GGH15 encodings for branching programs: **proofs** and **attacks**

Hoeteck Wee
CNRS & ENS

Yilei Chen (**BU**)
Vinod Vaikuntanathan (**MIT**)

GGH15 encodings

[**Gentry Gorbunov Halevi 15**]

– candidate for noisy **multi-linear** maps

[**Boneh Silverberg 03, Garg Gentry Halevi 13, Coron Lepoint Tibouchi 13**]

GGH15 encodings

[Gentry Gorbunov Halevi 15]

today. randomizing a **branching program** s.t.

i. hide program **ii.** some **functionality**

GGH15 encodings

[Gentry Gorbunov Halevi 15]

today. randomizing a **branching program** s.t.

i. hide program **ii.** some **functionality**

applications. from **LWE**

GGH15 encodings

[Gentry Gorbunov Halevi 15]

today. randomizing a **branching program** s.t.

i. **hide** program **ii.** some **functionality**

applications. from **LWE**

– private constrained PRFs **[Canetti Chen 17]**

– lockable obfuscation **[Goyal Koppula Waters, Wichs Zirdelis 17]**

– traitor tracing **[Goyal Koppula Waters 18, CVWWW 18]**

GGH15 encodings

[Gentry Gorbunov Halevi 15]

today. randomizing a **branching program** s.t.

i. hide program **ii.** some **functionality**

this talk.

1 **GGH15 encodings**: construction and proofs

GGH15 encodings

[Gentry Gorbunov Halevi 15]

today. randomizing a **branching program** s.t.

i. hide program **ii.** some **functionality**

this talk.

1. **GGH15 encodings**: construction and proofs
2. **obfuscation**: candidates and attacks

LWE assumption [Regev 05]

$$(\mathbf{A},\ \mathbf{s}\mathbf{A}+\mathbf{e}) \approx_c \text{uniform}$$

LWE assumption [Regev 05]

$$(\mathbf{A},\ \mathbf{SA}+\mathbf{E}) \approx_c \text{uniform}$$

LWE assumption [Regev 05]

$$(\mathbf{A},\ (\mathbf{I}_2 \otimes \mathbf{S})\mathbf{A} + \mathbf{E}) \approx_c \text{uniform}$$

$$\begin{bmatrix} \mathbf{S} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{bmatrix} \begin{bmatrix} \mathbf{A} \end{bmatrix} + \begin{bmatrix} \mathbf{E} \end{bmatrix}$$

LWE assumption [Regev 05]

$$(\mathbf{A},\ (\mathbf{I}_2 \otimes \mathbf{S})\mathbf{A} + \mathbf{E}) \approx_c \text{uniform}$$

$$\begin{bmatrix} \mathbf{S} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{bmatrix} \begin{bmatrix} \overline{\mathbf{A}} \\ \underline{\mathbf{A}} \end{bmatrix} + \begin{bmatrix} \mathbf{E} \end{bmatrix}$$

LWE assumption [Regev 05]

$$(\mathbf{A},\ (\mathbf{I}_2 \otimes \mathbf{S})\mathbf{A} + \mathbf{E}) \approx_c \text{uniform}$$

$$\boxed{\begin{matrix}\mathbf{S}\overline{\mathbf{A}} \\ \mathbf{S}\underline{\mathbf{A}}\end{matrix}} + \boxed{\mathbf{E}}$$

LWE assumption [Regev 05]

$$(\mathbf{A},\ (\mathbf{M} \otimes \mathbf{S})\mathbf{A} + \mathbf{E}) \approx_c \text{uniform}$$

$$\boxed{(\mathbf{M} \otimes \mathbf{S})\mathbf{A}} + \boxed{\quad \mathbf{E} \quad}$$

for any **permutation** matrix $\mathbf{M}$

LWE assumption [Regev 05]

$$(\mathbf{A}, \ \underset{\sim}{(\mathbf{M} \otimes \mathbf{S})\mathbf{A}}) \approx_c \text{uniform}$$

$$\boxed{(\mathbf{M} \otimes \mathbf{S})\mathbf{A}} + \boxed{\quad \mathbf{E} \quad}$$

for any **permutation** matrix $\mathbf{M}$

branching programs

$$\begin{matrix} \mathbf{M}_{1,0} & \mathbf{M}_{2,0} & \cdots & \mathbf{M}_{\ell,0} \\ \mathbf{M}_{1,1} & \mathbf{M}_{2,1} & \cdots & \mathbf{M}_{\ell,1} \end{matrix}$$

branching programs

$$\begin{array}{cccc} \boxed{\mathbf{M}_{1,0}} & \mathbf{M}_{2,0} & \cdots & \boxed{\mathbf{M}_{\ell,0}} \\ \mathbf{M}_{1,1} & \boxed{\mathbf{M}_{2,1}} & \cdots & \mathbf{M}_{\ell,1} \end{array}$$

evaluation. $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_i} \stackrel{?}{=}$ fixed matrix

branching programs

$$\begin{matrix} (a_1) & (a_2) & \cdots & (a_n) \\ (1-a_1) & (1-a_2) & \cdots & (1-a_n) \end{matrix}$$

evaluation. $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_i} \stackrel{?}{=}$ fixed matrix

example. $f_{\mathbf{a}}(\mathbf{x}) = 1$ iff $\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} 0$ (1×1 matrices)

branching programs

$$\begin{array}{cccc} (a_1) & (a_2) & \cdots & (a_n) \\ (1-a_1) & (1-a_2) & \cdots & (1-a_n) \end{array}$$

evaluation. $\mathbf{M_x} = \prod \mathbf{M}_{i,x_i} \stackrel{?}{=}$ fixed matrix

example. $f_\mathbf{a}(\mathbf{x}) = 1$ iff $\mathbf{M_x} \stackrel{?}{=} 0$ (1×1 matrices)

$f_\mathbf{a}(\mathbf{x}) = (\mathbf{x} \stackrel{?}{\neq} \mathbf{a})$ point functions

branching programs

$$\begin{matrix} \boxed{\mathbf{M}_{1,0}} & \mathbf{M}_{2,0} & \cdots & \boxed{\mathbf{M}_{\ell,0}} \\ \mathbf{M}_{1,1} & \boxed{\mathbf{M}_{2,1}} & \cdots & \mathbf{M}_{\ell,1} \end{matrix}$$

evaluation. $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_i} \stackrel{?}{=}$ fixed matrix

barrington's. 5×5 permutation matrices = NC^1

❶ **GGH15** encodings

construction and proofs

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$\mathbf{M}_{1,0}$ $\mathbf{M}_{2,0}$

$\mathbf{M}_{1,1}$ $\mathbf{M}_{2,1}$

evaluation. $\mathbf{M}_{\mathbf{x}}$

goals. **i.** **hide** program **ii.** some **functionality**

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0}$ $\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0}$

$\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1}$ $\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1}$

evaluation. $\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}}$

goals. i. hide program **ii.** some **functionality**

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$\mathbf{A}_0$

$\mathbf{A}_0^{-1}(\ \mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0}\ )$ $\qquad \mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0}$

$\mathbf{A}_0^{-1}(\ \mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1}\ )$ $\qquad \mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1}$

evaluation. $\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}}$

goals. i. **hide** program **ii.** some **functionality**

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0}) \quad)$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1}) \quad)$$

evaluation. $\mathbf{M}_\mathbf{x} \otimes \mathbf{S}_\mathbf{x}$

goals. i. **hide** program **ii.** some **functionality**

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$\mathbf{A}_0$

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1)$ $\mathbf{A}_1^{-1}((\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2)$

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1)$ $\mathbf{A}_1^{-1}((\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2)$

evaluation. $(\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell$

goals. i. **hide** program **ii.** some **functionality**

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}(\underbrace{(\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underbrace{(\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2})$$

$$\mathbf{A}_0^{-1}(\underbrace{(\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underbrace{(\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2})$$

evaluation. $\underbrace{(\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell}$

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2)$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2)$$

evaluation. $(\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell$

note. $\mathbf{M}_{i,b}, \mathbf{S}_{i,b}$ are small **[ACPS09]**

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}(\underbrace{(\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underbrace{(\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2})$$

$$\mathbf{A}_0^{-1}(\underbrace{(\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underbrace{(\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2})$$

evaluation. $\underbrace{(\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell}$

generalization. $\mathbf{M} \otimes \mathbf{S} \mapsto \begin{pmatrix} \mathbf{M} & \\ & \mathbf{S} \end{pmatrix}$

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}(\underset{\sim}{(\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underset{\sim}{(\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2})$$

$$\mathbf{A}_0^{-1}(\underset{\sim}{(\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underset{\sim}{(\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2})$$

evaluation. $\underset{\sim}{(\mathbf{M}_\mathbf{x} \otimes \mathbf{S}_\mathbf{x})\mathbf{A}_\ell}$

generalization. $\mathbf{M} \otimes \mathbf{S} \mapsto \begin{pmatrix} \mathbf{M} & \\ & \mathbf{S} \end{pmatrix}$ or $\begin{pmatrix} \mathbf{M} \otimes \mathbf{S} & \\ & \mathbf{S} \end{pmatrix}$

GGH15 encodings

[Gentry Gorbunov Halevi 15, Canetti Chen 17, ...]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}\big(\underbrace{(\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1}\big) \quad \mathbf{A}_1^{-1}\big(\underbrace{(\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2}\big)$$

$$\mathbf{A}_0^{-1}\big(\underbrace{(\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1}\big) \quad \mathbf{A}_1^{-1}\big(\underbrace{(\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2}\big)$$

evaluation. $(\mathbf{M}_\mathbf{x} \otimes \mathbf{S}_\mathbf{x})\mathbf{A}_\ell$

functionality. can derive $\mathbf{S}_\mathbf{x}\overline{\mathbf{A}}_\ell \approx$ a PRF **[CC17, BLMR13]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2)$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2)$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$$

$$\mathbf{A}_0^{-1}(\underbrace{(\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underbrace{(\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2})$$

$$\mathbf{A}_0^{-1}(\underbrace{(\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underbrace{(\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2})$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$$

$$\mathbf{A}_0^{-1}(\underset{\sim}{(\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underset{\sim}{(\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2})$$

$$\mathbf{A}_0^{-1}(\underset{\sim}{(\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1}) \quad \mathbf{A}_1^{-1}(\underset{\sim}{(\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2})$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,0} \otimes \mathbf{S}_{2,0})\mathbf{A}_2)$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}((\mathbf{M}_{2,1} \otimes \mathbf{S}_{2,1})\mathbf{A}_2)$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1)$ $\mathbf{A}_1^{-1}$(uniform)

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1)$ $\mathbf{A}_1^{-1}$(uniform)

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}(\text{uniform})$$

$$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1) \quad \mathbf{A}_1^{-1}(\text{uniform})$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1)$ uniform

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1)$ uniform

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,0} \otimes \mathbf{S}_{1,0})\mathbf{A}_1)$ uniform

$\mathbf{A}_0^{-1}((\mathbf{M}_{1,1} \otimes \mathbf{S}_{1,1})\mathbf{A}_1)$ uniform

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$

$\mathbf{A}_0^{-1}$(uniform) uniform

$\mathbf{A}_0^{-1}$(uniform) uniform

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

semantic **security**

[Canetti Chen 17, GKW17, WZ17]

$\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$

uniform uniform

uniform uniform

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **permutation** matrices

proof. $\longleftarrow$ **[BVWW16]**

this work

[Chen Vaikuntanathan W]

hiding **non-permutation** branching programs

this work

[Chen Vaikuntanathan W]

hiding **non-permutation** branching programs

– more **efficient**

– more **expressive** in read-once setting

this work

[Chen Vaikuntanathan W]

hiding **non-permutation** branching programs

$(\mathbf{M} \otimes \mathbf{S})\mathbf{A}$ **not** pseudorandom

goal. hide $\mathbf{M}_{i,b}$'s given

$$\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_\ell$$

$$\mathbf{A}_{i-1}^{-1}((\mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i)$$

this work

[Chen Vaikuntanathan W]

hiding non-permutation branching programs

$(\mathbf{M} \otimes \mathbf{S})\mathbf{A}$ **not** pseudorandom

goal. hide $\mathbf{M}_{i,b}$'s given

$$\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_\ell$$

$$\mathbf{A}_{i-1}^{-1}\left(\begin{pmatrix} \mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b} & \\ & \mathbf{S}_{i,b} \end{pmatrix} \mathbf{A}_i \right)$$

this work

[Chen Vaikuntanathan W]

hiding non-permutation branching programs

$(\mathbf{M} \otimes \mathbf{S})\mathbf{A}$ **not** pseudorandom

goal. hide $\mathbf{M}_{i,b}$'s given

$$\mathbf{J}\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_\ell$$

$$\mathbf{A}_{i-1}^{-1}\left(\begin{pmatrix} \mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b} & \\ & \mathbf{S}_{i,b} \end{pmatrix} \mathbf{A}_i\right)$$

this work

[Chen Vaikuntanathan W]

hiding **non-permutation** branching programs

$\underset{\sim}{(\mathbf{M} \otimes \mathbf{S})\mathbf{A}}$ **not** pseudorandom

goal. hide $\mathbf{M}_{i,b}$'s given

$$\mathbf{J}\mathbf{A}_0, \{\, \mathbf{S}_{i,b} \,\}_{i \in [\ell], b \in \{0,1\}}$$

$$\mathbf{A}_{i-1}^{-1}(\begin{pmatrix} \mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b} & \\ & \mathbf{S}_{i,b} \end{pmatrix} \mathbf{A}_i)$$

this work

[Chen Vaikuntanathan W]

hiding non-permutation branching programs

$\underbrace{(\mathbf{M} \otimes \mathbf{S})\mathbf{A}}$ **not** pseudorandom

goal. hide $\mathbf{M}_{i,b}$'s given

$$\mathbf{J}\mathbf{A}_0, \{\, \mathbf{S}_{i,b} \,\}_{i \in [\ell], b \in \{0,1\}}$$

$$\mathbf{A}_{i-1}^{-1}\left(\begin{pmatrix} \mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b} & \\ & \mathbf{S}_{i,b} \end{pmatrix} \mathbf{A}_i \right)$$

new **computational** lemma

$\mathbf{A}^{-1}(\mathbf{Z} + \mathbf{E})$ **hides** $\mathbf{Z}$

$$\boxed{\mathbf{A}}^{-1}\left(\boxed{\mathbf{Z}} + \boxed{\mathbf{E}}\right)$$

new **computational** lemma

$$\mathbf{A}^{-1}(\mathbf{Z} + \mathbf{E}) \text{ **hides** } \mathbf{Z}$$

$$\boxed{\mathbf{A}}^{-1}\left(\boxed{\mathbf{Z}} + \boxed{\mathbf{E}}\right)$$

idea. embed LWE secret into $\mathbf{A}$

"target switching" in [**Goyal Koppula Waters 18**]

new **computational** lemma

$\mathbf{A}^{-1}(\mathbf{Z}+\mathbf{E})$ **hides** $\mathbf{Z}$

$$\boxed{\mathbf{A}_1 \mid \mathbf{A}_2}^{-1}\left(\boxed{\quad\mathbf{Z}\quad} + \boxed{\quad\mathbf{E}\quad}\right)$$

new **computational** lemma

$$\mathbf{A}^{-1}(\mathbf{Z} + \mathbf{E}) \text{ **hides** } \mathbf{Z}$$

$$\boxed{\mathbf{A}_1 \mid \mathbf{A}_2}^{-1}\left(\boxed{\mathbf{Z}} + \boxed{\mathbf{E}}\right)$$

$$\approx_s \quad \boxed{\begin{matrix} -\mathbf{U} \\ \mathbf{A}_2^{-1}(\mathbf{A}_1\mathbf{U}+\mathbf{Z}+\mathbf{E}) \end{matrix}}$$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\, \mathbf{A}_0$$

$$\mathbf{A}_0^{-1}\left(\begin{pmatrix} \mathbf{M}_{1,0} & \\ & \mathbf{S}_{1,0} \end{pmatrix}\mathbf{A}_1\right) \quad \mathbf{A}_1^{-1}\left(\begin{pmatrix} \mathbf{M}_{2,0} & \\ & \mathbf{S}_{2,0} \end{pmatrix}\mathbf{A}_2\right)$$

$$\mathbf{A}_0^{-1}\left(\begin{pmatrix} \mathbf{M}_{1,1} & \\ & \mathbf{S}_{1,1} \end{pmatrix}\mathbf{A}_1\right) \quad \mathbf{A}_1^{-1}\left(\begin{pmatrix} \mathbf{M}_{2,1} & \\ & \mathbf{S}_{2,1} \end{pmatrix}\mathbf{A}_2\right)$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **any** matrices

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\underbrace{\mathbf{A}_0^{-1}\left(\begin{pmatrix}\mathbf{M}_{1,0} & \\ & \mathbf{S}_{1,0}\end{pmatrix}\mathbf{A}_1\right)} \quad \underbrace{\mathbf{A}_1^{-1}\left(\begin{pmatrix}\mathbf{M}_{2,0} & \\ & \mathbf{S}_{2,0}\end{pmatrix}\mathbf{A}_2\right)}$$

$$\underbrace{\mathbf{A}_0^{-1}\left(\begin{pmatrix}\mathbf{M}_{1,1} & \\ & \mathbf{S}_{1,1}\end{pmatrix}\mathbf{A}_1\right)} \quad \underbrace{\mathbf{A}_1^{-1}\left(\begin{pmatrix}\mathbf{M}_{2,1} & \\ & \mathbf{S}_{2,1}\end{pmatrix}\mathbf{A}_2\right)}$$

lemma. hides $\{\mathbf{M}_{i,b}\}$ for **any** matrices

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \underset{\sim\sim\sim}{\mathbf{M}_{1,0}\overline{\mathbf{A}}_1} \\ \\ \underset{\sim\sim\sim}{\mathbf{S}_{1,0}\underline{\mathbf{A}}_1} \end{pmatrix} \qquad \mathbf{A}_1^{-1}\begin{pmatrix} \underset{\sim\sim\sim}{\mathbf{M}_{2,0}\overline{\mathbf{A}}_2} \\ \\ \underset{\sim\sim\sim}{\mathbf{S}_{2,0}\underline{\mathbf{A}}_2} \end{pmatrix}$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \underset{\sim\sim\sim}{\mathbf{M}_{1,1}\overline{\mathbf{A}}_1} \\ \\ \underset{\sim\sim\sim}{\mathbf{S}_{1,1}\underline{\mathbf{A}}_1} \end{pmatrix} \qquad \mathbf{A}_1^{-1}\begin{pmatrix} \underset{\sim\sim\sim}{\mathbf{M}_{2,1}\overline{\mathbf{A}}_2} \\ \\ \underset{\sim\sim\sim}{\mathbf{S}_{2,1}\underline{\mathbf{A}}_2} \end{pmatrix}$$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \mathbf{M}_{1,0}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,0}\underline{\mathbf{A}}_1 \end{pmatrix} \qquad \mathbf{A}_1^{-1}\begin{pmatrix} \mathbf{M}_{2,0}\overline{\mathbf{A}}_2 \\ \mathbf{S}_{2,0}\underline{\mathbf{A}}_2 \end{pmatrix}$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \mathbf{M}_{1,1}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,1}\underline{\mathbf{A}}_1 \end{pmatrix} \qquad \mathbf{A}_1^{-1}\begin{pmatrix} \mathbf{M}_{2,1}\overline{\mathbf{A}}_2 \\ \mathbf{S}_{2,1}\underline{\mathbf{A}}_2 \end{pmatrix}$$

proof. **(1)** $\longleftarrow$ **(2)** mask $\overline{\mathbf{A}}_0$ **(3)** $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\mathbf{A}_0^{-1}\left(\underbrace{\mathbf{M}_{1,0}\overline{\mathbf{A}}_1}_{\sim} \atop \underbrace{\mathbf{S}_{1,0}\underline{\mathbf{A}}_1}_{\sim}\right) \qquad \mathbf{A}_1^{-1}\left(\underbrace{\mathbf{M}_{2,0}\overline{\mathbf{A}}_2}_{\sim} \atop \underbrace{\mathbf{S}_{2,0}\underline{\mathbf{A}}_2}_{\sim}\right)$$

$$\mathbf{A}_0^{-1}\left(\underbrace{\mathbf{M}_{1,1}\overline{\mathbf{A}}_1}_{\sim} \atop \underbrace{\mathbf{S}_{1,1}\underline{\mathbf{A}}_1}_{\sim}\right) \qquad \mathbf{A}_1^{-1}\left(\underbrace{\mathbf{M}_{2,1}\overline{\mathbf{A}}_2}_{\sim} \atop \underbrace{\mathbf{S}_{2,1}\underline{\mathbf{A}}_2}_{\sim}\right)$$

proof. **(1)** $\longleftarrow$ (2) mask $\overline{\mathbf{A}}_0$ $\overline{(3)}$ $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$

$\mathbf{A}_0^{-1}\begin{pmatrix}\mathbf{M}_{1,0}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,0}\underline{\mathbf{A}}_1\end{pmatrix}$ $\qquad$ $\mathbf{A}_1^{-1}\begin{pmatrix}\mathbf{M}_{2,0}\overline{\mathbf{A}}_2 \\ \text{uniform}\end{pmatrix}$

$\mathbf{A}_0^{-1}\begin{pmatrix}\mathbf{M}_{1,1}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,1}\underline{\mathbf{A}}_1\end{pmatrix}$ $\qquad$ $\mathbf{A}_1^{-1}\begin{pmatrix}\mathbf{M}_{2,1}\overline{\mathbf{A}}_2 \\ \text{uniform}\end{pmatrix}$

proof. (1) $\longleftarrow$ (2) mask $\overline{\mathbf{A}}_0$ $\overline{(3)}$ $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\,\mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \mathbf{M}_{1,0}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,0}\underline{\mathbf{A}}_1 \end{pmatrix} \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,0}\overline{\mathbf{A}}_2)$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \mathbf{M}_{1,1}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,1}\underline{\mathbf{A}}_1 \end{pmatrix} \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,1}\overline{\mathbf{A}}_2)$$

proof. **(1)** $\longleftarrow$ (2) mask $\overline{\mathbf{A}}_0$ (3) $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \mathbf{M}_{1,0}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,0}\underline{\mathbf{A}}_1 \end{pmatrix} \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,0}\overline{\mathbf{A}}_2)$$

$$\mathbf{A}_0^{-1}\begin{pmatrix} \mathbf{M}_{1,1}\overline{\mathbf{A}}_1 \\ \mathbf{S}_{1,1}\underline{\mathbf{A}}_1 \end{pmatrix} \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,1}\overline{\mathbf{A}}_2)$$

proof. **(1)** $\longleftarrow$ (2) mask $\overline{\mathbf{A}}_0$ $\overline{(3)}$ $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\, \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\mathbf{A}_0^{-1}\Big(\underbrace{\mathbf{M}_{1,0}\overline{\mathbf{A}}_1}_{\text{uniform}}\Big) \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,0}\overline{\mathbf{A}}_2)$$

$$\mathbf{A}_0^{-1}\Big(\underbrace{\mathbf{M}_{1,1}\overline{\mathbf{A}}_1}_{\text{uniform}}\Big) \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,1}\overline{\mathbf{A}}_2)$$

proof. **(1)** $\longleftarrow$ (2) mask $\overline{\mathbf{A}}_0$ (3) $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$[\star \mid \mathbf{I}]\ \mathbf{A}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\overline{\mathbf{A}}_0^{-1}(\mathbf{M}_{1,0}\overline{\mathbf{A}}_1) \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,0}\overline{\mathbf{A}}_2)$$

$$\overline{\mathbf{A}}_0^{-1}(\mathbf{M}_{1,1}\overline{\mathbf{A}}_1) \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,1}\overline{\mathbf{A}}_2)$$

proof. **(1)** $\longleftarrow$ (2) mask $\overline{\mathbf{A}}_0$ (3) $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$\underline{\mathbf{A}}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\overline{\mathbf{A}}_0^{-1}(\mathbf{M}_{1,0}\overline{\mathbf{A}}_1) \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,0}\overline{\mathbf{A}}_2)$$

$$\overline{\mathbf{A}}_0^{-1}(\mathbf{M}_{1,1}\overline{\mathbf{A}}_1) \qquad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,1}\overline{\mathbf{A}}_2)$$

proof. **(1)** $\longleftarrow$ **(2)** mask $\overline{\mathbf{A}}_0$ **(3)** $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$\underline{\mathbf{A}}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

$$\overline{\mathbf{A}}_0^{-1}(\underset{\sim}{\mathbf{M}_{1,0}\overline{\mathbf{A}}_1}) \qquad \overline{\mathbf{A}}_1^{-1}(\underset{\sim}{\mathbf{M}_{2,0}\overline{\mathbf{A}}_2})$$

$$\overline{\mathbf{A}}_0^{-1}(\underset{\sim}{\mathbf{M}_{1,1}\overline{\mathbf{A}}_1}) \qquad \overline{\mathbf{A}}_1^{-1}(\underset{\sim}{\mathbf{M}_{2,1}\overline{\mathbf{A}}_2})$$

proof. **(1)** $\longleftarrow$ **(2)** mask $\overline{\mathbf{A}}_0$ **(3)** $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$\underline{\mathbf{A}}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

uniform $\quad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,0}\overline{\mathbf{A}}_2)$

uniform $\quad \overline{\mathbf{A}}_1^{-1}(\mathbf{M}_{2,1}\overline{\mathbf{A}}_2)$

proof. **(1)** $\longleftarrow$ **(2)** mask $\overline{\mathbf{A}}_0$ **(3)** $\longrightarrow$

semantic **security**

[Chen Vaikuntanathan W 18]

$$\underline{\mathbf{A}}_0, \mathbf{S}_{1,b}, \mathbf{S}_{2,b}, \overline{\mathbf{A}}_2$$

uniform

uniform

uniform

uniform

proof. **(1)** $\longleftarrow$ **(2)** mask $\overline{\mathbf{A}}_0$ **(3)** $\longrightarrow$

➋ obfuscation

candidates and attacks

obfuscation via GGH15

[Halevi Halevi Stephens-Davidowitz Shoup 17, ...]

input. read-**once** program $\mathbf{M_x} \stackrel{?}{=} \mathbf{0}$

goal. obfuscate, i.e. leak nothing beyond functionality

obfuscation via GGH15

[Halevi Halevi Stephens-Davidowitz Shoup 17, ...]

input. read-**once** program $\mathbf{M_x} \stackrel{?}{=} \mathbf{0}$

output.

$$\mathbf{A}_0,\ \{\ \mathbf{A}_{i-1}^{-1}\big(\underset{\sim}{(\mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i}\big)\ \}_{i\in[\ell],b\in\{0,1\}}$$

obfuscation via GGH15

[Halevi Halevi Stephens-Davidowitz Shoup 17, ...]

input. read-**once** program $\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$

output.

$$\mathbf{A}_0, \; \{ \mathbf{A}_{i-1}^{-1}\big(\underbrace{(\mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i}\big) \}_{i \in [\ell], b \in \{0,1\}}$$

evaluation. $\underbrace{(\;\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell} \stackrel{?}{\approx} \mathbf{0}$

$$\iff \quad \mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$$

obfuscation via GGH15

[Halevi Halevi Stephens-Davidowitz Shoup 17, ...]

input. read-**once** program $\mathbf{u}\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$

output.

$$\mathbf{A}_0, \ \{ \mathbf{A}_{i-1}^{-1}(\underbrace{(\mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i}) \}_{i \in [\ell], b \in \{0,1\}}$$

evaluation. $\underbrace{(\ \mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell} \stackrel{?}{\approx} \mathbf{0}$

$$\Longleftrightarrow \quad \mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$$

obfuscation via GGH15

[Halevi Halevi Stephens-Davidowitz Shoup 17, ...]

input. read-**once** program $\mathbf{u}\mathbf{M}_\mathbf{x} \stackrel{?}{=} \mathbf{0}$

output.

$$(\mathbf{u} \otimes \mathbf{I})\mathbf{A}_0, \ \{ \mathbf{A}_{i-1}^{-1}((\mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i) \}_{i \in [\ell], b \in \{0,1\}}$$

evaluation. $(\mathbf{u}\mathbf{M}_\mathbf{x} \otimes \mathbf{S}_\mathbf{x})\mathbf{A}_\ell \stackrel{?}{\approx} \mathbf{0}$

$$\iff \mathbf{u}\mathbf{M}_\mathbf{x} \stackrel{?}{=} \mathbf{0}$$

obfuscation via GGH15

[Halevi Halevi Stephens-Davidowitz Shoup 17, ...]

input. read-**once** program $\mathbf{u}\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$

output.

$$(\mathbf{u} \otimes \mathbf{I})\mathbf{A}_0, \ \{ \mathbf{A}_{i-1}^{-1}((\mathbf{M}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i) \}_{i \in [\ell], b \in \{0,1\}}$$

evaluation. $(\mathbf{u}\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell \stackrel{?}{\approx} \mathbf{0}$

$$\iff \mathbf{u}\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$$

" within the realm of feasibility " **[HHSS17]**

rank **attack**

[Chen Vaikuntanathan W 18]

1. $\textbf{eval}(x_i \mid y_j) \approx 0, \quad i,j \in [L]$

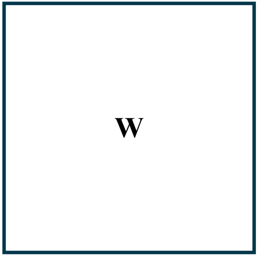
starting point
[CHLRS15, CLLT16, CGH17]

rank **attack**

[Chen Vaikuntanathan W 18]

1. $w_{ij} := \textbf{eval}(x_i \mid y_j) \approx 0, \quad i,j \in [L]$

2. $\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L}$

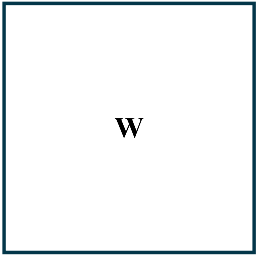


starting point
[CHLRS15, CLLT16, CGH17]

rank **attack**

[Chen Vaikuntanathan W 18]

1. $w_{ij} := \textbf{eval}(x_i \mid y_j) \approx 0, \quad i,j \in [L]$
2. $\textbf{rank}(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L})$



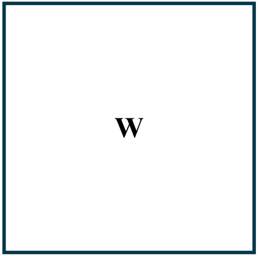
starting point

[CHLRS15, CLLT16, CGH17]

rank **attack**

[Chen Vaikuntanathan W 18]

1. $w_{ij} := \textbf{eval}(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. $\textbf{rank}(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L})$



starting point

[CHLRS15, CLLT16, CGH17]

rank **attack**

[Chen Vaikuntanathan W 18]

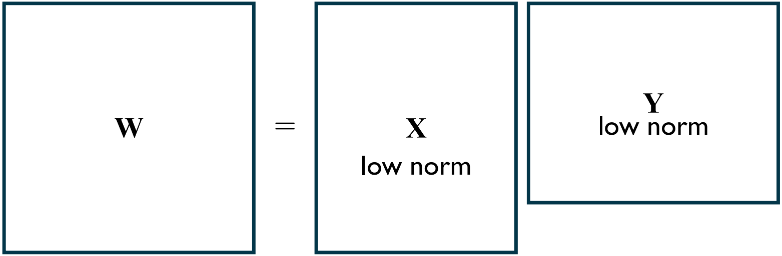
1. $w_{ij} :=$ **eval**$(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. **rank**$(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L})$

$$\mathbf{W} = \begin{bmatrix} - & \hat{\mathbf{x}}_1 & - \\ - & \hat{\mathbf{x}}_2 & - \\ & \vdots & \\ - & \hat{\mathbf{x}}_L & - \end{bmatrix} \begin{bmatrix} | & | & & | \\ \hat{\mathbf{y}}_1 & \hat{\mathbf{y}}_2 & \cdots & \hat{\mathbf{y}}_L \\ | & | & & | \end{bmatrix}$$

rank **attack**

[Chen Vaikuntanathan W 18]

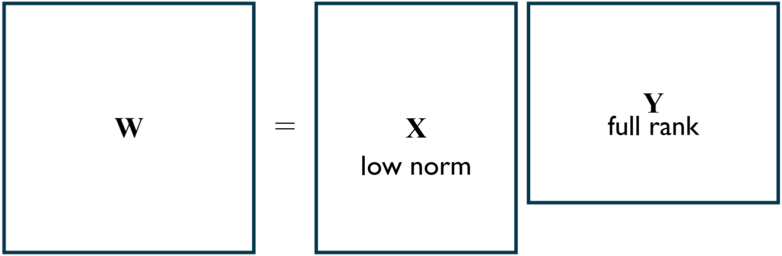
1. $w_{ij} := \textbf{eval}(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. $\textbf{rank}(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L})$



rank **attack**

[Chen Vaikuntanathan W 18]

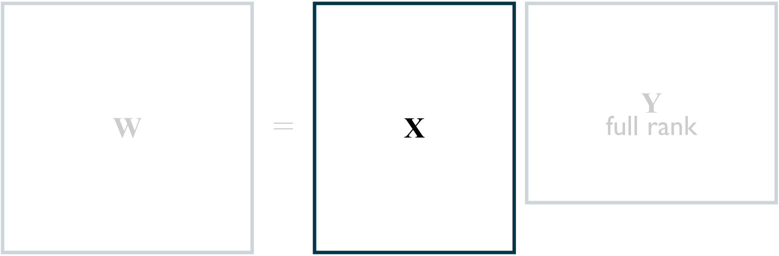
1. $w_{ij} := \textbf{eval}(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. $\textbf{rank}(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L})$



rank **attack**

[Chen Vaikuntanathan W 18]

1. $w_{ij} := \textbf{eval}(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. $\textbf{rank}(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L}) = \textbf{rank}(\mathbf{X})$



rank **attack**

[Chen Vaikuntanathan W 18]

1. $w_{ij} :=$ **eval**$(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. **rank**$(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L}) =$ **rank**$(\mathbf{X})$

$$\mathbf{W} = \begin{pmatrix} \mathbf{u}\mathbf{M}_{x_1} \otimes \mathbf{S}_{x_1} \mid \mathbf{e}_1 \\ \mathbf{u}\mathbf{M}_{x_2} \otimes \mathbf{S}_{x_2} \mid \mathbf{e}_2 \\ \vdots \\ \mathbf{u}\mathbf{M}_{x_L} \otimes \mathbf{S}_{x_L} \mid \mathbf{e}_L \end{pmatrix} \mathbf{Y}$$

full rank

rank **attack**

[Chen Vaikuntanathan W 18]

1. $w_{ij} :=$ **eval**$(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. **rank**$(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L}) =$ **rank**$(\mathbf{X})$

$$\mathbf{W} = \begin{pmatrix} \mathbf{u}\mathbf{M}_{x_1} \\ \mathbf{u}\mathbf{M}_{x_2} \\ \vdots \\ \mathbf{u}\mathbf{M}_{x_L} \end{pmatrix} \mathbf{Y}$$

$\mathbf{Y}$ full rank

rank **attack**: workarounds?

[Chen Vaikuntanathan W 18]

rank **attack**: workarounds?

[**Chen Vaikuntanathan W 18**]

1. avoid encodings of **zeroes**

– $\mathbf{u}\mathbf{M}_\mathbf{x} \neq \mathbf{0}$ for all $\mathbf{x}$

– candidate for witness encryption via [GLW14]

rank **attack**: workarounds?

[**Chen Vaikuntanathan W 18**]

1. avoid encodings of **zeroes**
   - $\mathbf{uM_x} \neq \mathbf{0}$ for all $\mathbf{x}$
   - candidate for witness encryption via [**GLW14**]
2. read-**many**
   - $O(\text{size}^c)$ attack for read-c [**ADGM17, CLTT17**]
   - candidate for obfuscation

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}\mathbf{M}_{\mathbf{x}} \stackrel{?}{=} \mathbf{0}$

output.

$$(\hat{\mathbf{u}} \otimes \mathbf{I})\mathbf{A}_0, \ \{ \mathbf{A}_{i-1}^{-1}(\underbrace{(\hat{\mathbf{M}}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i}) \}_{i \in [\ell], b \in \{0,1\}}$$

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}\mathbf{M}_\mathbf{x} \stackrel{?}{=} \mathbf{0}$

output.

$$(\hat{\mathbf{u}} \otimes \mathbf{I})\mathbf{A}_0, \ \{ \mathbf{A}_{i-1}^{-1}((\hat{\mathbf{M}}_{i,b} \otimes \mathbf{S}_{i,b})\mathbf{A}_i) \}_{i \in [\ell], b \in \{0,1\}}$$

$$\hat{\mathbf{M}}_{i,b} = \begin{pmatrix} \mathbf{M}_{i,b} & & & \\ & \mathbf{R}_{i,b}^{(1)} & & \\ & & \ddots & \\ & & & \mathbf{R}_{i,b}^{(\ell)} \end{pmatrix} \quad \mathbf{R}_{i,b}^{(j)} \in \mathbb{Z}^{2 \times 2}$$

❸ obfuscation

some thoughts

obfuscation from **lattices**

1. via **functional** encryption **[BV15, AJ15, ...]**

2. via **GGH15** encodings

obfuscation from **lattices**

1. via **functional** encryption **[BV15, AJ15, ...]**

– ABE + FHE **[GVW15, GKPVZ13, GVW12, A17, BTVW17]**

– **bottleneck.** inner product + rounding/noise

2. via **GGH15** encodings

obfuscation from **lattices**

1. via **functional** encryption **[BV15, AJ15, ...]**
   – ABE + FHE **[GVW15, GKPVZ13, GVW12, A17, BTVW17]**
   – **bottleneck.** inner product + rounding/noise

2. via **GGH15** encodings
   – **bottleneck.** encodings of zeroes

obfuscation: small steps

1. **weaker** primitives from LWE

– lockable obfuscation, mixed FE, ...

obfuscation: small steps

1. **weaker** primitives from LWE

– lockable obfuscation, mixed FE, ...

2. targets for **crypt-analysis**

– minimal work-arounds

obfuscation: small steps

1. **weaker** primitives from LWE
   – lockable obfuscation, mixed FE, ...
2. targets for **crypt-analysis**
   – minimal work-arounds
3. candidates from "**crypt-analyzable**" assumptions

obfuscation: small steps

1. **weaker** primitives from LWE
   – lockable obfuscation, mixed FE, ...
2. targets for **crypt-analysis**
   – minimal work-arounds
3. candidates from "**crypt-analyzable**" assumptions

// merci !