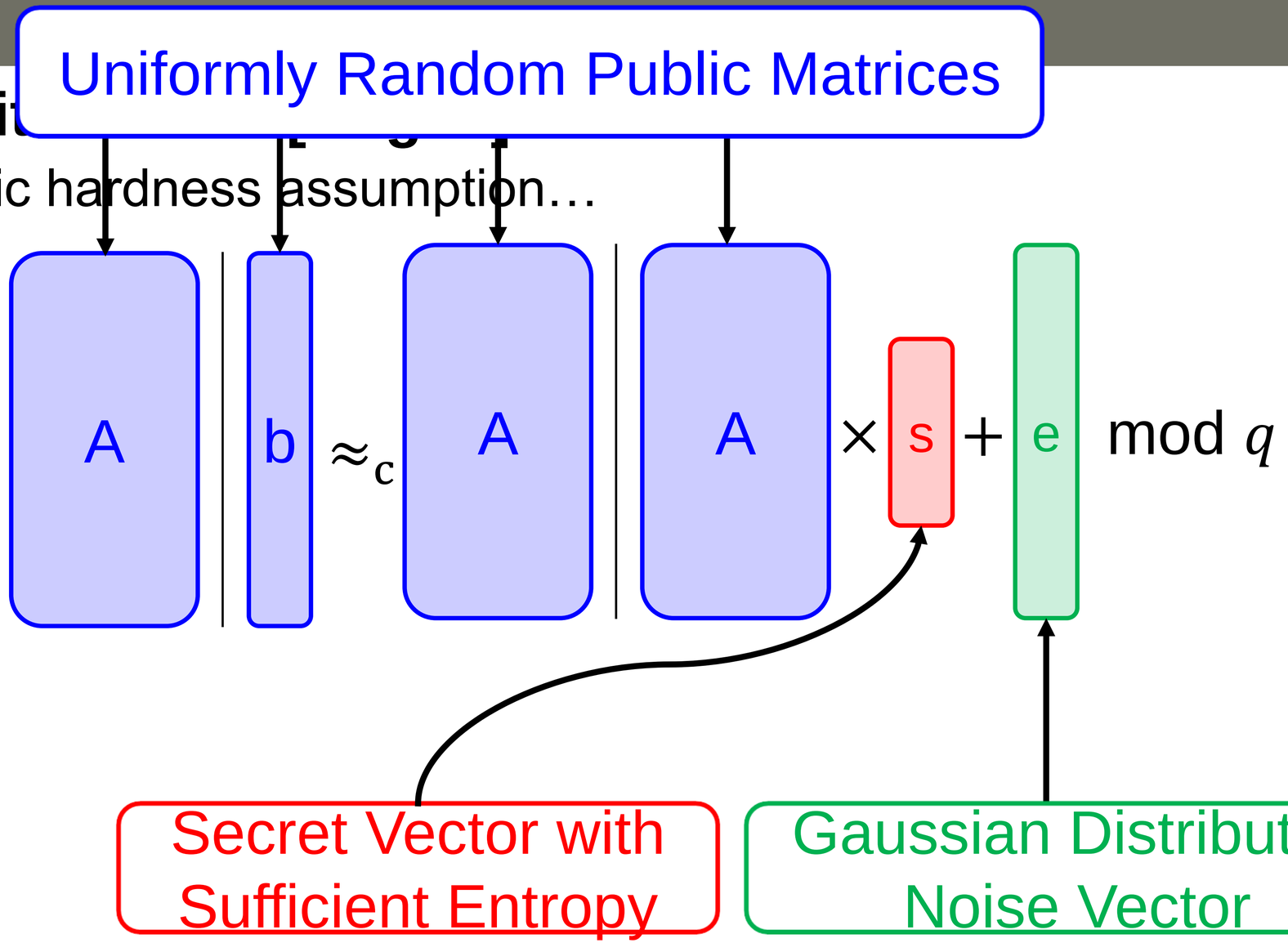
Impossibility Results for Lattice-Based Functional Encryption Schemes

Akın Ünal
ETH Zürich, Zürich, Switzerland
auenal@inf.ethz.ch
(Work done while the author was at KIT – Karlsruhe Institute of Technology, Karlsruhe, Germany.)

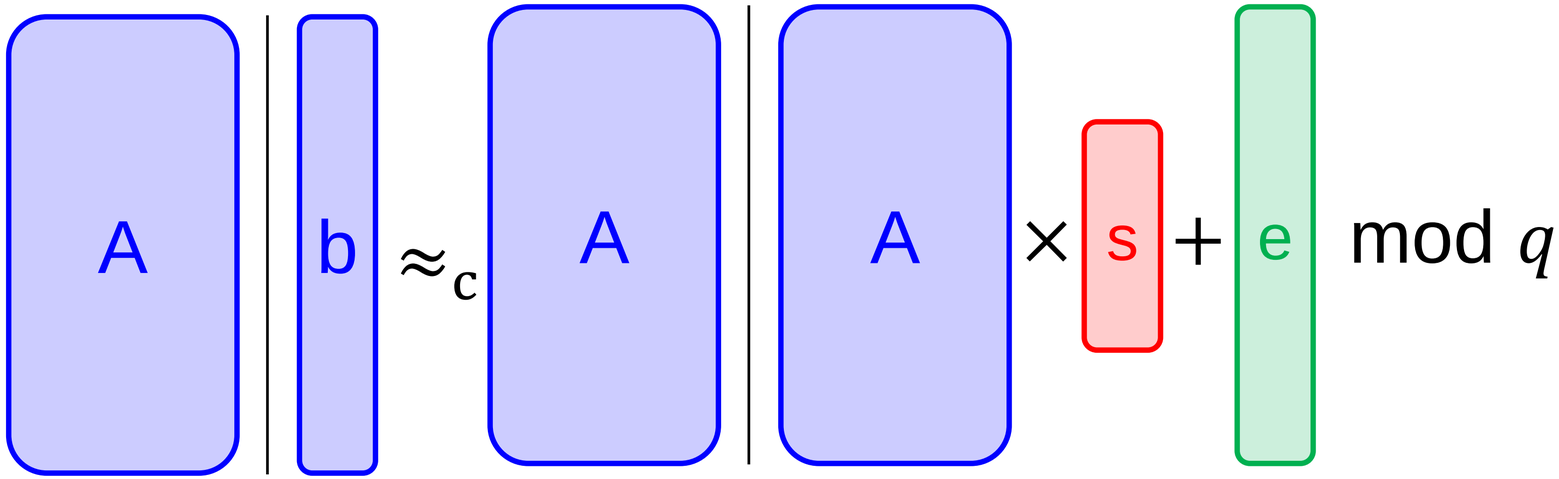
Learning wit

A cryptographic hardness assumption…



Learning with Errors [Reg05]

A cryptographic hardness assumption…

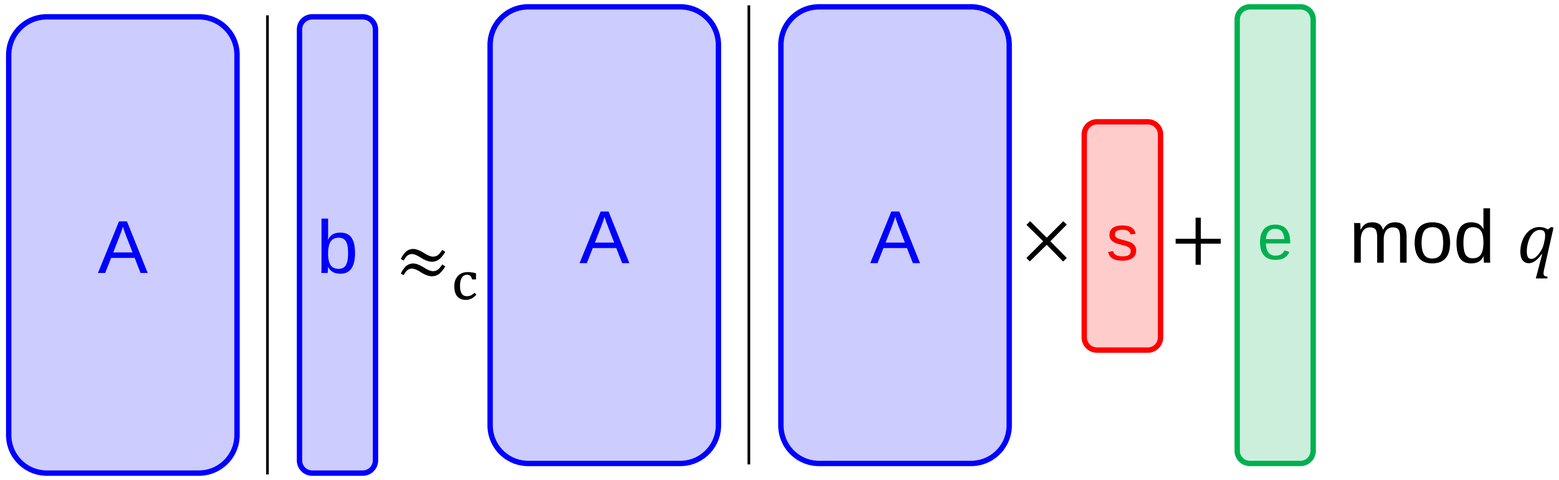


with strong homomorphic properties which enables a lot of different cryptographic primitives:

- Fully Homomorphic Encryption [BV11]
- Lockable Obfuscation [GKW17, WZ17]
- Attribute-Based Encryption [GVW13, BGG+14]

Learning with Errors [Reg05]

A cryptographic hardness assumption…



with strong homomorphic properties which enables a lot of different cryptographic primitives:

- Fully Homomorphic Encryption [BV11]
- Lockable Obfuscation [GKW17, WZ17]
- Attribute-Based Encryption [GVW13, GGHSW13]

But what about Functional Encryption?

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption		✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption		
Compact Quadratic FE	✓ [BCFG17]	
Compact Cubic FE		
(Non-Compact Const.-degree FE)	✓	✓

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption		
Compact Quadratic FE	✓ [BCFG17]	
Compact Cubic FE		
(Non-Compact Const.-degree FE)		

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Compact Quadratic FE	✓ [BCFG17]	✗
Compact Cubic FE		
(Non-Compact Const.-degree FE)	✓	✓

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Compact Quadratic FE	✓ [BCFG17]	✗
Compact Cubic FE		
(Non-Compact Const.-degree FE)	✓	✓

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Compact Quadratic FE	✓ [BCFG17]	✗
Compact Cubic FE	✗	✗
(Non-Compact Const.-degree FE)		

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Compact Quadratic FE	✓	✗
Compact Cubic FE	This (+ additional assumptions) would imply Indistinguishability Obfuscation. [LT17]	✗
(Non-Compact Const.-degree FE)		

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Quadratic FE	✓ [BCFG17]	✗
Compact Cubic FE	✗	✗
(Non-Compact Const.-degree FE)	✓	✓

By Linearization

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Compact Quadratic FE	✓ [BCFG17]	✗
Compact Cubic FE	✗	✗
(Non-Compact Const.-degree FE)	✓	✓

(We do not list IBE, ABE and Bounded-Collusion FE here.)

Comparing Functional Encryption Schemes

	Pairing-Based Schemes	Lattice-Based Schemes
Inner-Product Encryption	✓	✓ [AFV11, ALS16]
Function-Hiding Inner-Product Encryption	✓ [BJK15, DDM16, Lin17, ACF+18]	✗
Compact Quadratic FE	✓ [BCFG17]	✗
Compact Cubic FE	✗	✗
(Non-Compact Const.-degree FE)	✓	✓

Question

What hinders us from constructing function-hiding inner-product encryption schemes whose security can be proven solely from the learning with errors assumption?

Maybe fundamental mathematical barriers…

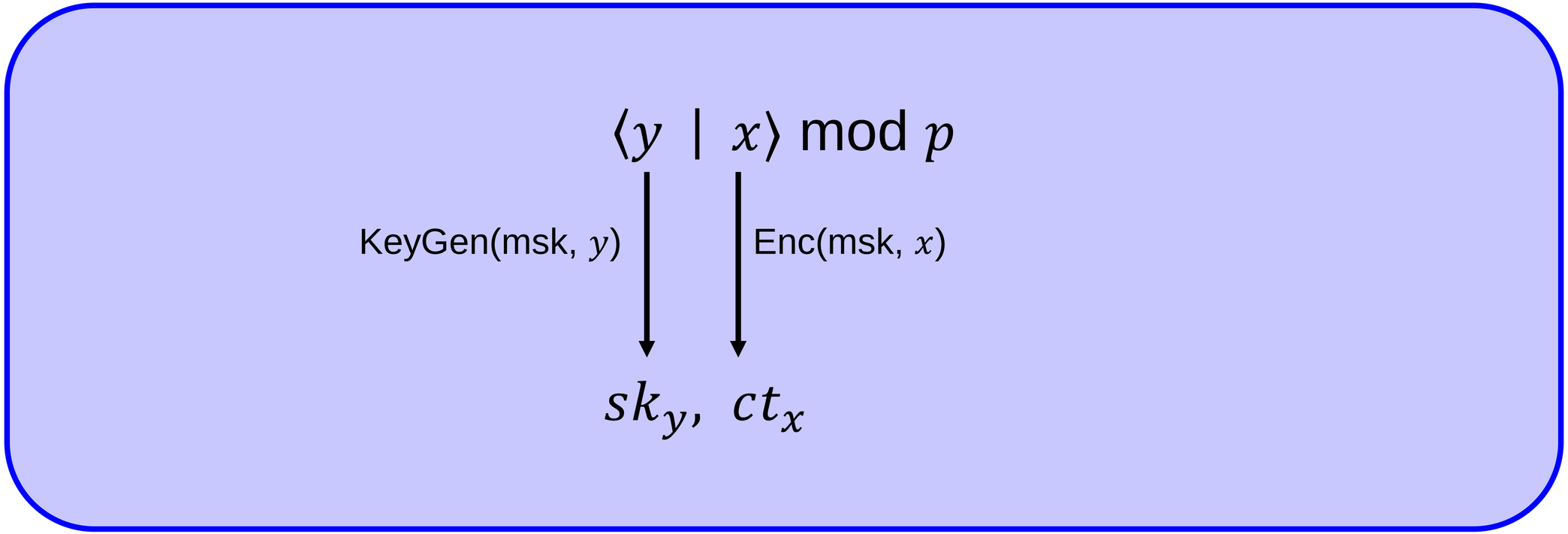
Secret-Key Inner-Product Encryption

- Messages and functions are vectors $x, y \in \mathbb{Z}_p^n$.
- Setup(1^λ) generates a **master secret key** msk.

$$\langle y \mid x \rangle \bmod p$$

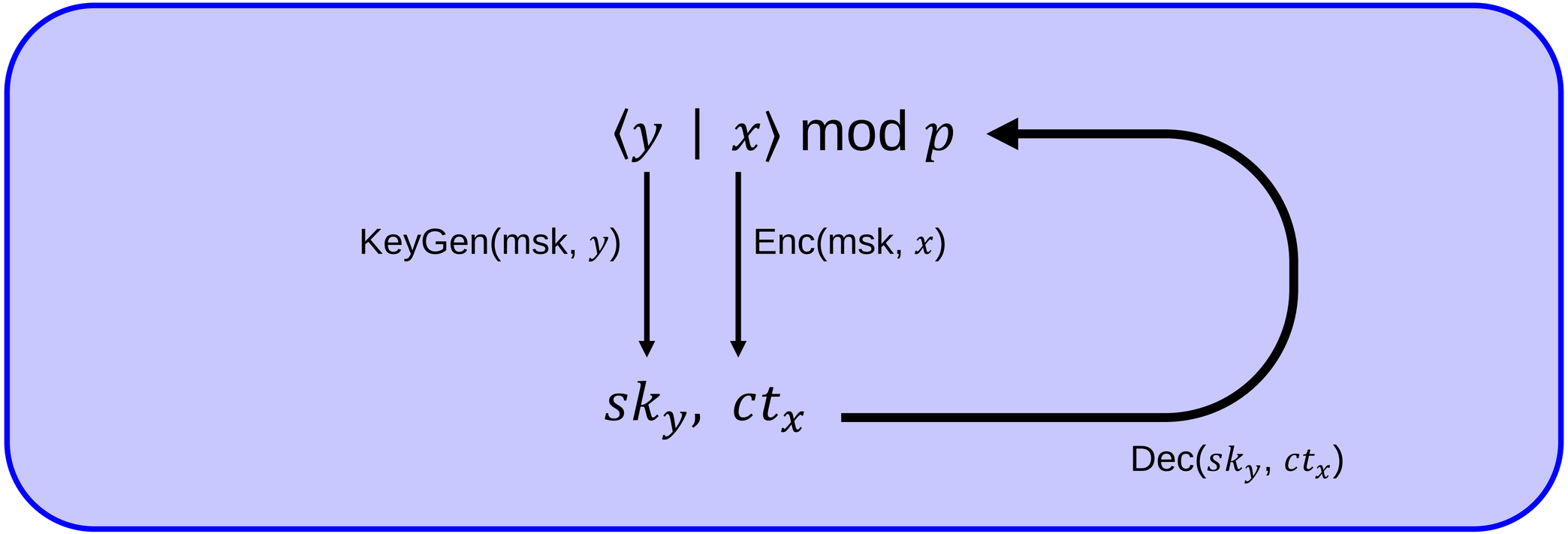
Secret-Key Inner-Product Encryption

- Messages and functions are vectors $x, y \in \mathbb{Z}_p^n$.
- Setup(1^λ) generates a **master secret key** msk.

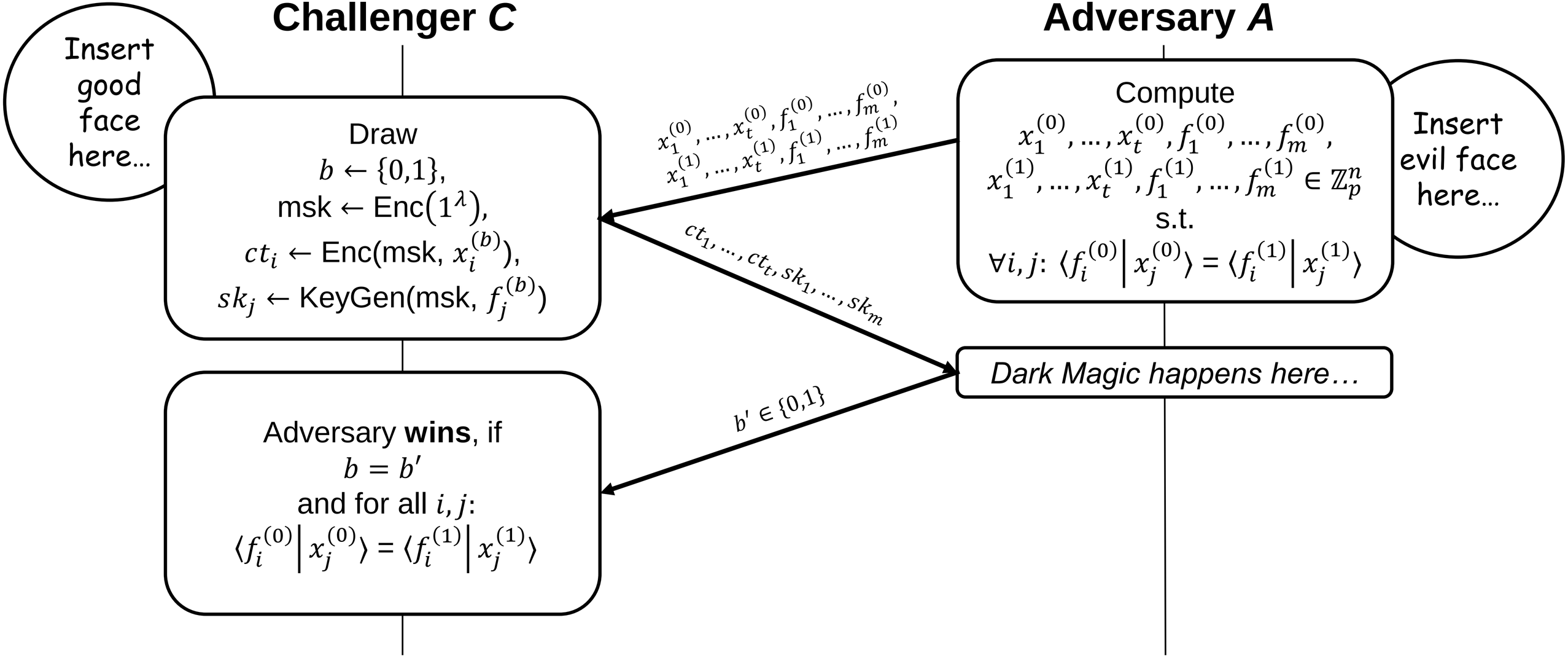


Secret-Key Inner-Product Encryption

- Messages and functions are vectors $x, y \in \mathbb{Z}_p^n$.
- Setup(1^λ) generates a **master secret key** msk.



Selective Function-Hiding IND-CPA Security



Selective Function-Hiding IND-CPA Security

- The **advantage** of the adversary A is:

$$\mathrm{Adv}(A)_{m-fh-IND-CPA} := 2 \times \Pr[A \text{ wins}] - 1.$$

- For $m = m(\lambda)$ secret keys, the IPE scheme is called

selectively m-function-hiding IND-CPA secure,

if $\mathrm{Adv}(A)_{m-fh-IND-CPA} \in \mathrm{negl}(\lambda)$ for each ppt A.

- The IPE scheme is called

(unbounded) selectively function-hiding IND-CPA secure,

if it is sel. m-function-hiding IND-CPA secure for each $m \in \mathrm{poly}(\lambda)$.

Contribution

Idealized Impossibility “Theorem”.

There does not exist a lattice-based Inner-Product Encryption scheme which is function-hiding secure.

This really has to mean something!

Idea: Replace „lattice-based“ by common design patterns of lattice-based crypto-schemes.

Common Design Patterns: Linear Decryption

In most cases:

- Ciphertexts ct_x and secret keys sk_f are vectors over $\mathbb{Z}_q$.
- Decryption has the following formula:

$$\mathbf{Dec}(\boldsymbol{sk_f}, \boldsymbol{ct_x}) := \left\lceil \frac{\langle sk_f \mid ct_x \rangle \bmod q}{\left\lfloor \frac{q}{p} \right\rfloor} \right\rfloor \in \mathbb{Z}_p$$

Common Design Patterns: Offline/Online-Encryption [HW14,AR17]

Almost always: Encryption follows an offline/online-pattern.

Offline Phase: compute arbitrary complex randomness without looking at input x.

Online Phase: combine randomness with x in a very simple way (by evaluating const-degree polynomials at x).

Enc(msk, x):

- Compute s multinomial degree-d integer polynomials $(r_1, \dots, r_s) \leftarrow \text{Enc}_{off}(msk)$.
- Compute and output $ct_x := \big(r_1(x), \dots, r_s(x)\big) \bmod q \in \mathbb{Z}_q^s$.

Common Design Patterns: Offline/Online-Encryption [HW14,AR17]

Almost always: Encryption follows an offline/online-pattern.

Offline Phase: compute arbitrary complex randomness without looking at input x.

Online Phase: combine randomness with x in a very simple way (by evaluating const-degree polynomials at x).

We call d the **depth** of the encryption algorithm.

Enc(msk, x):

- Compute s multinomial degree-d integer polynomials $(r_1, \dots, r_s) \leftarrow \text{Enc}_{off}(msk)$.
- Compute and output $ct_x := \left(r_1(x), \dots, r_s(x)\right) \bmod q \in \mathbb{Z}_q^s$.

Contribution

Our Impossibility Theorem.

An Inner-Product Encryption scheme

- *with* ***Linear Decryption***
- *and* ***Offline/Online-Encryption of const. depth***

cannot be selectively function-hiding IND-CPA secure.

Contribution

Our Impossibility Theorem.

An Inner-Product Encryption scheme

- *with* ***Linear Decryption***
- *and* ***Offline/Online-Encryption of const. depth***

cannot be selectively $m + 1$ *function-hiding IND-CPA secure,*

for some $m \in poly(\lambda)$ *which depends on the scheme.*

Contribution

Our Impossibility Theorem.

An Inner-Product Encryption sch

- *with* ***Linear Decryption***
- *and* ***Offline/Online-Encryption of const. depth***

cannot be selectively $m + 1$ *function-hiding IND-CPA secure,*

for some $m \in poly(\lambda)$ *which depends on the scheme.*

We need:
q is prime, $\frac{q}{p}$ is bounded by a polynomial, p is greater than some constant.

Offline/Online-Encryption

Enc(msk, x):

- Compute s multinomial degree-d integer polynomials $(r_1, \dots, r_s) \leftarrow \text{Enc}_{off}(msk)$.
- Compute and output $ct_x := \big(r_1(x), \dots, r_s(x)\big) \bmod q \in \mathbb{Z}_q^s$.

Encryption Algorithm of depth d …

Offline/Online-Encryption

Enc(msk, x):

- Compute s multinomial degree-d integer polynomials $(r_1, \dots, r_s) \leftarrow \text{Enc}_{off}(msk)$.
- Compute and output $ct_x := \big(r_1(x), \dots, r_s(x)\big)$ **mod** $q \in \mathbb{Z}_q^s$.

Encryption Algorithm of depth d …

… **over** $\mathbb{Z}_q$.

Offline/Online-Encryption

Enc(msk, x):

- Compute s multinomial degree-d integer polynomials $(r_1, \dots, r_s) \leftarrow \text{Enc}_{off}(msk)$.
- Compute and output $ct_x := (r_1(x), \dots, r_s(x)) \in \mathbb{Z}^s$.

Encryption Algorithm of depth d …

… **over** $\mathbb{Z}$.

Offline/Online-Encryption

Enc : Encryption Algorithm of depth d over $\mathbb{Z}$.

↳ Each ciphertext $ct_x \leftarrow$Enc(msk,x) is an integer vector $ct_x \in \mathbb{Z}^s$.

Enc is **of width** $B = B(\lambda)$, if

$\Pr[ct_x \in \{-B, \dots, B\}^s \mid ct_x \leftarrow \text{Enc}(\text{msk}, x)] \geq 1 - \text{negl}(\lambda)$.

Offline/Online-Encryption

Enc : Encryption Algorithm of depth d over $\mathbb{Z}_q$.

↳ Each ciphertext $ct_x \leftarrow$Enc(msk,x) is a vector $ct_x \in \mathbb{Z}_q^s$.

Enc is **of width** $B = B(\lambda)$, if

$$\Pr[ct_x \in \{-B, \dots, B\}^s \mid ct_x \leftarrow \text{Enc}(\text{msk},x)] \geq 1 - \text{negl}(\lambda).$$

Under the identification:

$$\mathbb{Z}_q \triangleq \left\{-\frac{q-1}{2}, \dots, 0, \dots, \frac{q-1}{2}\right\} \subset \mathbb{Z}$$

Contribution

Our Impossibility Theorem.

Let q prime, $\frac{q}{p}$ bounded by a polynomial, p greater than some constant.

An Inner-Product Encryption scheme

- *with **Linear Decryption***
- *and **Offline/Online-Encryption of const. depth***

<u>cannot</u> be selectively $m + 1$ function-hiding IND-CPA secure.

Technical Overview

$m + 1$ function-hiding IND-CPA secure IPE scheme of constant depth over $\mathbb{Z}_q$ with linear decryption

… transformed by adversary to …

IND-CPA secure SKE scheme of width $\frac{q}{p}$ and constant depth over $\mathbb{Z}_q$

… transformed by adversary to …

IND-CPA secure SKE scheme of polynomial width and constant depth over $\mathbb{Z}$

… broken by general adversary!

Technical Overview: Step 1

$m + 1$ function-hiding IND-CPA secure IPE scheme of constant depth over $\mathbb{Z}_q$ with linear decryption

Trade Off
Function-Hiding *and* **Linear Decryption**
Against
Short Ciphertexts*!*

IND-CPA secure SKE scheme of width $\frac{q}{p}$ and constant depth over $\mathbb{Z}_q$

Technical Overview: Step 1

$m + 1$ function-hiding IND-CPA secure IPE scheme of constant depth over $\mathbb{Z}_q$ with linear decryption

- Adversary draws m keys for the zero function vector $sk_1, \ldots, sk_m \leftarrow$KeyGen(msk, 0)
- Correctness $\Rightarrow$ Dec$(sk_i, ct_x) = \left\lceil \langle sk_i | ct_x \rangle / \left\lfloor \frac{q}{p} \right\rfloor \right\rfloor = 0$

$$\Rightarrow (\langle sk_1 | ct_x \rangle, \ldots, \langle sk_m | ct_x \rangle) \in \left\{ -\left\lfloor \frac{q}{p} \right\rfloor, \ldots, \left\lfloor \frac{q}{p} \right\rfloor \right\}^m$$

Decryption Noises

IND-CPA secure SKE scheme of width $\frac{q}{p}$ and constant depth over $\mathbb{Z}_q$

Technical Overview: Step 1

$m + 1$ function-hiding IND-CPA secure IPE scheme of constant depth over $\mathbb{Z}_q$ with linear decryption

- Adversary draws m keys for the zero function vector $sk_1, \dots, sk_m \leftarrow$KeyGen(msk, 0)
- Correctness ⇒ Dec$(sk_i, ct_x) = \left\lceil \langle sk_i |\, ct_x \rangle \,/\, \left\lfloor \frac{q}{p} \right\rfloor \right\rfloor = 0$

  $\Rightarrow (\langle sk_1 | ct_x \rangle, \dots, \langle sk_m | ct_x \rangle) \in \left\{ -\left\lfloor \frac{q}{p} \right\rfloor, \dots, \left\lfloor \frac{q}{p} \right\rfloor \right\}^m$
- Function-Hiding ⇒ Pr$[sk_y \in \text{span}_{\mathbb{Z}_q}\{sk_1, \dots, sk_m\}] \notin \text{negl}(\lambda)$

  $\Rightarrow \langle sk_y | ct_x \rangle$ can be reconstructed from $\langle sk_1 | ct_x \rangle, \dots, \langle sk_m | ct_x \rangle$

⇒ Use the vector $(\langle sk_1 | ct_x \rangle, \dots, \langle sk_m | ct_x \rangle) \in \mathbb{Z}_q^m$ as new ciphertext in SKE for x.

IND-CPA secure SKE scheme of width $\frac{q}{p}$ and constant depth over $\mathbb{Z}_q$

Technical Overview: Step 2

IND-CPA secure SKE scheme of width $\frac{q}{p}$ and constant depth over $\mathbb{Z}_q$

Get Rid Of Arithmetic Reduction in Online Part!

IND-CPA secure SKE scheme of polynomial width and constant depth over $\mathbb{Z}$

Technical Overview: Step 2

IND-CPA secure SKE scheme of width $\frac{q}{p}$ and constant depth over $\mathbb{Z}_q$

Very rough Idea:

- $(r_1, \ldots, r_s) \leftarrow \text{Enc}_{off}(msk)$
- Each r_i has small output values

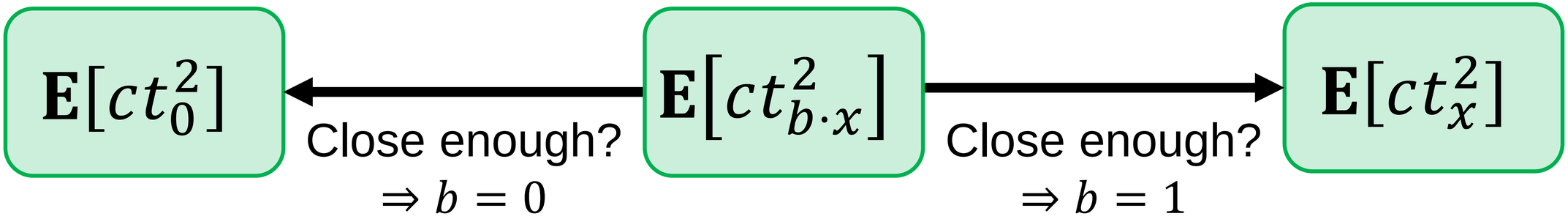
  $\Rightarrow$ Each r_i has small coefficients
- When we evaluate a polynomial with small coefficients on a small input, then the result is in $\left\{-\frac{q-1}{2}, \ldots, 0, \ldots, \frac{q-1}{2}\right\}$, even without applying arithmetic reduction modulo q.

IND-CPA secure SKE scheme of polynomial width and constant depth over $\mathbb{Z}$

Technical Overview: Step 3

IND-CPA secure SKE scheme of polynomial width and const. depth over $\mathbb{Z}$

- Adversary submits messages 0, $b \cdot x$ and x.
- He estimates $\mathbf{E}[ct_0^2]$, $\mathbf{E}[ct_{b\cdot x}^2]$ and $\mathbf{E}[ct_x^2]$.



- Rest of proof is just Mathematics.

Conclusion

A lattice-based FE scheme which uses popular design choices for encryption (*online/offline-encryption*) and decryption (*linear decryption*) cannot be function-hiding IND-CPA secure.

References I

Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu, *Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings*, CRYPTO 2018, Part I (Hovav Shacham and Alexandra Boldyreva, eds.), LNCS, vol. 10991, Springer, Heidelberg, August 2018, pp. 597–627.

Shweta Agrawal, David Mandell Freeman, and Vinod Vaikuntanathan, *Functional encryption for inner product predicates from learning with errors*, ASIACRYPT 2011 (Dong Hoon Lee and Xiaoyun Wang, eds.), LNCS, vol. 7073, Springer, Heidelberg, December 2011, pp. 21–40.

References II

Shweta Agrawal, Benoît Libert, and Damien Stehlé, *Fully secure functional encryption for inner products, from standard assumptions*, CRYPTO 2016, Part III (Matthew Robshaw and Jonathan Katz, eds.), LNCS, vol. 9816, Springer, Heidelberg, August 2016, pp. 333–362.

Shweta Agrawal and Alon Rosen, *Functional encryption for bounded collusions, revisited*, TCC 2017, Part I (Yael Kalai and Leonid Reyzin, eds.), LNCS, vol. 10677, Springer, Heidelberg, November 2017, pp. 173–205.

References III

Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, and Romain Gay, *Practical functional encryption for quadratic functions with applications to predicate encryption*, CRYPTO 2017, Part I (Jonathan Katz and Hovav Shacham, eds.), LNCS, vol. 10401, Springer, Heidelberg, August 2017, pp. 67–98.

Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy, *Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits*, EUROCRYPT 2014 (Phong Q. Nguyen and Elisabeth Oswald, eds.), LNCS, vol. 8441, Springer, Heidelberg, May 2014, pp. 533–556.

References IV

- Allison Bishop, Abhishek Jain, and Lucas Kowalczyk, *Function-hiding inner product encryption*, ASIACRYPT 2015, Part I (Tetsu Iwata and Jung Hee Cheon, eds.), LNCS, vol. 9452, Springer, Heidelberg, November / December 2015, pp. 470–491.
- Zvika Brakerski and Vinod Vaikuntanathan, *Efficient fully homomorphic encryption from (standard) LWE*, 52nd FOCS (Rafail Ostrovsky, ed.), IEEE Computer Society Press, October 2011, pp. 97–106.
- Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay, *Functional encryption for inner product with full function privacy*, PKC 2016, Part I (Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, eds.), LNCS, vol. 9614, Springer, Heidelberg, March 2016, pp. 164–195.

References V


Rishab Goyal, Venkata Koppula, and Brent Waters, *Lockable obfuscation*, 58th FOCS (Chris Umans, ed.), IEEE Computer Society Press, October 2017, pp. 612–621.


Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee, *Attribute-based encryption for circuits*, 45th ACM STOC (Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, eds.), ACM Press, June 2013, pp. 545–554.


Susan Hohenberger and Brent Waters, *Online/offline attribute-based encryption*, PKC 2014 (Hugo Krawczyk, ed.), LNCS, vol. 8383, Springer, Heidelberg, March 2014, pp. 293–310.

References VI


Huijia Lin, *Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs*, CRYPTO 2017, Part I (Jonathan Katz and Hovav Shacham, eds.), LNCS, vol. 10401, Springer, Heidelberg, August 2017, pp. 599–629.


Huijia Lin and Stefano Tessaro, *Indistinguishability obfuscation from trilinear maps and block-wise local PRGs*, CRYPTO 2017, Part I (Jonathan Katz and Hovav Shacham, eds.), LNCS, vol. 10401, Springer, Heidelberg, August 2017, pp. 630–660.


Oded Regev, *On lattices, learning with errors, random linear codes, and cryptography*, 37th ACM STOC (Harold N. Gabow and Ronald Fagin, eds.), ACM Press, May 2005, pp. 84–93.

References VII

Daniel Wichs and Giorgos Zirdelis, *Obfuscating compute-and-compare programs under LWE*, 58th FOCS (Chris Umans, ed.), IEEE Computer Society Press, October 2017, pp. 600–611.