Multi-Client Attribute-Based and Predicate Encryption, Revisited

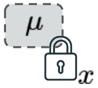
Robert Schädlich*

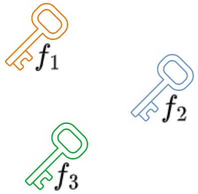
May 15, 2025

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

Attribute-Based Encryption (ABE) [SW05]

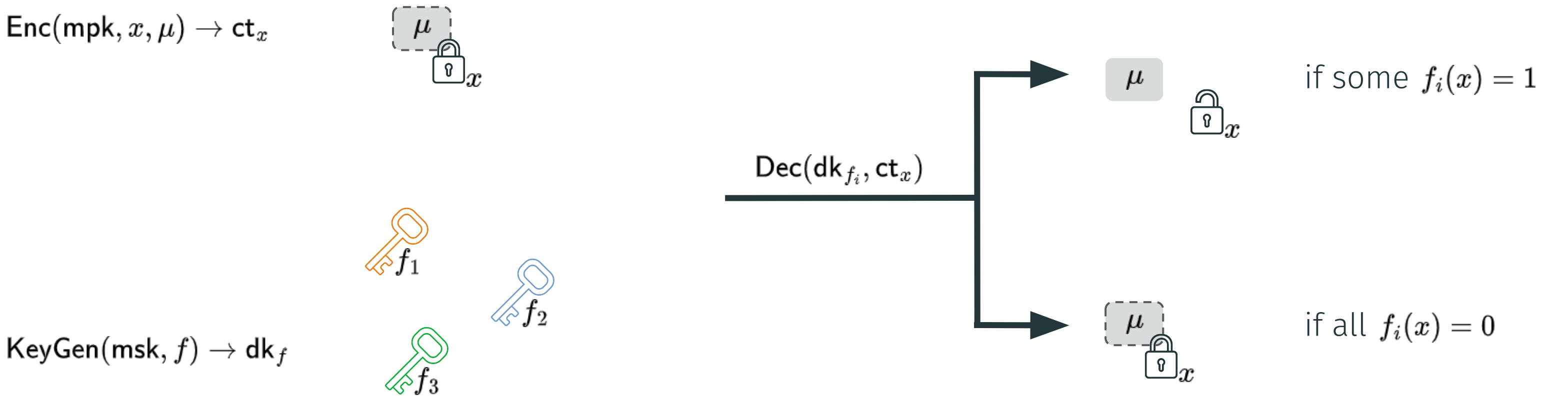
$\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x$





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

Attribute-Based Encryption (ABE) [SW05]



Attribute-Based Encryption (ABE) [SW05]

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

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

μ x

f_1 f_2 f_3

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

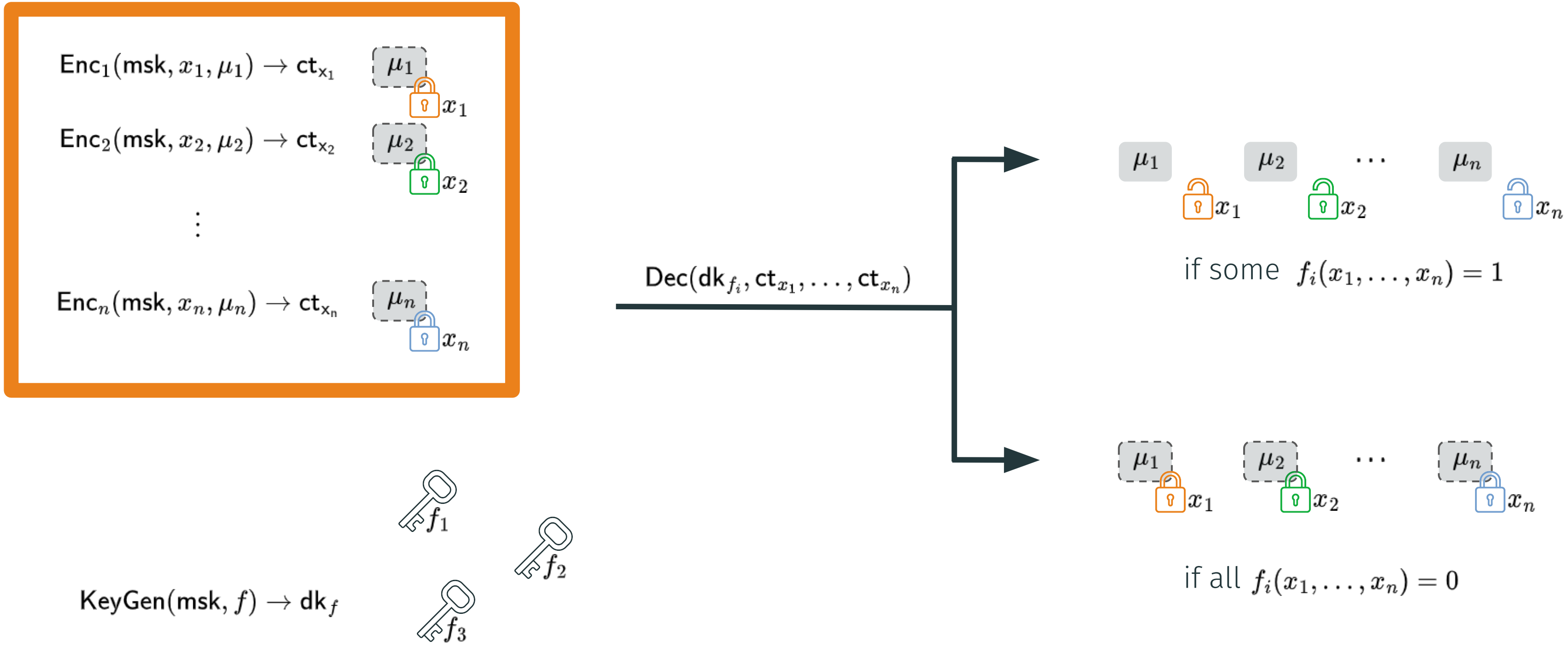
public input

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

μ x if some $f_i(x) = 1$

μ x 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

$\mathsf{Enc}(\mathsf{sk}_1, \mathsf{lab}, x_1, \mu_1) \to \mathsf{ct}_{\mathsf{lab},x_1}$ μ_1 x_1

$\mathsf{Enc}(\mathsf{sk}_2, \mathsf{lab}, x_2, \mu_2) \to \mathsf{ct}_{\mathsf{lab},x_2}$ μ_2 x_2

$\vdots$

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

$\mathsf{Dec}(\mathsf{dk}_{f_i}, \mathsf{ct}_{\mathsf{lab},x_1}, \ldots, \mathsf{ct}_{\mathsf{lab},x_n})$

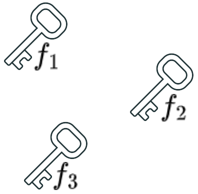
μ_1 x_1 μ_2 x_2 $\cdots$ μ_n x_n

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

μ_1 x_1 μ_2 x_2 $\cdots$ μ_n x_n

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

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



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

1st new feature:
separation & corruption of secret keys

$\mathsf{Enc}(\mathsf{sk}_1, \mathsf{lab}, x_1, \mu_1) \to \mathsf{ct}_{\mathsf{lab},x_1}$ μ_1 x_1

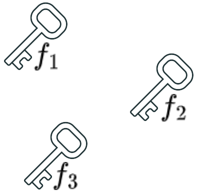
$\mathsf{Enc}(\mathsf{sk}_2, \mathsf{lab}, x_2, \mu_2) \to \mathsf{ct}_{\mathsf{lab},x_2}$ μ_2 x_2

$\vdots$

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

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

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



$\mathsf{Dec}(\mathsf{dk}_{f_i}, \mathsf{ct}_{\mathsf{lab},x_1}, \ldots, \mathsf{ct}_{\mathsf{lab},x_n})$

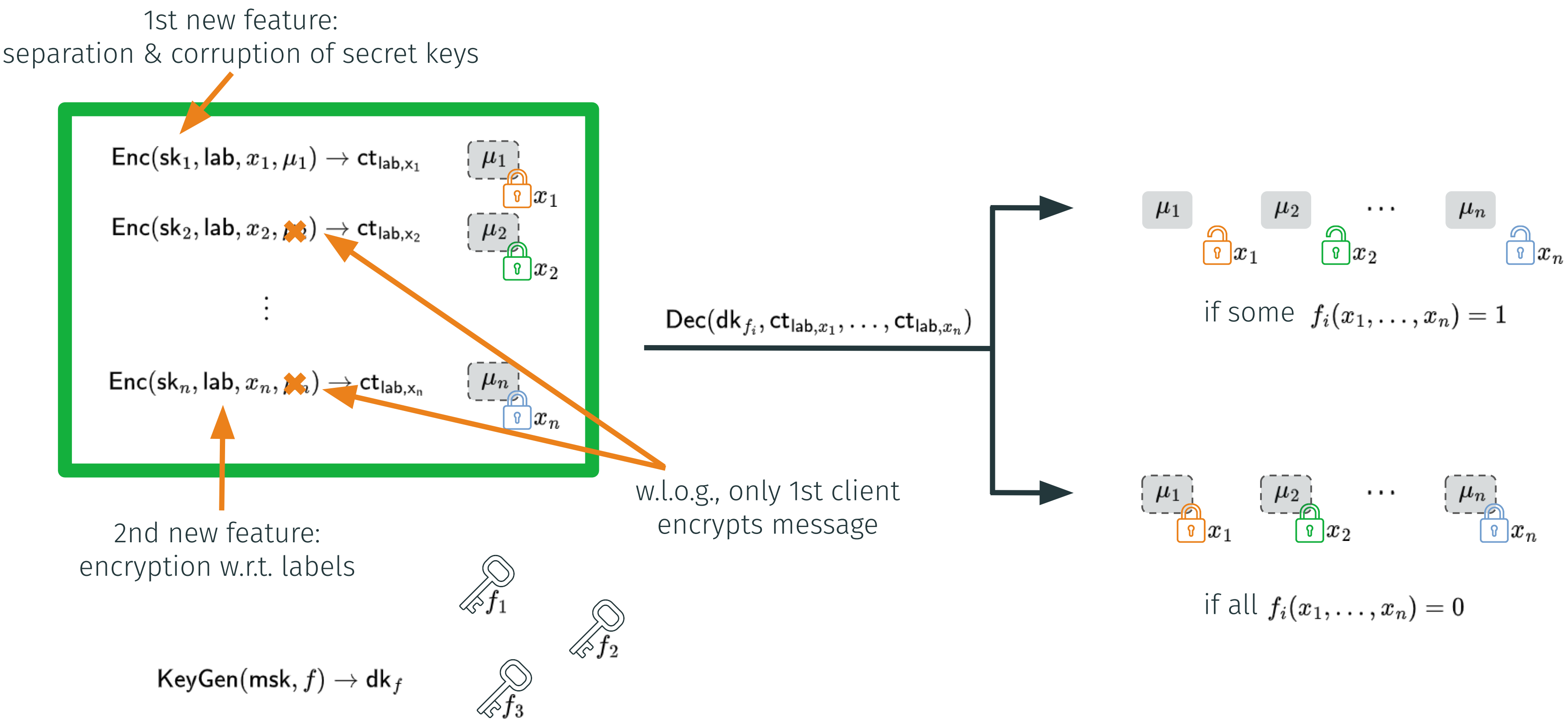
μ_1 x_1 μ_2 x_2 $\cdots$ μ_n x_n

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

μ_1 x_1 μ_2 x_2 $\cdots$ μ_n x_n

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

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



MI-ABE and MC-ABE for Conjunction Policies

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

Work	Policy Class	Assumption	Corruption	Labels	Collusions
[C:ATY23]	NC^1	MDDH	✔	✘	✔
[this work]	**NC^1**	**MDDH**	✔	✔	✔
[EC:FFMV23]	P	LWE	✔	✘	✘
[this work]	**P**	**LWE**	✔	✔	(✔)

MI-ABE and MC-ABE for Conjunct

$f(x_1, \ldots, x_n) = f_1(x_1)$

Generic Compiler of [TCC:PS24]

- MC-ABE -> MC-PE
- constant arity
- based on LWE

Work	Policy Class	Assumption	Corruption	Labels	Collusions	Attribute-Hiding
[C:ATY23]	NC^1	MDDH	✔	✘	✔	✔
[this work]	NC^1	**MDDH**	✔	✔	✔	✔
[EC:FFMV23]	P	LWE	✔	✘	✘	✔
[this work]	**P**	**LWE**	✔	✔	(✔)	✔

MI-ABE and MC-ABE for Global Policies

Work	Policy Class	Assumption	Corruption	Labels	Arity	Attribute-Hiding
[C:AYY22]	NC^1	KOALA, LWE	✘	✘	2	✔
[C:ARYY23]	P	private-coin evasive LWE, tensor LWE, LWE	✘	✘	poly	✘
[TCC:PS24]	NC^0 (and more)	SXDH	✔	✔	poly	✘
[this work]	**succinctly enumerable**	**MDDH**	✔	✔	**poly**	✘
[this work]	**succinctly enumerable**	**public-coin evasive LWE, LWE**	✔	✔	**poly**	✘

MI-ABE and MC-ABE for Global Policies

Work	Policy Class	Assumption	Corruption	Labels	Arity	Attribute-Hiding
[C:AYY22]	NC^1	KOALA, LWE	✘	✘	2	✔
[C:ARYY23]	P	private-coin evasive LWE, tensor LWE, LWE	✘	✘	const	✔
[TCC:PS24]	NC^0 (and more)	SXDH	✔	✔	const	✔
[this work]	**succinctly enumerable**	**MDDH**	✔	✔	**const**	✔
[this work]	**succinctly enumerable**	**public-coin evasive LWE, LWE**	✔	✔	**const**	✔

Framework for Single-Client ABE

(Pairing-Based) IPFE

(Exact) LSSS

$\Big\} \longrightarrow$ Single-Client ABE

Inner-Product Functional Encryption

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

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

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

Linear Secret Sharing Scheme

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

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

Framework for Single-Client ABE

(Pairing-Based) IPFE

(Exact) LSSS

→ Single-Client ABE ←

Evasive IPFE [HLL24]

Noisy Linear Garbling

Inner-Product Functional Encryption

$\mathbf{u}$ — ict$([\mathbf{u}]_1)$

$\mathbf{v}$ — 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 $(s_1^{x_1}, \ldots, s_n^{x_n}) \approx \$$

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

$$\left.\begin{array}{l} \mathsf{ict}_0([r, \mu]_1), \{\mathsf{ict}_{i,x_i}([r]_1)\}_{i \in [n]} \\ \mathsf{idk}_0([s, 1]_2), \{\mathsf{idk}_{i,b}([s_i^b]_2)\}_{i \in [n]}^{b \in \{0,1\}} \end{array}\right\} \longrightarrow [rs + \mu]_{\mathrm{t}}, \{[r s_i^{x_i}]_{\mathrm{t}}\}_{i \in [n]}$$

Inner-Product Functional Encryption

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

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

$$\left.\begin{array}{l} \mathsf{ict}([\mathbf{u}]_1) \\ \mathsf{idk}([\mathbf{v}]_2) \end{array}\right\} \longrightarrow [\mathbf{u}^\top \mathbf{v}]_{\mathrm{t}}$$

Linear Secret Sharing Scheme

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

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

Framework for Si

How to distribute this?

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

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

$$\longrightarrow [rs + \mu]_{\mathrm{t}}, \{[r s_i^{x_i}]_{\mathrm{t}}\}_{i \in [n]}$$

Inner-Product Functional Encryption

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

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

$$\longrightarrow [\mathbf{u}^\top \mathbf{v}]_{\mathrm{t}}$$

Linear Secret Sharing Scheme

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

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

Distributed Encryption

$\mathsf{ct}_{\mathsf{lab},\mathbf{x}}$ $\boxed{\mu}$ $\mathsf{lab}, \mathbf{x} = (x_1, \ldots, x_n)$

$\mathsf{ict}_0([r, \mu]_1), \{\mathsf{ict}_{i,x_i}([r]_1)\}_{i \in [n]}$

$\mathsf{ct}_{\mathsf{lab},x_1}$ $\boxed{\mu}$ lab, x_1

$\mathsf{ict}_0([r, \mu]_1), \mathsf{ict}_{1,x_1}([r]_1)$

$\mathsf{ict}_{2,x_2}([r]_1)$

$\vdots$

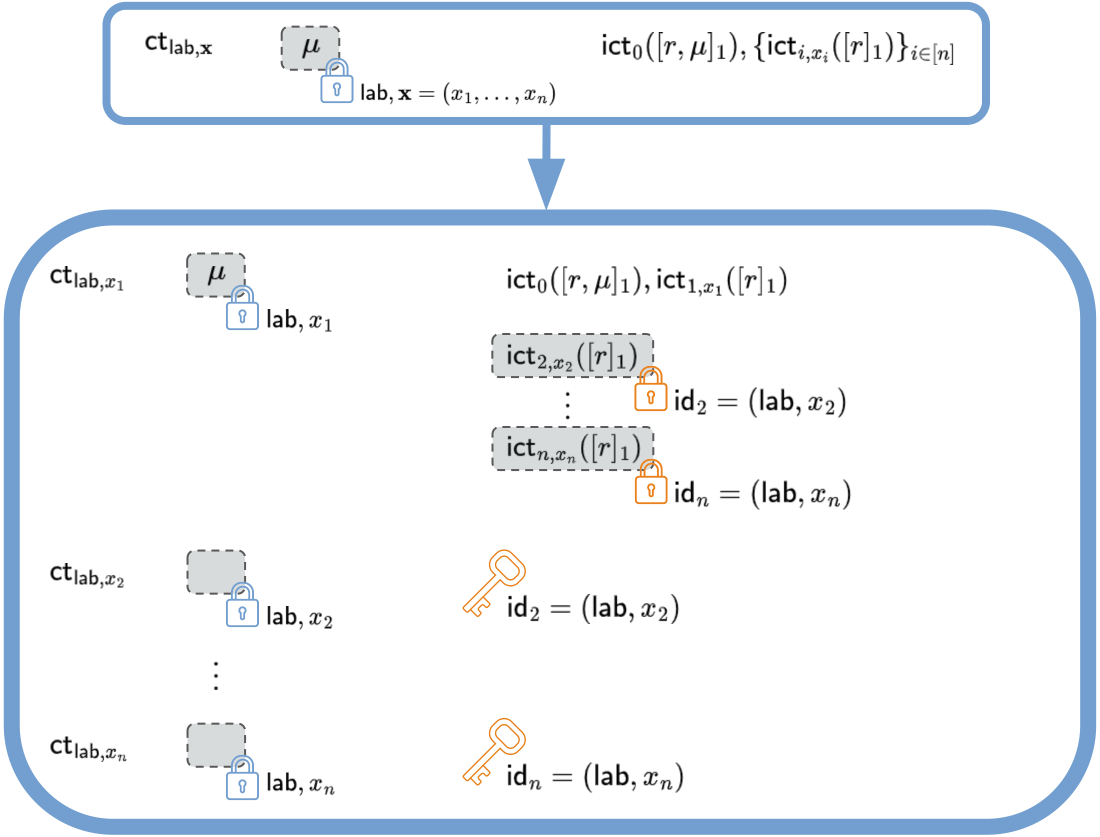
$\mathsf{ict}_{n,x_n}([r]_1)$

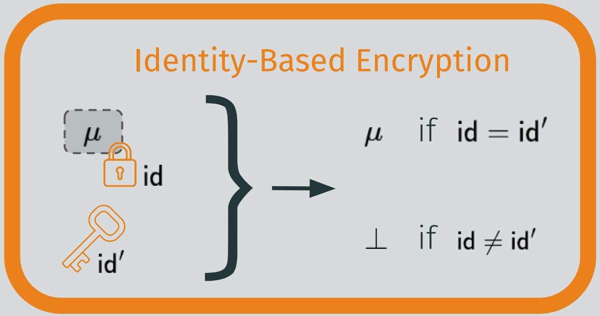
$\mathsf{ct}_{\mathsf{lab},x_2}$ lab, x_2

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ lab, x_n

Distributed Encryption





Distributed Encryption

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

$\mathsf{ct}_{\mathsf{lab},x_1}$ μ lab, x_1

$$\left\{ \begin{array}{l} \mathsf{ict}_0([r,\mu]_1), \mathsf{ict}_{1,x_1}([r]_1) \\ \mathsf{ict}_{2,x_2}([r]_1) \quad \mathsf{id}_2 = (\mathsf{lab}, x_2) \\ \vdots \\ \mathsf{ict}_{n,x_n}([r]_1) \quad \mathsf{id}_n = (\mathsf{lab}, x_n) \end{array} \right\}_{(x_2,\ldots,x_n)}$$

$\mathsf{ct}_{\mathsf{lab},x_2}$ lab, x_2 $\mathsf{id}_2 = (\mathsf{lab}, x_2)$

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ lab, x_n $\mathsf{id}_n = (\mathsf{lab}, x_n)$

Identity-Based Encryption

$$\left.\begin{array}{l} \mu \ \ \mathsf{id} \\ \mathsf{id}' \end{array}\right\} \longrightarrow \begin{cases} \mu & \text{if } \mathsf{id} = \mathsf{id}' \\ \perp & \text{if } \mathsf{id} \neq \mathsf{id}' \end{cases}$$

Distributed Encryption

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

$\mathsf{ct}_{\mathsf{lab},x_1}$ μ lab, x_1

$$\left\{ \begin{array}{l} \mathsf{ict}_0([r,\mu]_1), \mathsf{ict}_{1,x_1}([r]_1) \\ \mathsf{ict}_{2,x_2}([r]_1) \quad \mathsf{id}_2 = (\mathsf{lab}, x_2) \\ \vdots \\ \mathsf{ict}_{n,x_n}([r]_1) \quad \mathsf{id}_n = (\mathsf{lab}, x_n) \end{array} \right\}$$

$(x_2, \ldots, x_n)$

$\mathsf{ct}_{\mathsf{lab},x_2}$ lab, x_2 $\mathsf{id}_2 = (\mathsf{lab}, x_2)$

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ lab, x_n $\mathsf{id}_n = (\mathsf{lab}, x_n)$

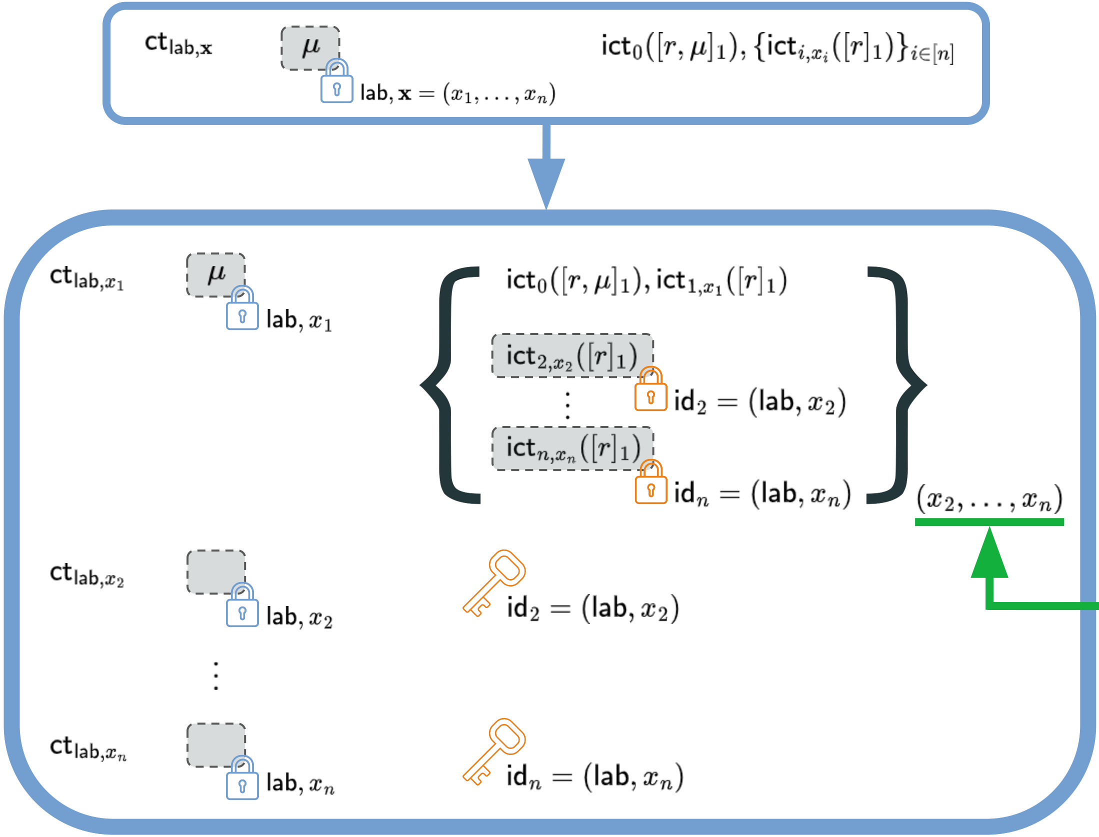
Identity-Based Encryption

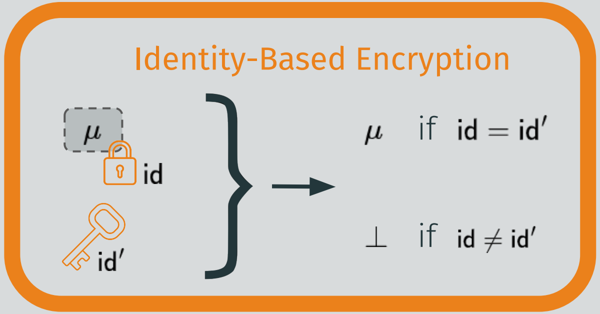
μ id, id' $\rightarrow$ μ if $\mathsf{id} = \mathsf{id}'$; $\perp$ if $\mathsf{id} \neq \mathsf{id}'$

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

- **O(1)-size subsets of [*n*]:**
  - ⇝ NC^0 policies [TCC:PS24]
- **O(1)-size subsets of [2;*n*]:**
  - ⇝ policies with constant bit dependency on slots 2, ..., *n*
  - ⇝ policies with poly-size accepting sets on slots 2, ..., *n*

Distributed Encryption

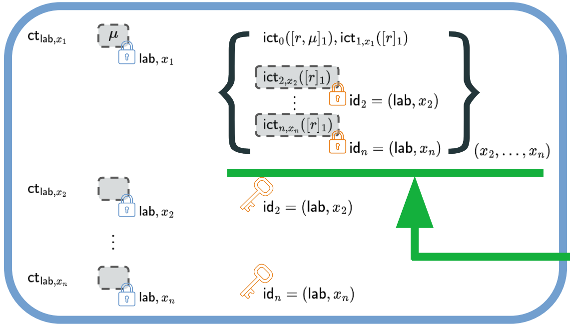




Examples of Succinctly Enumerable Policy Classes

- O(1)-size subsets of [*n*]:
  - ⇝ NC^0 policies [TCC:PS24]
- O(1)-size subsets of [2;*n*]:
  - ⇝ policies with constant bit dependency on slots 2, ..., *n*
  - ⇝ policies with poly-size accepting sets on slots 2, ..., *n*

Succinct Enumerability

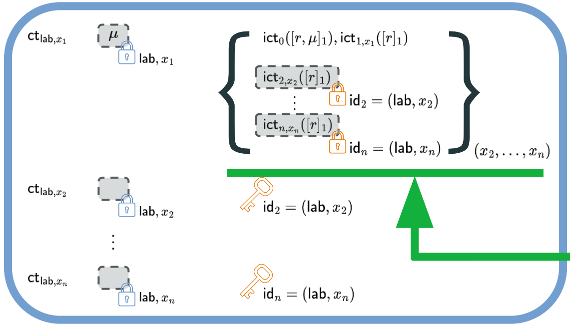


Succinct Enumerability

there exists $V \subseteq \{0, 1, \star\}^{[2;n]}$ such that

- succinctness: $|V| = \mathsf{poly}(\lambda)$

Succinct Enumerability



Succinct Enumerability

there exists $V \subseteq \{0,1,\star\}^{[2;n]}$ such that

- **succinctness:** $|V| = \mathsf{poly}(\lambda)$
- **correctness:** for all $\mathbf{x}$ such that $f(\mathbf{x}) = 1$, there exists $\mathbf{v} \in V$ such that $\mathbf{x} \in X_{\mathbf{v}}$
- **security:** f is constant on $X_{\mathbf{v}}$ for each $\mathbf{v} \in V$

Notation

$X_{\mathbf{v}} = \{\mathbf{x} \in \{0,1\}^n \mid \forall i \in [2;n] : v_i \neq \star \implies v_i = x_i\}$, e.g., $X_{(1,\star,1,0,\star)} = \{(1,0,1,0,0),(1,0,1,0,1),(1,1,1,0,0),(1,1,1,0,1)\}$

Construction for Conjunction Policies

$\mathsf{ct}_{\mathsf{lab},x_1}$ $\boxed{\mu}$ lab, x_1

$\mathsf{ct}_{\mathsf{lab},x_2}$ lab, x_2

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ lab, x_n

dk_f $f = (f_1, \ldots, f_n)$

Attribute-Based Inner-Product Functional Encryption

$$\left.\begin{array}{l} \boxed{\mathbf{u}} \quad \mathsf{ict}(x, [\mathbf{u}]_1) \\ \mathbf{v} \quad \mathsf{idk}(f, [\mathbf{v}]_2) \end{array}\right\} \longrightarrow \begin{array}{ll} [\mathbf{u}^\top \mathbf{v}]_t & \text{if } f(x) = 1 \\ \perp & \text{if } f(x) = 0 \end{array}$$

Construction for Conjunction Policies

$\mathsf{ct}_{\mathsf{lab},x_1}$ $\quad \mu \quad$ lab, x_1 $\quad \mathsf{ict}_1(x_1, [t_{\mathsf{lab},1}, r]_1),\ c = [\mu]_{\mathrm{t}} + H([r]_{\mathrm{t}})$

$\mathsf{ct}_{\mathsf{lab},x_2}$ $\quad$ lab, x_2 $\quad \mathsf{ict}_2(x_2, [t_{\mathsf{lab},2}]_1)$

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ $\quad$ lab, x_n $\quad \mathsf{ict}_n(x_n, [t_{\mathsf{lab},n}]_1)$

dk_f $\quad f = (f_1, \ldots, f_n)$ $\quad \mathsf{idk}_1(f_1, [s, 1]_2),\ \{\mathsf{idk}_i(f_i, [s]_2)\}_{i \in [2;n]}$

Attribute-Based Inner-Product Functional Encryption

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

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

$$\left.\begin{array}{l} \mathsf{ict}(x, [\mathbf{u}]_1) \\ \mathsf{idk}(f, [\mathbf{v}]_2) \end{array}\right\} \longrightarrow \begin{cases} [\mathbf{u}^\top \mathbf{v}]_{\mathrm{t}} & \text{if } f(x) = 1 \\ \perp & \text{if } f(x) = 0 \end{cases}$$

$$t_{\mathsf{lab},1} = -\textstyle\sum_{i=2}^{n} \mathsf{PRF}_{K_i}(\mathsf{lab})$$
$$t_{\mathsf{lab},2} = \mathsf{PRF}_{K_2}(\mathsf{lab})$$
$$\vdots$$
$$t_{\mathsf{lab},n} = \mathsf{PRF}_{K_n}(\mathsf{lab})$$

Construction for Conjunction Policies

$\mathsf{ct}_{\mathsf{lab},x_1}$	μ lab, x_1	$\mathsf{ict}_1(x_1, [t_{\mathsf{lab},1}, r]_1),\ c = [\mu]_t + H([r]_t)$	
$\mathsf{ct}_{\mathsf{lab},x_2}$	lab, x_2	$\mathsf{ict}_2(x_2, [t_{\mathsf{lab},2}]_1)$	$c = [\mu]_t + H([r]_t),\ [st_{\mathsf{lab},1} + r]_t,\ \{[st_{\mathsf{lab},i}\}_{i\in[2;n]}$
	$\vdots$		
$\mathsf{ct}_{\mathsf{lab},x_n}$	lab, x_n	$\mathsf{ict}_n(x_n, [t_{\mathsf{lab},n}]_1)$	
dk_f	$f = (f_1, \ldots, f_n)$	$\mathsf{idk}_1(f_1, [s, 1]_2),\ \{\mathsf{idk}_i(f_i, [s]_2)\}_{i\in[2;n]}$	

Attribute-Based Inner-Product Functional Encryption

$$\left.\begin{array}{ll} \mathbf{u} & \mathsf{ict}(x, [\mathbf{u}]_1) \\ \mathbf{v} & \mathsf{idk}(f, [\mathbf{v}]_2) \end{array}\right\} \longrightarrow \begin{array}{ll} [\mathbf{u}^\top \mathbf{v}]_t & \text{if } f(x) = 1 \\ \perp & \text{if } f(x) = 0 \end{array}$$

$$t_{\mathsf{lab},1} = -\sum_{i=2}^{n} \mathsf{PRF}_{K_i}(\mathsf{lab})$$

$$t_{\mathsf{lab},2} = \mathsf{PRF}_{K_2}(\mathsf{lab})$$

$$\vdots$$

$$t_{\mathsf{lab},n} = \mathsf{PRF}_{K_n}(\mathsf{lab})$$

Construction for Conjunction Policies

$\mathsf{ct}_{\mathsf{lab},x_1}$ μ lab, x_1 $\mathsf{ict}_1(x_1, [t_{\mathsf{lab},1}, r]_1),\ c = [\mu]_{\mathsf{t}} + H([r]_{\mathsf{t}})$

$\mathsf{ct}_{\mathsf{lab},x_2}$ lab, x_2 $\mathsf{ict}_2(x_2, [t_{\mathsf{lab},2}]_1)$

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ lab, x_n $\mathsf{ict}_n(x_n, [t_{\mathsf{lab},n}]_1)$

dk_f $f = (f_1, \ldots, f_n)$ $\mathsf{idk}_1(f_1, [s, 1]_2),\ \{\mathsf{idk}_i(f_i, [s]_2)\}_{i\in[2;n]}$

$\Bigg\}$ $c = [\mu]_{\mathsf{t}} + H([r]_{\mathsf{t}}),\ [st_{\mathsf{lab},1} + r]_{\mathsf{t}},\ \{[st_{\mathsf{lab},i}\}_{i\in[2;n]}$

Security

$f_1(x_1) = 0$: ✔

$f_i(x_i) = 0$ for $i \in [2;n]$:

Construction for Conjunction Policies

$\mathsf{ct}_{\mathsf{lab},x_1}$ — μ ; lab, x_1 — $\mathsf{ict}_1(x_1, [t_{\mathsf{lab},1}, r]_1),\ c = [\mu]_{\mathsf{t}} + H([r]_{\mathsf{t}})$

$\mathsf{ct}_{\mathsf{lab},x_2}$ — lab, x_2 — $\mathsf{ict}_2(x_2, [t_{\mathsf{lab},2}]_1)$

$\vdots$

$\mathsf{ct}_{\mathsf{lab},x_n}$ — lab, x_n — $\mathsf{ict}_n(x_n, [t_{\mathsf{lab},n}]_1)$

dk_f — $f = (f_1, \ldots, f_n)$ — $\mathsf{idk}_1(f_1, [s, 1]_2),\ \{\mathsf{idk}_i(f_i, [s]_2)\}_{i\in[2;n]}$

$$\left.\right\}\ c = [\mu]_{\mathsf{t}} + H([r]_{\mathsf{t}}),\ [st_{\mathsf{lab},1} + r]_{\mathsf{t}},\ \{[st_{\mathsf{lab},i}\}_{i\in[2;n]}$$

Security

$f_1(x_1) = 0$: ✔

$f_i(x_i) = 0$ for $i \in [2;n]$: apply DDH and PRF security, then argue $\{[s'_{\mathsf{lab}} + r_j]_{\mathsf{t}}, H([r_j]_{\mathsf{t}})\}_j \approx_c \{[s'_{\mathsf{lab}} + r_j]_{\mathsf{t}}, [\delta_j]_{\mathsf{t}}\}_j$ ✔

Conclusion

Construction of MC-ABE for Conjunction Policies

- conjunctions of NC^1 from MDDH on pairings
- conjunctions of P from LWE with bounded collusions

Construction of MC-ABE for Global Policies

- succinctly enumerable policy classes
- instantiation from MDDH on pairings or public-coin evasive LWE

Conclusion

Construction of MC-ABE for Conjunction Policies

- conjunctions of NC^1 from MDDH on pairings
- conjunctions of P from LWE with bounded collusions

Construction of MC-ABE for Global Policies

- succinctly enumerable policy classes
- instantiation from MDDH on pairings or public-coin evasive LWE

Thank you for your attention!

ia.cr/2025/821