# Expedition to Obfustopia: From Well-Studied Assumptions to New Frontier

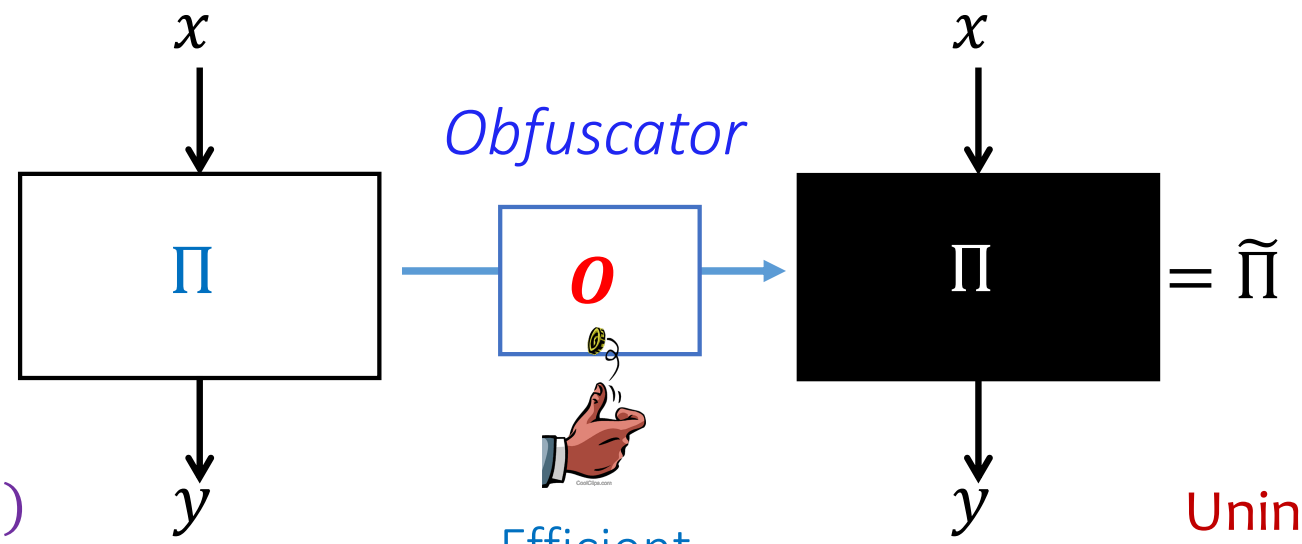
**Huijia (Rachel) Lin**

**UW**

Thanks to Yao-Ching Hiesh, Aayush Jain, Stefano Tessaro for their generous help

# Conception: One-Way Compilers [Diffie-Hellman 1976]

Can we efficiently transform a program into one
that is functionally equivalent and hides secrets?




$\forall x, \tilde{\Pi}(x) = \Pi(x)$

Efficient
randomized algorithm

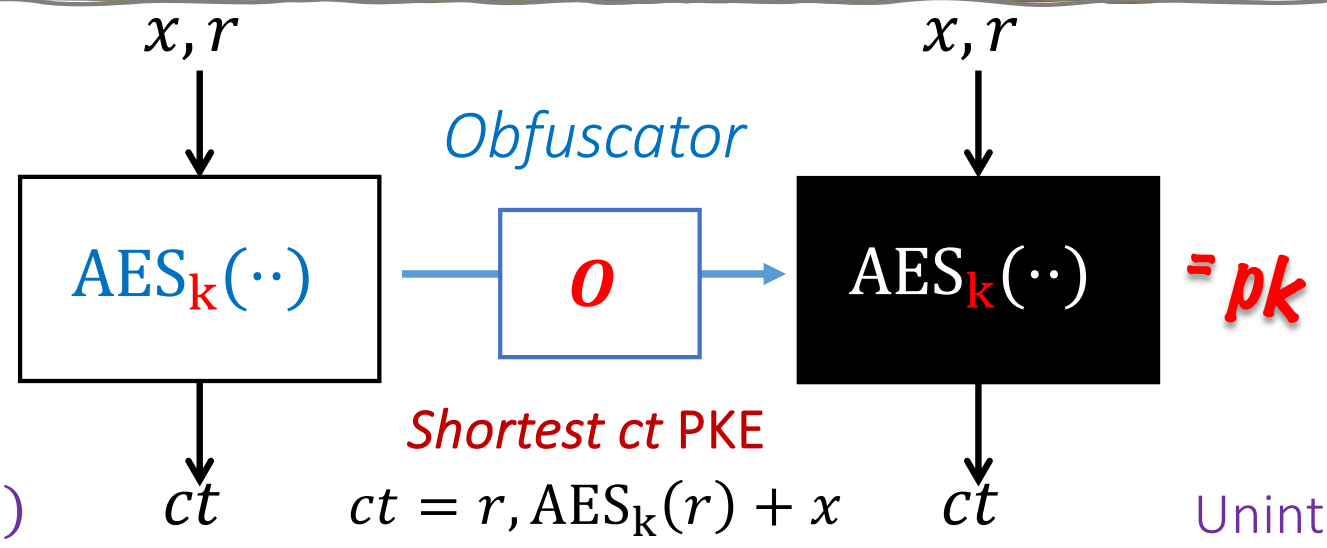
Unintelligible

# Conception: One-Way Compilers [Diffie-Hellman 1976]

Does public-key crypto exist?

Obfuscated secret key encryption

➔ *public key encryption*



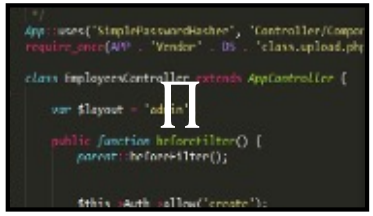

$\forall x, \widetilde{\Pi}(x) = \Pi(x)$

Unintelligible

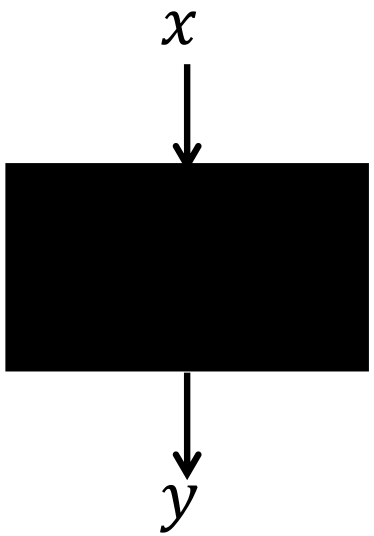
# Ideal Obfuscation for General Programs [Hada00, BGIRSVY01]

White-box access

Black-box access

$\tilde{\Pi} =$  $\Pi$

$\approx^*$

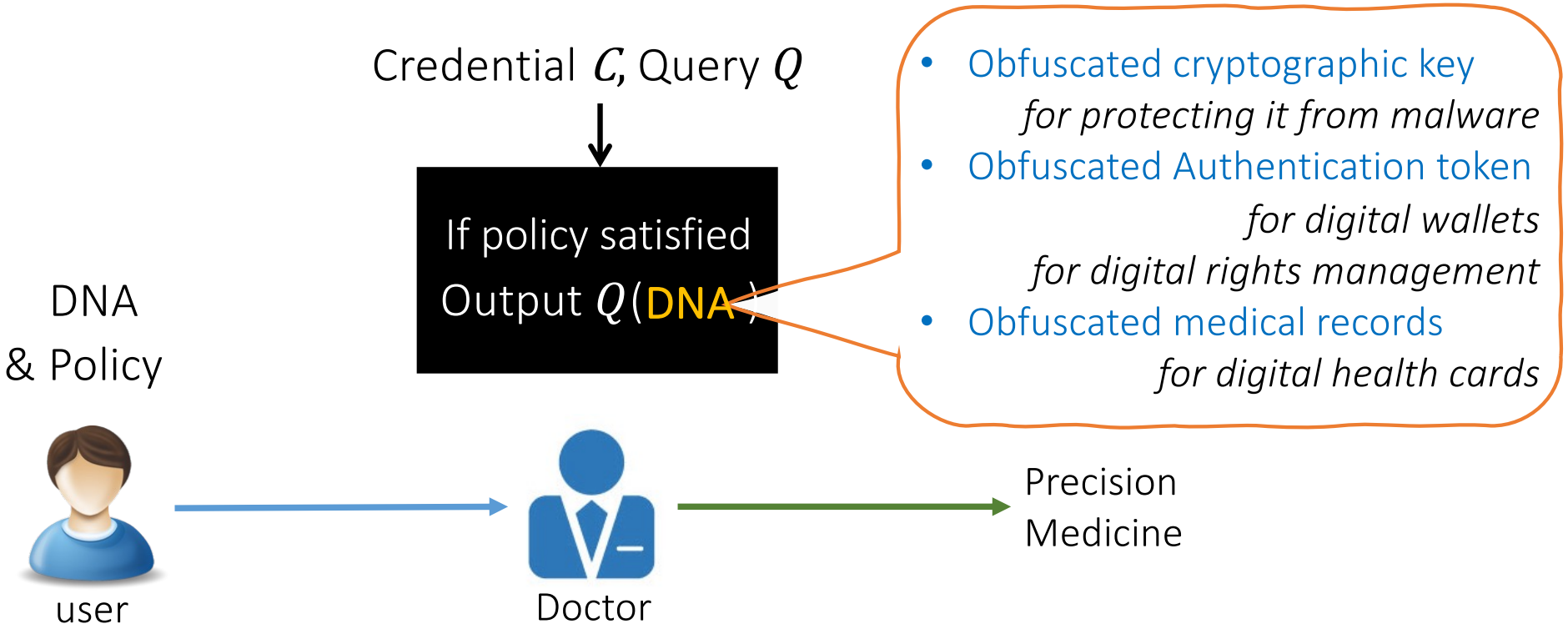


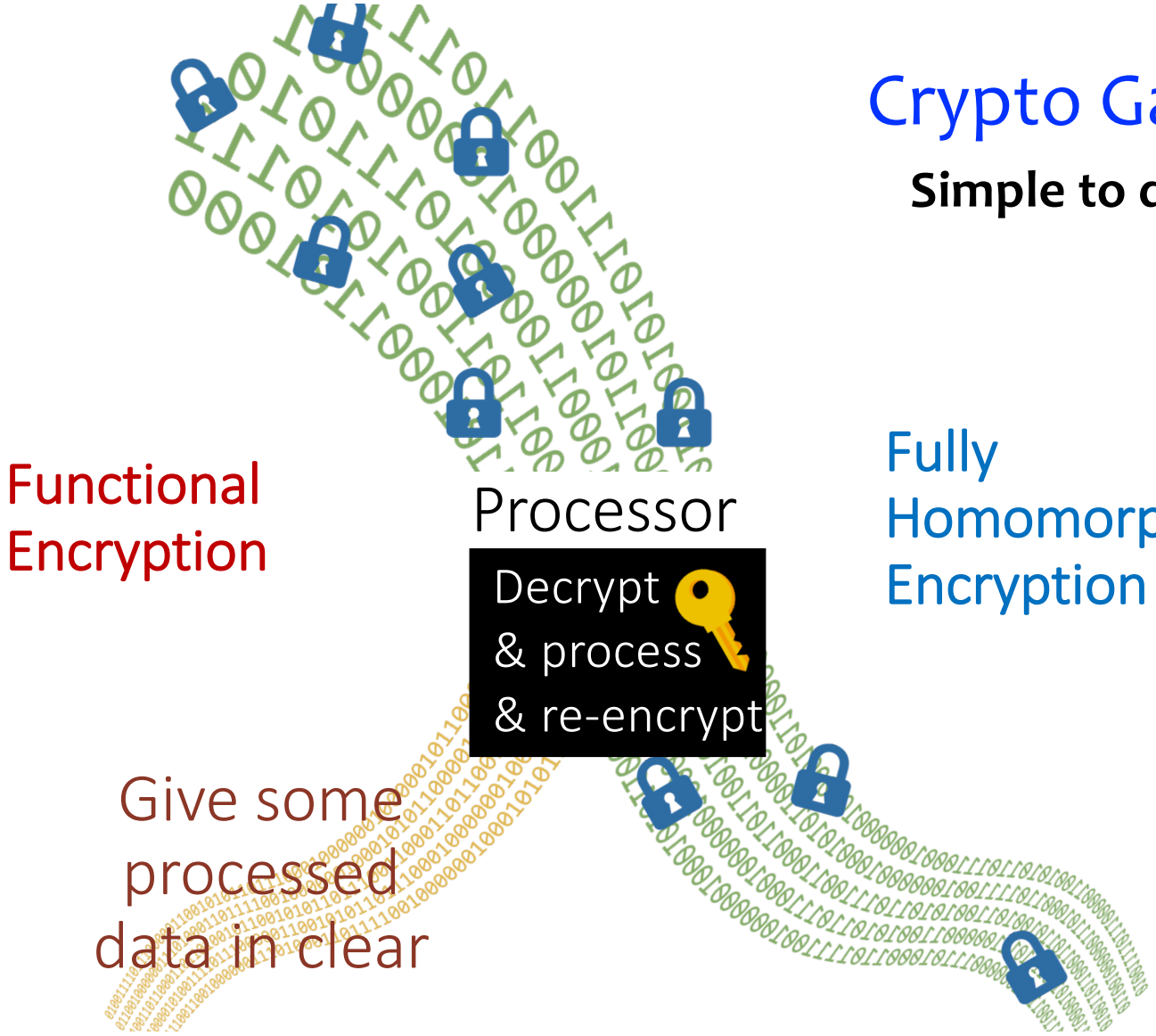

Hide secrets not efficiently learnable
from the input-output behavior of $\Pi$

*up to polynomial time computation advantage

# “Usable” Secrets

Enforce *fine-grained* access to data



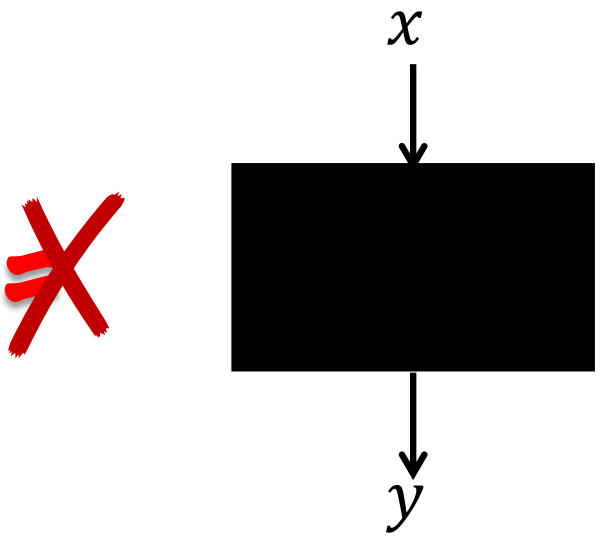

Crypto Galore!
Simple to design!
Functional Encryption
Processor
Decrypt & process & re-encrypt
Fully Homomorphic Encryption
Give some processed data in clear

# Impossibility: Ideal Obfuscation [Hadaoo, BGIRSVY01]

White-box access


Have a program that computes $\Pi$

Black-box access



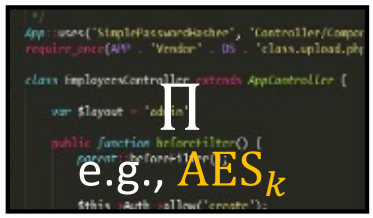

Cannot learn a program that computes $\Pi$

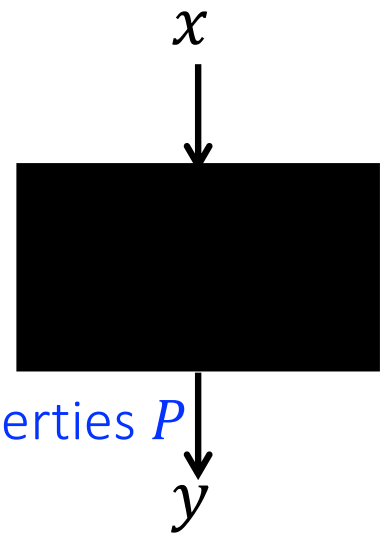
For all black-box unlearnable programs

# Virtual Black-Box (VBB) [Hada00, BGIRSVY01]

White-box access

Black-box access




Natural

protecting specific properties $P$

e.g., $P(\mathrm{AES}_k) = k$

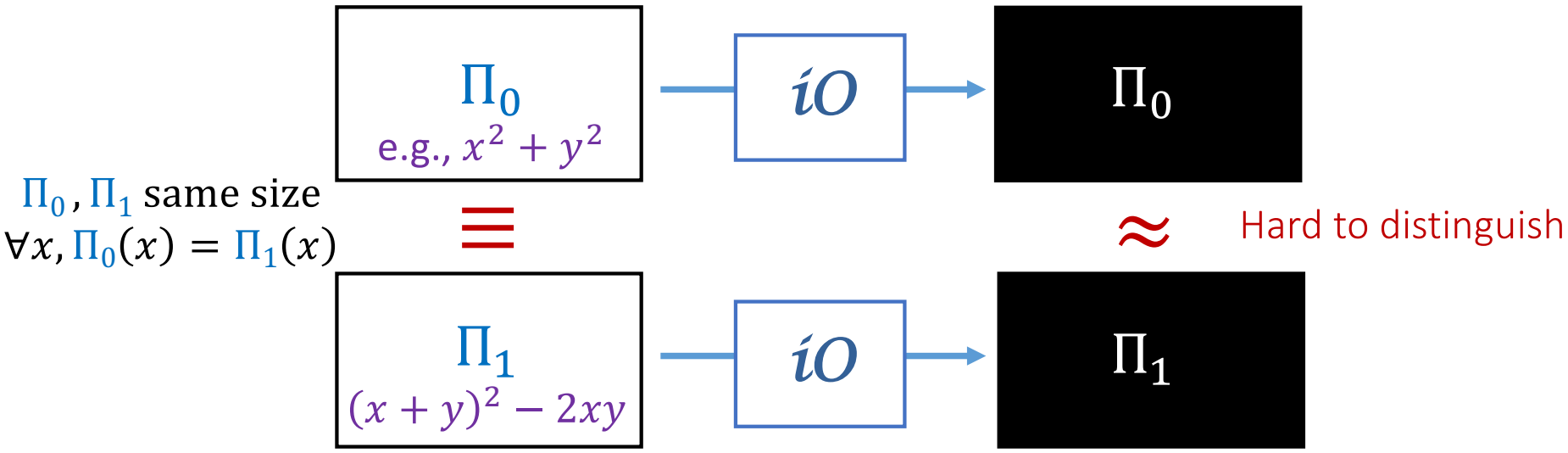
$P(\Pi)$ learnable from white box **only if** $P(\Pi)$ learnable from black box

[BGIRSVY01] ruled out VBB for general predicate properties $P$

by showing contrived counterexamples $(\Pi, P)$

# Indistinguishability Obfuscaiton (iO) [BGIRSVY01]

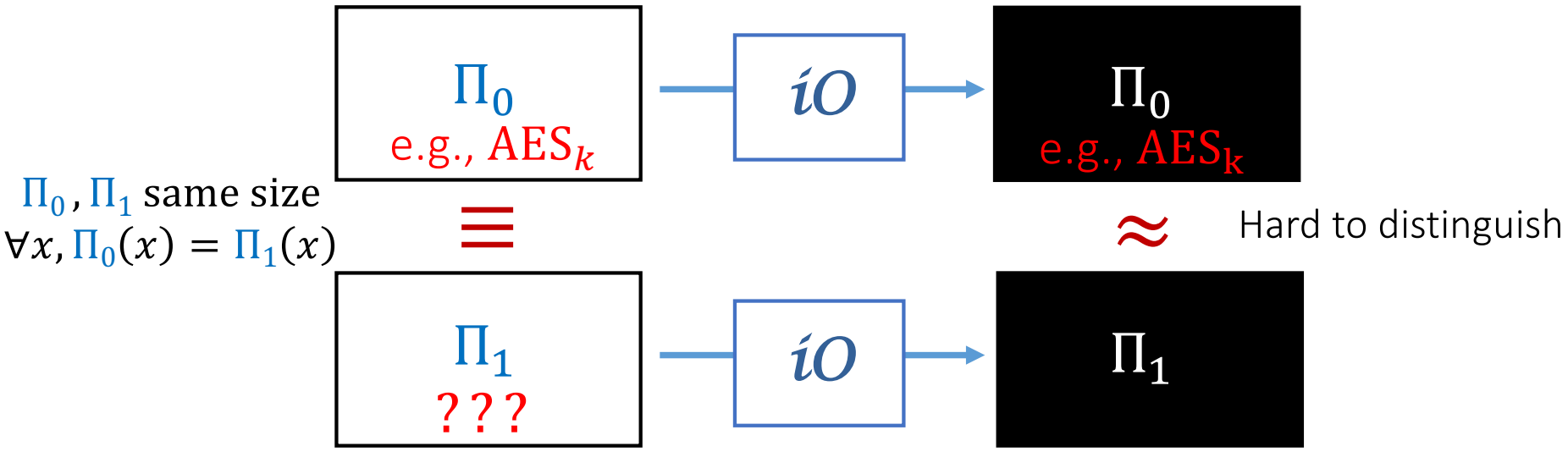
Is iO useful?  Can we construct iO?




Hide implementation difference

# What does iO hide?

e.g., Does $iO(\mathrm{AES}_k)$ hide $k$?

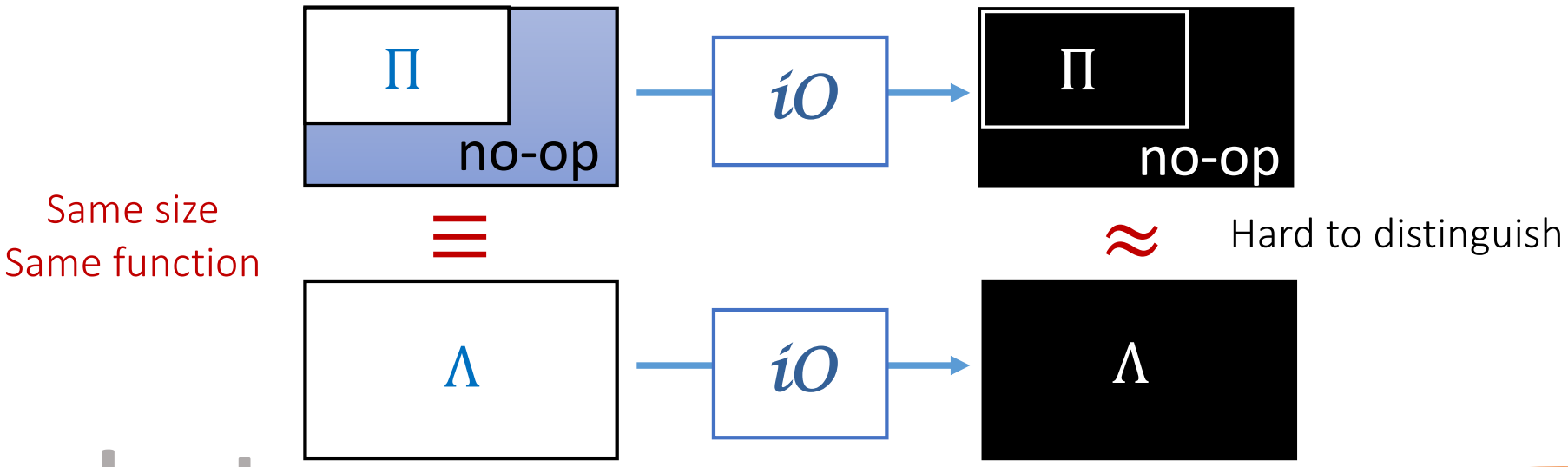



Hide implementation difference

Weak << VBB

# iO, the Best Possible Obfuscation [BGIRSVY'01,GR'08]

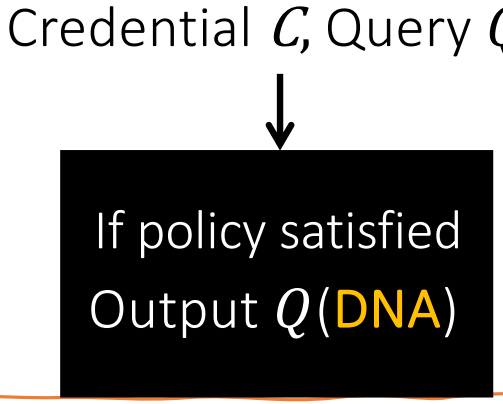
Then $iO(\underline{\text{padded}}\ \Pi)$ is as secure as $iO(\Lambda)$, hence as secure as $\Lambda$




**Best-Possible Heuristic:** $iO(\Pi)$ hides the best-possible to be hidden,
partially justified by best-possible obfuscation [GR08]

**Best-Possible Heuristic:** $iO(\Pi)$ hides the best-possible to be hidden,
partially justified by best-possible obfuscation [GR08]

# What Does the Best Possible Obfuscation Hide?

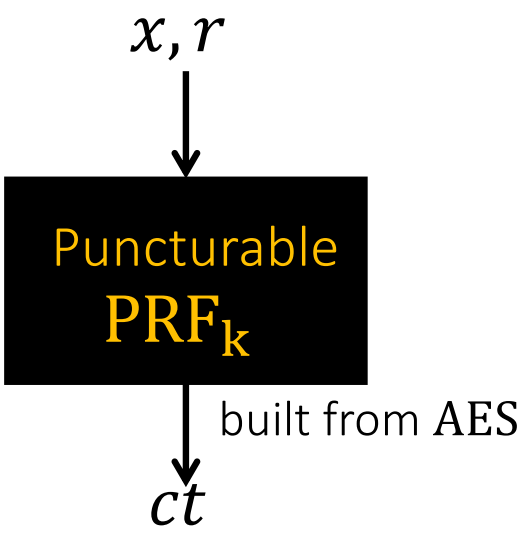



**VBB Heuristic:** VBB possible for **natural** $\Pi$ and $P$ (e.g., key recovery of $\mathrm{AES}_k$)
partially justified in the Pseudo Random Oracle (PRO) Model [JLLW24]

**RO Heuristic:** White-box access to $\mathrm{SHA3}(k,\cdot)$ = Black-box access to $\mathrm{RO}$
*Effectively,* the code of $\mathrm{SHA3}(k,\cdot)$ acts as a VBB obfuscation of $\mathrm{PRF}_k$

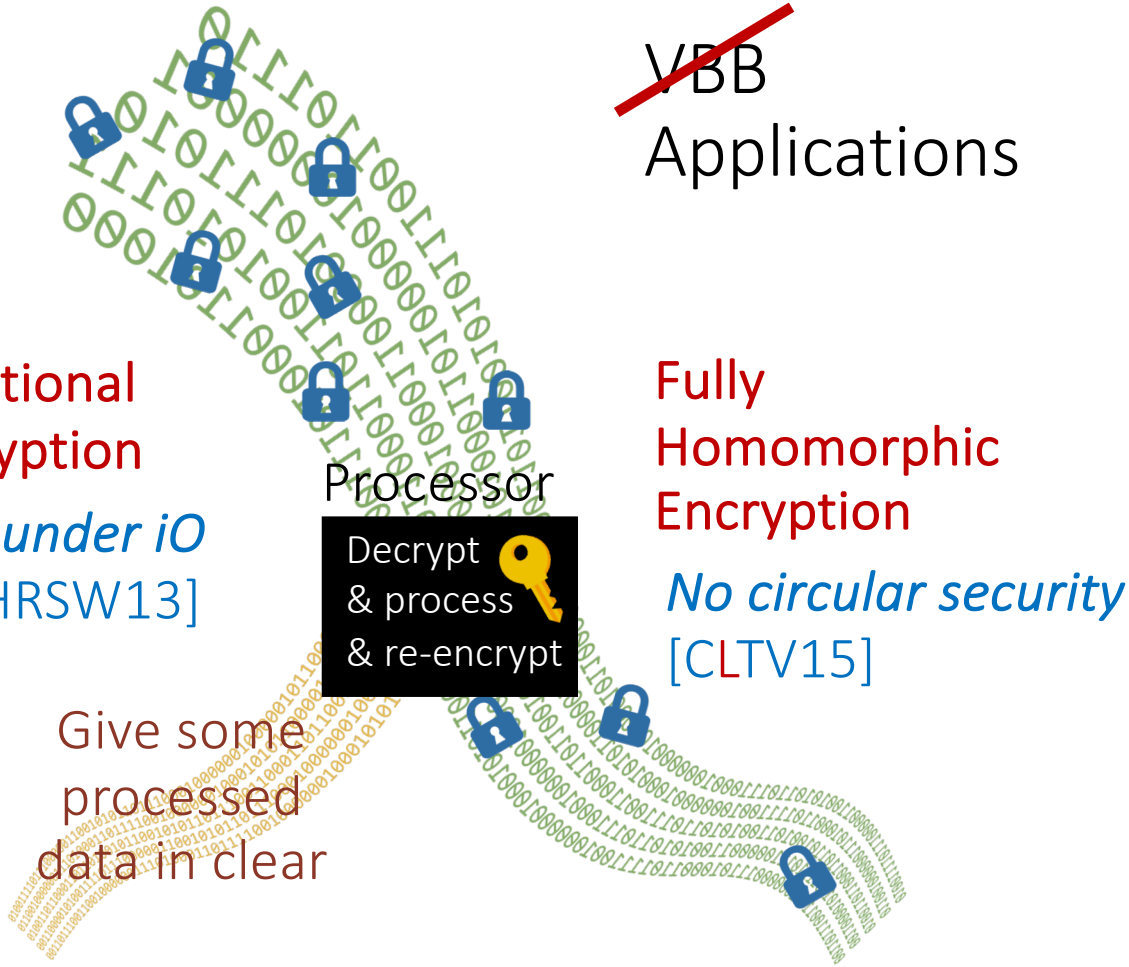
# Punctured Programs Technique

[Sahai-Waters14]




*Shortest ct* PKE

$ct = r, \mathrm{AES}_k(r) + x$




~~VBB~~

IO

Applications

Functional Encryption

*Only under iO*

[GGHRSW13]

Fully Homomorphic Encryption

*No circular security*

[CLTV15]

# Obfustopia

**Still, Simple to design!**

iO +

minimal hardness

NP ⊊ ioBPP

↓

Most Crypto

One-Way Functions

Public Key Encryption

Hardness of Finding Nash

Short Signature

Trapdoor Permutation

Identity-Based Encryption

Attribute-Based Encryption

Fully Homomorphic Encryption *

Multiparty Computation

(Non-Interactive) Zero-Knowledge

Two-Round MPC

Hardness of finding Nash

Functional Encryption

Witness Encryption

(Doubly) Deniable Encryption

Secret Sharing for NP

Correlation Intractable Hash

SNARG for NP in the standard model

Multi-Party Non-Interactive Key Exchange

OWF with poly hard core bits

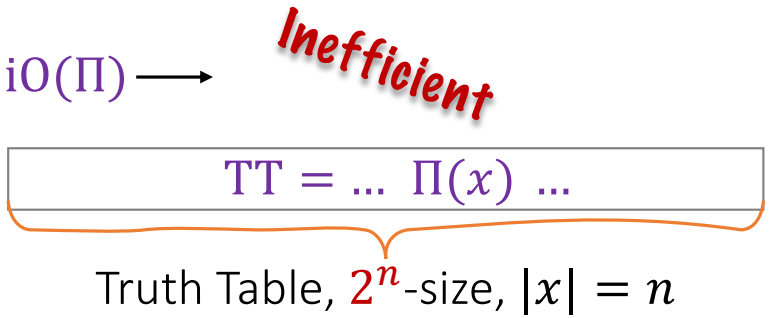
Succinct Garbled RAM

Multilinear Map

Constant Round Concurrent ZK

Publicly verifiable quantum money

# Can We Construct iO?



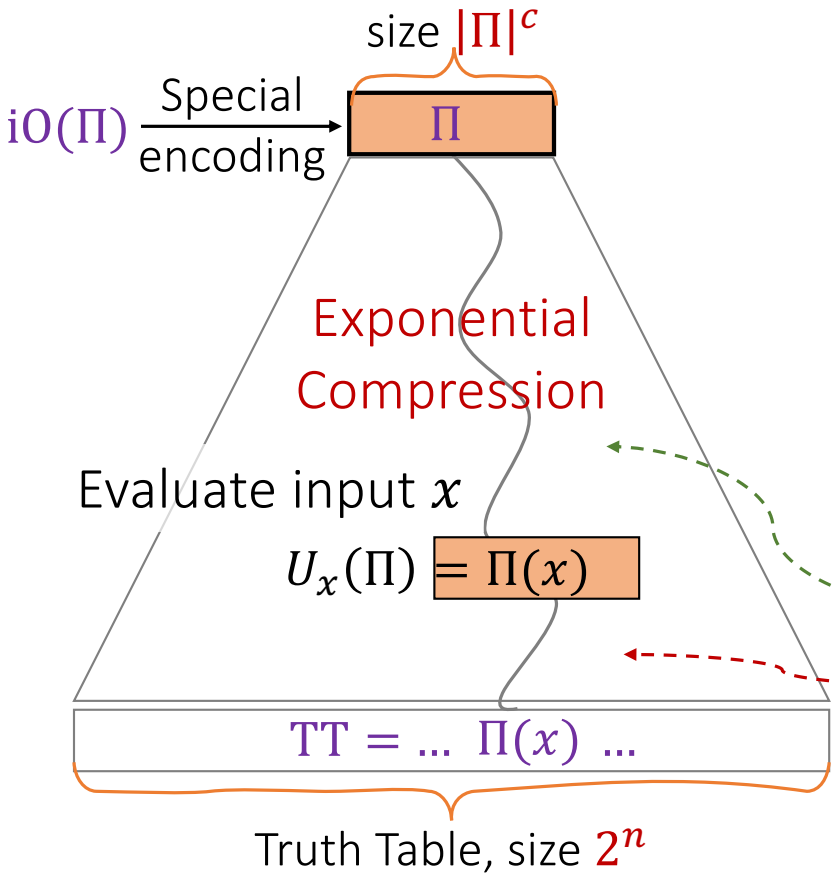

Perfect Security:

If $\Pi_0, \Pi_1$ compute the same function then $\mathrm{TT}_0 = \mathrm{TT}_1$

Another view of iO security:

Reveal $\mathrm{TT}$, and nothing else of $\Pi$

# Can We Construct iO?




Security:

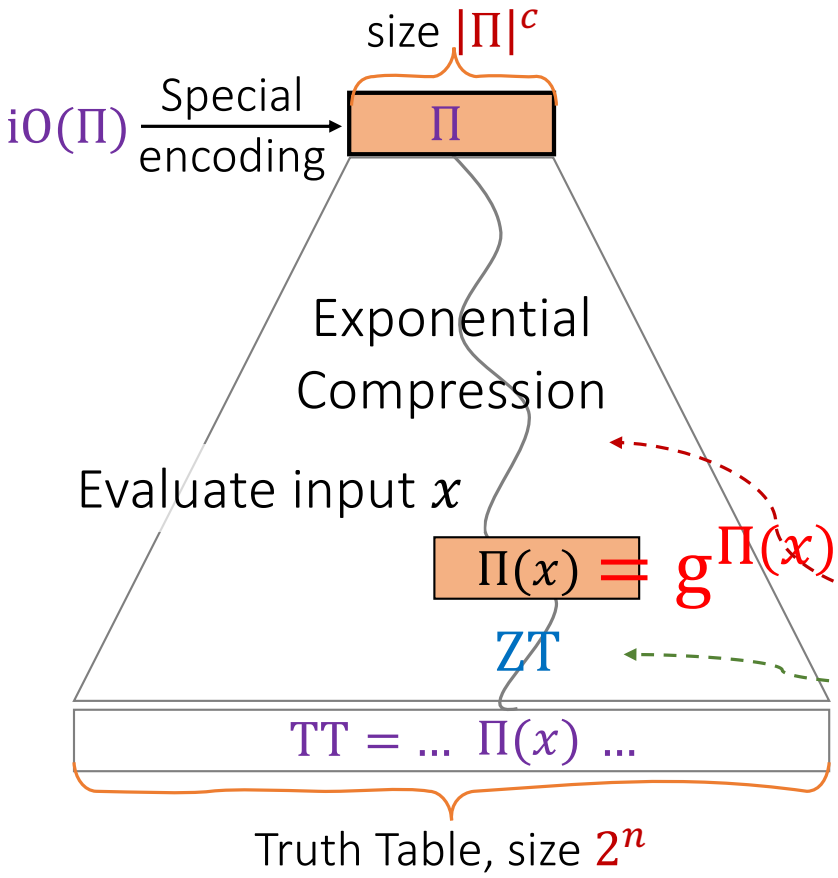
Reveal $TT$, and nothing else of $\Pi$

*Compare to FHE:*

✓ Homomorphic evaluation of input $x$

✗ Don't know how to reveal output

# Can We Construct iO?




Security:

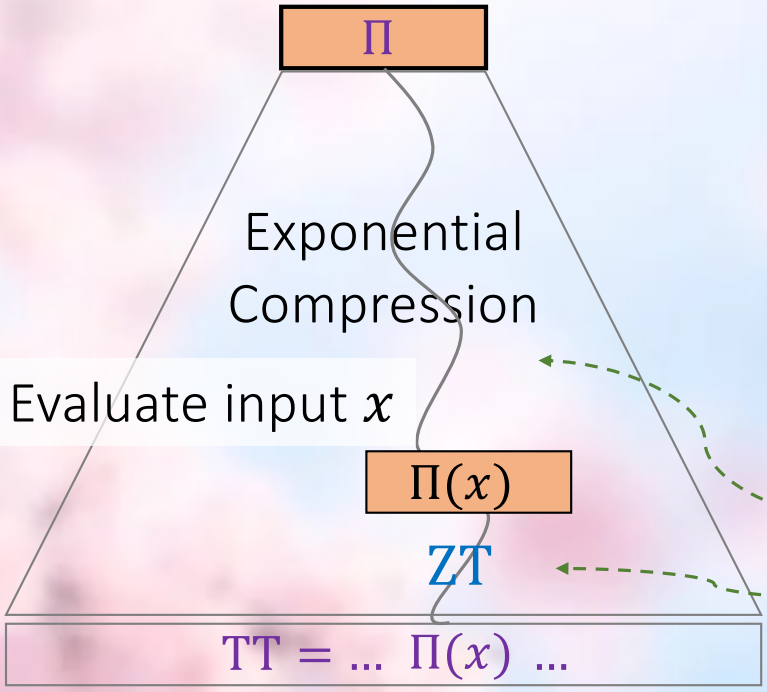
Reveal TT, and nothing else of $\Pi$

*Compare to pairing groups:*

✗ Homomorphic deg 2 evaluation

✓ Zero test to reveal output, only

# First iO [Garg-Gentry-Halevi-Raykova-Sahai-Waters'13]




lattice-based candidate

**Multi-linear maps**

[GGH13,CLT13,GGH15,CLT15…]

*Using multi-linear maps for iO*

✓ Homomorphic evaluation of input $x$

✓ Zero test to reveal output, only

**Explosion of iO**

[BR14, BGKPS14, PST14, GLSW14, AGIS14, Zim15, AB15, GMMSSZ16, DGGMM16, GJ18, BIJMSZ20 …]

# Attacks and Repairs

iO from

IO resisting

Zero

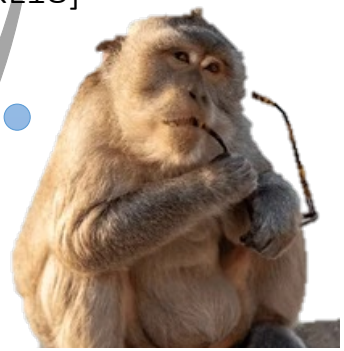
Perfect "scientific thriller"!

iO is fascinating, mysterious, and challenging

*Time to try a different approach!*

Other Types of Math

[GJ18, BIJMSZ20, CCMR24]



## 2015-2020, which minimal objects imply iO?

[Lin16, LV16, Lin17, AS17, LT17, GJK18, BIJMSZ20, Agr19, AJS18, LM18, AJS18, JLMS19, JLS19, AP20,GJLS21]

***Simpler Tools Suffice for iO e.g.,***

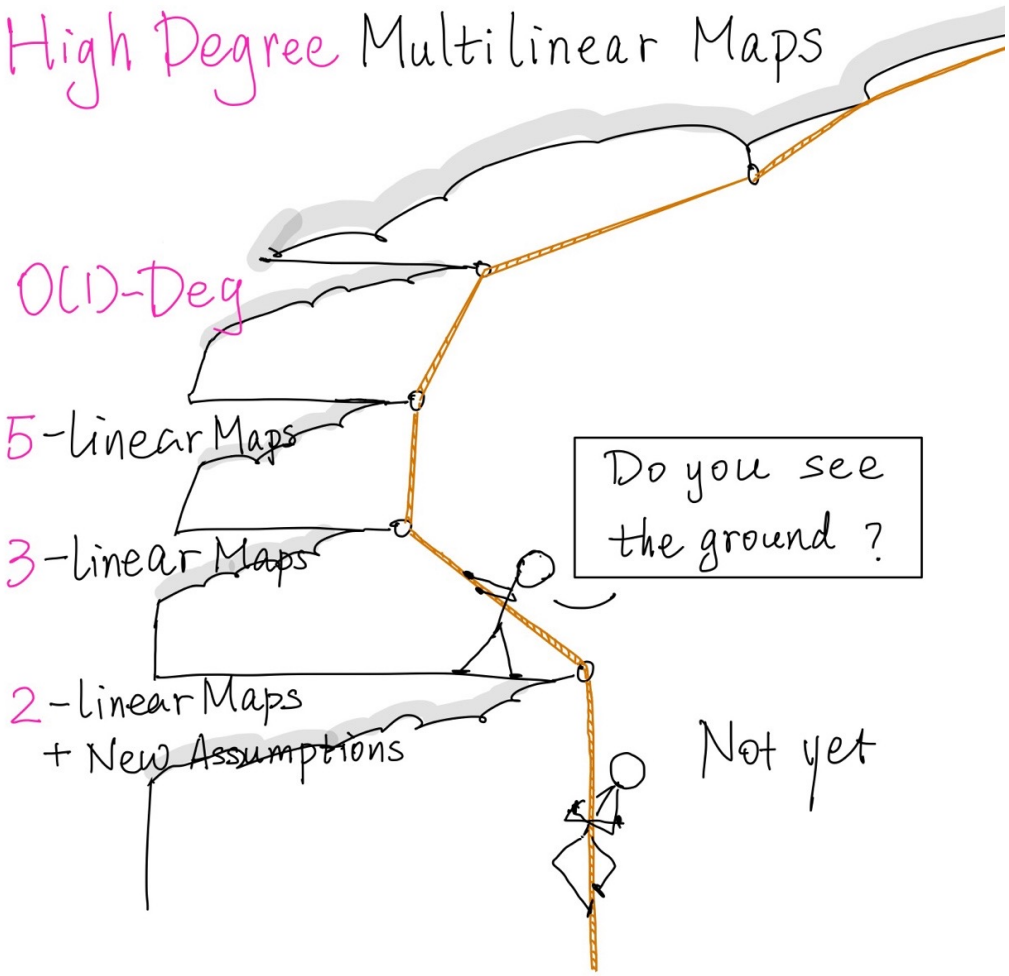
Functional Encryption (FE) [AJ15,BV15]

Exponential Efficiency iO (xiO) [LPST16]

***Simpler Programs Suffice e.g.,***

$NC^0$ assuming PRG in $NC^0$ [Lin16]

LWE Sampler [WW22]



# 2021-2022, foundations

Theorem [Jain-L-Sahai21, Jain-L-Sahai22]:
iO from three well-studied assumptions

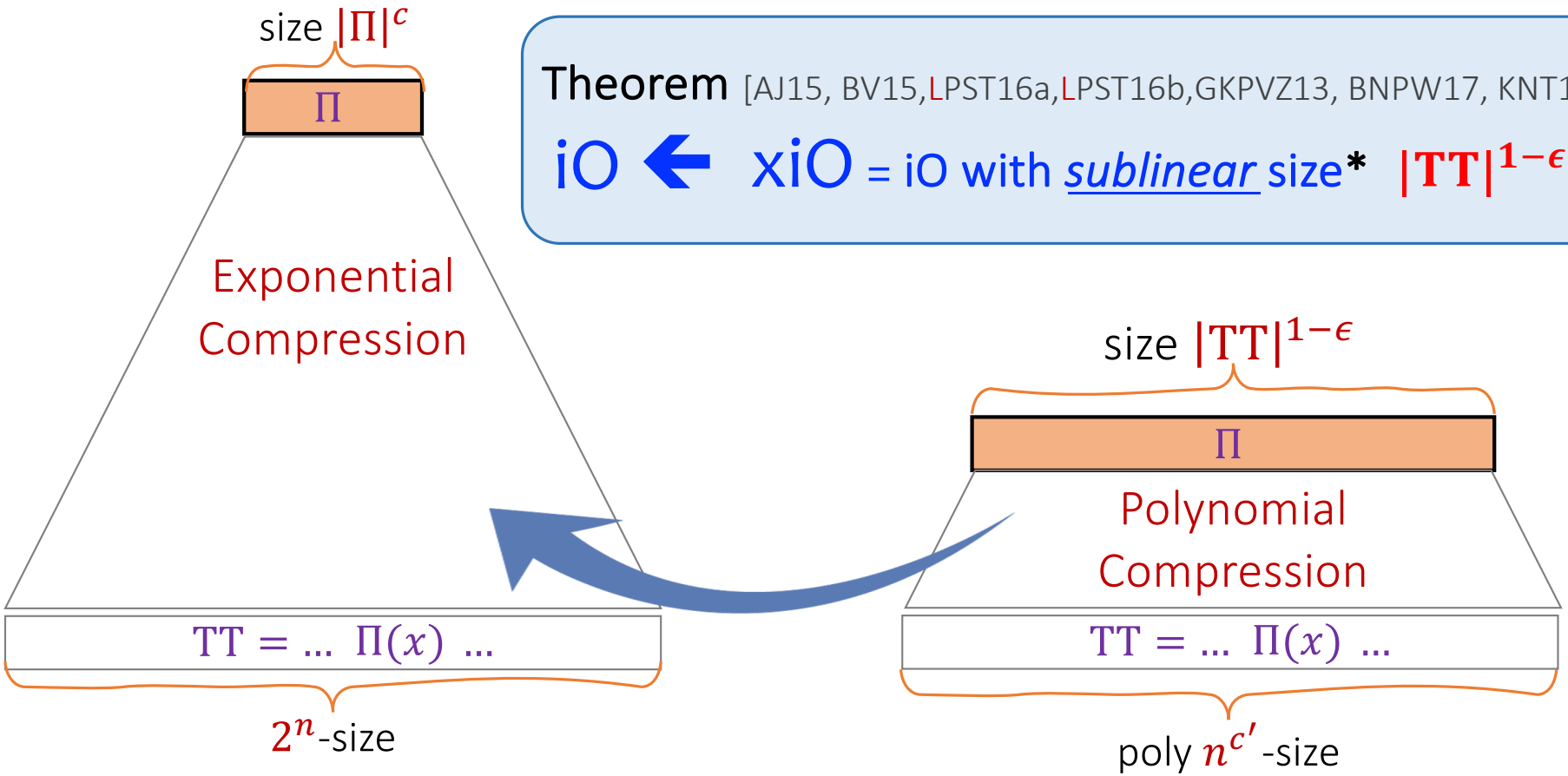
1. Learning parity with noise, LPN, over large field $\mathbb{F}_p$ [IPS09]
2. Local pseudo-random generator, PRG in $NC^0$ [Gol00]
3. Decision linear, DLIN, on symmetric bilinear map [BBS04]

All with subexponential security level

or sparse LPN [RVV24]

- History of study and application in crypto
- Connection with coding theory, information theory, complexity theory, number theory & algebra

# Exponential Efficiency iO (xiO) [L-Pass-Seth-Telang16b]



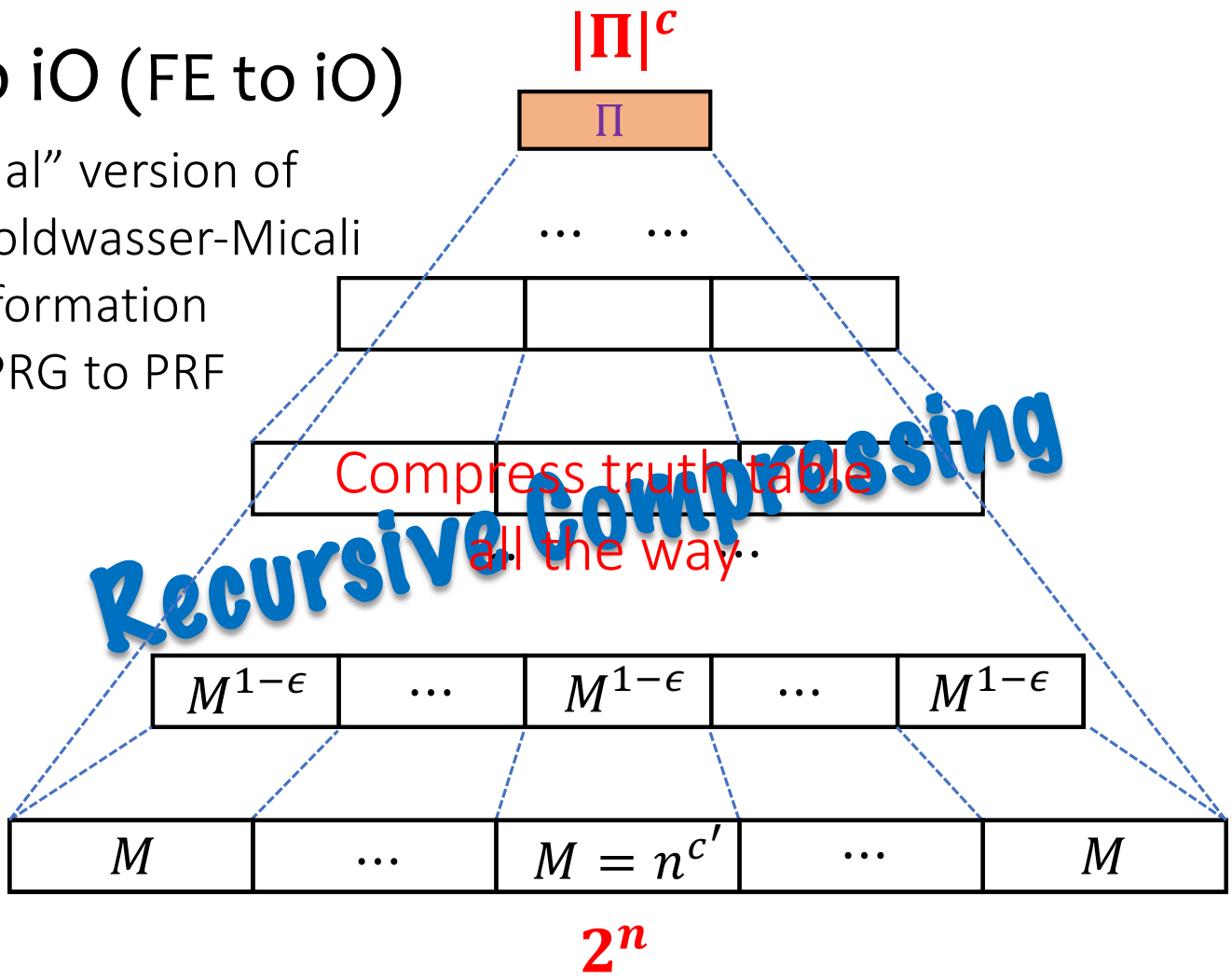

**Theorem** [AJ15, BV15, LPST16a, LPST16b, GKPVZ13, BNPW17, KNT18]

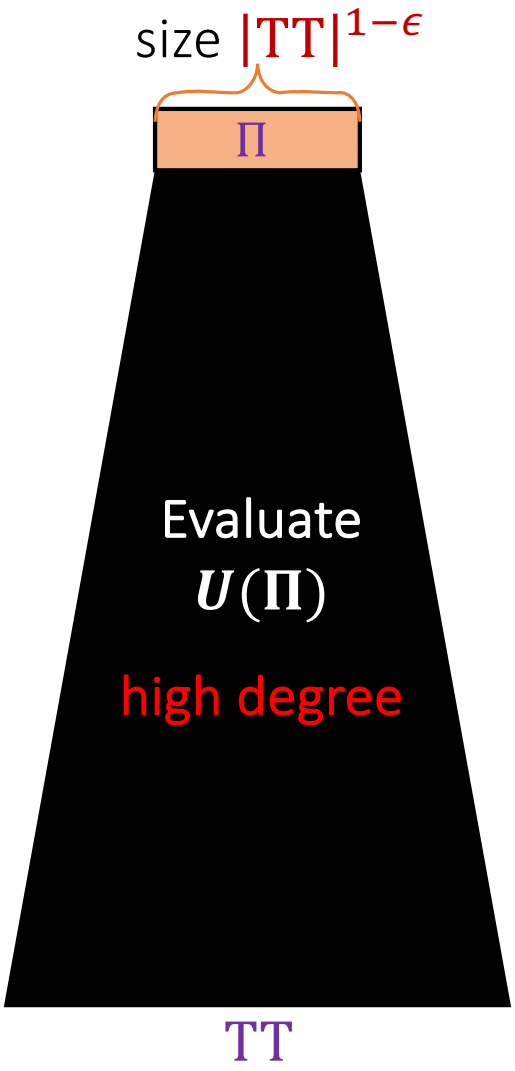
iO ← xiO = iO with *sublinear* size* $|\mathrm{TT}|^{1-\epsilon}$

* Time-efficiency needed

# xiO to iO (FE to iO)

"Functional" version of Goldreich-Goldwasser-Micali transformation from PRG to PRF






# xiO, still challenging

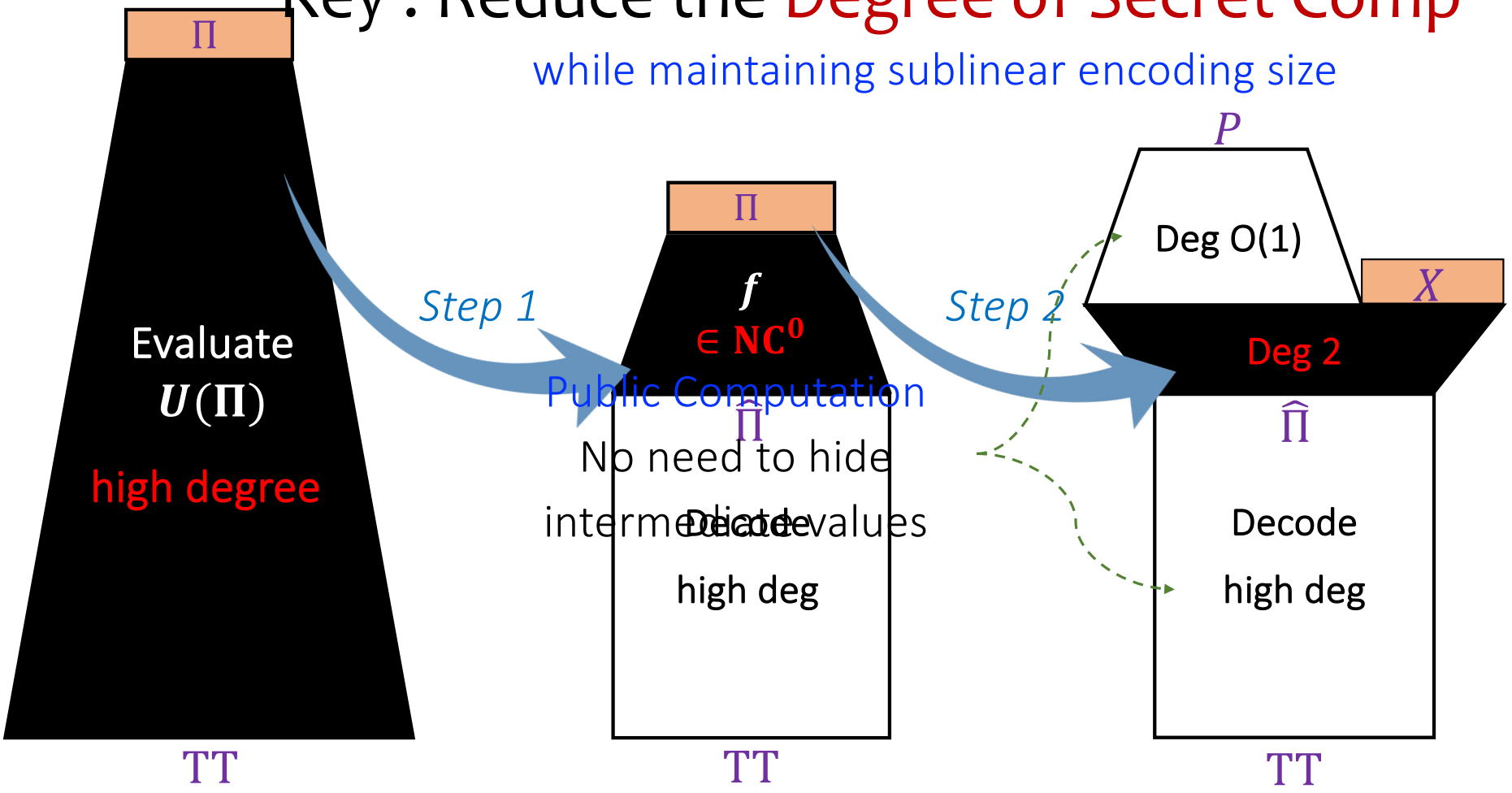
"secret computation"

To hide $\Pi$, it necessary to hide
*every intermediate computation value*
*(except for the final outputs)*

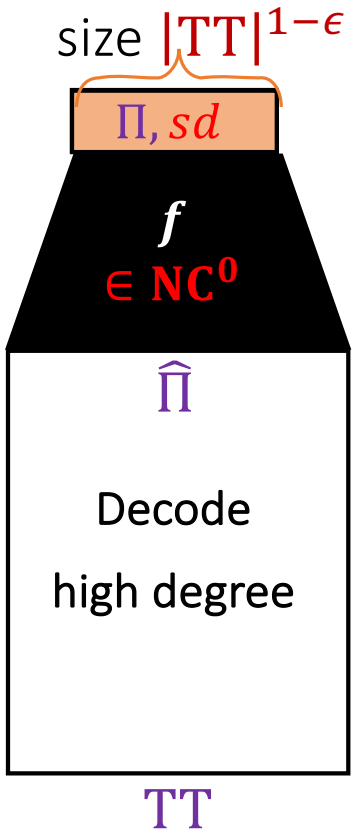
➔ complex, high degree, secret computation

# Key : Reduce the Degree of Secret Comp

while maintaining sublinear encoding size



# Reduce Secret Computation to $\mathrm{NC}^0$




**Randomized encoding (RE)** [Yao82,IK02,AIK04]

from Complex computation $U(\Pi) = \mathrm{TT}$

to Simple $f(\Pi; sd) = \mathrm{RE}(U; \Pi; r) = \widehat{\Pi}\mathrm{PRG}(sd)) = \widehat{\Pi}$

s.t. $\widehat{\Pi}$ reveals TT, only

randomness $r$ must be hidden,

and $sd$ is long: $|sd| \gg |\mathrm{TT}|^{1-\epsilon}$

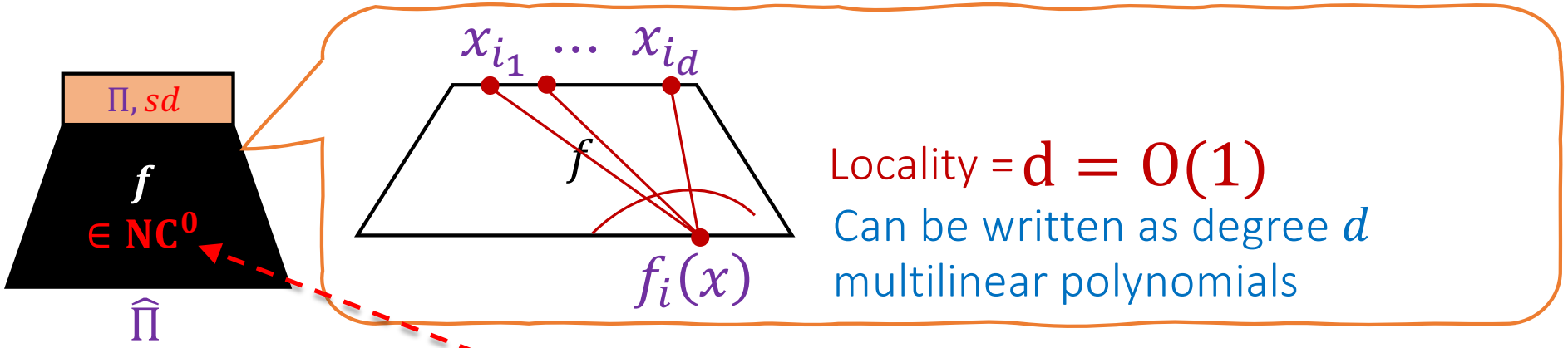
*Assume PRG in $\mathrm{NC}^0$.*

*Expand to long seed*

**Theorem** [Lin16] *Assume PRG in NC0*

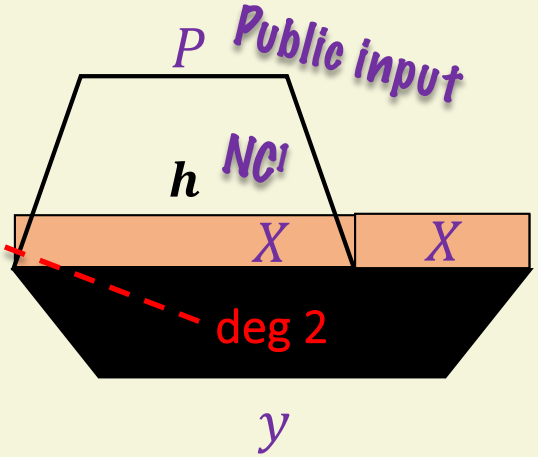
xiO ← xiO for $\mathrm{NC}^0$

# xiO for NC⁰, Still Challenging




*Assume pairing*

Perform degree 2 secret computation revealing only the outputs



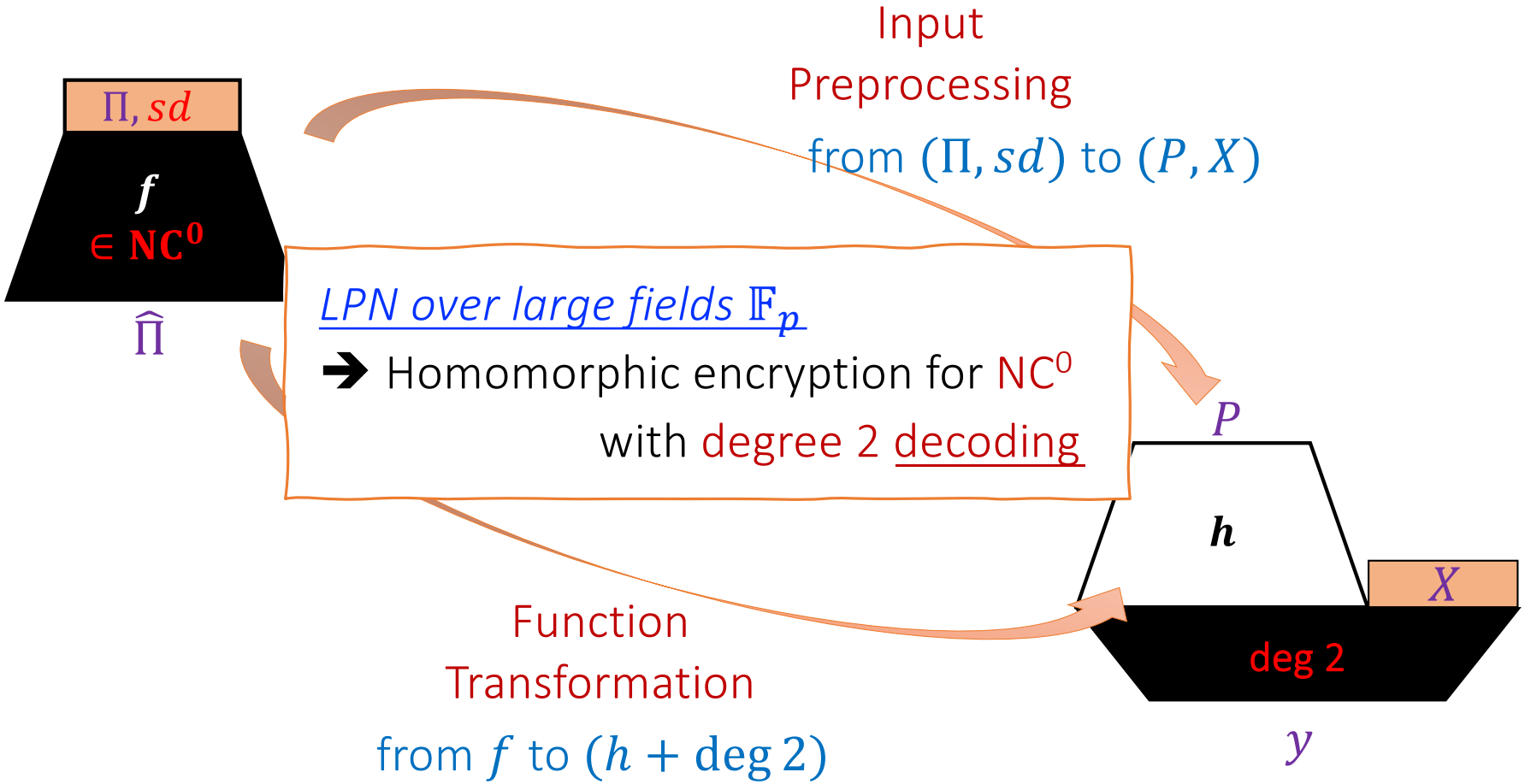

**Theorem** [Lin17,AJLMS18,JLMS19,JLS19,Wee20]

*Assume DLin over Pairing*

$$\text{xiO}^* \text{ for } \{y_i = \langle h_i(P), X \otimes X \rangle\}$$

* Stronger: partially hiding FE

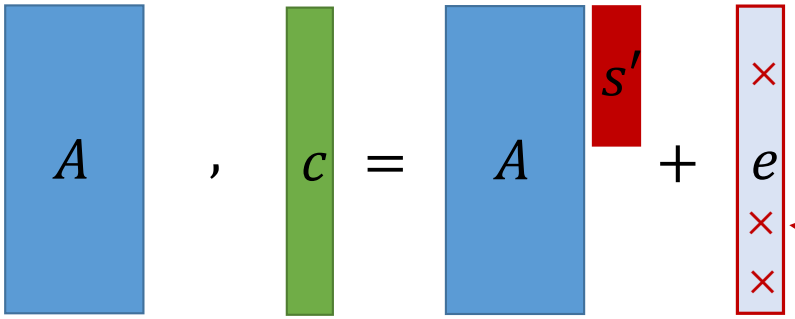
# Reduce Secret Computation to Degree 2 [JLS21,JLS22]



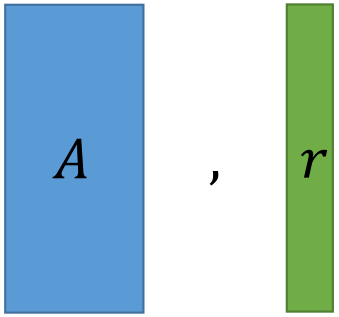
# Learning Parity with Noises (LPN) [BFKL94,IPS09]

Prime modulus $p$ $\quad A \leftarrow \mathbb{F}_p^{l \times k}, l > k \quad s' \leftarrow \mathbb{F}_p^k$

Hard to decode random linear codes with errors




$\approx$ Hard to distinguish



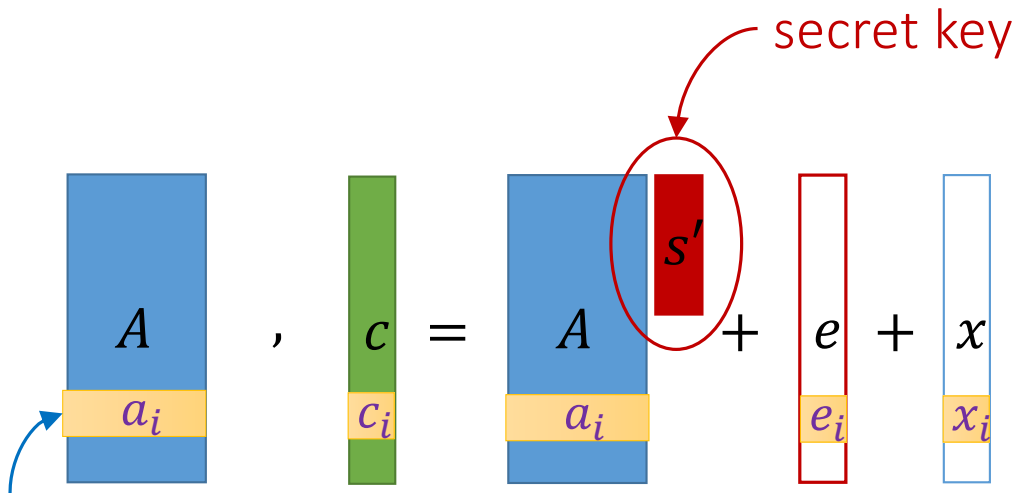

$r \leftarrow \mathbb{F}_p^l$

SPARSE errors: For $0 < \delta < 1$, e.g., $\delta = \mathbf{0.01}$

$$e_i = \begin{cases} u_i \leftarrow \mathbb{F}_p & \text{Inverse poly rate } \frac{1}{k^\delta} \\ 0 & \text{otherwise} \end{cases}$$

- Long history of study in coding theory
- Best Known Attacks $O\left(2^{k^{1-\delta}}\right)$ [EKM17]
- When $\delta$<0.5, unknown if LPN implies PKE

# LPN ➔ Secret Key Encryption




a ciphertext: $\boldsymbol{ct_i = (a_i, c_i)}$ $\boldsymbol{c_i = a_i \cdot s' + x_i + e_i}$

Approximate linear decryption:

$$\langle \underbrace{(\boldsymbol{a_i, c_i})}_{ct_i}, \underbrace{(\boldsymbol{-s', 1})}_{s} \rangle = \boldsymbol{x_i + e_i}$$

# LPN ➔ Homomorphic Encryption for $NC^0$

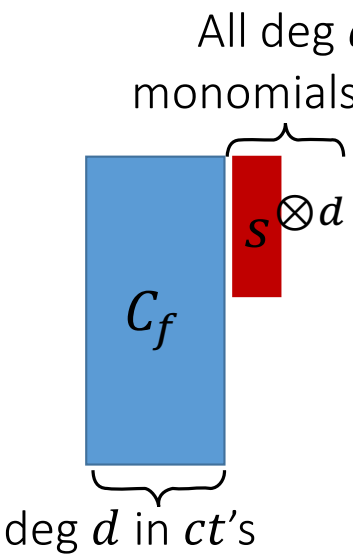
Homomorphic mult:

$$\langle ct_i, s\rangle \cdot \langle ct_j, s\rangle = (x_i + e_i) \cdot (x_j + e_j)$$

$$\langle ct_i \otimes ct_j, s \otimes s\rangle = x_i x_j + e_{ij}$$

---

Homomorphic evaluation:




$f \in \mathrm{NC}^0$

constant deg $d$ poly in $\mathbb{F}_p$

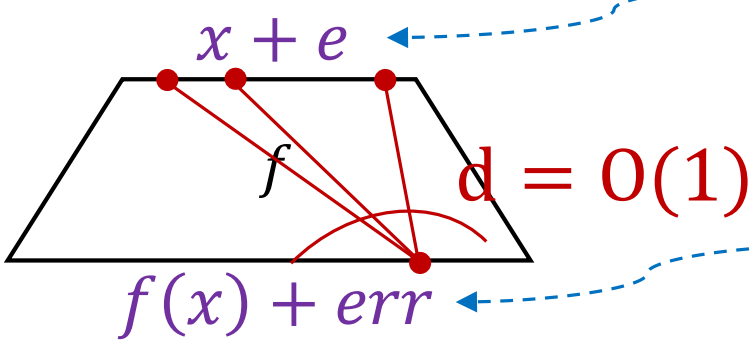
Local

$=$ $f(x+e) = f(x) + err$

Sparse

# If $f$ is local, $err$ sparse

Every output element depends on a constant number of input elements




**Sparse input error**

$$\Pr[e_j \neq 0] = \frac{1}{k^{\delta}}$$

**Sparse output error**

$err_i \neq 0$ iff one of its neighbor $e_i \neq 0$

$$\Pr[err_i \neq 0] \leq \frac{O(1)}{k^{\delta}}$$

Homomorphic Evaluation for $NC^0$

$$C_f \cdot s^{\otimes d} = f(x) + err$$

Sparse

# Degree 2 Decoding

High degree

$\mathrm{Dec}(C_f, s)$: $\mathrm{ErrCorrect}\left(C_f \cdot s^{\otimes d}\right) = f(x) + err$

insecure to leak $err$

---

Relaxation: Allow decoding secret $X$ to depend on $s, f, x, e$

Deg 2

$\mathrm{Decode}(C_f, X)$: $X$ is short, sublinear in $|f(x)|$

size $\leq m^{1-\epsilon} \leq |f(x)|^{1-\epsilon'}$

$X = (s^{\otimes d}, U, V)$

Sparse

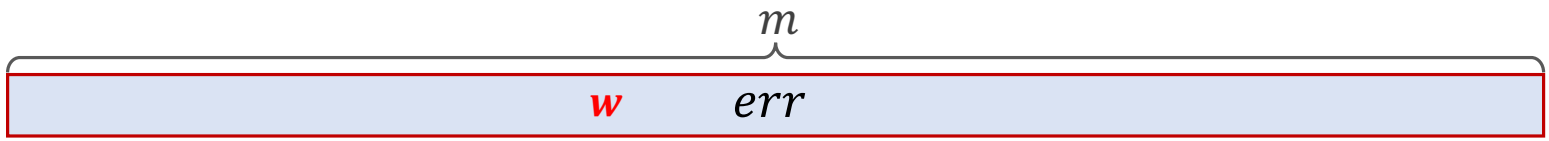
$C_f \cdot s^{\otimes d} - \mathrm{Expand}(U, V) = f(x)$

$\mathrm{Compress}(err) = U, V$ size = $|U, V| < m^{1-\epsilon}$

$\mathrm{Expand}(U, V) = err$ degree 2

# The Compression Task – A taste of idea

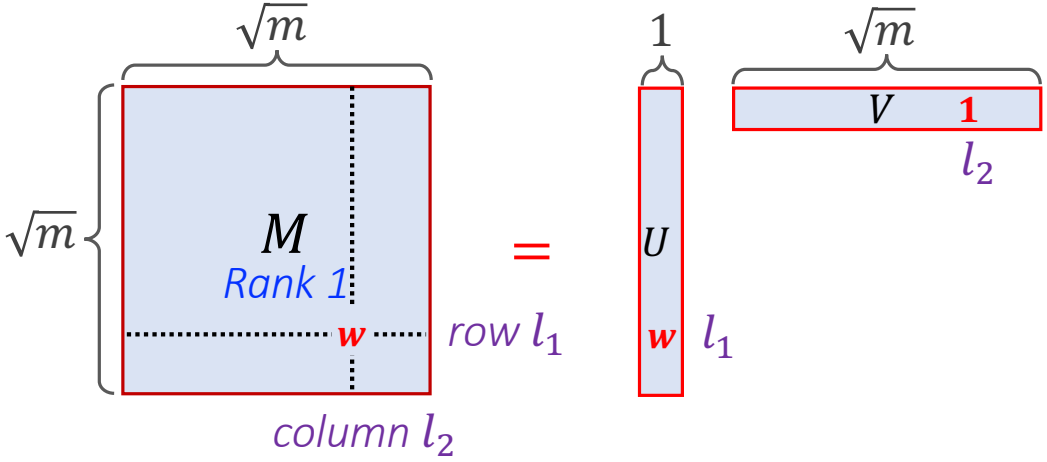
Toy Case: $err$ contains $1$ non-zero errors (generalize to few errors)




$\text{Compress}(err) = U, V$

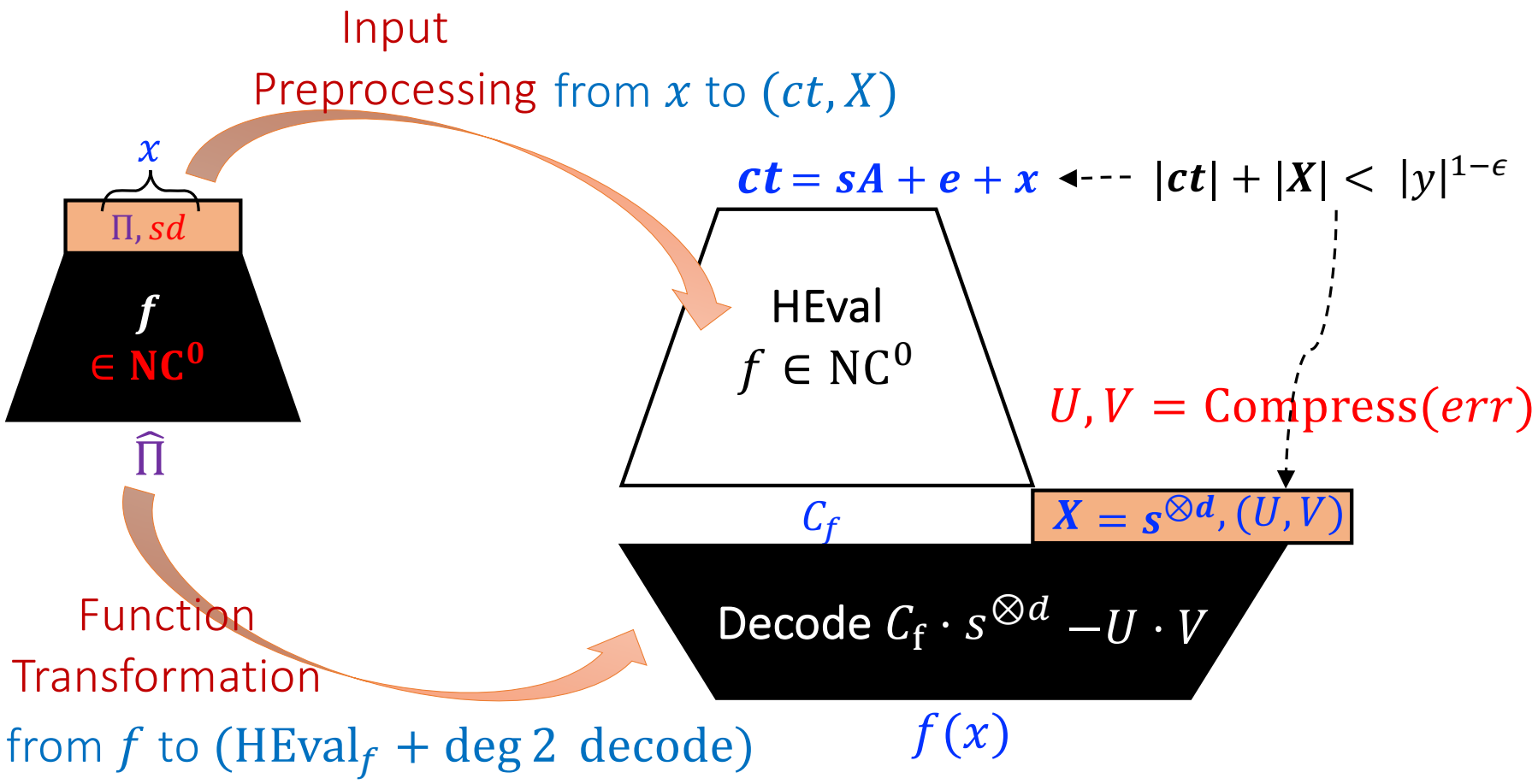
$|U, V| = 2\times\sqrt{m}$

$\text{Expand}(U, V) = U \cdot V = err$




**Lemma** [JLS21] Compression for any $\frac{1}{k^{\delta}}$-sparse err vector, $\delta \in (0,1)$

xiO for NC⁰ LPN Homomorphic Encryption



# Wide Open


*from* LPN over $\mathbb{F}_p$

PRG in $NC^0$ & Pairing

No Lattice!

quantum easy

"Minimal" assumptions that imply iO?

- Less number of assumptions?
- Remove PRG in $NC^0$?
- polynomial hardness suffice?

More efficient constructions?

- Efficient xiO (FE) to iO transformation?

Post-quantum Security?

- iO from LWE or not?

Challenge: Lattice based iO

# Grand Goal: iO from Standard Lattice Assumptions!

Poll:

A. Optimistic > 70%
B. Half-half 30% ~ 70%
C. Pessimistic < 30%

So far,

candidates based on multilinear maps
[GGHRSW13…]

or, candidates inspired by FHE
[BDGM20,GP21,BDGM22,WW21,DQVWW21,HJL25]

Security based on
new, simple-to-state, lattice assumptions

*Circular Shield-Randomness Security* [GP21,BDGM22]
*Homomorphic Pseudorandom LWE Samples* [WW21]
*Subspace Flooding Assumption* [DQVWW21]
*Circular Security with Random Opening* [HJL25]

LWE with Hints

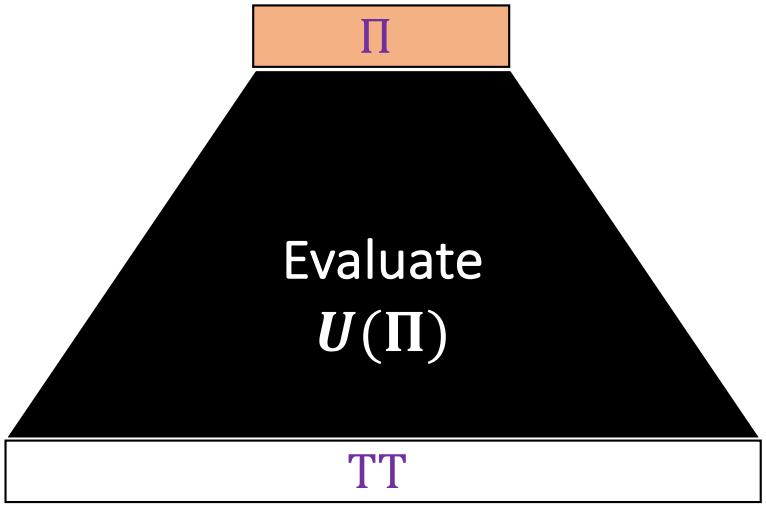
# LWE

(Circular) LWE:

$$\bar{A} = \begin{pmatrix} A \\ sA + e \end{pmatrix} + f^{\text{circ}}(s) \approx \$$$

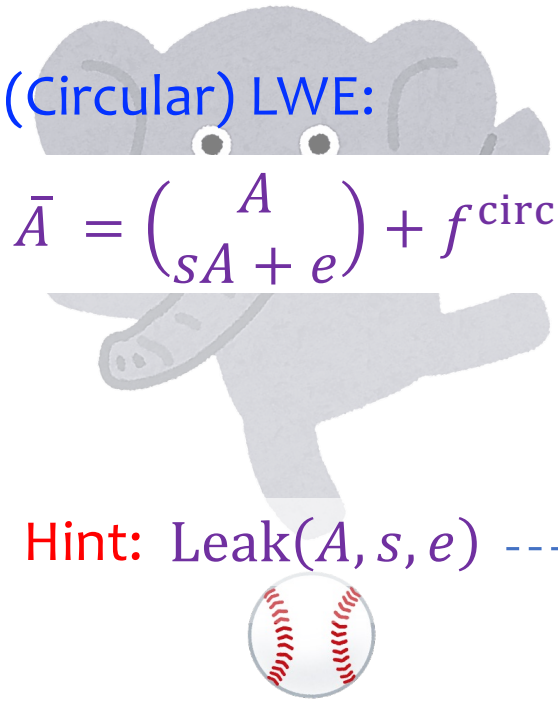
➔ Fully homomorphic encryption
[Gentry09, BV11,GSW13… ]

# xiO



# LWE with Hints

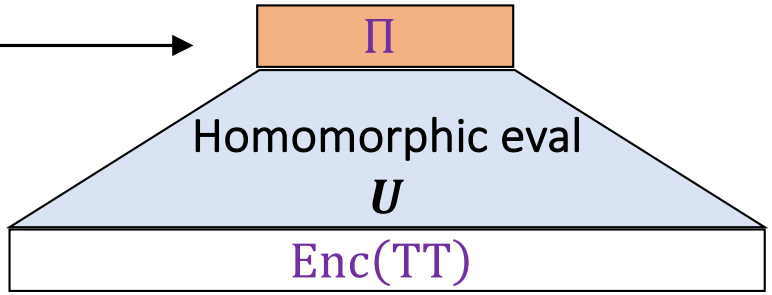
# xiO



(Circular) LWE:

$$\bar{A} = \begin{pmatrix} A \\ sA + e \end{pmatrix} + f^{\text{circ}}(s)$$






Hint: $\text{Leak}(A, s, e)$ ------- ~~facilitates~~ ------- Opening $\theta$

TT

Idea [Brakerski-Döttling-Garg-Malavolta'20]:
Provide a short opening $\theta$, $|\theta| < |\text{TT}|^{1-\epsilon}$,
that opens Enc(TT), but not Enc(Π)

# What Hints?

(Circular) LWE:

$$\bar{A} = \begin{pmatrix} A \\ sA + e \end{pmatrix} + f^{\text{circ}}(s)$$

Function of the secret leak$(s)$

→ leak$(e)$ [WW21,DQVWW21]

Inhomogenous trapdoor $T_B = B^{-1}(P)$

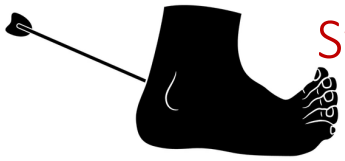
→ leak$(e)$ [BDJMMPV2,AKY24]

Opening $R$ of a ct of zero w.r.t. a pk

[GP21,BDGM22]

Hint: leak$(A, s, e)$

(+ noise leakage)



Structural vulnerabilities in hints (+ noise leakage), alone

[HJL21,JLLS23,DJMMV25,AMYY25,HJL25]

# Provably Secure Hints?

(Circular) LWE:

$$\bar{A} = \begin{pmatrix} A \\ sA + e \end{pmatrix} + f^{\mathrm{circ}}(s)$$

Hint: $\mathrm{leak}(A, s, e)$

Opening $R$ of a Regev Encryption $\mathrm{ct}$ of zero w.r.t. a $\mathrm{pk}$

Circular security with random opening (CRO) assumption [Hsieh-Jain-L25]

Features:

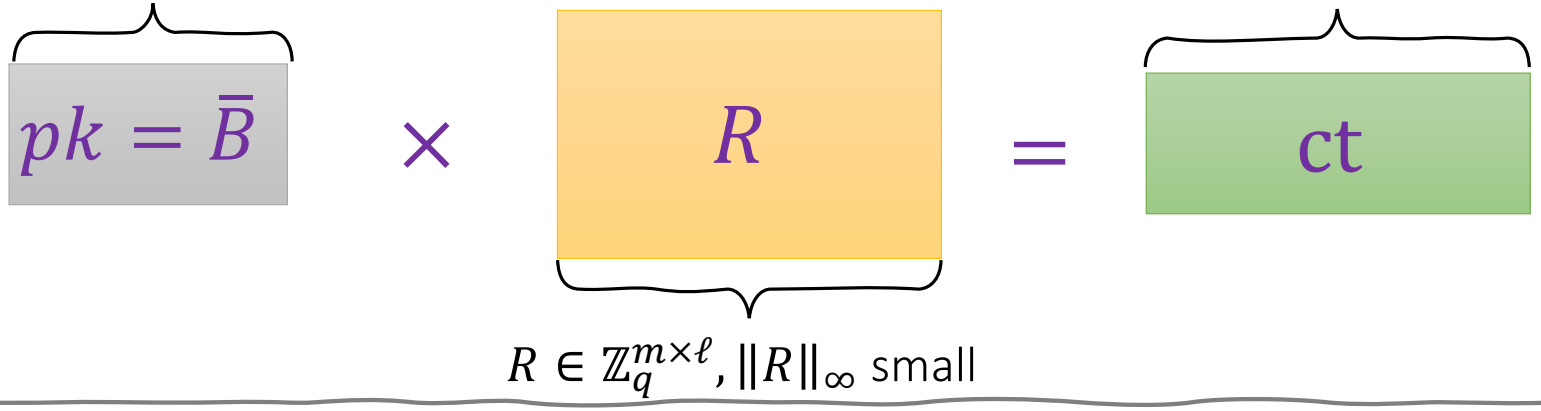
*Marginally random* hints

*No* natural noise leakage

No vulnerabilities in hints alone

# Regev Encryption [Reg05]: $\mathrm{RegE}_{pk}(0^\ell; R) = \mathrm{ct}$

$$pk = \bar{B} = \begin{pmatrix} B \\ rB + e_B \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m} \qquad ct = \begin{pmatrix} A = BR \\ rA + e_B R \end{pmatrix}$$



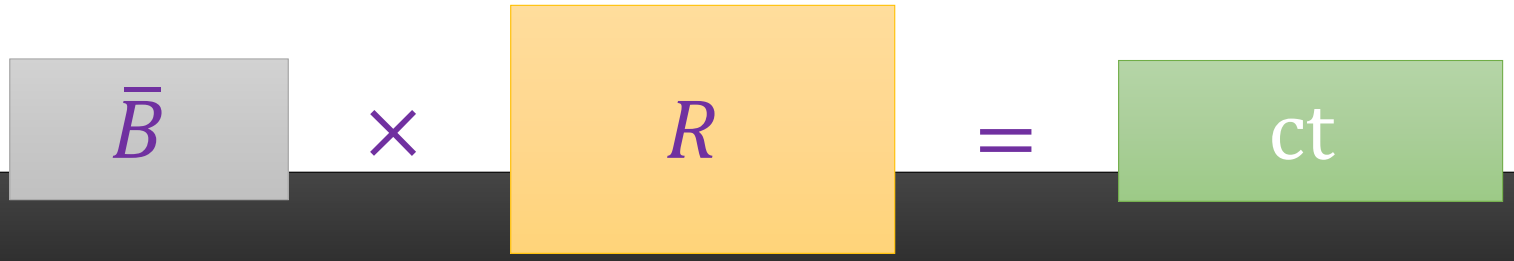

An opening of $\mathbf{ct}$ w.r.t. $\mathbf{pk} = \bar{B}$: $R'$, $\|R'\|$ small, $\bar{B}R' = \mathrm{ct}$

Random opening of $\mathbf{ct}$ w.r.t. $\mathbf{pk} = \bar{B}$: $R' \leftarrow \mathcal{D}_\sigma^{m\times\ell} | \bar{B}R' = \mathrm{ct}$

$\mathcal{D}_\sigma$ discrete gaussian with width $\sigma$

# Equivocability

Real $\bar{B} = \begin{pmatrix} B \\ rB + e_B \end{pmatrix}$ $2'.\ R \leftarrow \mathcal{D}_\sigma^{m\times\ell} | \bar{B}R = \mathrm{ct}$ $1'.\ \mathrm{ct} = \mathrm{Regev.Enc}(0, \bar{B}, R)$




Ideal $\bar{B} \leftarrow \$$ $2'.\ R \leftarrow \mathcal{D}_\sigma^{m\times\ell} | \bar{B}R = \mathrm{ct}$ $1'.\ \mathrm{ct} = *$ (arbitrary)

The ideal world can be efficiently realized by sampling random public key $\bar{B}$ with a trapdoor. [GPV08,MP12]

# Circular Security with Random Opening (CRO)

Regev PK

$\bar{B}$

$= \begin{pmatrix} B \\ rB + e_B \end{pmatrix}$

(Circular)-LWE samples

Samp

Special eval $F$

$ct$

$\approx$

Random PK

$\bar{B} \leftarrow \$$

Random samples

Samp $\leftarrow \$$

Special eval $F$

$ct$

Hint $= R \leftarrow \mathcal{D}_\sigma^{m\times\ell} | \bar{B}R = \mathbf{ct}$

Feature: $ct \approx_s \mathrm{RegE}_{\mathrm{pk}}(0^\ell, \mathcal{D}_\sigma^{m\times\ell})$

$R \approx_s \mathcal{D}_\sigma^{m\times\ell}$

$\Rightarrow$

$ct \approx_c \$$

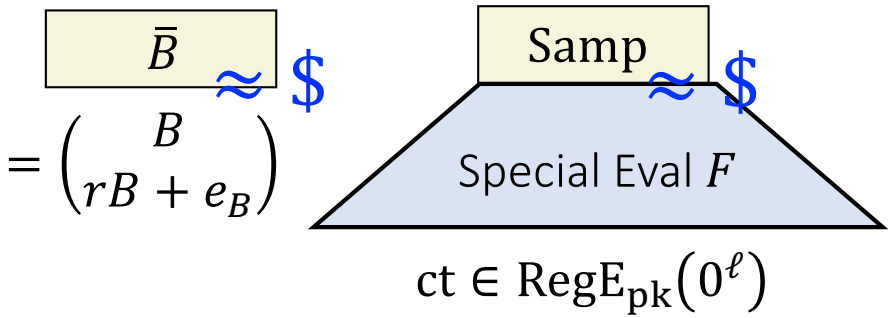
$R \approx_c \mathcal{D}_\sigma^{m\times\ell}$

**Theorem** [HJL25] CRO with specific $Samp$ and $F$ ➔ iO

# CRO

Regev PK

(Circular)-LWE samples




$\mathrm{Hint} = R \leftarrow \mathcal{D}_{\sigma}^{m \times \ell} | \bar{B}R = \mathrm{ct}$

Feature: $R \approx_s \mathcal{D}_{\sigma}^{m \times \ell}$ in real

$R \approx_c \mathcal{D}_{\sigma}^{m \times \ell}$ in ideal

# New Target

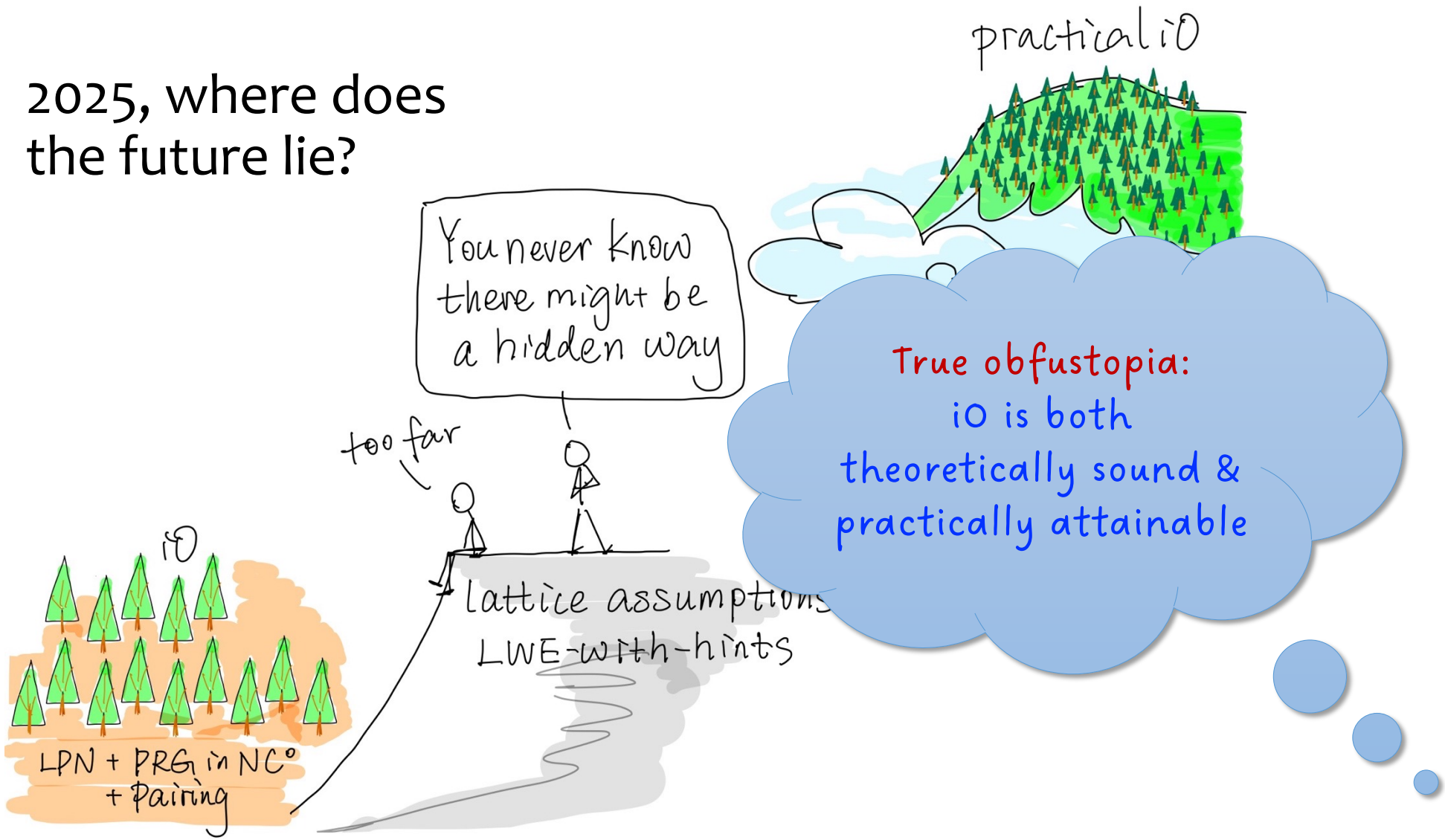
Hard to find attack on LWE components, by circular security

No attack on hint, since it is random

No attack by trivial combination , since $\bar{B}R$ is known as $F(Samp)$

Non-trivial ways of combining LWE & opening?

# 2025, where does the future lie?



Theoretical Practical


ABE FHE MPC PIR SNARK signature

"Minimal" assumptions for iO?

*Less number of assumptions?*

*Remove PRG in $NC^0$?*

*Polynomial hardness suffice?*

More efficient constructions?

*Efficient FE/xiO-to-iO transformation?*

Post-quantum Security?

*iO from LWE or not?*

## Practical iO

~~ambitious or naïve?~~

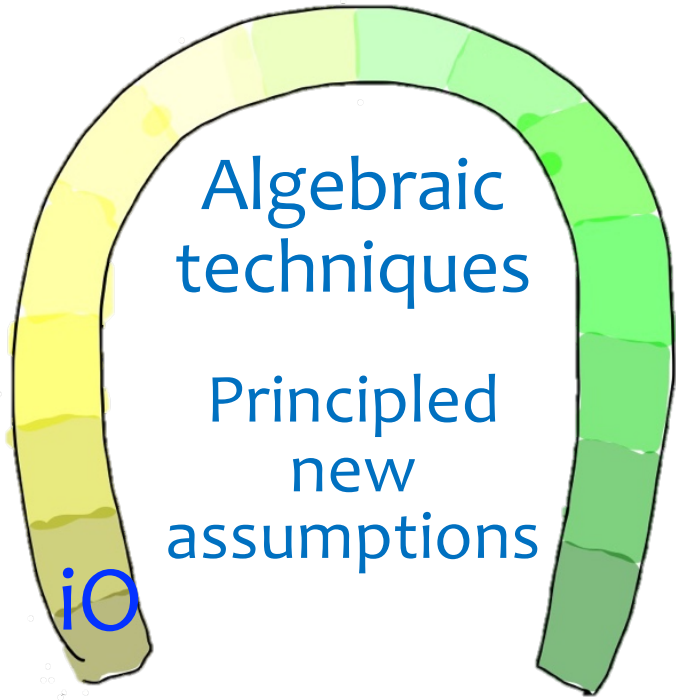
1. A worthy subject to study!
2. Great things always come out of ambitious pursuits.
3. Efficiency is a work of progress

# Opportunity of our time

Direct algebraic constructions

Close to direct algebraic: xiO, FE

Bounty: Efficient xiO/FE to iO




Theoretical Practical

# Thank you!