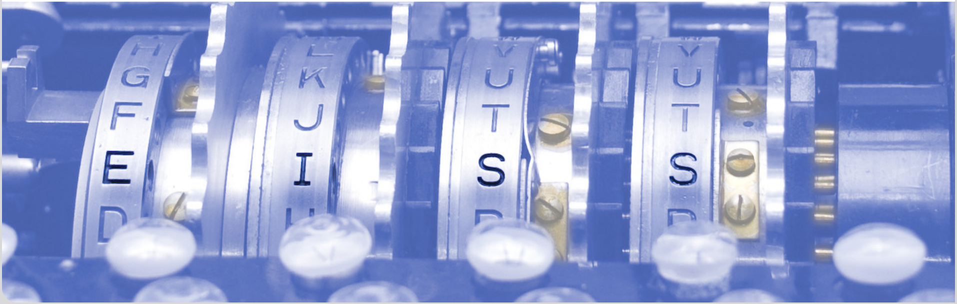
Karlsruhe Institute of Technology

Tightly secure hierarchical identity-based encryption

PKC 2019

Roman Langrehr and Jiaxin Pan

Department of Informatics, Institute of Theoretical Informatics



Our main construction

We construct the first HIBE with tight reduction in the standard model.

Scheme 1:

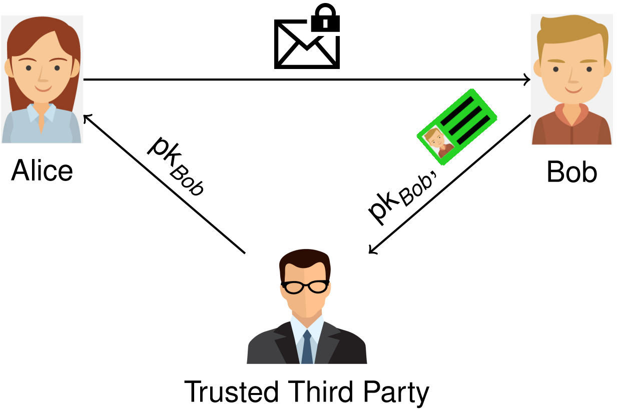
- ✓ $O(1)$ size ciphertexts
- ✗ longer user secret keys

Scheme 2:

- ✗ longer ciphertexts
- ✓ shorter user secret keys

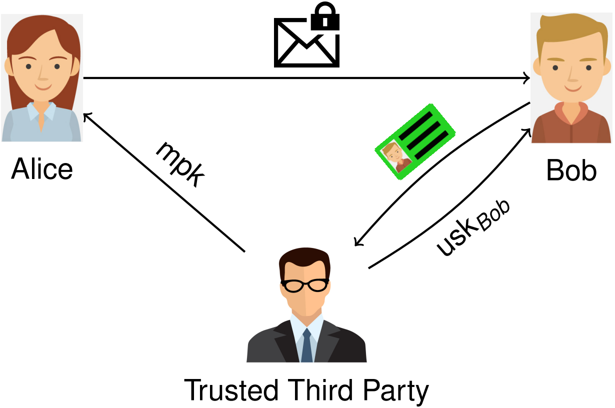
Outline

Public key encryption



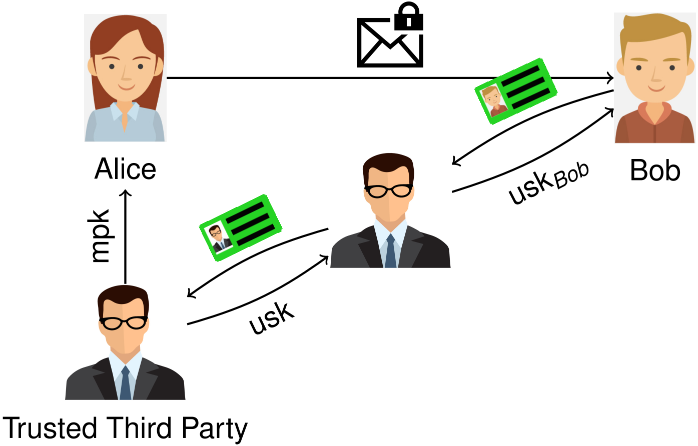
- Alice needs to obtain a public key for each member

Identity-based encryption



- Alice needs to obtain only the master public key
- Encryption with identities (e.g. e-mail address)

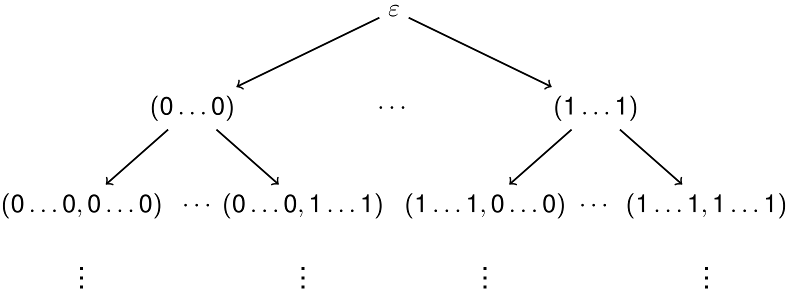
Hierarchical Identity-based encryption



- Hierarchy of key generators

Key delegation

Identities have the form $(\mathrm{id}_1, \ldots, \mathrm{id}_p)$.



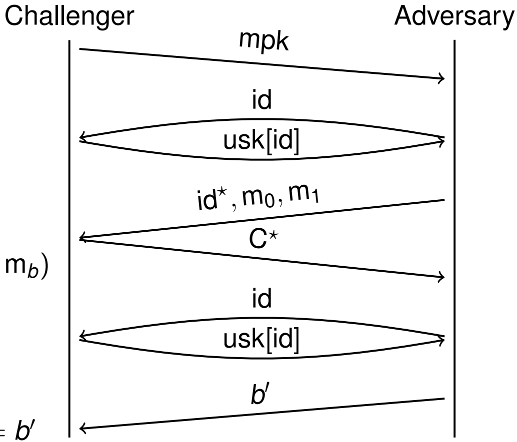
- Each user can generate keys for its children

Security game (IND-HID-CPA)

$b \xleftarrow{\$} \{0,1\}$

$C^\star \xleftarrow{\$} \mathrm{Enc}(\mathrm{mpk}, \mathrm{id}^\star, \mathrm{m}_b)$

$b = b'$



The adversary must not ask user secret keys for prefixes of $\mathrm{id}^\star$.

Tight security

Karlsruhe Institute of Technology

Scheme (e.g. HIBE)	Reduction →	Static assumption (e.g. Diffie Hellman)

Tight security

Scheme (e.g. HIBE)	—— Reduction ——→	Static assumption (e.g. Diffie Hellman)
Can be broken with probability ε using resources ρ.		Can be broken with probability ε/ℓ using resources ρ.

Tight security

Scheme (e.g. HIBE) —Reduction→ Static assumption (e.g. Diffie Hellman)

Scheme (e.g. HIBE)	Static assumption (e.g. Diffie Hellman)
Can be broken with probability ε using resources ρ.	Can be broken with probability ε/ℓ using resources ρ.

Security loss ℓ can depend on:

- scheme parameters
  - *L*: maximum hierarchy depth
  - α: bit length of identities
- λ: the security parameter
- the attacker's resources
  - *Q*: # user secret key queries

Larger security loss requires larger security parameter.

Tight security

Scheme (e.g. HIBE) —Reduction→ Static assumption (e.g. Diffie Hellman)

Can be broken with probability ε using resources ρ.

Can be broken with probability ε/ℓ using resources ρ.

Security loss ℓ can depend on:

- scheme parameters
  - L: maximum hierarchy depth
  - α: bit length of identities
- λ: the security parameter
- the attacker's resources
  - Q: # user secret key queries

Tight security:

- scheme parameters and λ: allowed
- the attacker's resources: not allowed

Larger security loss requires larger security parameter.

History: (H)IBE, tight security

Scheme	Hierarchical	Full Security	No ROM	Tight
[CW13], [BKP14],...	✗	✓	✓	✓
([BKP14])	✓	✗	✓	✓
[BBG05]	✓	✓	✗	(✓)
[Lew12], [BKP14],...	✓	✓	✓	✗
???	✓	✓	✓	✓

Recap of [BKP14]

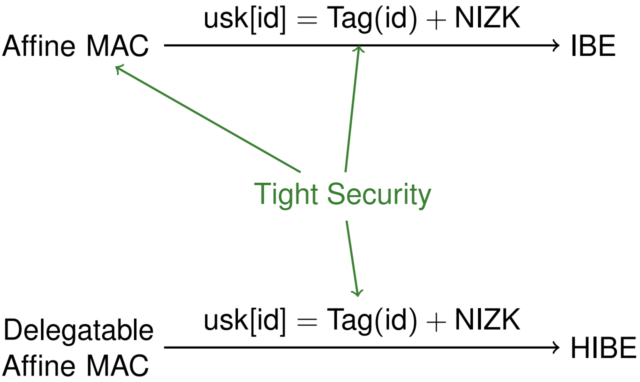
$$\text{Affine MAC} \xrightarrow{\mathsf{usk[id]} = \mathsf{Tag(id)} + \mathsf{NIZK}} \text{IBE}$$

Recap of [BKP14]

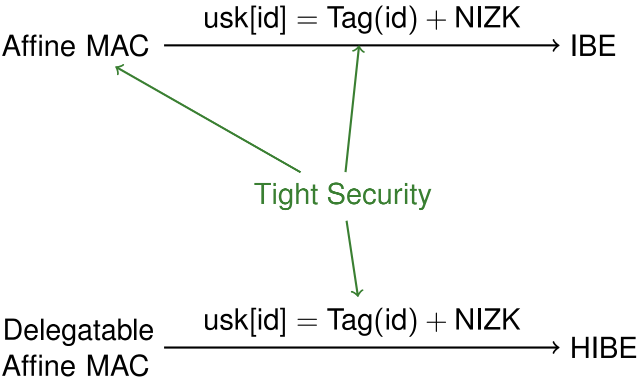
Affine MAC $\xrightarrow{\text{usk[id]} = \text{Tag(id)} + \text{NIZK}}$ IBE

Delegatable Affine MAC $\xrightarrow{\text{usk[id]} = \text{Tag(id)} + \text{NIZK}}$ HIBE

Recap of [BKP14]



Recap of [BKP14]



Problem: A Delegatable Affine MAC with tight security

Matrix Decisional Diffie-Hellman assumption

We assume prime order groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ with pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

Matrix Decisional Diffie-Hellman assumption

We assume prime order groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ with pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

Implicit Representation

$$[\mathbf{A}]_s := \begin{pmatrix} a_{1,1}\mathcal{P}_s & \dots & a_{1,m}\mathcal{P}_s \\ & \ddots & \\ a_{n,1}\mathcal{P}_s & \dots & a_{n,m}\mathcal{P}_s \end{pmatrix} \in \mathbb{G}_s^{n \times m},$$

where $s \in \{1, 2, T\}$.

Matrix Decisional Diffie-Hellman assumption

We assume prime order groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ with pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

Implicit Representation

$$[\mathbf{A}]_s := \begin{pmatrix} a_{1,1}\mathcal{P}_s & \dots & a_{1,m}\mathcal{P}_s \\ & \ddots & \\ a_{n,1}\mathcal{P}_s & \dots & a_{n,m}\mathcal{P}_s \end{pmatrix} \in \mathbb{G}_s^{n \times m},$$

where $s \in \{1, 2, T\}$.

$\mathcal{D}_k$-MDDH-assumption

$$([\mathbf{A}]_s, [\mathbf{Ar}]_s) \stackrel{c}{\approx} ([\mathbf{A}]_s, [\mathbf{w}]_s)$$

for $\mathbf{A} \stackrel{\$}{\leftarrow} \mathcal{D}_k \subset \mathbb{Z}_q^{n \times k}$ for $k < n$, $\mathbf{r} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^k$ and $\mathbf{w} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n$

[BKP14]: Affine MACs

- $\mathsf{Gen}_{\mathsf{MAC}}(1^\lambda)$:

$$\mathsf{sk} := \left(\mathbf{B}, \mathbf{x}_1, \ldots, \mathbf{x}_\ell, x_0' \right)$$

matrix distribution

uniform random

[BKP14]: Affine MACs

- Tag($sk_{MAC}, m \in \mathcal{S}$): ($[\mathbf{t}]_2, [u]_2$) with

$$\mathbf{t} = \mathbf{B}\,\mathbf{s}$$

matrix distribution

uniform random

pseudorandom

$$u = \sum_i f_i(m)\,\mathbf{x}_i^\top\,\mathbf{t} + x_0' \qquad (1)$$

Public functions $f_i : \mathcal{M} \to \mathbb{Z}_q$ define different concrete MACs.

[BKP14]: Affine MACs

Karlsruhe Institute of Technology

- $\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S})$: $([\mathbf{t}]_2, [u]_2)$ with

matrix distribution

uniform random

pseudorandom

$$\mathbf{t} = \mathbf{B}\mathbf{s}$$

$$u = \sum_i f_i(\mathsf{m})\, \mathbf{x}_i^\top \mathbf{t} + x_0' \qquad (1)$$

Public functions $f_i : \mathcal{M} \to \mathbb{Z}_q$ define different concrete MACs.

- $\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}, \tau = ([\mathbf{t}]_2, [u]_2))$ checks eq. (1).

[BKP14]: Delegatable Affine MACs

- Public values:

$$\left([\mathbf{B}]_2 , [\mathbf{B}^\top \mathbf{x}_1]_2 , \ldots , [\mathbf{B}^\top \mathbf{x}_\ell]_2 \right)$$

  Necessary for key delegation
- Flexible-length messages $m \in \mathcal{S}^{\leq L}$

Security of Affine MACs

- Security requirement: $[u_{\mathsf{m}}]_2$ is indistinguishable from a random value for m with fixed length.

Security of Affine MACs

- Security requirement: $[u_{\mathrm{m}}]_2$ is indistinguishable from a random value for m with fixed length.

$\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ in [BKP14] achieves this with a tight bit-by-bit randomization:

Proof idea in [BKP14]

- $x'_0 = \mathsf{RF}_0(\varepsilon)$
- $\mathsf{RF}_i(\mathrm{m}_{|i}) \overset{c}{\approx} \mathsf{RF}_{i+1}(\mathrm{m}_{|i+1})$ via

$$\mathsf{RF}_{i+1}(\mathrm{m}_{|i+1}) := \begin{cases} \mathsf{RF}_i(\mathrm{m}_{|i}) & \text{if } \mathrm{m}_{i+1} = 0 \\ \mathsf{RF}_i(\mathrm{m}_{|i}) + \mathsf{RF}'_i(\mathrm{m}_{|i}) & \text{if } \mathrm{m}_{i+1} = 1 \end{cases}$$

Security of Delegatable Affine MACs

- Security requirement: $[u_{\mathsf{m}}]_2$ is indistinguishable from a random value for m with flexible length.

Security of Delegatable Affine MACs

- Security requirement: $[u_{\mathsf{m}}]_2$ is indistinguishable from a random value for m with flexible length.

The problem with bit-by-bit randomization

- $x'_0 = \mathsf{RF}_0(\varepsilon)$
- $\mathsf{RF}_i(\mathsf{m}_{|i}) \overset{c}{\approx} \mathsf{RF}_{i+1}(\mathsf{m}_{|i+1})$ via

$$\mathsf{RF}_{i+1}(\mathsf{m}_{|i+1}) := \begin{cases} \mathsf{RF}_i(\mathsf{m}_{|i}) & \boxed{\text{if } \mathsf{m}_{i+1} \in \{0, \perp\}} \\ \mathsf{RF}_i(\mathsf{m}_{|i}) + \mathsf{RF}'_i(\mathsf{m}_{|i}) & \text{if } \mathsf{m}_{i+1} = 1 \end{cases}$$

Security of Delegatable Affine MACs

Karlsruhe Institute of Technology

- Security requirement: $[u_\mathsf{m}]_2$ is indistinguishable from a random value for m with flexible length.

The problem with bit-by-bit randomization

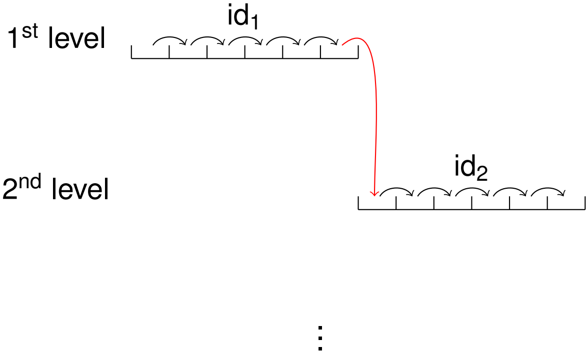
- $x_0' = \mathsf{RF}_0(\varepsilon)$
- $\mathsf{RF}_i(\mathsf{m}_{|i}) \overset{c}{\approx} \mathsf{RF}_{i+1}(\mathsf{m}_{|i+1})$ via

$$\mathsf{RF}_{i+1}(\mathsf{m}_{|i+1}) := \begin{cases} \mathsf{RF}_i(\mathsf{m}_{|i}) & \boxed{\text{if } \mathsf{m}_{i+1} \in \{0, \perp\}} \\ \mathsf{RF}_i(\mathsf{m}_{|i}) + \mathsf{RF}_i'(\mathsf{m}_{|i}) & \text{if } \mathsf{m}_{i+1} = 1 \end{cases}$$

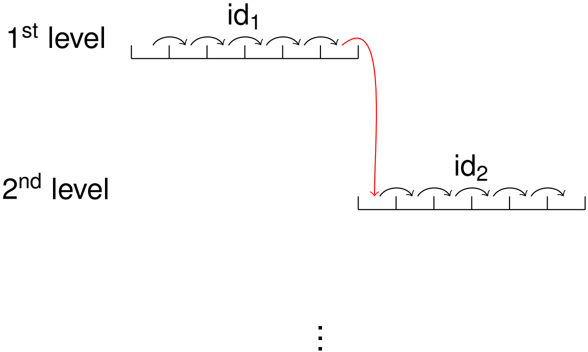
Example

$$\mathsf{RF}_{|\mathsf{id}_1|+1}(\mathsf{id}_1) = \mathsf{RF}_{|\mathsf{id}_1|+1}(\mathsf{id}_1, 0) \quad ↯$$

$\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ in the hierarchical setting

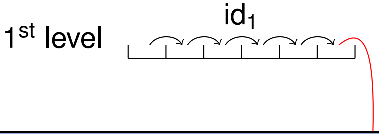


$\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ in the hierarchical setting



How can we randomize messages with flexible length?

$\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ in the hierarchical setting



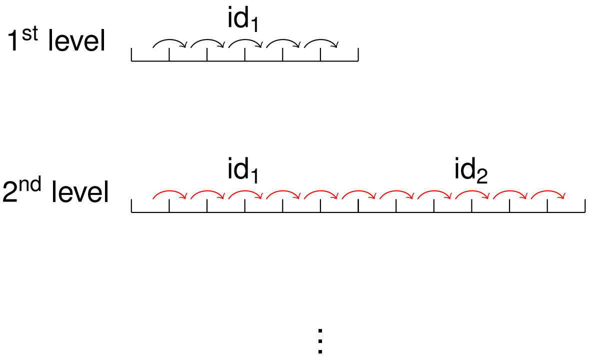
Solution: Independent randomization of each level

$\vdots$

How can we randomize messages with flexible length?

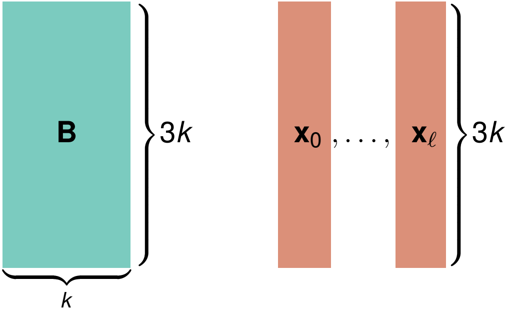
Our new MACs

Solution: Independent randomization of each level



Our new MACs

Randomization technique based on [GHKW16]:

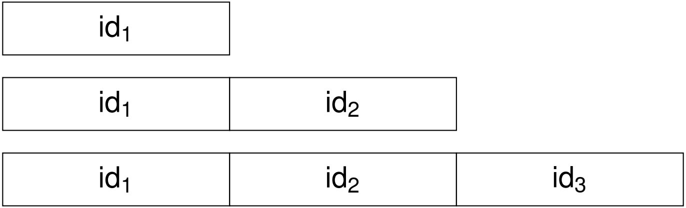


k dimensions are public

$2k$ dimensions are used for randomization

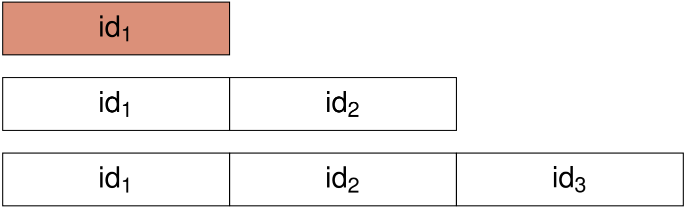
Construction 1

Randomize levels successively



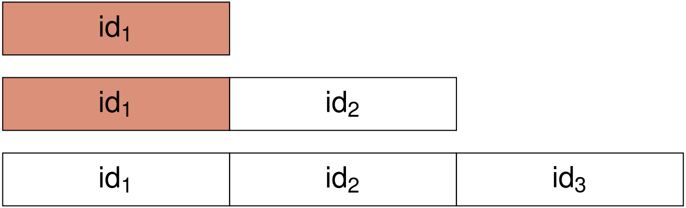
Construction 1

Randomize levels successively



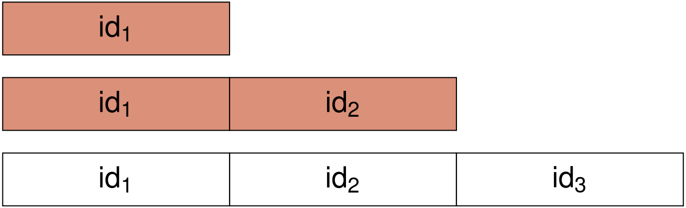
Construction 1

Randomize levels successively



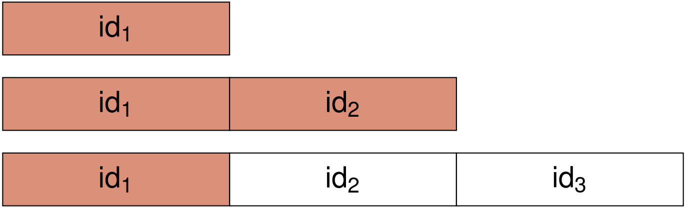
Construction 1

Randomize levels successively



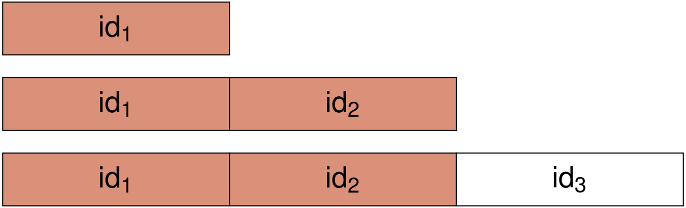
Construction 1

Randomize levels successively



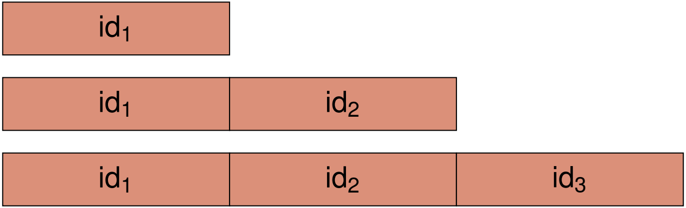
Construction 1

Randomize levels successively



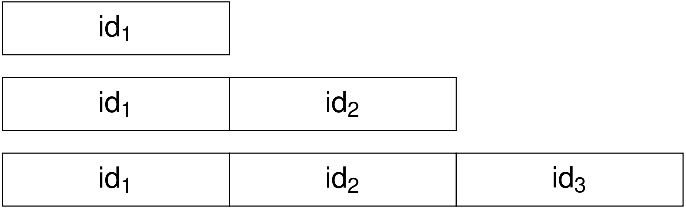
Construction 1

Randomize levels successively



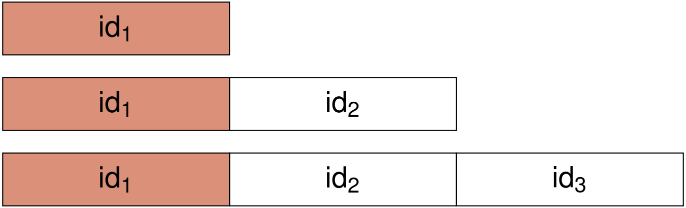
Construction 2

Randomize levels simultaneously



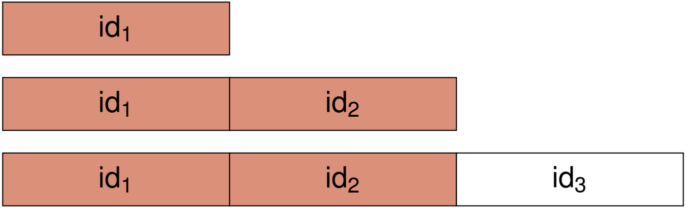
Construction 2

Randomize levels simultaneously



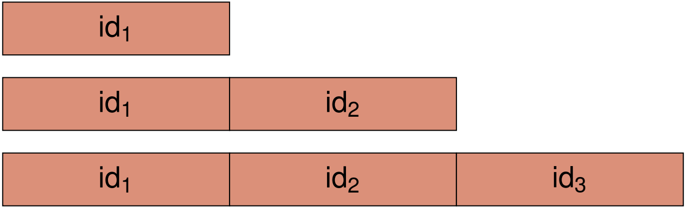
Construction 2

Randomize levels simultaneously



Construction 2

Randomize levels simultaneously



Our new MAC

Construction 1:

- Randomize levels successively
  - $\Rightarrow$ Security loss $O(\alpha L^2)$
- Constant size ciphertexts
- Uses the same **t** on all levels

Construction 2:

- Randomize levels simultaneously
  - $\Rightarrow$ Security loss $O(\alpha L)$
- $O(L)$ size ciphertexts
- Requires different values for **t** on each level
- Requires a generalization of the [BKP14] transformation

Overview of HIBE schemes

with full security and without random oracles.

Scheme	$\lvert mpk\rvert$	$\lvert usk\rvert$	$\lvert C\rvert$	Loss	Assumption
[Wat05]	$O(\alpha L)$	$O(\alpha L)$	$O(L)$	$O(\alpha Q)^L$	DBDH
[Wat09]	$O(L)$	$O(L)$	$O(L)$	$O(Q)$	2-LIN
[Lew12]	$O(1)$	$O(L)$	$O(L)$	$O(Q)$	2-LIN
[CW13]	$O(Lk^2)$	$O(Lk)$	$O(k)$	$O(Q)$	k-LIN
[BKP14]	$O(Lk^2)$	$O(Lk)$	$O(k)$	$O(Q)$	k-LIN
[GCTC16]	$O(1)$	$O(L)$	$O(L)$	$O(Q)$	SXDH
Ours (v. 1)	$O(\alpha L^2)$	$O(\alpha L^2)$	$O(1)$	$O(\alpha L^2)$	SXDH
Ours (v. 2)	$O(\alpha L^2)$	$O(L)$	$O(L)$	$O(\alpha L)$	SXDH

$\lvert mpk\rvert$, $\lvert usk\rvert$, $\lvert C\rvert$ are in number of group elements

- L: maximum hierarchy depth
- α: bit length of identities
- Q: # user secret key queries

Summary

- First tightly secure HIBE schemes in standard model
  - based on MDDH (e.g. SXDH or k-LIN) assumption

Core idea

New randomization technique for flexible length identities

Summary

Karlsruhe Institute of Technology

- First tightly secure HIBE schemes in standard model
  - based on MDDH (e.g. SXDH or k-LIN) assumption

Core idea

New randomization technique for flexible length identities

Implications

- tightly CCA-secure (H)IBE (via the CHK transformation using one-time signatures) and

Summary

- First tightly secure HIBE schemes in standard model
  - based on MDDH (e.g. SXDH or k-LIN) assumption

Core idea

New randomization technique for flexible length identities

Implications

- tightly CCA-secure (H)IBE (via the CHK transformation using one-time signatures) and
- the first tightly secure (hierarchical) identity-based signature scheme (via the Naor transformation).

Open Problems

Karlsruhe Institute of Technology

- Tight security in multi instance, multi challenge setting?
- Shorter public parameters?

References I

Dan Boneh, Xavier Boyen, and Eu-Jin Goh.
Hierarchical identity based encryption with constant size ciphertext.
In Ronald Cramer, editor, EUROCRYPT 2005, volume 3494 of LNCS, pages 440–456. Springer, Heidelberg, May 2005.

Olivier Blazy, Eike Kiltz, and Jiaxin Pan.
(Hierarchical) identity-based encryption from affine message authentication.
In Juan A. Garay and Rosario Gennaro, editors, CRYPTO 2014, Part I, volume 8616 of LNCS, pages 408–425. Springer, Heidelberg, August 2014.

References II

Jie Chen and Hoeteck Wee.
Fully, (almost) tightly secure IBE and dual system groups.
In Ran Canetti and Juan A. Garay, editors, CRYPTO 2013, Part II, volume 8043 of LNCS, pages 435–460. Springer, Heidelberg, August 2013.

Junqing Gong, Zhenfu Cao, Shaohua Tang, and Jie Chen.
Extended dual system group and shorter unbounded hierarchical identity based encryption.
Designs, Codes and Cryptography, 80(3):525–559, Sep 2016.

References III

- Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee.
  Tightly CCA-secure encryption without pairings.
  In Marc Fischlin and Jean-Sébastien Coron, editors, EUROCRYPT 2016, Part I, volume 9665 of LNCS, pages 1–27. Springer, Heidelberg, May 2016.
- Allison B. Lewko.
  Tools for simulating features of composite order bilinear groups in the prime order setting.
  In David Pointcheval and Thomas Johansson, editors, EUROCRYPT 2012, volume 7237 of LNCS, pages 318–335. Springer, Heidelberg, April 2012.

References IV

- Brent R. Waters.
  Efficient identity-based encryption without random oracles.
  In Ronald Cramer, editor, EUROCRYPT 2005, volume 3494 of LNCS, pages 114–127. Springer, Heidelberg, May 2005.
- Brent Waters.
  Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions.
  In Shai Halevi, editor, CRYPTO 2009, volume 5677 of LNCS, pages 619–636. Springer, Heidelberg, August 2009.

Pictures

Alice, Bob, Trusted Party: freepik.com
Encrypted Mail: Icon made by SimpleIcon from www.flaticon.com