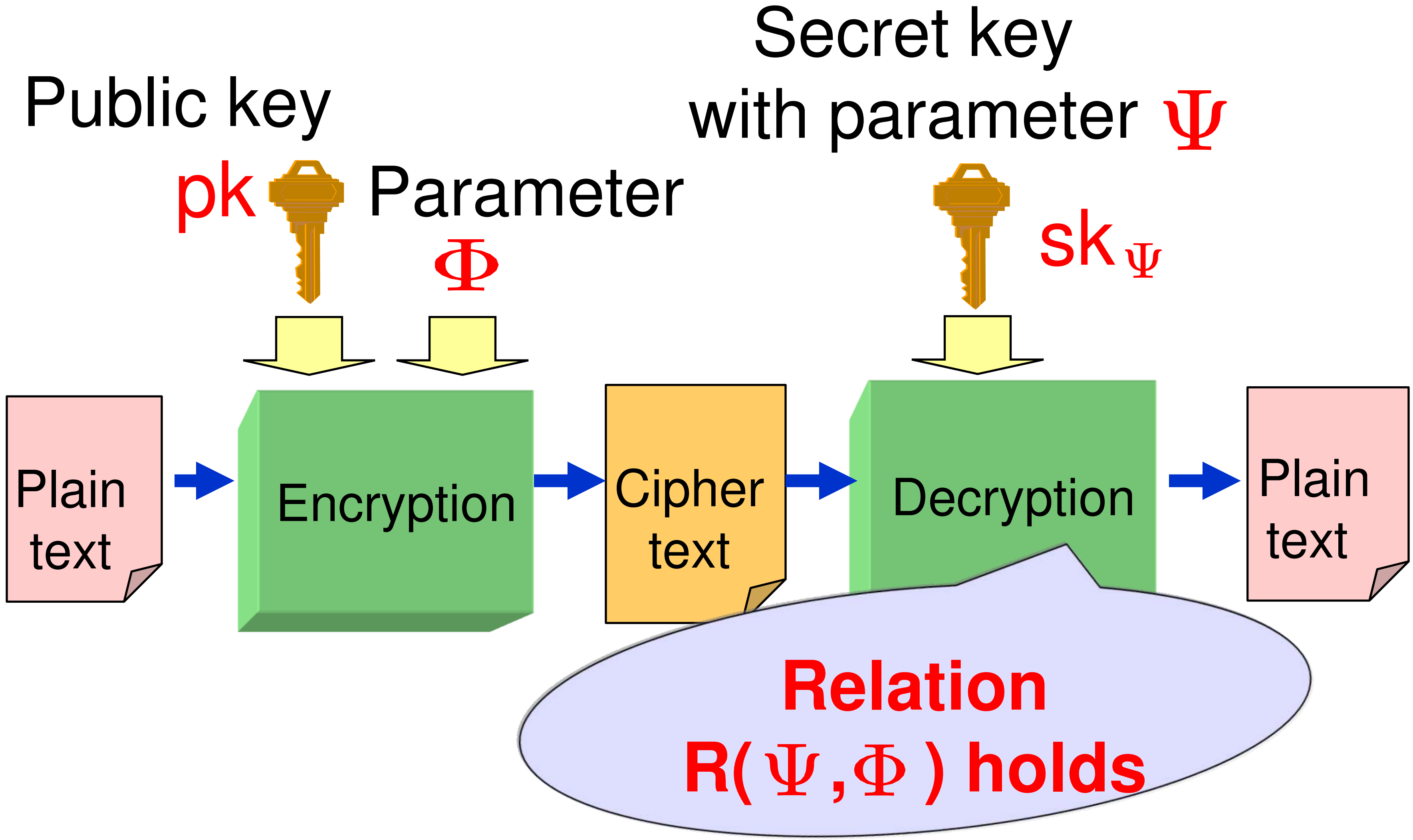
Fully Secure Unbounded Inner-Product and Attribute-Based Encryption

2012 / 12 / 4

Tatsuaki Okamoto (NTT)
Katsuyuki Takashima (Mitsubishi Electric)

Functional Encryption



- This type is called Predicate Encryption in [BSW11].

Previously Proposed Special Cases of FE

	Φ	Ψ	R
ID-based enc. (IBE)	ID	ID'	ID = ID'
Attribute-based enc. (ABE)	Attributes Γ	Access structure $\mathbb{S}$	$\mathbb{S}$ accepts Γ
	Access structure $\mathbb{S}$	Attributes Γ	
Inner-product enc. (IPE)	Vector $\overrightarrow{x}$	Vector $\overrightarrow{v}$	$\overrightarrow{x} \cdot \overrightarrow{v} = 0$

Key-policy (KP)-ABE
Ciphertext-policy (CP)-ABE

- In ABE, access structures are usually given by span programs.
- In IPE, the anonymity of vector $\vec{x}$ (attribute-hiding security) is usually required. Any CNF or DNF formula can be realized by inner-product predicates.

Inner-Product Predicates [KSW 08]

- $R(\vec{v}, \vec{x}) = 1 \iff \vec{x} \cdot \vec{v} = 0$

- (Example 1) Equality (ID-based encryption etc.)

  $\overrightarrow{x} := \delta(x, 1)$, $\overrightarrow{v} := \sigma(1, -a)$: 2-dimensional vectors

  ⇨ $x = a \Leftrightarrow \overrightarrow{x} \cdot \overrightarrow{v} = 0$ for any random δ and σ

  (Example 2) $(x = a) \wedge (y = b) \Leftrightarrow \forall(\delta, \sigma, \delta', \sigma')\ [\delta\delta'(x - a) + \sigma\sigma'(y - b) = 0]$

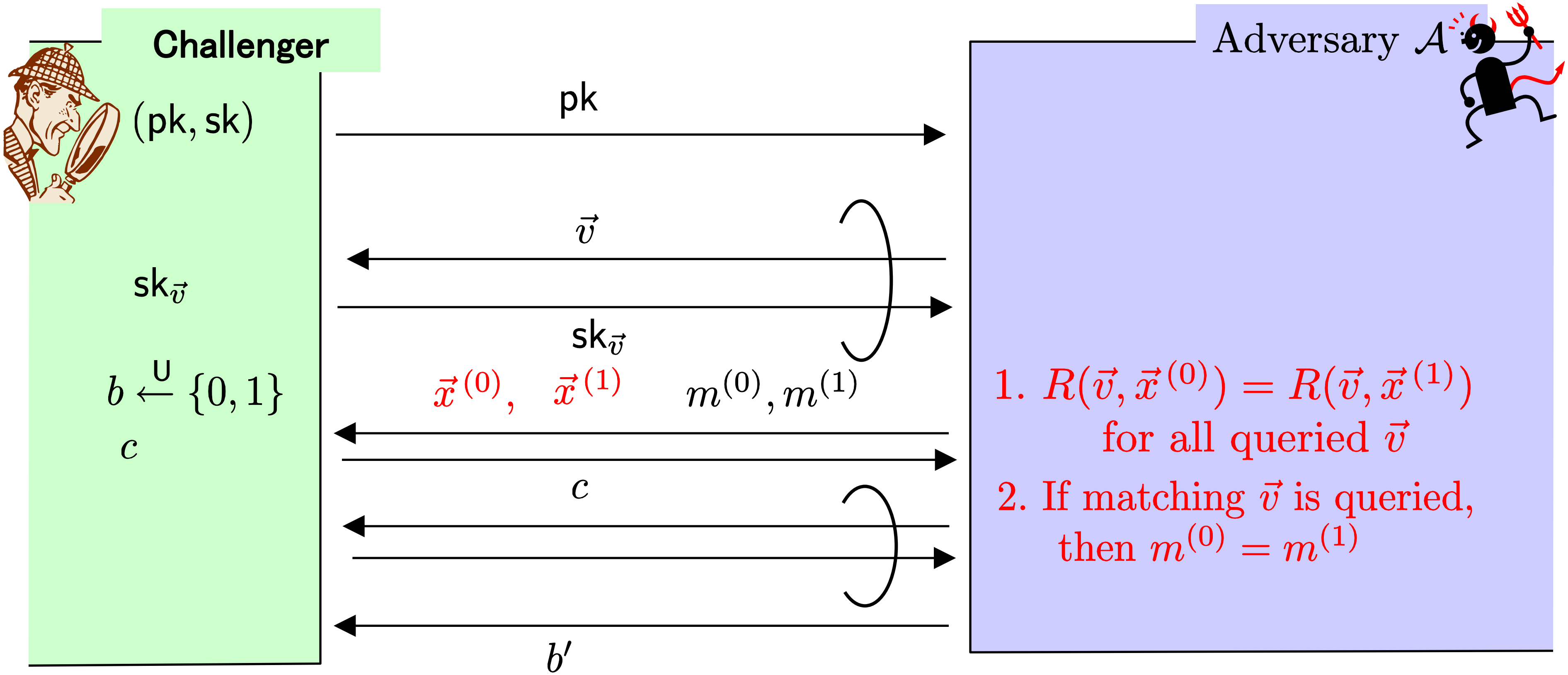
  ⇨ $\overrightarrow{x} := (\delta(x, 1), \sigma(y, 1))$, $\overrightarrow{v} := (\delta'(1, -a), \sigma'(1, -b))$:
  4-dimensional vectors

  (Example 3) $(x = a) \vee (x = b) \Leftrightarrow (x - a)(x - b) = x^2 - (a + b)x + ab = 0$

  ⇨ $\overrightarrow{x} := \delta(x^2, x, 1)$, $\overrightarrow{v} := \sigma(1, -(a + b), ab)$: 3-dimensional vectors

  ⇨ Any CNF, DNF formula can be realized by inner-product predicate.

Adaptively Secure & Fully Attribute-Hiding (AH) IPE



Adversary $\mathcal{A}$ wins if $b = b'$.

No additional information on $\vec{x}$ is revealed even to any person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $R(\vec{v}, \vec{x}) = 1$.

Unbounded FE

- All previous constructions of IPE and ABE except Lewko-Waters unbounded ABE are bounded, in the sense that the public parameters (pk) impose additional limitations on the parameters ($\Phi, \ \Psi$) for encryption and decryption keys,

  e.g., available dimension n in existing IPE is bounded by pk.

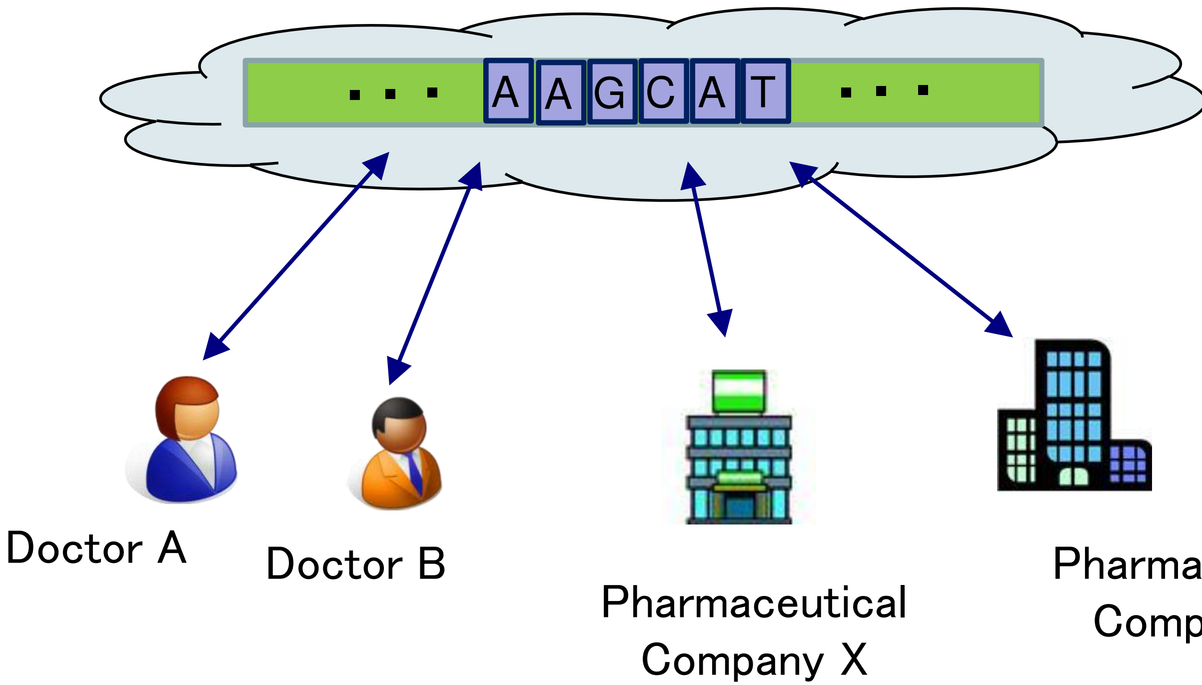
- In practice, it is highly desirable that the parameters ($\Phi, \ \Psi$) should be flexible or unbounded by pk fixed at setup, since if we set pk for a possible maximum size, the size of pk should be huge.

- Existing IPE schemes have another restriction on the parameters (vectors), i.e., dimensions of attributes and predicates should be equivalent. ↑

Why is it a restriction ?

Genetic Profile Data Predicate Search (I)

- A large amount of sensitive genetic profile data of an individual are stored in a remote server
- Only a part of the profile is examined in many applications (for various purposes)



Data Processing and Retrieval

Genetic Profile Data Predicate Search (II)

- Genetic property variables $X_1, \ldots, X_{100}$;
  Alice's values $x_1, \ldots, x_{100}$
- Evaluate if $f(x_1, \ldots, x_{100}) = 0$ for an examination of a degree-3 polynomial f

⇒ $\vec{x} := (1, x_1, \ldots, x_{100}, x_1x_2, \ldots, x_{100}^2, x_1^3, x_1^2x_2, \ldots, x_{100}^3)$
whose dimension is around 10^6

- Predicate for $\vec{v}$, $((X_5 = a) \vee (X_{16} = b)) \wedge (X_{57} = c)$

⇔ Polynomial $f := r_1(X_5 - a)(X_{16} - b) + r_2(X_{57} - c)$
$= (r_1ab - r_2c) - r_1bX_5 - r_1aX_{16} + r_2X_{57} + r_1X_5X_{16}$

$(r_1, r_2 \stackrel{\mathsf{U}}{\leftarrow} \mathbb{F}_q)$

⇔ $\vec{v} := ((r_1ab - r_2c), 0, \ldots, 0, -r_1b, 0, \ldots, 0, -r_1a, 0, \ldots, 0, r_2, 0, \ldots, 0, r_1, 0, \ldots, 0)$

Effective dimension of $\vec{v}$ is 5, instead of 10^6 !!

Generalized Inner-Product

- Generalized (attribute and predicate) vectors
  - $\vec{x} := \{(t, x_t) \,|\, t \in I_{\vec{x}},\ x_t \in \mathbb{F}_q\} \setminus \{\vec{0}\}$ with finite index set $I_{\vec{x}} \subset \mathbb{N}$
  - $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}},\ v_t \in \mathbb{F}_q\} \setminus \{\vec{0}\}$ with finite index set $I_{\vec{v}} \subset \mathbb{N}$
  - If $I_{\vec{x}} = \{1, \ldots, n\}$, $\vec{x} = (x_1, \ldots, x_n)$ i.e., conventional vector
- Three types of generalized IPE with respect to the decryption condition
  - For Type 1, $R(\vec{v}, \vec{x}) = 1 \Leftrightarrow I_{\vec{v}} \subseteq I_{\vec{x}}$ and $\sum_{t \in I_{\vec{v}}} v_t x_t = 0$.
  - For Type 2, $R(\vec{v}, \vec{x}) = 1 \Leftrightarrow I_{\vec{v}} \supseteq I_{\vec{x}}$ and $\sum_{t \in I_{\vec{x}}} v_t x_t = 0$.
  - For Type 0, for $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{x} := (x_1, \ldots, x_{n'})$,

    $$R(\vec{v}, \vec{x}) = 1 \Leftrightarrow n = n' \text{ and } \sum_{t=1}^{n} v_t x_t = 0.$$

Previous Work on Unbounded FE [LW11]

- Unbounded HIBE that is fully secure in the standard model
- Unbounded KP-ABE that is selectively secure

Our Results

- We introduce a new concept of IPE, generalized IPE
  - Type 0, Type 1, Type 2
- present the first unbounded IPE schemes
  - adaptively secure and fully attribute-hiding under DLIN (in the standard model)
- present the first unbounded KP- and CP-ABE schemes that are fully secure (adaptively payload-hiding) under DLIN

Dual Pairing Vector Space Approach (I)

- Vector space $\mathbb{V} := \mathbb{G}^N$ using symmetric pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$, where G is a generator of $\mathbb{G}$

- **(Canonical) pairing operation:**

For $\boldsymbol{x} := (x_1 G, \ldots, x_N G) \in \mathbb{V}$ and $\boldsymbol{y} := (y_1 G, \ldots, y_N G) \in \mathbb{V}$,

$$e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(x_i G, y_i G) \in \mathbb{G}_T.$$

⇨ $e(\boldsymbol{x}, \boldsymbol{y}) = e(G, G)^{\vec{x} \cdot \vec{y}}$, where $\vec{x} := (x_1, \ldots, x_N)$, $\vec{y} := (y_1, \ldots, y_N)$.

- **Dual bases :**

$\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$: basis of $\mathbb{V}$ s.t. $X := (\chi_{i,j}) \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q)$,

$\boldsymbol{b}_i := (\chi_{i,1} G, \ldots, \chi_{i,N} G)$ for $i = 1, \ldots, N.$

$\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$ s.t. $\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $(\vartheta_{i,j}) := \psi (X^{\mathrm{T}})^{-1}$,

$\boldsymbol{b}_i^* = (\vartheta_{i,1} G, \ldots, \vartheta_{i,N} G)$ for $i = 1, \ldots, N.$

⇨ $(\mathbb{B}, \mathbb{B}^*)$: dual orthonormal bases, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}_i^*) = g_T$,

$e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = 1 \text{ for } i \neq j$ where $g_T = e(G, G)^{\psi}$

DPVS Approach (II)

- Dual Pairing Vector Space (DPVS) approach :

  Cryptographic Construction using $\mathbb{V}$ with (the canonical pairing and) random dual bases as a master key pair

  - DLIN-based security (from [OT10] machinery)

- **Notation :**

  For $\vec{x} := (x_1, \ldots, x_N)$ and $\vec{y} := (y_1, \ldots, y_N)$, we denote

$$\boldsymbol{x} := (\vec{x})_{\mathbb{B}} := (x_1, \ldots, x_N)_{\mathbb{B}} := x_1 \boldsymbol{b}_1 + \cdots + x_N \boldsymbol{b}_N \in \mathbb{V},$$
$$\boldsymbol{y} := (\vec{y})_{\mathbb{B}^*} := (y_1, \ldots, y_N)_{\mathbb{B}^*} := y_1 \boldsymbol{b}_1^* + \cdots + y_N \boldsymbol{b}_N^* \in \mathbb{V}.$$

$\Longrightarrow$ $e(\boldsymbol{x}, \boldsymbol{y}) = g_T^{\vec{x} \cdot \vec{y}} \in \mathbb{G}_T$ where $g_T = e(G, G)^{\psi}$

Basic Idea for Constructing IPE using DPVS

- Setup : $(\mathsf{param}, \mathbb{B}, \mathbb{B}^*)$: $(n+1)$-dim. param. with dual bases

  $\mathsf{pk} := (\mathsf{param}, \mathbb{B}), \quad \mathsf{sk} := \mathbb{B}^*$

- KeyGen$(\mathsf{sk}, \vec{v} := (v_1, \ldots, v_n))$:

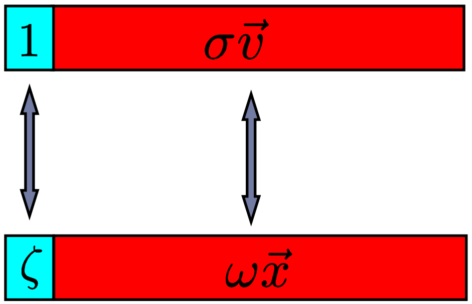
  $$\boldsymbol{k}^* := \boldsymbol{b}_0^* + \sigma(v_1 \boldsymbol{b}_1^* + \cdots + v_n \boldsymbol{b}_n^*)$$
  $$= (\ 1,\ \ \sigma\vec{v}\ )_{\mathbb{B}^*}$$

- Enc$(\mathsf{pk}, \vec{x} := (x_1, \ldots, x_n), m)$:

  $$\boldsymbol{c}_1 := \zeta \boldsymbol{b}_0 + \omega(x_1 \boldsymbol{b}_1 + \cdots + x_n \boldsymbol{b}_n)$$
  $$= (\ \zeta,\ \ \omega\vec{x}\ )_{\mathbb{B}}$$

  $c_2 := g_T^{\zeta} \cdot m$, where $g_T := e(\boldsymbol{b}_i, \boldsymbol{b}_i^*)$

- Dec$(\mathsf{pk}, \boldsymbol{k}^*, (\boldsymbol{c}_1, c_2))$: $m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$



$\zeta + \sigma\omega\,(\vec{v} \cdot \vec{x})$
$= \zeta$ if $\vec{v} \cdot \vec{x} = 0$,
random
if $\vec{v} \cdot \vec{x} \neq 0$.

Adaptively Fully-Attribute-Hiding IPE [OT12a]

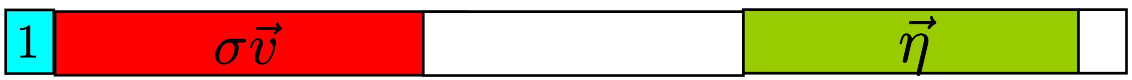
- Setup : $(\mathsf{param}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+2)$

  $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{b}_{3n+1}^*, \ldots, \boldsymbol{b}_{4n}^*),$

  $\mathsf{pk} := (\mathsf{param}, \widehat{\mathbb{B}}), \quad \mathsf{sk} := \widehat{\mathbb{B}}^*$

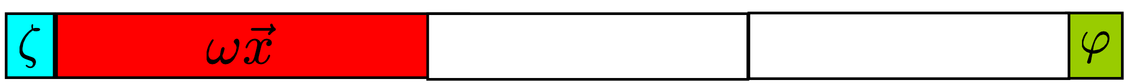
- KeyGen$(\mathsf{sk}, \vec{v})$:

$$\boldsymbol{k}^* := (\ \overbrace{1,}^{1}\ \overbrace{\sigma\vec{v},}^{n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\vec{\eta},}^{n}\ \overbrace{0}^{1}\ )_{\mathbb{B}^*},$$



- Enc$(\mathsf{pk}, \vec{x}, m)$:

$$\boldsymbol{c}_1 := (\ \overbrace{\zeta,}^{1}\ \overbrace{\omega\vec{x},}^{n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{0^{n},}^{n}\ \overbrace{\varphi}^{1}\ )_{\mathbb{B}},$$



$c_2 := g_T^{\zeta} \cdot m, \quad$ where $\quad g_T := e(\boldsymbol{b}_i, \boldsymbol{b}_i^*)$

- Dec$(\mathsf{pk}, \boldsymbol{k}^*, (\boldsymbol{c}_1, c_2))$: $\quad m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$

Key Techniques for Fully Secure Unbounded FE

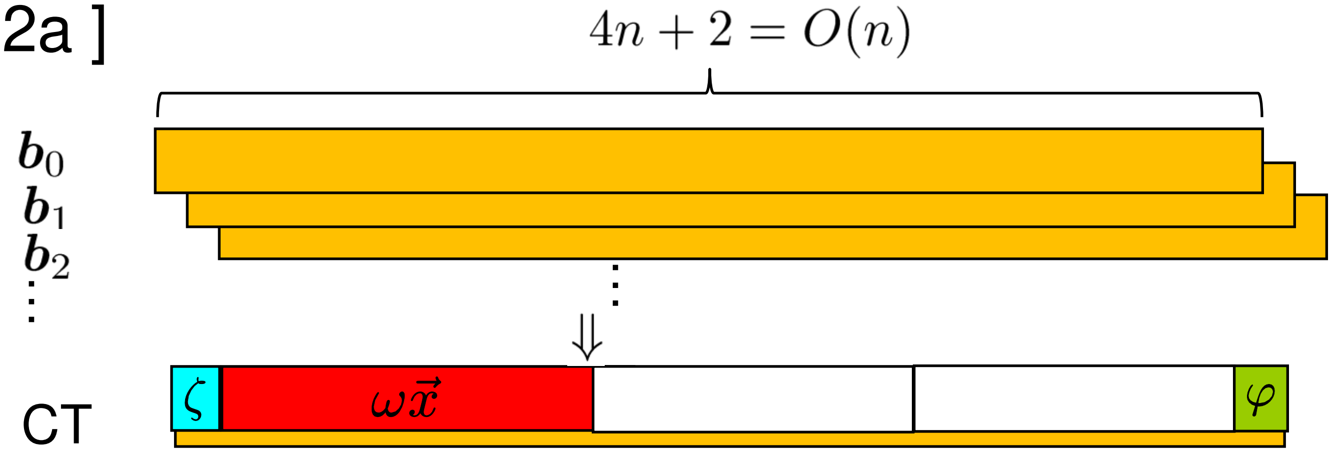
- The difficulty of realizing fully secure unbounded IPE (or ABE) arises from the hardness of supplying an unbounded amount of randomness consistent with the complicated key-query condition under a "constant size" pk

- We develop novel techniques, indexing and consistent randomness amplification technique
  - indexing:
    supply a source of unbounded amount of randomness
  - consistent randomness amplification:
    amplify the randomness of the source and
    adjust the distribution consistently with the condition

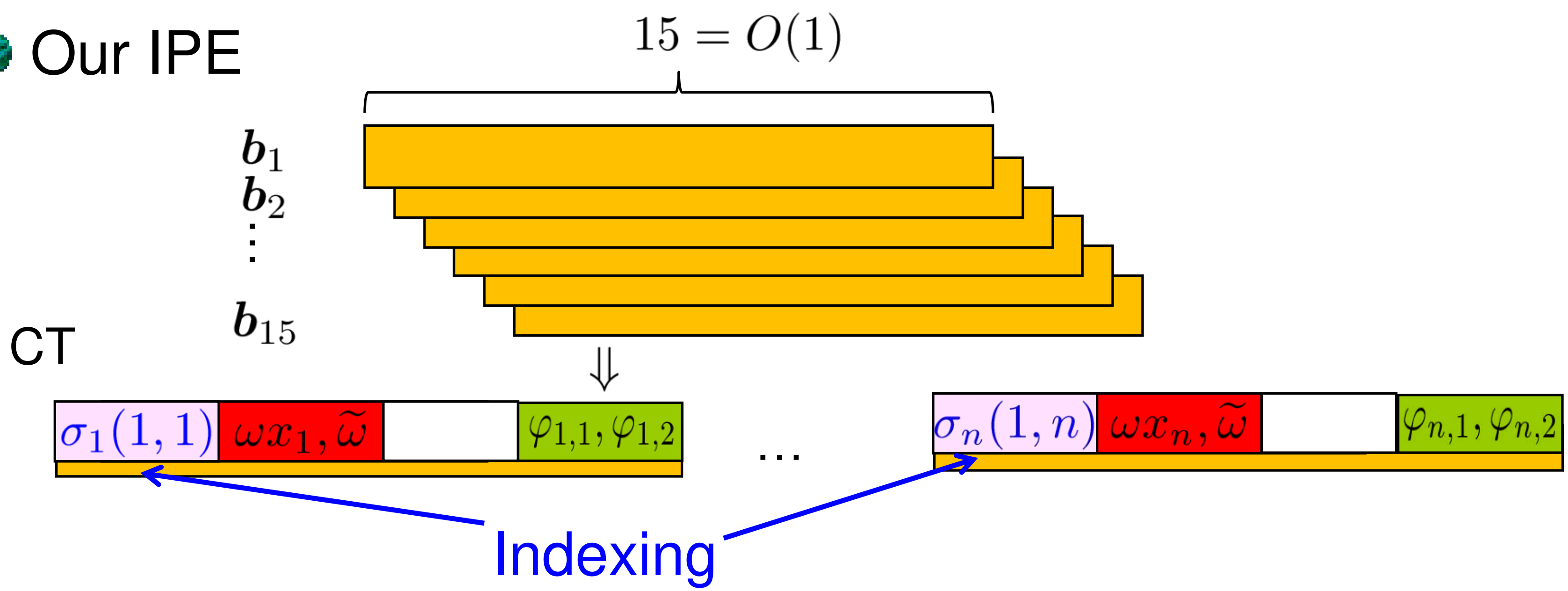
Indexing for Type 1 IPE (I)

For simplicity, $I_{\vec{x}} := \{1, \dots, n\}$

- [OT12a]

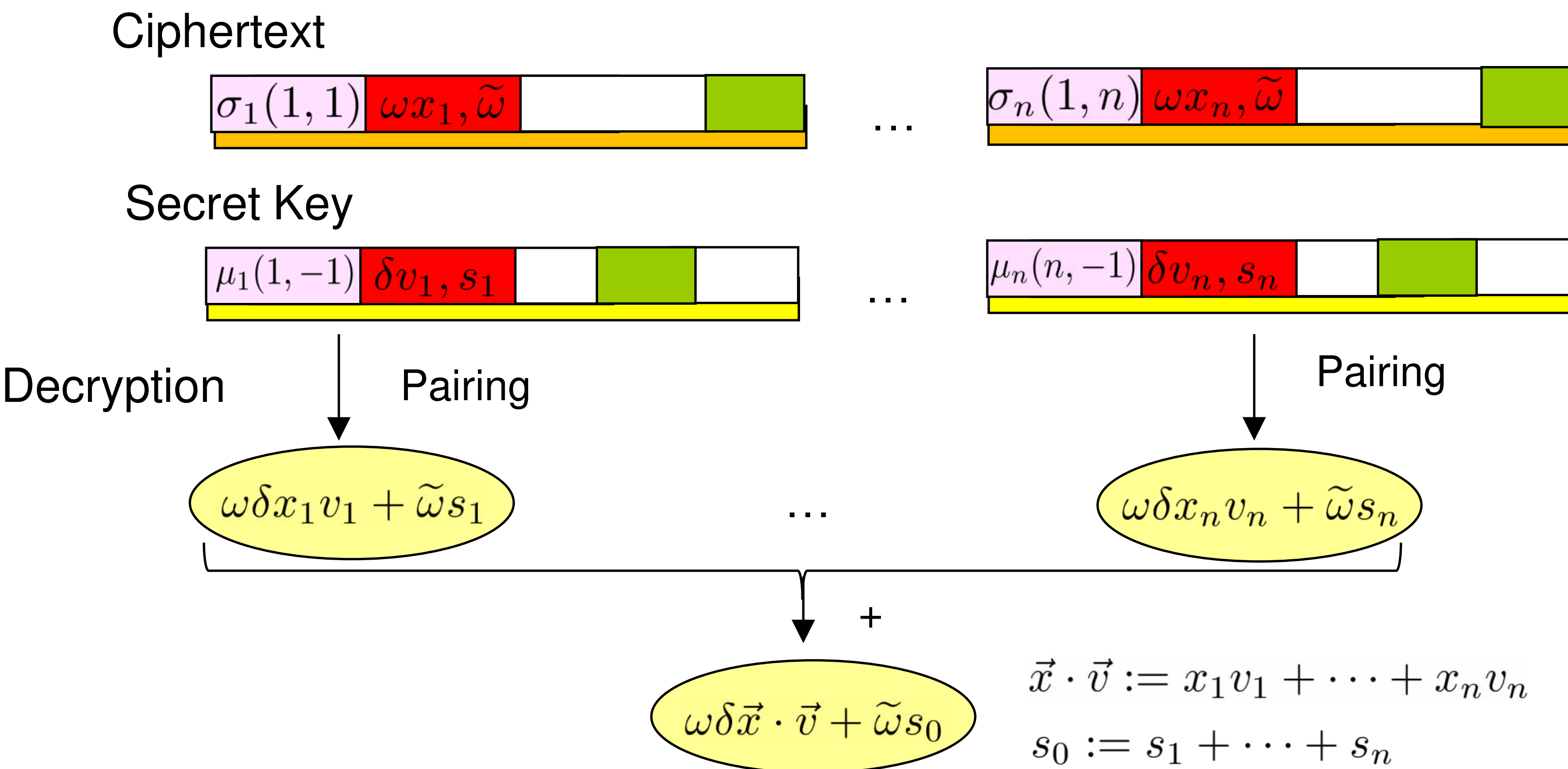


- Our IPE



Indexing for Type 1 IPE (II)

Assume $n = n'$



$$\vec{x}\cdot\vec{v} := x_1 v_1 + \cdots + x_n v_n$$

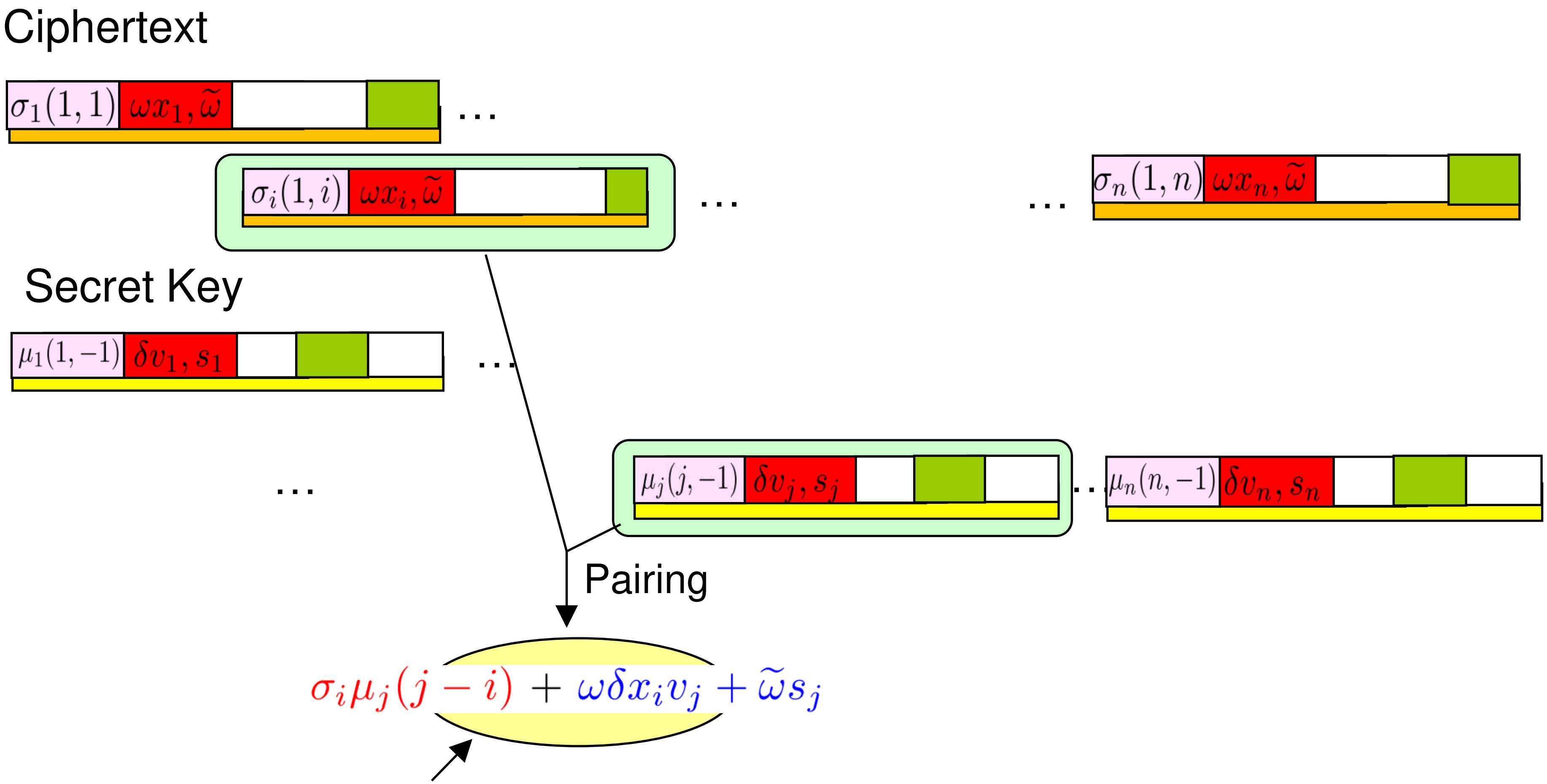
$$s_0 := s_1 + \cdots + s_n$$

Correctness

If $\vec{x}\cdot\vec{v} = 0,$ $\omega\delta\vec{x}\cdot\vec{v} + \widetilde{\omega} s_0 = \widetilde{\omega} s_0$ is recovered and the secret $\widetilde{\omega} s_0$ is used for correct decryption.

Indexing for Type 1 IPE (III)

- Pairing elements for $i \neq j$



- Correlation from index part, $\sigma_i \mu_j (j-i)$, randomizes $\omega \delta x_i v_j + \widetilde{\omega} s_j$ (prevention of collusion attack)

Adaptively Fully-AH Unbounded Type 1 IPE

Setup(1^λ) : $(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15))$,

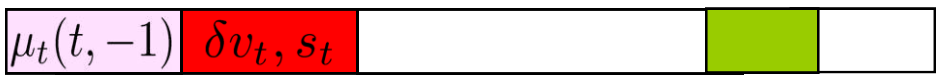
pk $:= (1^\lambda,\ \mathsf{param},\ \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15}))$,

sk $:= (\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, .., \boldsymbol{b}_4^*, \boldsymbol{b}_{12}^*, \boldsymbol{b}_{13}^*))$.

KeyGen(pk, sk, $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$) : $s_t \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t \in I_{\vec{v}}$, $s_0 := \sum_{t \in I_{\vec{v}}} s_t$,

$$\boldsymbol{k}_0^* := (\ -s_0,\ 0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*},$$

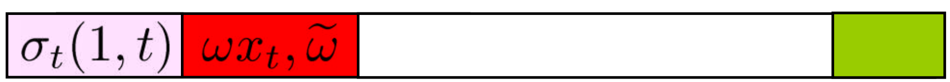
$$\boldsymbol{k}_t^* := (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t}^{4}\ \ \overbrace{0^7,}^{7}\ \ \overbrace{\eta_{t,1}, \eta_{t,2},}^{2}\ \ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*} \quad \text{for } t \in I_{\vec{v}}$$



Enc(pk, m, $\vec{x} := \{(t, x_t) \mid t \in I_{\vec{x}}\}$) : $\widetilde{\omega} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_0 := (\ \widetilde{\omega},\ 0,\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \qquad c_T := g_T^\zeta m,$$

$$\boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega x_t,\ \widetilde{\omega}}^{4}\ \ \overbrace{0^7,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\varphi_{t,1}, \varphi_{t,2}}^{2}\ )_{\mathbb{B}} \quad \text{for } t \in I_{\vec{x}}$$



Dec(pk, $\mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$, $\mathsf{ct}_{\vec{x}} := (I_{\vec{x}}, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$) :

if $I_{\vec{v}} \subseteq I_{\vec{x}}$, $K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{t \in I_{\vec{v}}} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*)$, return c_T / K, else, return $\perp$.

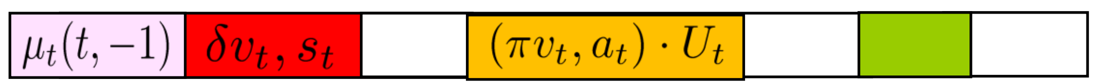
Consistent Randomness Amplification

normal secret key: $\boldsymbol{k}_t^* := (\mu_t(t,-1), \delta v_t, s_t, \boxed{0^7}, \ldots)_{\mathbb{B}^*}$

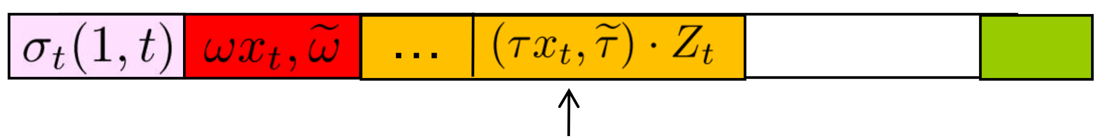
normal ciphertext: $\boldsymbol{c}_t := (\sigma_t(1,t),\ \omega x_t,\ \widetilde{\omega}, \boxed{0^7}, \ldots)_{\mathbb{B}}$

Computational & Information-Theoretical Changes

$\boldsymbol{k}_t^* := (\mu_t(t,-1), \delta v_t, s_t, \boxed{0^4, (\pi v_t, a_t)\cdot U_t,\ 0},\ \ldots)_{\mathbb{B}^*}$



$\boldsymbol{c}_t := (\sigma_t(1,\ t), \omega x_t,\ \widetilde{\omega}, \boxed{\ldots, (\tau x_t, \widetilde{\tau})\cdot Z_t,\ 0}, \ldots)_{\mathbb{B}}$



Amplified consistently with the key condition

where $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$ and $U_t := (Z_t^{\mathrm{T}})^{-1}$

Comparison of IPE Schemes

	KSW08	OT10	OT12a		OT12b	
			(basic)	(variant)	(type 1 or 2)	(type 0)
Bounded or Unbounded	bounded	bounded	bounded		unbounded	
Restriction on IP relation	restricted*	restricted	restricted		relaxed	restricted
Security	selective & fully-AH	adaptive & weakly-AH	adaptive & fully-AH		adaptive & fully-AH	
Order of $\mathbb{G}$	composite	prime	prime		prime	
Assump.	2 variants of GSD	DLIN	DLIN		DLIN	
PK size	$O(n)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n)\lvert\mathbb{G}\rvert$	$O(1)\lvert\mathbb{G}\rvert$	$O(1)\lvert\mathbb{G}\rvert$
SK size	$(2n+1)\lvert\mathbb{G}\rvert$	$(3n+2)\lvert\mathbb{G}\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$	$11\lvert\mathbb{G}\rvert$	$(15n+5)\lvert\mathbb{G}\rvert$	$(21n+9)\lvert\mathbb{G}\rvert$
CT size	$(2n+1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(3n+2)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(4n+2)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(5n+1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(15n'+5)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(21n'+9)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$

* It can be easily relaxed.

$n := \sharp I_{\vec{v}},\ n' := \sharp I_{\vec{x}}$: dimensions of predicate vector and attribute vector

$\lvert\mathbb{G}\rvert$, $\lvert\mathbb{G}_T\rvert$: size of an element of $\mathbb{G}$, $\mathbb{G}_T$

AH, IP, GSD : attribute-hiding, inner product, general subgroup decision

PK, SK, CT : public key, secret key, ciphertext