Compact Adaptively Secure ABE from k-Lin: Beyond NC^1 and Towards NL

Huijia (Rachel) Lin and Ji Luo

UNIVERSITY *of* WASHINGTON

Attribute-Based Encryption [SW05]

$\mathsf{Setup} \to \mathsf{mpk}, \mathsf{msk}$

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

policy

Compact: $|\mathsf{ct}| = O(|x|)$

Expressive:

$f \in$ powerful class of functions

sk

x, ct

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

attribute message

$\mathsf{Dec}(\mathsf{sk}, f, \mathsf{ct}, x) \to \mu f(x)$

Correctness. Learn μ if $f(x) \neq 0$

(sk is authorized)

Attribute-Based Encryption [SW05]

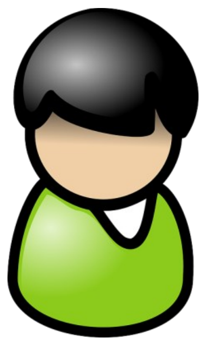
$\mathsf{Setup} \to \mathsf{mpk}, \mathsf{msk}$

$\mathsf{KeyGen}(\mathsf{msk}, f_i) \to \mathsf{sk}_i$

Collusion Resistance

Message is hidden given arbitrary number of unauthorized keys.

sk_i's



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

x, ct

Security. Hide μ if $f_i(x) = 0$ for all i

(sk_i's are unauthorized)

Adaptive IND-CPA Security

Exp_b

$\xrightarrow{\text{mpk}}$

$\xleftarrow{f_q}$

$\xrightarrow{\mathrm{sk}_{f_q}}$

$\xleftarrow{x,\ \mu_0,\ \mu_1}$

$\xrightarrow{\mathrm{ct} \leftarrow \mathrm{Enc}(x,\ \mu_b)}$

$\xleftarrow{f_q}$

$\xrightarrow{\mathrm{sk}_{f_q}}$

if for all queried keys $f_q(x) = 0$, then $\mathrm{Exp}_0 \approx \mathrm{Exp}_1$

~~(Weaker) Selective~~ IND-CPA Security

Adaptive Security

~~x~~

mpk

f_q

sk_{f_q}

Exp$_b$

μ_0, μ_1

$\mathrm{ct} \leftarrow \mathrm{Enc}(x, \mu_b)$

f_q

sk_{f_q}

if for all queried keys $f_q(x) = 0$, then $\mathrm{Exp}_0 \approx \mathrm{Exp}_1$

Challenging to have it all

- ★ Compactness: $|\mathsf{ct}| = O(|x|)$
- ★ Adaptive Security
- ★ Standard Assumptions

not flexible

NC^1 and ABP
are **non-uniform:**

Each sk works with
attribute of **fixed** length.

Goal. Have it ALL for expressive classes of policies.

Previously, the largest class was $\mathbf{NC^1}$ [KW19].

Contribution 1. Extend to **ABP**.

Arithmetic **B**ranching **P**rograms $\supseteq \mathrm{NC}^1$, **arithmetic** computation over $\mathbb{Z}_p$.

Challenging to have it all

- ★ Compactness: $|\mathrm{ct}| = O(|x|)$
- ★ Adaptive Security
- ★ Standard Assumptions

flexible

ABE for **uniform** computation:

Each sk works with attribute of **any** length.

Contribution 2. **DFA, NFA** (regular languages)

the **first** ABE for uniform computation with all above

L, NL * (log-space Turing machines)

* relaxed compactness

Related Works: Non-Uniform Model

NOT compact

[LOSTW10] for MSP

NOT adaptive

[GPSW06] for MSP
[GVW13, BGGHNSVV14] for P/poly

NON-standard assumptions

[LW12] for MSP
q-type assumption

---

all-in-one: compact, adaptive, standard assumptions

[KW19] for NC^1

this work for ABP $\Longleftarrow$ k-Lin in pairing groups

concurrent [GW20] for BP

Related Works: Uniform Model

NOT compact **or** **NOT adaptive** **or** **NON-standard assumptions**

[Wat12, Att14, AMY19, GWW19] for DFA

concurrent [GW20] for NFA

all-in-one: compact, adaptive, standard assumptions

this work for DFA, NFA

concurrent [GW20] for DFA

k-Lin

beyond finite automata

[AS16] for P (FE, based on iO)

this work for L, NL $|\mathrm{ct}| = O\big(|x|TS2^S\big)$ $|\mathrm{sk}| = O(|\mathrm{TM}|)$ (relaxed compactness)

New General Framework

computational tool

Inner-**P**roduct
Functional **E**ncryption

information-theoretic tool

Arithmetic **K**ey
Garbling **S**cheme

special randomized encoding

1-ABE = 1-key
1-ciphertext
secret-key

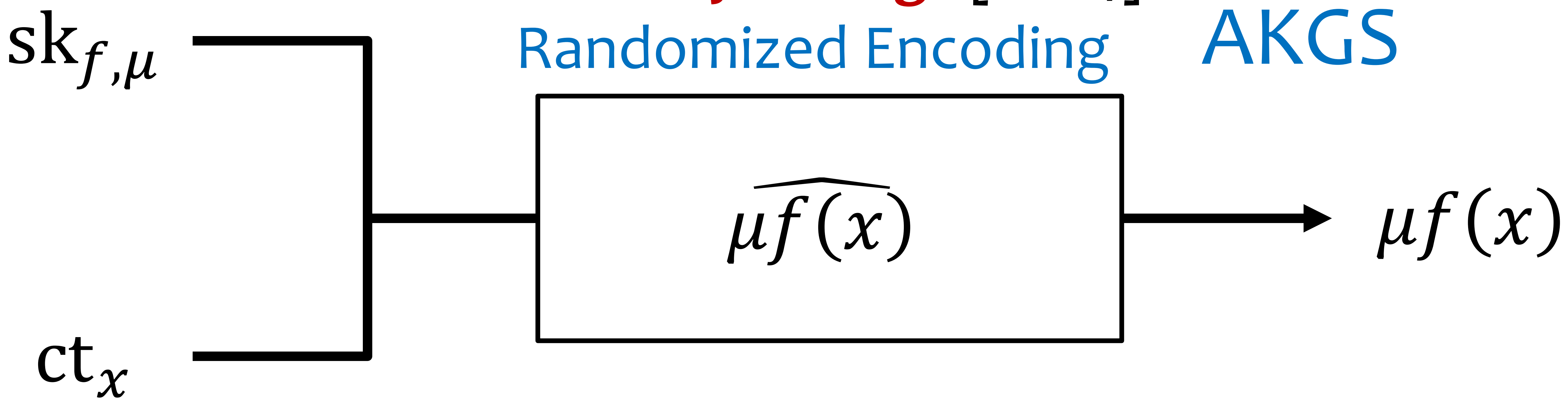
ABE

1-ABE via AKGS and IPFE

convenience – μ in secret key

Partially Hiding [IW14]
Randomized Encoding

AKGS



use μ as one-time pad

Secure: $\widehat{\mu f(x)}$ hides μ beyond $\mu f(x)$.
It does **not** hide f, x.

compute using IPFE $\Longrightarrow$ Simple: RE is **linear** in x.

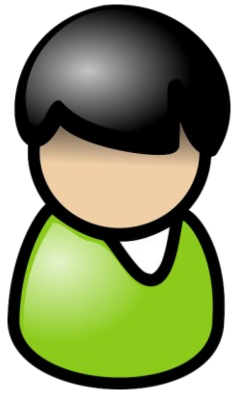
Arithmetic Key Garbling Scheme

1. Label functions: $L_1, \ldots, L_m \leftarrow \mathrm{Garble}(f, \mu; r)$
2. Garblings: $\ell_1, \ldots, \ell_m = L_1(x), \ldots, L_m(x)$

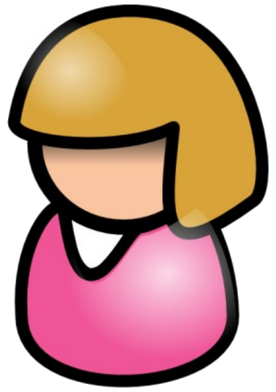
a.k.a. “labels”

$f: \mathbb{Z}_p^n \to \mathbb{Z}_p$

$x \in \mathbb{Z}_p^n$



$f, x, \ell_1, \ldots, \ell_m$



$\mathrm{Eval}(f, x, \ell_1, \ldots, \ell_m) = \mu f(x)$

Security (partial hiding).

$$\mathrm{Sim}\big(\underline{f, x}, \mu f(x)\big) \to \ell_1, \ldots, \ell_m$$

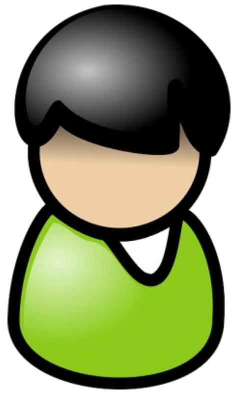
not hidden

Arithmetic Key Garbling Scheme

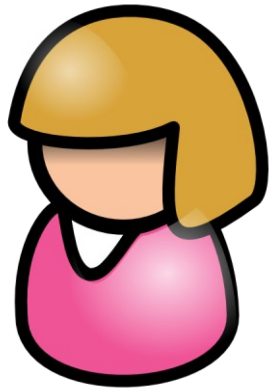
1. Label functions: $L_1, \dots, L_m \leftarrow \mathsf{Garble}(f, \mu; r)$
2. Garblings: $\ell_1, \dots, \ell_m = L_1(x), \dots, L_m(x)$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$

$x \in \mathbb{Z}_p^n$



$f, x, \ell_1, \dots, \ell_m$



$\mathsf{Eval}(f, x, \ell_1, \dots, \ell_m) = \mu f(x)$

Linearity.

1. $L_1, \dots, L_m$ are linear in x: $L_j(x) = \langle L_j, x \rangle$
2. coefficients of $L_1, \dots, L_m$ are linear in μ, r
3. Eval is linear in $\ell_1, \dots, \ell_m$

thanks to partial hiding

Inner-Product Functional Encryption

$$\left.\begin{aligned} \mathrm{isk} &\leftarrow \mathrm{KeyGen}(\mathrm{msk}, \boldsymbol{v}) \\ \mathrm{ict} &\leftarrow \mathrm{Enc}(\mathrm{msk}, \boldsymbol{u}) \end{aligned}\right\} \xrightarrow{\mathrm{Dec}} \langle \boldsymbol{u}, \boldsymbol{v} \rangle$$

Function-Hiding Property

$$\begin{Bmatrix} \mathrm{isk}(\boldsymbol{v}_1) & \mathrm{isk}(\boldsymbol{v}_2) & \cdots & \mathrm{isk}(\boldsymbol{v}_I) \\ \mathrm{isk}(\boldsymbol{u}_1) & \mathrm{ict}(\boldsymbol{u}_2) & \cdots & \mathrm{ict}(\boldsymbol{u}_J) \end{Bmatrix}$$

Adaptive Security:
isk/ict can interleave.

if $\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle = \langle \boldsymbol{u}'_i, \boldsymbol{v}'_j \rangle$ for all i, j

$$\approx \begin{Bmatrix} \mathrm{isk}(\boldsymbol{v}'_1) & \mathrm{isk}(\boldsymbol{v}'_2) & \cdots & \mathrm{isk}(\boldsymbol{v}'_I) \\ \mathrm{isk}(\boldsymbol{u}'_1) & \mathrm{ict}(\boldsymbol{u}'_2) & \cdots & \mathrm{ict}(\boldsymbol{u}'_J) \end{Bmatrix}$$

Pairing-Based IPFE [ALS16, LV16]

$[\![\mathrm{isk}]\!]_2 \leftarrow \mathrm{KeyGen}(\mathrm{msk}, [\![\boldsymbol{v}]\!]_2)$

$[\![\mathrm{ict}]\!]_1 \leftarrow \mathrm{Enc}(\mathrm{msk}, [\![\boldsymbol{u}]\!]_1)$

$\xrightarrow[\text{= pairing}]{\mathrm{Dec}} [\![\langle \boldsymbol{u}, \boldsymbol{v} \rangle]\!]_{\mathrm{T}}$

Asymmetric Pairing Groups

$G_1\colon \quad [\![a]\!]_1 = g_1^a$

$G_2\colon \quad [\![b]\!]_2 = g_2^b$

$\xrightarrow[\text{operation}]{\text{pairing}} [\![ab]\!]_{\mathrm{T}} = g_{\mathrm{T}}^{ab} \in G_{\mathrm{T}}$

1-ABE via AKGS and IPFE

$$L_1, \ldots, L_m \leftarrow \mathrm{Garble}(f, \mu)$$

$$\mathrm{sk}_{f,\mu} = \{\mathrm{isk}(L_j)\}_{j \in [m]}$$

$$\mathrm{ct}_x = \mathrm{ict}(x)$$

IPFE Dec

labels in the exponent

$$[\![\ell_j = L_j(x)]\!]_{\mathrm{T}}$$

Eval

✔ linear

$$[\![\mu f(x)]\!]_{\mathrm{T}}$$

Intuitions for Security.

- IPFE $\Longrightarrow$ only ℓ_j's are revealed
- AKGS $\Longrightarrow$ only $\mu f(x)$ is revealed

Selective Security of 1-ABE

Real World

Next step: hardwire labels in secret key

$\xleftarrow{x}$ s.t. $f(x) = 0$

want. μ is hidden

$\mathrm{sk}_{f,\mu}$ $\{\, \mathrm{isk}(\; L_j \quad 0 \;)\,\}$

$L_1, \ldots, L_m \leftarrow \mathrm{Garble}(f, \mu)$

$\ell_j = L_j(x)$

ct_x $\mathrm{ict}(\; x \quad 0 \;)$

Hardwire Labels in Secret Key via IPFE

Next step: simulate labels

$\xleftarrow{\quad x \quad}$ s.t. $f(x) = 0$

want. μ is hidden

$\mathrm{sk}_{f,\mu}$ $\{\,\mathrm{isk}\,(\;0\quad \ell_j\;)\,\}$

$L_1, \ldots, L_m \leftarrow \mathrm{Garble}(f, \mu)$

$\ell_j = L_j(x)$

ct_x $\mathrm{ict}\,(\;x\quad 1\;)$

Simulate Labels via AKGS

$\xleftarrow{\quad x \quad}$ s.t. $f(x) = 0$

want. μ is hidden ✔

$\mathrm{sk}_{f,\mu}$ $\{\, \mathrm{isk}\,(\quad 0 \quad \ell_j \quad)\,\}$

$\ell_1, \ldots, \ell_m \leftarrow \mathrm{Sim}\big(f, x, \mu \underbrace{f(x)}_{=0}\big)$

ct_x $\mathrm{ict}\,(\quad x \quad 1 \quad)$

Adaptive Security?

need x to simulate

$\mathrm{sk}_{f,\mu}$ $\{\, \mathrm{isk}\,(\quad 0 \quad \ell_j \quad)\,\}$ $\quad \ell_1, \dots, \ell_m \leftarrow \mathrm{Sim}\big(f, x, \underbrace{\mu f(x)}_{=0}\big)$

$\xleftarrow{x}$ s.t. $f(x) = 0$

ct_x $\quad \mathrm{ict}\,(\quad x \quad 1 \quad)$

Idea. Rely on special structure of simulator.

Special Simulation Structure

Real Garbling

$\ell_1, \dots, \ell_m$ are uniformly random subject to correctness:

$$\mathrm{Eval}(f, x, \ell_1, \dots, \ell_m) = \mu f(x).$$

linear constraint

Simulator

1. Draw $\ell_2, \dots, \ell_m \leftarrow \mathbb{Z}_p$. ☺ independent of x
2. Find unique ℓ_1 s.t. evaluation is correct.

☺ only one label depends on x

Simulation for Adaptive Security

equation depends on x

$\mathrm{sk}_{f,\mu}$	$\mathrm{isk}(\ 0 \quad \ell_1\ )$	find ℓ_1 s.t. $\mathrm{Eval}(f, x, \ldots) = \mu f(x) = 0$
	$\mathrm{isk}(\ 0 \quad \ell_2\ )$	$\ell_2 \leftarrow \mathbb{Z}_p$
	$\vdots$	$\vdots$
	$\mathrm{isk}(\ 0 \quad \ell_j\ )$	$\ell_j \leftarrow \mathbb{Z}_p$
	$\vdots$	$\vdots$

$\xleftarrow{\ x\ }$ s.t. $f(x) = 0$

ct_x $\quad \mathrm{ict}(\ x \quad 1\ )$

Idea. Put ℓ_1 in ciphertext

Simulation for Adaptive Security

valid simulation strategy

$$\mathsf{sk}_{f,\mu} \quad \mathsf{isk}(\;0 \quad 1 \quad 0\;)$$

$$\mathsf{isk}(\;0 \quad 0 \quad \ell_2\;) \qquad \ell_2 \leftarrow \mathbb{Z}_p$$

$$\vdots \qquad\qquad \vdots$$

$$\mathsf{isk}(\;0 \quad 0 \quad \ell_j\;) \qquad \ell_j \leftarrow \mathbb{Z}_p$$

$$\vdots \qquad\qquad \vdots$$

$$\xleftarrow{\;x\;} \text{ s.t. } f(x) = 0$$

find ℓ_1 s.t. $\mathsf{Eval}(f, x, \ldots) = 0$

$$\mathsf{ct}_x \quad \mathsf{ict}(\;x \quad \ell_1 \quad 1\;)$$

Real World vs. Simulation

Real World

$\mathrm{sk}_{f,\mu}$ $\quad \mathrm{isk}(\ L_1 \quad 0 \quad 0\ )$

$_{j>1}\ \{\mathrm{isk}(\ L_j \quad 0 \quad 0\ )\}$

ct_x $\quad \mathrm{ict}(\ x \quad 0 \quad 0\ )$

$L_1, \ldots, L_m \leftarrow \mathrm{Garble}(f, \mu)$

$\ell_1, \ldots, \ell_m = L_1(x), \ldots, L_m(x)$

honestly generated labels

Simulation

$\mathrm{sk}_{f,\mu}$ $\quad \mathrm{isk}(\ 0 \quad 1 \quad 0\ )$

$_{j>1}\ \{\mathrm{isk}(\ 0 \quad 0 \quad \ell_j\ )\}$

ct_x $\quad \mathrm{ict}(\ x \quad \ell_1 \quad 1\ )$

$\ell_2, \ldots, \ell_m \leftarrow \mathbb{Z}_p$

find ℓ_1 s.t. $\mathrm{Eval}(\cdots) = \mu f(x) = 0$

simulated labels

$?\ \approx$

need **same labels** to use IPFE

$\equiv$

same distribution of labels

Bridging the Gap: Piecewise Security

$$L_1, \ldots, L_m \leftarrow \mathrm{Garble}(f, \mu)$$

Labels are **marginally random** given subsequent label functions.

for $j > 1$ and all x:

$$\left(L_j(x), L_{j+1}, \ldots, L_m\right) \equiv \left(\$, L_{j+1}, \ldots, L_m\right)$$

piecewise security

ℓ_1 is uniquely determined by $\mathrm{Eval}(\cdots) = \mu f(x)$.

We show that AKGS for ABP [IW14] is piecewise secure.

Adaptive Security of 1-ABE

Real World

Next step: hardwire ℓ_1 in ciphertext

$\mathrm{sk}_{f,\mu}$ isk(L_1 0 0 0)

isk(L_2 0 0 0)

$\vdots$

isk(L_j 0 0 0)

$\vdots$

$\xleftarrow{\quad x \quad}$ s.t. $f(x) = 0$

$\ell_1 = L_1(x)$

ct_x ict(x 0 0 0)

Hardwire ℓ_1 in Ciphertext via IPFE

Next step: find unique ℓ_1 from correctness equation

$\mathrm{sk}_{f,\mu}$ $\mathrm{isk}(\ 0 \quad 1 \quad 0 \quad 0\ )$

$\mathrm{isk}(\ L_2 \quad 0 \quad 0 \quad 0\ )$

$\vdots$

$\mathrm{isk}(\ L_j \quad 0 \quad 0 \quad 0\ )$

$\vdots$

$\xleftarrow{\ x\ }$ s.t. $f(x) = 0$

ct_x $\mathrm{ict}(\ x \quad \ell_1 \quad 0 \quad 0\ )$

$\ell_1 = L_1(x)$

Find Unique ℓ_1 via AKGS

$\mathsf{sk}_{f,\mu}$ $\quad \mathsf{isk}(\ 0 \quad 1 \quad 0 \quad 0\ )$

$\quad \mathsf{isk}(\ L_2 \quad 0 \quad 0 \quad 0\ )$

$\quad \vdots$

$\quad \mathsf{isk}(\ L_j \quad 0 \quad 0 \quad 0\ )$

$\quad \vdots$

$\xleftarrow{\quad x \quad}$ s.t. $f(x) = 0$

ct_x $\quad \mathsf{ict}(\ x \quad \ell_1 \quad 0 \quad 0\ )$

find ℓ_1 s.t.
$\mathrm{Eval}(\cdots) = \mu f(x)$

Goal. Simulate ℓ_2 as Random

Next step: hardwire ℓ_2 in ciphertext

$\mathrm{sk}_{f,\mu}$ $\quad \mathrm{isk}(\ 0 \quad 1 \quad 0 \quad 0\ )$

$\mathrm{isk}(\ L_2 \quad 0 \quad 0 \quad 0\ )$ $\quad \ell_2 = L_2(x)$

$\vdots$

$\mathrm{isk}(\ L_j \quad 0 \quad 0 \quad 0\ )$

$\vdots$

$\xleftarrow{\quad x \quad}$ s.t. $f(x) = 0$

find ℓ_1 s.t.
$\mathrm{Eval}(\cdots) = \mu f(x) = 0$

ct_x $\quad \mathrm{ict}(\ x \quad \ell_1 \quad 0 \quad 0\ )$

Hardwire ℓ_2 in Ciphertext via IPFE

Next step: replace ℓ_2 by random

$$\mathrm{sk}_{f,\mu} \quad \mathrm{isk}(\;0 \quad 1 \quad 0 \quad 0\;)$$

$$\mathrm{isk}(\;0 \quad 0 \quad 0 \quad 1\;) \qquad \ell_2 = L_2(x)$$

$$\vdots$$

$$\mathrm{isk}(\;\boxed{L_j} \quad 0 \quad 0 \quad 0\;)$$

$$\vdots$$

$$\xleftarrow{\;x\;} \text{ s.t. } f(x) = 0$$

find ℓ_1 s.t.

$\mathrm{Eval}(\cdots) = \mu f(x) = 0$

$$\mathrm{ct}_x \quad \mathrm{ict}(\;x \quad \boxed{\ell_1} \quad 0 \quad \boxed{\ell_2}\;)$$

Replace ℓ_2 by Random via AKGS

Next step: put ℓ_2 back into secret key

$\mathrm{sk}_{f,\mu}$	isk (	0	1	0	0	)
	isk (	0	0	0	1	)
	$\vdots$					
	isk (	L_j	0	0	0	)
	$\vdots$					
ct_x	ict (	x	ℓ_1	0	ℓ_2	)

$\xleftarrow{x}$ s.t. $f(x) = 0$

$\ell_2 \leftarrow \mathbb{Z}_p$

find ℓ_1 s.t.
$\mathrm{Eval}(\cdots) = \mu f(x) = 0$

Put ℓ_2 Back into Secret Key via IPFE

Goal achieved: simulate ℓ_2

Next step: simulate the other labels

$$
\begin{array}{lllllll}
\mathrm{sk}_{f,\mu} & \mathrm{isk}\,(& 0 & 1 & 0 & 0 &) \\
 & \mathrm{isk}\,(& 0 & 0 & \ell_2 & 0 &) \\
 & \vdots & & & & & \\
 & \mathrm{isk}\,(& L_j & 0 & 0 & 0 &) \\
 & \vdots & & & & & \\
\mathrm{ct}_x & \mathrm{ict}\,(& x & \ell_1 & 1 & 0 &)
\end{array}
$$

$\xleftarrow{\;x\;}$ s.t. $f(x) = 0$

$\ell_2 \leftarrow \mathbb{Z}_p$

find ℓ_1 s.t.
$\mathrm{Eval}(\cdots) = \mu f(x) = 0$

Adaptive Security of 1-ABE

Final Simulation

μ is hidden ✓

$\mathrm{sk}_{f,\mu}$ isk (0 1 0 0)

isk (0 0 ℓ_2 0) $\ell_2 \leftarrow \mathbb{Z}_p$

$\vdots$ $\vdots$

isk (0 0 ℓ_j 0) $\ell_j \leftarrow \mathbb{Z}_p$

$\vdots$ $\vdots$

$\xleftarrow{x}$ s.t. $f(x) = 0$

find ℓ_1 s.t.
$\mathrm{Eval}(\cdots) = \mu f(x) = 0$

ct_x ict (x ℓ_1 1 0)

Adaptively Secure 1-ABE

multi $\{\,\mathrm{sk}\,\}$ $\{\,\mathrm{isk}(\ L_j\ )\,\}$

1 ct $\mathrm{ict}(\ x\ )$

uses msk

? multi-ciphertext security

? make it public-key

Multi-Ciphertext Security

$\mathrm{sk} \quad \{ [\![\mathrm{isk}(\; L_j \;)]\!]_2 \}$

$\mathrm{ct}_1 \quad [\![\mathrm{ict}(\; x_1 \;)]\!]_1$

$\mathrm{ct}_2 \quad [\![\mathrm{ict}(\; x_2 \;)]\!]_1$

$[\![L_j(x_1)]\!]_\mathrm{T}$

$[\![L_j(x_2)]\!]_\mathrm{T}$

Problem. Label functions (its randomness) cannot be reused.

Idea. Use DDH to rerandomize them.

Multi-Ciphertext Security

sk $\{ [\![\mathrm{isk}(\, L_j \,)]\!]_2 \}$

ct$_1$ $[\![\mathrm{ict}(\, \rho_1 x_1 \,)]\!]_1$

ct$_2$ $[\![\mathrm{ict}(\, \rho_2 x_2 \,)]\!]_1$

Intuition. Label functions are pseudorandom via DDH.

$[\![\rho_1 L_j(x_1)]\!]_\mathrm{T}$

$[\![\rho_2 L_j(x_2)]\!]_\mathrm{T}$

Problem. $[\![\rho L_j]\!]_\mathrm{T}$ is not pseudorandom given $[\![\rho]\!]_1, [\![L_j]\!]_2$.

Idea. Use IPFE to move ρ into the same group as L_j's, then use DDH.

Adaptively Secure Secret-Key ABE

multi $\{\ \mathrm{sk}\ \}$ $\{\ [\![\ \mathrm{isk}\ (\ \ L_j\ \ )\ ]\!]_2\ \}$

multi $\{\ \mathrm{ct}\ \}$ $[\![\ \mathrm{ict}\ (\ \ \rho x\ \ )\ ]\!]_1$

uses msk

multi-ciphertext security

Slotted IPFE ++

make it public-key

Public-Key ABE via Slotted IPFE ++

for scheme | for proof

IPFE with **public slot** + **private slot**

KeyGen needs msk

multi $\{\ \mathrm{sk}\ \}$ $\quad \{\ [\![\ \mathrm{isk}\ (\quad L_j \quad\quad 0 \quad)\ ]\!]_2\ \}$

not hidden — function-hiding

multi $\{\ \mathrm{ct}\ \}$ $\quad [\![\ \mathrm{ict}\ (\quad \rho x \quad\quad 0 \quad)\ ]\!]_1$

Enc using mpk (or msk) — Enc needs msk

make it public-key

function-hiding IPFE

piecewise secure AKGS

for ABP

1-ABE

uniform computation: more challenges

slotted IPFE

full ABE

for ABP

Ideas for Uniform Model

DFA/NFA/L/NL = matrix multiplication

✔ piecewise secure AKGS for each input length

✘ **unique challenge:**

$$\#[\ell, \boldsymbol{r}] \propto |x|TS2^S|\mathrm{TM}| \quad \text{(or } |x| \cdot |\mathrm{TM}| \text{ for DFA/NFA)}$$

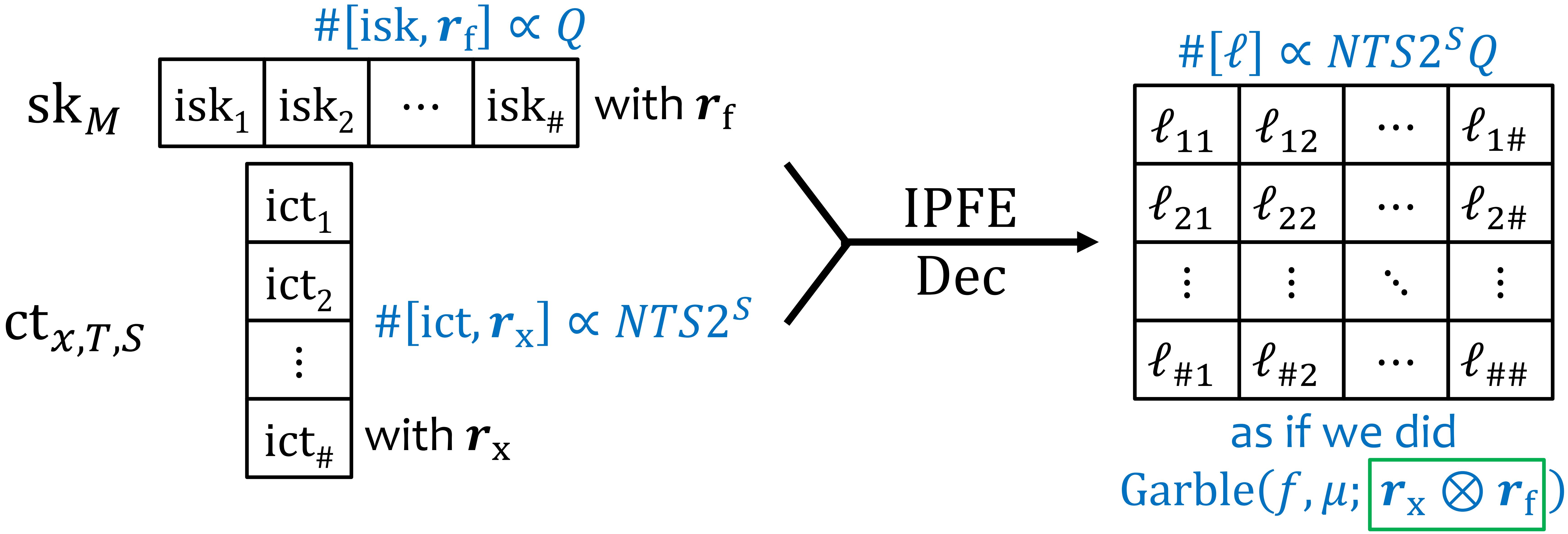
$$\Downarrow$$

$$|\mathrm{ct}| \propto |x|TS2^S$$

$$|\mathrm{sk}| \propto |\mathrm{TM}|$$

Neither sk nor ct can fit all label functions / labels!

Tensoring for Expansion



Intuition. $[\![\boldsymbol{r}_\mathrm{x} \otimes \boldsymbol{r}_\mathrm{f}]\!]_\mathrm{T} \overset{\mathrm{DDH}}{\approx} [\![\boldsymbol{r}]\!]_\mathrm{T}$

function-hiding IPFE

piecewise secure AKGS

1-ABE

slotted IPFE

full ABE for ABP / DFA/NFA / L/NL

Thank you!

ia.cr/2020/318