Counterexamples to New Circular Security Assumptions Underlying iO

H., Aayush Jain, Rachel Lin
(Berk.) (UCLA) (UW)

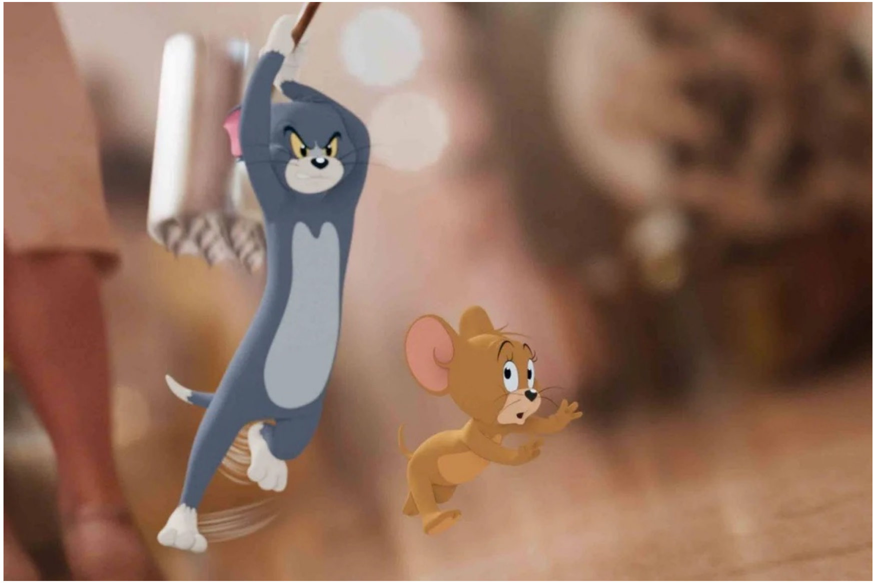
Crypto '21

Indistinguishability Obfuscation (iO):

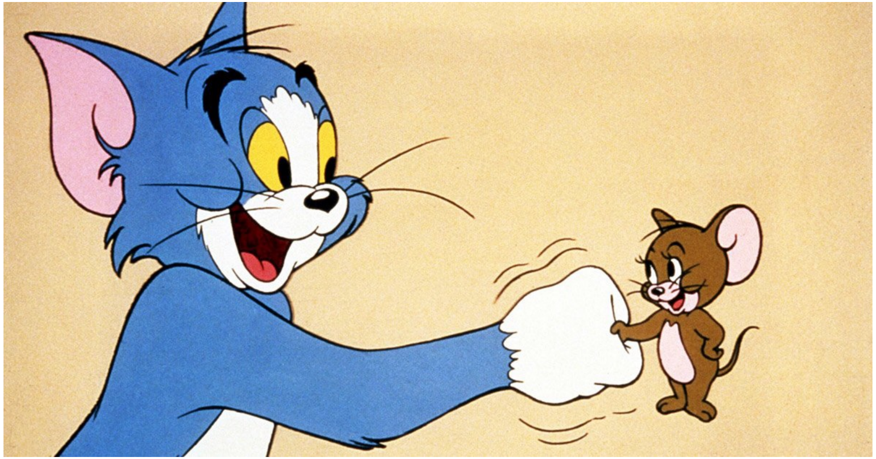
Extremly useful crypto primitive

Indistinguishability Obfuscation (iO):

Extremely useful and elusive crypto primitive

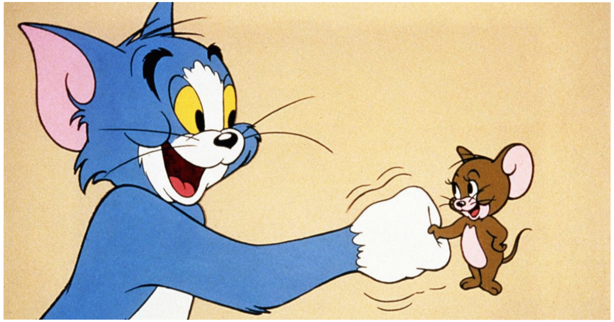


construction → attack → construction → attack → construction → ...



construction → attack → construction → attack → construction → ...

Simplification of assumptions & constructions



construction → attack → construction → attack → construction → ...

$\longrightarrow$

Simplification of assumptions & constructions

Led to recent iO from LWE, LPN, PRG in NCO, SXDH [Jain-Lin-Sahai]

Post-quantum iO ?

Simpler constructions ?

Post-quantum iO ?

Simpler constructions?

Natural apprach: base iO on lattices only

Recent works:

new, simple iO constructions

- [Brakerski-Döttling-Garg-Malavolta '20]
- [Gay-Pass '20]
- [Wee-Wichs '20]

Clean, simple-to-state assumptions!

LWE + circular security + randomness leakage (from some FHE Evals) $\Rightarrow$ iO

Now imperative to cryptoanalyze

LWE + circular security
+ randomness leakage $\Rightarrow$ iO
(from some FHE Evals)

-type assumptions

Our Results (in a nutshell):

forms of

LWE + circular security
+ randomness leakage
(from some FHE Evals)

assumptions

(as in [Gay-Pass '20, Wee-Wichs '20])

are false.

Strategy, Constructions of

[Brakerski-Döttling-Garg-Malavolta '20]
[Gay-Pass '20]
[Wee-Wichs '20]

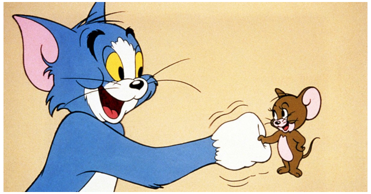
unbroken, promising!

Our Results (in a nutshell):

forms of LWE + circular security + randomness leakage (from some FHE Evals) assumptions

(as in [Gay-Pass '20, Wee-Wichs '20])

are false.



Hope: attacks lead to refined (& secure??) assumps.

NEW [Devadas-Quach-Vaikuntanathan-Wee-Wichs]

very simple & concrete assumption

Rest of talk:

Assumption of [Gay-Pass '20]
and our attack

Let's fix a "nice" fully-homomorphic encryption scheme.

Eg. Gentry-Sahai-Waters (GSW)

LWE + Circular security + randomness leakage (from some FHE Evals) $\Rightarrow$ iO

2-circular security: $(sk_1, pk_1) \leftarrow \text{Setup}$

$(sk_2, pk_2) \leftarrow \text{Setup}$

publish $\text{Enc}(pk_1, sk_2), \text{Enc}(pk_2, sk_1)$

Believed secure for "natural" schemes

Underlies unlevelled FHE

LWE + circular security
+ randomness leakage
(from some FHE Evals) $\Rightarrow$ iO

Chosen-plaintext security w/ "Shielded randomness leakage" [GP 20]:

- Adversary A chooses m_0, m_1
- $b \sim \{0,1\}$
- publish $ct = Enc(m_b)$
- A can call SRL (poly. times)
- A guesses b

Chosen-plaintext security w/

LWE + circular security
+ randomness leakage
(from some FHE Evals) ⇒ iO

"Shielded randomness leakage" [GP 20]:

- Adversary A chooses m_0, m_1
- $b \sim \{0,1\}$
- publish $ct = \mathrm{Enc}(m_b)$
- A can call SRL (poly. times)
- A guesses b

SRL Oracle Θ:

- $ct^* = \mathrm{Enc}(0, R^*)$
- A chooses
  $f_{ct^*} : m_b \to \{0,1\}$
- Θ returns $\underbrace{R^* - R_{f_{ct^*}}}_{\mathrm{Eval}(f, m_b) = \mathrm{Enc}(f(m_b), R_f)}$

LWE + Circular security
+ randomness leakage
(from some FHE Evals) ⇒ iO

Chosen-plaintext security w/ "Shielded randomness leakage" [GP 20].

Secure for GSW under LWE

Gay-Pass $\mathcal{O}_{SRL}$-CIRC conjecture:

For "natural" schemes S,

S 2-circ. secure + S SRL secure $\Rightarrow$ S secure against both leakages simultaneously

Our attack: Counterexample when S is GSW*

* "Vanilla" GSW!, No addn'l circuit gates or parity constraints.

Our Attack:

Given: - $ct = Enc(m_b)$,
- key cycle

Get to choose circuit $f: m^b \to \{0,1\}$

depending on:

- $ct^* = Enc(0, R^*)$
- the key-cycle

Observe $R_f - R^*$

Our Attack:

Given: - $ct = Enc(m_b)$,
- key cycle

Get to choose circuit $f : m^b \to \{0,1\}$ depending on:

- $ct^* = Enc(0, R^*)$
- the key-cycle

Observe $R_f - R^*$

$U = pk$, $R = $ (rand.)

Observation 1:

FHE Eval of $m^b \cdot 0$ moves m^b into rand.

$$(UR + m^b \cdot G) \cdot G^{-1}(UR' + 0 \cdot G)$$

$$=$$

$$U(RG^{-1}(UR' + 0 \cdot G) + m^b \cdot R')$$

Our Attack:

Given: - $ct = Enc(m_b)$,
- key cycle

Get to choose circuit $f : m^b \to \{0,1\}$
depending on:
- $ct^* = Enc(0, R^*)$
- the key-cycle

Observe $R_f - R^*$

$$U(\underbrace{R G^{-1}(UR' + 0 \cdot G) + m^b \cdot R'})$$

Will be "shielded" w/ R^*

Use key cycle to access R^* inside f !!

Our Attack:

Given: - $ct = Enc(m_b)$,
- key cycle

Get to choose circuit $f : m^b \to \{0,1\}$

depending on:

- $ct^* = Enc(0, R^*)$
- the key-cycle

Observe $R_f - R^*$

$$U(\underbrace{RG^{-1}(UR' + 0 \cdot G) + m^b \cdot R'})$$

Will be "shielded" w/ R^*

Use key cycle to access R^* inside f !!

use sk_1 (under pk_2) to find $(-sk_1, 1)^T ct^* = e^T R^*$

"short" vec. from decryption

Our Attack:

Given: - $ct = Enc(m_b)$,
- key cycle

Get to choose circuit $f : m^b \to \{0,1\}$ depending on:

- $ct^* = Enc(0, R^*)$
- the key-cycle

Observe $R_f - R^*$

Now can get:

$$RG^{-1}(UR' + 0 \cdot G)$$
$$+ (m_b + e^T R^* v)R'$$ for any vec v we want
$$- R^*$$

Choose v s.t. $G^{-1}(UR' + 0 \cdot G)v = 0$

⇒ find $(m_b + e^T R^* v) R'v + R^* v$

Our Attack:

Given: - $ct = Enc(m_b)$,
- key cycle

Get to choose circuit $f : m^b \to \{0,1\}$

depending on:

- $ct^* = Enc(0, R^*)$
- the key-cycle

Observe $R_f - R^*$

Now can get:

$$RG^{-1}(UR' + 0 \cdot G)$$
$$+ (m_b + e^T R^* v) R'$$
$$- R^*$$

for any vec v we want

Choose v s.t. $G^{-1}(UR' + 0 \cdot G) v = 0$

$\Rightarrow$ find $(m_b + e^T R^* v) R' v + R^* v \}$

use to build lin. system solved by e

Conclusions

- Security of LWE + circular security + randomness leakage (from some FHE Evals) sensitive to particular structure of leakages
  ⇒ general versions likely false
- Natural next question: more specific assump of [Devadas-Quach-Vaikuntanathan-Wee-Wichs] ?
- Other versions which avoid attack?