Multi-Input Quadratic Functional Encryption: Stronger Security, Broader Functionality

TCC 2022

Shweta Agrawal (IIT Madras)
Rishab Goyal (UW-Madison)
Junichi Tomida (NTT Social Informatics Laboratories)

Functional Encryption (FE) [O'Neill10][BSW11]

$\mathsf{pk}, \mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$

$\mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f)$

sk

ct

$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, x)$

$f(x) \leftarrow \mathsf{Dec}(\mathsf{ct}, \mathsf{sk})$

Multi-input Functional Encryption (MIFE) [GGGJKLSSZ14]

1. Secret-Key Multi-Input Functional Encryption (SK-MIFE)
2. Multi-input Functional Encryption (MIFE)

SK-MIFE < MIFE

Secret-Key Multi-Input Functional Encryption (SK-MIFE)

$\mathsf{pk}, \color{red}{\mathsf{msk}} \leftarrow \mathsf{Setup}(1^\lambda)$

$\mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f)$

$\mathsf{ct}_1 \leftarrow \mathsf{Enc}(\color{red}{\mathsf{msk}}, 1, x_1)$

⋮

$\mathsf{ct}_n \leftarrow \mathsf{Enc}(\color{red}{\mathsf{msk}}, n, x_n)$

sk

$\mathsf{ct}_1, \dots, \mathsf{ct}_n$

$f(x_1, \dots, x_n) \leftarrow \mathsf{Dec}(\mathsf{ct}_1, \dots, \mathsf{ct}_n, \mathsf{sk})$

× Security of the system is broken if one of the encryptors is corrupted.

Multi-Input Functional Encryption (MIFE)

$\mathrm{pk}, \mathrm{ek}_1, \ldots, \mathrm{ek}_n, \mathrm{msk} \leftarrow \mathrm{Setup}(1^\lambda)$

$\mathrm{sk} \leftarrow \mathrm{KeyGen}(\mathrm{msk}, f)$

sk

$\mathrm{ct}_1 \leftarrow \mathrm{Enc}(\mathrm{ek}_1, x_1)$

⋮

$\mathrm{ct}_n \leftarrow \mathrm{Enc}(\mathrm{ek}_n, x_n)$

$\mathrm{ct}_1, \ldots, \mathrm{ct}_n$

$f(x_1, \ldots, x_n) \leftarrow \mathrm{Dec}(\mathrm{ct}_1, \ldots, \mathrm{ct}_n, \mathrm{sk})$

Comparison of MIFE Schemes and Our Result

Reference	MIFE Model	Function Class	Assumption
[GGG+14][BGJS15] [AJ15][BKS16]	MIFE	General functions (all circuits, TMs)	Obfuscation (iO, diO)
[AGRW17][ACFGU18]	SK-MIFE	Inner Product	MDDH, LWE, DCR
[CDGHP18][ABG19]	MIFE	Inner Product +Labeling	MDDH, LWE, DCR
[AGT21]	SK-MIFE	Quadratic functions	MDDH
Ours1	MIFE	Quadratic functions	SXDH
Ours2	SK-MIFE	Quadratic functions +Labeling	SXDH

$\mathbf{x} = (\mathbf{x}_1 || \ldots || \mathbf{x}_n)$
Inner Product: $f_{\mathbf{c}}(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \langle \mathbf{x}, \mathbf{c} \rangle$
Quadratic Functions: $f_{\mathbf{c}}(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \langle \mathbf{x} \otimes \mathbf{x}, \mathbf{c} \rangle$

High-Level Overview

1. SK-MIFE with a special homomorphic property P can be generically converted to MIFE for the same class.
2. The AGT SK-MIFE scheme for QFs does not meet P.
3. We modify the AGT scheme to satisfy P.
4. Then we apply the conversion to the modified SK-MIFE scheme for QFs with P.

The Property P for SK-MIFE

- For all $i \in [n]$, there exist elementary messages $e_1, \dots e_d$ and an efficient algorithm $\widetilde{\mathrm{Enc}}$ s.t. for all x_i

$$\{\mathrm{ct}_i : \mathrm{ct}_i \leftarrow \mathrm{Enc}(\mathrm{msk}, i, x_i)\}$$

$$\approx_s$$

$$\left\{\mathrm{ct}_i : \widetilde{\mathrm{ct}}_{i,j} \leftarrow \mathrm{Enc}\left(\mathrm{msk}, i, e_j\right), \mathrm{ct}_i \leftarrow \widetilde{\mathrm{Enc}}\left(\left\{\widetilde{\mathrm{ct}}_{i,j}\right\}_{j \in [d]}, x_i\right)\right\}$$

Enc ek_i in MIFE

The Property P in the AGT Scheme

- If the AGT scheme satisfies

$$\mathrm{ct}_i[\mathbf{x}_1] + \mathrm{ct}_i[\mathbf{x}_2] = \mathrm{ct}_i[\mathbf{x}_1 + \mathbf{x}_2]$$

we can set the elementary messages to be the vectors $(\mathbf{e}_1, \dots \mathbf{e}_n)$ of the canonical basis.

- $\widetilde{\mathrm{Enc}}$ works as $\mathrm{ct}_i[\mathbf{x}] = \sum \mathbf{x}[j]\mathrm{ct}_i[\mathbf{e}_j]$.

- But it is not the case.

The Structure of the AGT Scheme

- A ciphertext for $\mathbf{x}_i$ of the AGT scheme:

$$[\mathbf{v}_i \mathbf{M}_i] \qquad [\mathbf{M}] = g^{\mathbf{M}} \text{ denotes element-wise exponentiation}$$

$\mathbf{M}_i$ is a common matrix for all $\mathbf{ct}_i$, $\mathbf{v}_i$ consists of

1. 1
2. an entry of $\mathbf{x}_i$
3. a random element in $\mathbb{Z}_p$
4. an element of the tuple $(b, c, b\ell, c\ell)$

- We show the elements of item 4 can be removed!

- Item 1 to 3 are amenable to the homomorphism

$$\mathbf{ct}_i[\mathbf{x}_1] + \mathbf{ct}_i[\mathbf{x}_2] - \mathbf{ct}_i[\mathbf{0}] = \mathbf{ct}_i[\mathbf{x}_1 + \mathbf{x}_2]$$

Randomization Trick

1. 1
2. an entry of $\mathbf{x}_i$
3. a random element in $\mathbb{Z}_p$

- Item 1 to 3 are amenable to the homomorphism

$$\mathrm{ct}_i[\mathbf{x}_1] + \mathrm{ct}_i[\mathbf{x}_2] - \mathrm{ct}_i[\mathbf{0}] = \mathrm{ct}_i[\mathbf{x}_1 + \mathbf{x}_2]$$

- After the homomorphic computation, elements in item 3 are not random.

- Adding

$\sum_j r_j(\mathrm{ct}_{i,j}[\mathbf{0}] - \mathrm{ct}_{i,j}[\mathbf{0}])$: elements for 1 and 2 are 0 in the red part.

Summary and Open Question

- MIFE for QFs
- SK-MIFE for QFs with labeling

- Open question
  - MIFE for QFs with labeling (MCFE for QFs)