Simulation Secure Multi-Input Quadratic Functional Encryption

Ferran Alborch Escobar [1,2,3] Sébastien Canard [2] Fabien Laguillaumie [3]

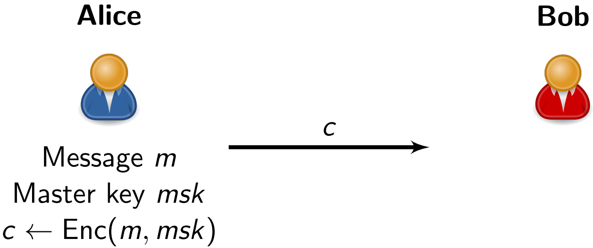
[1] Orange Innovation, Caen, France

[2] Télécom Paris, Palaiseau, France

[3] Université de Montpellier, Montpellier, France

August 28th 2024

(Secret-key) Functional Encryption [BSW11, Boneh et al. TCC'11]



Alice

Bob

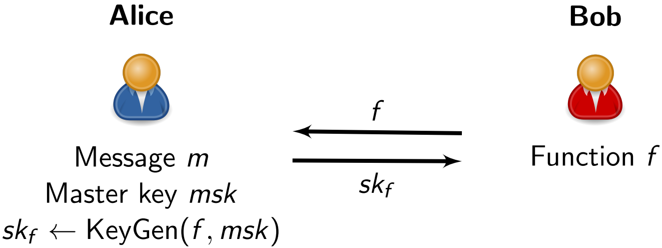
c

Message m

Master key msk

$c \leftarrow \mathrm{Enc}(m, msk)$

(Secret-key) Functional Encryption [BSW11, Boneh et al. TCC'11]



Alice

Message m
Master key msk
$sk_f \leftarrow \mathrm{KeyGen}(f, msk)$

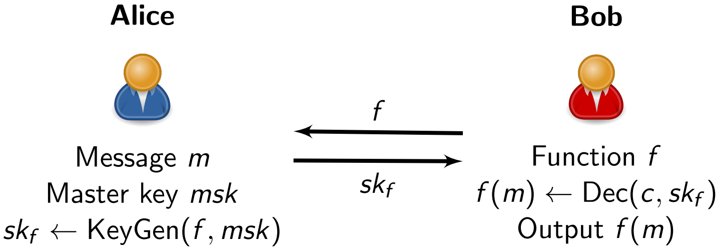
f

sk_f

Bob

Function f

(Secret-key) Functional Encryption [BSW11, Boneh et al. TCC'11]



Alice

Message m

Master key msk

$sk_f \leftarrow \text{KeyGen}(f, msk)$

f

sk_f

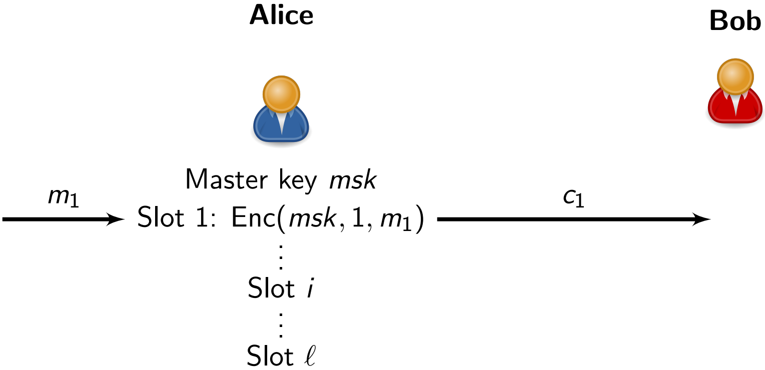
Bob

Function f

$f(m) \leftarrow \text{Dec}(c, sk_f)$

Output $f(m)$

(Secret-key) Multi-input Functional Encryption [GGG$^+$14, Goldwasser et al. EUROCRYPT'14]



Alice

Bob

m_1

Master key msk

Slot 1: $\mathsf{Enc}(msk, 1, m_1)$

c_1

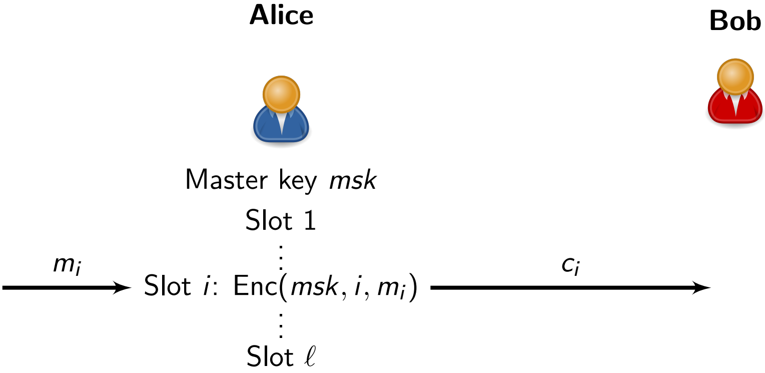
$\vdots$

Slot i

$\vdots$

Slot ℓ

(Secret-key) Multi-input Functional Encryption [GGG+14, Goldwasser et al. EUROCRYPT'14]



Alice

Bob

Master key *msk*

Slot 1

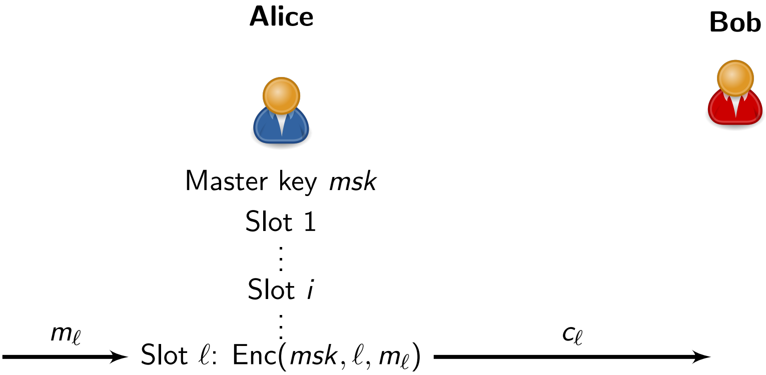
$\vdots$

$\xrightarrow{m_i}$ Slot i: $\mathsf{Enc}(msk, i, m_i)$ $\xrightarrow{c_i}$

$\vdots$

Slot ℓ

(Secret-key) Multi-input Functional Encryption [GGG+14, Goldwasser et al. EUROCRYPT'14]



Alice

Bob

Master key msk

Slot 1

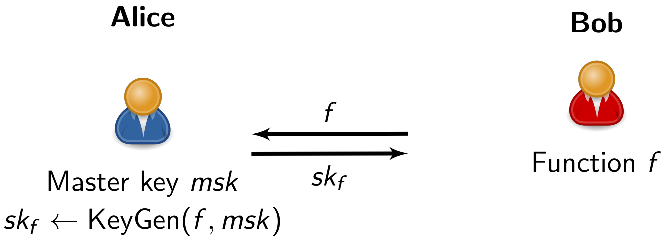
$\vdots$

Slot i

$\vdots$

m_ℓ Slot ℓ: $\mathsf{Enc}(msk, \ell, m_\ell)$ c_ℓ

(Secret-key) Multi-input Functional Encryption [GGG+14, Goldwasser et al. EUROCRYPT'14]



Alice

Master key msk

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

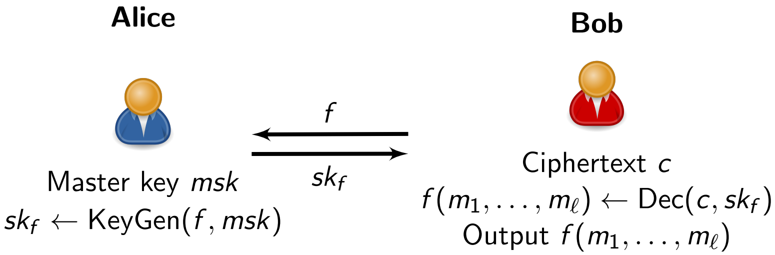
f

sk_f

Bob

Function f

(Secret-key) Multi-input Functional Encryption [GGG+14, Goldwasser et al. EUROCRYPT'14]



Alice

Master key msk

$sk_f \leftarrow \text{KeyGen}(f, msk)$

f

sk_f

Bob

Ciphertext c

$f(m_1, \ldots, m_\ell) \leftarrow \text{Dec}(c, sk_f)$

Output $f(m_1, \ldots, m_\ell)$

Applications of Multi-input Functional Encryption

- Searching over encrypted data [GGG$^+$14, Goldwasser et al. EUROCRYPT'14]
- Federated learning [XBZ$^+$19, Xu et al. AISec'19]
- Differential Privacy [AECLP24, Alborch Escobar et al. PETS'24]

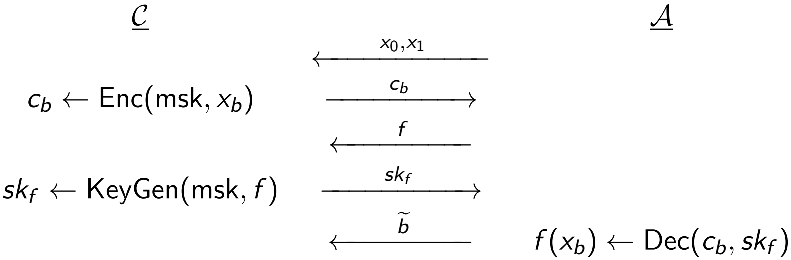
Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

Experiment *b*:



$\underline{\mathcal{C}}$ $\underline{\mathcal{A}}$

$\xleftarrow{x_0, x_1}$

$c_b \leftarrow \mathsf{Enc}(\mathsf{msk}, x_b)$ $\xrightarrow{c_b}$

$\xleftarrow{f}$

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

$\xleftarrow{\widetilde{b}}$ $f(x_b) \leftarrow \mathsf{Dec}(c_b, sk_f)$

Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

Experiment *b*:

$\underline{\mathcal{C}}$ $\qquad\qquad\qquad$ $\underline{\mathcal{A}}$

$$\xleftarrow{\quad x_0, x_1 \quad}$$

$$c_b \leftarrow \mathrm{Enc}(\mathrm{msk}, x_b) \qquad \xrightarrow{\quad c_b \quad}$$

$$\xleftarrow{\quad f \quad}$$

$$sk_f \leftarrow \mathrm{KeyGen}(\mathrm{msk}, f) \qquad \xrightarrow{\quad sk_f \quad}$$

$$\xleftarrow{\quad \widetilde{b} \quad} \qquad f(x_b) \leftarrow \mathrm{Dec}(c_b, sk_f)$$

Needs $f(x_0) = f(x_1)$

Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

```
$\mathsf{Exp}^{real}_{\mathcal{A}}(1^\lambda)$
$x \leftarrow \mathcal{A}(1^\lambda)$
$\mathsf{msk} \leftarrow \mathsf{SetUp}(1^\lambda)$
$c_x \leftarrow \mathsf{Enc}(\mathsf{msk}, x)$
$\gamma \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, f)}(c_x)$
```

```
$\mathsf{Exp}^{ideal}_{\mathcal{A},\mathsf{Sim}}(1^\lambda)$
$x \leftarrow \mathcal{A}(1^\lambda)$
$\widetilde{\mathsf{msk}} \leftarrow \mathsf{SetUpSim}(1^\lambda)$
$\widetilde{c} \leftarrow \mathsf{EncSim}(\widetilde{\mathsf{msk}})$
$\gamma \leftarrow \mathcal{A}^{\mathsf{KeyGenSim}(\widetilde{\mathsf{msk}}, f, f(x))}(\widetilde{c})$
```

Show real and ideal experiments are indistinguishable

Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

- Selective vs. adaptive
  - Adaptive is stronger
  - Impossibility results for adaptive ([BSW11, Boneh et al. TCC'11], ...)

Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

- Selective vs. adaptive
  - Adaptive is stronger
  - Impossibility results for adaptive ([BSW11, Boneh et al. TCC'11], ...)

Security of (Multi-Input) Functional Encryption

- Indistinguishability vs. simulation-based
  - Simulation-based stronger [AGVW13, Agrawal et al. CRYPTO'13] and more composable
  - Impossibility results for simulation-based ([BSW11, Boneh et al. TCC'11], ...)

- Selective vs. adaptive
  - Adaptive is stronger
  - Impossibility results for adaptive ([BSW11, Boneh et al. TCC'11], ...)

- Function-hiding functional encryption [SSW09, Shen et al. TCC'09]
  - Additional security property
  - Indistinguishability and simulation-based variants
  - Only in secret-key

State of the Art in MIFE

- Inner-product function: input $\boldsymbol{x}$ and function $\boldsymbol{y}$ output $\boldsymbol{x}^\top \boldsymbol{y}$ ($\sum \boldsymbol{x}_i^\top \boldsymbol{y}_i$ in multi-input)
  - Generic transformation from IPFE exists [ACF+18, Abdalla et al. CRYPTO'18].

State of the Art in MIFE

- Inner-product function: input $\boldsymbol{x}$ and function $\boldsymbol{y}$ output $\boldsymbol{x}^\top \boldsymbol{y}$ ($\sum \boldsymbol{x}_i^\top \boldsymbol{y}_i$ in multi-input)
  - Generic transformation from IPFE exists [ACF+18, Abdalla et al. CRYPTO'18].
- Quadratic function: input $\boldsymbol{x}$ and function $\boldsymbol{F}$ output $\boldsymbol{x}^\top \boldsymbol{F} \boldsymbol{x}$ ($\sum \boldsymbol{x}_i^\top \boldsymbol{F}_{i,j} \boldsymbol{x}_{\boldsymbol{j}}$ in multi-input)

Table: State of the art. We consider ℓ inputs of size n or 1 input of size $n\ell$.

Proposal	Functionality	Simulation security	Ciphertext size
Naive	QFE	✓	$O(n^2\ell^2)$
[Gay20, Gay PKC'20]	QFE	✓	$O(n\ell)$
[AGT22, Agrawal et al. TCC'22]	MIQFE	✗	$O(n\ell)$

State of the Art in MIFE

- Inner-product function: input $\boldsymbol{x}$ and function $\boldsymbol{y}$ output $\boldsymbol{x}^\top \boldsymbol{y}$ ($\sum \boldsymbol{x}_i^\top \boldsymbol{y}_i$ in multi-input)
  - Generic transformation from IPFE exists [ACF+18, Abdalla et al. CRYPTO'18].
- Quadratic function: input $\boldsymbol{x}$ and function $\boldsymbol{F}$ output $\boldsymbol{x}^\top \boldsymbol{F} \boldsymbol{x}$ ($\sum \boldsymbol{x}_i^\top \boldsymbol{F}_{i,j} \boldsymbol{x}_{\boldsymbol{j}}$ in multi-input)

Table: State of the art. We consider ℓ inputs of size n or 1 input of size $n\ell$.

Proposal	Functionality	Simulation security	Ciphertext size
Naive	QFE	✓	$O(n^2\ell^2)$
[Gay20, Gay PKC'20]	QFE	✓	$O(n\ell)$
[AGT22, Agrawal et al. TCC'22]	MIQFE	✗	$O(n\ell)$
Our construction	MIQFE	✓	$O(n\ell^2)$

Results I: Transformation from function-hiding IPFE to MIQFE

- Transformation from function-hiding IPFE to MIQFE keeping simulation security

```
$\underline{\mathbf{SetUp}^{\mathsf{MIQFE}}(1^\kappa)}$ :
$\mathcal{PG} \leftarrow \mathsf{PGGen}(1^\kappa)$
$\boldsymbol{u}_i \xleftarrow{\$} \mathbb{Z}_p^n,\ c_i \xleftarrow{\$} \mathbb{Z}_p,\ \boldsymbol{w}_{i,j} \xleftarrow{\$} \mathbb{Z}_p^{2n}\ \ i,j \in [\ell]$
$(param_{i,j}^{\mathsf{IPFE}}, \mathsf{msk}_{i,j}^{\mathsf{IPFE}}) \leftarrow \mathsf{SetUp}^{\mathsf{IPFE}}(1^\kappa, \mathcal{PG})$
$param^{\mathsf{MIQFE}} = \mathcal{PG}$
$\mathsf{msk}^{\mathsf{MIQFE}} = (\boldsymbol{u}_i, c_i, \boldsymbol{w}_{i,j}, \mathsf{msk}_{i,j}^{\mathsf{IPFE}})$
```

```
$\underline{\mathbf{Enc}^{\mathsf{MIQFE}}(\mathsf{msk}^{\mathsf{MIQFE}}, i, \boldsymbol{x}_i)}$ :
$\boldsymbol{ct}_{\boldsymbol{x}_i} := \boldsymbol{x}_i + c_i \boldsymbol{u}_i$
$c_{i,j} \leftarrow \mathsf{Enc}^{\mathsf{IPFE}}\left(\mathsf{msk}_{i,j}^{\mathsf{IPFE}}, \boldsymbol{w}_{i,j} + c_j \begin{pmatrix} \boldsymbol{ct}_{\boldsymbol{x}_i} \\ \boldsymbol{x}_i \end{pmatrix}\right)$
$c_{\boldsymbol{x}_i} = (\boldsymbol{ct}_{\boldsymbol{x}_i}, c_{i,j})$
```

```
$\underline{\mathbf{KeyGen}^{\mathsf{MIQFE}}(\mathsf{msk}^{\mathsf{MIQFE}}, \boldsymbol{F})}$ :
$sk_{i,j} \leftarrow \mathsf{KeyGen}^{\mathsf{IPFE}}\left(\mathsf{msk}_{i,j}^{\mathsf{IPFE}}, \begin{pmatrix} \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \\ \boldsymbol{F}_{i,j} \boldsymbol{u}_j \end{pmatrix}\right)$
$zk_{\boldsymbol{F}} \leftarrow \sum_{i,j \in [\ell]} \boldsymbol{w}_{i,j}^\top \begin{pmatrix} \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \\ \boldsymbol{F}_{i,j} \boldsymbol{u}_j \end{pmatrix}$
$sk_{\boldsymbol{F}} = (\boldsymbol{F}, sk_{i,j}, zk_{\boldsymbol{F}})$
```

```
$\underline{\mathbf{Dec}^{\mathsf{MIQFE}}(c_{\boldsymbol{x}_1}, \ldots, c_{\boldsymbol{x}_\ell}, sk_{\boldsymbol{F}})}$ :
$[d_{i,j}]_T \leftarrow \mathsf{IPFE.Dec}(\mathsf{IPFE}.c_{i,j}, \mathsf{IPFE}.sk_{i,j})$
$[v]_T := \left(\sum_{i,j \in [\ell]} [\boldsymbol{ct}_{\boldsymbol{x}_i}^\top \boldsymbol{F}_{i,j} \boldsymbol{ct}_{\boldsymbol{x}_j}]_T - [d_{i,j}]_T\right) + [zk_{\boldsymbol{F}}]_T$
$s \leftarrow \log([v]_T)$
```

Results I: Transformation from function-hiding IPFE to MIQFE

- Transformation from function-hiding IPFE to MIQFE keeping simulation security

One-time pad $\boldsymbol{ct}_{\boldsymbol{x_i}}$

Compute the quadratic function over $\boldsymbol{ct}_{\boldsymbol{x_i}}$

$\underline{\mathbf{Enc}^{\mathsf{MIQFE}}(\mathsf{msk}^{\mathsf{MIQFE}}, i, \boldsymbol{x}_i)}$:

$\boldsymbol{ct}_{\boldsymbol{x}_i} := \boldsymbol{x}_i + c_i \boldsymbol{u}_i$

$c_{i,j} \leftarrow \mathsf{Enc}^{\mathsf{IPFE}}\left(\mathsf{msk}^{\mathsf{IPFE}}_{i,j}, \boldsymbol{w}_{i,j} + c_j \begin{pmatrix} \boldsymbol{ct}_{\boldsymbol{x}_i} \\ \boldsymbol{x}_i \end{pmatrix}\right)$

$c_{\boldsymbol{x}_i} = (\boldsymbol{ct}_{\boldsymbol{x}_i}, c_{i,j})$

Extra noise terms:
$c_i \boldsymbol{u}_i^\top \boldsymbol{F}_{i,j} \boldsymbol{x}_j + \boldsymbol{x}_i^\top \boldsymbol{F}_{i,j} c_j \boldsymbol{u}_j + c_i \boldsymbol{u}_i^\top \boldsymbol{F}_{i,j} c_j \boldsymbol{u}_j$

$\underline{\mathbf{Dec}^{\mathsf{MIQFE}}(c_{\boldsymbol{x}_1}, \ldots, c_{\boldsymbol{x}_\ell}, sk_{\boldsymbol{F}})}$:

$[d_{i,j}]_T \leftarrow \mathsf{IPFE.Dec}(\mathsf{IPFE}.c_{i,j}, \mathsf{IPFE}.sk_{i,j})$

$[v]_T := \left(\sum_{i,j\in[\ell]} [\boldsymbol{ct}_{\boldsymbol{x}_i}^\top \boldsymbol{F}_{i,j} \boldsymbol{ct}_{\boldsymbol{x}_j}]_T - [d_{i,j}]_T\right) + [zk_{\boldsymbol{F}}]_T$

$s \leftarrow \log([v]_T)$

Results I: Transformation from function-hiding IPFE to MIQFE

- Transformation from function-hiding IPFE to MIQFE keeping simulation security

Use IPFE to compute extra terms

“Interweave” terms from $\boldsymbol{F}_{i,j}$ and $\boldsymbol{F}_{j,i}$, in $d_{i,j}$:

Compute $c_j \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \boldsymbol{x}_i + \boldsymbol{x}_j^\top \boldsymbol{F}_{j,i} c_i \boldsymbol{u}_i + c_j \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} c_i \boldsymbol{u}_i$ for j, i

Compute $c_i \boldsymbol{u}_i^\top \boldsymbol{F}_{i,j} \boldsymbol{x}_j + \boldsymbol{x}_i^\top \boldsymbol{F}_{i,j} c_j \boldsymbol{u}_j + c_i \boldsymbol{u}_i^\top \boldsymbol{F}_{i,j} c_j \boldsymbol{u}_j$ for i, j

$\underline{\mathbf{Enc}^{\mathsf{MIQFE}}(\mathsf{msk}^{\mathsf{MIQFE}}, i, \boldsymbol{x}_i)}$:

$$\boldsymbol{ct}_{\boldsymbol{x}_i} := \boldsymbol{x}_i + c_i \boldsymbol{u}_i$$
$$c_{i,j} \leftarrow \mathsf{Enc}^{\mathsf{IPFE}}\left(\mathsf{msk}^{\mathsf{IPFE}}_{i,j}, \boldsymbol{w}_{i,j} + c_j \begin{pmatrix} \boldsymbol{ct}_{\boldsymbol{x}_i} \\ \boldsymbol{x}_i \end{pmatrix}\right)$$
$$c_{\boldsymbol{x}_i} = (\boldsymbol{ct}_{\boldsymbol{x}_i}, c_{i,j})$$

$\underline{\mathbf{KeyGen}^{\mathsf{MIQFE}}(\mathsf{msk}^{\mathsf{MIQFE}}, \boldsymbol{F})}$:

$$sk_{i,j} \leftarrow \mathsf{KeyGen}^{\mathsf{IPFE}}\left(\mathsf{msk}^{\mathsf{IPFE}}_{i,j}, \begin{pmatrix} \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \\ \boldsymbol{F}_{i,j} \boldsymbol{u}_j \end{pmatrix}\right)$$
$$zk_{\boldsymbol{F}} \leftarrow \sum_{i,j \in [\ell]} \boldsymbol{w}_{i,j}^\top \begin{pmatrix} \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \\ \boldsymbol{F}_{i,j} \boldsymbol{u}_j \end{pmatrix}$$
$$sk_{\boldsymbol{F}} = (\boldsymbol{F}, sk_{i,j}, zk_{\boldsymbol{F}})$$

$\underline{\mathbf{Dec}^{\mathsf{MIQFE}}(c_{\boldsymbol{x}_1}, \ldots, c_{\boldsymbol{x}_\ell}, sk_{\boldsymbol{F}})}$:

$$[d_{i,j}]_T \leftarrow \mathsf{IPFE.Dec}(\mathsf{IPFE}.c_{i,j}, \mathsf{IPFE}.sk_{i,j})$$
$$[v]_T := \left(\sum_{i,j \in [\ell]} [\boldsymbol{ct}_{\boldsymbol{x}_i}^\top \boldsymbol{F}_{i,j} \boldsymbol{ct}_{\boldsymbol{x}_j}]_T - [d_{i,j}]_T\right) + [zk_{\boldsymbol{F}}]_T$$
$$s \leftarrow \log([v]_T)$$

Results I: Transformation from function-hiding IPFE to MIQFE

- Transformation from function-hiding IPFE to MIQFE keeping simulation security

One-time pad $\boldsymbol{w}$ for IPFE input

To ensure output can only be recovered with all inputs

$\underline{\textbf{KeyGen}^{\text{MIQFE}}(\text{msk}^{\text{MIQFE}}, \boldsymbol{F})}$:

$$sk_{i,j} \leftarrow \text{KeyGen}^{\text{IPFE}}\left(\text{msk}^{\text{IPFE}}_{i,j}, \begin{pmatrix} \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \\ \boldsymbol{F}_{i,j}\boldsymbol{u}_j \end{pmatrix}\right)$$

$$zk_{\boldsymbol{F}} \leftarrow \sum_{i,j\in[\ell]} \boldsymbol{w}_{i,j}^\top \begin{pmatrix} \boldsymbol{u}_j^\top \boldsymbol{F}_{j,i} \\ \boldsymbol{F}_{i,j}\boldsymbol{u}_j \end{pmatrix}$$

$$sk_{\boldsymbol{F}} = (\boldsymbol{F}, sk_{i,j}, zk_{\boldsymbol{F}})$$

$\underline{\textbf{Enc}^{\text{MIQFE}}(\text{msk}^{\text{MIQFE}}, i, \boldsymbol{x}_i)}$:

$$\boldsymbol{ct}_{\boldsymbol{x}_i} := \boldsymbol{x}_i + c_i \boldsymbol{u}_i$$

$$c_{i,j} \leftarrow \text{Enc}^{\text{IPFE}}\left(\text{msk}^{\text{IPFE}}_{i,j}, \boldsymbol{w}_{i,j} + c_j \begin{pmatrix} \boldsymbol{ct}_{\boldsymbol{x}_i} \\ \boldsymbol{x}_i \end{pmatrix}\right)$$

$$c_{\boldsymbol{x}_i} = (\boldsymbol{ct}_{\boldsymbol{x}_i}, c_{i,j})$$

$\underline{\textbf{Dec}^{\text{MIQFE}}(c_{\boldsymbol{x}_1}, \ldots, c_{\boldsymbol{x}_\ell}, sk_{\boldsymbol{F}})}$:

$$[d_{i,j}]_T \leftarrow \text{IPFE.Dec}(\text{IPFE}.c_{i,j}, \text{IPFE}.sk_{i,j})$$

$$[v]_T := \left(\sum_{i,j\in[\ell]} [\boldsymbol{ct}_{\boldsymbol{x}_i}^\top \boldsymbol{F}_{i,j} \boldsymbol{ct}_{\boldsymbol{x}_j}]_T - [d_{i,j}]_T\right) + [zk_{\boldsymbol{F}}]_T$$

$$s \leftarrow \log([v]_T)$$

Results I: Transformation from function-hiding IPFE to MIQFE

- Transformation from function-hiding IPFE to MIQFE keeping simulation security

Theorem

The MIQFE *scheme is one selective multi-input simulation secure, if the underlying inner-product functional encryption scheme is one selective function-hiding simulation secure. In other words, for any* PPT *adversary $\mathcal{A}$ there exist* PPT *adversaries $\mathcal{B}$ such that*

$$\mathsf{Adv}^{\mathsf{MI-SIM}}_{\mathsf{MIQFE}}(\mathcal{A}) \leq \ell^2 \cdot \mathsf{Adv}^{\mathsf{FH\text{-}SIM}}_{\mathsf{IPFE}}(\mathcal{B}) + \frac{\ell}{p}.$$

- Proof intuition: First simulate $\boldsymbol{ct}_{\boldsymbol{x}_i}$ with uniformly at random and modify the rest accordingly. Then swap for the ℓ^2 function-hiding IPFE simulators. Finally use that $\boldsymbol{w}_{i,j}$ are uniformly at random to simulate $d_{i,j}$.

Results II: function-hiding IPFE

- We need simulation secure function-hiding IPFE

Table: State of the art.

Proposal	Functionality	Simulation security	Model
[Lin17, Lin CRYPTO'17]	FH-IPFE	✗	Standard
[KLM$^+$18, Kim et al. SCN'18]	FH-IPFE	✓	GGM

Results II: function-hiding IPFE

- We need simulation secure function-hiding IPFE

Table: State of the art.

Proposal	Functionality	Simulation security	Model
[Lin17, Lin CRYPTO'17]	FH-IPFE	✗	Standard
[KLM$^+$18, Kim et al. SCN'18]	FH-IPFE	✓	GGM
Our construction	FH-IPFE	✓	Standard

Results II: function-hiding IPFE

- Pairing-based from nesting twice an IPFE scheme
  - [ABCP15, Abdalla et al. PKC'15], for msk $= \boldsymbol{u}$ then

$$\underline{\mathbf{KeyGen}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{y})}:$$

$$sk_{\boldsymbol{y}} = \begin{pmatrix} -\boldsymbol{u}^\top \boldsymbol{y} \\ \boldsymbol{y} \end{pmatrix}$$

Results II: function-hiding IPFE

- Pairing-based from nesting twice an IPFE scheme
  - [ABCP15, Abdalla et al. PKC'15], for $\mathsf{msk} = \boldsymbol{u}$ then

$$\underline{\textbf{KeyGen}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{y})}: \\ sk_{\boldsymbol{y}} = \begin{pmatrix} -\boldsymbol{u}^\top \boldsymbol{y} \\ \boldsymbol{y} \end{pmatrix}$$

- To solve this

$$\mathsf{KeyGen}^{\mathsf{IPFE}}(\boldsymbol{y}) = \mathsf{KeyGen}^{\mathsf{out}}(\mathsf{Enc}^{\mathsf{in}}(\boldsymbol{y})) \mid \mathsf{Enc}^{\mathsf{IPFE}}(\boldsymbol{x}) = \mathsf{Enc}^{\mathsf{out}}(\mathsf{KeyGen}^{\mathsf{in}}(\boldsymbol{x}))$$

Results II: function-hiding IPFE

Pairing-friendly groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$
$$e([a]_1, [b]_2) \to [a \cdot b]_T$$

- Pairing-based from nesting twice an IPFE scheme

$$\mathsf{KeyGen}^{\mathsf{IPFE}}(\boldsymbol{y}) = \mathsf{KeyGen}^{\mathsf{out}}(\mathsf{Enc}^{\mathsf{in}}(\boldsymbol{y})) \mid \mathsf{Enc}^{\mathsf{IPFE}}(\boldsymbol{x}) = \mathsf{Enc}^{\mathsf{out}}(\mathsf{KeyGen}^{\mathsf{in}}(\boldsymbol{x}))$$

$\underline{\mathbf{SetUp}^{\mathsf{IPFE}}(1^\kappa, \mathcal{PG})}$:

$\boldsymbol{u} \overset{\$}{\leftarrow} \mathbb{Z}_p^{n+1}$, $\boldsymbol{v} \overset{\$}{\leftarrow} \mathbb{Z}_p^n$

$param^{\mathsf{IPFE}} = \mathcal{PG}$

$\mathsf{msk}^{\mathsf{IPFE}} = (\boldsymbol{u}, \boldsymbol{v})$

$\underline{\mathbf{KeyGen}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{y})}$:

$t \overset{\$}{\leftarrow} \mathbb{Z}_p$

$$sk_1 := \left[-\boldsymbol{u}^\top \begin{pmatrix} t \\ \boldsymbol{y} + t \cdot \boldsymbol{v} \end{pmatrix}\right]_2, \; sk_2 := \left[\begin{pmatrix} t \\ \boldsymbol{y} + t \cdot \boldsymbol{v} \end{pmatrix}\right]_2$$

$sk_{\boldsymbol{y}} = (sk_1, sk_2)$

$\underline{\mathbf{Enc}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{x})}$:

$c \overset{\$}{\leftarrow} \mathbb{Z}_p$

$$ct_1 := [c]_1, \; ct_2 := \left[\begin{pmatrix} -\boldsymbol{v}^\top \boldsymbol{x} \\ \boldsymbol{x} \end{pmatrix} + c \cdot \boldsymbol{u}\right]_1$$

$c_{\boldsymbol{x}} = (ct_1, ct_2)$

$\underline{\mathbf{Dec}^{\mathsf{IPFE}}(c_{\boldsymbol{x}}, sk_{\boldsymbol{y}})}$:

$[v]_T := e(ct_1, sk_1) + e(ct_2, sk_2)$

$s \leftarrow \log([v]_T)$

Results II: function-hiding IPFE

Pairing-friendly groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$
$$e([a]_1, [b]_2) \to [a \cdot b]_T$$

- Pairing-based from nesting twice an IPFE scheme

$$\mathsf{KeyGen}^{\mathsf{IPFE}}(\boldsymbol{y}) = \mathsf{KeyGen}^{\mathsf{out}}(\mathsf{Enc}^{\mathsf{in}}(\boldsymbol{y})) \mid \mathsf{Enc}^{\mathsf{IPFE}}(\boldsymbol{x}) = \mathsf{Enc}^{\mathsf{out}}(\mathsf{KeyGen}^{\mathsf{in}}(\boldsymbol{x}))$$

$\underline{\textbf{SetUp}^{\mathsf{IPFE}}(1^\kappa, \mathcal{PG})}$:

$\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_p^{n+1}$, $\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_p^{n}$

$param^{\mathsf{IPFE}} = \mathcal{PG}$

$\mathsf{msk}^{\mathsf{IPFE}} = (\boldsymbol{u}, \boldsymbol{v})$

$\underline{\textbf{KeyGen}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{y})}$:

$t \xleftarrow{\$} \mathbb{Z}_p$

$$sk_1 := \left[-\boldsymbol{u}^\top \begin{pmatrix} t \\ \boldsymbol{y} + t \cdot \boldsymbol{v} \end{pmatrix} \right]_2, \; sk_2 := \left[\begin{pmatrix} t \\ \boldsymbol{y} + t \cdot \boldsymbol{v} \end{pmatrix} \right]_2$$

$sk_{\boldsymbol{y}} = (sk_1, sk_2)$

$\underline{\textbf{Enc}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{x})}$:

$c \xleftarrow{\$} \mathbb{Z}_p$

$$ct_1 := [c]_1, \; ct_2 := \left[\begin{pmatrix} -\boldsymbol{v}^\top \boldsymbol{x} \\ \boldsymbol{x} \end{pmatrix} + c \cdot \boldsymbol{u} \right]_1$$

$c_{\boldsymbol{x}} = (ct_1, ct_2)$

$\underline{\textbf{Dec}^{\mathsf{IPFE}}(c_{\boldsymbol{x}}, sk_{\boldsymbol{y}})}$:

$[v]_T := e(ct_1, sk_1) + e(ct_2, sk_2)$

$s \leftarrow \log([v]_T)$

Results II: function-hiding IPFE

- Pairing-based from nesting twice an IPFE scheme

Theorem

The IPFE *scheme is one selective function-hiding simulation secure, if the* DDH *assumption holds in group* $\mathbb{G}_2$*. In other words, for any* PPT *adversary* $\mathcal{A}$ *there exists a* PPT *adversary* $\mathcal{B}$ *such that*

$$\mathsf{Adv}^{\mathsf{FH\text{-}SIM}}_{\mathsf{IPFE}}(\mathcal{A}) \leq 2Q_{sk} \cdot \mathsf{Adv}^{\mathsf{DDH}}_{\mathbb{G}_2}(\mathcal{B}) + \frac{1}{p} + \frac{2Q_{sk}}{p-1}.$$

where Q_{sk} *denotes the number of queries performed to* KeyGen*.*

- Proof intuition: First simulate ct_2 with uniformly at random. Then use the n-fold DDH assumption for each functional key query to simulate the functional keys.

Efficiency Considerations and Open Problems

Table: Efficiency estimates for our MIQFE and IPFE constructions.

	Secret key	Ciphertext (per input)	Functional key
Generic MIQFE	$\ell^2 \cdot \mathsf{IPFE}^{2n}_{\mathsf{msk}} + \ell(1+n)\lvert p\rvert + \ell^2 2n\lvert p\rvert$	$\ell \cdot \mathsf{IPFE}^{2n}_{c_x} + n\lvert p\rvert$	$\ell^2 \cdot \mathsf{IPFE}^{2n}_{sk_y} + \lvert p\rvert$
FH-IPFE	$(2n+1)\lvert p\rvert$	$(n+2)\lvert\mathbb{G}_1\rvert$	$(n+2)\lvert\mathbb{G}_2\rvert$
Concrete MIQFE	$\ell^2(4n+1)\lvert p\rvert + \ell(1+n)\lvert p\rvert + \ell^2 2n\lvert p\rvert$	$\ell \cdot (2n+2)\lvert\mathbb{G}_1\rvert + n\lvert p\rvert$	$\ell^2 \cdot (2n+2)\lvert\mathbb{G}_2\rvert + \lvert p\rvert$

Efficiency Considerations and Open Problems

Table: Efficiency estimates for our MIQFE and IPFE constructions.

	Secret key	Ciphertext (per input)	Functional key
Generic MIQFE	$\ell^2 \cdot \mathsf{IPFE}^{2n}_{\mathsf{msk}} + \ell(1+n)\lvert p\rvert + \ell^2 2n\lvert p\rvert$	$\ell \cdot \mathsf{IPFE}^{2n}_{c_x} + n\lvert p\rvert$	$\ell^2 \cdot \mathsf{IPFE}^{2n}_{sk_y} + \lvert p\rvert$
FH-IPFE	$(2n+1)\lvert p\rvert$	$(n+2)\lvert\mathbb{G}_1\rvert$	$(n+2)\lvert\mathbb{G}_2\rvert$
Concrete MIQFE	$\ell^2(4n+1)\lvert p\rvert + \ell(1+n)\lvert p\rvert + \ell^2 2n\lvert p\rvert$	$\ell \cdot (2n+2)\lvert\mathbb{G}_1\rvert + n\lvert p\rvert$	$\ell^2 \cdot (2n+2)\lvert\mathbb{G}_2\rvert + \lvert p\rvert$

Open problems:

- Improving ciphertext size to $O(n\ell)$
- Transformation directly from QFE

Thank you for your attention

Questions?

Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval.
Simple functional encryption schemes for inner products.
In Jonathan Katz, editor, *Public-Key Cryptography – PKC 2015*, pages 733–751, Berlin, Heidelberg, 2015. Springer.

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.
In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 597–627, Cham, 2018. Springer International Publishing.

Ferran Alborch Escobar, Sébastien Canard, Fabien Laguillaumie, and Duong Hieu Phan.
Computational differential privacy for encrypted databases supporting linear queries.
Proceedings on Privacy Enhancing Technologies, 2024(4):583—-604, 2024.

Shweta Agrawal, Rishab Goyal, and Junichi Tomida.
Multi-input quadratic functional encryption: Stronger security, broader functionality.
In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography*, pages 711–740, Cham, 2022. Springer Nature Switzerland.

Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee.
Functional encryption: New perspectives and lower bounds.
In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, pages 500–518, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

Dan Boneh, Amit Sahai, and Brent Waters.
Functional encryption: Definitions and challenges.
In Yuval Ishai, editor, *Theory of Cryptography*, pages 253–273, Berlin, Heidelberg, 2011. Springer.

Romain Gay.
A new paradigm for public-key functional encryption for degree-2 polynomials.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 95–120, Cham, 2020. Springer International Publishing.

Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou.
Multi-input functional encryption.

In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, pages 578–602, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

Sam Kim, Kevin Lewi, Avradip Mandal, Hart Montgomery, Arnab Roy, and David J. Wu.
Function-hiding inner product encryption is practical.
In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks*, pages 544–562, Cham, 2018. Springer International Publishing.

Huijia Lin.
Indistinguishability obfuscation from sxdh on 5-linear maps and locality-5 prgs.
In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 599–629, Cham, 2017. Springer International Publishing.

Emily Shen, Elaine Shi, and Brent Waters.
Predicate privacy in encryption systems.
In Omer Reingold, editor, *Theory of Cryptography*, pages 457–473, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

Runhua Xu, Nathalie Baracaldo, Yi Zhou, Ali Anwar, and Heiko Ludwig.
Hybridalpha: An efficient approach for privacy-preserving federated learning.

In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, AISec'19, page 13–23, New York, NY, USA, 2019. Association for Computing Machinery.