HIBE with Tight Multi-challenge Security

Roman Langrehr ETH Zurich (Switzerland), Part of the work done at KIT (Karlsruhe, Germany)

Jiaxin Pan NTNU (Trondheim, Norway)

Outline

(H)IBE

Tight multi-challenge security

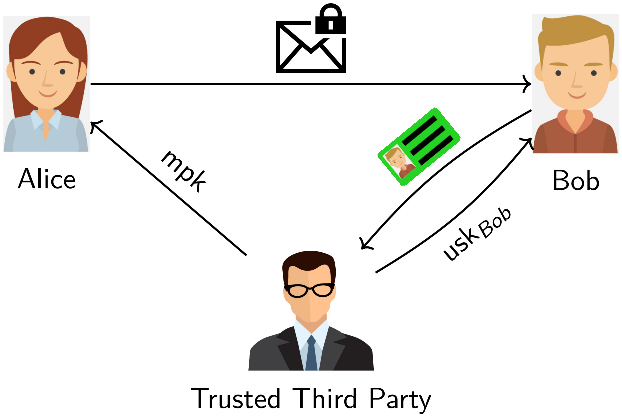
Related works

The difficulty

Our solution

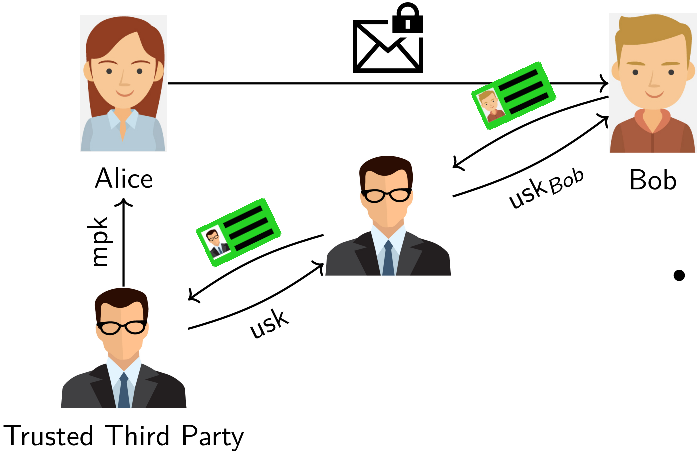
Future work

Identity-based encryption



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

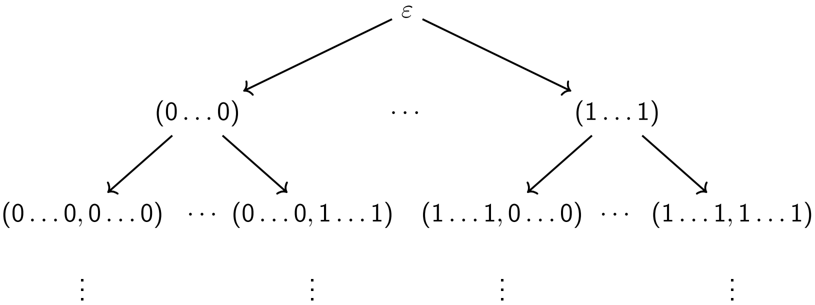
Hierarchical Identity-based encryption



- Hierarchy of key generators

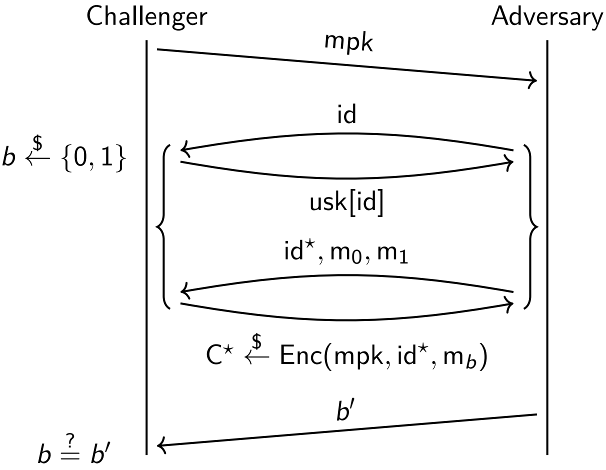
Key delegation

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



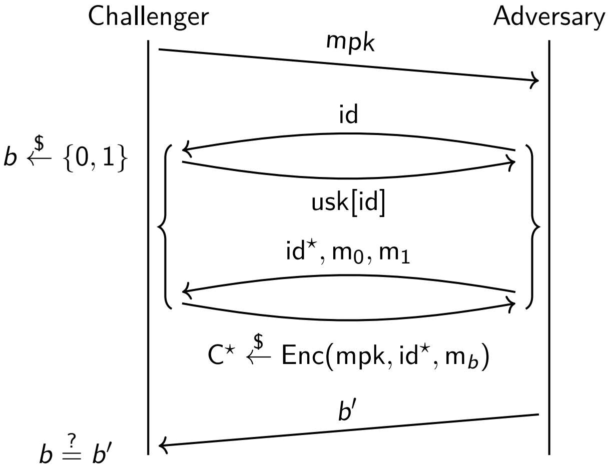
- Each user can generate keys for its children

Security game (IND-HID-CPA)



- The adversary must not ask user secret keys for prefixes of challenge identities ($\mathsf{id}^\star$).

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.

Tight security

$$\begin{array}{ccc} \text{Scheme} & \xrightarrow{\text{Reduction}} & \text{Assumption} \\ \text{(e.g. HIBE)} & & \text{(e.g. Diffie-Hellman)} \end{array}$$

Tight security

Scheme (e.g. HIBE) $\xrightarrow{\text{Reduction}}$ 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

$$\begin{array}{ccc} \text{Scheme} & \xrightarrow{\text{Reduction}} & \text{Assumption} \\ \text{(e.g. HIBE)} & & \text{(e.g. Diffie-Hellman)} \end{array}$$

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

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

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

Tight security

$$\begin{array}{ccc} \text{Scheme} & \xrightarrow{\text{Reduction}} & \text{Assumption} \\ \text{(e.g. HIBE)} & & \text{(e.g. Diffie-Hellman)} \end{array}$$

Can be broken with probability ε using resources ρ.

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

Larger security loss requires larger security parameter.

Security loss ℓ can depend on:

Tight security:

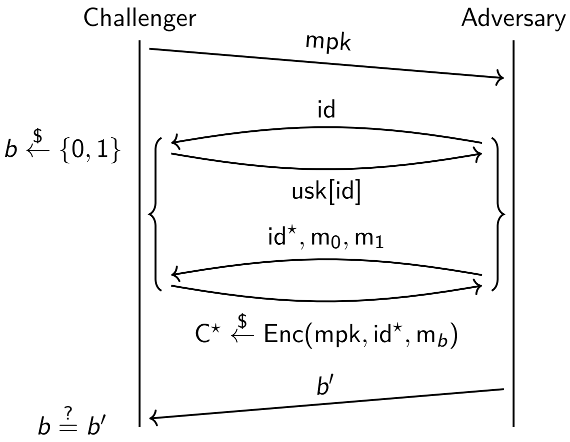
- scheme parameters (e.g. maximum hierarchy depth L)
- λ: the security parameter

allowed

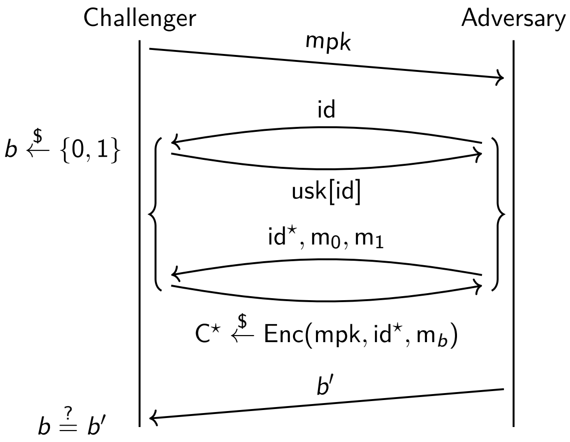
- the attacker's resources (e.g. # user secret key queries Q_k or # challenge ciphertext queries Q_c)

not allowed

Multi-challenge security



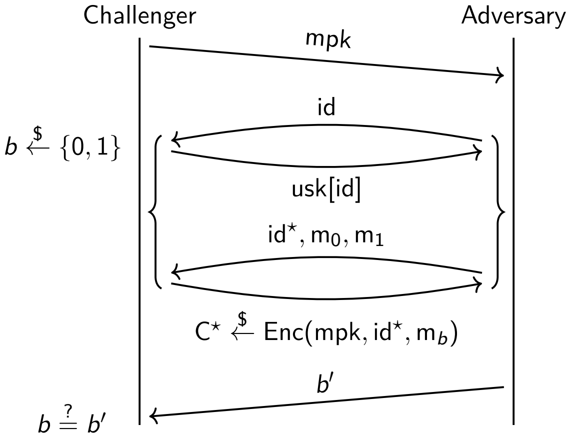
Multi-challenge security



Single-challenge security

Multi-challenge security

Multi-challenge security

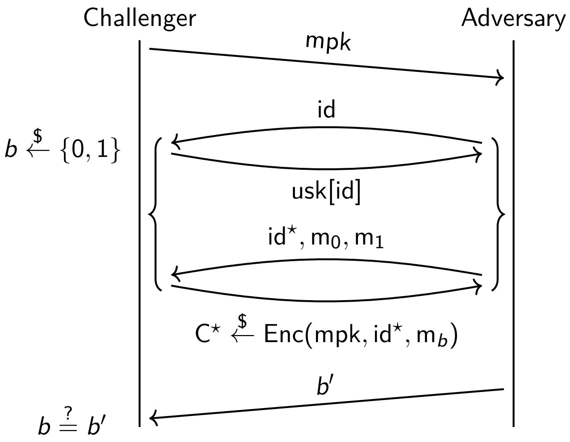


Single-challenge security

$\downarrow$ generic: $\mathcal{O}(Q_c)$ loss

Multi-challenge security

Multi-challenge security



Single-challenge security

$\big\downarrow$ generic: $\mathcal{O}(Q_c)$ loss

Multi-challenge security

Tight multi-instance security: Easy to achieve by rerandomizing the master public key.

History: HIBE

HIBEs in prime-order pairing groups:

[Wat09], [CW13], [BKP14]	$\mathcal{O}(Q_k)$ (single-challenge)
[Lew12], [GCTC16]	$\mathcal{O}(Q_k L)$ (single-challenge)
[LP19]	$\mathcal{O}(nL^2)$ resp. $\mathcal{O}(nL)$ (single-challenge)
This work	$\mathcal{O}(nL^2)$ (multi-challenge)

- Q_k: # user secret key queries
- L: maximum hierarchy depth
- n: Bit-length of the identities

History: Tight 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

History: Tight 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 single-challenge HIBE $+$ Tight multi-challenge IBE $\overset{?}{\rightarrow}$ Tight multi-challenge HIBE

IND-HID-CPA security for (H)IBE

The challenge:

- The reduction must answer user secret key queries for $\mathsf{id}_1, \ldots, \mathsf{id}_{Q_k}$.
- The reduction must take advantage of the adversaries decryption capabilities for $\mathsf{id}_1^\star, \ldots, \mathsf{id}_{Q_c}^\star$.
- The adversary adaptively chooses $\mathsf{id}_1, \ldots, \mathsf{id}_{Q_k}$ and $\mathsf{id}_1^\star, \ldots, \mathsf{id}_{Q_c}^\star$.

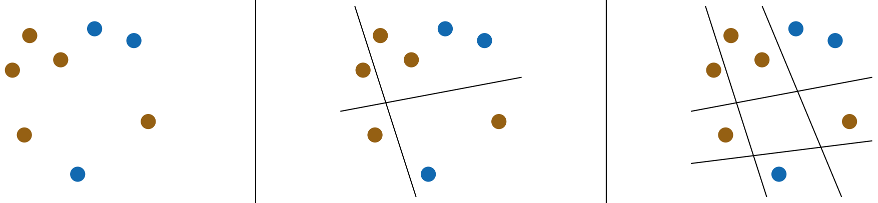
Partitioning

- Different parts use ”slightly different“ secret key.
- A usk key from one part is not helpful for decrypting a ciphertext from a different part.

Partitioning

- Different parts use "slightly different" secret key.
- A usk key from one part is not helpful for decrypting a ciphertext from a different part.

Initial | Intermediate | Final

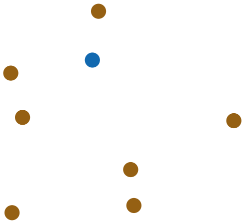


One partition | | Separated ● from ●

● Queried user secret key ● Challenge ciphertext

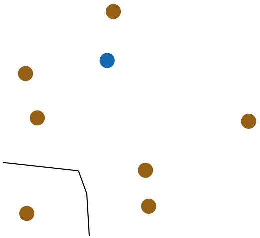
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



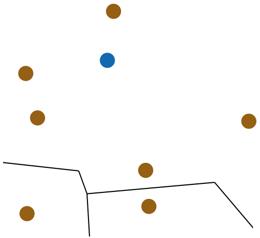
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



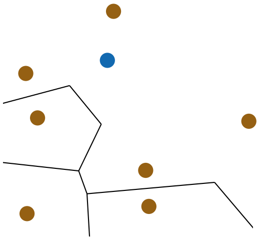
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



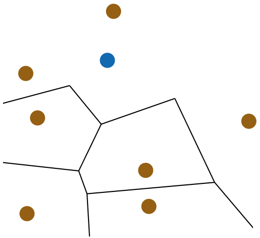
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



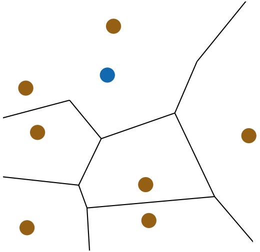
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



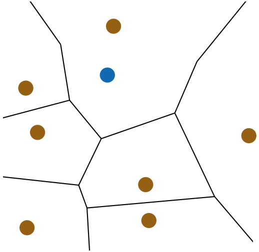
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



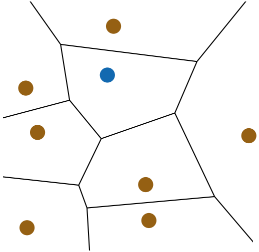
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



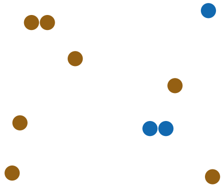
Query-by-query Partitioning

- Typically used by non-tight (H)IBE schemes
- $\mathcal{O}(Q_k)$ security loss



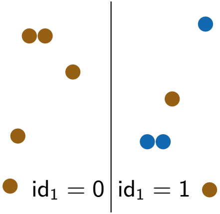
Bit-by-bit Partitioning

- Typically used by tight (H)IBE schemes.
- One part per identity
- $\mathcal{O}(n)$ security loss



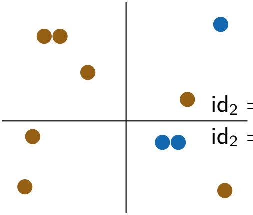
Bit-by-bit Partitioning

- Typically used by tight (H)IBE schemes.
- One part per identity
- $\mathcal{O}(n)$ security loss



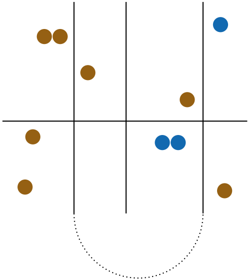
Bit-by-bit Partitioning

- Typically used by tight (H)IBE schemes.
- One part per identity
- $\mathcal{O}(n)$ security loss



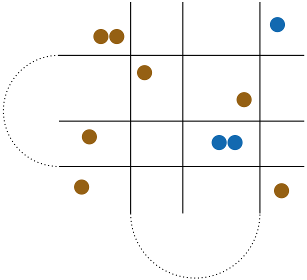
Bit-by-bit Partitioning

- Typically used by tight (H)IBE schemes.
- One part per identity
- $\mathcal{O}(n)$ security loss



Bit-by-bit Partitioning

- Typically used by tight (H)IBE schemes.
- One part per identity
- $\mathcal{O}(n)$ security loss



Partitioning techniques

1. Embedding a challenge of the underlying assumption...
   - ...in a part of the msk that appears only in user secret keys with $id_i = b$.
   - ...“reacts” with the randomness of the usk resp. ciphertext.

Partitioning techniques

1. Embedding a challenge of the underlying assumption...
   - ...in a part of the msk that appears only in user secret keys with $id_i = b$.
   - ..."reacts" with the randomness of the usk resp. ciphertext.
2. Choose randomness of a subspace [GHKW16]
   - hides part of the msk from usk queries.

Usage in the single-challenge setting

Tight IBE:

Scheme	Challenge queries	usk queries
[CW13],[BKP14]	(information-theoretic)	Embedding a challenge

Usage in the single-challenge setting

Tight IBE:

Scheme	Challenge queries	usk queries
[CW13],[BKP14]	(information-theoretic)	Embedding a challenge

Tight HIBE:

Scheme	Challenge queries	usk queries
[LP19]	(information-theoretic)	Subspace

Usage in the multi-challenge setting

Tight IBE:

Scheme	Challenge queries	usk queries
[GDCC16], [HJP18]	Subspace	Embedding a challenge

[BKP14]
(single-challenge IBE)

Use [GHKW16] for
the challenge queries

Use [GHKW16]
for the usk queries

[GDCC16], [HJP18]
(multi-challenge IBE)

[LP19]
(single-challenge HIBE)

[BKP14]
(single-challenge IBE)

Use [GHKW16] for
the challenge queries

Use [GHKW16]
for the usk queries

[GDCC16], [HJP18]
(multi-challenge IBE)

[LP19]
(single-challenge HIBE)

New tight
multi-challenge HIBE?

[BKP14]
(single-challenge IBE)

Use [GHKW16] for
the challenge queries

Use [GHKW16]
for the usk queries

[GDCC16], [HJP18]
(multi-challenge IBE)

[LP19]
(single-challenge HIBE)

Doesn't work

New tight
multi-challenge HIBE?

Simplified version of BKP-like schemes

- Master secret key:
  For every bit position $i \in \{1, \ldots, n \cdot L\}$ and bit $b \in \{0, 1\}$: $\boxed{\mathbf{X}_{i,b}}$

Simplified version of BKP-like schemes

- Master secret key:
  For every bit position $i \in \{1, \ldots, n \cdot L\}$ and bit $b \in \{0, 1\}$: $\boxed{\mathbf{X}_{i,b}}$

usk randomness

- User secret key for id: $\boxed{\sum_i^{|\mathrm{id}|} \mathbf{X}_{i,\mathrm{id}[i]}}\ \boxed{\mathbf{t}}$

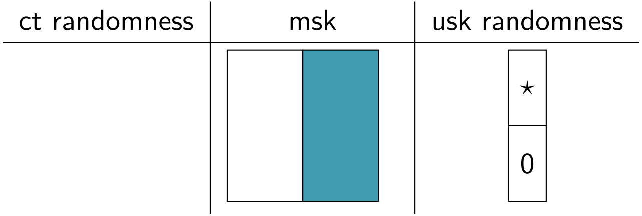
Simplified version of BKP-like schemes

- Master secret key:
  For every bit position $i \in \{1, \ldots, n \cdot L\}$ and bit $b \in \{0, 1\}$: $\boxed{\mathbf{X}_{i,b}}$
- User secret key for id: $\boxed{\sum_i^{|\mathrm{id}|} \mathbf{X}_{i,\mathrm{id}[i]}}$ $\boxed{\mathbf{t}}$
- Challenge ciphertext for id*: $\underset{\boxed{\mathbf{h}^\top}}{\overset{\text{ct randomness}}{\downarrow}}$ $\boxed{\sum_i^{|\mathrm{id}^\star|} \mathbf{X}_{i,\mathrm{id}^\star[i]}}$

The difficulty

Use the [GHKW16] subspace technique for the user secret keys [LP19].

In a suitable (hidden) basis:

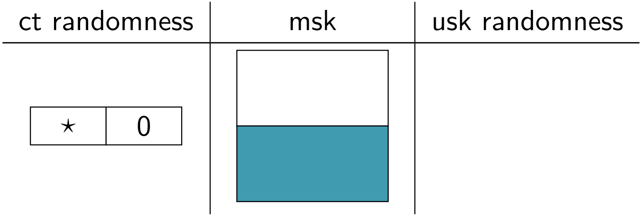


Half of the entropy is hidden. ✓

The difficulty

Use the [GHKW16] subspace technique for the challenge ciphertexts [GDCC16, HJP18].

In a suitable (hidden) basis:

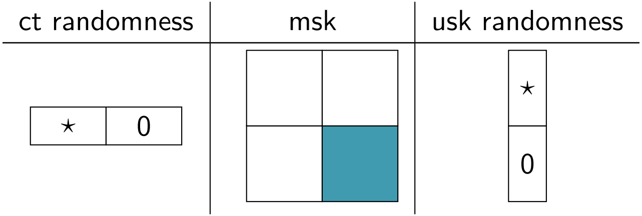


Half of the entropy is hidden. ✓

The difficulty

Use the [GHKW16] subspace technique for both usks and cts.

In a suitable (hidden) basis:



Only one quarter of the entropy is hidden. ✗

Our solution

New technique to randomize multiple challenge ciphertexts. . .

- . . .based on the "Embedding a challenge" approach.
- . . .achieves the same efficiency.
- . . .compatible with [LP19]

Our solution

Previous work (only IBE)

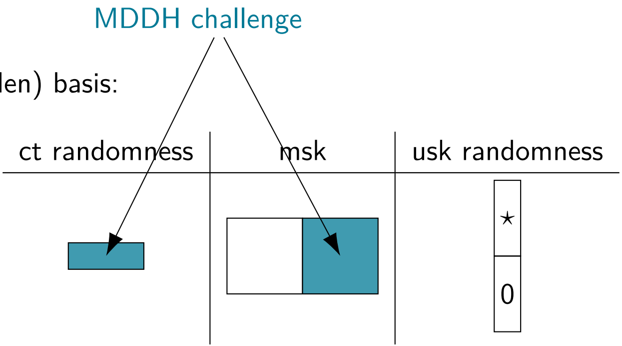
Scheme	Challenge queries	usk queries
[GDCC16], [HJP18]	Subspace	Embedding a challenge

This work (also HIBE)

Scheme	Challenge queries	usk queries
This work	Embedding a challenge	Subspace

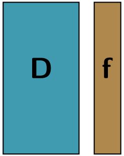
Our solution

In a suitable (hidden) basis:



Our solution – More details

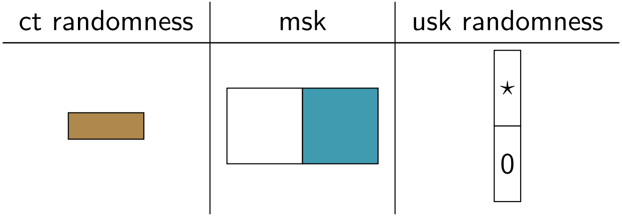
MDDH challenge:



$\mathbf{f} \in \mathrm{Span}(\mathbf{D})$ or

$\mathbf{f}$ is uniformly random

In a suitable (hidden) basis:

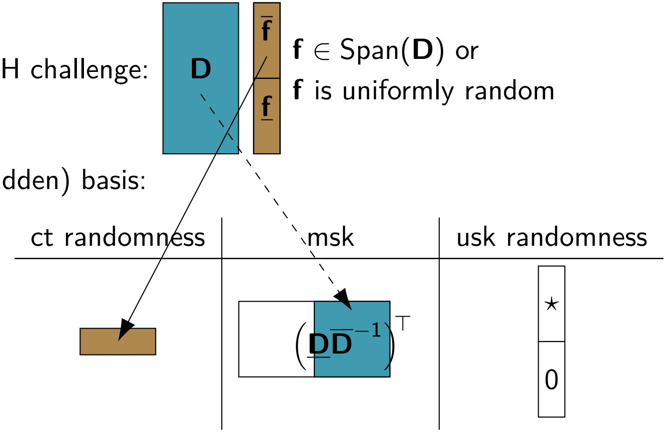


Our solution – More details

MDDH challenge:

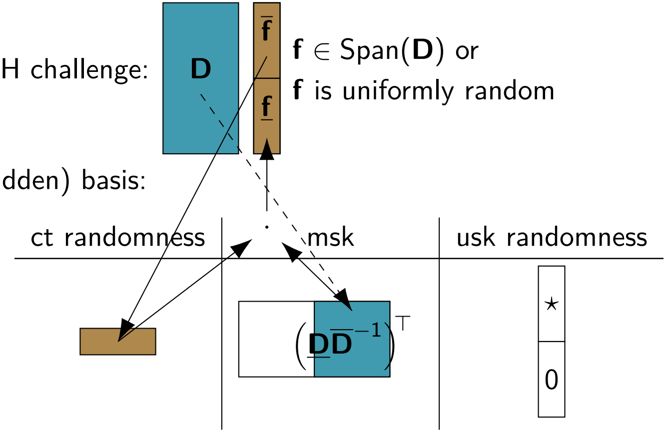
$\mathbf{f} \in \mathrm{Span}(\mathbf{D})$ or
$\mathbf{f}$ is uniformly random

In a suitable (hidden) basis:



Our solution – More details

MDDH challenge:

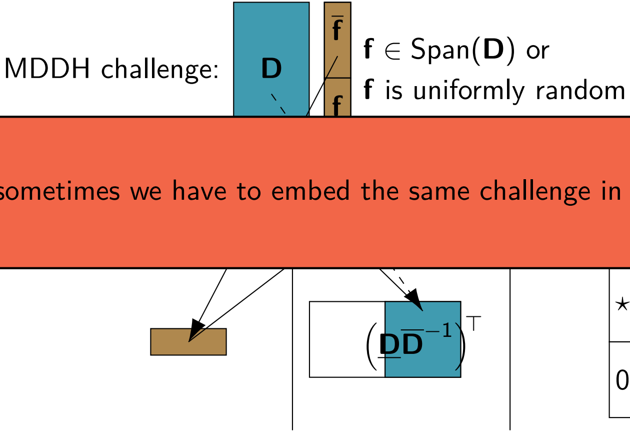


$\mathbf{f} \in \mathrm{Span}(\mathbf{D})$ or

$\mathbf{f}$ is uniformly random

In a suitable (hidden) basis:

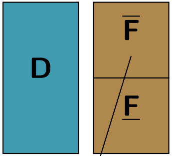
Our solution – More details



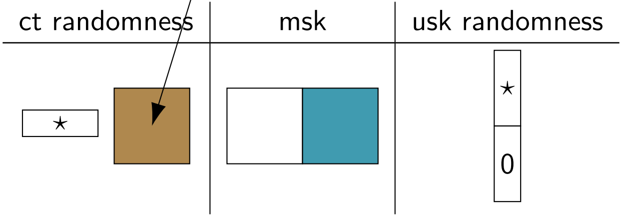
But sometimes we have to embed the same challenge in multiple ciphertexts!

Our solution – More details

MDDH challenge:



In a suitable (hidden) basis:



Comparison of HIBEs (in prime-order pairing groups)

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{usk}\rvert$	$\lvert\mathsf{C}\rvert$	Loss	MC	Assumption
[Wat05]	$\mathcal{O}(nL)$	$\mathcal{O}(nL)$	$\mathcal{O}(p)$	$\mathcal{O}(nQ_k)^L$	✗	DBDH
[Wat09]	$\mathcal{O}(L)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(Q_k)$	✗	2-LIN
[Lew12]	$\mathcal{O}(1)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(Q_k)$	✗	2-LIN
[CW13]	$\mathcal{O}(L)$	$\mathcal{O}(L)$	$\mathcal{O}(1)$	$\mathcal{O}(Q_k)$	✗	SXDH
[BKP14]	$\mathcal{O}(L)$	$\mathcal{O}(L)$	$\mathcal{O}(1)$	$\mathcal{O}(Q_k)$	✗	SXDH
[GCTC16]	$\mathcal{O}(1)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(Q_k)$	✗	SXDH
$[\text{LP19}]_1$	$\mathcal{O}(nL^2)$	$\mathcal{O}(nL^2)$	$\mathcal{O}(1)$	$\mathcal{O}(nL^2)$	✗	SXDH
$[\text{LP19}]_1^{\mathcal{H}}$	$\mathcal{O}(\gamma L)$	$\mathcal{O}(\gamma L)$	$\mathcal{O}(1)$	$\mathcal{O}(\gamma L)$	✗	SXDH
$[\text{LP19}]_2$	$\mathcal{O}(nL^2)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(nL)$	✗	SXDH
$[\text{LP19}]_2^{\mathcal{H}}$	$\mathcal{O}(\gamma L)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(\gamma)$	✗	SXDH
Ours_1	$\mathcal{O}(nL^2)$	$\mathcal{O}(nL^2)$	$\mathcal{O}(1)$	$\mathcal{O}(nL^2)$	✓	SXDH
$\text{Ours}_1^{\mathcal{H}}$	$\mathcal{O}(\gamma L)$	$\mathcal{O}(\gamma L)$	$\mathcal{O}(1)$	$\mathcal{O}(\gamma L)$	✓	SXDH
Ours_2	$\mathcal{O}(nL^2)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(nL^2)$	✓	SXDH
$\text{Ours}_2^{\mathcal{H}}$	$\mathcal{O}(\gamma L)$	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(\gamma L)$	✓	SXDH

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

Future work: Beyond bit-by-bit partitioning

[AHY15] achieved a trade-off between mpk and usk/C size for IBE:

Parameter $c \in [0, 1]$

Scheme	$\lvert\text{mpk}\rvert$	$\lvert\text{usk}\rvert$	$\lvert\text{C}\rvert$	Loss
[AHY15]	$\mathcal{O}(n^{1-c})$	$\mathcal{O}(n^{c})$	$\mathcal{O}(n^{c})$	$\mathcal{O}(n)$

Future work: Beyond bit-by-bit partitioning

[AHY15] achieved a trade-off between mpk and usk/C size for IBE:
Parameter $c \in [0, 1]$

Scheme	$\|\mathsf{mpk}\|$	$\|\mathsf{usk}\|$	$\|\mathsf{C}\|$	Loss
[AHY15]	$\mathcal{O}(n^{1-c})$	$\mathcal{O}(n^{c})$	$\mathcal{O}(n^{c})$	$\mathcal{O}(n)$

[CGW17] achieved constant size mpk (and tighter security loss) in composite-order pairing groups (4 factors):

Scheme	$\|\mathsf{mpk}\|$	$\|\mathsf{usk}\|$	$\|\mathsf{C}\|$	Loss
[CGW17]	3	1	1	$\mathcal{O}(\log(Q_k))$

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, Junqing Gong, and Jian Weng.
Tightly secure IBE under constant-size master public key.
In Serge Fehr, editor, PKC 2017, Part I, volume 10174 of LNCS, pages 207–231. Springer, Heidelberg, March 2017.
doi:10.1007/978-3-662-54365-8_9.

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.

References III

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.

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.

References IV

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.

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.
doi:10.1007/978-3-662-49890-3_1.

References V

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.

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.

References VI

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.

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.
doi:10.1007/11426639_7.

References VII

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.
doi:10.1007/978-3-642-03356-8_36.

Pictures

Alice, Bob, Trusted Party: freepik.com

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