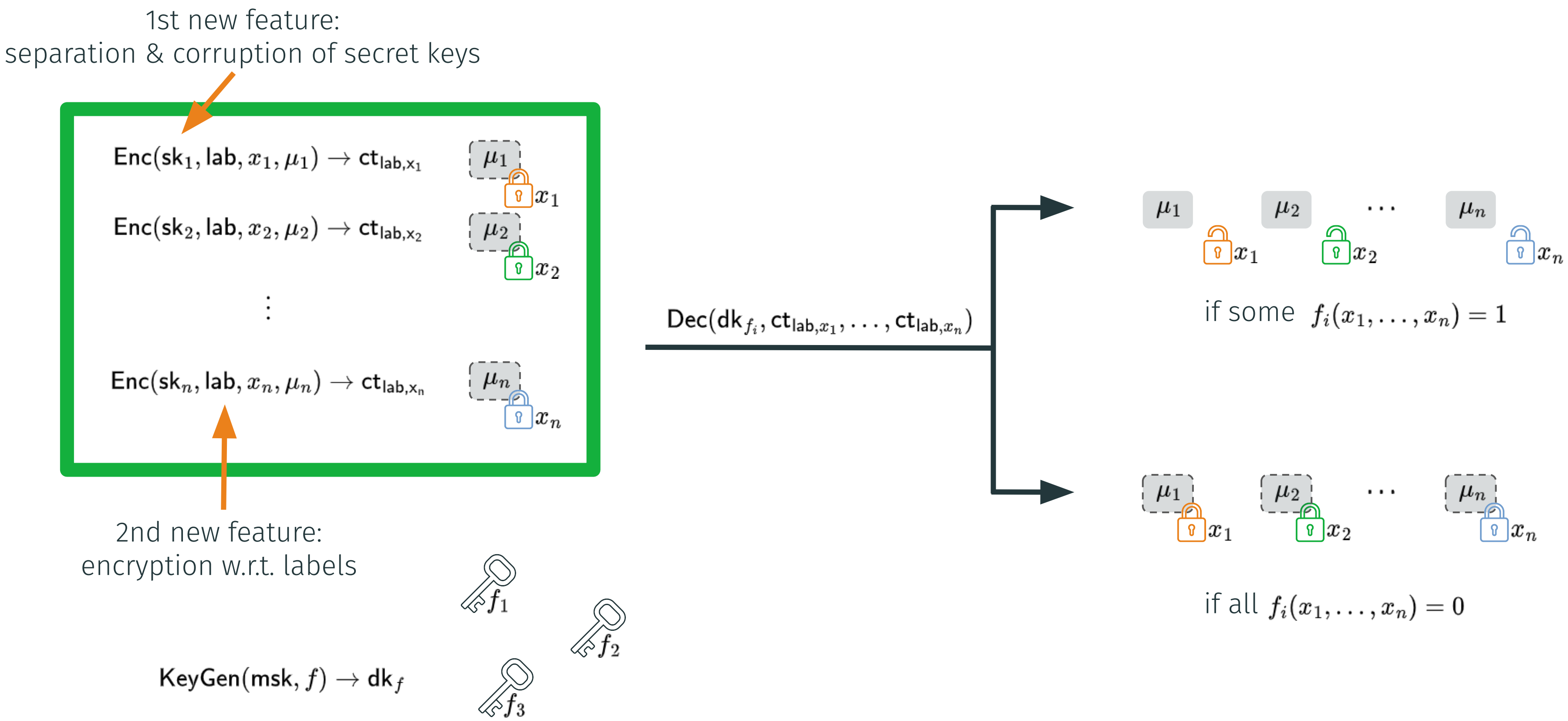
Multi-Input Attribute-Based Encryption (MI-ABE) [BJK+18]



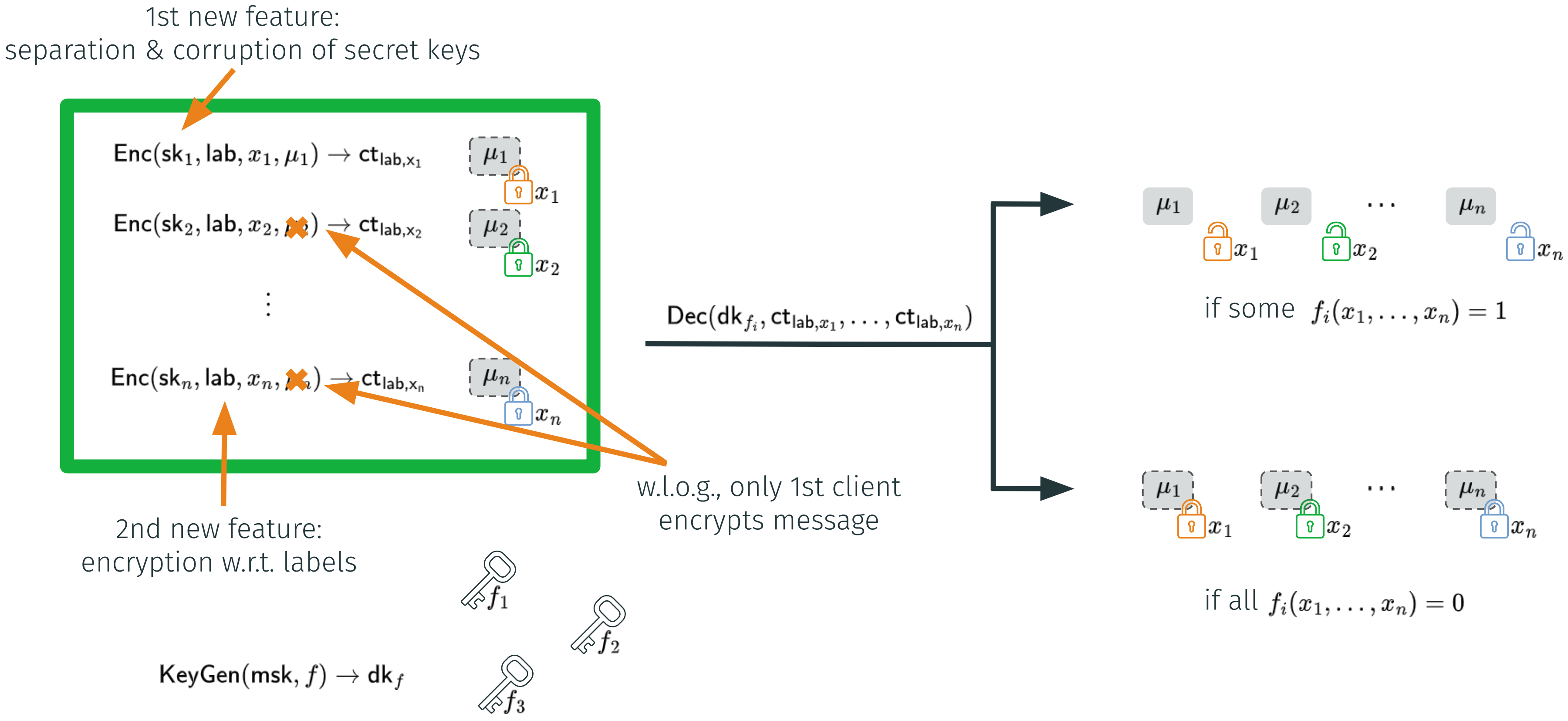
Multi-Client Attribute-Based Encryption (MC-ABE)



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



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



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	

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

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		

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

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]		

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

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 $\Longrightarrow$ Witness Encryption for NP

Contributions (MC-ABE)

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

We consider settings that circumvent this implication.

1) **Weaker Policies ($\rightsquigarrow$ 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 $\Longrightarrow$ Witness Encryption for NP

We consider settings that circumvent this implication.

1) **Weaker Policies ($\rightsquigarrow$ cannot verify NP relation)**
   - MC-ABE for NC^0 policies
   - MC-ABE for constant-threshold policies

2) **Short Inputs ($\rightsquigarrow$ WE with exp-size ciphertexts)**
   - MC-ABE for NC^1 for parameters s.t. $|x_1| + \cdots + |x_n| = O(\log \lambda)$

Contributions (MC-ABE)

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

We consider settings that circumvent this implication.

1) **Weaker Policies ($\rightsquigarrow$ cannot verify NP relation)**
   - MC-ABE for NC^0 policies
   - MC-ABE for constant-threshold policies

2) **Short Inputs ($\rightsquigarrow$ WE with exp-size ciphertexts)**
   - MC-ABE for NC^1 for parameters s.t. $|x_1| + \cdots + |x_n| = O(\log \lambda)$

3) **Weaker Security Model ($\rightsquigarrow$ MC-ABE with OT labels $\not\Rightarrow$ 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 $\Longrightarrow$ 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 $\Longrightarrow$ 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 $\Longrightarrow$ Constant-Arity MC-PE

Framework for Pairing-based KP-ABE

Pairing-based IPFE

(Information-theoretic) LSSS

} → (Single-Client) ABE

Inner-Product Functional Encryption

$\mathbf{u}$: $\mathsf{ict}([\mathbf{u}]_1)$

$\mathbf{v}$: $\mathsf{idk}([\mathbf{v}]_2)$

} → $[\mathbf{u}^\top \mathbf{v}]_t$

Linear Secret Sharing Scheme

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

- if $f(x_1, \dots, x_n) = 1$, then
  $\mathsf{FindCoeff}(x_1, \dots, x_n, f) \to (\omega_1, \dots, \omega_n)$, s.t. $\sum_{i \in [n]} \omega_i \cdot s_i^{x_i} = s$
- if $f(x_1, \dots, x_n) = 0$, then $(s_1^{x_1}, \dots, s_n^{x_n}) \approx \$$

Framework for Pairing-based KP-ABE

$\mathsf{ct}_{\mathbf{x}}$ $\quad \mu$ $\quad \mathsf{lab}, \mathbf{x} = (x_1, \ldots, x_n)$ $\quad \mathsf{ict}_0([r, \mu]_1), \{\mathsf{ict}_{i,x_i}([r]_1)\}_{i \in [n]}$

dk_f $\quad f$ $\quad \mathsf{idk}_0([s, 1]_2), \{\mathsf{idk}_{i,b}([s_i^b]_2)\}_{i \in [n]}^{b \in \{0,1\}}$

$\longrightarrow [rs + \mu]_t, \{[rs_i^{x_i}]_t\}_{i \in [n]}$

Inner-Product Functional Encryption

$\mathbf{u}$ $\quad \mathsf{ict}([\mathbf{u}]_1)$

$\mathbf{v}$ $\quad \mathsf{idk}([\mathbf{v}]_2)$

$\longrightarrow [\mathbf{u}^\top \mathbf{v}]_t$

Linear Secret Sharing Scheme

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

- if $f(x_1, \ldots, x_n) = 1$, then
  $\mathsf{FindCoeff}(x_1, \ldots, x_n, f) \rightarrow (\omega_1, \ldots, \omega_n)$, s.t. $\sum_{i \in [n]} \omega_i \cdot s_i^{x_i} = s$
- if $f(x_1, \ldots, x_n) = 0$, then $(s_1^{x_1}, \ldots, s_n^{x_n}) \approx \$$

Framework for Pairi

How to distribute this?

$\mathsf{ct}_{\mathbf{x}}$ — μ locked under lab, $\mathbf{x} = (x_1, \ldots, x_n)$ — $\mathsf{ict}_0([r, \mu]_1), \{\mathsf{ict}_{i,x_i}([r]_1)\}_{i \in [n]}$

dk_f — f — $\mathsf{idk}_0([s, 1]_2), \{\mathsf{idk}_{i,b}([s_i^b]_2)\}_{i \in [n]}^{b \in \{0,1\}}$

$\rightarrow [rs + \mu]_t, \{[rs_i^{x_i}]_t\}_{i \in [n]}$

Inner-Product Functional Encryption

$\mathbf{u}$: $\mathsf{ict}([\mathbf{u}]_1)$

$\mathbf{v}$: $\mathsf{idk}([\mathbf{v}]_2)$

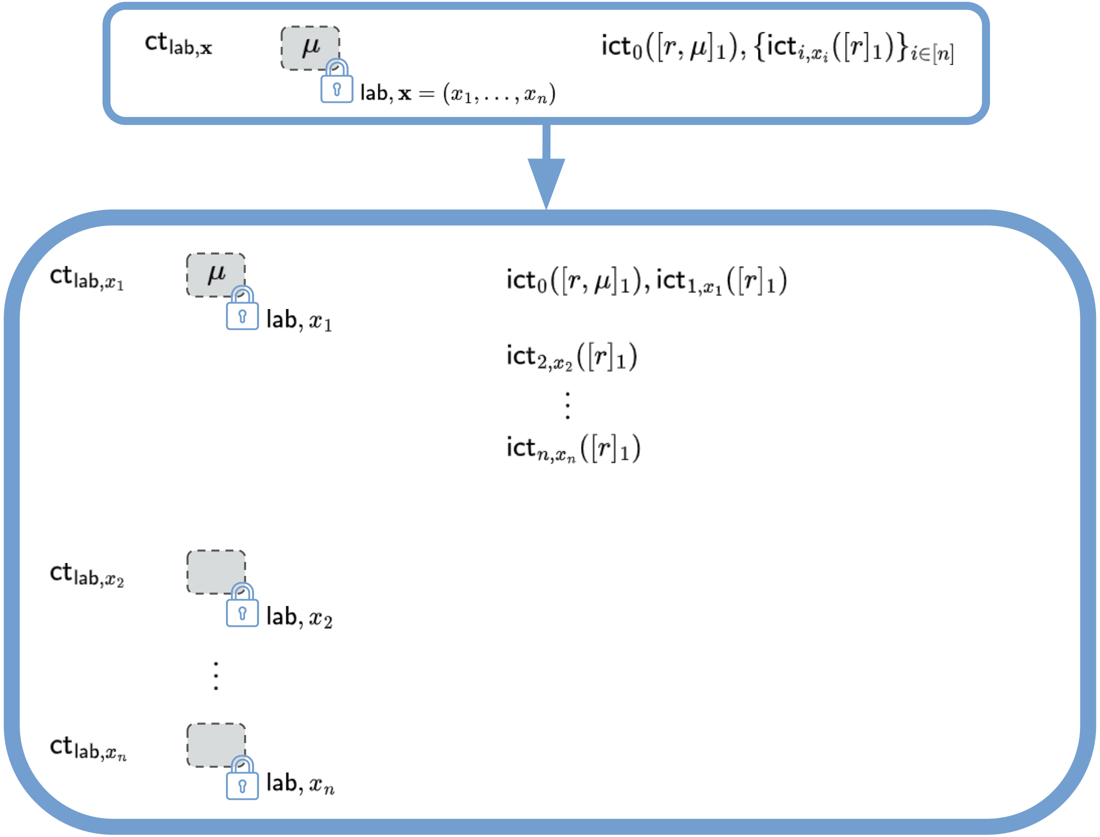
$\rightarrow [\mathbf{u}^\top \mathbf{v}]_t$

Linear Secret Sharing Scheme

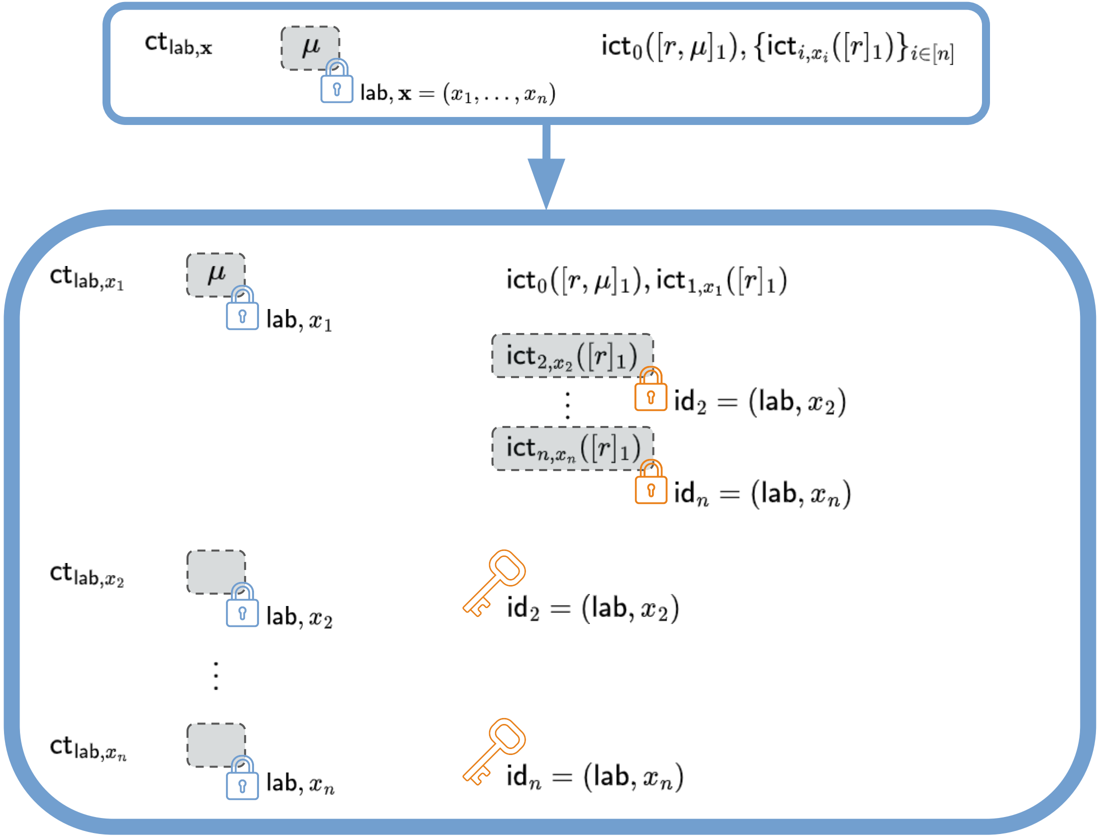
$\mathsf{Share}(s, f) \rightarrow (s_1^0, \ldots, s_n^0, s_1^1, \ldots, s_n^1)$

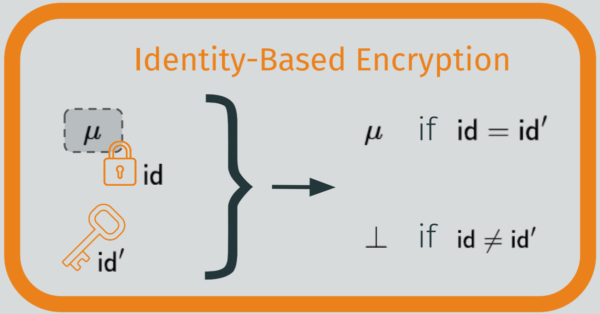
- if $f(x_1, \ldots, x_n) = 1$, then $\mathsf{FindCoeff}(x_1, \ldots, x_n, f) \rightarrow (\omega_1, \ldots, \omega_n)$, s.t. $\sum_{i \in [n]} \omega_i \cdot s_i^{x_i} = s$
- if $f(x_1, \ldots, x_n) = 0$, then $(s_1^{x_1}, \ldots, s_n^{x_n}) \approx \$$

Distributed Encryption

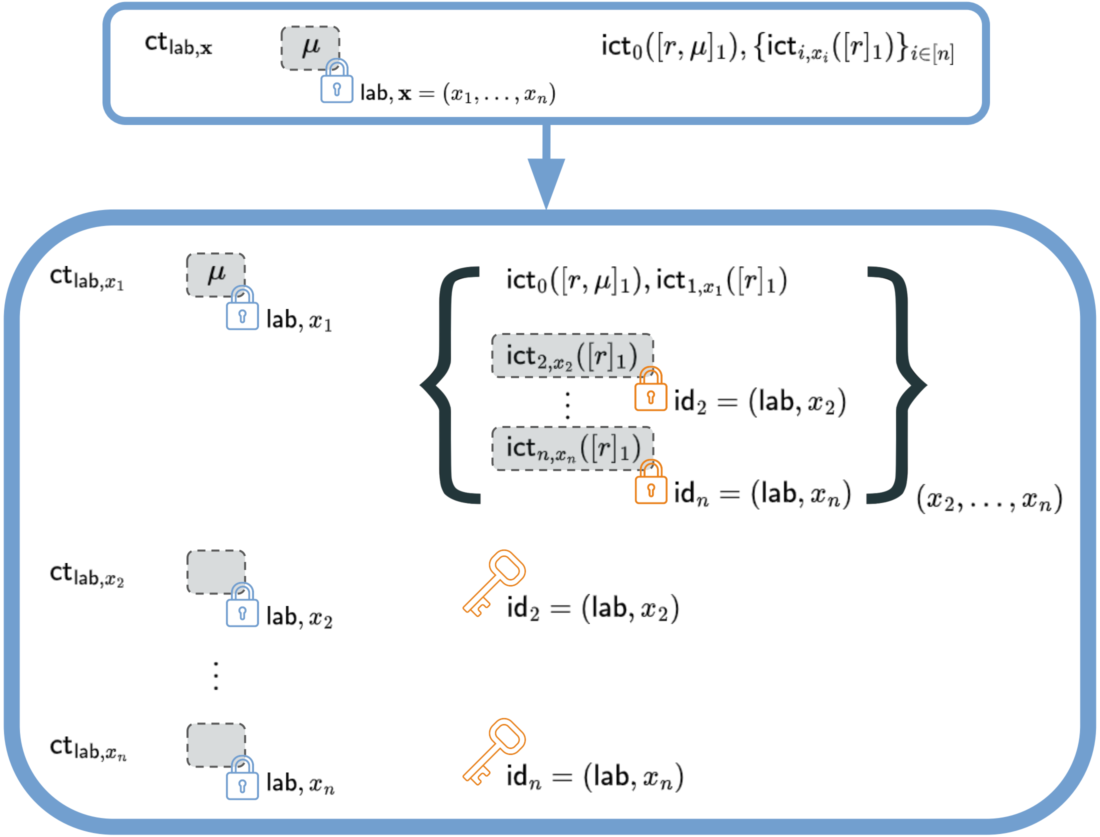


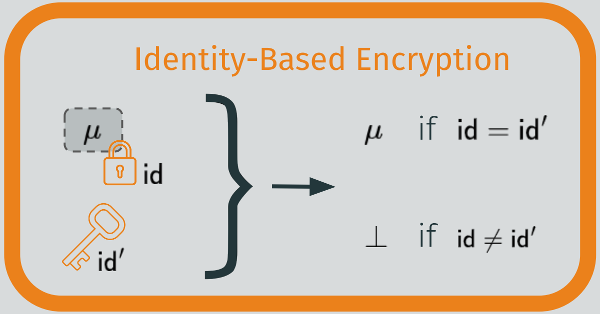
Distributed Encryption



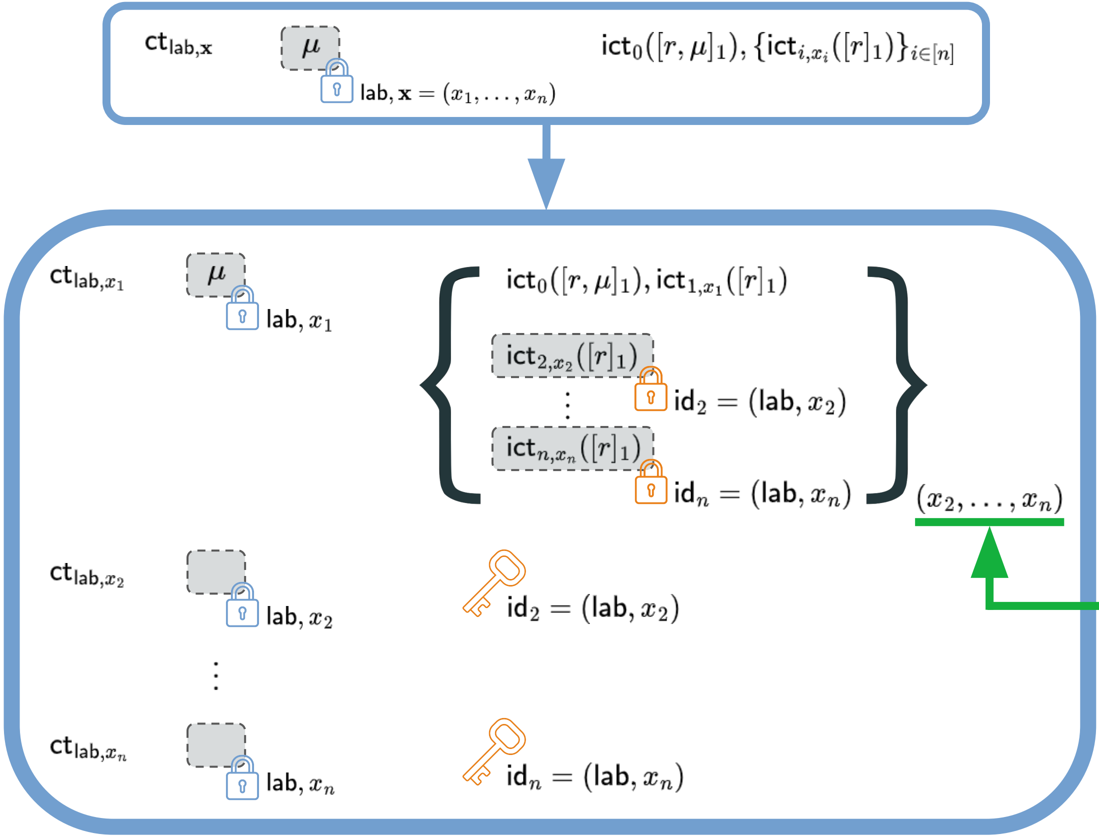


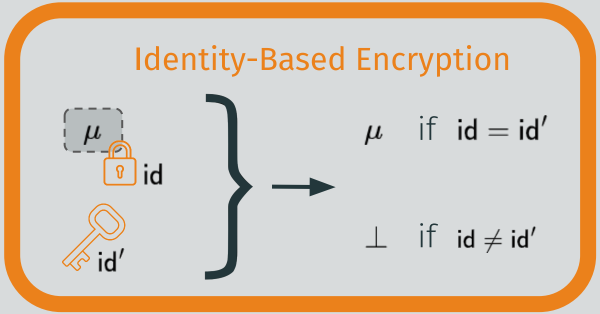
Distributed Encryption





Distributed Encryption

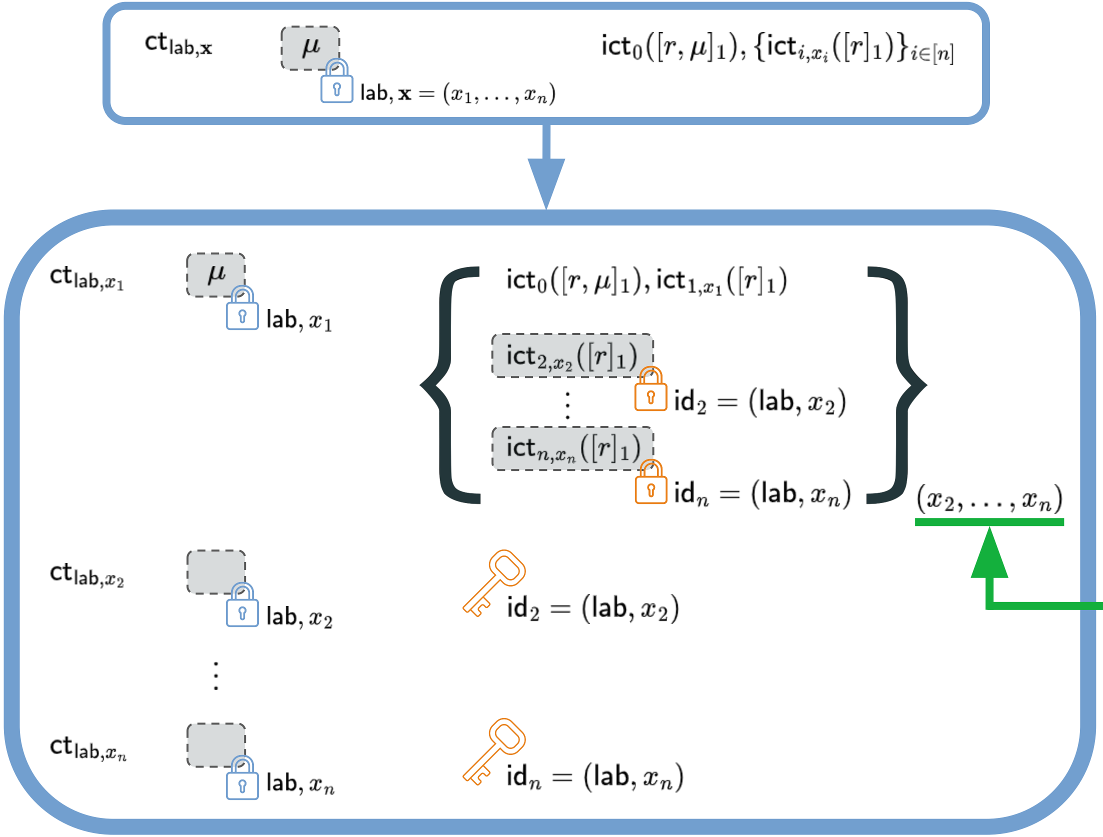


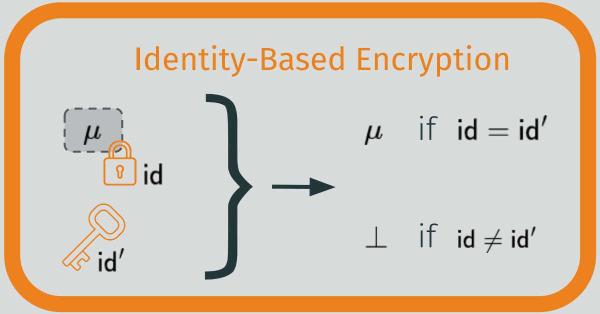


Which $(x_2, \ldots, x_n) \in \{0,1\}^{n-1}$ do we need?

- **all** ⇝ NC^1 policies for $O(\log \lambda)$ inputs

Distributed Encryption





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

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

Conclusion

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

Conclusion

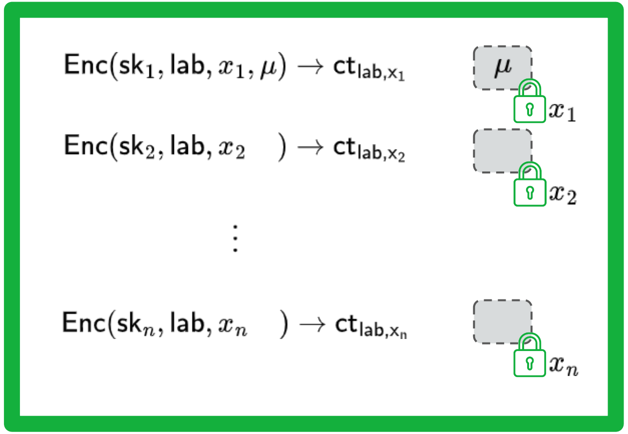
- definition of MC-ABE and MC-PE
- construction of MC-ABE for global policies from SXDH
- generic compiler for constant-arity MC-ABE $\Longrightarrow$ constant-arity MC-PE from LWE
- previous to this work, these results were unknown even for MI-ABE

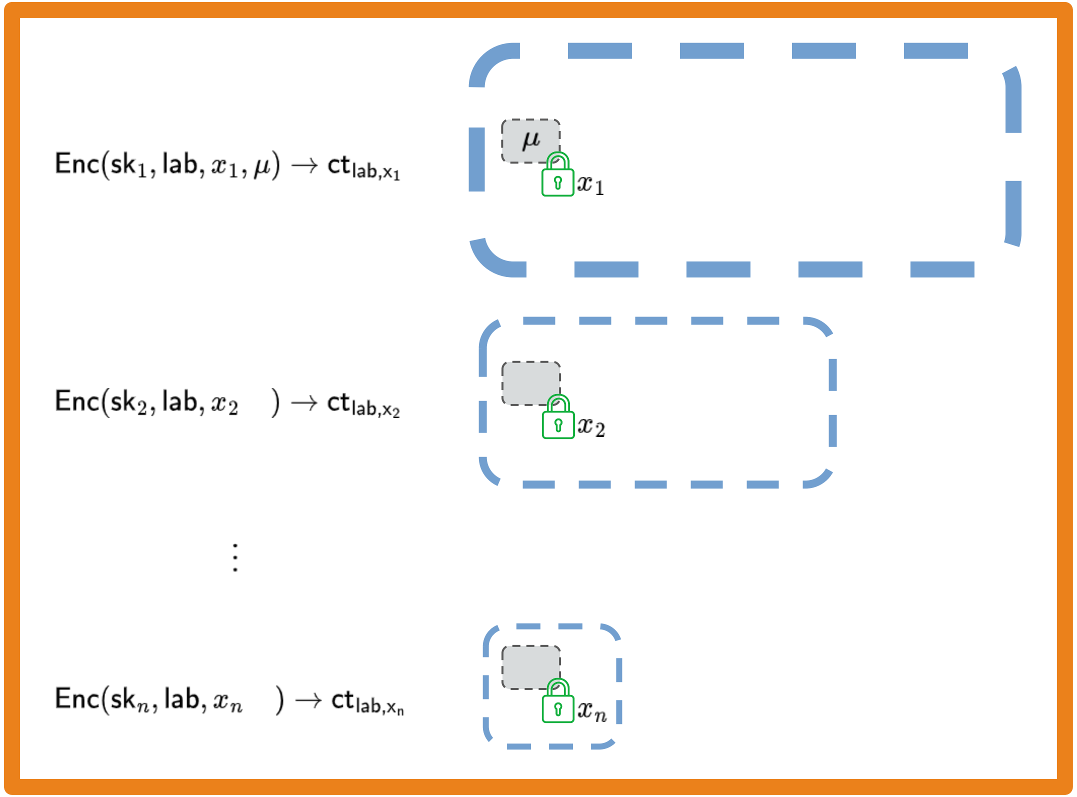
Thank you for your attention!

ia.cr/2024/1945

ADDITIONAL MATERIAL

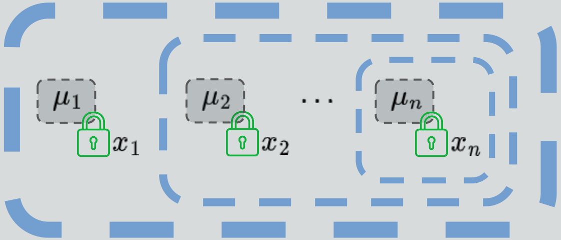
From MC-ABE to MC-PE using Lockable Obfuscation





From MC-ABE to MC-PE using Lockable Obfuscation

"Communication" between the obfuscated circuits?



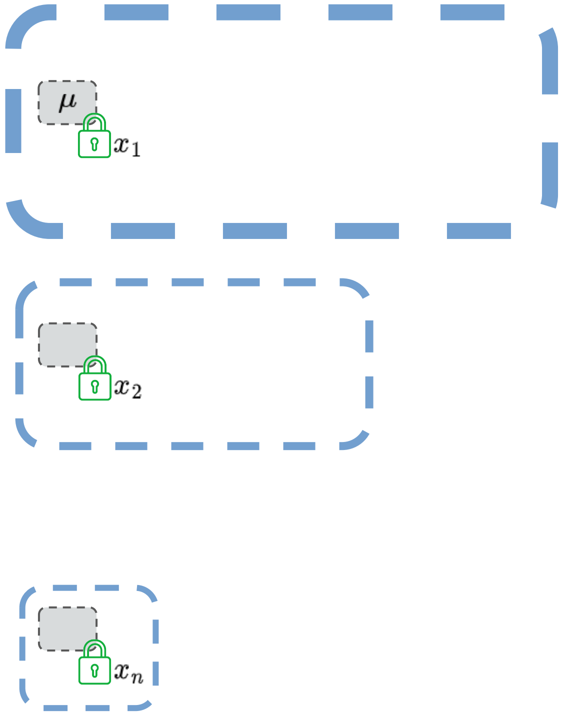
nested evaluation checks
global authorization

$\mathsf{Enc}(\mathsf{sk}_1, \mathsf{lab}, x_1, \mu) \to \mathsf{ct}_{\mathsf{lab},\mathsf{x}_1}$

$\mathsf{Enc}(\mathsf{sk}_2, \mathsf{lab}, x_2 \quad) \to \mathsf{ct}_{\mathsf{lab},\mathsf{x}_2}$

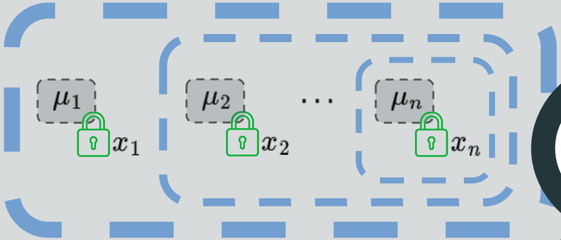
$\vdots$

$\mathsf{Enc}(\mathsf{sk}_n, \mathsf{lab}, x_n \quad) \to \mathsf{ct}_{\mathsf{lab},\mathsf{x}_n}$



From MC-ABE to MC-PE using Lockable Obfuscation

"Communication" between the obfuscated circuits?



nested evaluation checks **global** authorization