Indistinguishability Obfuscation Without Maps: Attacks and Fixes for Noisy Linear FE

Shweta Agrawal[1], **Alice Pellet-Mary**[2]

[1] IIT Madras, [2] KU Leuven

Eurocrypt 2020

https://eprint.iacr.org/2020/415.pdf

What is this talk about?

Cryptanalytic study of an iO construction [Agr19].

[Agr19] S. Agrawal. Indistinguishability obfuscation without multilinear maps: New techniques for bootstrapping and instantiation. Eurocrypt.

What is this talk about?

Cryptanalytic study of an iO construction [Agr19].

$\Rightarrow$ 2 attacks

$\Rightarrow$ 1 repaired construction

[Agr19] S. Agrawal. Indistinguishability obfuscation without multilinear maps: New techniques for bootstrapping and instantiation. Eurocrypt.

Obfuscation

iO is "crypto-complete": implies witness encryption, functional encryption, deniable encryption, oblivious transfer, traitor tracing, multilinear maps...

Two main approaches to build candidate iO:

- Direct constructions
  - using multilinear maps
- Bootstrapping approaches
  - reduction to weak forms of functional encryption

References can be found at https://tel.archives-ouvertes.fr/tel-02337930/document, page 107

Obfuscation

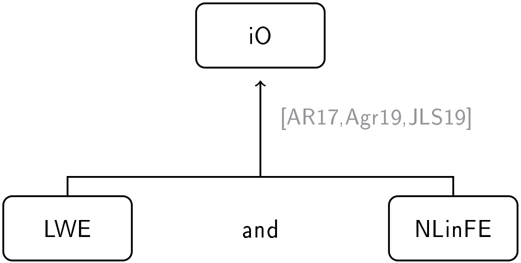
iO is "crypto-complete": implies witness encryption, functional encryption, deniable encryption, oblivious transfer, traitor tracing, multilinear maps...

Two main approaches to build candidate iO:

- Direct constructions
  - using multilinear maps
- Bootstrapping approaches
  - reduction to weak forms of functional encryption

References can be found at https://tel.archives-ouvertes.fr/tel-02337930/document, page 107

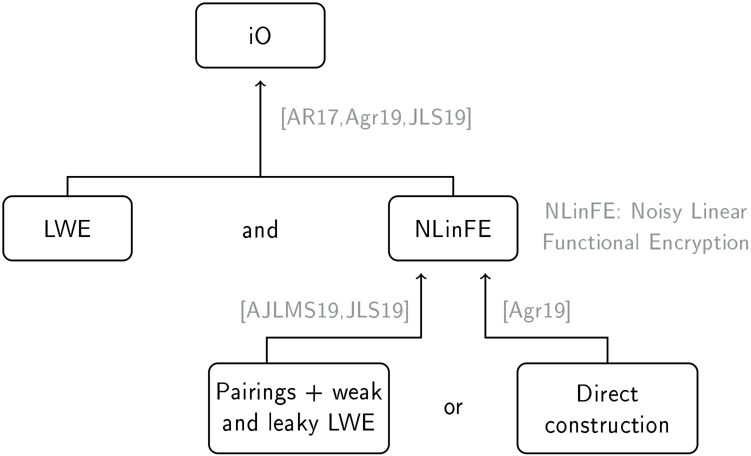
Agrawal's construction of iO



NLinFE: Noisy Linear Functional Encryption

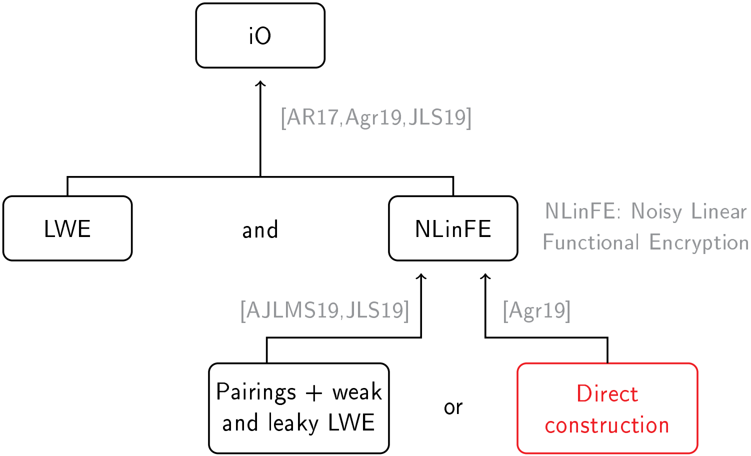
[AR17] S. Agrawal and A. Rosen. Functional encryption for bounded collusions, revisited. TCC.
[Agr19] S. Agrawal. Indistinguishability obfuscation without multilinear maps: New techniques for bootstrapping and instantiation. Eurocrypt.
[JLS19] A. Jain and H. Lin and A. Sahai. Simplifying Constructions and Assumptions for iO. ePrint.

Agrawal's construction of iO



[Agr19] S. Agrawal. Indistinguishability obfuscation without multilinear maps: New techniques for bootstrapping and instantiation. Eurocrypt.
[AJLMS19] P. Ananth, A. Jain, H. Lin, C. Matt and A. Sahai. Indistinguishability Obfuscation Without Multilinear Maps: New Paradigms via Low Degree Weak Pseudorandomness and Security Amplification. Crypto.
[JLS19] A. Jain, H. Lin and A. Sahai. Simplifying Constructions and Assumptions for iO. ePrint.

Agrawal's construction of iO



[Agr19] S. Agrawal. Indistinguishability obfuscation without multilinear maps: New techniques for bootstrapping and instantiation. Eurocrypt.
[AJLMS19] P. Ananth, A. Jain, H. Lin, C. Matt and A. Sahai. Indistinguishability Obfuscation Without Multilinear Maps: New Paradigms via Low Degree Weak Pseudorandomness and Security Amplification. Crypto.
[JLS19] A. Jain, H. Lin and A. Sahai. Simplifying Constructions and Assumptions for iO. ePrint.

NLinFE

Authority

User

$\mathrm{ct}_{\vec{x}} \leftarrow \mathtt{Enc}(\mathrm{MSK}, \vec{x})$

$\mathrm{sk}_{\vec{z}} \leftarrow \mathtt{KeyGen}(\mathrm{MSK}, \vec{z})$

$\mathtt{Dec}(\mathrm{sk}_{\vec{z}}, \mathrm{ct}_{\vec{x}}) = \langle \vec{z}, \vec{x} \rangle$

$\Rightarrow$ hides everything except $\langle \vec{z}, \vec{x} \rangle$

LinFE

NLinFE

Authority

User

$\mathrm{ct}_{\vec{x}} \leftarrow \texttt{Enc}(\mathrm{MSK}, \vec{x})$

$\mathrm{sk}_{\vec{z}} \leftarrow \texttt{KeyGen}(\mathrm{MSK}, \vec{z})$

$\texttt{Dec}(\mathrm{sk}_{\vec{z}}, \mathrm{ct}_{\vec{x}}) = \langle \vec{z}, \vec{x} \rangle + \text{noise}$

$\Rightarrow$ hides everything except $\approx \langle \vec{z}, \vec{x} \rangle$

$\Rightarrow$ hides the last bits of $\langle \vec{z}, \vec{x} \rangle$

NLinFE

Previous work and contributions

[Agr19]: proved her construction secure in a weak model (under non standard assumptions) if **only one** ciphertext available to the attacker

Our contribution: more cryptanalysis

Previous work and contributions

[Agr19]: proved her construction secure in a weak model (under non standard assumptions) if **only one** ciphertext available to the attacker

Our contribution: more cryptanalysis

- Two attacks (using multiple ciphertexts)
  - multi-ciphertexts attack
  - rank attack

Previous work and contributions

[Agr19]: proved her construction secure in a weak model (under non standard assumptions) if **only one** ciphertext available to the attacker

Our contribution: more cryptanalysis

- Two attacks (using multiple ciphertexts)
  - multi-ciphertexts attack
  - rank attack
- A fixed construction
  - prevents the two attacks
  - we also study other possible attacks
  - propose parameters setting which we believe is secure (even quantumly)

Outline of the talk

1. Multi-ciphertexts attack

2. Rank attack

Outline of the talk

1. Multi-ciphertexts attack

2. Rank attack

RLWE with correlated noise

Notations

Everything in $R_q = \mathbb{Z}_q[X]/(X^n + 1)$
blue: small

RLWE with correlated noise

Notations

Everything in $R_q = \mathbb{Z}_q[X]/(X^n + 1)$
blue: small

Multiple-small-secrets RLWE: Distinguish uniform in R_q from

$$\Big(a_i \,,\, b_{ij} = a_i s_j + e_{ij} \bmod q\Big)_{i,j}$$

RLWE with correlated noise

Notations

Everything in $R_q = \mathbb{Z}_q[X]/(X^n+1)$
blue: small

Multiple-small-secrets RLWE: Distinguish uniform in R_q from

$$\Big(a_i\,,\, b_{ij} = a_i s_j + e_{ij} \bmod q\Big)_{i,j}$$

[Agr19]'s construction needs multiplicativity of the ciphertexts

$$b_{ij} b_{k\ell} = \underbrace{a_i a_k}_{a'} \cdot \underbrace{s_j s_\ell}_{s'} + \underbrace{a_i s_j \cdot e_{k\ell} + a_k s_\ell \cdot e_{ij}}_{\text{too large}} + \underbrace{e_{ij} e_{k\ell}}_{\text{small}}$$

RLWE with correlated noise

Notations

Everything in $R_q = \mathbb{Z}_q[X]/(X^n + 1)$
blue: small

NTRU

$$\frac{f_i}{g} \bmod q \approx_c \text{unif}$$

RLWE with correlated noise: Distinguish uniform in R_q from

$$\left(a_i = \frac{f_i}{g},\; b_{ij} = a_i s_j + g \cdot e_{ij} \bmod q\right)_{i,j}$$

[Agr19]'s construction needs multiplicativity of the ciphertexts

$$b_{ij} b_{k\ell} = \underbrace{a_i a_k}_{a'} \cdot \underbrace{s_j s_\ell}_{s'} + \underbrace{a_i s_j \cdot g e_{k\ell} + a_k s_\ell \cdot g e_{ij}}_{\text{too large}} + \underbrace{g^2 e_{ij} e_{k\ell}}_{\text{small}}$$

RLWE with correlated noise

Notations

Everything in $R_q = \mathbb{Z}_q[X]/(X^n+1)$
blue: small

NTRU

$$\frac{f_i}{g} \bmod q \approx_c \text{unif}$$

RLWE with correlated noise: Distinguish uniform in R_q from

$$\left(a_i = \frac{f_i}{g},\ b_{ij} = a_i s_j + g \cdot e_{ij} \bmod q\right)_{i,j}$$

[Agr19]'s construction needs multiplicativity of the ciphertexts

$$b_{ij} b_{k\ell} = \underbrace{a_i a_k}_{a'} \cdot \underbrace{s_j s_\ell}_{s'} + \underbrace{f_i s_j \cdot e_{k\ell} + f_k s_\ell \cdot e_{ij}}_{\text{small}} + \underbrace{g^2 e_{ij} e_{k\ell}}_{\text{small}} \quad ✓$$

Simple distinguishing attack

Input:

(2 labels, 1 secret)

$$\left(a_1 = \frac{f_1}{g}\,,\ b_1 = a_1 s + g e_1\right)$$

$$\left(a_2 = \frac{f_2}{g}\,,\ b_2 = a_2 s + g e_2\right)$$

Simple distinguishing attack

Input:

(2 labels, 1 secret)

$$(a_1 = \frac{f_1}{g}\,,\ b_1 = a_1 s + g e_1)$$

$$(a_2 = \frac{f_2}{g}\,,\ b_2 = a_2 s + g e_2)$$

Attack:

$$a_1 b_2 - a_2 b_1 = a_1 a_2 s + a_1 g e_2 - a_2 a_1 s - a_2 g e_1$$

Simple distinguishing attack

Input:

(2 labels, 1 secret)

$$(a_1 = \frac{f_1}{g},\ b_1 = a_1 s + g e_1)$$

$$(a_2 = \frac{f_2}{g},\ b_2 = a_2 s + g e_2)$$

Attack:

$$a_1 b_2 - a_2 b_1 = \cancel{a_1 a_2 s} + a_1 g e_2 - \cancel{a_2 a_1 s} - a_2 g e_1$$

Simple distinguishing attack

Input:

(2 labels, 1 secret)

$$\left(a_1 = \frac{f_1}{g},\ b_1 = a_1 s + g e_1\right)$$

$$\left(a_2 = \frac{f_2}{g},\ b_2 = a_2 s + g e_2\right)$$

Attack:

$$a_1 b_2 - a_2 b_1 = \underbrace{f_1 e_2 - f_2 e_1}_{\text{small}}$$

Simple distinguishing attack

Input:

(2 labels, 1 secret)

$$(a_1 = \frac{f_1}{g}, \; b_1 = a_1 s + g e_1)$$

$$(a_2 = \frac{f_2}{g}, \; b_2 = a_2 s + g e_2)$$

Attack:

$$a_1 b_2 - a_2 b_1 = \underbrace{f_1 e_2 - f_2 e_1}_{\text{small}}$$

$\Rightarrow$ can be distinguished from uniform

Simple distinguishing attack

Input:

(2 labels, 1 secret)

$$\left(a_1 = \frac{f_1}{g}\,,\ b_1 = a_1 s + g e_1\right)$$

$$\left(a_2 = \frac{f_2}{g}\,,\ b_2 = a_2 s + g e_2\right)$$

Attack:

$$a_1 b_2 - a_2 b_1 = \underbrace{f_1 e_2 - f_2 e_1}_{\text{small}}$$

$\Rightarrow$ can be distinguished from uniform

Fix: the a_i's need not be public

Multi-ciphertexts attack

Input:
(2 labels, 1 secret)

$$b_{11} = a_1 s_1 + g e_{11} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad (a_2 = \frac{f_2}{g})$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \frac{f_2}{g})$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \frac{f_2}{g})$$

Attack:

$$\boxed{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \frac{f_2}{g})$$

Attack:

$$\boxed{B} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} s_1 & s_2 \end{pmatrix} + g \cdot \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}$$

Multi-ciphertexts attack

Input:

(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \frac{f_2}{g})$$

Attack:

$$\boxed{B} = \frac{1}{g} \cdot \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \begin{pmatrix} s_1 & s_2 \end{pmatrix} + g \cdot \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \tfrac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \tfrac{f_2}{g})$$

Attack:

$$B = \frac{1}{g} \cdot C + g \cdot E$$

$$\mathrm{rank}(C) = 1$$

$$\mathrm{rank}(E) = 2$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \frac{f_2}{g})$$

Attack:

$$B = \frac{1}{g} \cdot C + g \cdot E \qquad \mathrm{rank}(C) = 1, \quad \mathrm{rank}(E) = 2$$

$$\det(B) = \frac{1}{g^2} \cdot \det(C) + \det(C_1 | E_2) + \det(E_1 | C_2) + g^2 \cdot \det(E)$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad \left(a_1 = \frac{f_1}{g}\right)$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad \left(a_2 = \frac{f_2}{g}\right)$$

Attack:

$$B = \frac{1}{g} \cdot C + g \cdot E \qquad \mathrm{rank}(C) = 1, \quad \mathrm{rank}(E) = 2$$

$$\det(B) = \underbrace{\frac{1}{g^2} \cdot \det(C)}_{=0} + \underbrace{\det(C_1 | E_2) + \det(E_1 | C_2) + g^2 \cdot \det(E)}_{\text{small}}$$

Multi-ciphertexts attack

Input:
(2 labels, 2 secrets)

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad \left(a_1 = \frac{f_1}{g}\right)$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad \left(a_2 = \frac{f_2}{g}\right)$$

Attack:

$$B = \frac{1}{g} \cdot C + g \cdot E \qquad \mathrm{rank}(C) = 1, \quad \mathrm{rank}(E) = 2$$

$$\det(B) = \underbrace{\frac{1}{g^2} \cdot \det(C)}_{=0} + \underbrace{\det(C_1 \,|\, E_2) + \det(E_1 \,|\, C_2) + g^2 \cdot \det(E)}_{\text{small}}$$

$\Rightarrow$ can be distinguished from uniform

Fixing the multi-ciphertexts attack

Fix: ensure that $\text{rank}(C) = 2$

Fixing the multi-ciphertexts attack

Fix: ensure that $\mathrm{rank}(C) = 2$

Input:

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \tfrac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \tfrac{f_2}{g})$$

Attack:

$$B = \frac{1}{g} \cdot C + g \cdot E$$

$$\mathrm{rank}(C) = 1$$

$$\mathrm{rank}(E) = 2$$

$$\det(B) = \underbrace{\frac{1}{g^2} \cdot \det(C)}_{=0} + \underbrace{\det(C_1 | E_2) + \det(E_1 | C_2) + g^2 \cdot \det(E)}_{\text{small}}$$

Fixing the multi-ciphertexts attack

Fix: ensure that rank(C) = 2

Input:

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \tfrac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \tfrac{f_2}{g})$$

Attack:

$$B = \frac{1}{g} \cdot C + g \cdot E$$

rank(C) = 2

rank(E) = 2

$$\det(B) = \underbrace{\frac{1}{g^2} \cdot \det(C)}_{\text{large}} + \underbrace{\det(C_1 | E_2) + \det(E_1 | C_2) + g^2 \cdot \det(E)}_{\text{small}}$$

Fixing the multi-ciphertexts attack

Fix: ensure that $\mathrm{rank}(C) = 2$

Input:

$$b_{11} = a_1 s_1 + g e_{11} \qquad b_{12} = a_1 s_2 + g e_{12} \qquad (a_1 = \tfrac{f_1}{g})$$

$$b_{21} = a_2 s_1 + g e_{21} \qquad b_{22} = a_2 s_2 + g e_{22} \qquad (a_2 = \tfrac{f_2}{g})$$

Attack:

$$\boxed{B} = \frac{1}{g} \cdot \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \begin{pmatrix} s_1 & s_2 \end{pmatrix} + g \cdot \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}$$

Fixing the multi-ciphertexts attack

Fix: ensure that $\text{rank}(C) = 2$

Input:

$$b_{11} = \langle a_1, s_1 \rangle + g e_{11} \qquad b_{12} = \langle a_1, s_2 \rangle + g e_{12} \qquad (a_1 = \frac{f_1}{g})$$

$$b_{21} = \langle a_2, s_1 \rangle + g e_{21} \qquad b_{22} = \langle a_2, s_2 \rangle + g e_{22} \qquad (a_2 = \frac{f_2}{g})$$

Attack:

$$\boxed{B} = \frac{1}{g} \cdot \begin{pmatrix} — & f_1 & — \\ — & f_2 & — \end{pmatrix} \begin{pmatrix} | & | \\ s_1 & s_2 \\ | & | \end{pmatrix} + g \cdot \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}$$

Fixing the multi-ciphertexts attack

Fix: ensure that $\mathrm{rank}(C) = 2$

Input:

$$b_{11} = \langle a_1, s_1 \rangle + g e_{11} \qquad b_{12} = \langle a_1, s_2 \rangle + g e_{12} \qquad (a_1 = \tfrac{f_1}{g})$$

$$b_{21} = \langle a_2, s_1 \rangle + g e_{21} \qquad b_{22} = \langle a_2, s_2 \rangle + g e_{22} \qquad (a_2 = \tfrac{f_2}{g})$$

Attack:

$$\boxed{\;B\;} = \frac{1}{g} \cdot \begin{pmatrix} - & f_1 & - \\ - & f_2 & - \end{pmatrix} \begin{pmatrix} | & | \\ s_1 & s_2 \\ | & | \end{pmatrix} + g \cdot \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}$$

$\Rightarrow$ "Module-LWE with correlated noise" seems to prevent the attack

(if dim of vectors is large enough)

Outline of the talk

1. Multi-ciphertexts attack

2. Rank attack

Context

The adversary can honestly play the following game

$\mathcal{C}$		$\mathcal{A}$
sample $b \leftarrow \{0,1\}$		sample μ small
	$\xleftarrow{\mu}$	
compute large noise N if $b = 0$ $\quad x \leftarrow N$ if $b = 1$ $\quad x \leftarrow N + \mu$		repeat
	$\xrightarrow{x}$	
		guess b

The noise term N

$$N = \sum_{\ell,i,j} v_{ij}^{\times} \Big[p_1^2 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$+ p_1 p_0 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$+ p_1 (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$

$$+ p_0^2 \cdot (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$

$$+ p_0 (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell) \Big]$$

The noise term N

$$
\begin{aligned}
N = \sum_{\ell,i,j} v_{ij}^{\times} \Big[& p_1^2 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell) \\
& + p_1 p_0 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell) \\
& + p_1 (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell) \\
& + p_0^2 \cdot (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell) \\
& + p_0 (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell) \Big]
\end{aligned}
$$

p_0, p_1 are known and $p_1 \gg p_0 \gg$ all the rest

$\Rightarrow$ can split the noise terms according to p_1^2, $p_1 p_0$, p_1, p_0^2 and p_0.

The noise term N

$$N \bmod p_1^2 = \sum_{\ell,i,j} v_{ij}^{\times} \Big[p_1^2 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$
$$+ p_1 p_0 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$
$$+ p_1 (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$
$$+ p_0^2 \cdot (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$
$$+ p_0 (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell) \Big]$$

p_0, p_1 are known and $p_1 \gg p_0 \gg$ all the rest

$\Rightarrow$ can split the noise terms according to p_1^2, $p_1 p_0$, p_1, p_0^2 and p_0.

The noise term N

$$(N \bmod p_1^2) \bmod p_1 p_0 = \sum_{\ell,i,j} v_{ij}^{\times} \Big[p_1^2 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$
$$+ p_1 p_0 \cdot (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$
$$+ p_1 (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$
$$+ p_0^2 \cdot (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$
$$+ p_0 (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell) \Big]$$

p_0, p_1 are known and $p_1 \gg p_0 \gg$ all the rest

$\Rightarrow$ can split the noise terms according to p_1^2, $p_1 p_0$, p_1, p_0^2 and p_0.

The rank attack

$$p_1^2 \cdot \sum_{\ell,i,j} v_{ij}^{\times} \quad (g_2^{\ell} \cdot \tilde{\xi}_{1i}^{\ell} \cdot g_1^{\ell} \cdot \tilde{\xi}_{2j}^{\ell})$$

$$p_1 p_0 \cdot \sum_{\ell,i,j} v_{ij}^{\times} \quad (g_2^{\ell} \cdot \tilde{\xi}_{1i}^{\ell} \cdot g_1^{\ell} \cdot \xi_{2j}^{\ell} + g_2^{\ell} \cdot \xi_{1i}^{\ell} \cdot g_1^{\ell} \cdot \tilde{\xi}_{2j}^{\ell})$$

$$p_1 \cdot \sum_{\ell,i,j} v_{ij}^{\times} \quad (f_{1i}^{\ell} \cdot t_1 \cdot \tilde{\xi}_{2j}^{\ell} + f_{2j}^{\ell} \cdot t_2 \cdot \tilde{\xi}_{1i}^{\ell})$$

$$p_0^2 \cdot \sum_{\ell,i,j} v_{ij}^{\times} \quad (g_2^{\ell} \cdot \xi_{1i}^{\ell} \cdot g_1^{\ell} \cdot \xi_{2j}^{\ell})$$

$$p_0 \cdot \sum_{\ell,i,j} v_{ij}^{\times} \quad (f_{1i}^{\ell} \cdot t_1 \cdot \xi_{2j}^{\ell} + f_{2j}^{\ell} \cdot t_2 \cdot \xi_{1i}^{\ell})$$

The rank attack

$$\sum_{\ell,i,j} v_{ij}^{\times} \;\; (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \;\; (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \;\; (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \;\; (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \;\; (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell)$$

The rank attack

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell)$$

green: good noise terms (hide the challenge)
red: bad noise terms (do not hide the challenge)

The rank attack

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$

$$\sum_{\ell,i,j} v_{ij}^{\times} \ \ (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$

$$\boxed{\sum_{\ell,i,j} v_{ij}^{\times} \ \ (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell) + (0 \text{ or } \mu)}$$

green: good noise terms (hide the challenge)
red: bad noise terms (do not hide the challenge)

Fixing the rank attack

Idea: remove the moduli p_0 and p_1 $\Rightarrow$ cannot split the noise term anymore

$$N = \sum_{\ell,i,j} v_{ij}^{\times} \Big[p_1^2 (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$
$$+ p_1 p_0 (g_2^\ell \cdot \tilde{\xi}_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell + g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \tilde{\xi}_{2j}^\ell)$$
$$+ p_1 (f_{1i}^\ell \cdot t_1 \cdot \tilde{\xi}_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \tilde{\xi}_{1i}^\ell)$$
$$+ p_0^2 (g_2^\ell \cdot \xi_{1i}^\ell \cdot g_1^\ell \cdot \xi_{2j}^\ell)$$
$$+ p_0 (f_{1i}^\ell \cdot t_1 \cdot \xi_{2j}^\ell + f_{2j}^\ell \cdot t_2 \cdot \xi_{1i}^\ell) \Big]$$

Further cryptanalysis

- Describe other potential attacks
  - what can be obtained from these attacks
  - why this does not break the scheme
    or what constraint on parameters prevents the attack

Further cryptanalysis

- Describe other potential attacks
  - what can be obtained from these attacks
  - why this does not break the scheme
    or what constraint on parameters prevents the attack
- Quantum computer does not seem to help the attacker

Further cryptanalysis

- Describe other potential attacks
  - what can be obtained from these attacks
  - why this does not break the scheme
    or what constraint on parameters prevents the attack
- Quantum computer does not seem to help the attacker
- Propose a concrete set of parameters (asymptotic)
  - see Section 7.7

https://eprint.iacr.org/2020/415.pdf

Open problems

- Prove the scheme from simpler assumptions (cf [JLS19])?
  - e.g., module-LWE with correlated noise $+ \cdots$?
- Find different attacks?
  - The 2 attacks share similarities with attacks against multilinear map based obfuscators, why?

[JLS19] A. Jain and H. Lin and A. Sahai. Simplifying Constructions and Assumptions for iO. ePrint.

Open problems

- Prove the scheme from simpler assumptions (cf [JLS19])?
  - e.g., module-LWE with correlated noise $+ \cdots$?
- Find different attacks?
  - The 2 attacks share similarities with attacks against multilinear map based obfuscators, why?

Thank you

[JLS19] A. Jain and H. Lin and A. Sahai. Simplifying Constructions and Assumptions for iO. ePrint.