Efficient KDM-CCA Secure Public-Key Encryption for Polynomial Functions

Shuai Han, Shengli Liu, and Lin Lyu

1. Shanghai Jiao Tong University
2. State Key Laboratory of Cryptology
3. Westone Cryptologic Research Center

Asiacrypt 2016, Hanoi, Vietnam

Key-Dependent Message

- KDM security: allow adversary to access encryptions of messages, which are closely dependent on the secret keys.

$$\mathsf{Enc}(\mathsf{pk}, f(\mathsf{sk}))$$

Key-Dependent Message

- KDM security: allow adversary to access encryptions of messages, which are closely dependent on the secret keys.

$$\mathsf{Enc}(\mathsf{pk}, f(\mathsf{sk}))$$

- Applications:
  - Hard disk encryption
  - Anonymous credential system

Key-Dependent Message

- KDM security: allow adversary to access encryptions of messages, which are closely dependent on the secret keys.

$$\mathsf{Enc}(\mathsf{pk}, f(\mathsf{sk}))$$

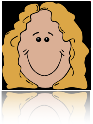
- Applications:
  - Hard disk encryption
  - Anonymous credential system

- Traditional security notion does not imply KDM security.
  [ABBC'10, CGH'12, MO'14, BHW'15, KRW'15, KW'16, AP'16] $\cdots$

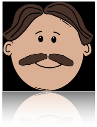
Public-Key Encryption

PKE = (Setup, Gen, Enc, Dec):

$(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$



Alice



Bob

Public-Key Encryption

PKE = (Setup, Gen, Enc, Dec):

$(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$

pke.ct

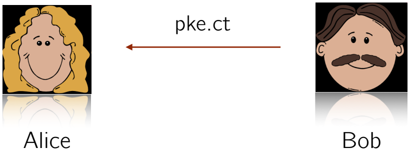
$\mathsf{pke.ct} \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}, m)$

Alice

Bob

Public-Key Encryption

$\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:



$(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$

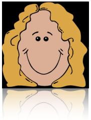
$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{pke.ct})$

$\mathsf{pke.ct}$

$\mathsf{pke.ct} \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{m})$

KDM Security

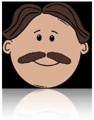
$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$



User 1

$\cdots$

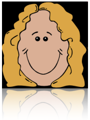
$(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$



User i

$\cdots$

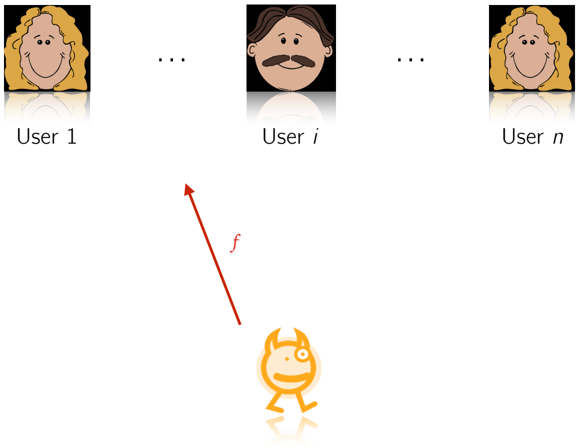
$(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$



User n

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

KDM Security



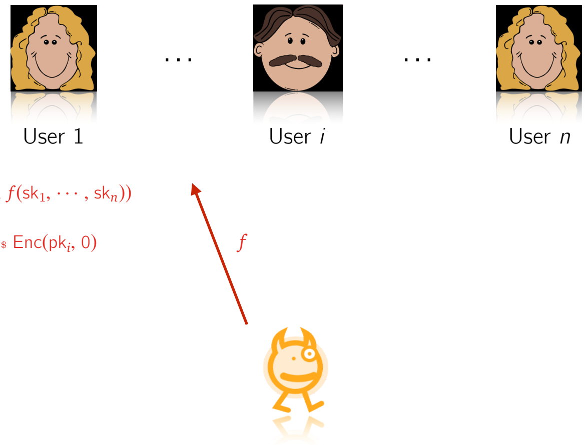
$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$

User 1 $\cdots$ User *i* $\cdots$ User *n*

f

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

KDM Security



$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_\$ \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_\$ \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_\$ \mathsf{Gen}(\mathsf{prm})$

User 1 ⋯ User *i* ⋯ User *n*

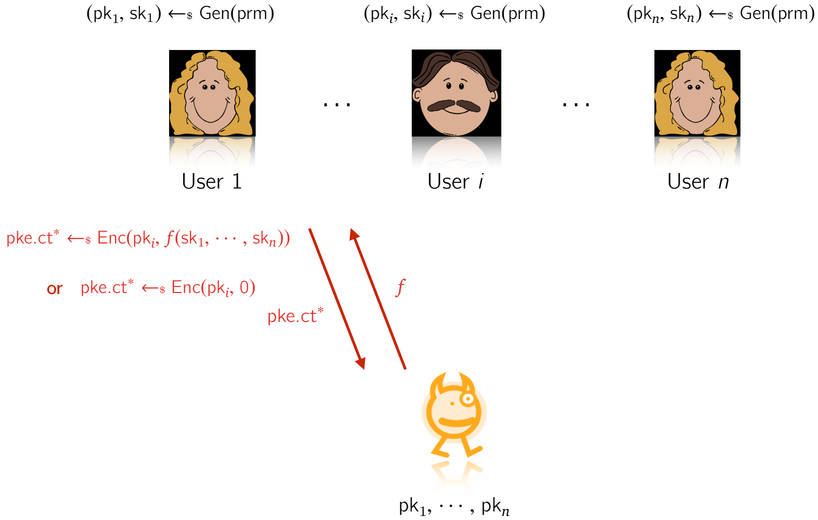
$\mathsf{pke.ct}^* \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}_i, f(\mathsf{sk}_1, \cdots, \mathsf{sk}_n))$

or $\mathsf{pke.ct}^* \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}_i, 0)$

f

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

KDM Security



$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$

User 1 $\cdots$ User i $\cdots$ User n

$\mathsf{pke.ct}^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}_i, f(\mathsf{sk}_1, \cdots, \mathsf{sk}_n))$

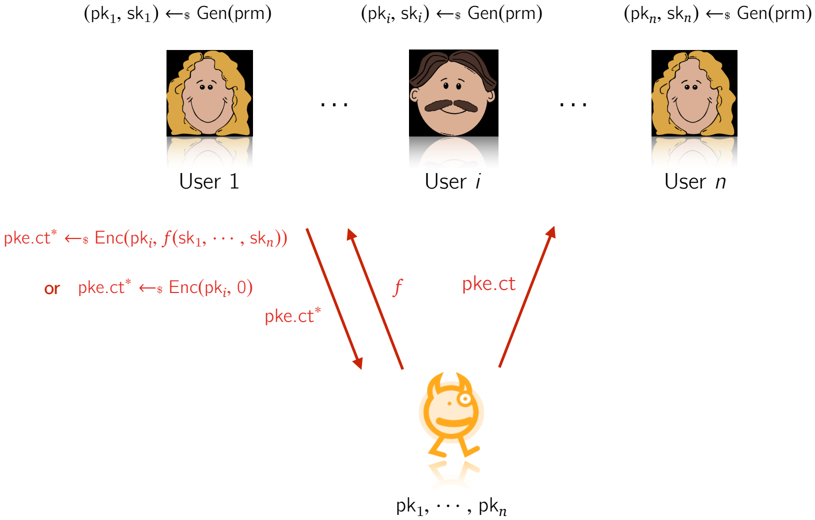
or $\mathsf{pke.ct}^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}_i, 0)$

$\mathsf{pke.ct}^*$

f

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

KDM Security



$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_\$ \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_\$ \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_\$ \mathsf{Gen}(\mathsf{prm})$

User 1

User i

User n

$\mathsf{pke.ct}^* \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}_i, f(\mathsf{sk}_1, \cdots, \mathsf{sk}_n))$

or $\mathsf{pke.ct}^* \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}_i, 0)$

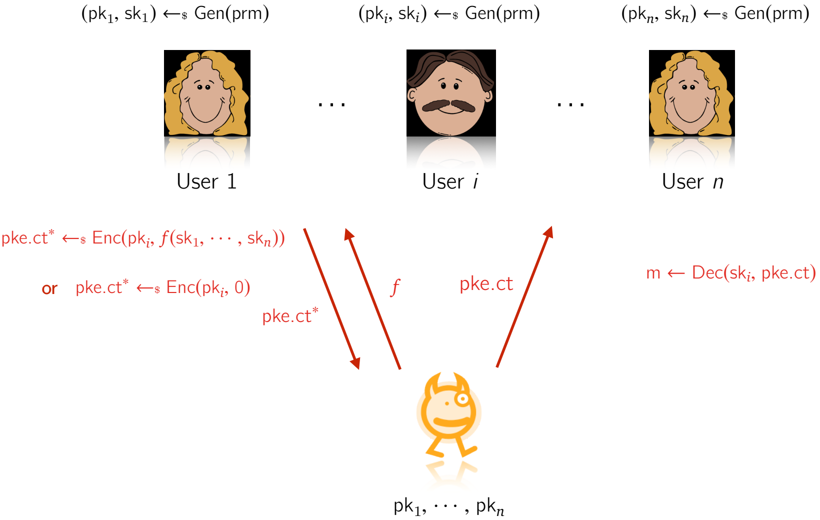
$\mathsf{pke.ct}^*$

f

$\mathsf{pke.ct}$

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

KDM Security



$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $\cdots$ $(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$

User 1 User i User n

$\mathsf{pke.ct}^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}_i, f(\mathsf{sk}_1, \cdots, \mathsf{sk}_n))$

or $\mathsf{pke.ct}^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}_i, 0)$

$\mathsf{pke.ct}^*$

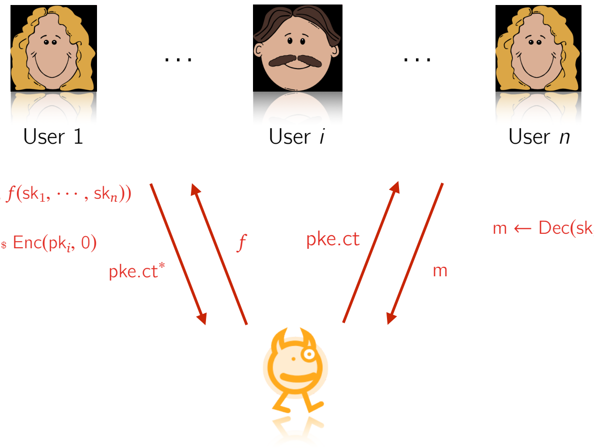
f

$\mathsf{pke.ct}$

$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_i, \mathsf{pke.ct})$

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

KDM Security



$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$ $(\mathsf{pk}_n, \mathsf{sk}_n) \leftarrow_{\$} \mathsf{Gen}(\mathsf{prm})$

User 1 $\cdots$ User i $\cdots$ User n

$\mathsf{pke.ct}^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}_i, f(\mathsf{sk}_1, \cdots, \mathsf{sk}_n))$

or $\mathsf{pke.ct}^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}_i, 0)$

$\mathsf{pke.ct}^*$

f

pke.ct

m

$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_i, \mathsf{pke.ct})$

$\mathsf{pk}_1, \cdots, \mathsf{pk}_n$

Function Set of KDM Security

KDM security is related to a set of functions $\mathcal{F}$ from $\mathcal{SK} \times \cdots \times \mathcal{SK}$ to $\mathcal{M}$.

- $\mathcal{F}_{\mathsf{circ}}$: the set of selection functions.

$$f : (\mathsf{sk}_1, \cdots, \mathsf{sk}_n) \longmapsto \mathsf{sk}_i$$

- $\mathcal{F}_{\mathsf{aff}}$: the set of affine functions.

$$f : (\mathsf{sk}_1, \cdots, \mathsf{sk}_n) \longmapsto \sum_{i=1}^{n} a_i \cdot \mathsf{sk}_i + b$$

- $\mathcal{F}_{\mathsf{poly}}^{d}$: the set of polynomial functions of bounded degree d.

$$f : (\mathsf{sk}_1, \cdots, \mathsf{sk}_n) \longmapsto \sum_{0 \le c_1 + \cdots + c_n \le d} a_{(c_1, \cdots, c_n)} \cdot \mathsf{sk}_1^{c_1} \cdots \mathsf{sk}_n^{c_n}$$

Function Set of KDM Security

KDM security is related to a set of functions $\mathcal{F}$ from $\mathcal{SK} \times \cdots \times \mathcal{SK}$ to $\mathcal{M}$.

- $\mathcal{F}_{\mathsf{circ}}$: the set of selection functions.

$$f : (\mathsf{sk}_1, \cdots, \mathsf{sk}_n) \longmapsto \mathsf{sk}_i$$

- $\mathcal{F}_{\mathsf{aff}}$: the set of affine functions.

$$f : (\mathsf{sk}_1, \cdots, \mathsf{sk}_n) \longmapsto \sum_{i=1}^{n} a_i \cdot \mathsf{sk}_i + b$$

- $\mathcal{F}^{d}_{\mathsf{poly}}$: the set of polynomial functions of bounded degree d.

$$f : (\mathsf{sk}_1, \cdots, \mathsf{sk}_n) \longmapsto \sum_{0 \le c_1 + \cdots + c_n \le d} a_{(c_1, \cdots, c_n)} \cdot \mathsf{sk}_1^{c_1} \cdots \mathsf{sk}_n^{c_n}$$

The larger $\mathcal{F}$ is, the stronger the security is.

Related Works: KDM-CPA secure PKE

PKE Scheme	KDM-CPA Function Set	KDM-CCA?	|Ciphertext|	Assumption
[BHHO'08], [BG'10]	$\mathcal{F}_{\mathsf{aff}}$	–	$O(\ell)\ \lvert\mathbb{G}\rvert$	DDH/QR/DCR
[ACPS'09]	$\mathcal{F}_{\mathsf{aff}}$	–	$O(1)\ \lvert\mathbb{G}\rvert$	LWE
[BGK'11]	$\mathcal{F}^{d}_{\mathsf{poly}}$	–	$O(\ell^{d+1})\ \lvert\mathbb{G}\rvert$	DDH/LWE
[MTY'11]	$\mathcal{F}^{d}_{\mathsf{poly}}$	–	$O(d)\ \lvert\mathbb{G}\rvert$	DCR

- ℓ: security parameter.
- d: bounded degree of polynomial functions.

Related Works: KDM-CCA secure PKE

PKE Scheme	KDM-CCA Function Set	KDM-CCA?	|Ciphertext|	Assumption
[BHHO'08] + [CCS'09]	$\mathcal{F}_{\text{aff}}$	√	$O(\ell)$ $\lvert\mathbb{G}\rvert$	DDH
[Hofheinz'13]	$\mathcal{F}_{\text{circ}}$	√	$O(1)$ $\lvert\mathbb{G}\rvert$	DDH & DCR
[LLJ'15]	$\mathcal{F}_{\text{aff}}$	?	$O(1)$ $\lvert\mathbb{G}\rvert$	DDH & DCR

- ℓ: security parameter.
- d: bounded degree of polynomial functions.

Our Contribution

PKE Scheme	KDM-CCA Function Set	KDM-CCA?	|Ciphertext|	Assumption
Our first scheme	$\mathcal{F}_{\mathsf{aff}}$	$\surd$	$O(1)\ \lvert\mathbb{G}\rvert$	DDH & DCR
Our second scheme	$\mathcal{F}_{\mathsf{poly}}^{d}$	$\surd$	$O(d^9)\ \lvert\mathbb{G}\rvert$	DDH & DCR

- We give the first efficient KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA secure PKE with compact ciphertexts.
  - Compact: the ciphertexts consist only a constant number of group elements.
  - Efficient: our scheme is free of NIZK and free of pairing.

Our Contribution

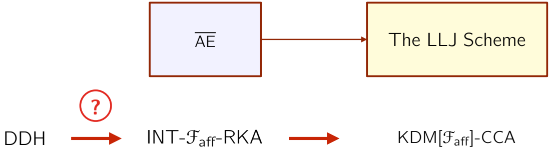
PKE Scheme	KDM-CCA Function Set	KDM-CCA?	|Ciphertext|	Assumption
Our first scheme	$\mathcal{F}_{\mathsf{aff}}$	$\surd$	$O(1)\ \lvert\mathbb{G}\rvert$	DDH & DCR
Our second scheme	$\mathcal{F}^{d}_{\mathsf{poly}}$	$\surd$	$O(d^9)\ \lvert\mathbb{G}\rvert$	DDH & DCR

- We give the first efficient KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA secure PKE with compact ciphertexts.
  - Compact: the ciphertexts consist only a constant number of group elements.
  - Efficient: our scheme is free of NIZK and free of pairing.
- We extend our technique, and construct the first efficient KDM[$\mathcal{F}^{d}_{\mathsf{poly}}$]-CCA secure PKE with almost compact ciphertexts.

Synopsis

1. The LLJ Scheme [Lu, Li and Jia, 2015]
2. Introducing: Authenticated Encryption with Auxiliary-Input
3. KDM-CCA secure PKE for Affine Functions
4. KDM-CCA secure PKE for Polynomial Functions

The LLJ Scheme from Related-Key Attack secure “$\overline{\text{AE}}$”



$\overline{\text{AE}}$

The LLJ Scheme

?

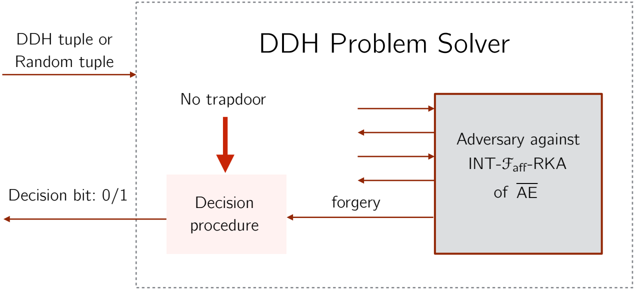
DDH

INT-$\mathcal{F}_{\text{aff}}$-RKA

KDM[$\mathcal{F}_{\text{aff}}$]-CCA

- One essential building block called “Authenticated Encryption” ($\overline{\text{AE}}$) is employed.
- The “INT-$\mathcal{F}_{\text{aff}}$-RKA” (ciphertext-integrity against related-key attacks) security proof of the LLJ’s $\overline{\text{AE}}$ does not go through to the DDH assumption.

INT-$\mathcal{F}_{\text{aff}}$-RKA security of LLJ's $\overline{\text{AE}}$



- LLJ's $\overline{\text{AE}}$: (ElGamal)-type.

$$(g^r, g^{kr}).$$

- The DDH adversary does not have any trapdoor to convert the forgery from the adversary of $\overline{\text{AE}}$ to a decision bit in an efficient way.

Synopsis

1. The LLJ Scheme [Lu, Li and Jia, 2015]
2. Introducing: Authenticated Encryption with Auxiliary-Input
3. KDM-CCA secure PKE for Affine Functions
4. KDM-CCA secure PKE for Polynomial Functions

A Plausible Solution

- Our new AIAE: (Kurosawa-Desmedt [KD'04])-type.

$$\left(g_1^r, g_2^r, g_1^{r(k_1+k_3t)}, g_2^{r(k_2+k_4t)}\right).$$

A Plausible Solution

- Our new AIAE: (Kurosawa-Desmedt [KD'04])-type.

$$\left(g_1^r, g_2^r, g_1^{r(k_1+k_3t)}, g_2^{r(k_2+k_4t)}\right).$$

New Problem!

The secret key of our AIAE consists of several elements $\mathsf{k} = (k_1, k_2, k_3, k_4)$.

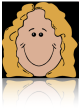
The affine function of k is too complicated to prove the INT-$\mathcal{F}_{\mathsf{aff}}$-RKA security.

$$f : (k_1, k_2, k_3, k_4) \longmapsto (\sum_{i=1}^{4} a_{i,1} \cdot k_i + b_1, \sum_{i=1}^{4} a_{i,2} \cdot k_i + b_2, \sum_{i=1}^{4} a_{i,3} \cdot k_i + b_3, \sum_{i=1}^{4} a_{i,4} \cdot k_i + b_4)$$

Our Solution: Authenticated Encryption with Auxiliary-Input

AIAE = (AIAE.Setup, AIAE.Enc, AIAE.Dec):

k



Alice

k

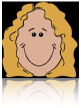
Bob

- We introduce "Authenticated Encryption with Auxiliary-Input" (AIAE).

Our Solution: Authenticated Encryption with Auxiliary-Input

AIAE = (AIAE.Setup, AIAE.Enc, AIAE.Dec):

k



Alice

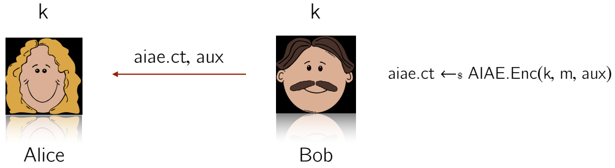
k

Bob

- We introduce “Authenticated Encryption with Auxiliary-Input” (AIAE).
  - AIAE must have auxiliary input “aux”.

Our Solution: Authenticated Encryption with Auxiliary-Input

AIAE = (AIAE.Setup, AIAE.Enc, AIAE.Dec):



k

k

aiae.ct, aux

aiae.ct $\leftarrow_{\$}$ AIAE.Enc(k, m, aux)

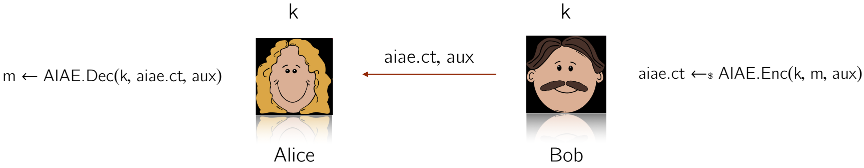
Alice

Bob

- We introduce "Authenticated Encryption with Auxiliary-Input" (AIAE).
    - AIAE must have auxiliary input "aux".

Our Solution: Authenticated Encryption with Auxiliary-Input

AIAE = (AIAE.Setup, AIAE.Enc, AIAE.Dec):



k

k

m ← AIAE.Dec(k, aiae.ct, aux)

aiae.ct, aux

aiae.ct $\leftarrow_{\$}$ AIAE.Enc(k, m, aux)

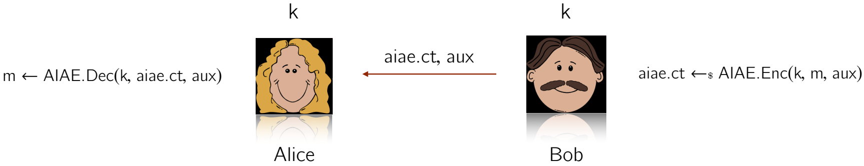
Alice

Bob

- We introduce "Authenticated Encryption with Auxiliary-Input" (AIAE).
  - AIAE must have auxiliary input "aux".

Our Solution: Authenticated Encryption with Auxiliary-Input

AIAE = (AIAE.Setup, AIAE.Enc, AIAE.Dec):



m $\leftarrow$ AIAE.Dec(k, aiae.ct, aux)

k

Alice

aiae.ct, aux

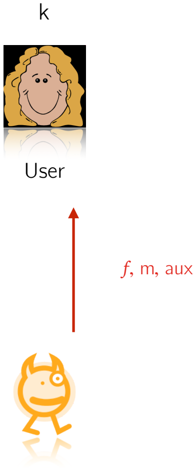
k

Bob

aiae.ct $\leftarrow_{\$}$ AIAE.Enc(k, m, aux)

- We introduce "Authenticated Encryption with Auxiliary-Input" (AIAE).
  - AIAE must have auxiliary input "aux".
  - Weak INT-$\mathcal{F}$-RKA security: an additional "special rule" for the forgery.

Weak INT-$\mathcal{F}$-RKA security for AIAE

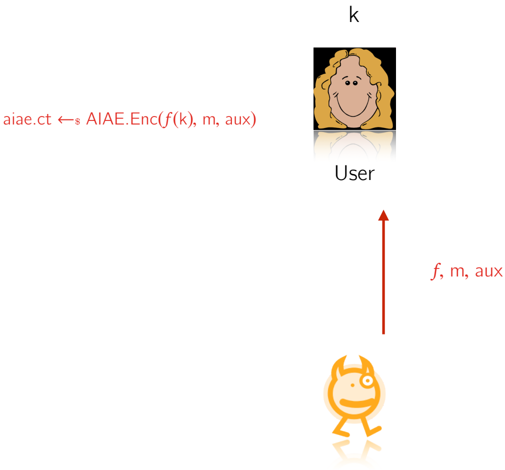


k

User

f, m, aux

Weak INT-$\mathcal{F}$-RKA security for AIAE



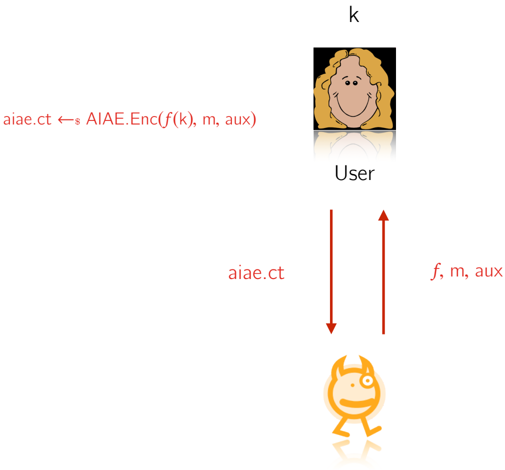
k

$\mathsf{aiae.ct} \leftarrow_{\$} \mathsf{AIAE.Enc}(f(\mathsf{k}), \mathsf{m}, \mathsf{aux})$

User

f, m, aux

Weak INT-$\mathcal{F}$-RKA security for AIAE



k

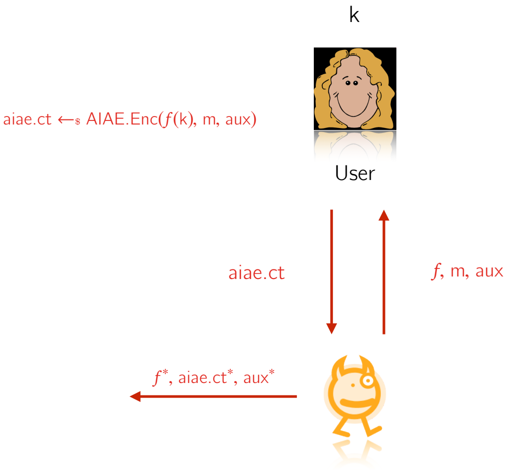
User

aiae.ct $\leftarrow_{\$}$ AIAE.Enc(f(k), m, aux)

aiae.ct

f, m, aux

Weak INT-$\mathcal{F}$-RKA security for AIAE



k

User

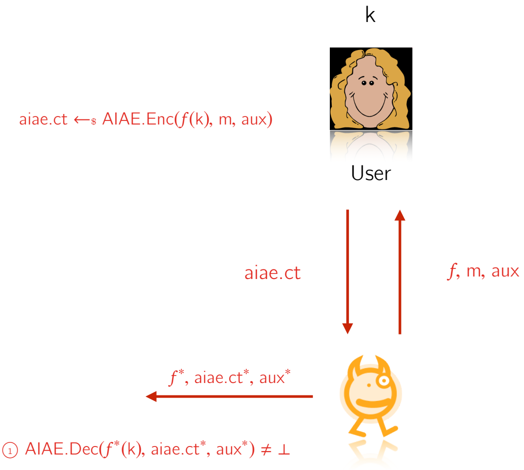
aiae.ct $\leftarrow_{\$}$ AIAE.Enc(f(k), m, aux)

aiae.ct

f, m, aux

f^*, aiae.ct*, aux*

Weak INT-$\mathcal{F}$-RKA security for AIAE



k

$\text{aiae.ct} \leftarrow_{\$} \text{AIAE.Enc}(f(\text{k}), \text{m}, \text{aux})$

User

aiae.ct

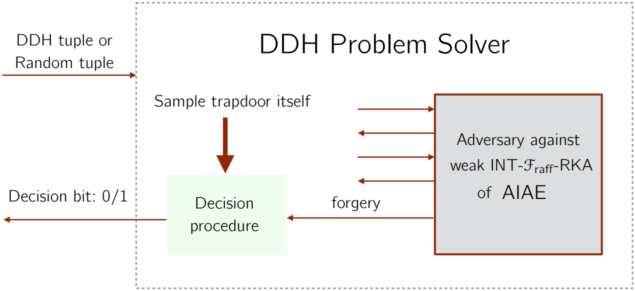
f, m, aux

f^*, aiae.ct*, aux*

① $\text{AIAE.Dec}(f^*(\text{k}), \text{aiae.ct}^*, \text{aux}^*) \neq \perp$

② Special rule

Our AIAE



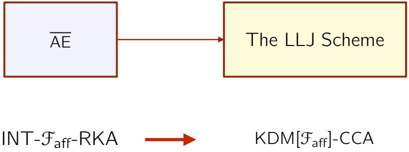
- We prove the weak INT-$\mathcal{F}_{\text{raff}}$-RKA security of our AIAE w.r.t. a smaller restricted affine function set $\mathcal{F}_{\text{raff}}$.

$$f : (k_1, k_2, k_3, k_4) \longmapsto (a \cdot k_1 + b_1, a \cdot k_2 + b_2, a \cdot k_3 + b_3, a \cdot k_4 + b_4)$$

Synopsis

1. The LLJ Scheme [Lu, Li and Jia, 2015]
2. Introducing: Authenticated Encryption with Auxiliary-Input
3. KDM-CCA secure PKE for Affine Functions
4. KDM-CCA secure PKE for Polynomial Functions

The LLJ's Method does not work for Our AIAE



$\overline{\mathsf{AE}}$ → The LLJ Scheme

INT-$\mathcal{F}_{\mathsf{aff}}$-RKA → KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA

- Our AIAE only achieves a very weak INT-$\mathcal{F}_{\mathsf{raff}}$-RKA security w.r.t. a small $\mathcal{F}_{\mathsf{raff}}$.

We cannot apply the LLJ's method to construct KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA secure PKE.

Our Approach

- Build KDM-CCA secure PKE from three building blocks: KEM, $\mathcal{E}$ and AIAE.
  - KEM: a key encapsulation mechanism.

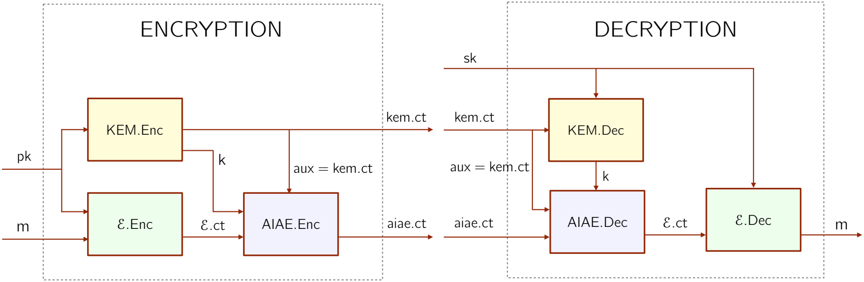
    $$(\mathsf{k}, \mathsf{kem.ct}) \leftarrow_{\$} \mathsf{KEM.Enc}(\mathsf{pk}), \qquad \mathsf{k} \leftarrow \mathsf{KEM.Dec}(\mathsf{sk}, \mathsf{kem.ct}).$$

  - $\mathcal{E}$: a public-key encryption scheme.

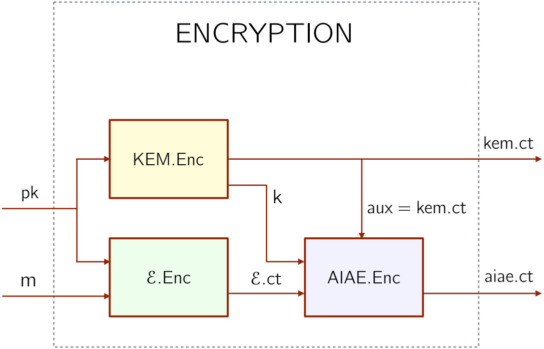
    $$\mathcal{E}.\mathsf{ct} \leftarrow_{\$} \mathcal{E}.\mathsf{Enc}(\mathsf{pk}, \mathsf{m}), \qquad \mathsf{m} \leftarrow \mathcal{E}.\mathsf{Dec}(\mathsf{sk}, \mathcal{E}.\mathsf{ct}).$$

  - AIAE: an authenticated encryption with auxiliary-input.

    $$\mathsf{AIAE.ct} \leftarrow_{\$} \mathsf{AIAE.Enc}(\mathsf{k}, \mathsf{m}, \mathsf{aux}), \qquad \mathsf{m} \leftarrow \mathsf{AIAE.Dec}(\mathsf{k}, \mathsf{AIAE.ct}, \mathsf{aux}).$$

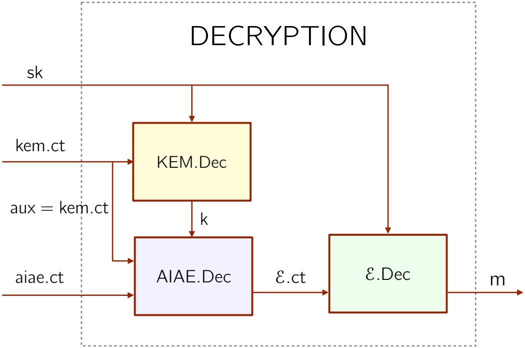


Our Construction



- KEM and $\mathcal{E}$ share the same key pair (pk, sk).
- AIAE.Enc uses k encapsulated by KEM to encrypt $\mathcal{E}$.ct with aux = kem.ct.

Our Construction

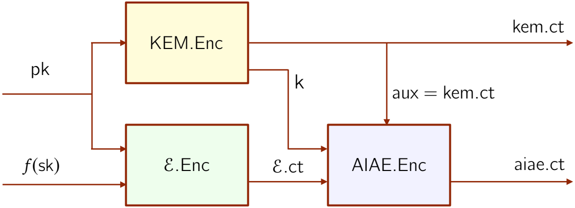


- KEM and $\mathcal{E}$ share the same key pair (pk, sk).

- AIAE.Enc uses k encapsulated by KEM to encrypt $\mathcal{E}$.ct with aux = kem.ct.

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

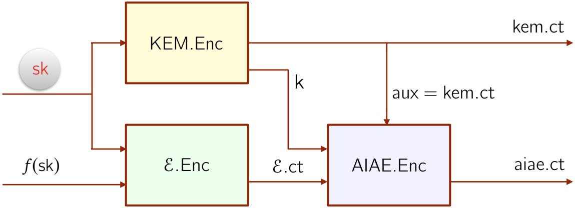
The Encryption Oracle:



- Divide the secret key sk to two independent parts, 🟦 sk mod N ▨ sk mod $\phi(N)$

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

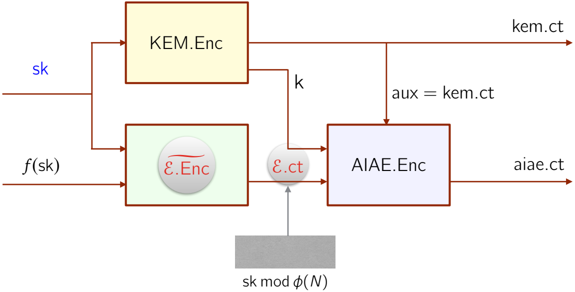
The Encryption Oracle:



- Use sk to answer the encryption queries.

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

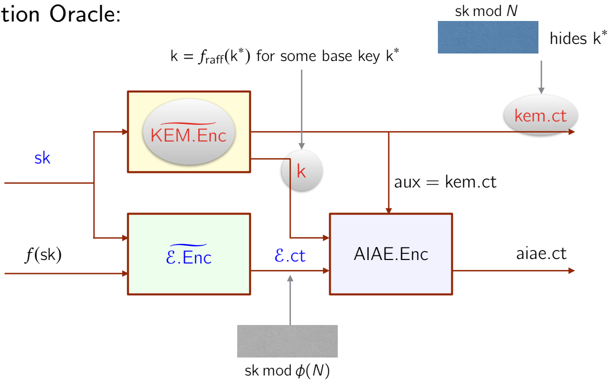
The Encryption Oracle:



- Under the DCR assumption, $\mathcal{E}.\mathsf{Enc}$ is changed to $\widetilde{\mathcal{E}.\mathsf{Enc}}$.
  - $\widetilde{\mathcal{E}.\mathsf{Enc}}$ behaves like an entropy filter for $\mathcal{F}_{\mathsf{aff}}$, such that $\underset{\text{sk mod } N}{▨}$ is reserved.

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

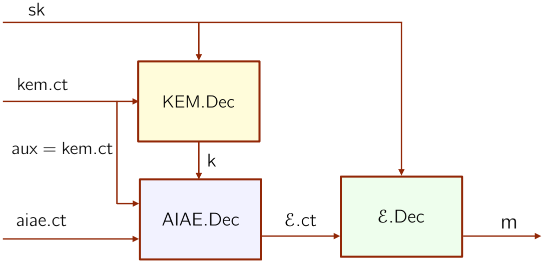
The Encryption Oracle:


sk mod N
hides k^*
$k = f_{\mathsf{raff}}(k^*)$ for some base key k^*
kem.ct
$\widetilde{\mathsf{KEM.Enc}}$
sk
k
aux = kem.ct
$f(\mathsf{sk})$
$\widetilde{\mathcal{E}.\mathsf{Enc}}$
$\mathcal{E}$.ct
AIAE.Enc
aiae.ct
sk mod $\phi(N)$

- Under the DCR assumption, KEM.Enc is changed to $\widetilde{\mathsf{KEM.Enc}}$.
  - k is expressed as an $\mathcal{F}_{\mathsf{raff}}$-function of a fixed base key k^*.
  - In kem.ct, ▨ protects the base key k^*.
    sk mod N

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

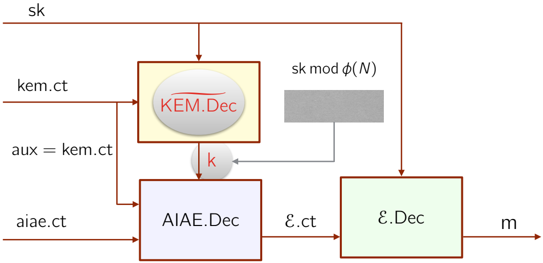
The Decryption Oracle:



- Divide the secret key sk to two independent parts, 🟦 sk mod N ▨ sk mod $\phi(N)$

Proof Idea of KDM[$\mathcal{F}_{\text{aff}}$]-CCA Security

The Decryption Oracle:



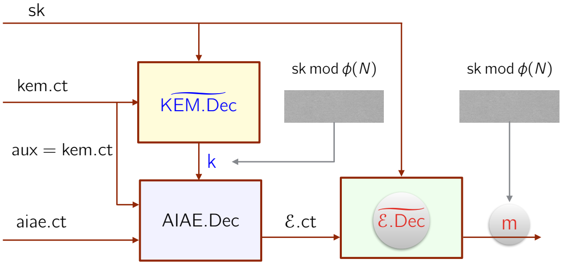
- $\widetilde{\text{KEM.Dec}}$ rejects the query, if the computation of k involves ▨ .

  sk mod N

  – By the weak INT-$\mathcal{F}_{\text{raff}}$-RKA security of AIAE, this change is computationally indistinguishable.

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

The Decryption Oracle:



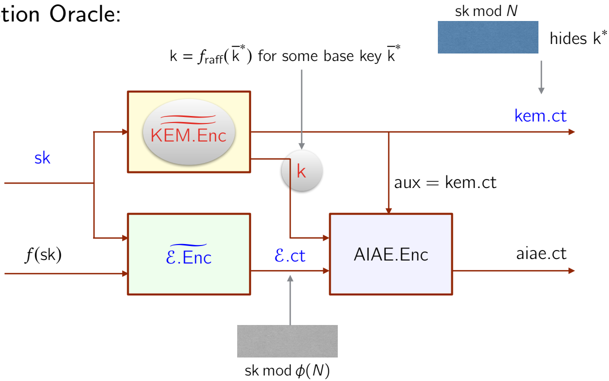
- $\widetilde{\mathcal{E}\text{.Dec}}$ rejects the query, if the computation of m involves ▨ .

  sk mod N

  - Since $\mathcal{E}$ has an authentication functionality, this change is computationally indistinguishable.

Proof Idea of KDM[$\mathcal{F}_{\text{aff}}$]-CCA Security

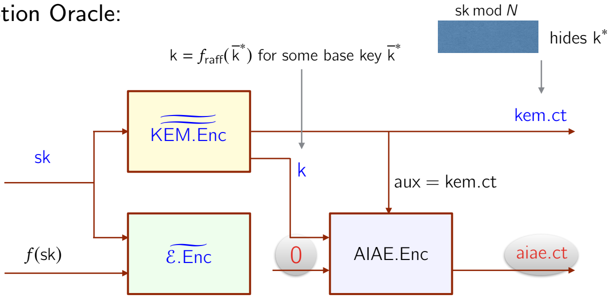
The Encryption Oracle:


sk mod N
hides k^*
$\mathsf{k} = f_{\text{raff}}(\overline{\mathsf{k}}^*)$ for some base key $\overline{\mathsf{k}}^*$
kem.ct
$\widetilde{\text{KEM.Enc}}$
k
sk
aux = kem.ct
f(sk)
$\widetilde{\mathcal{E}.\text{Enc}}$
$\mathcal{E}$.ct
AIAE.Enc
aiae.ct
sk mod $\phi(N)$

- We compute k as $\mathcal{F}_{\text{raff}}$-functions of an independent base key $\overline{\mathsf{k}}^*$.
  - In $\widetilde{\mathcal{E}.\text{Enc}}$ and the Decryption Oracle, ▨ is not involved.
    sk mod N
  - In kem.ct, the base key k^* is protected by ▨ perfectly.
    sk mod N

Proof Idea of KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA Security

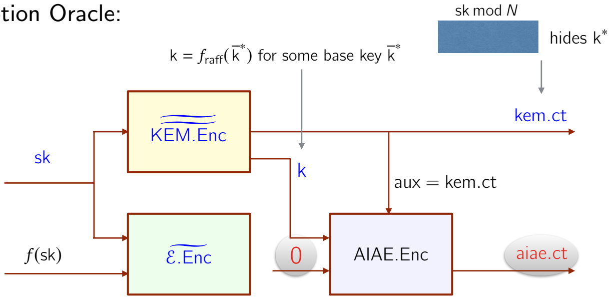
The Encryption Oracle:


sk mod N
hides k*
k = $f_{\mathsf{raff}}(\overline{\mathsf{k}}^*)$ for some base key $\overline{\mathsf{k}}^*$
kem.ct
$\widetilde{\mathsf{KEM.Enc}}$
sk
k
aux = kem.ct
f(sk)
$\widetilde{\mathcal{E}}$.Enc
0
AIAE.Enc
aiae.ct

- By the IND-$\mathcal{F}_{\mathsf{raff}}$-RKA security of AIAE, we change aiae.ct as encryptions of 0.
  - k is an $\mathcal{F}_{\mathsf{raff}}$-function of $\overline{\mathsf{k}}^*$, which is independent of other parts of the game.

Proof Idea of KDM[$\mathcal{F}_{\text{aff}}$]-CCA Security

The Encryption Oracle:

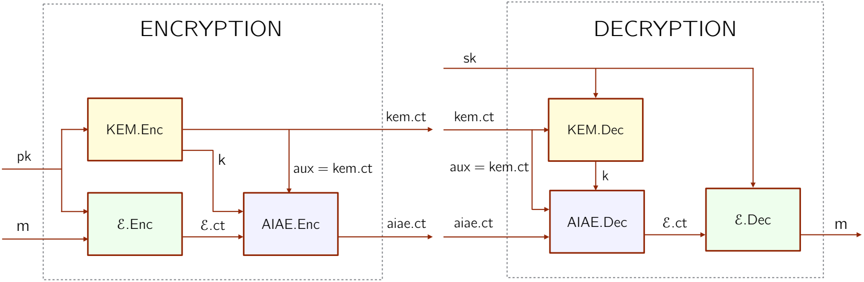

sk mod N
hides k^*
$\mathsf{k} = f_{\text{raff}}(\bar{\mathsf{k}}^*)$ for some base key $\bar{\mathsf{k}}^*$
kem.ct
$\widetilde{\widetilde{\text{KEM}}}$.Enc
sk
k
aux = kem.ct
$\widetilde{\mathcal{E}}$.Enc
$f(\mathsf{sk})$
0
AIAE.Enc
aiae.ct

- By the IND-$\mathcal{F}_{\text{raff}}$-RKA security of AIAE, we change aiae.ct as encryptions of 0.
  - k is an $\mathcal{F}_{\text{raff}}$-function of $\bar{\mathsf{k}}^*$, which is independent of other parts of the game.
- The advantage of the adversary is zero.

Synopsis

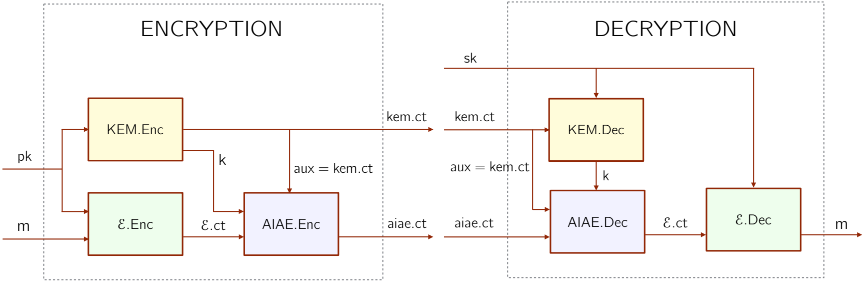
1. The LLJ Scheme [Lu, Li and Jia, 2015]
2. Introducing: Authenticated Encryption with Auxiliary-Input
3. KDM-CCA secure PKE for Affine Functions
4. KDM-CCA secure PKE for Polynomial Functions

Our Approach



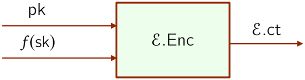
- We design a new $\mathcal{E}$: an entropy filter for the set of polynomial functions $\mathcal{F}^d_{\text{poly}}$.
    - Entropy Filter ([LLJ'15]): through some computationally indistinguishable change, $\underset{\text{sk mod } N}{\blacksquare}$ can be reserved by $\mathcal{E}$.Enc(pk, f(sk)), for $f \in \mathcal{F}^d_{\text{poly}}$.

Our Approach



- We design a new $\mathcal{E}$: an entropy filter for the set of polynomial functions $\mathcal{F}^d_{\text{poly}}$.
  - Entropy Filter ([LLJ'15]): through some computationally indistinguishable change, sk mod N can be reserved by $\mathcal{E}$.Enc(pk, f(sk)), for $f \in \mathcal{F}^d_{\text{poly}}$.
- The other two building blocks KEM and AIAE are the same.

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$


pk

$f(\mathsf{sk})$

$\mathcal{E}$.Enc

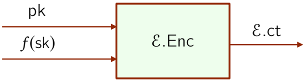
$\mathcal{E}$.ct

$\mathcal{E}$.ct = (table, e, t)

- prm = $(g_1, \cdots, g_5)$. sk = $(x_1, \cdots, x_4, y_1, \cdots, y_4)$.

  pk = $(h_1, \cdots, h_4) = (g_1^{-x_1} g_2^{-y_1}, g_2^{-x_2} g_3^{-y_2}, g_3^{-x_3} g_4^{-y_3}, g_4^{-x_4} g_5^{-y_4})$.

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$



$\mathcal{E}$.ct = (table, e, t)

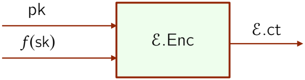
- prm = $(g_1, \cdots, g_5)$. sk = $(x_1, \cdots, x_4, y_1, \cdots, y_4)$.

  pk = $(h_1, \cdots, h_4) = (g_1^{-x_1} g_2^{-y_1}, g_2^{-x_2} g_3^{-y_2}, g_3^{-x_3} g_4^{-y_3}, g_4^{-x_4} g_5^{-y_4})$.

- For $j \in [0, 8]$,

$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline \end{array}\,. \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}}\,.$$

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$



$\mathcal{E}.\mathsf{ct} = (\mathsf{table}, e, t)$

- prm $= (g_1, \cdots, g_5)$. sk $= (x_1, \cdots, x_4, y_1, \cdots, y_4)$.

  pk $= (h_1, \cdots, h_4) = (g_1^{-x_1} g_2^{-y_1}, g_2^{-x_2} g_3^{-y_2}, g_3^{-x_3} g_4^{-y_3}, g_4^{-x_4} g_5^{-y_4})$.

- For $j \in [0, 8]$,

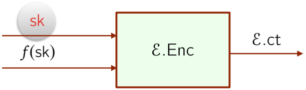
$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline \end{array}. \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}}.$$

- table $=$

$$\begin{array}{|c|c|c|c|}\hline u_{0,1} & u_{0,2} & \cdots & u_{0,8} \\ \hline u_{1,1} \cdot v_0 & u_{1,2} & \cdots & u_{1,8} \\ \hline u_{2,1} & u_{2,2} \cdot v_1 & \cdots & u_{2,8} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline u_{8,1} & u_{8,2} & \cdots & u_{8,8} \cdot v_7 \\ \hline \end{array}.$$

- $e = v_8 \cdot T^{f(\mathsf{sk})}$. $\quad t = g_1^{f(\mathsf{sk}) \bmod \phi(N)}$.

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$



$\mathcal{E}$.ct = (table, e, t)

- For $j \in [0, 8]$,

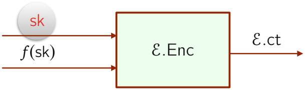
$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline \end{array} . \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}} .$$

$$\Rightarrow \hat{v}_j = u_{j,1}^{-x_1} u_{j,2}^{-y_1} u_{j,3}^{-x_2} u_{j,4}^{-y_2} u_{j,5}^{-x_3} u_{j,6}^{-y_3} u_{j,7}^{-x_4} u_{j,8}^{-y_4}$$

- table =

$u_{0,1}$	$u_{0,2}$	$\cdots$	$u_{0,8}$	$\Rightarrow \hat{v}_0 = v_0$
$u_{1,1} \cdot v_0$	$u_{1,2}$	$\cdots$	$u_{1,8}$	$\Rightarrow \hat{v}_1 = v_1$
$u_{2,1}$	$u_{2,2} \cdot v_1$	$\cdots$	$u_{2,8}$	$\Rightarrow \hat{v}_2 = v_2$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$u_{8,1}$	$u_{8,2}$	$\cdots$	$u_{8,8} \cdot v_7$	$\Rightarrow \hat{v}_8 = v_8$

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$



$\mathcal{E}$.ct = (table, e, t)

- For $j \in [0, 8]$,

$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline \end{array} . \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}} .$$

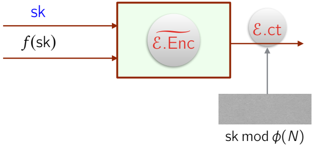
$$\Rightarrow \hat{v}_j = u_{j,1}^{-x_1} u_{j,2}^{-y_1} u_{j,3}^{-x_2} u_{j,4}^{-y_2} u_{j,5}^{-x_3} u_{j,6}^{-y_3} u_{j,7}^{-x_4} u_{j,8}^{-y_4}$$

- table =

$$\begin{array}{|c|c|c|c|l}\cline{1-4} u_{0,1} & u_{0,2} & \cdots & u_{0,8} & \Rightarrow \hat{v}_0 = v_0 \\ \cline{1-4} u_{1,1} \cdot v_0 & u_{1,2} & \cdots & u_{1,8} & \Rightarrow \hat{v}_1 = v_1 \\ \cline{1-4} u_{2,1} & u_{2,2} \cdot v_1 & \cdots & u_{2,8} & \Rightarrow \hat{v}_2 = v_2 \\ \cline{1-4} \vdots & \vdots & \ddots & \vdots & \\ \cline{1-4} u_{8,1} & u_{8,2} & \cdots & u_{8,8} \cdot v_7 & \Rightarrow \hat{v}_8 = v_8 \\ \cline{1-4} \end{array}$$

- $e = v_8 \cdot T^{f(\mathsf{sk})} \Rightarrow e = \hat{v}_8 \cdot T^{f(\mathsf{sk})}$. $\quad t = g_1^{f(\mathsf{sk}) \bmod \phi(N)}$.

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$



$\mathcal{E}$.ct = (table, e, t)

- For $j \in [0, 8]$,

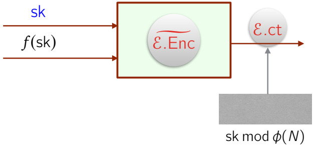
$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline \end{array} . \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}} .$$

$$\Rightarrow \hat{v}_j = u_{j,1}^{-x_1} u_{j,2}^{-y_1} u_{j,3}^{-x_2} u_{j,4}^{-y_2} u_{j,5}^{-x_3} u_{j,6}^{-y_3} u_{j,7}^{-x_4} u_{j,8}^{-y_4}$$

- table =

$u_{0,1}$	$u_{0,2}$	$\cdots$	$u_{0,8}$	$\Rightarrow \hat{v}_0 = v_0$
$u_{1,1} \cdot v_0 \cdot T^a$	$u_{1,2}$	$\cdots$	$u_{1,8}$	$\Rightarrow \hat{v}_1 = v_1 \cdot T^{-ax_1}$
$u_{2,1}$	$u_{2,2} \cdot v_1$	$\cdots$	$u_{2,8}$	$\Rightarrow \hat{v}_2 = v_2 \cdot T^{-ax_1 y_1}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$u_{8,1}$	$u_{8,2}$	$\cdots$	$u_{8,8} \cdot v_7$	$\Rightarrow \hat{v}_8 = v_8 \cdot T^{-ax_1 y_1 \cdots x_4 y_4} = v_8 \cdot T^{-f(\mathsf{sk})}$

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1y_1x_2y_2x_3y_3x_4y_4$



$\mathcal{E}.\mathsf{ct} = (\mathsf{table}, e, t)$

- For $j \in [0, 8]$,

$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline\end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline\end{array}. \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}}.$$

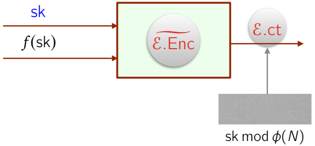
$$\Rightarrow \hat{v}_j = u_{j,1}^{-x_1} u_{j,2}^{-y_1} u_{j,3}^{-x_2} u_{j,4}^{-y_2} u_{j,5}^{-x_3} u_{j,6}^{-y_3} u_{j,7}^{-x_4} u_{j,8}^{-y_4}$$

- table =

$$\begin{array}{|c|c|c|c|l}\hline u_{0,1} & u_{0,2} & \cdots & u_{0,8} & \Rightarrow \hat{v}_0 = v_0 \\ \hline u_{1,1} \cdot v_0 \cdot \textcircled{T^a} & u_{1,2} & \cdots & u_{1,8} & \Rightarrow \hat{v}_1 = v_1 \cdot T^{-ax_1} \\ \hline u_{2,1} & u_{2,2} \cdot v_1 & \cdots & u_{2,8} & \Rightarrow \hat{v}_2 = v_2 \cdot T^{-ax_1y_1} \\ \hline \vdots & \vdots & \ddots & \vdots & \\ \hline u_{8,1} & u_{8,2} & \cdots & u_{8,8} \cdot v_7 & \Rightarrow \hat{v}_8 = v_8 \cdot T^{-ax_1y_1\cdots x_4y_4} = v_8 \cdot T^{-f(\mathsf{sk})} \\ \hline\end{array}$$

- $e = v_8 \cdot T^{f(\mathsf{sk})} \Rightarrow e = \hat{v}_8 \cdot T^{f(\mathsf{sk})} \Rightarrow e = v_8.$ $\qquad t = g_1^{f(\mathsf{sk}) \bmod \phi(N)}.$

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1y_1x_2y_2x_3y_3x_4y_4$


sk
$f(\mathsf{sk})$
$\widetilde{\mathcal{E}.\mathsf{Enc}}$
$\mathcal{E}.\mathsf{ct}$
sk mod $\phi(N)$

$\mathcal{E}.\mathsf{ct} = (\mathsf{table}, e, t)$

- For $j \in [0, 8]$,

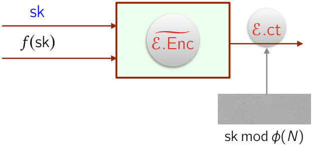
$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline\end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline\end{array}. \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}}.$$

- table =

$u_{0,1}$	$u_{0,2}$	$\cdots$	$u_{0,8}$
$u_{1,1} \cdot v_0 \cdot T^a$	$u_{1,2}$	$\cdots$	$u_{1,8}$
$u_{2,1}$	$u_{2,2} \cdot v_1$	$\cdots$	$u_{2,8}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$u_{8,1}$	$u_{8,2}$	$\cdots$	$u_{8,8} \cdot v_7$

- $e = v_8$. $\quad t = g_1^{f(\mathsf{sk}) \bmod \phi(N)}$.

$\mathcal{E}$ designed for monomial $f(\mathsf{sk}) = a \cdot x_1 y_1 x_2 y_2 x_3 y_3 x_4 y_4$



$\mathcal{E}$.ct = (table, e, t)

- For $j \in [0, 8]$,

$$\begin{array}{|c|c|c|c|}\hline u_{j,1} & u_{j,2} & \cdots & u_{j,8} \\ \hline\end{array} = \begin{array}{|c|c|c|c|c|c|c|c|}\hline g_1^{r_{j,1}} & g_2^{r_{j,1}} & g_2^{r_{j,2}} & g_3^{r_{j,2}} & g_3^{r_{j,3}} & g_4^{r_{j,3}} & g_4^{r_{j,4}} & g_5^{r_{j,4}} \\ \hline\end{array}. \quad v_j = h_1^{r_{j,1}} h_2^{r_{j,2}} h_3^{r_{j,3}} h_4^{r_{j,4}}.$$

- table =

$u_{0,1}$	$u_{0,2}$	$\cdots$	$u_{0,8}$
$u_{1,1} \cdot v_0 \cdot T^a$	$u_{1,2}$	$\cdots$	$u_{1,8}$
$u_{2,1}$	$u_{2,2} \cdot v_1$	$\cdots$	$u_{2,8}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$u_{8,1}$	$u_{8,2}$	$\cdots$	$u_{8,8} \cdot v_7$

- $e = v_8$. $\qquad t = g_1^{f(\mathsf{sk}) \bmod \phi(N)}$.

$\widetilde{\mathcal{E}}$.Enc behaves like an entropy filter for the monomial.

General $\mathcal{E}$ designed for Polynomial Functions

- A polynomial function f in $\mathsf{sk} = (x_1, \cdots, x_4, y_1, \cdots, y_4)$ of degree d is

$$f(\mathsf{sk}) = \sum_{0 \leq c_1 + \cdots + c_8 \leq d} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}.$$

General $\mathcal{E}$ designed for Polynomial Functions

- A polynomial function f in $\mathsf{sk} = (x_1, \cdots, x_4, y_1, \cdots, y_4)$ of degree d is

$$f(\mathsf{sk}) = \sum_{0 \le c_1 + \cdots + c_8 \le d} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}.$$

- For each monomial $\mathsf{c} = (c_1, \cdots, c_8)$, $\mathcal{E}$.Enc creates a pair of $\mathsf{table}^{(\mathsf{c})}$ and $v^{(\mathsf{c})}$.

  The products of these $v^{(\mathsf{c})}$ are used to hide the message: $e = \prod_{\mathsf{c}} v^{(\mathsf{c})} \cdot T^{f(\mathsf{sk})}$.

General $\mathcal{E}$ designed for Polynomial Functions

- A polynomial function f in $\mathsf{sk} = (x_1, \cdots, x_4, y_1, \cdots, y_4)$ of degree d is

$$f(\mathsf{sk}) = \sum_{0 \le c_1 + \cdots + c_8 \le d} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}.$$

- For each monomial $\mathsf{c} = (c_1, \cdots, c_8)$, $\mathcal{E}$.Enc creates a pair of table$^{(\mathsf{c})}$ and $v^{(\mathsf{c})}$.

  The products of these $v^{(\mathsf{c})}$ are used to hide the message: $e = \prod_{\mathsf{c}} v^{(\mathsf{c})} \cdot T^{f(\mathsf{sk})}$.

- Under the DCR assumption, $\mathcal{E}$.Enc is changed to $\widetilde{\mathcal{E}.\mathsf{Enc}}$, such that each $v^{(\mathsf{c})}$ is multiplied with an additional term:

$$\hat{v}^{(\mathsf{c})} = v^{(\mathsf{c})} \cdot T^{-a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}}.$$

General $\mathcal{E}$ designed for Polynomial Functions

- A polynomial function f in $\mathsf{sk} = (x_1, \cdots, x_4, y_1, \cdots, y_4)$ of degree d is

$$f(\mathsf{sk}) = \sum_{0 \le c_1 + \cdots + c_8 \le d} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}.$$

- For each monomial $\mathsf{c} = (c_1, \cdots, c_8)$, $\mathcal{E}$.Enc creates a pair of table$^{(\mathsf{c})}$ and $v^{(\mathsf{c})}$.

  The products of these $v^{(\mathsf{c})}$ are used to hide the message: $e = \prod_{\mathsf{c}} v^{(\mathsf{c})} \cdot T^{f(\mathsf{sk})}$.

- Under the DCR assumption, $\mathcal{E}$.Enc is changed to $\widetilde{\mathcal{E}.\mathsf{Enc}}$, such that each $v^{(\mathsf{c})}$ is multiplied with an additional term:

$$\hat{v}^{(\mathsf{c})} = v^{(\mathsf{c})} \cdot T^{-a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}}.$$

  Consequently,

$$e = \prod_{\mathsf{c}} \hat{v}^{(\mathsf{c})} \cdot T^{f(\mathsf{sk})} = \prod_{\mathsf{c}} v^{(\mathsf{c})} \cdot T^{-\sum_{\mathsf{c}} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}} \cdot T^{f(\mathsf{sk})} = \prod_{\mathsf{c}} v^{(\mathsf{c})}.$$

General $\mathcal{E}$ designed for Polynomial Functions

- A polynomial function f in $\mathsf{sk} = (x_1, \cdots, x_4, y_1, \cdots, y_4)$ of degree d is

$$f(\mathsf{sk}) = \sum_{0 \le c_1 + \cdots + c_8 \le d} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}.$$

- For each monomial $\mathsf{c} = (c_1, \cdots, c_8)$, $\mathcal{E}$.Enc creates a pair of table$^{(\mathsf{c})}$ and $v^{(\mathsf{c})}$.

  The products of these $v^{(\mathsf{c})}$ are used to hide the message: $e = \prod_{\mathsf{c}} v^{(\mathsf{c})} \cdot T^{f(\mathsf{sk})}$.

- Under the DCR assumption, $\mathcal{E}$.Enc is changed to $\widetilde{\mathcal{E}.\mathsf{Enc}}$, such that each $v^{(\mathsf{c})}$ is multiplied with an additional term:

$$\hat{v}^{(\mathsf{c})} = v^{(\mathsf{c})} \cdot T^{-a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}}.$$

  Consequently,

$$e = \prod_{\mathsf{c}} \hat{v}^{(\mathsf{c})} \cdot T^{f(\mathsf{sk})} = \prod_{\mathsf{c}} v^{(\mathsf{c})} \cdot T^{-\sum_{\mathsf{c}} a_{(c_1, \cdots, c_8)} \cdot x_1^{c_1} y_1^{c_2} \cdots x_4^{c_7} y_4^{c_8}} \cdot T^{f(\mathsf{sk})} = \prod_{\mathsf{c}} v^{(\mathsf{c})}.$$

$\widetilde{\mathcal{E}.\mathsf{Enc}}$ behaves like an entropy filter for polynomial functions.

Conclusion

Conclusion

In this work, we propose:

- A new approach for constructing KDM-CCA secure PKE scheme, from KEM, $\mathcal{E}$, and a new primitive called “AIAE”.

Conclusion

In this work, we propose:

- A new approach for constructing KDM-CCA secure PKE scheme, from KEM, $\mathcal{E}$, and a new primitive called "AIAE".
- Efficient KDM[$\mathcal{F}_{\mathsf{aff}}$]-CCA secure PKE with compact ciphertexts.
- Efficient KDM[$\mathcal{F}^{d}_{\mathsf{poly}}$]-CCA secure PKE with almost compact ciphertexts.

Thank You