Obfuscation from LWE? proofs, attacks, candidates

Hoeteck Wee
CNRS & ENS

obfuscation

[BGIRSVY01, H00, GR07, GGHRSW13]

obfuscation

[BGIRSVY01, H00, GR07, GGHRSW13]

$$C$$

obfuscation

[BGIRSVY01, H00, GR07, GGHRSW13]

$$\begin{array}{c} C \\ \big\downarrow \\ \mathcal{O}(C) \end{array}$$

obfuscation

[BGIRSVY01, H00, GR07, GGHRSW13]

$$C \qquad \equiv \qquad C'$$

$$\forall x : C(x) = C'(x)$$

$$\mathcal{O}(C)$$

obfuscation

[BGIRSVY01, H00, GR07, GGHRSW13]

$$C \qquad \equiv \qquad C'$$

$$\forall x : C(x) = C'(x)$$

$$\mathcal{O}(C) \;\approx_c\; \mathcal{O}(C')$$

obfuscation

[BGIRSVY01, H00, GR07, GGHRSW13]

from **LWE** *?*

candidates, proofs, and attacks

preliminaries

LWE assumption [Regev 05]

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

$$\boxed{\mathbf{s}}\ \boxed{\quad\mathbf{A}\quad} + \boxed{\quad\mathbf{e}\quad}$$

LWE assumption [Regev 05]

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

$$\boxed{\mathbf{S}}\ \boxed{\quad\mathbf{A}\quad} + \boxed{\quad\mathbf{E}\quad}$$

LWE assumption [Regev 05]

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

$$\boxed{\begin{matrix} \mathbf{S} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{matrix}} \ \boxed{\quad\mathbf{A}\quad} + \boxed{\quad\mathbf{E}\quad}$$

LWE assumption [Regev 05]

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

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

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]

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

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

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

LWE assumption [Regev 05]

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

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

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

branching programs

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

$$\in \{0,1\}^{\mathsf{poly} \times \mathsf{poly}}$$

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. accept iff $\mathbf{M_x} = \prod \mathbf{M}_{i,x_i} = \mathbf{0}$

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. accept iff $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_i} = \mathbf{0}$

– read-many $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_{i+1 \bmod n}}$, $|x| = n \ll \ell$

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. accept iff $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_i} = \mathbf{0}$

- read-many $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_{i+1 \bmod n}}$, $|x| = n \ll \ell$
- captures both logspace and NC^1

branching programs

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

evaluation. accept iff $\mathbf{u}\mathbf{M}_{\mathbf{x}} = \mathbf{u} \prod \mathbf{M}_{i,x_i} = \mathbf{0}$

– read-many $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_{i+1 \bmod n}}$, $|x| = n \ll \ell$

– captures both logspace and NC^1

branching programs

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

evaluation. accept iff $\mathbf{M}_\mathbf{x} = \prod \mathbf{M}_{i,x_i} = \mathbf{0}$

example. $(1 \times 1$ matrices)

branching programs

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

evaluation. accept iff $\mathbf{M}_{\mathbf{x}} = \prod \mathbf{M}_{i,x_i} = \mathbf{0}$

example. accept iff $\mathbf{x} \neq \mathbf{a}$ (1×1 matrices)

obfuscation

FIRST principles

obfuscation via GGH15

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

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

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

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

obfuscation via GGH15

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

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

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

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

obfuscation via GGH15

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

$\boxed{(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = \mathbf{AC} \otimes \mathbf{BD}}$

obfuscation via GGH15

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

obfuscation via GGH15

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

$\mathbf{A}_0$ need a trapdoor to sample short pre-image of $\mathbf{A}_0$

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

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

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

obfuscation via GGH15

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

obfuscation via GGH15

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

obfuscation via GGH15

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

obfuscation via GGH15

[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. $\underbrace{(\mathbf{M}_\mathbf{x} \otimes \mathbf{S}_\mathbf{x})\mathbf{A}_\ell}$ $\quad \mathbf{M}_{i,b}, \mathbf{S}_{i,b}$ small **[ACPS09]**

obfuscation via GGH15

[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. $(\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell \approx \mathbf{0}$

$$\iff \mathbf{M}_{\mathbf{x}} = \mathbf{0}$$

obfuscation via GGH15

[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. $\underbrace{(\mathbf{M}_\mathbf{x} \otimes \mathbf{S}_\mathbf{x})\mathbf{A}_\ell} \approx \mathbf{0} \Rightarrow$ accept

obfuscation via GGH15

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

$$(\mathbf{u} \otimes \mathbf{I})\mathbf{A}_0$$

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

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

evaluation. $\underbrace{(\mathbf{u}\mathbf{M}_{\mathbf{x}} \otimes \mathbf{S}_{\mathbf{x}})\mathbf{A}_\ell} \approx \mathbf{0} \Rightarrow$ accept

obfuscation via GGH15

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

$$(\mathbf{u} \otimes \mathbf{I})\mathbf{A}_0$$

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

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

candidate obfuscation for NC^1 !

[GGHRSW13, HHRS17, ...]

obfuscation via GGH15

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

$$(\mathbf{u} \otimes \mathbf{I})\mathbf{A}_0$$

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

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

Q. $\mathcal{O}(\mathbf{u}, \{\mathbf{M}_{i,b}\}) \overset{?}{\approx}_c \mathcal{O}(\mathbf{u}', \{\mathbf{M}'_{i,b}\})$

if $(\mathbf{u}, \{\mathbf{M}_{i,b}\}) \equiv (\mathbf{u}', \{\mathbf{M}'_{i,b}\})$

obfuscation via GGH15

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

$$(\mathbf{u} \otimes \mathbf{I})\mathbf{A}_0$$

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

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

Q. $\mathcal{O}(\mathbf{u}, \{\mathbf{M}_{i,b}\}) \overset{?}{\approx}_c \mathcal{O}(\mathbf{u}', \{\mathbf{M}'_{i,b}\})$

if $\forall \mathbf{x} : \mathbf{u}\mathbf{M}_\mathbf{x} = 0 \iff \mathbf{u}'\mathbf{M}'_\mathbf{x} = 0$

$$\text{all}\left(\mathbf{u}, \{\mathbf{M}_{i,b}\}\right)$$

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq \mathbf{0}$

some accept

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq \mathbf{0}$

some accept

attacks

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_\mathbf{x} \neq 0$

some accept

proofs

attacks

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq \mathbf{0}$

some accept

diagonal $\mathbf{M}_{i,b}$

$\Rightarrow$ witness enc

attacks

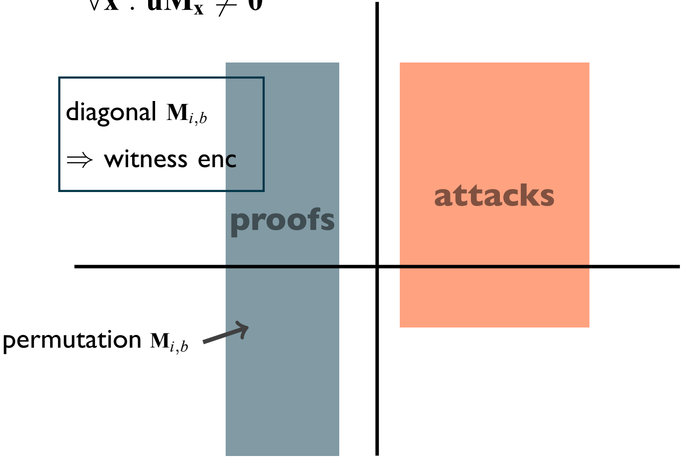
read-once

proofs

read-many

all reject $\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq \mathbf{0}$

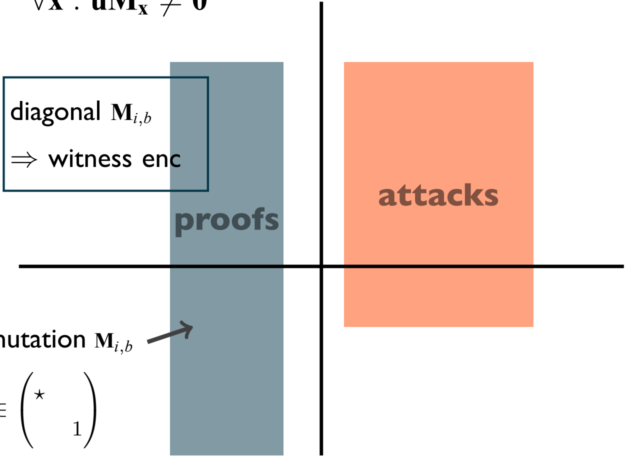
some accept



all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq 0$

some accept



permutation $\mathbf{M}_{i,b}$

$$\mathbf{M}_{i,b} \in \begin{pmatrix} \star & \\ & 1 \end{pmatrix}$$

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_\mathbf{x} \neq \mathbf{0}$

some accept

diagonal $\mathbf{M}_{i,b}$

$\Rightarrow$ witness enc

proofs

attacks

permutation $\mathbf{M}_{i,b}$

$\mathbf{M}_{i,b} \in \begin{pmatrix} \star & \\ & 1 \end{pmatrix}$

candidate

NC^1 obfuscation

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq \mathbf{0}$

some accept

1

proofs

2

attacks

candidate 3

NC^1 obfuscation

permutation $\mathbf{M}_{i,b}$

$$\mathbf{M}_{i,b} \in \begin{pmatrix} \star & \\ & 1 \end{pmatrix}$$

all reject

$\forall \mathbf{x} : \mathbf{u}\mathbf{M}_{\mathbf{x}} \neq \mathbf{0}$

1

proofs

permutation $\mathbf{M}_{i,b}$

$\mathbf{M}_{i,b} \in \begin{pmatrix} \star & \\ 1 & \end{pmatrix}$ [CVW18]

some accept

attacks

2

candidate

3

NC^1 obfuscation

❶ proofs

secure $\mathcal{O}$(permutation)

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0$$

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

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

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

secure $\mathcal{O}$(permutation)

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0$$

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

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

corollaries.

- private constrained PRFs **[Canetti Chen 17]**
- lockable obfuscation **[Goyal Koppula Waters, Wichs Zirdelis 17]**
- traitor tracing **[Goyal Koppula Waters 18, CVWWW 18]**

secure $\mathcal{O}$(permutation)

[Canetti Chen 17, GKW17, WZ17]

$$\mathbf{A}_0$$

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

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

lemma. $\approx_c$ random, for **permutation** matrices

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

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

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

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

secure $\mathcal{O}$(permutation)

[Canetti Chen 17, GKW17, WZ17]

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

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

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

lemma. $\approx_c$ random, for **permutation** matrices

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

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

proof. $\longleftarrow$ [BVWW16]

secure $\mathcal{O}$(permutation)

[Canetti Chen 17, GKW17, WZ17]

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

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

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

lemma. $\approx_c$ random, for **permutation** matrices

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

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

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

secure $\mathcal{O}$(permutation)

[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. $\approx_c$ random, for **permutation** matrices

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

secure $\mathcal{O}$(permutation)

[Canetti Chen 17, GKW17, WZ17]

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

uniform uniform

uniform uniform

lemma. $\approx_c$ random, for **permutation** matrices

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

❷ attacks

$\mathcal{O}$(read-**once**)

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

input. read-**once** program $\mathbf{u}$, $\{\mathbf{M}_{i,b}\}$

output.

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

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

rank **attack**

[Chen Vaikuntanathan W 18]

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

L^2 accepting inputs $x_i \mid y_j$ where $x_i, y_j \in \{0,1\}^{\ell/2}$

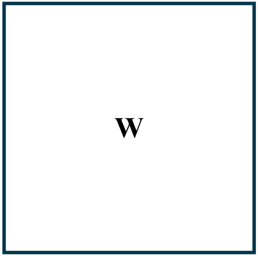
starting point

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

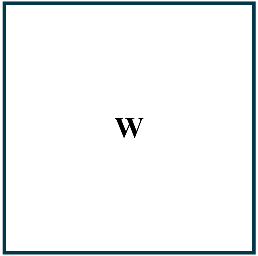


starting point
[CHLRS15, CLLT16, CGH17]

rank **attack**

[Chen Vaikuntanathan W 18]

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



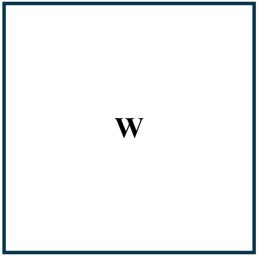
starting point

[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]

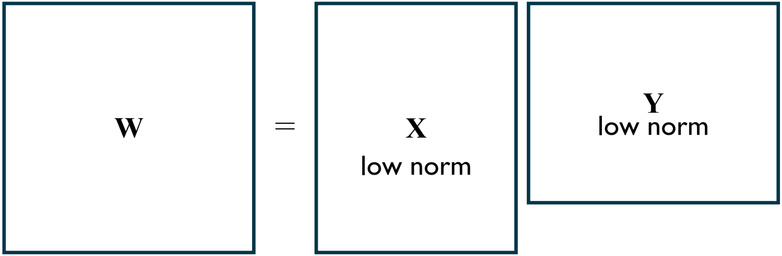
1. $w_{ij} :=$ **eval**$(x_i \mid y_j) = \langle \hat{\mathbf{x}}_i, \hat{\mathbf{y}}_j \rangle$ assuming read-once
2. **rank**$(\mathbf{W} = (w_{ij}) \in \mathbb{Z}^{L \times L})$

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

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

$\mathbf{W}$ = $\mathbf{X}$ $\mathbf{Y}$

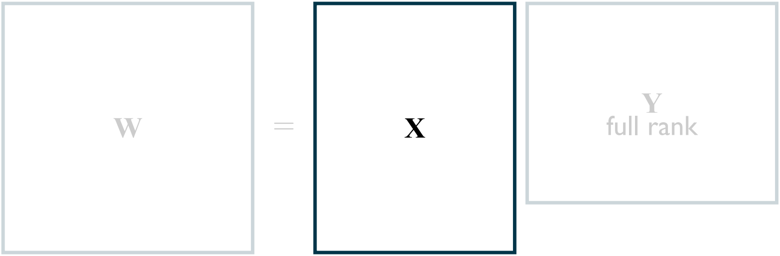
$\mathbf{X}$ low norm

$\mathbf{Y}$ full rank

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

$$\boxed{\mathbf{W}} = \boxed{\begin{array}{c} \mathbf{uM}_{x_1} \otimes \mathbf{S}_{x_1} \mid \mathbf{e}_1 \\ \mathbf{uM}_{x_2} \otimes \mathbf{S}_{x_2} \mid \mathbf{e}_2 \\ \vdots \\ \mathbf{uM}_{x_L} \otimes \mathbf{S}_{x_L} \mid \mathbf{e}_L \end{array}} \boxed{\begin{array}{c} \mathbf{Y} \\ \text{full rank} \end{array}}$$

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

$$\boxed{\mathbf{W}} = \boxed{\begin{matrix} \mathbf{uM}_{x_1} \\ \mathbf{uM}_{x_2} \\ \vdots \\ \mathbf{uM}_{x_L} \end{matrix}} \boxed{\begin{matrix} \mathbf{Y} \\ \text{full rank} \end{matrix}}$$

rank **attack**

[**Chen Vaikuntanathan W 18**]

read-**many**

$O(\text{size}^c)$ attack for read-c [**ADGM17, CLTT17**]

intuition. read-$c \mapsto$ read-once, size $O(\text{size}^c)$

rank **attack**

[Chen Vaikuntanathan W 18]

read-**many**

$O(\text{size}^c)$ attack for read-c **[ADGM17, CLTT17]**

intuition. read-$c \mapsto$ read-once, size $O(\text{size}^c)$

i.e., attack **fails** if c is very large

❸ candidate

witness encryption?

[Chen Vaikuntanathan W 18]

input. SAT formula ϕ, message $\mu \in \{0, 1\}$

enc(ϕ, μ) leaks μ iff ϕ is satisfiable

witness encryption?

[Chen Vaikuntanathan W 18]

input. SAT formula ϕ, message $\mu \in \{0,1\}$

$\mathbf{u} = (1 \ \cdots \ 1)$

$\mathbf{M}_{i,b}$ diagonal matrices, dim = # clauses

$\mathbf{u}\mathbf{M}_{\mathbf{x}} = \mathbf{0}$ iff ϕ is satisfiable [GLW14]

witness encryption?

[Chen Vaikuntanathan W 18]

input. SAT formula ϕ, message $\mu \in \{0,1\}$

$\hat{\mathbf{u}} = (1 \ \cdots \ 1 \ 1)$

$\hat{\mathbf{M}}_{i,b}$ diagonal matrices, dim = # clauses $+1$

$\hat{\mathbf{u}}\hat{\mathbf{M}}_{\mathbf{x}} = (\mathbf{0} \ \ \mu)$ if ϕ is satisfiable **[GLW14]**

witness encryption?

[Chen Vaikuntanathan W 18]

input. SAT formula ϕ, message $\mu \in \{0, 1\}$

$$\hat{\mathbf{u}} = (1 \;\; \cdots \;\; 1 \; 1)$$

$\hat{\mathbf{M}}_{i,b}$ diagonal matrices, dim = # clauses $+1$

$\hat{\mathbf{u}}\hat{\mathbf{M}}_{\mathbf{x}} = (\mathbf{0} \;\; \mu)$ if ϕ is satisfiable [GLW14]

output.

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

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}, \{\mathbf{M}_{i,b}\}$

output.

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

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}, \{\mathbf{M}_{i,b}\}$

output.

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

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}$, $\{\mathbf{M}_{i,b}\}$

output.

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

$$\hat{\mathbf{M}}_{i,b} = \begin{pmatrix} \mathbf{M}_{i,b} & & & \\ & \mathbf{R}_{i,b}^{(1)} & & \\ & & \ddots & \\ & & & \mathbf{R}_{i,b}^{(\ell)} \end{pmatrix}$$

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}$, $\{\mathbf{M}_{i,b}\}$

output.

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

$$\hat{\mathbf{M}}_{i,b} = \begin{pmatrix} \mathbf{M}_{i,b} & & & \\ & \mathbf{R}_{i,b}^{(1)} & & \\ & & \ddots & \\ & & & \mathbf{R}_{i,b}^{(\ell)} \end{pmatrix}$$

$\mathbf{R}_{i,b}^{(j)} \in \{0,1\}^{2\times 2}$

input consistency

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}, \{\mathbf{M}_{i,b}\}$

output.

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

status.

– **secure** in idealized model **[Bartusek Guan Ma Zhandry 18]**

simple obfuscation candidate

[Chen Vaikuntanathan W 18]

input. read-**many** program $\mathbf{u}, \{\mathbf{M}_{i,b}\}$

output.

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

status.

– **secure** in idealized model **[Bartusek Guan Ma Zhandry 18]**

– tweaks against statistical tests **[Cheon Cho Hhan Kim Lee 19]**

4 obfuscation

some thoughts

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 !