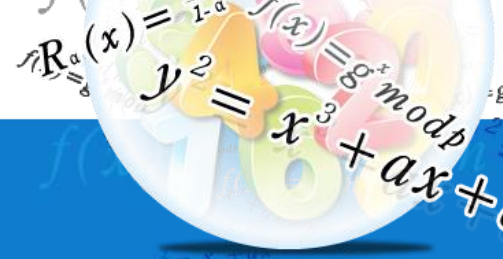


PKC 2016

Identity-based Hierarchical Key-insulated Encryption without Random Oracles

Yohei Watanabe[1,3] Junji Shikata[1,2]

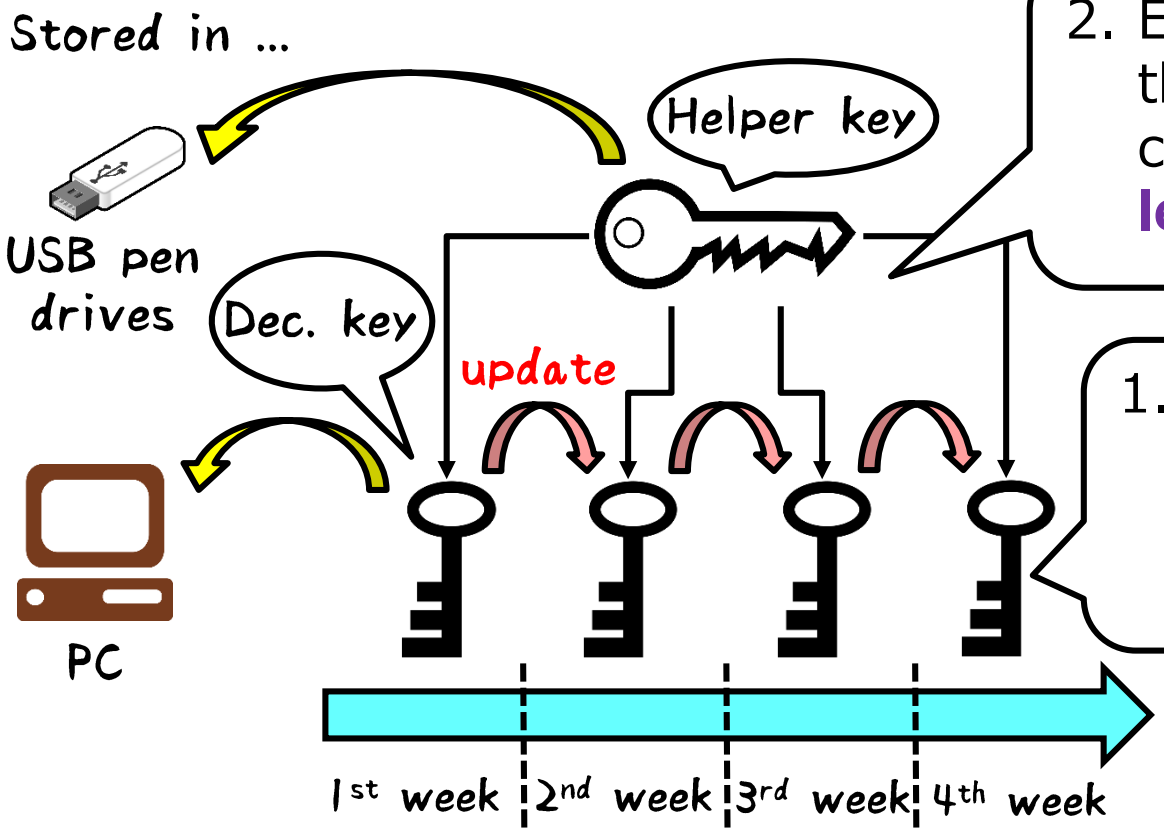
1 Graduate School of Environment and Information Sciences, YNU, Japan

2 Institute of Advanced Sciences, YNU, Japan

3. ITRI, AIST, Japan

Key Insulation [DKXY02]

◆ **One of solutions to *key exposure problem***

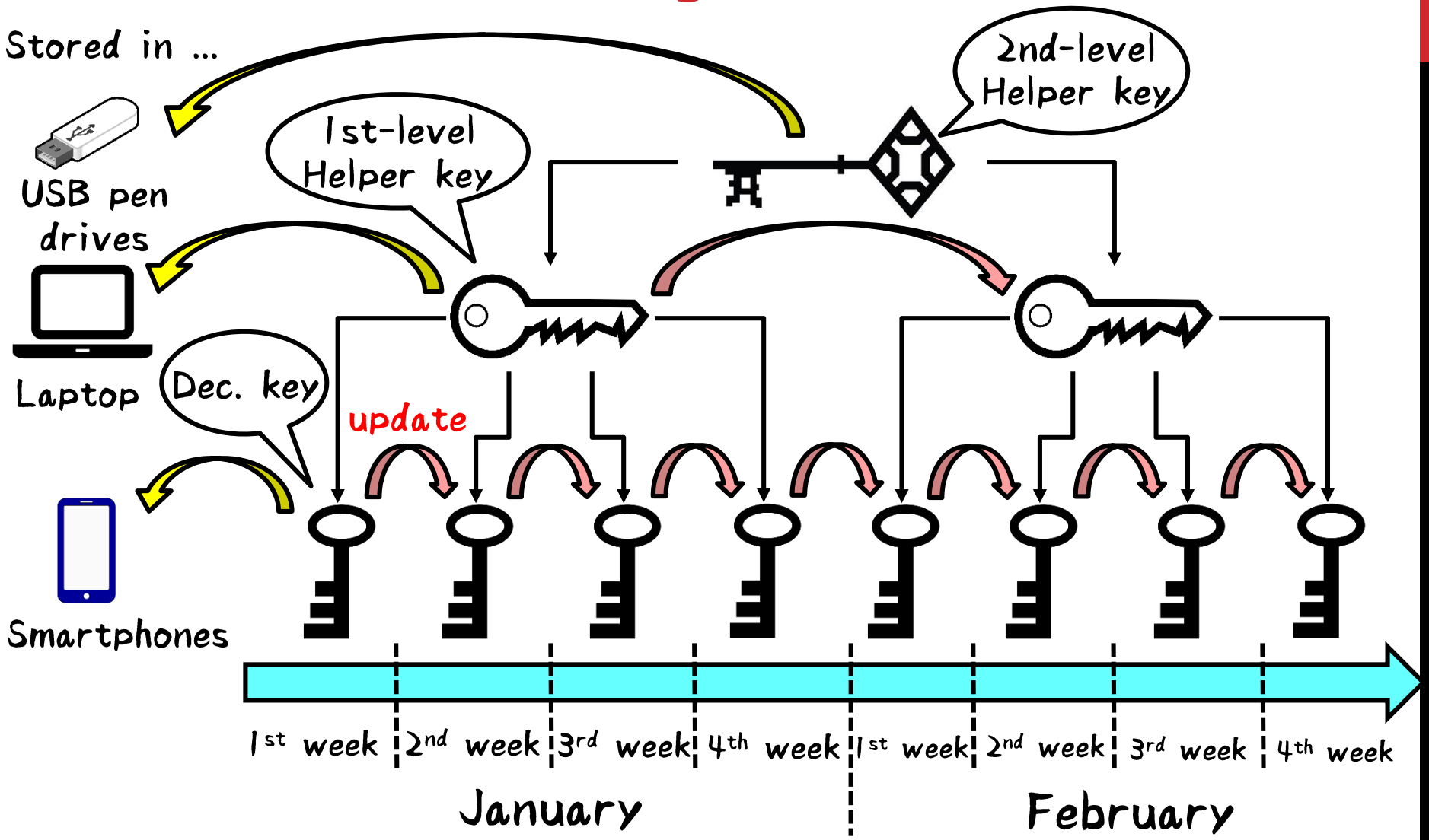


2. Even if is exposed, the security is not compromised **unless at least one is exposed**

1. If a number of are exposed, the fact does not affect at other time-periods

The scheme is { secure if it satisfies 1
strongly secure if it satisfies both 1 and 2

Hierarchical Key Insulation [HHSI05]

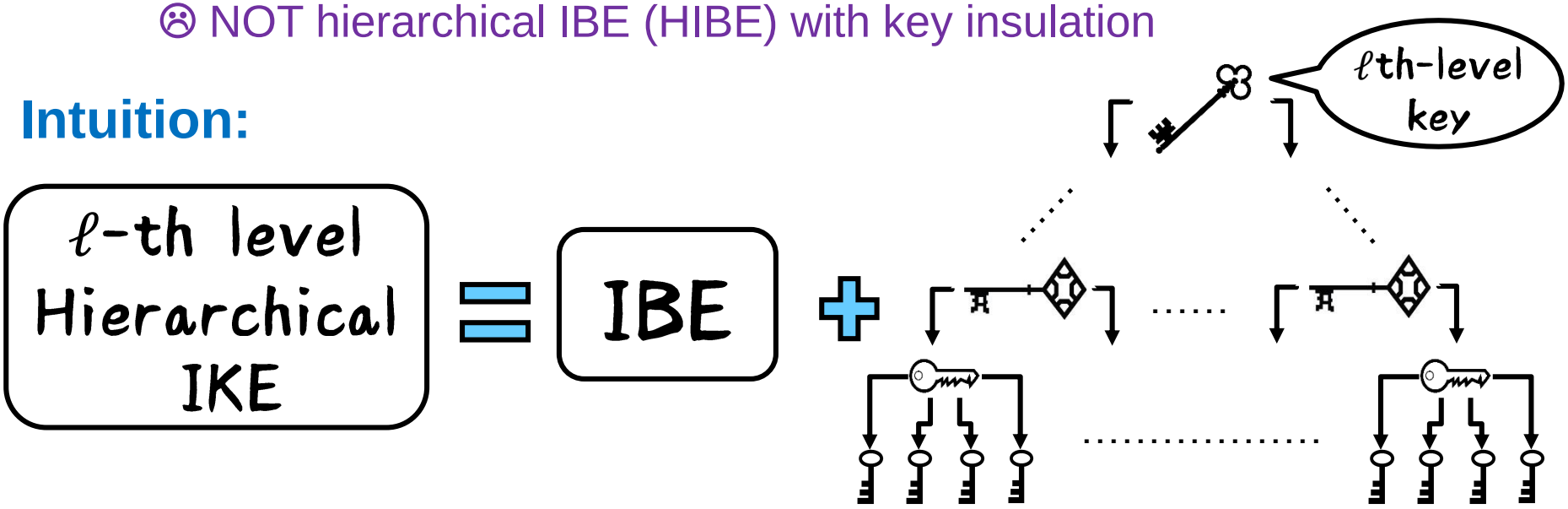


There seem to be various practical applications !

Identity-based Hierarchical Key-insulated Encryption [HHSI05]

- **Abbreviated to ``hierarchical IKE"**
  - ☺ Identity-based encryption (IBE) with hierarchical key insulation
  - ☹ NOT hierarchical IBE (HIBE) with key insulation

Intuition:



- **First proposed by Hanaoka et al. at ASIACRYPT 2005 [HHSI05]**
  - In the random oracle model (ROM)

However, NO known hierarchical IKE schemes w/o ROM !

Our Contribution

We propose an ℓ-level hierarchical IKE scheme that achieves:

(1) Strong security in the standard model from simple assumptions

- ✓ Using asymmetric pairing
- ✓ From Symmetric eXternal Diffie-Hellman (SXDH) assumption
- ✓ Based on Jutla-Roy HIBE [JR13] and its variant [RS14]

(2) Space efficiency (any parameters do not depend on ID-space sizes)

- ✓ Constant-size parameters when the hierarchy is one (i.e. $\ell = \mathbf{1}$)
  - ➢ Public parameters of the existing scheme [WLC+08] depend on ID-space sizes due to the underlying Waters IBE [wat05]

Why is achieving (1) and (2) challenging? (more on this later)

- ➢ **Hierarchical IKE from any HIBE does not satisfy strong security**
- ➢ **Proof technique of Waters dual-system IBE [Wat09] does not work well**

Type-3 Pairing and SXDH Assumption

Type-3 Pairing (asymmetric pairing)

- ✓ $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- ✓ No efficiently computable isomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$ are known

SXDH Assumption [BBS04]

- ✓ **Decisional Diffie–Hellman (DDH) assumptions hold in $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively**
- ✓ **Advantage of $\mathcal{A}$ in the DDHi game ($i \in \{1,2\}$) is defined by:**

$$Adv(\lambda) := Pr\left[b' = b \;\middle|\; \begin{array}{c} D := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \leftarrow \mathcal{G} \\ c_1, c_2 \leftarrow \mathbb{Z}_p, b \leftarrow \{0,1\} \\ \text{if } b = 0 \text{ then } T := g_i^{c_1 c_2} \text{ else } T \leftarrow \mathbb{G}_i \\ b' \leftarrow \mathcal{A}(D, g_i^{c_1}, g_i^{c_2}, T) \end{array} \right].$$

Time-period Map Function [HHSI05]

✓ **Functions for *"several kinds of time-periods"*** $\mathcal{T}_0, \ldots, \mathcal{T}_{\ell-1}$

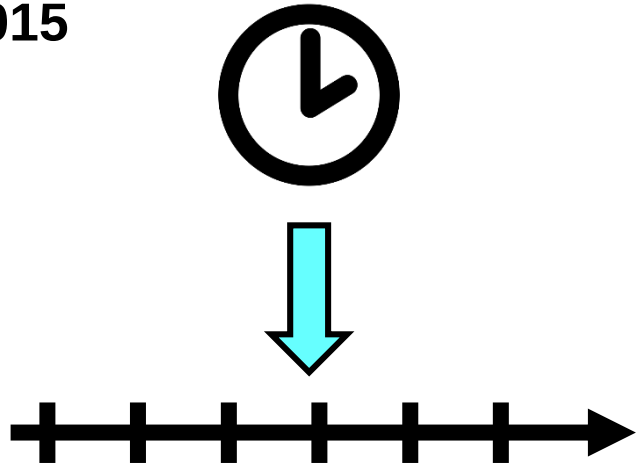
Example: $\ell = 4$, $\mathtt{time}$ **= 9:59 / 7th / Oct. / 2015**

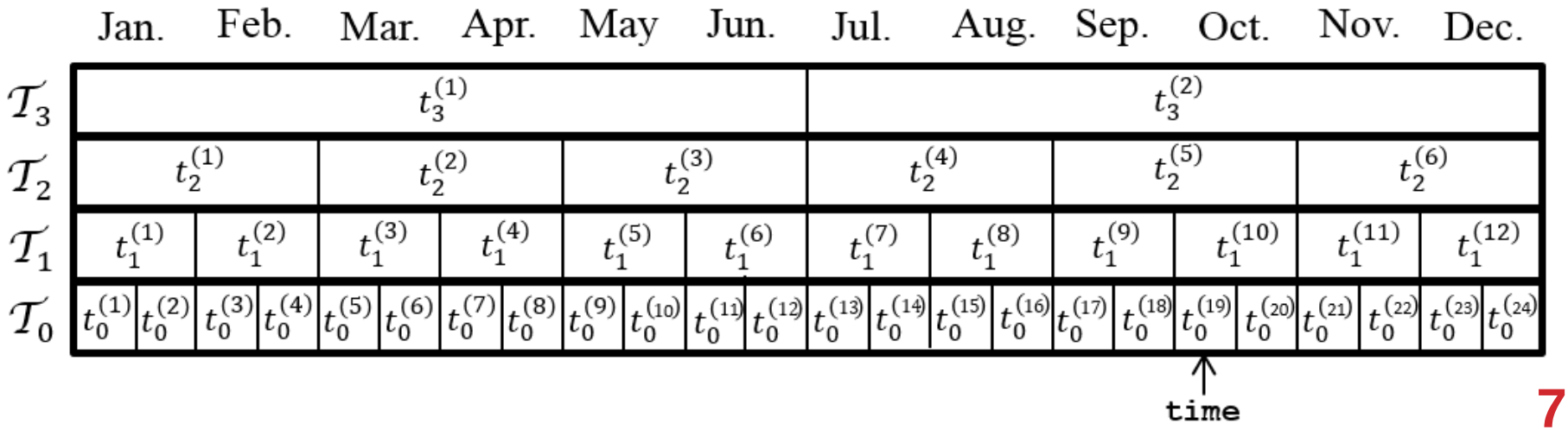
$\mathcal{T}_0(\mathtt{time}) = t_0^{(19)}$ **= 1st – 15th / Oct. / 2015,**

$\mathcal{T}_1(\mathtt{time}) = t_1^{(10)}$ **= Oct. / 2015,**

$\mathcal{T}_2(\mathtt{time}) = t_2^{(5)}$ **= Set. – Oct. / 2015,**

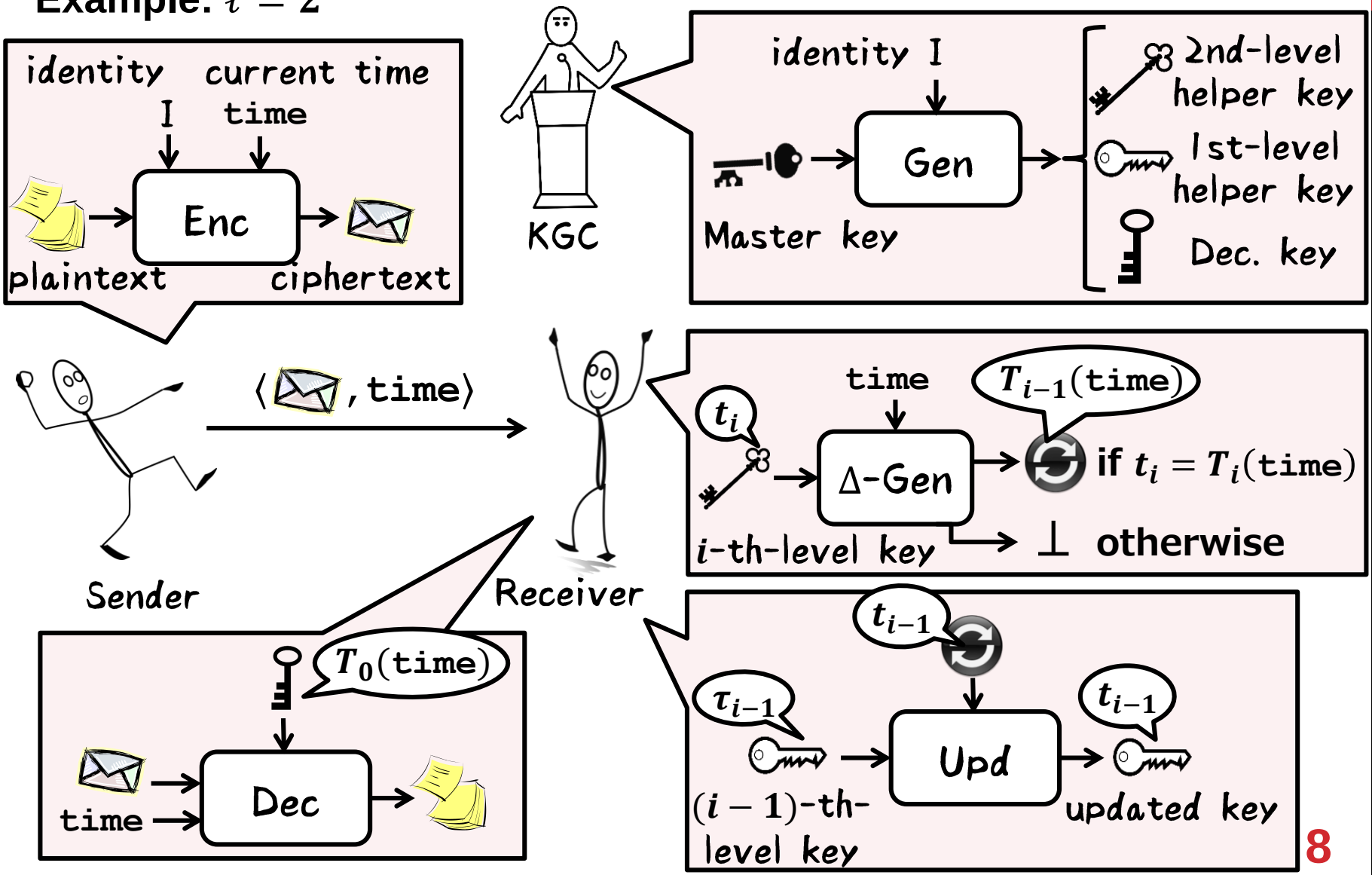
$\mathcal{T}_3(\mathtt{time}) = t_3^{(2)}$ **= Jul. – Dec. / 2015**





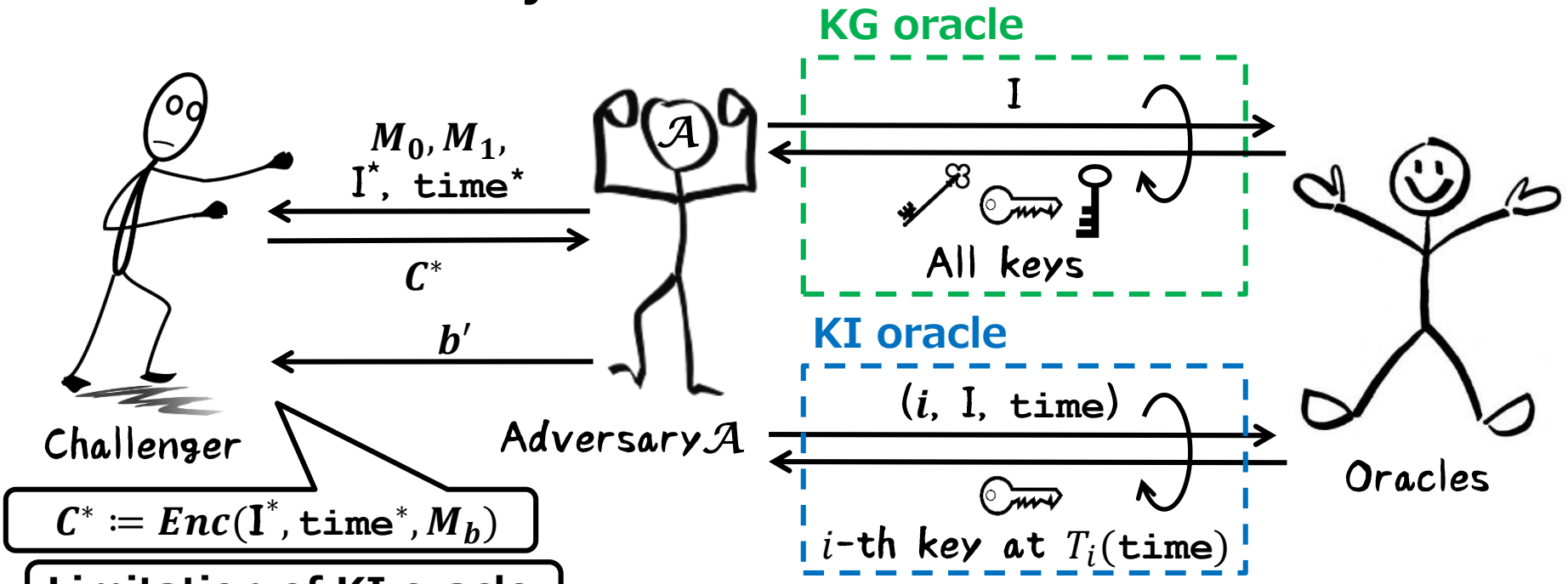
Hierarchical IKE: Model

Example: $\ell = 2$



Hierarchical IKE: Security

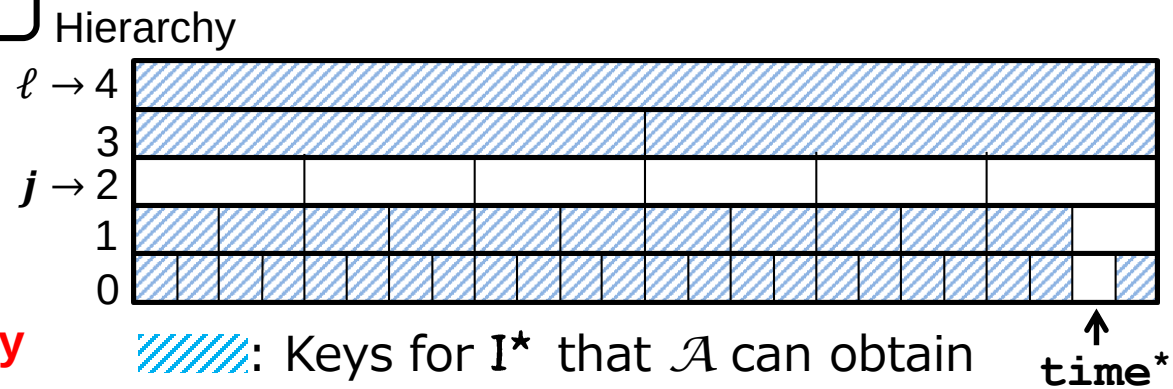
IND-KE-CPA security:



Limitation of KI oracle

$\mathcal{A}$ can issue any queries if there exists **at least one special level** $j \in \{0, \ldots, \ell\}$

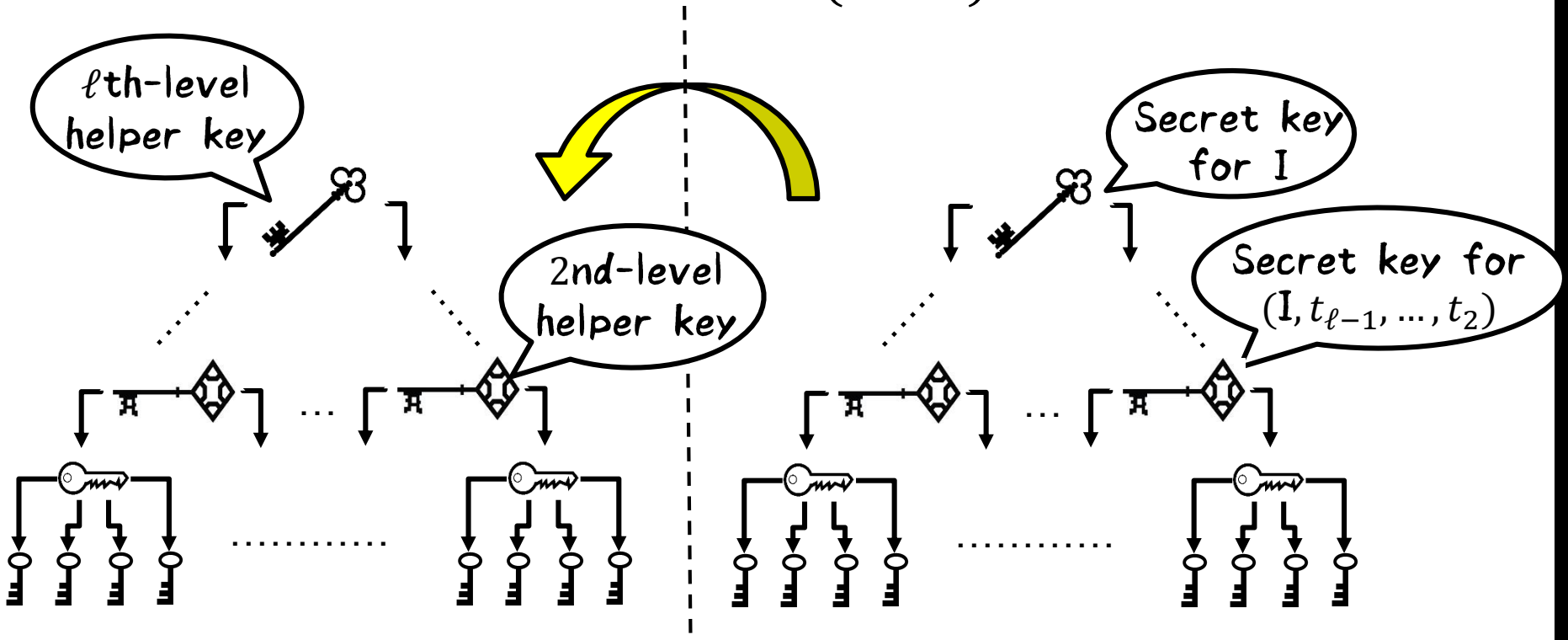
⇨ **include strong security**



Why Hierarchical IKE from HIBE is Insufficient

ℓ-level Hierarchical IKE

$(\ell + 1)$-level HIBE



If secret key for I is leaked, all other secret keys can be generated

⇒ the resulting scheme does not meet *strong* security

⇒ does not meet IND-KE-CPA security !

Why Waters' Technique Does Not Work

Waters dual system IBE [Wat09]

- Ciphertext ct contains $\boldsymbol{tag_C}$ and secret key sk_I contains $\boldsymbol{tag_K}$

Important proof technique:

Some pairwise independent function is embedded into the public parameter for cancelling values

- It raises $\boldsymbol{tag_C = tag_K}$ for the same identity $\mathbf{I}$
- However, **the proof works well** since it is enough to generate
  - Only $\boldsymbol{tag_K}$ for all identities $\mathbf{I} \neq \mathbf{I}^*$
  - Only $\boldsymbol{tag_C}$ for the target identity $\mathbf{I}^*$

On the other hand, in (hierarchical) IKE,

$\mathcal{A}$ can get secret keys for $\mathbf{I}^*$ (i.e. $\boldsymbol{tag_K}$) as well as for $\mathbf{I} \neq \mathbf{I}^*$

Waters' technique cannot seem to be applied !

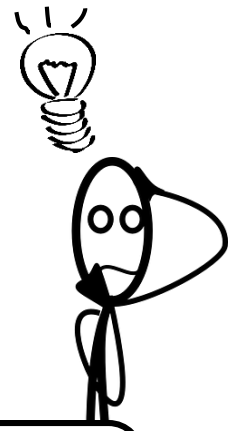
Why Jutla–Roy HIBE?

We can avoid such a collision problem!

✓ sk_I **does not contain any tag, though** ct **contains** tag

◆ **Jutla–Roy HIBE [JR13] and its variant [RS14]**

- ◆ Constant-size IBE (when $\ell = 1$)
- ◆ IND-ID-CPA security under the SXDH assumption
- ◆ Constant-size lowest-level key unlike **[Wat09,LW11]**
  - ➢ It leads to constant-size decryption key



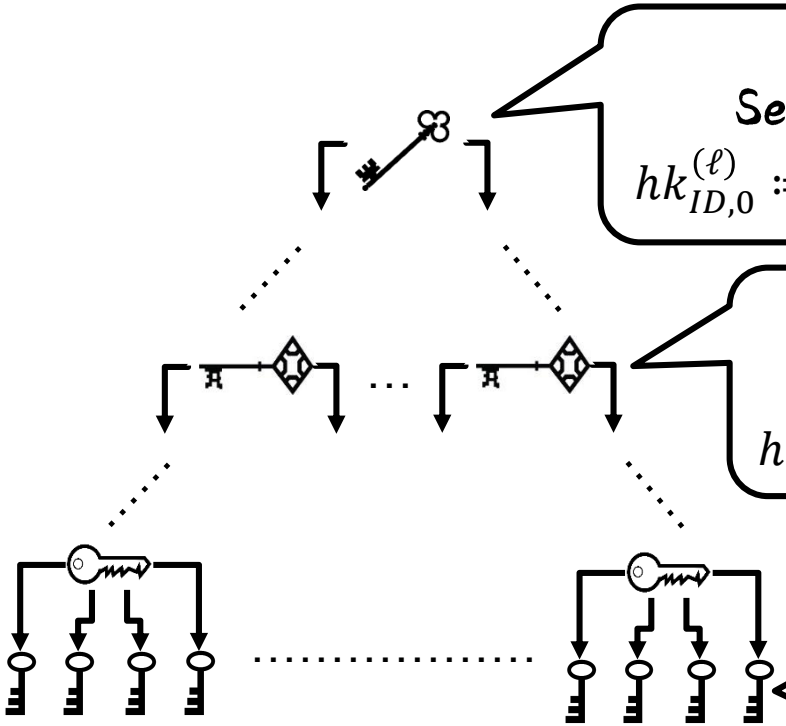
Remark

There might be other constant-size IBE schemes that can avoid the collision problem

Basic Idea of Our Construction

Specific $(\ell+1)$-level HIBE ($(\ell+1)$-level Jutla–Roy HIBE) +

(ℓ,ℓ)-secret sharing: secret B and shares β_i $(0 \le i \le \ell-1)$ s.t. $B = \sum_{i=0}^{\ell-1} \beta_i$



ℓ-th level helper key
Secret key for I + secret g^B
$hk_{ID,0}^{(\ell)} := (D_1, D_1', D_2, D_2', D_3 \cdot g^B, \{K_j, K_j'\}_{j=1}^{\ell-1})$

i-th level helper key
Secret key for $(I, t_{\ell-1}, \ldots, t_i)$ + $g^{-\beta_i}$
$hk_{ID,t_i}^{(i)} := (g^{-\beta_i}, D_1, D_1', D_2, D_2', D_3 \cdot g^{\sum_{j=0}^{i-1}\beta_j}, K_1, K_1')$

Decryption key
Secret key for $(ID, t_{\ell-1}, \ldots, t_0)$ + share $g^{-\beta_0}$
$dk_{ID,t_0} := (g^{-\beta_0}, D_1, D_1', D_2, D_2', D_3)$

All β_i are needed to generate correct decryption key $(D_1, D_1', D_2, D_2', D_3)$

Adversary cannot generate decryption key for I^* at time* !

Encryption and Decryption Procedure

$Enc(mpk, \mathrm{I}, \mathtt{time}, M)$:

$mpk := (z, g_1, g_1^{\alpha}, \{u_{1,j}\}_{j=0}^{\ell}, w_1, h_1, \dots)$

Choose $s, tag \leftarrow \mathbb{Z}_p$. Compute

$$C_0 := Mz^s, C_1 := g_1^s, C_2 := (g_1^{\alpha})^s, C_3 := \left(\prod_{j=0}^{\ell-1} \left(u_{1,j}^{t_j} \right) u_{1,\ell}^{\mathrm{I}} w_1^{tag} h_1 \right)^s,$$

where $t_j := T_j(\mathtt{time})$ $(0 \le j \le \ell - 1)$. Output $C := (C_0, C_1, C_2, C_3, tag)$.

$Dec(dk_{I,t_0}, \langle C, \mathtt{time} \rangle)$:

$dk_{I,t_0} := (R_0, D_1, D_1', D_2, D_2', D_3)$

$$M = \frac{C_0 \cdot e(C_3, D_3)}{e(C_1, D_1^{tag} D_1') e(C_2, D_2^{tag} D_2')}.$$

Parameter Evaluation and Comparison

$\#pp$	$\#dk$	$\#hk_i$	$\#C$	Enc. cost	Dec. cost
$(3\ell + 13)\|\mathbb{G}\|$	$6\|\mathbb{G}\|$	$(2i + 6)\|\mathbb{G}\|$	$4\|\mathbb{G}\| + \|\mathbb{Z}_p\|$	$[0,0,\ell + 4,1]$	$[3,0,2,0]$

$|\mathbb{G}|$: bit-length of a group element in $\mathbb{G}_1$, $\mathbb{G}_2$, or $\mathbb{G}_T$

$|\mathbb{Z}_p|$: bit-length of an element in $\mathbb{Z}_p$

$\#\boldsymbol{pp}, \#\boldsymbol{dk}, \#\boldsymbol{hk_i}, \#\boldsymbol{C}$: sizes of public parameter, dec. key, i-th helper key, and ciphertext

$[*,*,*,*]$: [pairing, multi-exp., regular-exp., fix-based-exp.]

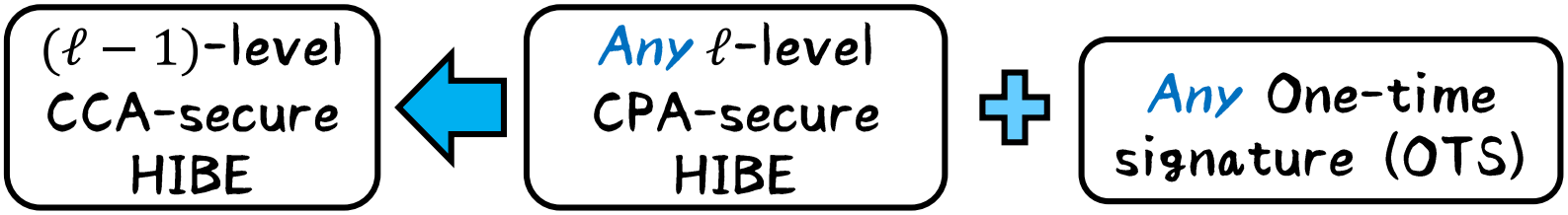
	$\#pp$	$\#dk$	$\#hk$	$\#C$	Enc. cost	Dec. cost	Assumption
HHSI05 $(\ell = 1)$	$\mathbf{2}\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	$\|\mathbb{G}\|$	$4\|\mathbb{G}\| + \|r\|$	$[1,0,2,1]$	$[4,0,2,1]$	**CBDH (in ROM)**
WLC+08 (threshold $t = 1$)	$(\mathbf{2n + 5})\|\mathbb{G}\|$	$4\|\mathbb{G}\|$	$2\|\mathbb{G}\|$	$4\|\mathbb{G}\|$	$[0,1,2,1]$	$[3,0,0,0]$	**DBDH**
Our scheme $(\ell = 1)$	$\mathbf{16}\|\mathbb{G}\|$	$6\|\mathbb{G}\|$	$7\|\mathbb{G}\|$	$4\|\mathbb{G}\| + \|\mathbb{Z}_p\|$	$[0,0,5,1]$	$[3,0,2,0]$	**SXDH**

$\boldsymbol{r}$: randomness that depends on the security parameter

$\boldsymbol{n}$: size of ID space (i.e., $\mathcal{I} \coloneqq \{0,1\}^n$)

CCA-secure Hierarchical IKE

An well-known transformation [CHK04,BCHK06] :



We cannot apply the transformation to a hierarchical IKE scheme in a generic way since it does not have delegating functionality:

However, by modifying the proposed hierarchical IKE scheme,
we can realize CCA-secure scheme based on the transformation:

Conclusion

We proposed ℓ-level hierarchical IKE scheme:

- **met strong security (IND-KE-CPA security) without ROM**
- **secure under the SXDH assumption, which is a simple, static one**
- **achieved constant-size parameters when $\ell = 1$**

We also showed CCA-secure scheme from

- **Proposed CPA-secure hierarchical IKE scheme; and**
- **Any one-time signature**