Lower Bounds for Lattice-based Compact Functional Encryption

Erkan Tairi
TU Wien, Vienna, Austria
→
DIENS, École normale supérieure, CNRS, Inria, PSL University, Paris, France

Akın Ünal
ETH Zurich, Zurich, Switzerland
→
IST Austria, Klosterneuburg, Austria

Overview

- Motivation
- Our Framework: Lattice-Based FE
- Our Lower Bound
- Our Tool and Proof Strategy
- Open Questions & Limits

Functional Encryption

A functional encryption (FE) scheme is (Setup, KeyGen, Enc, Dec) …

Functional Encryption

A functional encryption (FE) scheme is (Setup, KeyGen, Enc, Dec) …

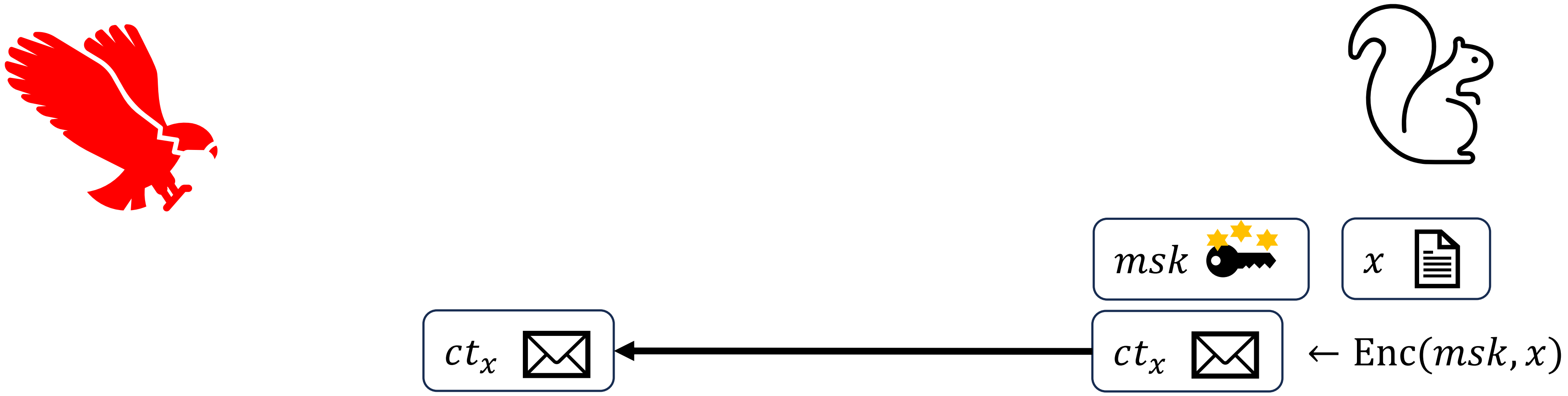
… you all know it by now.

(Symmetric) Functional Encryption

Functional encryption scheme FE=(Setup, KeyGen, Enc, Dec)

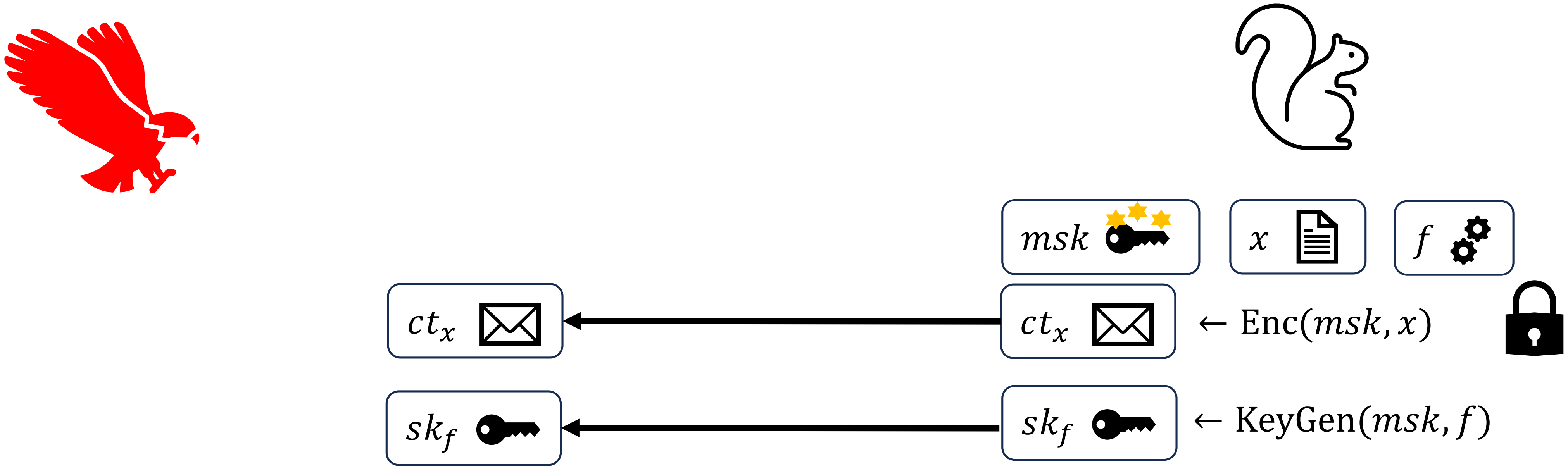
(Symmetric) Functional Encryption

Functional encryption scheme FE=(Setup, KeyGen, Enc, Dec)



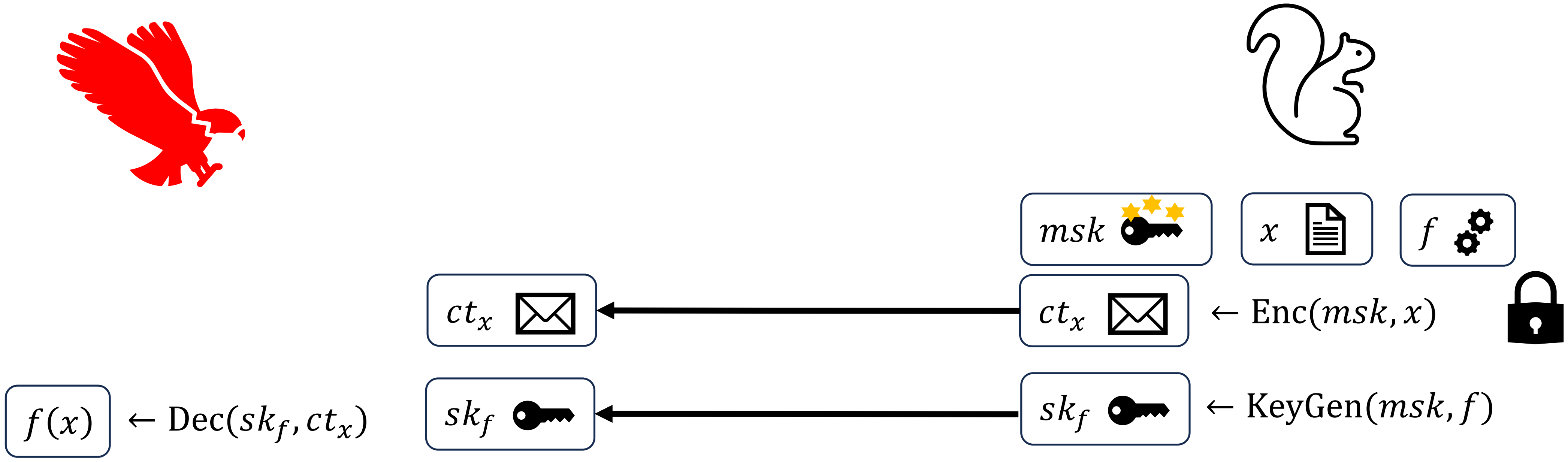
(Symmetric) Functional Encryption

Functional encryption scheme FE=(Setup, KeyGen, Enc, Dec)



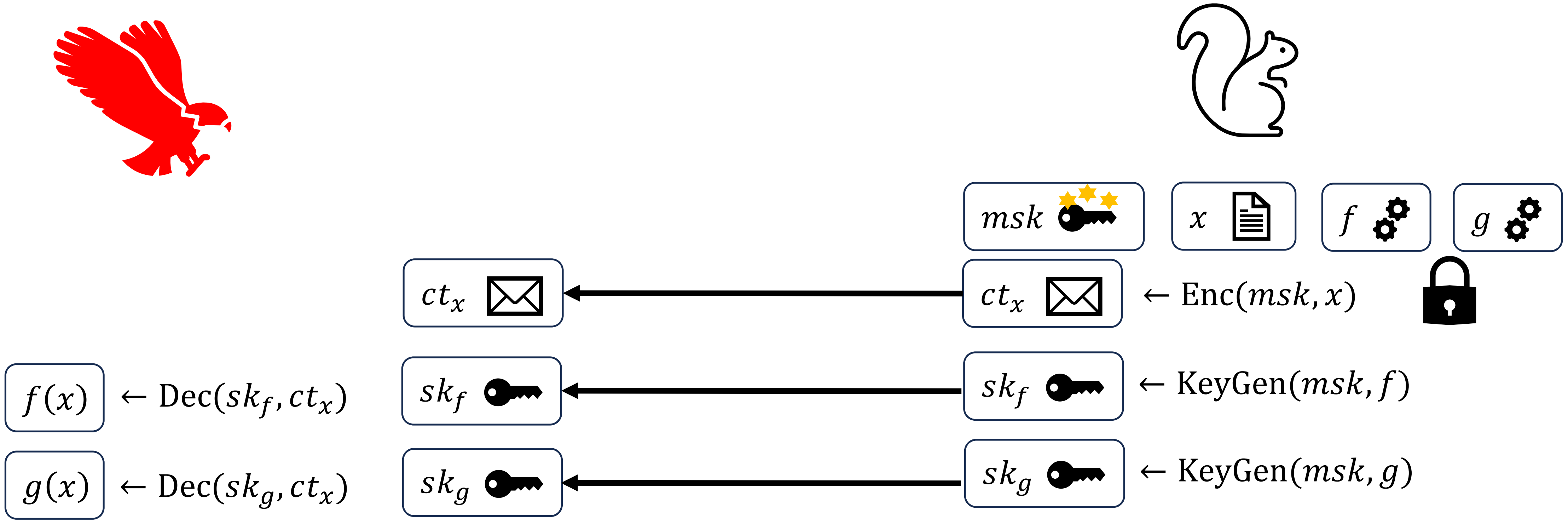
(Symmetric) Functional Encryption

Functional encryption scheme FE=(Setup, KeyGen, Enc, Dec)



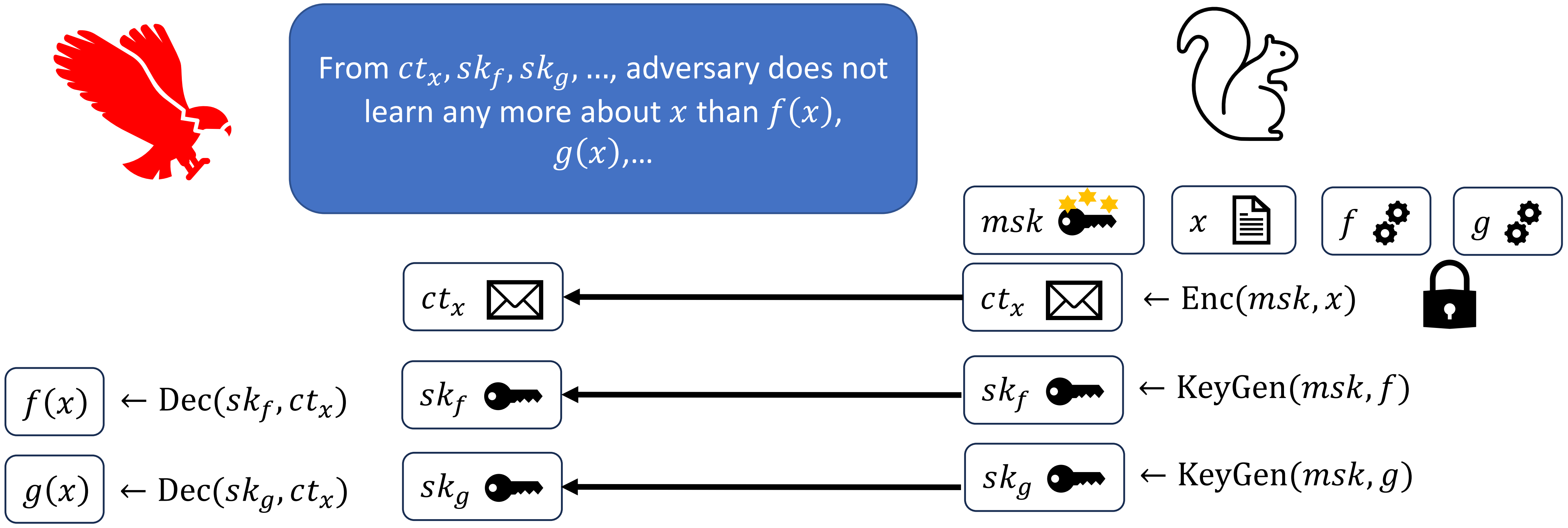
(Symmetric) Functional Encryption

Functional encryption scheme FE=(Setup, KeyGen, Enc, Dec)



(Symmetric) Functional Encryption

Functional encryption scheme FE=(Setup, KeyGen, Enc, Dec)



Important Terms

IND-CPA Security under Unbounded Collusions

Inner-Product Encryption / Linear FE

Quadratic FE

Important Terms

IND-CPA Security under Unbounded Collusions

An unbounded number of secret keys $sk_{f_1}, \ldots, sk_{f_Q}$ does not help at distinguishing ct_{x_1}, ct_{x_2} as long as $\forall i \in [Q]$: $f_i(x_1) = f_i(x_2)$.

Inner-Product Encryption / Linear FE

Quadratic FE

Important Terms

IND-CPA Security under Unbounded Collusions

An unbounded number of secret keys $sk_{f_1}, \dots, sk_{f_Q}$ does not help at distinguishing ct_{x_1}, ct_{x_2} as long as $\forall i \in [Q]$: $f_i(x_1) = f_i(x_2)$.

Inner-Product Encryption / Linear FE

FE schemes supports secret keys for linear functions:

$$f : \mathbb{Z}_p^n \to \mathbb{Z}_p, \qquad f(X) = \alpha_1 \cdot X_1 + \cdots + \alpha_n X_n$$

Quadratic FE

Important Terms

IND-CPA Security under Unbounded Collusions

An unbounded number of secret keys $sk_{f_1}, \dots, sk_{f_Q}$ does not help at distinguishing ct_{x_1}, ct_{x_2} as long as $\forall i \in [Q]$: $f_i(x_1) = f_i(x_2)$.

Inner-Product Encryption / Linear FE

FE schemes supports secret keys for linear functions:

$$f: \mathbb{Z}_p^n \to \mathbb{Z}_p, \qquad f(X) = \alpha_1 \cdot X_1 + \cdots + \alpha_n X_n$$

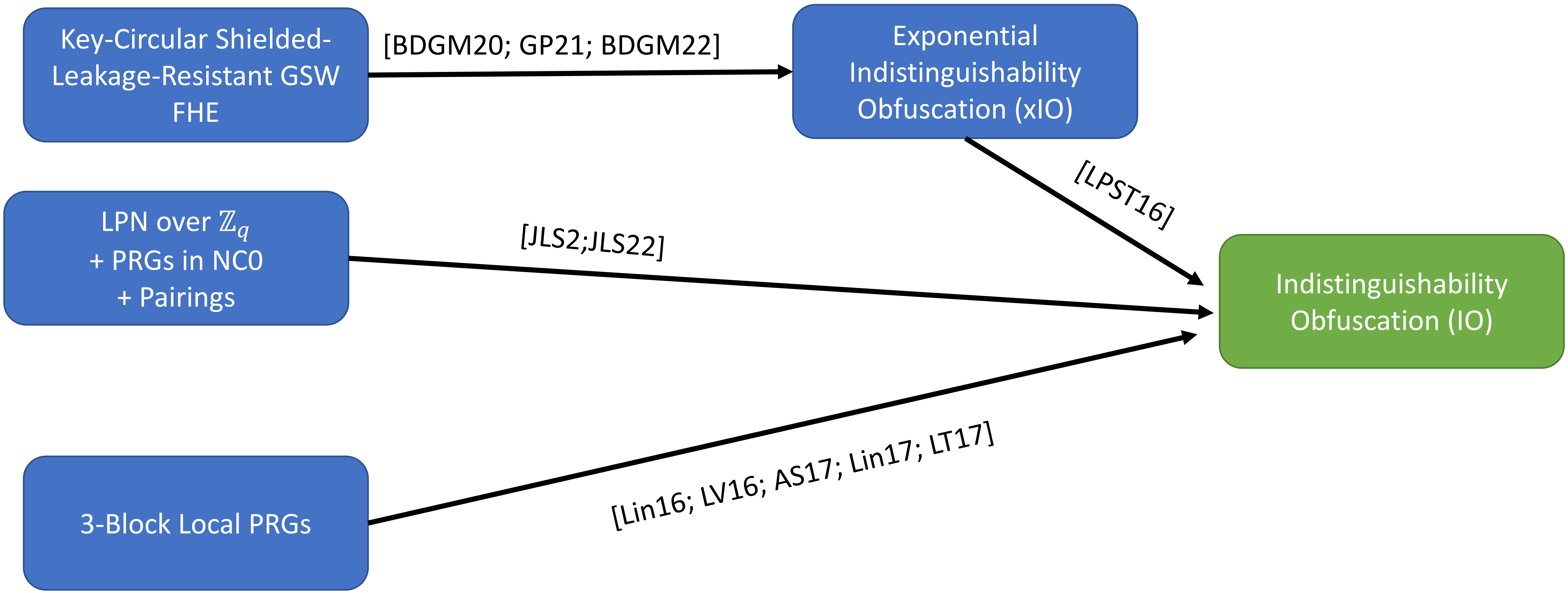
Quadratic FE

FE schemes can hand out secret keys for degree-2 functions

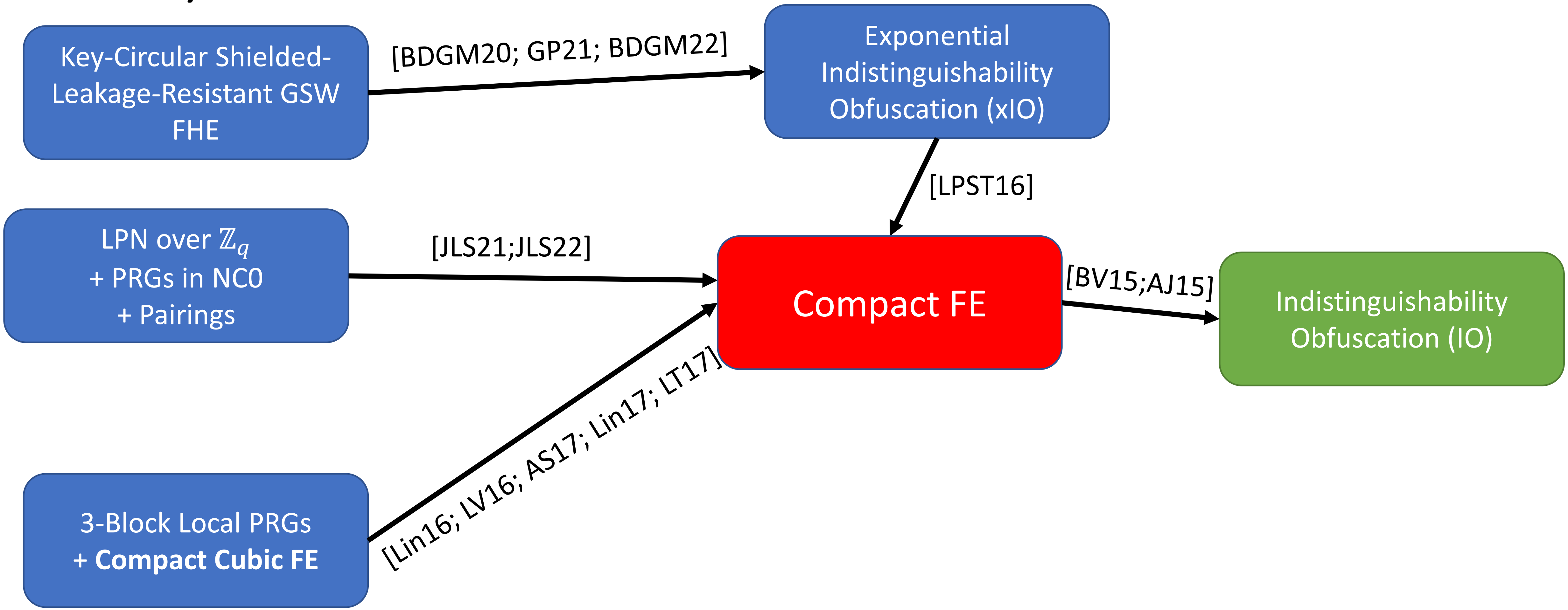
$$f: \mathbb{Z}_p^n \to \mathbb{Z}_p, \qquad f(X) = \sum_{1 \le i \le j \le n} \alpha_{i,j} \cdot X_i \cdot X_j$$

Why?

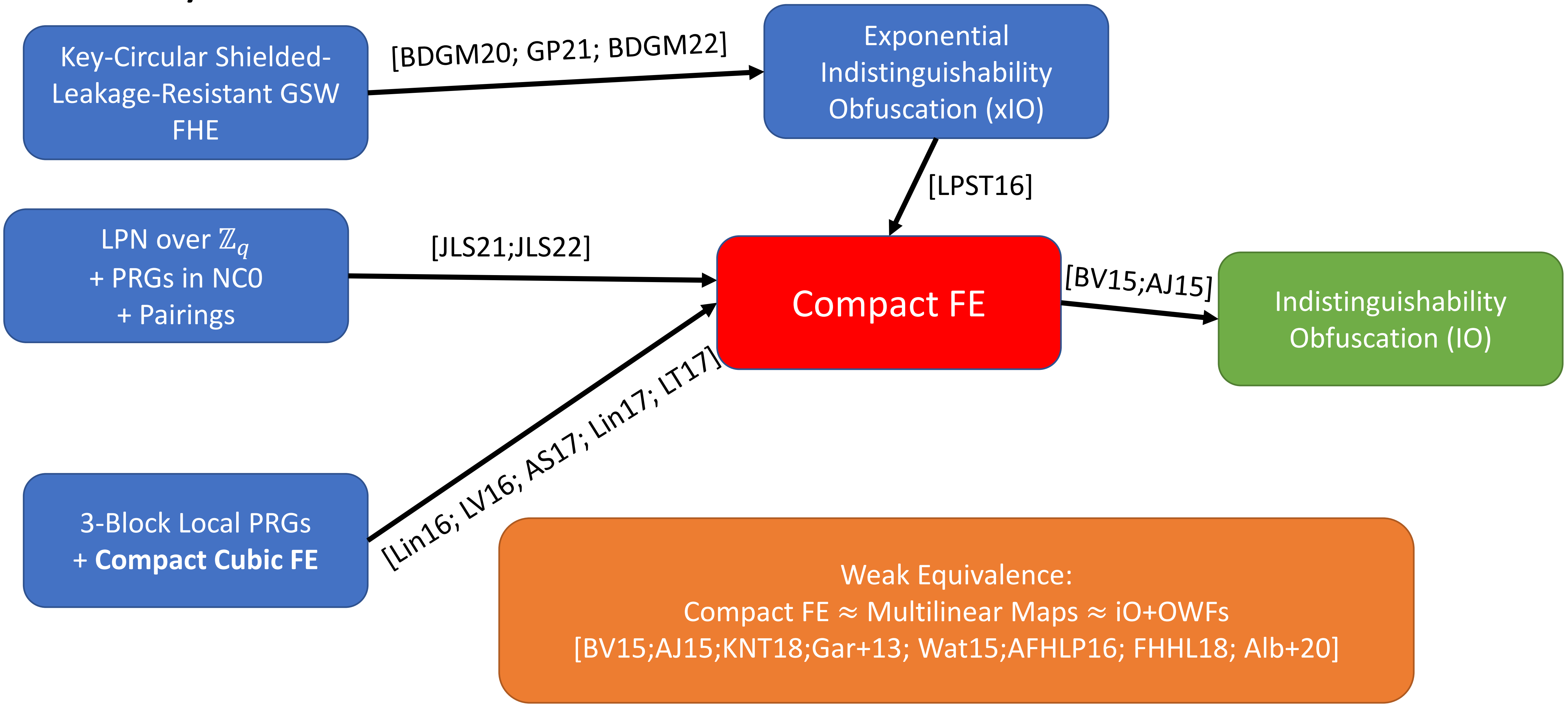
Why? Obfuscation!



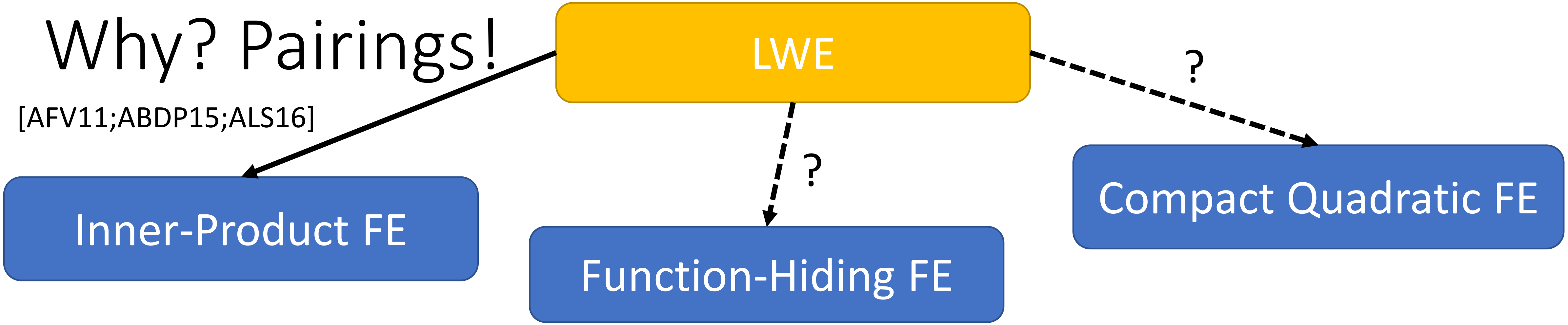
Why? Obfuscation!



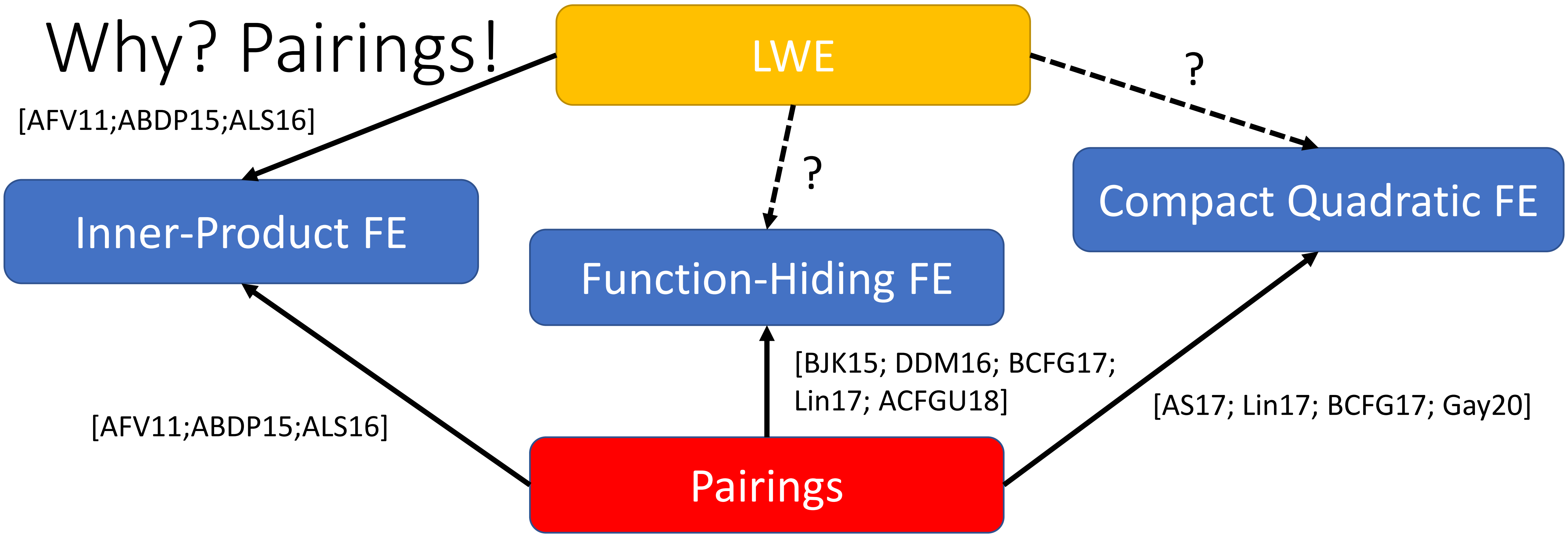
Why? Obfuscation!



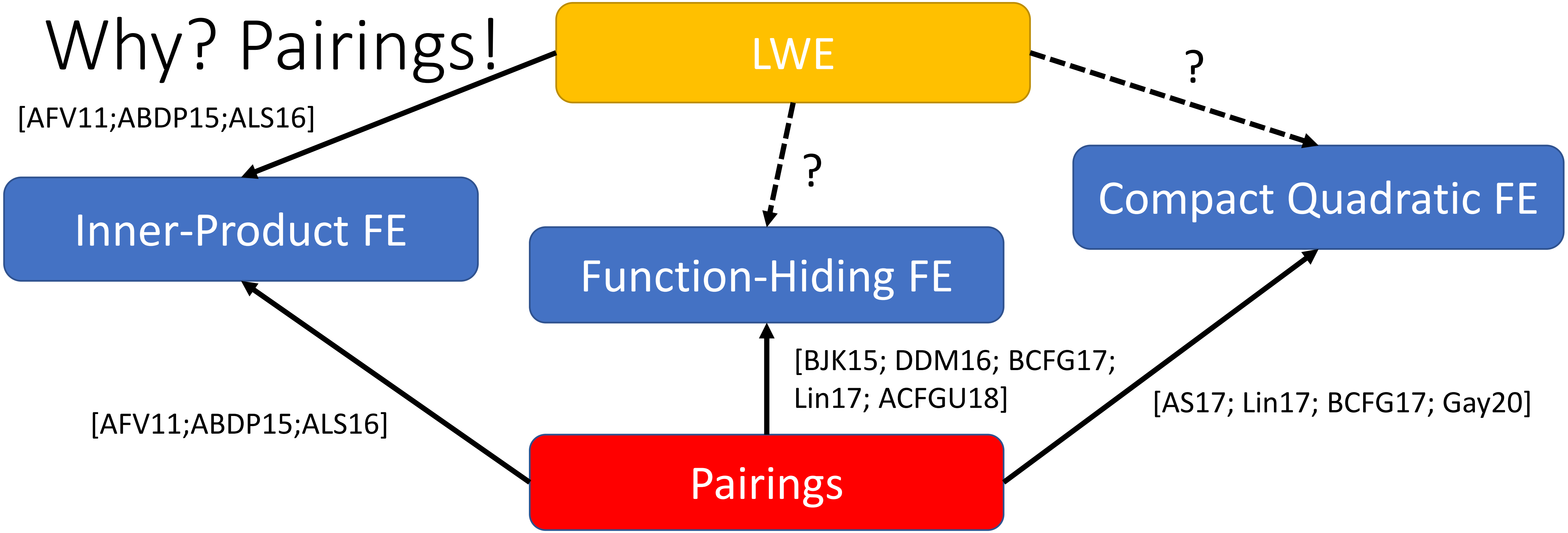
Why? Pairings!



Why? Pairings!



Why? Pairings!



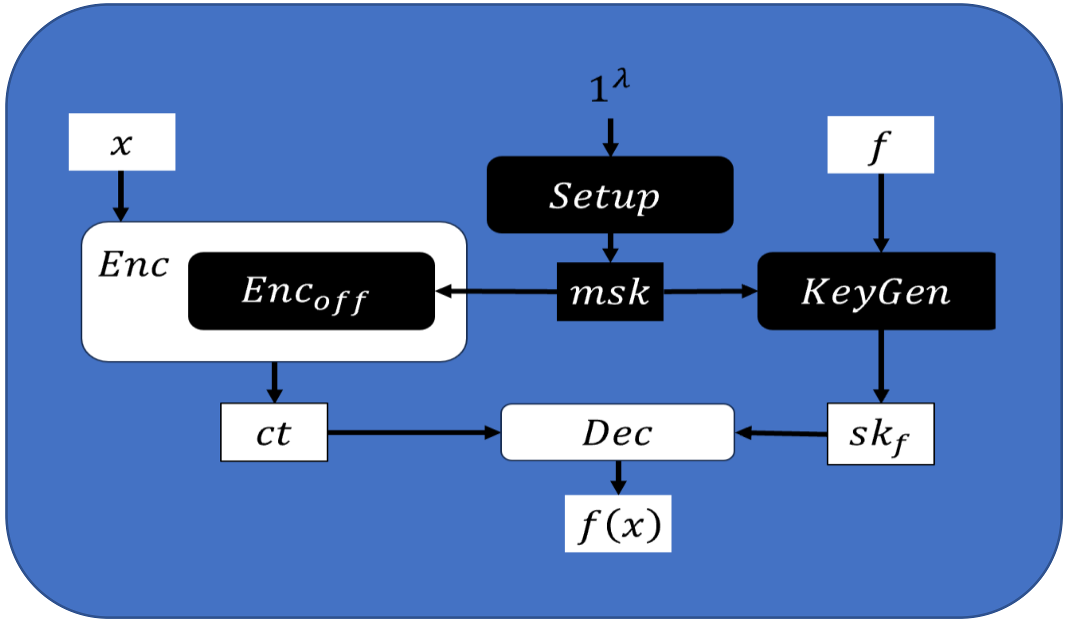
What are inherit limits to the power of LWE and other lattice-based Assumptions?

Our Results

- Revisit a Framework [Üna20] for Lattice-Based FE
- Prove Lower Bounds for Lattice-Based Quadratic Compact FE

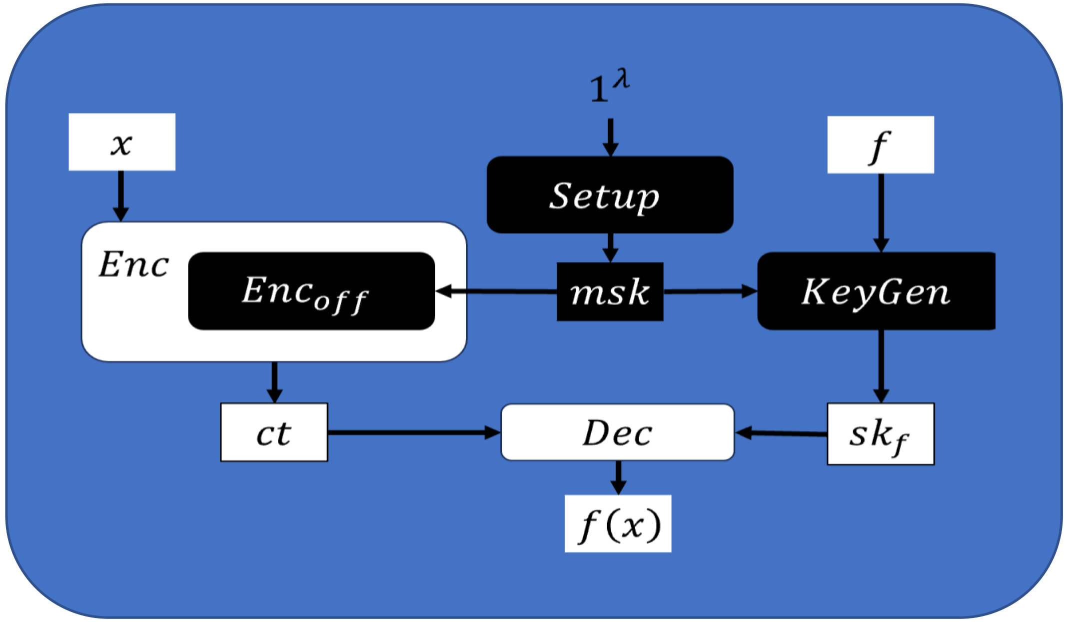
Our Results

- Revisit a Framework [Üna20] for Lattice-Based FE
- Prove Lower Bounds for Lattice-Based Quadratic Compact FE
  - Lower Bound is Not Black-Box



Our Results

- Revisit a Framework [Üna20] for Lattice-Based FE
- Prove Lower Bounds for Lattice-Based Quadratic Compact FE
  - Lower Bound is Not Black-Box
  - Result is agnostic to Assumptions (RingLWE, EvasiveLWE)



Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

- Ciphertexts are vectors $ct \in \mathbb{Z}_q^m$.

Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

- Ciphertexts are vectors $ct \in \mathbb{Z}_q^m$.
- Secret keys are polynomials $sk \in \mathbb{Z}_q[C_1, \dots, C_m]$ of constant degree.

Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

- Ciphertexts are vectors $ct \in \mathbb{Z}_q^m$.
- Secret keys are polynomials $sk \in \mathbb{Z}_q[C_1, \ldots, C_m]$ of constant degree.
- Dec(sk, ct) works by

$$\mathrm{Dec}(sk, ct) = \left\lfloor \frac{p}{q} \cdot sk(ct) \right\rceil \in \mathbb{Z}_p$$

Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

- Ciphertexts are vectors $ct \in \mathbb{Z}_q^m$.
- Secret keys are polynomials $sk \in \mathbb{Z}_q[C_1, \ldots, C_m]$ of constant degree.
- Dec(sk, ct) works by

$$\mathrm{Dec}(sk, ct) = \left\lfloor \frac{p}{q} \cdot sk(ct) \right\rceil \in \mathbb{Z}_p$$

- Enc(msk, x) is *offline / online of constant depth.*

Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

- Ciphertexts are vectors $ct \in \mathbb{Z}_q^m$.
- Secret keys are polynomials $sk \in \mathbb{Z}_q[C_1, \dots, C_m]$ of constant degree.
- Dec(sk, ct) works by

$$\mathrm{Dec}(sk, ct) = \left\lfloor \frac{p}{q} \cdot sk(ct) \right\rceil \in \mathbb{Z}_p$$

- Enc(msk, x) is *offline / online of constant depth.*

Framework captures most Lattice-Based Schemes.

Framework for Lattice-Based FE

FE=(Setup, KeyGen, Enc, Dec) is **lattice-based** if:

- Ciphertexts are vectors $ct \in \mathbb{Z}_q^m$.
- Secret keys are polynomials $sk \in \mathbb{Z}_q[C_1, \ldots, C_m]$ of constant degree.
- Dec(sk, ct) works by

$$\mathrm{Dec}(sk, ct) = \left\lfloor \frac{p}{q} \cdot sk(ct) \right\rceil \in \mathbb{Z}_p$$

- Enc(msk, x) is *offline / online of constant depth.*

Framework captures most Lattice-Based Schemes.

Exception: Fully Homomorphic Encryption, Bit-Decomposition

Our Theorem

Let FE=(Setup, KeyGen, Enc, Dec) be a Quadratic FE Scheme s.t.

- FE is *lattice-based*
- Ciphertexts are *linearly* compact, i.e., $m \in O(n)$
- Secret Keys are of *minimal* degree 2

Then, FE is either not IND-CPA secure or not correct.

Our Tool [Üna20, myPhDThesis]

Lemma

Let SKE=(Enc, Dec) be an SKE scheme for messages $x \in \mathbb{Z}_p$.

If

- each ciphertext ct_x lies in $\mathbb{Z}_q^m$,
- Enc is *offline / online of constant depth,*
- each ciphertext ct_x has a *short norm*

$$\|ct_x\| < B \in o(q),$$

then SKE is either not IND-CPA secure or not correct.

Our Tool [Üna20, myPhDThesis]

Lemma
Let SKE=(Enc, Dec) be an SKE scheme for messages $x \in \mathbb{Z}_p$.
If

- each ciphertext ct_x lies in $\mathbb{Z}_q^m$,
- Enc is *offline / online of constant depth,*
- each ciphertext ct_x has a *short norm*

$$\|ct_x\| < B \in o(q),$$

then SKE is either not IND-CPA secure or not correct.

There is no simple Encryption Scheme with Short Ciphertexts.

Our Tool [Üna20, myPhDThesis]

Lemma

Let SKE=(Enc, Dec) be an SKE scheme for messages $x \in \mathbb{Z}_p$.

If

- each ciphertext ct_x lies in $\mathbb{Z}_q^m$,
- Enc is *offline / online of constant depth,*
- each ciphertext ct_x has a *short norm*

$$\|ct_x\| < B \in o(q),$$

then SKE is either not IND-CPA secure or not correct.

Even Non-Negligible Correctness is not allowed.

Our Tool [Üna20, myPhDThesis]

Lemma
Let SKE=(Enc, Dec) be an SKE scheme for messages $x \in \mathbb{Z}_p$.
If

- each ciphertext ct_x lies in $\mathbb{Z}_q^m$,
- Enc is *offline / online of constant depth,*
- each ciphertext ct_x has a *short norm*

$$\|ct_x\| < B \in o(q),$$

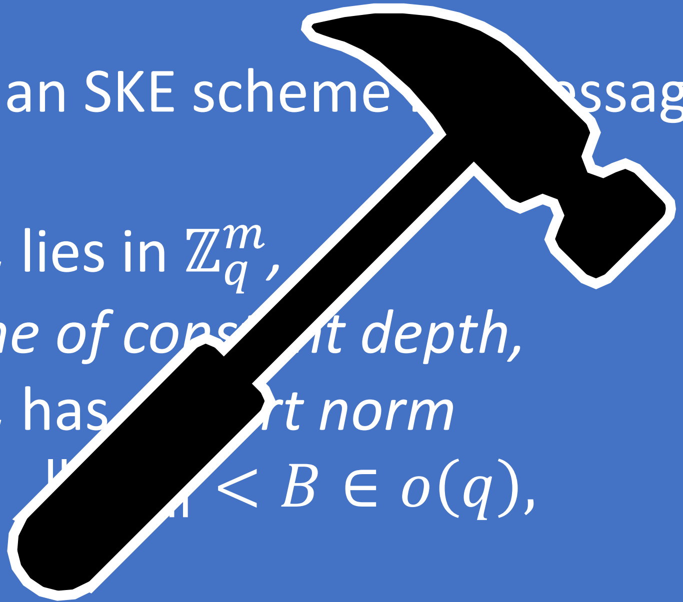
then SKE is either not IND-CPA secure or not correct.

Even Non-Negligible Correctness is not allowed.

Dec does not even need to be computable.

Our Tool [Üna20, myPhDThesis]

Lemma



Let SKE=(Enc, Dec) be an SKE scheme ... ssages $x \in \mathbb{Z}_p$.

If

- each ciphertext ct_x lies in $\mathbb{Z}_q^m$,
- Enc is *offline / online of cons... t depth,*
- each ciphertext ct_x has ... *rt norm*

$$\| ... \| < B \in o(q),$$

then SKE is either not IND-CPA secure or not correct.

Even Non-Negligible Correctness is not allowed.

Dec does not even need to be computable.

Our Proof Strategy

FE for deg-2 functions
- lattice-based
- linearly compact
- deg-2 Secret keys

↑

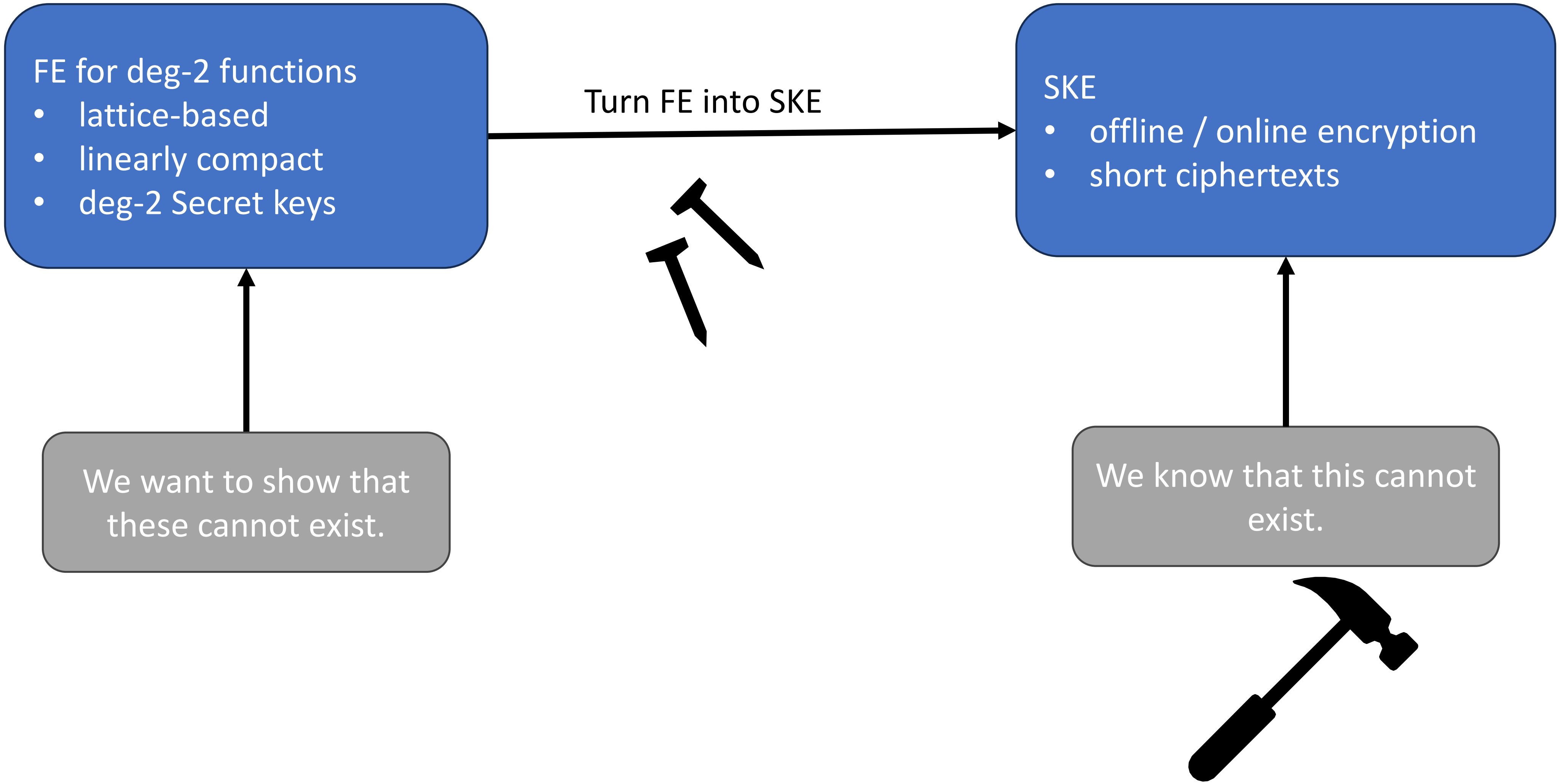
We want to show that these cannot exist.

SKE
- offline / online encryption
- short ciphertexts

↑

We know that this cannot exist.

Our Proof Strategy



Function Collection

FE=(Setup, KeyGen, Enc, Dec) Compact Quadratic FE

Function Collection

FE=(Setup, KeyGen, Enc, Dec) Compact Quadratic FE

For $1 \leq i < j \leq n$, set

$$f_{i,j}(X) \coloneqq X_i \cdot X_j$$

Function Collection

FE=(Setup, KeyGen, Enc, Dec) Compact Quadratic FE

For $1 \leq i < j \leq n$, set

$$f_{i,j}(X) \coloneqq X_i \cdot X_j$$

Each secret key

$$sk_{i,j} \leftarrow \mathrm{KeyGen}\left(msk, f_{i,j}\right)$$

is a deg-2 polynomial in $\mathbb{Z}_q[C_1, \dots, C_m]$

Function Collection

FE=(Setup, KeyGen, Enc, Dec) Compact Quadratic FE

For $1 \leq i < j \leq n$, set

$$f_{i,j}(X) \coloneqq X_i \cdot X_j$$

Each secret key

$$sk_{i,j} \leftarrow \mathrm{KeyGen}\left(msk, f_{i,j}\right)$$

is a deg-2 polynomial in $\mathbb{Z}_q[C_1, \ldots, C_m]$

We have for all $x \in \mathbb{Z}_p$

$$f_{i,j}(x, 1,0, \ldots, 0) = \begin{cases} x, & \text{if } (i,j) = (1,2) \\ 0, & \text{if } (i,j) \neq (1,2) \end{cases}$$

SKE Scheme SKE‘ = (Enc‘, Dec‘)

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\text{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \text{KeyGen}(msk, f_{i,j})$

Sample $ct \leftarrow \text{Enc}(msk, (x, 1, 0, \ldots, 0))$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \ldots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\mathrm{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \mathrm{KeyGen}\left(msk, f_{i,j}\right)$

Sample $ct \leftarrow \mathrm{Enc}\left(msk, (x, 1,0, \ldots, 0)\right)$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \ldots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

SKE’ is secure,
because FE is secure and

$$f_{i,j}(x, 1,0, \ldots, 0) = 0$$

for all $(i, j) \neq (1,2)$.

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\mathrm{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \mathrm{KeyGen}\big(msk, f_{i,j}\big)$

Sample $ct \leftarrow \mathrm{Enc}\big(msk, (x, 1,0, \ldots, 0)\big)$

Output $ct' \coloneqq \Big(sk_{2,3}(ct), \ldots, sk_{n-1,n}(ct)\Big) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

SKE’ is secure,
because FE is secure and

$$f_{i,j}(x, 1,0, \ldots, 0) = 0$$

for all $(i,j) \neq (1,2)$.

$\|ct'\|$ is short, because

$$0 = f_{i,j}(x, 1,0, \ldots 0) =$$

$$\mathrm{Dec}\big(sk_{i,j}, ct\big) = \left\lfloor sk_{i,j}(ct) \cdot \frac{p}{q} \right\rceil$$

for $(i,j) \neq (1,2)$.

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\text{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \text{KeyGen}(msk, f_{i,j})$

Sample $ct \leftarrow \text{Enc}(msk, (x, 1,0, \dots, 0))$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

$\text{Dec}'(msk, ct')$:

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\mathrm{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \mathrm{KeyGen}(msk, f_{i,j})$

Sample $ct \leftarrow \mathrm{Enc}(msk, (x, 1, 0, \ldots, 0))$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \ldots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

$\mathrm{Dec}'(msk, ct')$:

How do we compute $sk_{1,2}(ct)$ from $sk_{2,3}(ct)$,..., $sk_{n-1,n}(ct)$?

SKE Scheme SKE' = (Enc', Dec')

$\text{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \text{KeyGen}\left(msk, f_{i,j}\right)$

Sample $ct \leftarrow \text{Enc}\left(msk, (x, 1, 0, \ldots, 0)\right)$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \ldots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

$\text{Dec}'(msk, ct')$:

How do we compute $sk_{1,2}(ct)$ from $sk_{2,3}(ct), \ldots, sk_{n-1,n}(ct)$?

Use an Algebraic Relationship!

Algebraic Relations

- We have $\binom{n}{2} = \Theta(n^2)$ many polynomials $sk_{i,j} \in \mathbb{Z}_q[C_1, \ldots, C_m]$
- of degree 2
- over $m = O(n)$ variables.

Algebraic Relations

- We have $\binom{n}{2} = \Theta(n^2)$ many polynomials $sk_{i,j} \in \mathbb{Z}_q[C_1, \ldots, C_m]$
- of degree 2
- over $m = O(n)$ variables.

Theorem [Üna23] $\Rightarrow$
$sk_{1,2}, \ldots, sk_{n-1,n}$ admit an *algebraic relationship* h of constant degree.

Algebraic Relations

- We have $\binom{n}{2} = \Theta(n^2)$ many polynomials $sk_{i,j} \in \mathbb{Z}_q[C_1, \dots, C_m]$
- of degree 2
- over $m = O(n)$ variables.

Theorem [Üna23] $\Rightarrow$
$sk_{1,2}, \dots, sk_{n-1,n}$ admit an *algebraic relationship* h of constant degree.

I.e., there exists $h \in \mathbb{Z}_q\left[Y_{1,2}, \dots, Y_{n-1,n}\right]$ s.t.

$$h \neq 0,$$
$$h\left(sk_{1,2}(C), \dots, sk_{n-1,n}(C)\right) = 0,$$
$$\deg h \in O(1).$$

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\text{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \text{KeyGen}(msk, f_{i,j})$

Sample $ct \leftarrow \text{Enc}(msk, (x, 1,0, \dots, 0))$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

$\text{Dec}'(msk, ct')$:

Compute relationship $h(S_{1,2}, \dots, S_{n-1,n})$ among $sk_{i,j}$

Set $g(S_{1,2}) \coloneqq h\left(S_{1,2}, sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\right)$

Output $\left\lfloor r \cdot \frac{p}{q} \right\rfloor$ for $r \leftarrow g^{-1}(0)$.

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\text{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \text{KeyGen}\big(msk, f_{i,j}\big)$

Sample $ct \leftarrow \text{Enc}\big(msk, (x, 1,0, \dots, 0)\big)$

Output $ct' \coloneqq \big(sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\big) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

$g\left(sk_{1,2}(ct)\right) = h\left(sk_{1,2}(ct), \dots, sk_{n-1,n}(ct)\right) = 0$

$\text{Dec}'(msk, ct')$:

Compute relationship $h\big(S_{1,2}, \dots, S_{n-1,n}\big)$ among $sk_{i,j}$

Set $g(S_{1,2}) \coloneqq h\left(S_{1,2}, sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\right)$

Output $\left\lfloor r \cdot \frac{p}{q} \right\rceil$ for $r \leftarrow g^{-1}(0)$.

SKE Scheme SKE‘ = (Enc‘, Dec‘)

$\mathrm{Enc}'(msk, x)$:

Draw $sk_{i,j} \leftarrow \mathrm{KeyGen}\left(msk, f_{i,j}\right)$

Sample $ct \leftarrow \mathrm{Enc}\left(msk, (x, 1,0, \dots, 0)\right)$

Output $ct' \coloneqq \left(sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\right) \in \mathbb{Z}_q^{\binom{n}{2}-1}$

$g\left(sk_{1,2}(ct)\right) = h\left(sk_{1,2}(ct), \dots, sk_{n-1,n}(ct)\right) = 0$

$\mathrm{Dec}'(msk, ct')$:

Compute relationship $h\left(S_{1,2}, \dots, S_{n-1,n}\right)$ among $sk_{i,j}$

Set $g(S_{1,2}) \coloneqq h\left(S_{1,2}, sk_{2,3}(ct), \dots, sk_{n-1,n}(ct)\right)$

Output $\left\lfloor r \cdot \frac{p}{q} \right\rceil$ for $r \leftarrow g^{-1}(0)$.

Dec$\left(sk_{1,2}, ct\right) = \left\lfloor \frac{p}{q} \cdot sk_{1,2}(ct) \right\rceil = f_{1,2}(x, 1,0, \dots) = x$

SKE Scheme SKE‘ = (Enc‘, Dec‘)

Result

Quadratic FE, which is

- *Lattice-Based*
- *Linearly Compact* $m \in O(n)$
- Has Secret Keys of *Minimal* Degree 2

cannot Exist!

$ct)\big) = 0$

Output $\left\lfloor r \cdot \frac{p}{q} \right\rceil$ for $r \leftarrow g^{-1}(0)$.

$\mathrm{Dec}\big(sk_{1,2}, ct\big) = \left\lfloor \frac{p}{q} \cdot sk_{1,2}(ct) \right\rceil = f_{1,2}(x, 1{,}0, \dots) = x$

Open Questions & Limits

What about relaxed Parameters?

- (Relaxed) Compactness $m \in O\left(n^{2-\epsilon}\right)$
- Secret Keys of Any Constant Degree

$\Rightarrow$ New Methods necessary…

Open Questions & Limits

What about relaxed Parameters?

- (Relaxed) Compactness $m \in O\left(n^{2-\epsilon}\right)$
- Secret Keys of Any Constant Degree

⇒ New Methods necessary…

How can we cirumvent this result?

- Use FHE (Bit-Decomposition)
- What about $p = 2$?

Function-Hiding IPE for $p = 2$???

Can we have a *Binary Multiplication Scheme*?

- Keyed Distributions $Enc_0(msk), Enc_1(msk)$ over $\mathbb{Z}_q^m$
- Keyed Distributions $SK_0(msk), SK_1(msk)$ over $\mathbb{Z}_q^m$

Such that

- Given $Enc_0(msk)$, $\quad SK_0(msk) \approx_c SK_1(msk)$
- Given $SK_0(msk)$, $\quad Enc_0(msk) \approx_c Enc_1(msk)$
- For all $a, b \in \{0,1\}$, $ct \leftarrow Enc_a(msk)$, $sk \leftarrow SK_b(msk)$

$$\langle ct|sk\rangle = \begin{cases} \text{small if } & a \cdot b = 0 \\ \text{large if } & a \cdot b = 1 \end{cases}$$

Thank you for your Attention!!

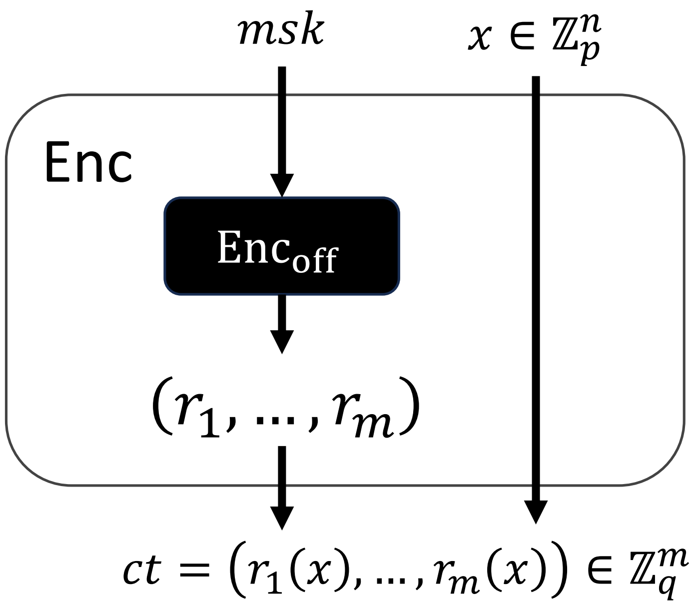
https://ia.cr/2023/719

(also, my phd thesis sooooooooon………)

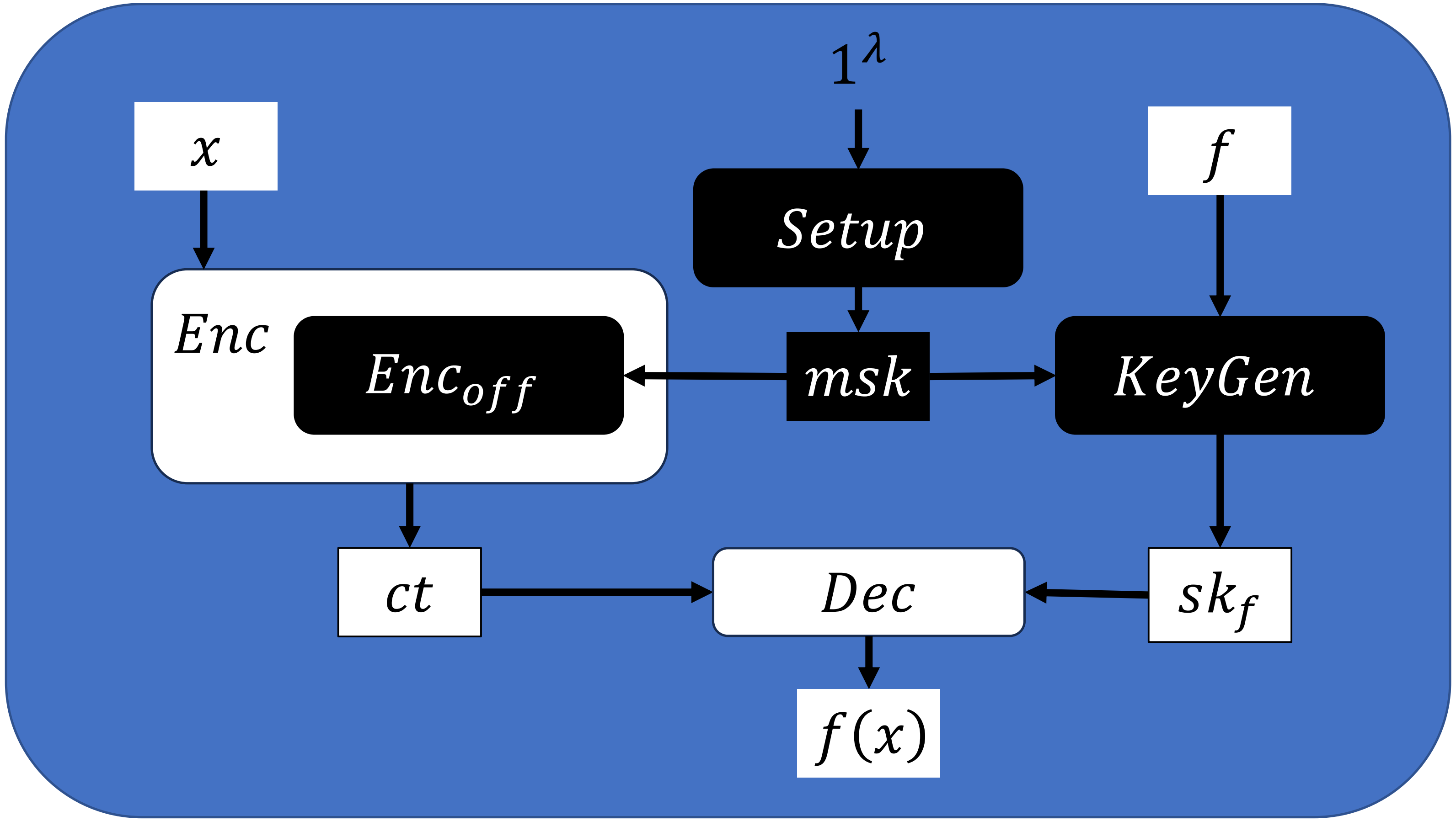
Offline / Online Encryption

- Messages are integer vectors $\{0, \ldots, p-1\}^n$.
- $\mathrm{Enc}(msk, x)$ has complex offline phase $\mathrm{Enc}_{\mathrm{off}}(msk)$, and a simple online phase (where it sees x and output of offline phase).

$r_1, \ldots, r_m \in \mathbb{Z}_q[X_1, \ldots, X_n]$ are polynomials of *constant* degree d.
d is the *depth* of Enc.



Black and White Boxes



More Limits on Lower Bounds for FE

- Time complexity of attack lies in $poly\left(\frac{q}{p}\right)$.
- q needs to be prime.
- $p \in \omega(1)$ needs to be larger than some constant.
- Bit-decomposition / inverse gadget-sampling is not covered by our model of *lattice-based* FE.
- Double Modulus at Decryption is not covered:

$$Dec(sk, ct) = \big((sk(ct)\ mod\ q)\ mod\ p'\big)\ mod\ p$$

The Ugly Details

- What if the algebraic relationship h among the secret keys is (almost) always zero?
- Homogeneity among Ciphertexts:
  For each message pair x, y: each low-degree polynomial g vanishes on $ct_x \leftarrow \text{Enc}(msk, x)$ with owp iff it vanishes on ct_y with owp.
- For Homogeneity, we need that $\deg h$ is constant.
- For that, we need linear compactness + minimal sk degree.

Can we do better?

Yes, but we need more polynomials $h_1, \ldots, h_\ell$ and better handling of probablities....

Algebraic Relationships [Üna23,myPhdThesis]

$f_1(X,Y) = X \cdot Y$ $\quad$ $f_2(X,Y) = X^2$ $\quad$ $f_3(X,Y) = Y^2$

$$h(T_1, T_2, T_3) = T_1^2 - T_2 \cdot T_3$$

$h\big(f_1(X,Y), f_2(X,Y), f_3(X,Y)\big) = 0$

Refutation

Does there exist $(x, y) \in \mathbb{R}^2$ s.t.

$$f_1(x,y) = 1$$
$$f_2(x,y) = 1$$
$$f_3(x,y) = 2 \quad ?$$

No, because $h(1,1,2) = 1^2 - 1 \cdot 2 = -1 \neq 0$!

Prediction

What values for $f_1(x,y)$ are possible if

$$f_2(x,y) = 2$$
$$f_3(x,y) = 2 \quad ?$$

$f_1(x,y) = \pm 2$, because $h(f_1(x,y), 2,2) = 0$.

Algebraic Relationships [Üna23,myPhdThesis]

$f_1(X,Y) = X \cdot Y$ $\quad$ $f_2(X,Y) = X^2$ $\quad$ $f_3(X,Y) = Y^2$

$h(f_1(X,Y), f_2(X,Y), f_3(X,Y)) = 0$

$$h(T_1, T_2, T_3) = T_1^2 - T_2 \cdot T_3$$

Refutation

Prediction

Do

ssible if

$= 0.$

Theorem

If $m \geq n^{1+e}$ and $\deg f_1, \ldots, \deg f_m \leq d$,

then an algebraic relationship h of degree $O\left(n^{1-\frac{e}{d-1}}\right)$ exists.

Intuition for Lower Bounds for FE

- We ask for keys for a lot of *useless* functions $f_{i,j}$.
  $\Rightarrow$ Noise of *useless* functions leaks *useful* information.

Example: $f_1 = X_1$, $f_2 = X_2$, $f_3 = X_1 \cdot X_2$. We have $f_1 = \frac{f_3}{f_2}$.

$f \mapsto sk_f$ is somewhat homomorphic. $\Rightarrow sk_{f_1} = \frac{sk_{f_3}}{sk_{f_2}}$.

Not a problem if decryption is noise-free: $ct \leftarrow \mathrm{Enc}\big(msk, (1,0)\big)$

$sk_{f_2}(ct) = 0, sk_{f_3}(ct) = 0 \Rightarrow sk_{f_1}(ct) = \frac{0}{0}$

In lattice-Setting, decryption is noisy:

$sk_{f_2}(ct) = \varepsilon_2 \neq 0, sk_{f_3}(ct) = \varepsilon_3 \neq 0 \Rightarrow sk_{f_1}(ct) = \frac{\varepsilon_3}{\varepsilon_2}$

Example: Function-Hiding IPE [Üna20]

- *Function-Hiding:* sk_f hides the function f it evaluates.
- Use embedding $\nu: \mathbb{Z}_p \to \mathbb{Z}_p^n$
$$\nu(x') = (x', 0, \dots, 0)$$
- Use function collection $f_1, \dots, f_Q, f_*$
$$f_1(X) = \cdots = f_Q(X) = 0$$
$$f_*(X) = X_1$$
- For $sk_1, \dots, sk_Q \leftarrow$KeyGen$(msk, 0)$ and Q large enough, we have
$$\Pr_{sk_* \leftarrow KeyGen(msk, f_*)}\left[sk_* \in span\left(sk_1, \dots, sk_Q\right)\right]$$
$$\approx \Pr_{sk_0 \leftarrow KeyGen(msk, 0)}\left[sk_0 \in span\left(sk_1, \dots, sk_Q\right)\right] \geq 1 - o(1)$$

Example: Function-Hiding IPE [Üna20]

- *Fu*
- Us
- Us

Reconstruction

$$sk_* = \alpha_1 \cdot sk_1 + \cdots + \alpha_Q \cdot sk_Q$$
$$\Rightarrow$$
$$sk_*(ct) = \alpha_1 \cdot sk_1(ct) + \cdots + \alpha_Q \cdot sk_Q(ct)$$

- For $sk_1, \dots, sk_Q$ ←KeyGen$(msk, 0)$ and Q large enough, we have

$$\Pr_{sk_* \leftarrow KeyGen(msk, f_*)}\left[sk_* \in span(sk_1, \dots, sk_Q)\right]$$
$$\approx \Pr_{sk_0 \leftarrow KeyGen(msk, 0)}\left[sk_0 \in span(sk_1, \dots, sk_Q)\right] \geq 1 - o(1)$$