Unbounded HIBE with Tight Security

Roman Langrehr	ETH Zurich (Switzerland), Part of the work done at KIT (Karlsruhe, Germany)
Jiaxin Pan	NTNU (Trondheim, Norway)

Outline

Unbounded HIBE

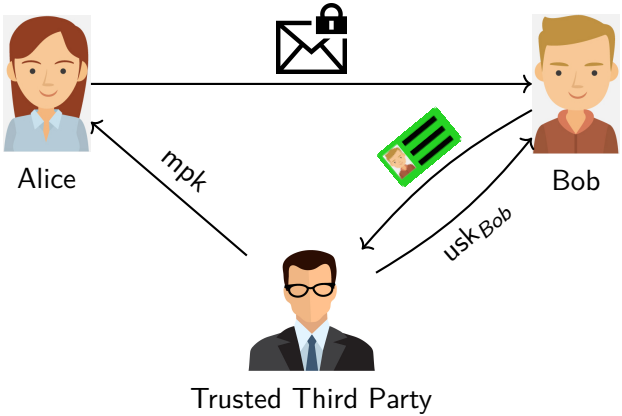
Tight security

Related works

Technical overview

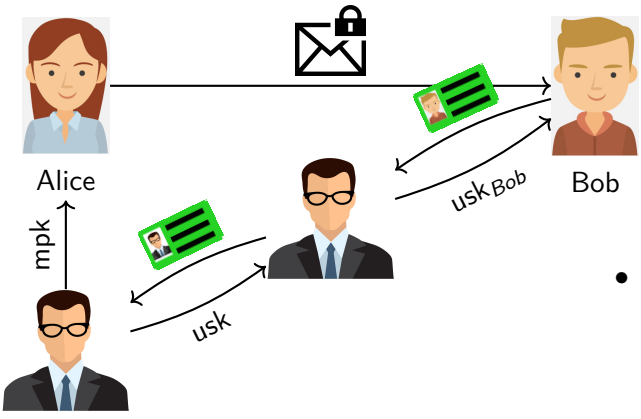
Future work

Identity-based encryption



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

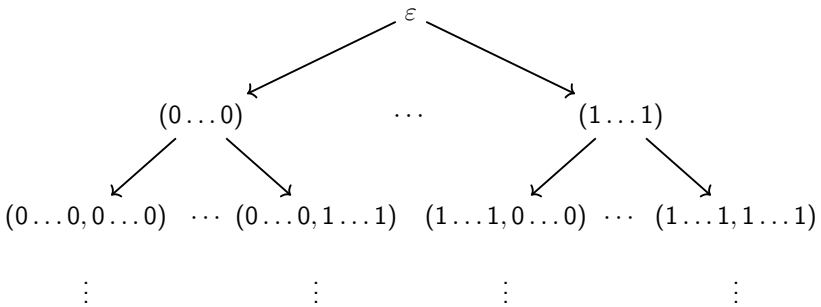
Hierarchical Identity-based encryption



- Hierarchy of key generators

Key delegation

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



- Each user can generate keys for its children

(Un)bounded HIBE

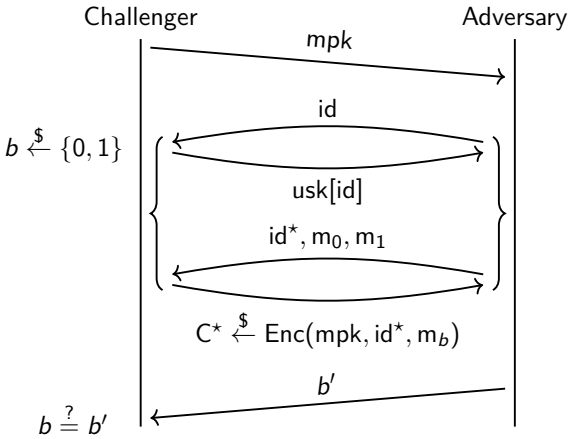
(Bounded) HIBE: Hierarchy depth L is fixed in advance

- mpk grows with L
- usks have a delegation term

Unbounded HIBE: No limit on the hierarchy depth

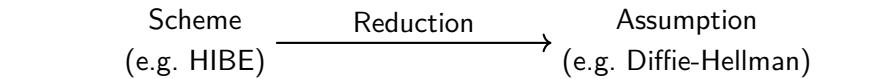
- More flexibility
- Better scalability

Security game (IND-HID-CPA)



- The adversary must not ask user secret keys for prefixes of challenge identities ($\mathsf{id}^\star$).
- IND-HID-CCA is easy once you have IND-HID-CPA.
- Master-key KDM-security can be achieved with [GGH20].

Tight security



Larger security loss requires larger security parameter.
Security loss ℓ can depend on:

- scheme parameters
- λ: the security parameter
- the attacker's resources (e.g. # user secret key queries Q_k or # challenge ciphertext queries Q_c, hierarchy depth L)

Tight security:

} allowed

} not allowed

History: Unbounded HIBE

Unbounded HIBEs:

[LW11]	CPG	$\mathcal{O}(Q_k L)$ (single-challenge)
[Lew12], [GCTC16]	PPG	$\mathcal{O}(Q_k L)$ (single-challenge)
[OT12] (weakly unbounded)	PPG	$\mathcal{O}(Q_k L^2)$ (single-challenge)
This work	PPG	$\mathcal{O}(\gamma)$ (multi-challenge)

- Q_k: # user secret key queries
- L: maximum hierarchy depth
- γ: Output bit length of a CRHF

History: Tight (H)IBE

Tight IBEs in prime-order pairing groups:

[CW13], [BKP14]	$\mathcal{O}(n)$ (single-challenge)
[AHY15], [GCD+16], [GDCC16], [HJP18]	$\mathcal{O}(n)$ (multi-challenge)

- n: Bit-length of the identities

Tight HIBEs in prime-order pairing groups:

[LP19]	$\mathcal{O}(\gamma)$ (single-challenge)
[LP20]	$\mathcal{O}(\gamma L)$ (multi-challenge)

- γ: Output bit length of a CRHF

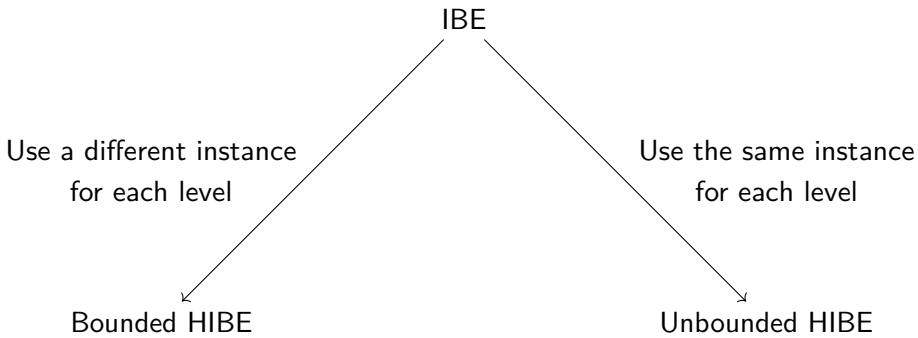
The gap

Scheme	|mpk|	|usk|	|C|	Loss	MC	Assumption
[LP20]	$\mathcal{O}(\gamma L L)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(\gamma L L)$	✓	SXDH

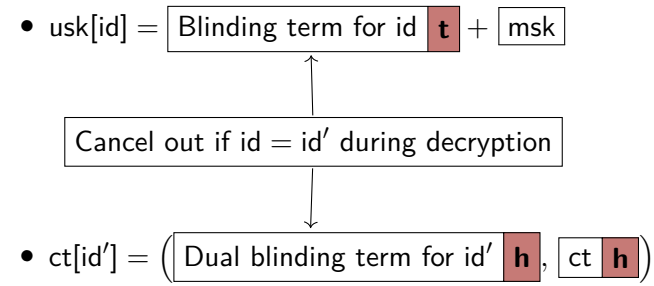
- L: maximum hierarchy depth
- p: actual hierarchy depth
- γ: bit-length of hashes

- We need to get rid of the factor L in $|\mathsf{mpk}|$ and in the security loss.

High-Level approach



IBE structure



Blinding terms

- Blinding term for x **t** $\cdot$ Dual blinding term for x **h** $= 0$
- Blinding term for x **t** is pseudorandom
  - If no dual blinding term for x is known
- Blinding terms are publicly sample
  - Dual blinding terms are not publicly sample
- Tight realization: Abstraction of [LP20]

Generalisation to Bounded HIBE

- $\mathsf{usk}[\mathsf{id}_1, \ldots, \mathsf{id}_p] = \sum_{i=1}^{p} \boxed{\text{Level } i \text{ blinding term for } H(\mathsf{id}_1 || \cdots || \mathsf{id}_i) \; \mathbf{t}_i} + \boxed{\mathsf{msk}}$
- Delegation: Blinding terms are publicly sampable
- $\mathsf{ct}[\mathsf{id}'_1, \ldots, \mathsf{id}'_{p'}] = \left(\left(\boxed{\text{Dual level } i \text{ blinding term for } H(\mathsf{id}'_1 || \cdots || \mathsf{id}'_i) \; \mathbf{h}} \right)_{1 \le i \le p'}, \boxed{\mathsf{ct} \; \mathbf{h}} \right)$

  Obstacles for Unbounded HIBE:

- mpk has size $\mathcal{O}(nL^2)$
  (n: bit-length of the identities)
  - Use a collision-resistant hash function H
- mpk has size $\mathcal{O}(\gamma L)$
  - Can we use the same blinding terms for all levels?

    $\Rightarrow$ We need individual randomness on the dual blinding terms

Unbounded HIBE

- $\mathsf{usk}[\mathsf{id}_1, \ldots, \mathsf{id}_p] = \Bigg(\sum_{i=1}^{p} \boxed{\text{Blinding term for “2”}\ \tilde{\mathbf{t}}_i} + \boxed{\mathsf{msk}},$

  $\Big(\boxed{\text{Blinding term for } H(\mathsf{id}_1 || \cdots || \mathsf{id}_i)\ \mathbf{t}_i} + \boxed{\text{Blinding term for “1”}\ \tilde{\mathbf{t}}_i} \Big)_{1 \le i \le p} \Bigg)$

- $\mathsf{ct}[\mathsf{id}'_1, \ldots, \mathsf{id}'_{p'}] = \Bigg(\Big(\boxed{\text{Dual blinding term for } H(\mathsf{id}'_1 || \cdots || \mathsf{id}'_i)\ \mathbf{h}_i},$

  $\boxed{\text{Dual blinding term for “1”}\ \mathbf{h}_i} + \boxed{\text{Dual blinding term for “2”}\ \tilde{\mathbf{h}}} \Big)_{1 \le i \le p'}, \boxed{\mathsf{ct}\ \tilde{\mathbf{h}}} \Bigg)$

Comparison of unbounded HIBEs (in prime-order pairing groups)

Scheme	|mpk|	|usk|	|C|	Loss	MC	Assumption
[Lew12]	$\mathcal{O}(1)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(Q_k)$	✗	2-LIN
[OT12]	$\mathcal{O}(1)$	$\mathcal{O}(p^2 L)$	$\mathcal{O}(p)$	$\mathcal{O}(Q_k L^2)$	✗	2-LIN
[GCTC16]	$\mathcal{O}(1)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(Q_k)$	✗	SXDH
Ours	$\mathcal{O}(\gamma)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(\gamma)$	✓	SXDH

- L: maximum hierarchy depth
- p: actual hierarchy depth
- γ: bit-length of hashes
- Q_k: # user secret key queries

[GGH20] Tight MC secure (IBE) $\Longrightarrow$ master-key KDM-secure (IBE)

- Same idea applies here $\Longrightarrow$ First unbounded HIBE with master-key KDM security

Future work

- Does the "inject-and-pack" strategy work in a more general setting, like predicate encryption?
- Can we have Unbounded HIBE with constant usk/ct size?

References I

Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada.
A framework for identity-based encryption with almost tight security.
In Tetsu Iwata and Jung Hee Cheon, editors, ASIACRYPT 2015, Part I, volume 9452 of LNCS, pages 521–549. Springer, Heidelberg, November / December 2015. doi:10.1007/978-3-662-48797-6_22.

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. doi:10.1007/978-3-662-44371-2_23.

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.
doi:10.1007/978-3-642-40084-1_25.


Junqing Gong, Jie Chen, Xiaolei Dong, Zhenfu Cao, and Shaohua Tang.
Extended nested dual system groups, revisited.
In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, PKC 2016, Part I, volume 9614 of LNCS, pages 133–163. Springer, Heidelberg, March 2016.
doi:10.1007/978-3-662-49384-7_6.

References III


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.
doi:10.1007/s10623-015-0117-z.


Junqing Gong, Xiaolei Dong, Jie Chen, and Zhenfu Cao.
Efficient IBE with tight reduction to standard assumption in the multi-challenge setting.
In Jung Hee Cheon and Tsuyoshi Takagi, editors, ASIACRYPT 2016, Part II, volume 10032 of LNCS, pages 624–654. Springer, Heidelberg, December 2016.
doi:10.1007/978-3-662-53890-6_21.

References IV


Sanjam Garg, Romain Gay, and Mohammad Hajiabadi.
Master-key KDM-secure IBE from pairings.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, PKC 2020, Part I, volume 12110 of LNCS, pages 123–152. Springer, Heidelberg, May 2020.
doi:10.1007/978-3-030-45374-9_5.


Dennis Hofheinz, Dingding Jia, and Jiaxin Pan.
Identity-based encryption tightly secure under chosen-ciphertext attacks.
In Thomas Peyrin and Steven Galbraith, editors, ASIACRYPT 2018, Part II, volume 11273 of LNCS, pages 190–220. Springer, Heidelberg, December 2018.
doi:10.1007/978-3-030-03329-3_7.

References V

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.

doi:10.1007/978-3-642-29011-4_20.

Roman Langrehr and Jiaxin Pan.

Tightly secure hierarchical identity-based encryption.

In Dongdai Lin and Kazue Sako, editors, PKC 2019, Part I, volume 11442 of LNCS, pages 436–465. Springer, Heidelberg, April 2019.

doi:10.1007/978-3-030-17253-4_15.

References VI


Roman Langrehr and Jiaxin Pan.
Hierarchical identity-based encryption with tight multi-challenge security.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, PKC 2020, Part I, volume 12110 of LNCS, pages 153–183. Springer, Heidelberg, May 2020.
doi:10.1007/978-3-030-45374-9_6.


Allison B. Lewko and Brent Waters.
Unbounded HIBE and attribute-based encryption.
In Kenneth G. Paterson, editor, EUROCRYPT 2011, volume 6632 of LNCS, pages 547–567. Springer, Heidelberg, May 2011.
doi:10.1007/978-3-642-20465-4_30.

References VII


Tatsuaki Okamoto and Katsuyuki Takashima.
Fully secure unbounded inner-product and attribute-based encryption.
In Xiaoyun Wang and Kazue Sako, editors, ASIACRYPT 2012, volume 7658 of LNCS, pages 349–366. Springer, Heidelberg, December 2012.
doi:10.1007/978-3-642-34961-4_22.

Pictures

Alice, Bob, Trusted Party: freepik.com

Encrypted Mail: Icon made by SimpleIcon from www.flaticon.com