Pseudorandom Obfuscation

And Applications

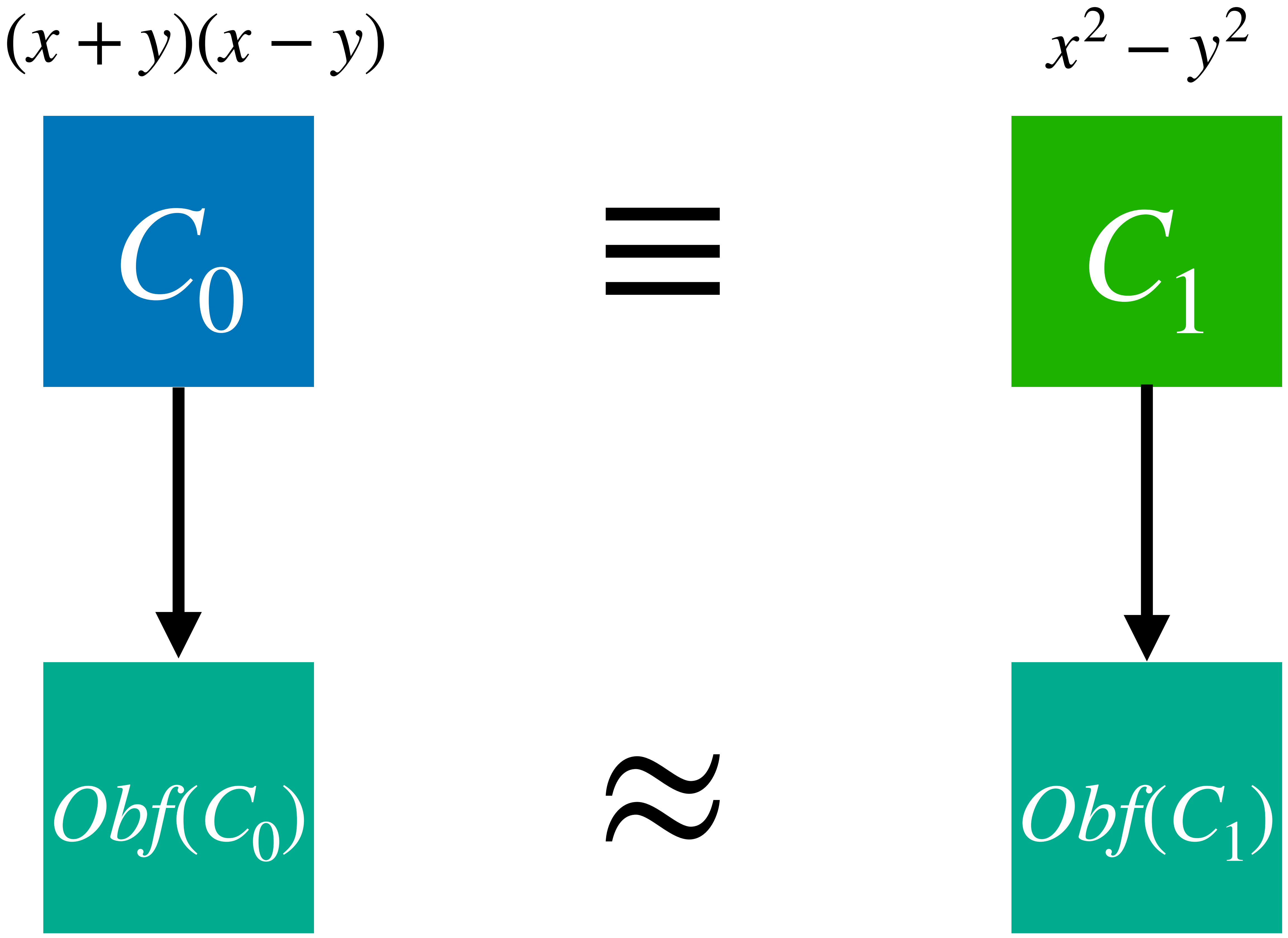
Based on joint work with Pedro Branco, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, Spencer Peters, Vinod Vaikuntanathan

Simons Obfuscation Workshop 2025

Nico Döttling, CISPA

European Research Council
Established by the European Commission

Indistinguishability Obfuscation
[BGI+01,GGH+13]



- Currently only candidates from standard assumptions follows the **[JLS20]** mould
- Critically relies on pairings for compactness (structure!)
- **[BDGM20]** paradigm: Only heuristic instantiations

iO: Swiss Army knife of Cryptography

(subexponential) iO is "crypto complete"

- iO + OWF
  - All the standard Stuff and more
  - PKE, Short Sigs, Perfect NIZKs (non-adaptive SNARGs), OT, Deniable Enc **[SW'14]**
  - FHE **[CLTV'15]**
  - WE **[GGHRSW'14]**
  - …
- iO + SSB
  - More advanced stuff
  - adaptive BE **[Zha'14]**
  - Succinct Garbling **[KLW'15]**
  - …

Or is it?
Limits of iO/VBB

- Doubly Efficient Private Information Retrieval
  - Constructions from Ring-LWE **[LMW'23]**
  - Black-box Separated from VBB **[LMW'25]**
- iO/VBB seems to hit a wall even with (seemingly) simpler tasks:
  - Pseudorandom Codes **[GGW'25, DMS'25]**
  - PKE with pseudorandom keys and ciphertexts

Pseudorandom Encryption

iO and pseudorandomness

		key		ciphertext	
SKE	K	uniform ✓	$r, PRF_K(r) \oplus m$	pseudorandom ✓	
ElGamal	g, h	uniform ✓	$g^r, h^r \cdot m$	pseudorandom under DDH ✓	
[SW'14]	$iO((r,m) \mapsto PRG(r), PRF_K(PRG(r)) \oplus m)$	**not pseudorandom** ✗	$PRG(r), PRF_K(PRG(r)) \oplus m$	pseudorandom ✓	

Even if F computes unstructured function, Obf(F) has structure

Compressing pseudorandom objects

- Pseudorandom keys and ciphertext ⇝ Equivocality (e.g. non-committing Enc)
- iO-based schemes: Structure needs to go somewhere (e.g. into CRS **[CPR17]**)
- Does obfuscation need to expose discernible structure?
- Or can it be pseudorandom?
- Advanced encryption schemes from **evasive LWE [Wee'22,Tsabary'22,VWW'22]** seemingly achieving this feat
- **Are there (achievable) notions of obfuscation which are not at odds with pseudorandomess?**

Rest of the Talk

- Pseudorandom Obfuscation
- Applications
  - FHE
  - Succinct Garbling
  - Succinct WE
- Counterexample & Alternative Notions
- Construction from evasive LWE via BDGM blueprint
- Natural Counterexamples against evasive LWE

Pseudorandom Obfuscation

Pseudorandom Obfuscation

- Can obfuscation $Obf(C)$ be unstructured?
- Can $Obf(C)$ be pseudorandom?
- $Obf(C)$ exposes $TT(C)$
  - **Minimum requirement:** C computes pseudorandom function!
  - Need to consider distributions of circuits
- How does one evaluate a random program?
- Need to fix “machine model” which interprets arbitrary strings as programs
  - $\rightarrow$ some form of universal circuit

Pseudorandom Obfuscation

Strongest Notion: Double Pseudorandomness

Precondition

$TT(C) \approx U$ given aux(C)

$$\Downarrow$$

Postcondition

$PRO(C) \approx u$ given aux(C)

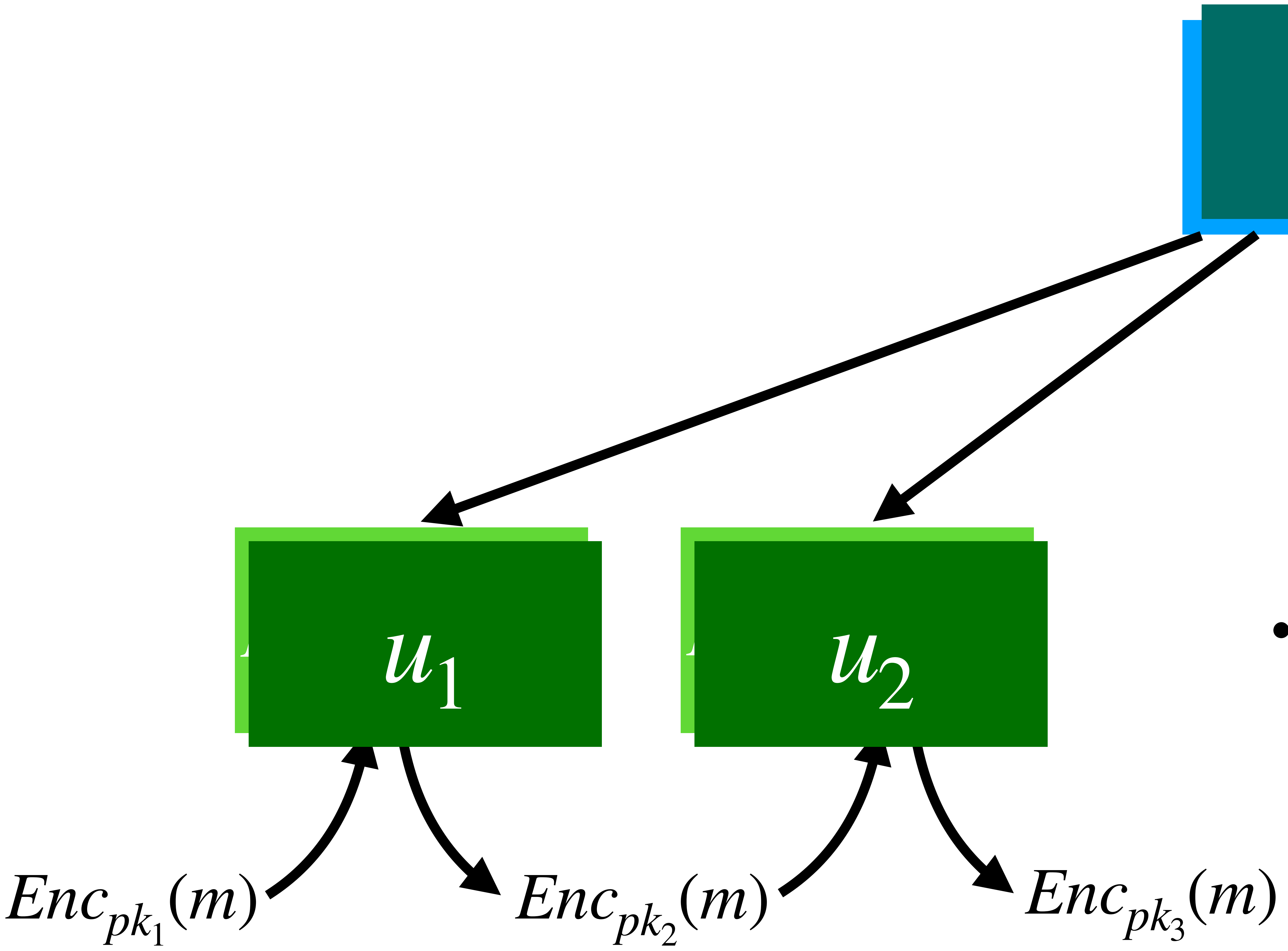
xPRO: $|PRO(C)| = |TT(C)|^{1-\epsilon}$

Applications

Fully Homomorphic Encryption

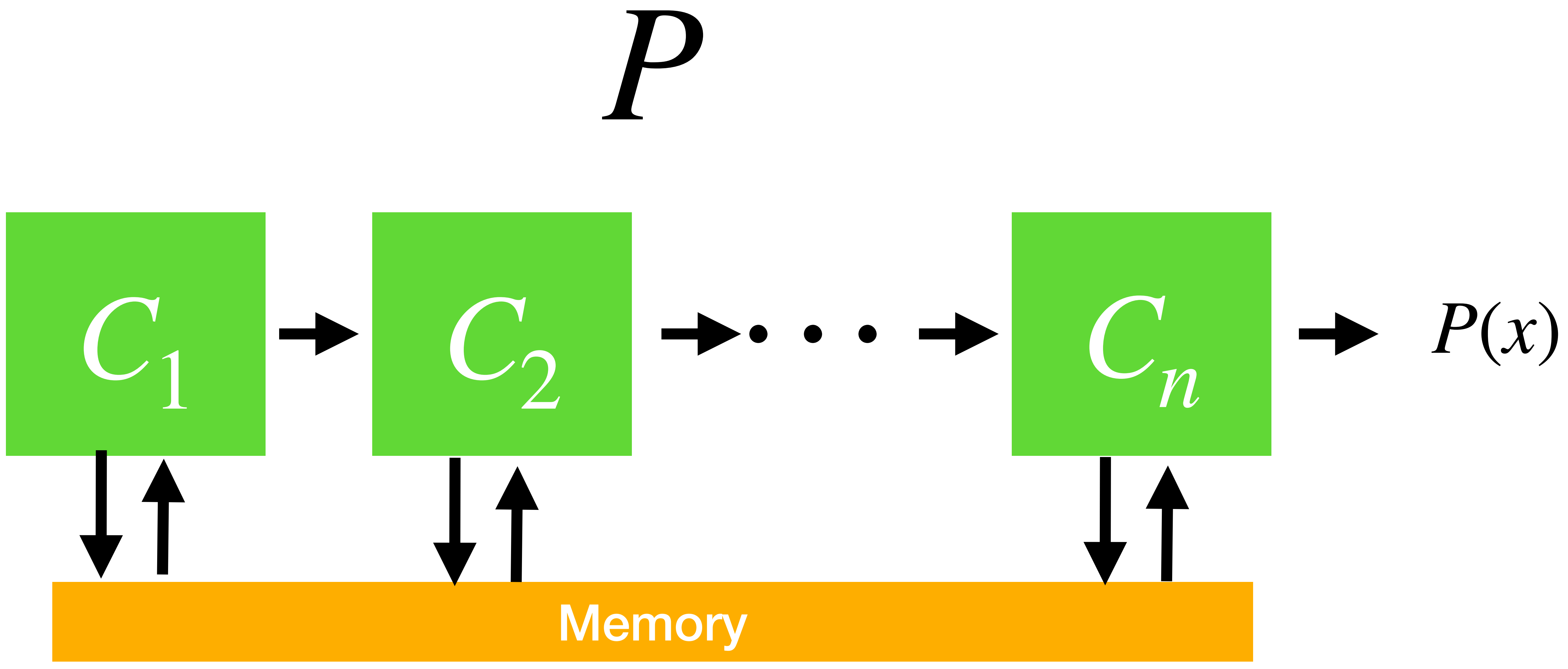
a la [CLTV'15]

- Levelled FHE: pk contains key chain
- Assume FHE with pseudorandom ciphertexts
- Long key chain: $N = 2^\lambda$
- Compute recryption keys locally



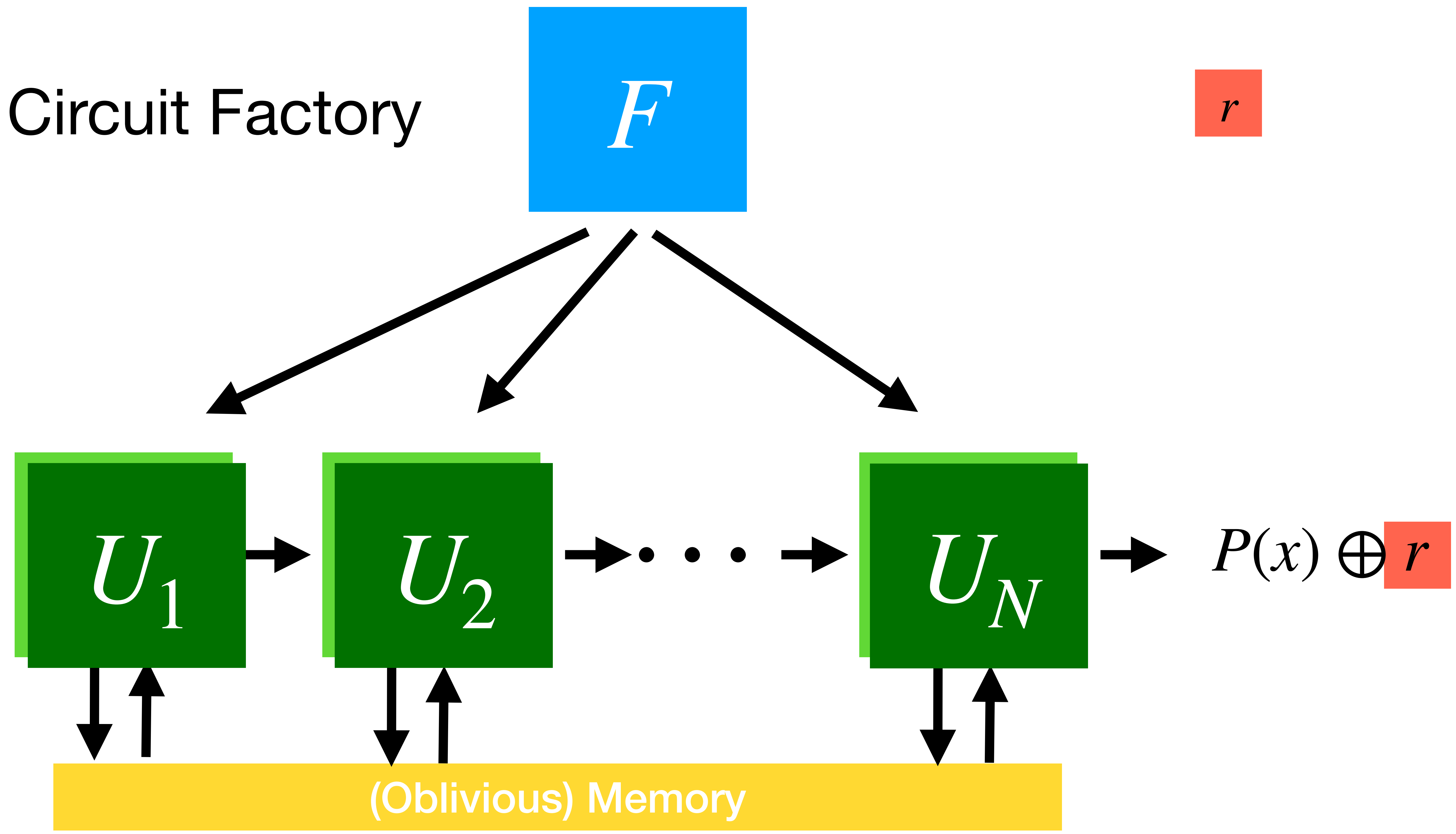
Succinct Garbling

- TM/RAM Computation via Step Circuits
- Oblivious memory access pattern

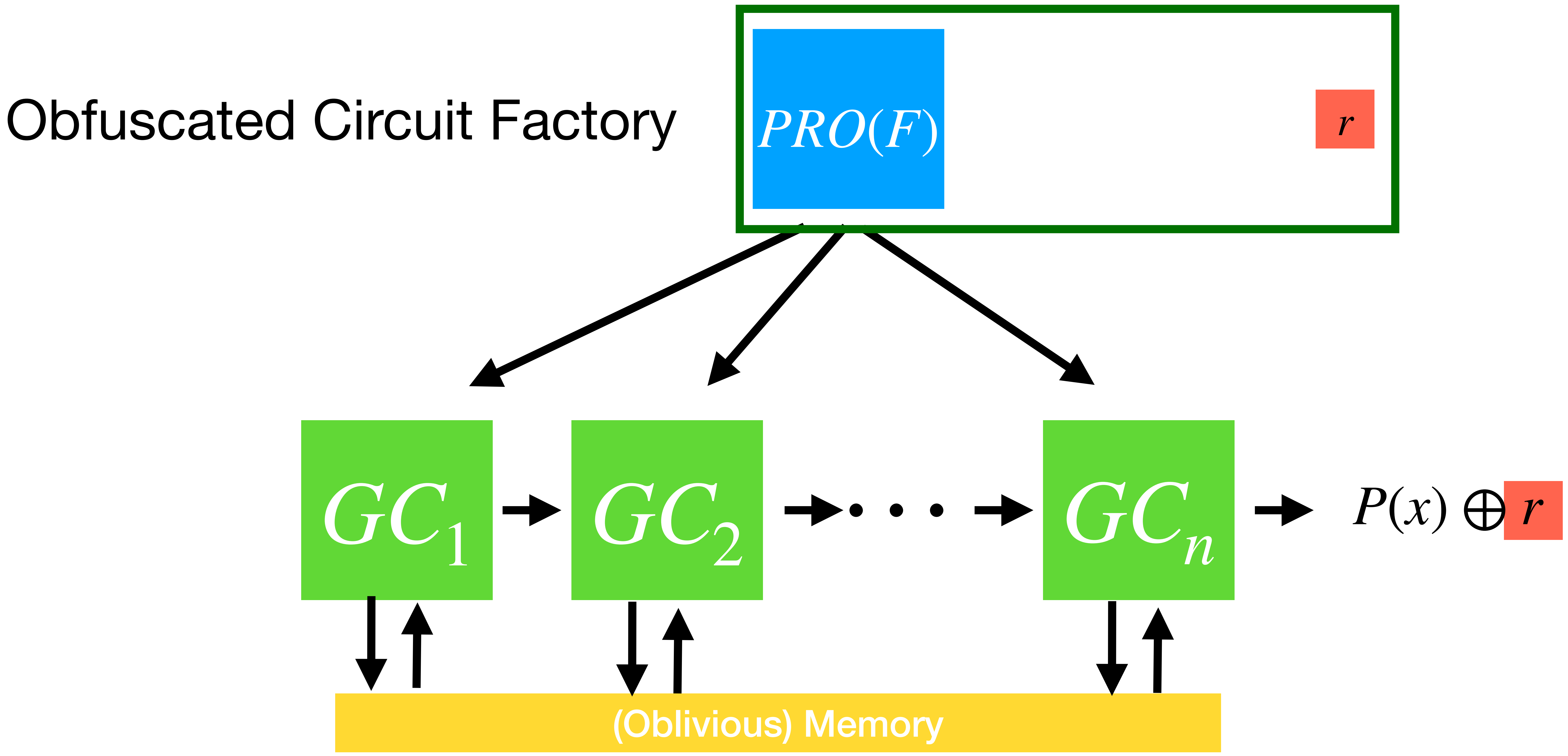


Succinct Garbling

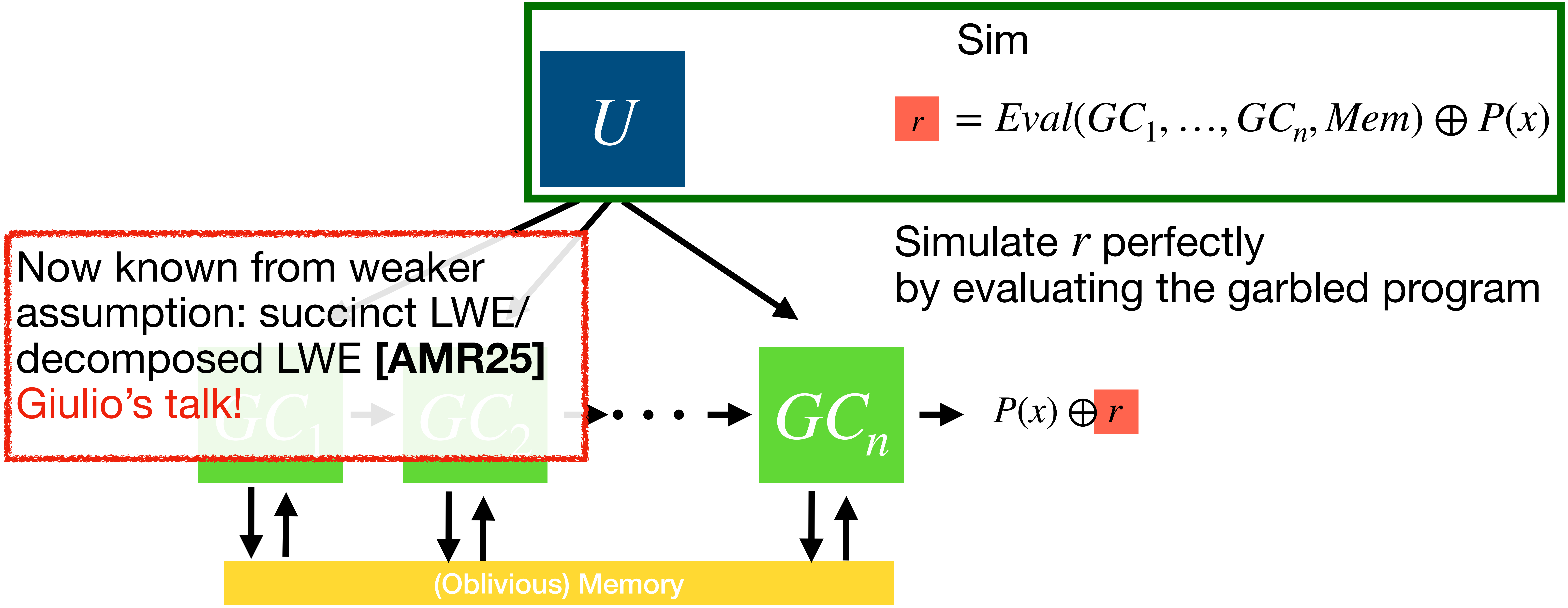
- Garble step circuits
- Last GC outputs a share of the result
- Other share given in plain
- [BLSV'18]: Point&Permute GC are pseudorandom ("Blind GC")
- Produce GCs via circuit factory



Succinct Garbling



Succinct Garbling



Simulate r perfectly
by evaluating the garbled program

Pseudorandom Witness Encryption

[GGHRSW'13] recipe

- Fix NP-language $\mathscr{L}$

C[m,x,K](w): Output

m if $Verify_{\mathscr{L}}(x, w) = 1$

$PRF_K(w)$ otherwise

prWE.Enc(x,m) = PRO(C[m,x,K])

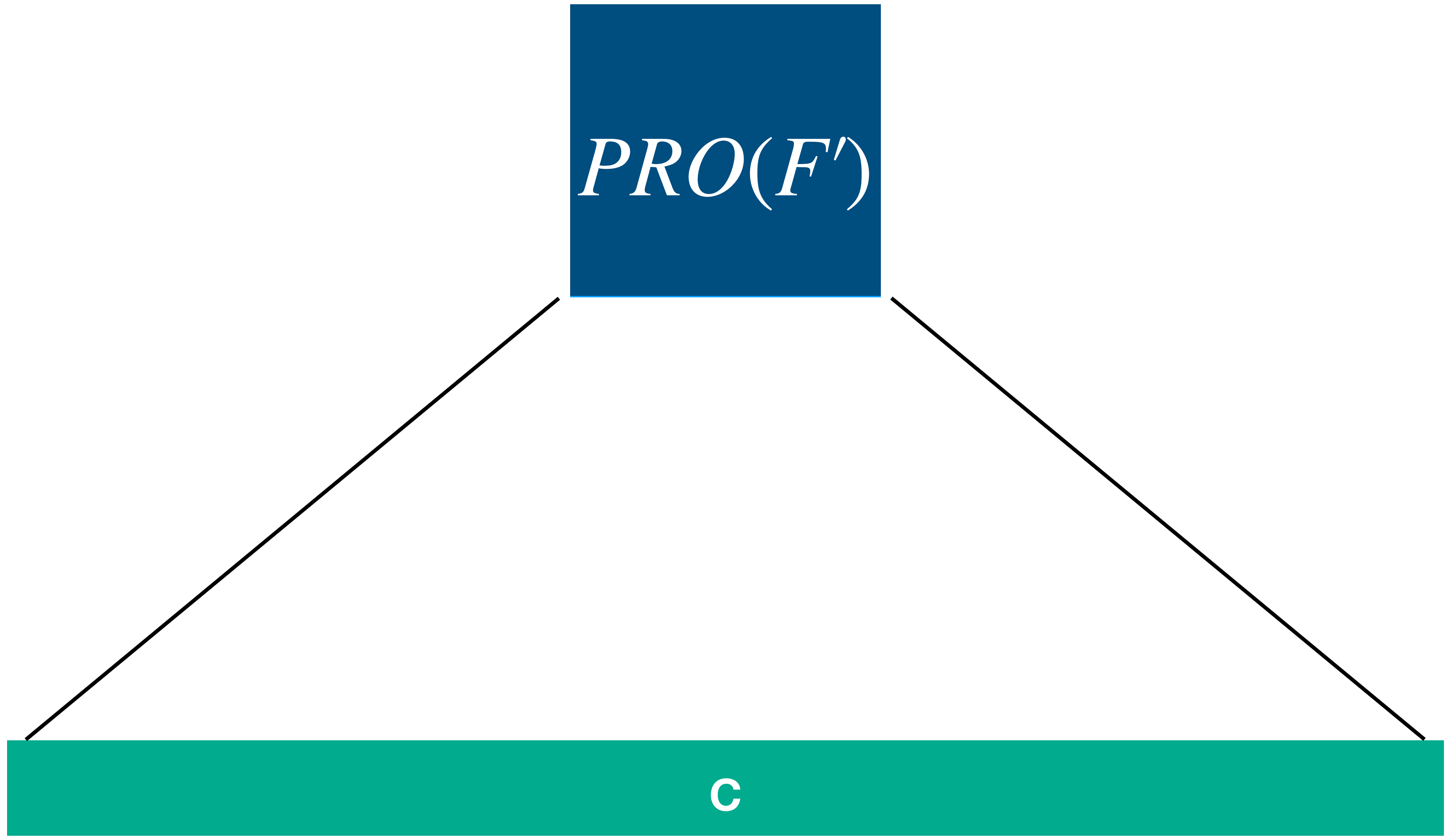
prWE.Dec(c,w) = c(w)

- If $x \notin \mathscr{L}$ then $C[m, x, K](\cdot) \equiv PRF_K(\cdot)$
- By PRO-security prWE.Enc(x,m) is pseudorandom if $x \notin \mathscr{L}$

Succinct Pseudorandom Witness Encryption

Compress further via PRO

- $|WE(x, m)| = poly(|C[x, K]|) = poly(|w|)$
- However, if $x \notin \mathscr{L}$, WE(x,m) is pseudorandom
- Hence $F'_{x,m}(i) = (prWE.Enc(x, m))_i$ is a pseudorandom function with domain-size $log(|w|)$
- Hence define $prWE'.Enc(x, m) = PRO(F'_{x,m})$
- Decrypting $c = prWE'.Enc(x, m)$ given witness w:
  - Set $c' = (c(i))_{i \in [|w|]}$
  - $m = c'(w)$



Issues with PRO

Counterexample to PRO

- Just seen: PRO ⇒ <u>pr</u>WE
  - Hides prWE hides false statements!
- The notion of PRO is “self-defeating”
- Idea: aux is prWE for following statement:
  - x s.t. exists small circuit C st. x = TT(c)
  - i.e. x has small Kolmogorov complexity

Counterexample to PRO

Precondition

	aux
$x = TT(PRF_K)$	prWE(“x is TT of small C”,0^λ)
$\approx$	
u	prWE(“u is ~~TT of~~ small C”,0^λ)
$\approx$	
u	prWE(“u’ is TT of small C”,0^λ)
$\approx$	
u	prWE(“x is TT of small C”,0^λ)

Counterexample to PRO

Postcondition

$x = TT(PRF_K) = TT(PRO(PRF_K))$

aux

$w =$ $PRO(PRF_K)$

prWE(“x is TT of small C”,0^λ)

$WE.Dec$

0^λ

Distinguisher!

u'

prWE(“x is TT of small C”,0^λ)

$WE.Dec$

$\perp$

A Weaker Notion

Indistinguishability PRO (iPRO)

$TT(F_K)$ $\approx$ U

$\Downarrow$

$iPRO(F_{K_0})$ $\approx$ $iPRO(F_{K_1})$

- iO for Pseudorandom Functions
- Implied by iO $\Rightarrow$ no counterexamples!

xiPRO: $|iPRO(C)| = |TT(C)|^{1-\epsilon}$

From xiPRO to xiO

$xiPRO(PRF_K(\cdot) + C(\cdot))$ $\cancel{xiPRO(PRF}_K(x))$

$xiPRO((i,j) \mapsto e(g_1^{x_i}, g_2^{x_2}) \cdot g_T^{C(i,j)})$ $e(g_1^{x_i}, g_2^{x_j})$ ~~via~~ $\cancel{(g_1^{x_i})_i, (g_2^{y_j})_j}$

via $QFE.Enc((x_i)_i, (y_j)_j)$
and $\{sk_{i,j}\}_{i,j}$

$\approx Sim(\{e(g_1^{x_i}, g_2^{x_j})\}_{i,j})$

- Hide the $g_1^{x_i}$, $g_2^{x_j}$ using wrapper of quadratic FE **[Wee'20]**
- Layer of amortisation of quadratic FE keys
- Does not go through local PRGs, LPN: "Coding Hardness"

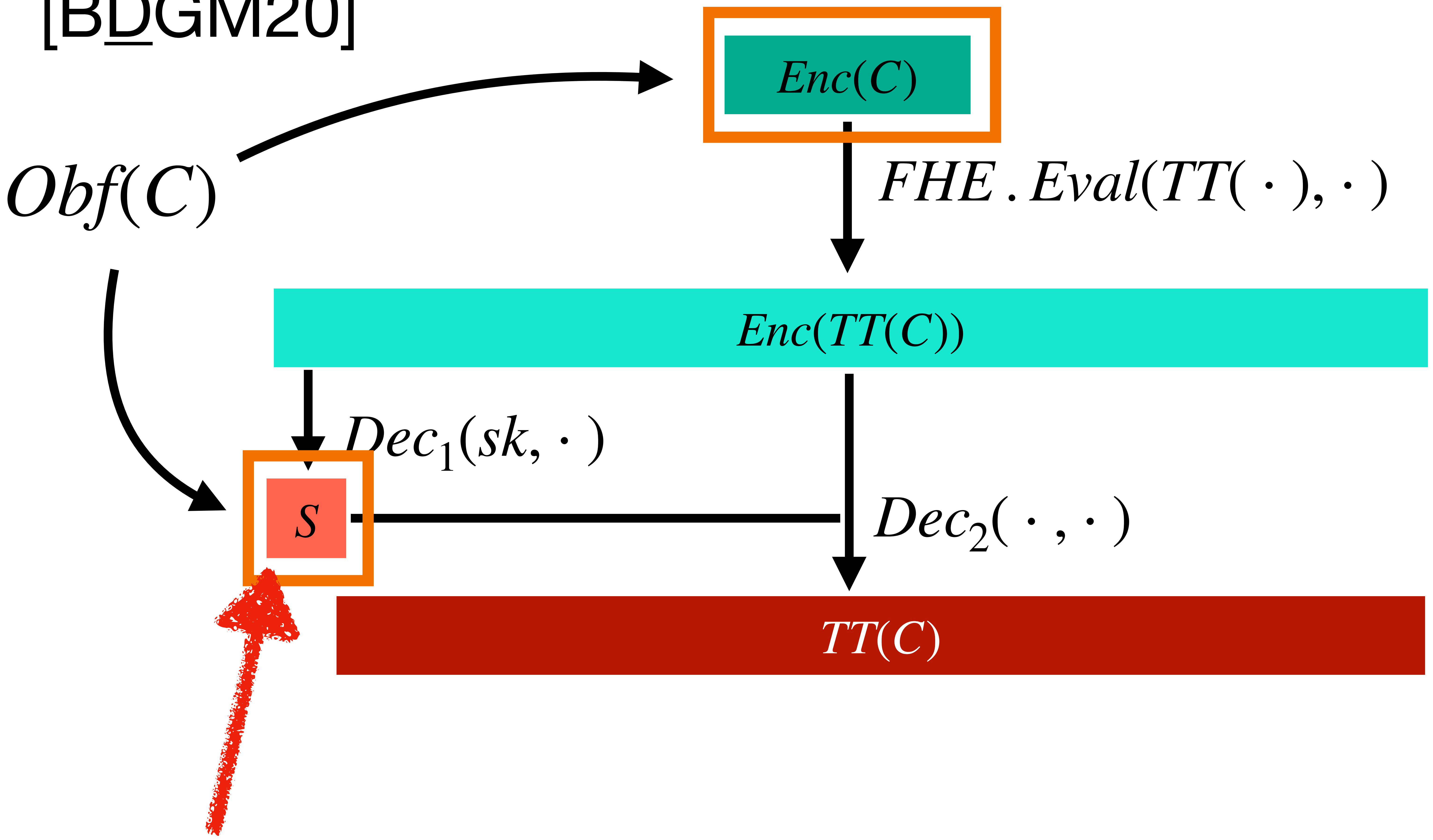
PRO from private-coin evasive LWE

xPRO: PRO with polynomial compression

- Suffices to construct exponentially efficient version xPRO
- Bootstrapping similar to **[BV15,AJ15]**
- Additional ingredients: Blind Garbled Circuits **[BLSV18]** and blind LFE (new)

BDGM Approach to xiO

[BDGM20]

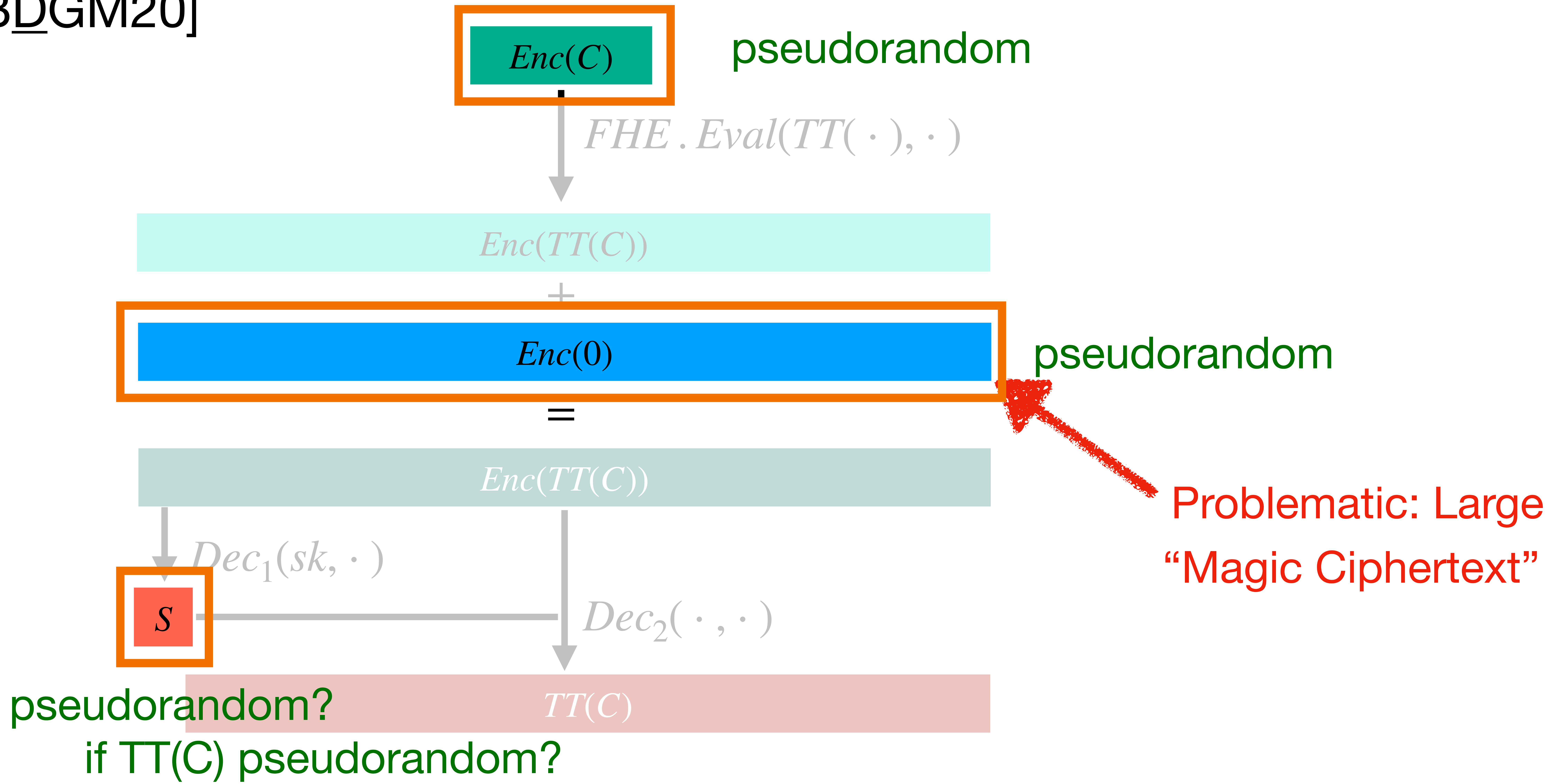


Dual-Regev Enc
(think hybrid encryption)

Leaks information about $FHE.sk$, C

BDGM Approach to xiO

[BDGM20]



Learning with Errors

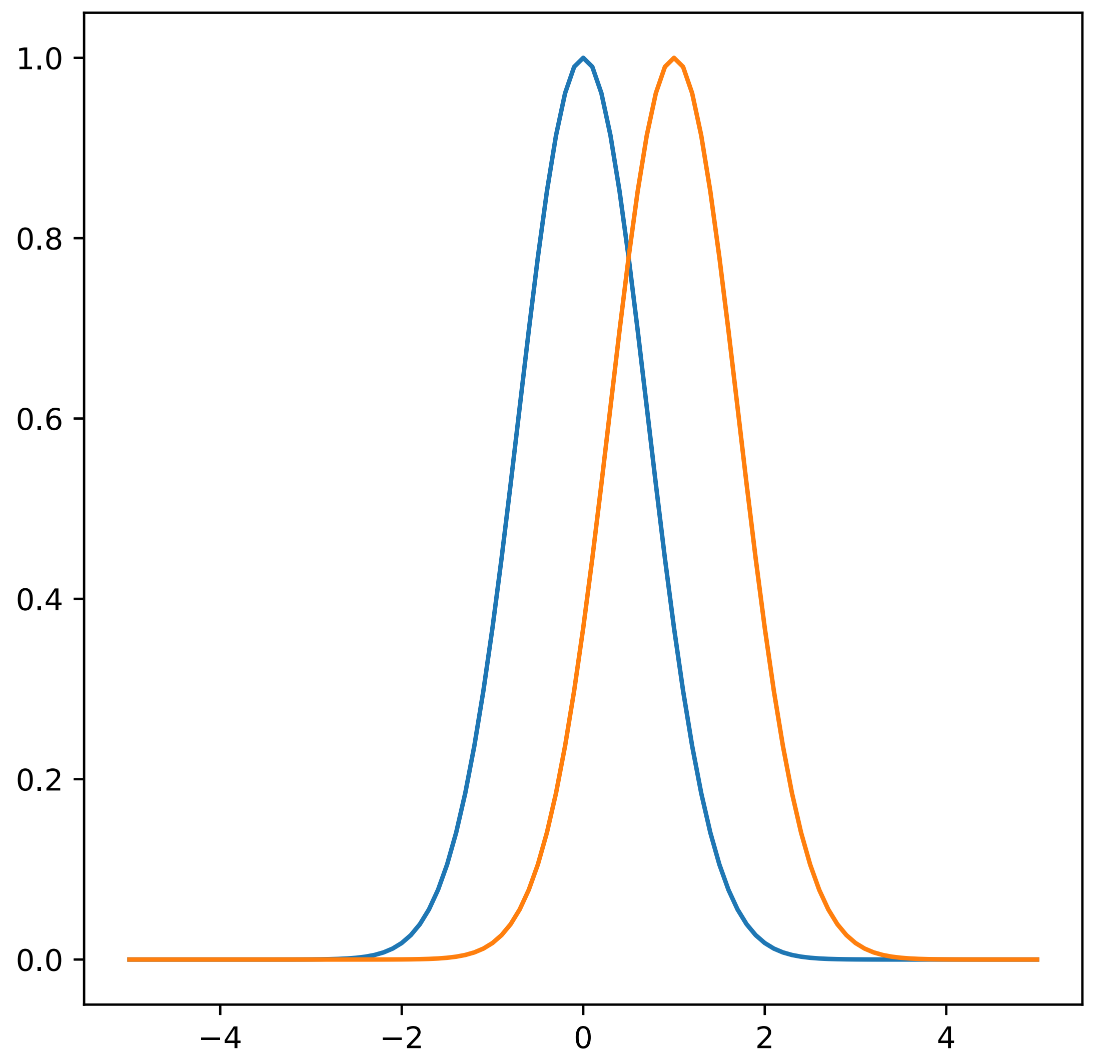
[Regev05]

$S \; A + E \approx U$ given A

gaussian

Noise Drowing/Flooding/Smudging

$E + Z \approx_s E$



Non-compact Magic Ciphertext

$\equiv$ xPRO Precondition

- Magic ciphertext is dual-Regev encryption of 0
- Idea: Magic ciphertext can be simulated given S and $TT(C)$
- E drowns noise artefacts
- Replace $Enc(C)$ with $Enc(0)$
- Pseudorandomness of TT(C) makes (simulated) magic ciphertext pseudorandom
- **Establishes PRO precondition**

$$Enc(0)$$

$$=$$

$$S' \quad P + E'$$

$$\approx$$

$$SP - Enc(TT(C)) + TT(C) + L(sk) + E$$

$$\approx$$

$$SP - Enc(TT(C)) + TT(C) + E$$

$$\approx$$

$$SP - Enc(TT(0)) + TT(C) + E$$

$$\approx$$

$$U$$

Compressing the Magic Ciphertext

Pseudodrowning

- Magic ciphertext $SP + E$ is as large as truth table $TT(C)$
- Need to compress $SP + E$
- **Evasive LWE Recipe/Heuristic:** Actual scheme contains a term $SB + E$ and a short matrix $B^{-1}(P)$ with $B \cdot B^{-1}(P) = P$

Compressing the Magic Ciphertext

Rationale

$$\left(S \; B + E \right) \; B^{-1}(P)$$

$$= S \; P \; + \; E \; B^{-1}(P)$$

In low rank subspace

Heuristic: behaves like

$$S \; P \; + \; E'$$

full rank

Private Coin Evasive LWE

[Tsabary'22,Wee'22,VWW'22]

If

Precondition

$$S B + E \;,\; S P + E' \;\approx\; U \;,\; U' \quad \text{given} \quad \text{aux}$$

Then

Postcondition

$$S B + E \;\approx\; U \quad \text{given} \quad B^{-1}(P) \quad \text{aux}$$

Compressing the Magic Ciphertext

Pseudodrowning

- **Evasive LWE Heuristic**: Only thing you can do with $B^{-1}(P)$ is expand samples and then ignore it
- Noise term in subspace behaves like a fresh gaussian noise term, use it to drown artefacts
- Evasive LWE is (essentially) always used for “pseudodrowning”

Direct Counterexamples to evasive LWE

- Evasive LWE counterexample from PRO is *contrived/pathologic*
- Direct/natural counterexample questioning the “pseudo-drowning” heuristic

Direct Counterexamples to evasive LWE

Precondition

aux

$$sB + e \quad sP + e' \quad sP - t \qquad t + e' \to e' \mod 2$$

$$\approx$$

$$u \quad u' \quad sP - t$$

Mask t reveals exactly LSBs of error e'

Direct Counterexamples to evasive LWE

aux

$B^{-1}(P)$ $\quad sP + eB^{-1}(P)$ $\quad sP - t$ $\qquad eB^{-1}(P) \mod 2$

$$\Cap$$

$Span(B^{-1}(P) \mod 2)$

Distinguisher!

$B^{-1}(P)$ $\quad u'$ $\quad sP - t$ $\qquad \tilde{u} \mod 2$

$$\not\Cap$$

$Span(B^{-1}(P) \mod 2)$

Takeaways

- PRO powerful tool to augment iO-like constructions with pseudorandomness properties
- In general too good to be true
- Notion of PRO suffers from counterexamples
- Concept of PRO shed light on issues with evasive LWE
- Fallback: iO for pseudorandom functions (iPRO), implies iO using standard pairing assumptions
- Looking ahead: Stronger Notions of PRO that do not suffer from counterexamples?

Thanks!