Recent Advances on Foundations of Program Obfuscation

Huijia (Rachel) Lin
UW

Recent Advances

Based on works [Agr18] [AJS18] **[LM18]**

+ follow-ups [JLMS19] [JLS19]

Shweta Agarwal

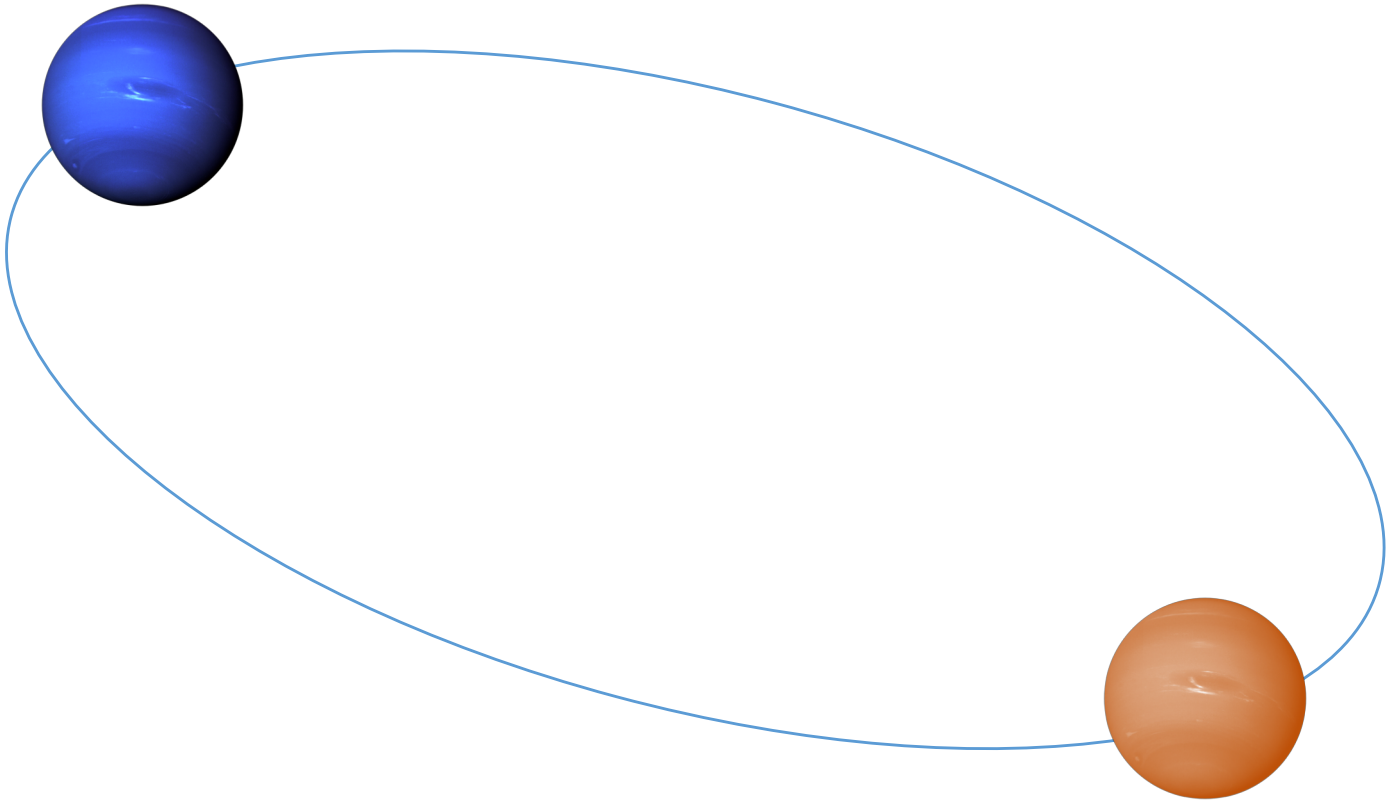
Prabhanjan Ananth

Aayush Jain

Christian Matt

Amit Sahai

Program Obfuscation



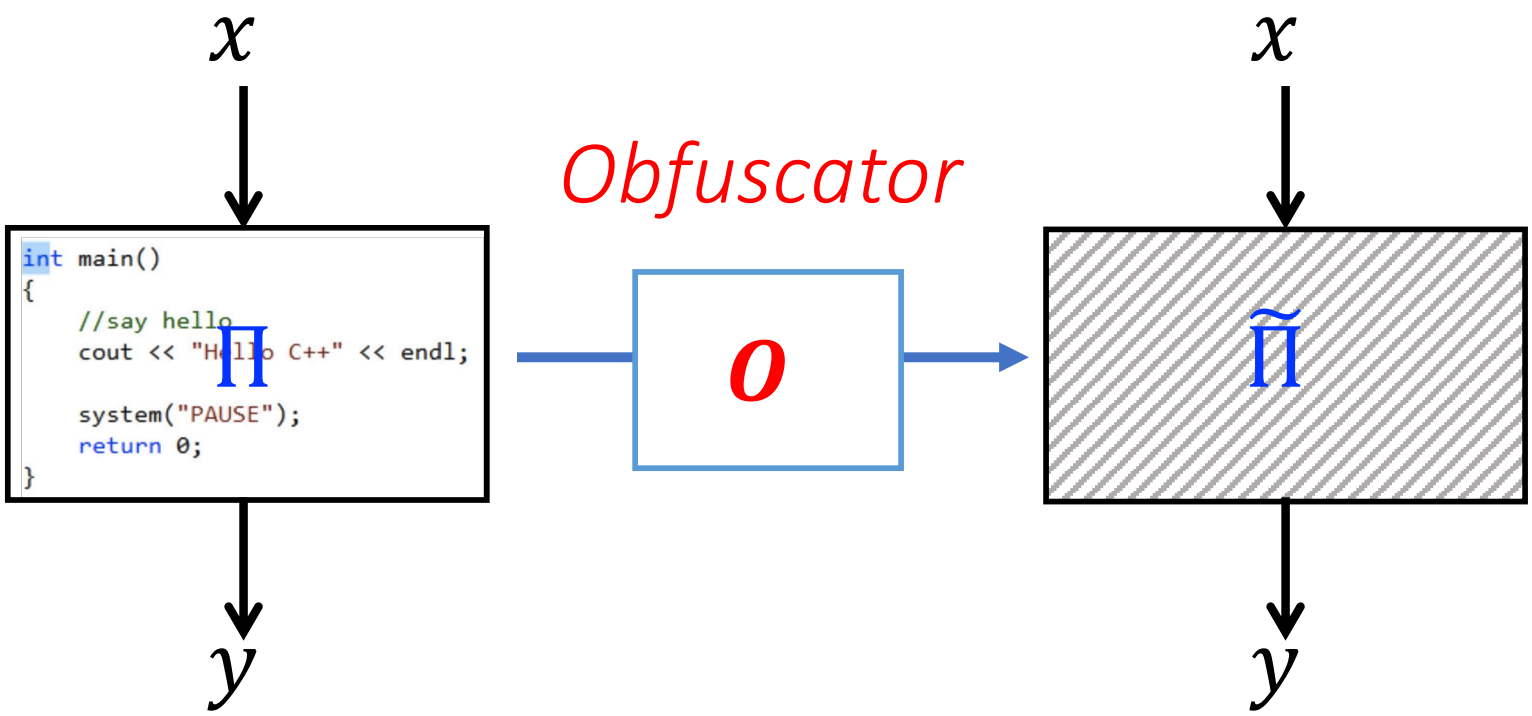
Simple and Weak

Pseudo Randomness Generators

+ LWE + Bilinear Maps

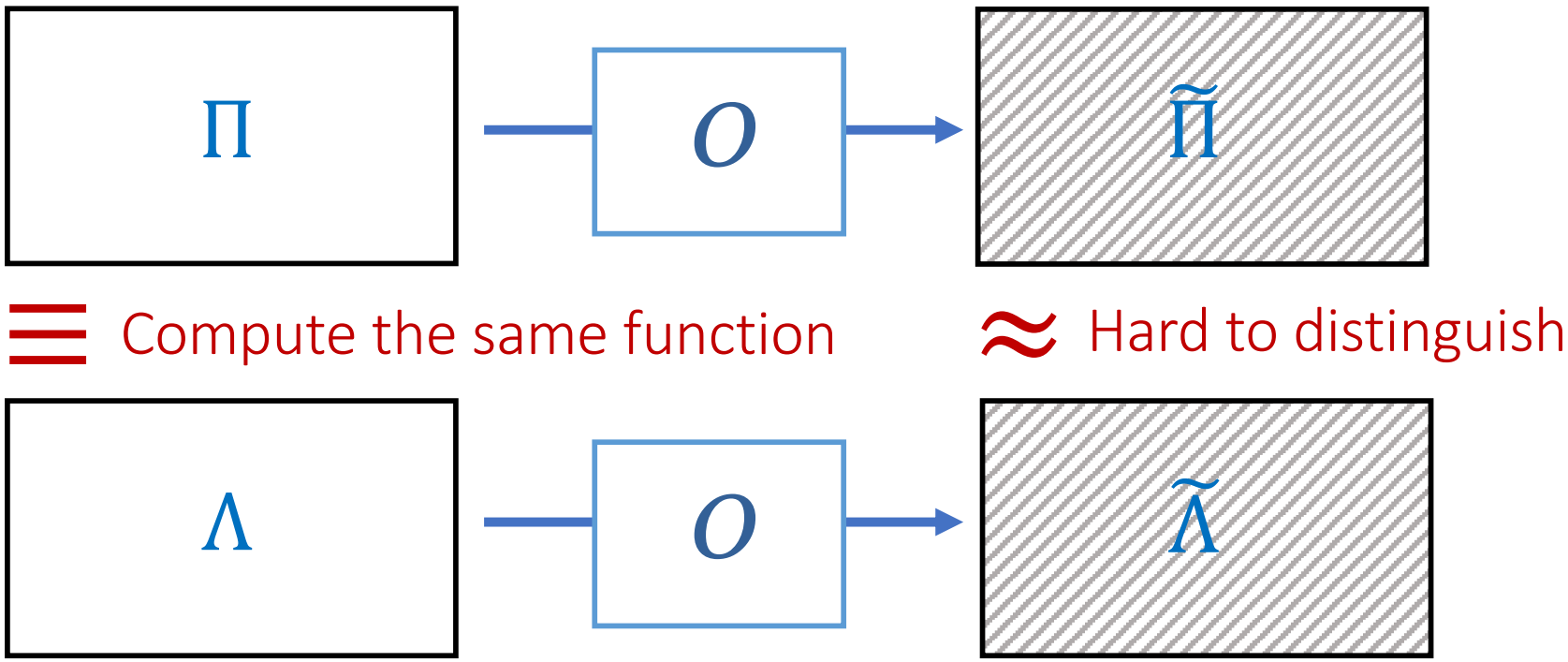
Program Obfuscation

Goal: Efficiently transform a program into one that *is functionally equivalent & unintelligible*



Mildly Blow-up in Size

Indistinguishability Obfuscation (IO) [BGIRSVY01]



Hide implementation difference

No general impossibility

Classical Crypto

Short signature

Trapdoor permutation

Public key encryption

Identity-Based Encryption

Attribute-Based Encryption

Fully Homomorphic Encryption

Multiparty Computation

(Non-Interactive) Zero-Knowledge

Powerful Abstraction

Correlation Intractable Hash from LWE

Two-Round MPC from 2-rnd OT

10 +

minimal crypto
(e.g., OWFs)

New Crypto

Functional Encryption

Witness Encryption

(Doubly) Deniable Encryption

Hardness of Finding Nash

Correlation Intractable Hash

Secret Sharing for NP

Multi-Party Non-Interactive Key Exchange

OWF with poly hard core bits

Succinct Garbled RAM

Two-Round MPC

Constant Round Concurrent ZK

……

IO ?

IO from M-linear maps

- Ultimate Prize:
  IO from Bilinear Maps
- Minimizing the degree M

IO from new math

e.g. tensor products [GJ18]

IO for limited class of functions
from standard assumptions

e.g., VBB for compute-&-compare from LWE [WZ17,GKW17]

First Generation IO

[GGHRSW13,BR14, BGKPS14, PST14, GLSW14, AGIS14, Zim15, AB15
GMMSSZ16, DGGMM16]

M-linear map for poly M

[BS02,Rot13,GGH13]

IO resisting Zeroizing Attacks

[GMMSSZ16, DGGMM16
CVW18]

Direct Attacks

[MSZ16,ADGM17,CGH17]

More Attacks

[Pellet-Mary18,CHKL18]

Candidates

[GGH13,CLT13,
GGH15,CLT15]

Zeroizing Attacks

[GGH13,CHL15,
GHMS14,BWZ14,
CGH15]

Other types of "simple" PRG?

Second Generation IO

[AJ15, BV15, LPST16, LPST16b, L16, LV16, AS17, L17, LT17]

3-linear map
+ "simple" PRG, block-locality 3
+ LWE

2-linear map

"super simple" PRG, block Locality 2, Impossible * [LV17,BBKK17]

*except for tiny expansion window ($n2^{b(1+\epsilon)}$)

ΔRG: Perturbation Resilient Generators [AJS18]

PFG: Pseudo Flawed-smudging Generators [LM18]

Third Generation IO

[Agr18, AJS18, LM18, JLMS19, JLS19]

2-linear map

+ “simple” and “weak” PRG

+ LWE

ΔRG: Perturbation Resilient Generators [AJS18]

PFG: Pseudo Flawed-smudging Generators [LM18]

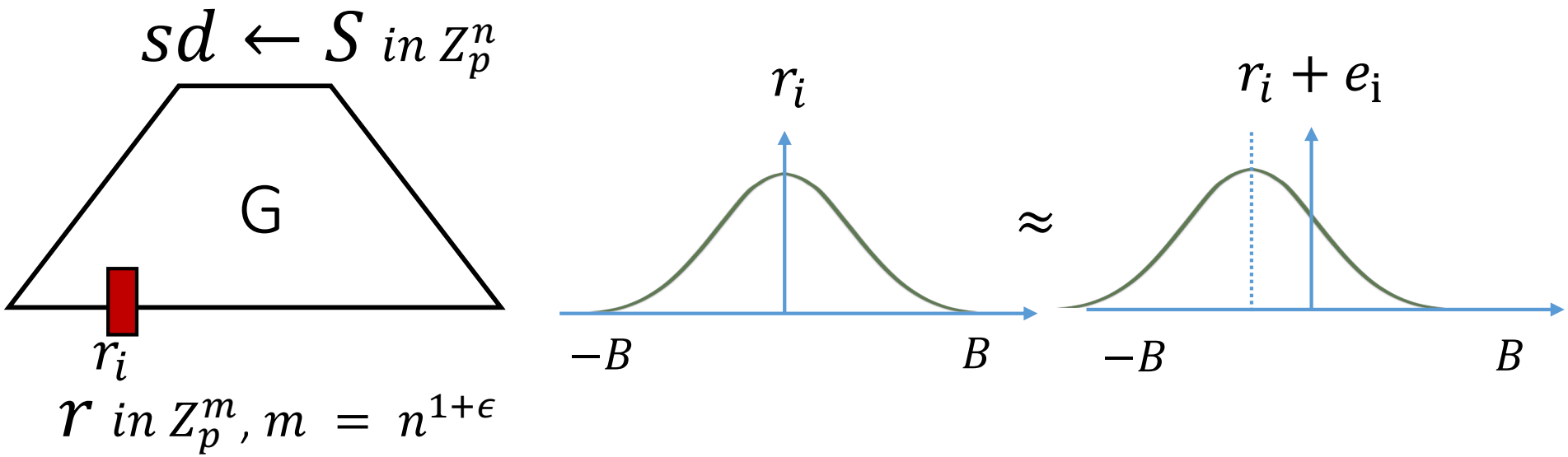
Flawed Intuition

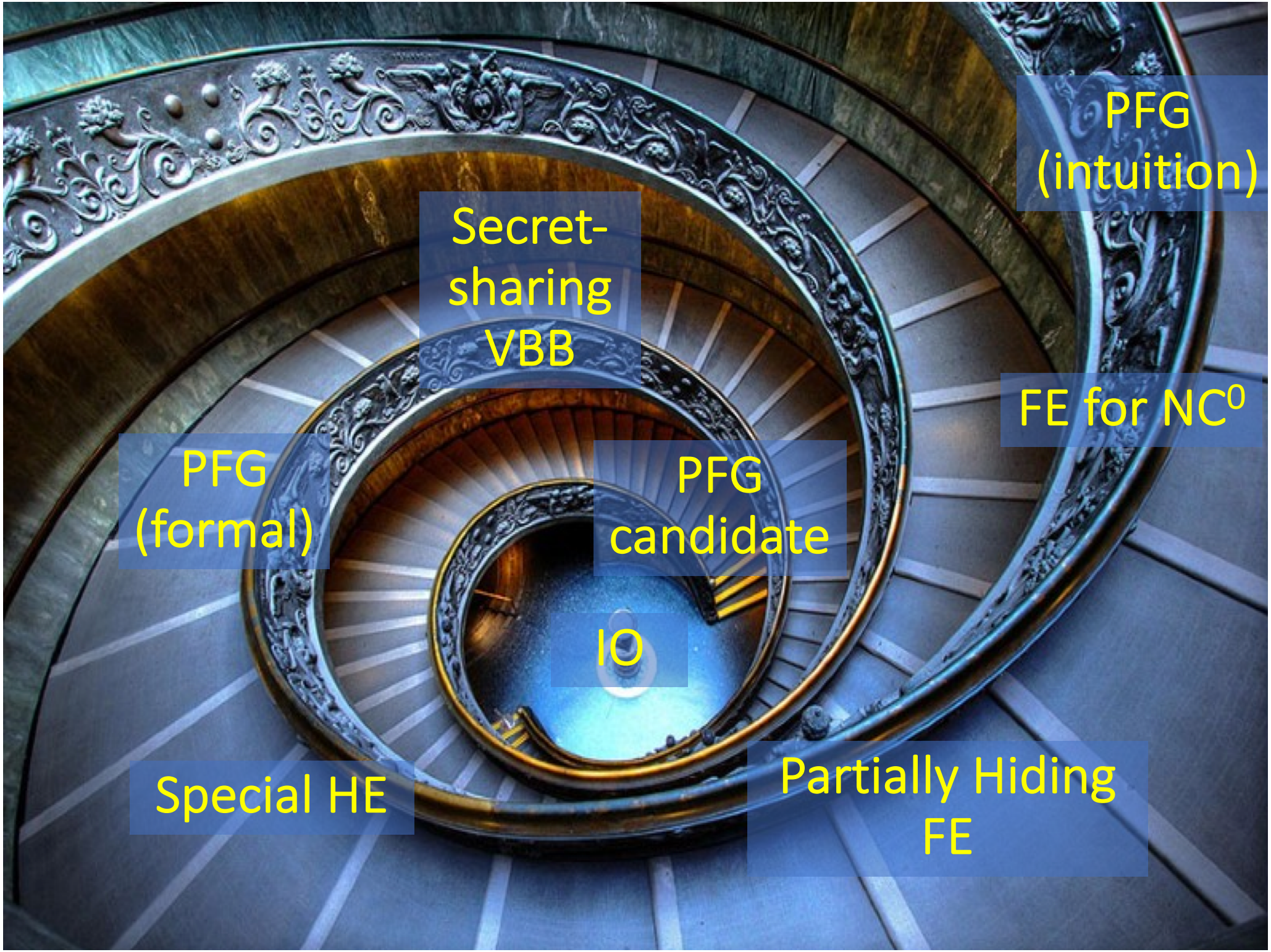
"Simple" Deg 2 poly in Z_p with **small outputs**

(small = poly, large = super-poly)

"Weak" pseudo-randomness

Outputs smudge/hide even **smaller** LWE noises [also in Agr18]

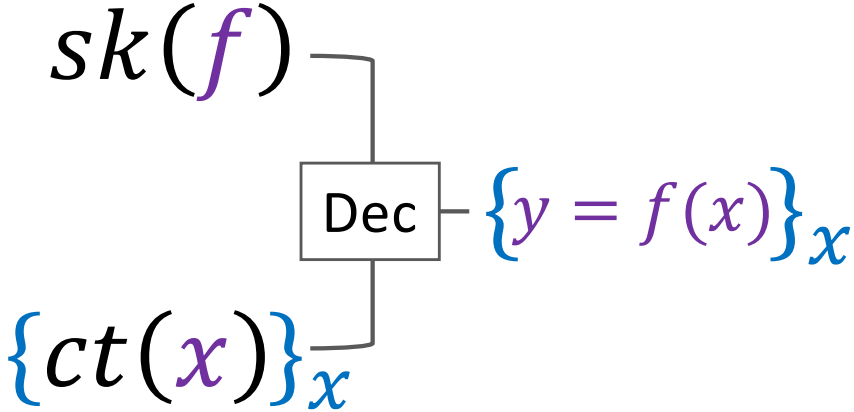



PFG
(intuition)
Secret-
sharing
VBB
FE for NC^0
PFG
(formal)
PFG
candidate
IO
Special HE
Partially Hiding
FE

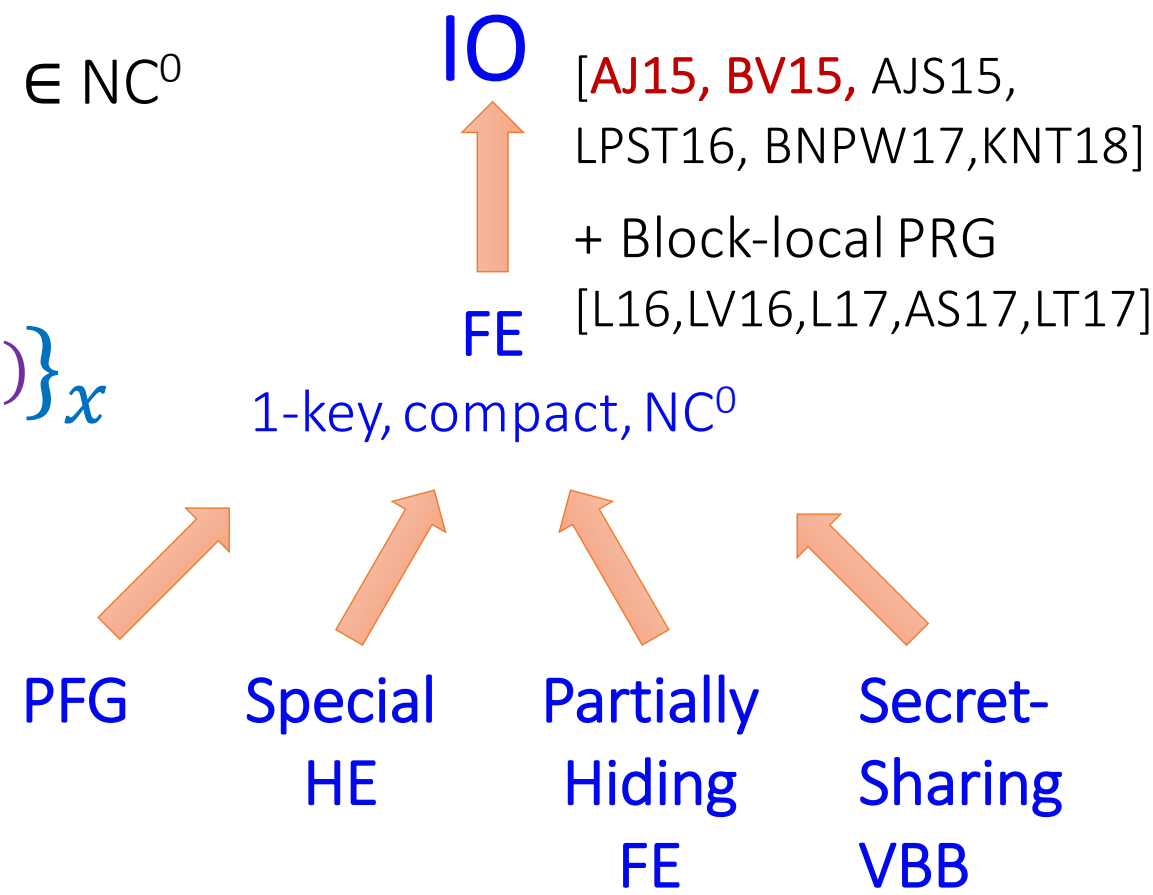
Starting Point

SKFE for NC^0

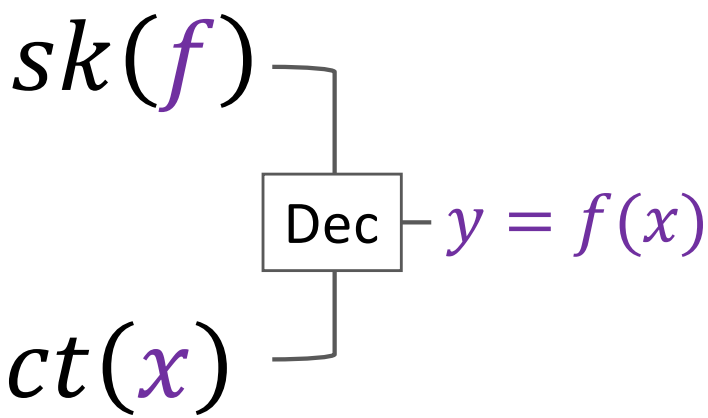
single f, long-output, $\in NC^0$

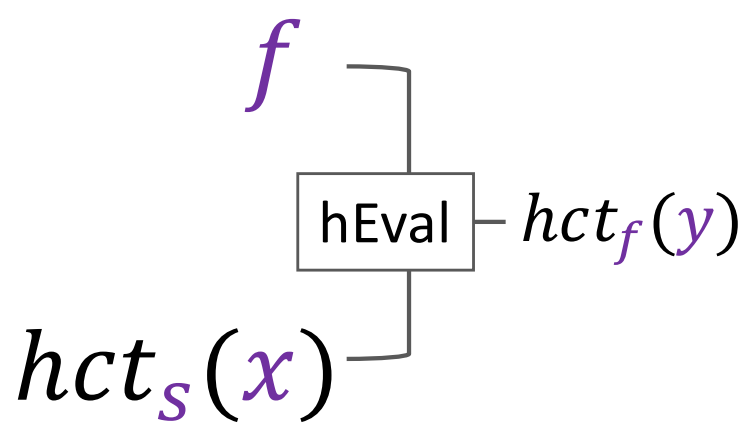


- Correctness: Reveal $\{y\}_x$
- Privacy: Reveal only $\{y\}_x$
- Compact: $|ct(x)| = \mathrm{poly}(|x|)|f|^{1-\epsilon}$



FE for NC^0 vs Homomorphic Encryption





- Privacy: Reveal **only** y
- Privacy: Reveal nothing

Need to decrypt, privately

Basic Approach

Bootstrapping via HE

FE for NC^0 Simple $\overline{\mathrm{FE}}$ HE [GVW12,GKP+13,GVW15, AR17,Agr18]

Ideally deg 2 FE [BCFG17,Lin17]

$sk(f)$ $\overline{sk}(h?)$ f

$\overline{\mathrm{Dec}}$ y hEval $hct_f(y)$

$ct(x)$ $\overline{ct}(?,?)$ $hct_s(x)$

- Privacy: Reveal only y
- Simplicity: $f \succ h$

Use FE to decrypt

First Attempt

[GVW12]

FE for NC^0 Simple $\overline{\mathrm{FE}}$

$sk(f)$ $\overline{sk}(h)$

$\boldsymbol{h(hct, s)}$:

1. $hct_f \leftarrow \mathrm{hEval}(f, hct)$
2. $y = \mathrm{hDec}(s, hct_f)$
   $= \mathrm{LDec}(s, hct_f)$ ~~mod 2~~

$ct(x)$ $\overline{ct}(hct, s)$ $hct_s(x)$

- Privacy: Reveal only y
- Simplicity: $f \succ h$

  $\mathrm{hDec} \in \mathrm{NC}^1$

  $\mathrm{hEval} \succ f$

Half Decrypt for Simplicity [GVW15]

FE for NC^0 Simple $\overline{\mathbf{FE}}$

$sk(f)$ $\overline{sk}(h)$

$\boldsymbol{h(hct, s)}$:

1. $hct_f \leftarrow \mathrm{hEval}(f, hct)$
2. $y + 2e = \mathrm{LDec}(s, hct_f)$

$ct(x)$ $\overline{ct}(hct, s)$ $hct_s(x)$

- Privacy: Reveal only $\mathrm{eve}(f, s, x)$ ✗
- Simplicity: $f \succ h$

$\mathrm{LDec} \in \deg 2$

$\mathrm{hEval} \succ f$

PFG for Privacy

[AJS18, Agr18, LM18]

FE for NC^0 Simple $\overline{\mathrm{FE}}$

$sk(f)$ $\overline{sk}(h)$

$\boldsymbol{h(hct, s, sd)}$:

1. $hct_f \leftarrow \mathrm{hEval}(f, hct)$
2. $y + 2e = \mathrm{LDec}(s, hct_f)$
3. $y + 2e + 2\mathrm{PFG}(sd)$

$ct(x)$ $\overline{ct}(hct, s, sd)$ $hct_s(x)$

Flawed

- Privacy: Reveal $\mathrm{PFG}(sd)$ hides e
- Simplicity: $f \succ h$

$\mathrm{LDec} \in \deg 2$

$\mathrm{hEval} \succ f$

Simplicity, Revisited

FE for NC^0 Simple $\overline{\mathrm{FE}}$

$sk(f)$ $\overline{sk}(h)$

$\boldsymbol{h(hct, s, sd)}$:

1. $hct_f \leftarrow \mathrm{hEval}(f, hct)$
2. $y + 2e = \mathrm{LDec}(s, hct)$
3. $y + 2e + 2\mathrm{PFG}(sd)$

$ct(x)$ $\overline{ct}(hct, s, sd)$ $hct_s(x)$

- Privacy: $e + \mathrm{PFG}(sd)$ hides e
- Simplicity: $f \succ h$

  $\mathrm{LDec} \in \deg 2$

  $\mathrm{hEval} \succ f$

Use Partially hiding FE (PHFE) *or* Special HE *Shweta's Talk!*

[AJS18] [AR17,Agr18,LM18,JLS19]

PHFE for Simplicity

[GVW12,GVW15,AJS18,LM18,JLS19]

	Deg-(O(1), 2)
FE for NC^0	$\overline{\text{PHFE}}$
$sk(f)$	$\overline{sk}(h)$
$ct(x)$	$\overline{ct}(hct, s, sd)\ hct_s(x)$

$h(hct, s, sd)$: **deg O(1), Public**

1. $hct_f \leftarrow \text{hEval}(f, hct)$
2. $y + 2e = \text{LDec}(s, hct)$
3. $y + 2e + 2\text{PFG}(sd)$

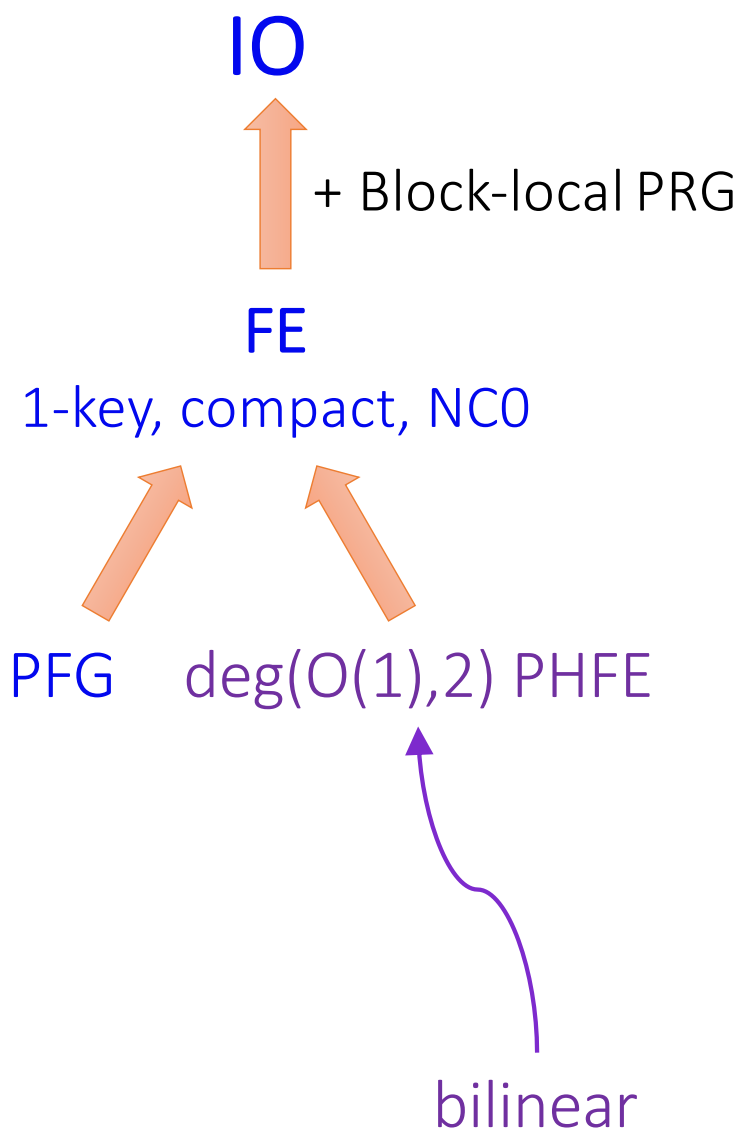
deg 2, Private

- Public input $A = hct$
- Private Input $B = (s, sd)$

PHFE: FE for

$$h(A, B) = \text{priv}(\text{pub}(\text{A}), \text{B})$$

Reveals output $y + 2e + 2\text{PFG}(sd)$ and public input $A = hct$



Open: FE for large outputs

Bilinear-based (PH)FE computes g_T^{output}

$\Rightarrow$ $\text{output} = y + 2e + 2\text{PFG}(sd)$ must be small to be extracted

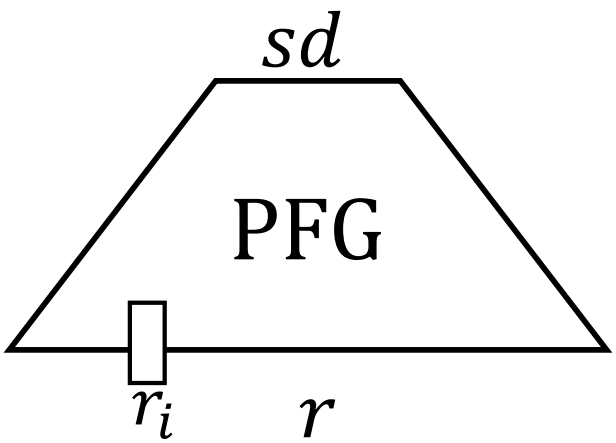
Weaken PFG

PFG:

$e + \text{PFG}(sd)$ hides e

$\Rightarrow$ $\text{PFG}(sd)$ must be large

Small $\mathbf{PFG}(\boldsymbol{sd})$ CANNOT smudge $\boldsymbol{e}$ completely

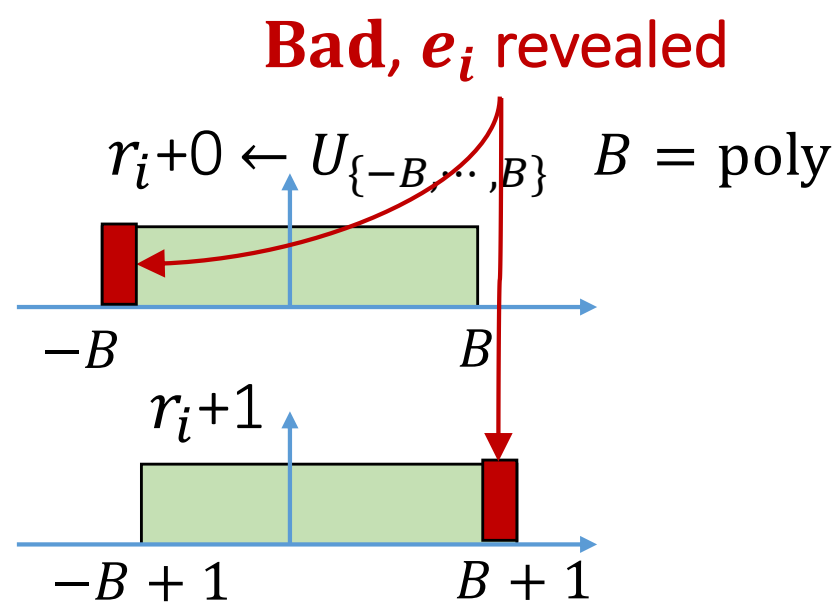


$(r + e, e) \not\approx (r + e, e')$

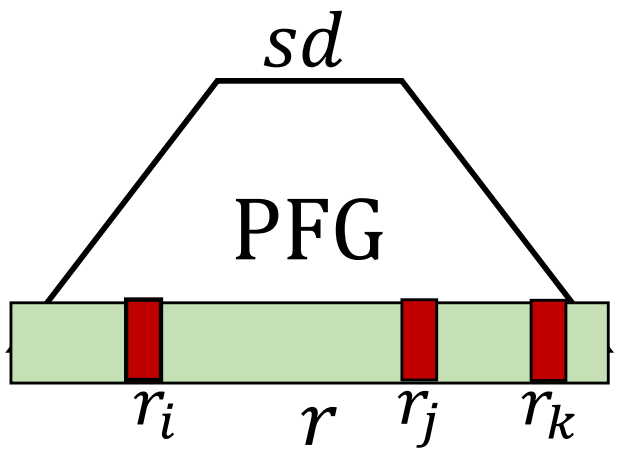
$\forall\, r_i \leftarrow$ poly-bounded distribution

$r_i \not\approx r_i{+}1$

E.g. $e_i \in \{0,1\}$



Best Possible: Small $\mathbf{PFG}(\boldsymbol{sd})$ smudges $\boldsymbol{e}$ partially



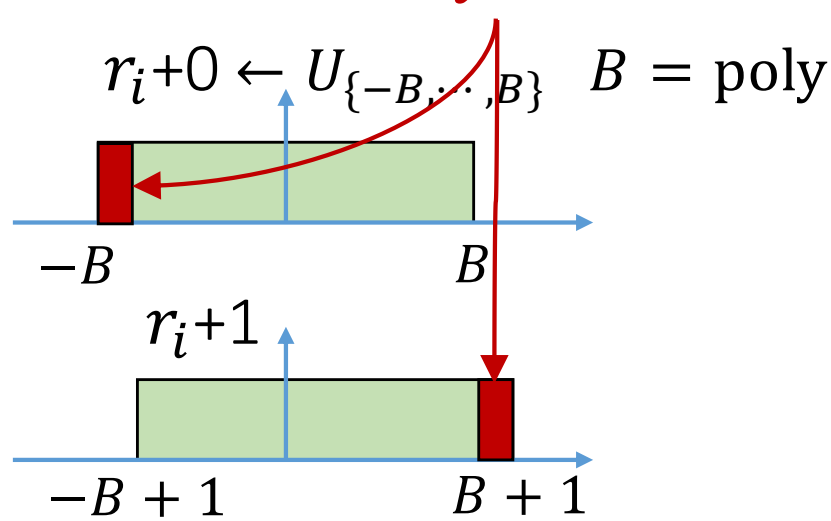
I, the set of bad coordinates

E.g. r_i independent

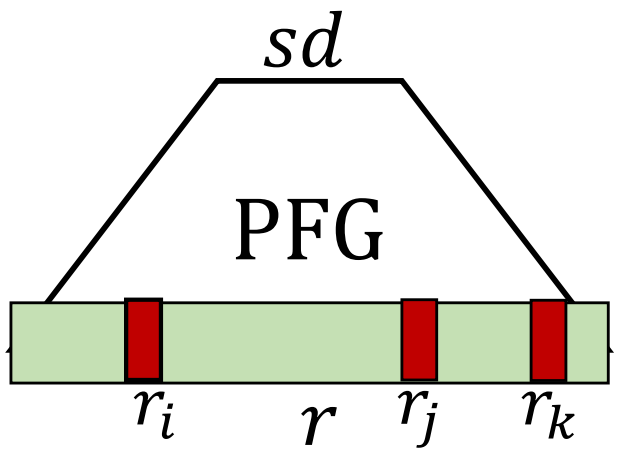
Given $e + r$, $e_{\bar{I}}$ hidden
e_I revealed

Hope: $\neg$**Bad**, $\boldsymbol{e_i}$ hidden

Bad, $\boldsymbol{e_i}$ revealed



PFG



I, the set of bad coordinates

Degree 2 over Z_p

Small output r (poly-bounded)

Weak pseudo-randomness

$r \approx \gamma \leftarrow \Gamma$, flawed smudging

Γ is flawed-smudging: $\forall$ small $e \leftarrow E$ (poly B-bounded)

(Informal) $\gamma + e$ hides e at *all-but-a-few* coordinates

in good case with $1/q(\lambda)$ *probability*

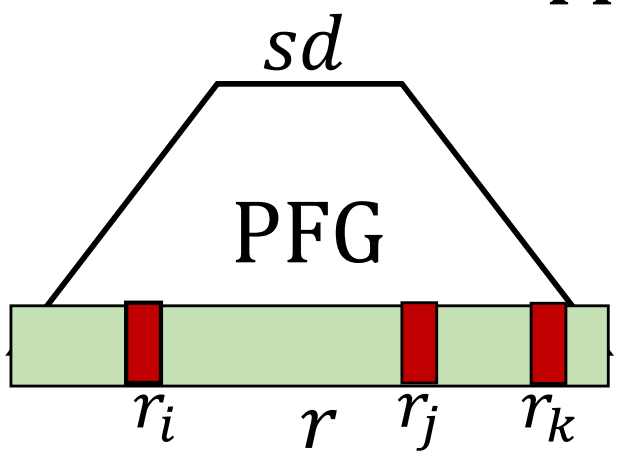
(formal) $\exists\ I$ correlated with e, γ

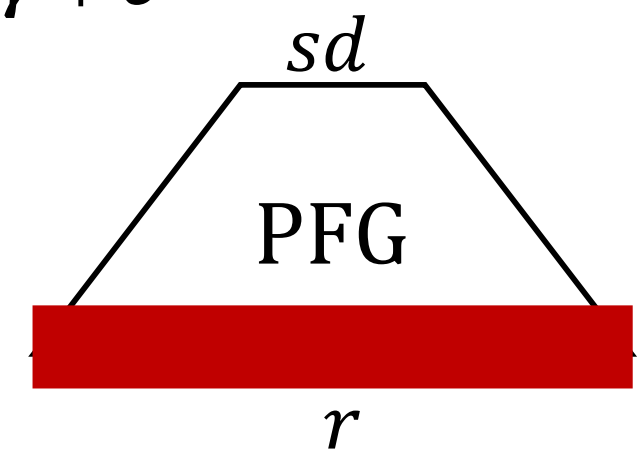
$$(e, \gamma + e, I) \cong (e', \gamma + e, I) \qquad e' \leftarrow E \mid e_I = e'_I$$

in good case with $1/q(\lambda)$ *probability*

PFG

$$\mathbf{PFG}(\boldsymbol{sd}) + \boldsymbol{e} \approx \boldsymbol{\gamma} + \boldsymbol{e}$$





I, the set of bad coordinates

Good with $1/q(\lambda)$ *probability*

$\boldsymbol{e_I}$ *revealed &* $\boldsymbol{e_{\bar{I}}}$ *hidden*

Bad with $1 - 1/q(\lambda)$ *probability*

all bets off, $\boldsymbol{e}$ *revealed*

Strong PFG, $I = \emptyset$

nothing revealed & $\boldsymbol{e}$ *hidden*

all bets off, $\boldsymbol{e}$ *revealed*

Deg-(O(1), 2)

1/q FE for NC^0 $\quad$ $\mathrm{PH}\overline{\mathrm{FE}}$

Use Strong PFG

$sk(f)$ $\quad$ $\overline{sk}(h)$

$\boldsymbol{h(hct, s, sd)}$:

1. $hct_f \leftarrow \mathrm{hEval}(f, hct)$
2. $y + 2e = \mathrm{LDec}(s, hct)$
3. $y + 2e + 2\mathrm{PFG}(sd)$

$ct(x)$ $\quad$ $\overline{ct}(hct, s, sd)$ $\; hct_s(x)$

At decryption, only $y + 2e + 2\mathrm{PFG}(sd)$ revealed

Strong PFG ➔

In good case w.p. $1/q(\lambda)$, FE secure, o.w., all bets off

Security Amplification vs Secret Sharing VBB

Bit-Fixing Secret Sharing [LM18]

$\mathrm{Share}(x) \rightarrow$ x_1 … [redacted] … x_Q

Eval Boolean g^j

Independently on shares

$\mathrm{Eval}(g^j, x_1)$ $\mathrm{Eval}(g^j, x_i)$ $\mathrm{Eval}(g^j, x_Q)$

$y^j = \mathrm{Recon}($ y_1^j … y_i^j … y_Q^j $)$

Efficiency: $|x_i| \sim |g^j|$, independent of # of computations

Security: If one input share hidden, only $\{y^j\}$ revealed

Secret Sharing VBB

Obfuscator | Server 1 | Server i | Server Q

$\text{Share}(P) \rightarrow$ P_1 … [redacted] … P_Q

$\text{Eval}(U(v^j,*), P_i)$

$\textbf{View} \approx \textbf{Sim}(\{y^j\})$

Diff from HSS [BGI14,BGI15…]
Public output reconstruction

y_1^j … y_i^j … y_Q^j

"Eval v^j"

Evaluator

$y^j = P(v^j)$

Secret Sharing VBB

Server 1 Server i Server Q

P_1 ... [redacted] ... P_Q

$\mathrm{Eval}(U(v^j,*), P_i)$

... y_i^j ... y_Q^j

Evaluator

$^j = P(v^j)$

SS-VBB ~ 2-mesg MPC w/ reusable 1st mesg

← Multikey FHE ← LWE [AJLTVW12, MW16,CM15,BP16,PS16]

← Bilinear map [BL19]

Security Amplification

FE’ $\qquad$ 1/q FE for P $\xleftarrow{\text{bootstrap}}$ 1/q FE for NC^0

Q >> q, w.h.p. some instance i is secure

$sk'(f)$: $\quad sk_1(g) \quad sk_i(g) \quad sk_Q(g)$

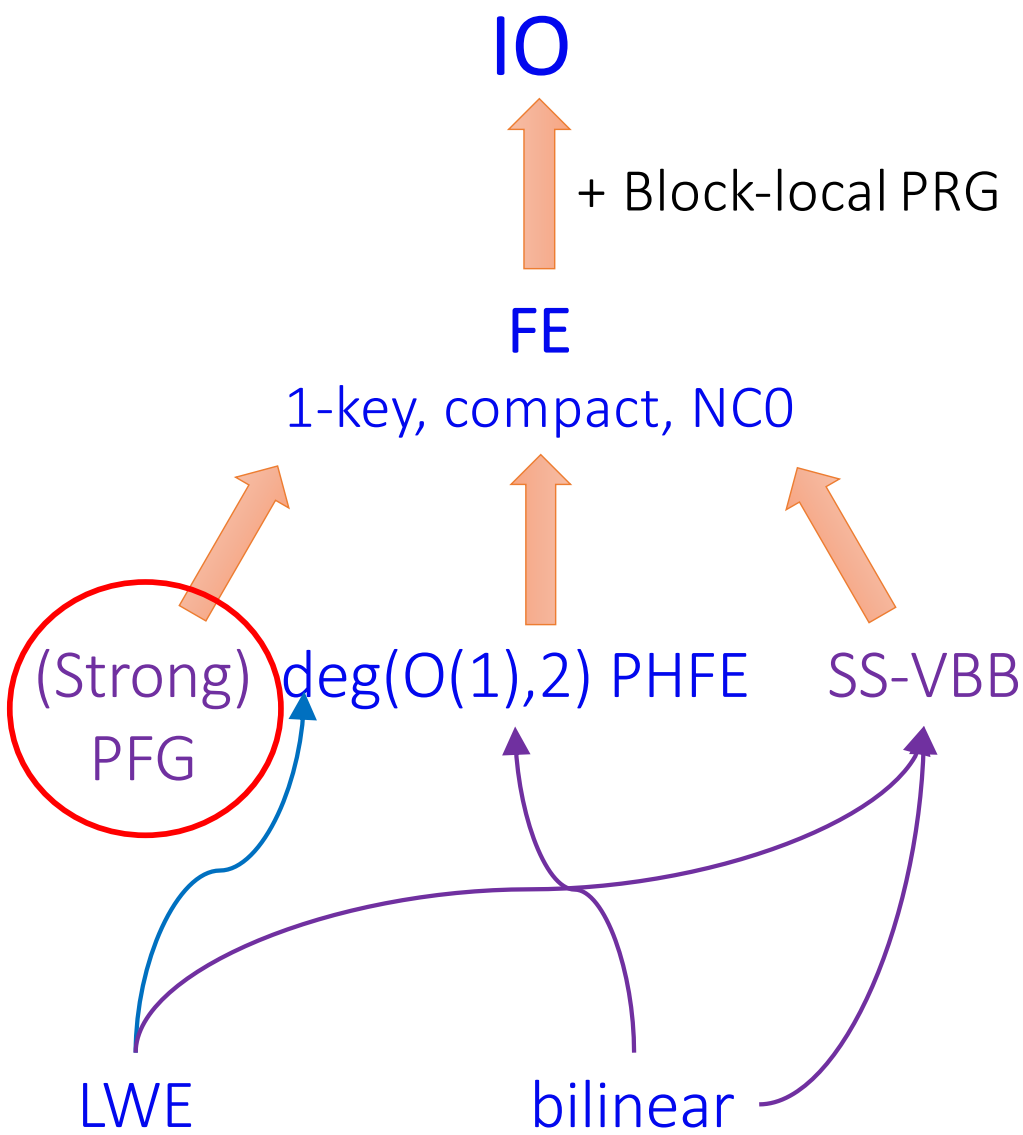
$g = \mathrm{Eval}(f, *)$

$ct'(x)$: $\quad ct_1(x_1) \quad ct_i$ [redacted] $\quad ct_Q(x_Q)$

By SS-VBB,
$\boldsymbol{x}$ hidden

$(\boldsymbol{sk_i}, \boldsymbol{ct_i})$ an independent instance

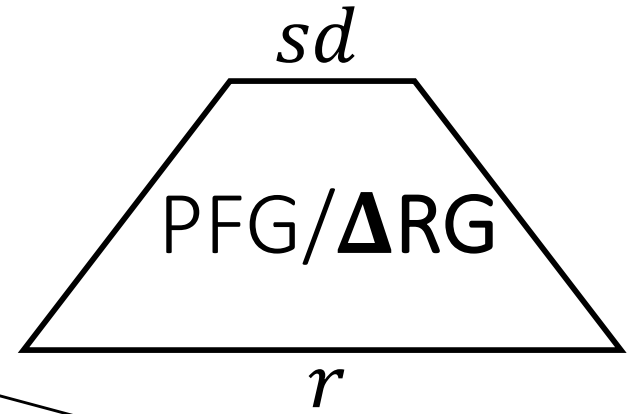
$y = \mathrm{Recon}(\ \{y_1\} \quad \{y_i\} \quad \{y_Q\}\ )$



Candidates
Comparison w/ ΔRG

Want: Candidate deg 2 poly over Z_p

w/ small flawed-smudging outputs



Attack by SOS [BHJKS18]

Random deg 2 multivariate poly

$$\boldsymbol{r_l = g_l(x, y) = \sum c_{i_1 i_2} x_{i_1} y_{i_2}}$$

~~over Z_p~~

degenerate to over Z

with small coefficients and inputs e.g., small Gaussian

Random deg 3 multivariate poly

$$\boldsymbol{r_l = g_l(x, y, z) = \sum c_{i_1 i_2 i_3} x_{i_1} y_{i_2} z_{i_3}}$$

over Z

The AJS18 Idea

Random deg-3 multivariate polynomial

$$r_l = g_l(x, y, z) = \sum c_{i_1 i_2 i_3} x_{i_1} y_{i_2} z_{i_3} \quad \text{over } Z$$

with small coefficients and inputs, e.g., small Gaussian

2-linear Map?

Hide y, z using 2-linear map, hide x as LWE noise

$$C = A, As' + x, \qquad Cs = x \qquad \text{for } s = (-s', 1)$$

Non-Degenerative

$$g(x, y, z) = g(Cs, y, z) = h(\underbrace{C, y}_{\text{Public seed}} \underbrace{\otimes s, z}_{\text{Private seed}})$$

Computable by deg (1,2)-PHFE

Hardness Assumptions [AJS18, JLMS19]

Given $\boldsymbol{C} = \boldsymbol{A}, \boldsymbol{A}\boldsymbol{s}' + \boldsymbol{x}, \quad \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) + \boldsymbol{e}$ hides $\boldsymbol{e}$ partially

1. $\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) + \boldsymbol{e}$ hides $\boldsymbol{e}$ partially

2. LWE Leakage Assumption

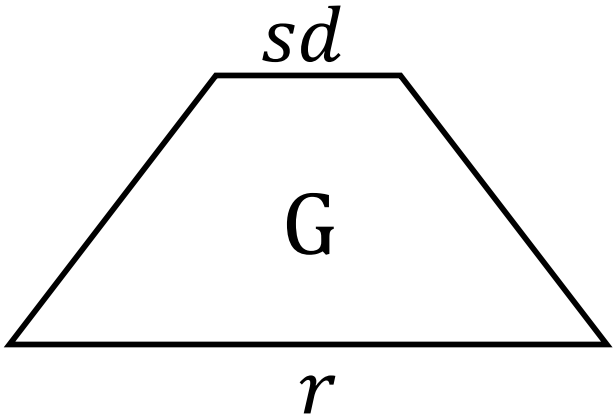
$$\boldsymbol{C} = \boldsymbol{A}, \boldsymbol{A}\boldsymbol{s}' + \boldsymbol{x}, \quad \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$$

$$\approx$$

$$\boldsymbol{C} = \boldsymbol{A}, \boldsymbol{A}\boldsymbol{s}' + \boldsymbol{x}', \quad \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$$

Naturally Generalize to Constant Degree g

Strong PFG v.s. ΔRG



Degree 2 over Z_p

r small

r smudges LWE noises partially

Strong PFG

$$\boldsymbol{r} \approx \boldsymbol{\gamma} \leftarrow \boldsymbol{\Gamma}$$

$$(\boldsymbol{e}, \boldsymbol{e} + \boldsymbol{\gamma}) \cong (\boldsymbol{e}', \boldsymbol{e} + \boldsymbol{\gamma})$$

where $\boldsymbol{e}' \leftarrow \boldsymbol{E}$

with probability 1/poly

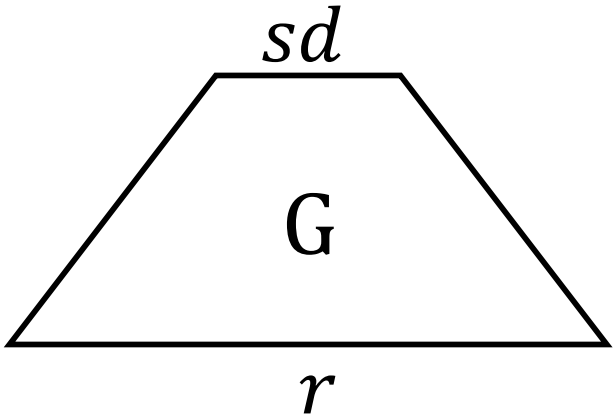
ΔRG

$$(\boldsymbol{e}, \boldsymbol{e} + \boldsymbol{r}) \approx_{\boldsymbol{Advt}} (\boldsymbol{e}', \boldsymbol{e} + \boldsymbol{r})$$

where $\boldsymbol{e}' \leftarrow \boldsymbol{E}$

advantage $Advt$ < 1-1/poly

PFG v.s. ΔRG



Degree 2 over Z_p

r small

r smudges LWE noises partially

PFG

$$\boldsymbol{r} \approx \boldsymbol{\gamma} \leftarrow \boldsymbol{\Gamma}$$

$$(\boldsymbol{e}, \boldsymbol{e} + \boldsymbol{\gamma}, \boldsymbol{I}) \cong (\boldsymbol{e}', \boldsymbol{e} + \boldsymbol{\gamma}, \boldsymbol{I})$$

where $\boldsymbol{e}' \leftarrow \boldsymbol{E} |\ \boldsymbol{e}'_{\boldsymbol{I}} = \boldsymbol{e}_{\boldsymbol{I}}$

with probability 1/poly

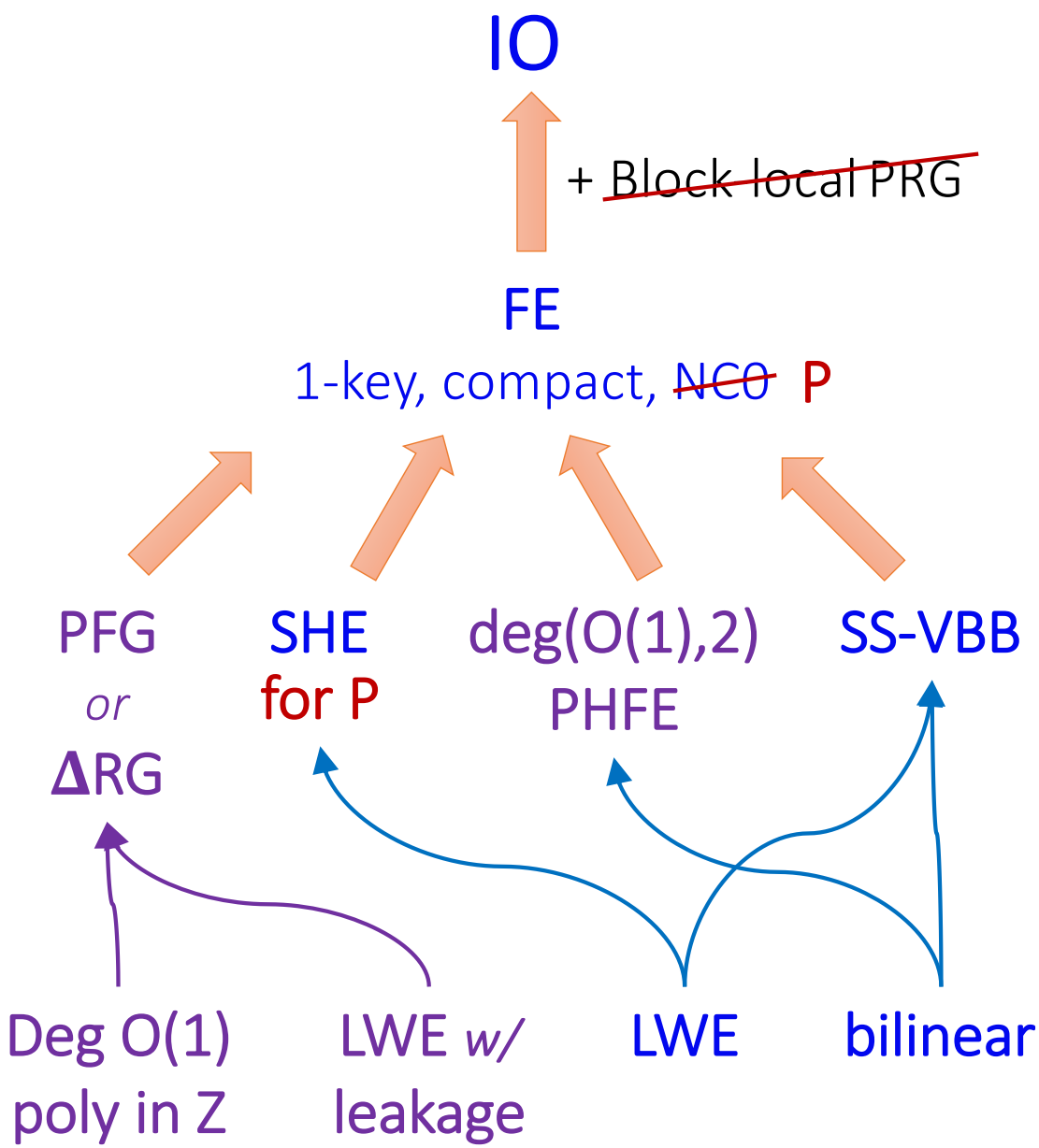
ΔRG

$$(\boldsymbol{e}, \boldsymbol{e} + \boldsymbol{r}) \approx_{\boldsymbol{Adv}} (\boldsymbol{e}', \boldsymbol{e} + \boldsymbol{r})$$

where $\boldsymbol{e}' \leftarrow \boldsymbol{E}$

advantage Adv < 1-1/poly

Different Security Amplification



PHFE for

- deg (1,2) [AJS18,LM18]
- deg (O(1),2) [JLMS19]
- (NC^1, deg 2) [JLS19]

SS-VBB

- from MKFHE [LM18]
- from bilinear map [BL19]

SHE for

- deg O(1) [BV12]
- NC^1 from RLWE [AR17]
- for P [JLS19] from LWE inspired by [GVW15]

Thank you!

Questions?

Answers may be obfuscated