CONSTANT-ROUND SIMULATION-SECURE COIN TOSSING EXTENSION WITH GUARANTEED OUTPUT

DAMIANO ABRAM
AARHUS UNIVERSITY
BOCCONI UNIVERSITY

JACK DOERNER
TECHNION
REICHMAN UNIVERSITY
BROWN UNIVERSITY

YUVAL ISHAI
TECHNION

VARUN NARAYANAN
UCLA

COIN TOSSING

$\mathcal{F}_n$

$r \xleftarrow{\$} \{0,1\}^n$

output r to everybody

COIN TOSSING

$\mathcal{F}_m$

$$\boxed{\begin{array}{c} r \xleftarrow{\$} \{0,1\}^m \\ \text{output } r \text{ to everybody} \end{array}}$$

dishonest majority + malicious corruption

<u>SIMULATION SECURITY</u>

COIN TOSSING

$\mathcal{F}_m$

$r \xleftarrow{\$} \{0,1\}^m$

output r to everybody

dishonest majority + malicious corruption

<u>SIMULATION SECURITY</u>

IMPOSSIBLE!

(even for computational security)

[CLEVE 86]

COIN TOSSING EXTENSION

- Bellare et al. (PODC '96)
- Hofheinz et al. (EUROCRYPT '06)

↓

neither focused on guaranteed output

$$\mathcal{F}_m$$

$$r \xleftarrow{\$} \{0,1\}^m$$

output r to everybody

COIN TOSSING EXTENSION

- Bellare et al. (PODC '96)
- Hofheinz et al. (EUROCRYPT '06)

↓

neither focused on guaranteed output

$\mathcal{F}_m$

$r \xleftarrow{\$} \{0,1\}^m$

output r to everybody

$\uparrow$ $n \ll m$

$\mathcal{F}_n$ $\quad n = \omega(\log \lambda)$

auxiliary resource "magic button" →

$s \xleftarrow{\$} \{0,1\}^n$

output s to everybody

COIN TOSSING EXTENSION

- Bellare et al. (PODC '96)
- Hofheinz et al. (EUROCRYPT '06)

↓

neither focused on guaranteed output

$\mathcal{F}_m$

$r \xleftarrow{\$} \{0,1\}^m$

output r to everybody

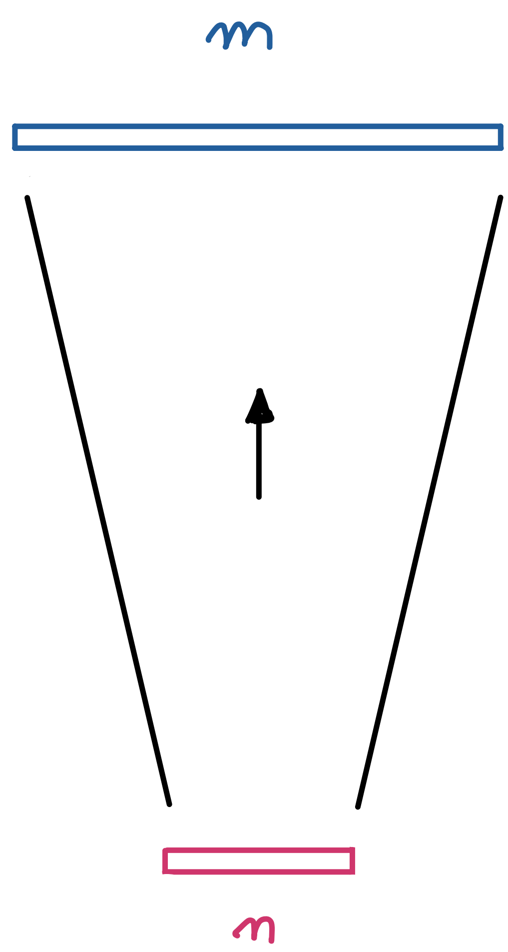
↑ $n \ll m$

$\mathcal{F}_n$ $\quad n = \omega(\log \lambda)$

auxiliary resource "magic button" →

$s \xleftarrow{\$} \{0,1\}^n$

output s to everybody



COIN TOSSING EXTENSION

- Bellare et al. (PODC '96)
- Hofheinz et al. (EUROCRYPT '06)

↓

neither focused on guaranteed output

$\mathcal{F}_m$

$r \xleftarrow{\$} \{0,1\}^m$

output r to everybody

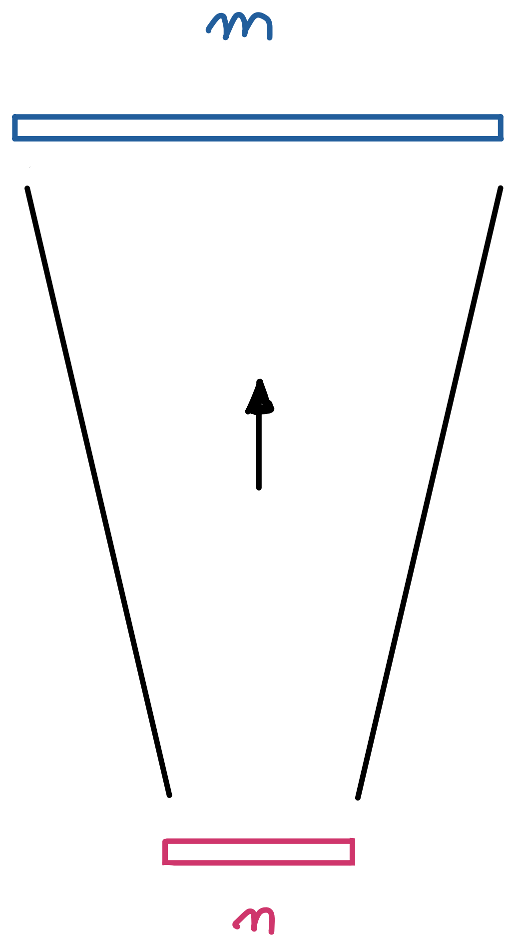
↑ $n \ll m$

$\mathcal{F}_n$ $\quad n = \omega(\log \lambda)$

auxiliary resource "magic button" (e.g. physical device or randomness beacon) →

$s \xleftarrow{\$} \{0,1\}^n$

output s to everybody



SOLUTIONS THAT DON'T WORK

ONLY GAME-BASED SECURITY

- BAD IDEA: PRGs

$r = PRG(s)$ looks random only if s is secret!

SOLUTIONS THAT DON'T WORK

ONLY GAME-BASED SECURITY

- BAD IDEA: PRGs

  $r = PRG(s)$ looks random only if s is secret!

if $\mathcal{H}$ = hash function

- BORING IDEA: random oracle

  $r = \mathcal{H}(s)$ looks random, but RO don't exist!

BETTER SOLUTION: RANDOMNESS EXTRACTORS

ALICE		BOB
	$a \xleftarrow{\$} \{0,1\}^L$	
	$\xrightarrow{\hspace{6em}}$	
	$\xleftarrow{\hspace{6em}}$	
	$b \xleftarrow{\$} \{0,1\}^L$	

BETTER SOLUTION: RANDOMNESS EXTRACTORS

ALICE

BOB

$a \xleftarrow{\$} \{0,1\}^L$

$b \xleftarrow{\$} \{0,1\}^L$

$\mathcal{F}_n \xrightarrow{\$} s$

BETTER SOLUTION: RANDOMNESS EXTRACTORS

ALICE

BOB

$a \xleftarrow{\$} \{0,1\}^L$

$b \xleftarrow{\$} \{0,1\}^L$

$\mathcal{F}_n \xrightarrow{\$} s$

$\boxed{\text{Output } r = Ext(s, a \| b)}$

random even if one party is corrupted

BETTER SOLUTION: RANDOMNESS EXTRACTORS

ALICE

BOB

$a \xleftarrow{\$} \{0,1\}^L$

$b \xleftarrow{\$} \{0,1\}^L$

$\mathcal{F}_n \xrightarrow{\$} s$

$\boxed{\text{Output } r = Ext(s, a \| b)}$

random even if one party is corrupted

<u>How do we simulate?</u>

EXPLAINABLE EXTRACTOR

$\forall$ adversary $\mathcal{A} \in \mathcal{C}$, $\exists$ PPT $Sim_{\mathcal{A}}$ s.t.

$$\left\{ r, s, a, b \;\middle|\; \begin{array}{l} a \xleftarrow{\$} \{0,1\}^{L} \\ b \xleftarrow{\$} \mathcal{A}(1^{\lambda}, a) \\ s \xleftarrow{\$} \{0,1\}^{m} \\ r \leftarrow Ext(s, a \| b) \end{array} \right\} \sim \left\{ r, s, a, b \;\middle|\; \begin{array}{l} r \xleftarrow{\$} \{0,1\}^{L} \\ (s, a, b) \xleftarrow{\$} Sim_{\mathcal{A}}(1^{\lambda}, r) \end{array} \right\}$$

EXPLAINABLE EXTRACTOR

$\forall$ adversary $\mathcal{A} \in \mathcal{C}$, $\exists$ PPT $Sim_{\mathcal{A}}$ s.t.

$$\left\{ r, s, x \;\middle|\; \begin{array}{l} x \xleftarrow{\$} \mathcal{A}(1^\lambda, a) \\ s \xleftarrow{\$} \{0,1\}^n \\ r \leftarrow Ext(s, x) \end{array} \right\} \sim \left\{ r, s, x \;\middle|\; \begin{array}{l} r \xleftarrow{\$} \{0,1\}^L \\ (s, x) \xleftarrow{\$} Sim_{\mathcal{A}}(1^\lambda, r) \end{array} \right\}$$

EX: STRONG EXTRACTORS WITH $O(\log \lambda)$ - STRETCH

$Ext(s, x) = (s, y)$ where $|y| = O(\log \lambda)$

EXPLAINABLE EXTRACTOR

$\forall$ adversary $\mathcal{A} \in \mathcal{C}$, $\exists$ PPT $\mathrm{Sim}_{\mathcal{A}}$ s.t.

$$\left\{ r, s, x \;\middle|\; \begin{array}{l} x \xleftarrow{\$} \mathcal{A}(1^\lambda, a) \\ s \xleftarrow{\$} \{0,1\}^m \\ r \leftarrow \mathrm{Ext}(s, x) \end{array} \right\} \sim \left\{ r, s, x \;\middle|\; \begin{array}{l} r \xleftarrow{\$} \{0,1\}^L \\ (s, x) \xleftarrow{\$} \mathrm{Sim}_{\mathcal{A}}(1^\lambda, r) \end{array} \right\}$$

EX: STRONG EXTRACTORS WITH $O(\log \lambda)$ - STRETCH

$$\mathrm{Ext}(s, x) = (s, y) \quad \text{where} \quad |y| = O(\log \lambda)$$

$\mathrm{Sim}_{\mathcal{A}}$ can brute-force for x!

$\downarrow$

1-round statistical CTE with $O(\log \lambda)$-stretch [HMU06]

O(1)-ROUND CTE WITH ARBITRARY STRETCH

computational security:

O(1)-ROUND CTE WITH ARBITRARY STRETCH

computational security:

ASSUMPTION	# PARTIES	# ROUNDS
coin tossing with abort	2	$O(1)$

O(1)-ROUND CTE WITH ARBITRARY STRETCH

computational security:

ASSUMPTION	# PARTIES	# ROUNDS
coin tossing with abort	2	$O(1)$
coin tossing with identifiable abort	N	$O(N)$

O(1)-ROUND CTE WITH ARBITRARY STRETCH

computational security:

ASSUMPTION	# PARTIES	# ROUNDS	MODEL
coin tossing with abort	2	$O(1)$	it depends...
coin tossing with identifiable abort	N	$O(N)$	it depends...
OWF [Goyal et al]	N	$O(N)$	standalone

O(1)-ROUND CTE WITH ARBITRARY STRETCH

computational security:

ASSUMPTION	# PARTIES	# ROUNDS	MODEL
coin tossing with abort	2	$O(1)$	it depends...
coin tossing with identifiable abort	N	$O(N)$	it depends...
OWF [Goyal et al]	N	$O(N)$	standalone
DDH / Paillier / class groups	N	1	UC + reusable CRS

O(1)-ROUND CTE WITH ARBITRARY STRETCH

computational security:

ASSUMPTION	# PARTIES	# ROUNDS	MODEL	ADAPTIVE CORRUPTION
coin tossing with abort	2	$O(1)$	it depends...	it depends...
coin tossing with identifiable abort	N	$O(N)$	it depends...	it depends...
OWF [Goyal et al]	N	$O(N)$	standalone	?
DDH / Paillier / class groups	N	1	UC + reusable CRS	NO
LWE with $\omega(\lambda^{\log \lambda})$ modulus-noise ratio	N	1	UC	YES

O(1)-ROUND CTE WITH ARBITRARY STRETCH

statistical security:

- impossibility for standalone black-box simulation

  R-round CTE has $O(R \cdot \log \lambda)$ stretch

O(1)-ROUND CTE WITH ARBITRARY STRETCH

statistical security:

- impossibility for standalone black-box simulation

R-round CTE has $O(R \cdot \log \lambda)$ stretch

generalisation:

- 1-round, 1-call secure sampling from any distribution (λ-bit, unstructured, reusable CRS)

iO + indistinguishability-preserving distributed samplers

$$\mathcal{F}_n \ \boxed{\text{Output } s \xleftarrow{\$} \{0,1\}^n \text{ to everybody}} \longrightarrow \boxed{\text{Output } R \xleftarrow{\$} D(1^\lambda) \text{ to everybody}} \ \mathcal{F}_D$$

NI-CTE FROM LWE

1st ingredient:

$(G,+)$ ← large group

$H = \langle h \rangle$ ← hidden cyclic subgroup

$g \xleftarrow{\$} G$ looks like $g \xleftarrow{\$} H$

NI-CTE FROM LWE

1st ingredient:

$(G,+) \leftarrow$ large group

$H = \langle h \rangle \leftarrow$ hidden cyclic subgroup

$g \xleftarrow{\$} G$ looks like $g \xleftarrow{\$} H$

2nd ingredient:

lossy trapdoor function f (unstructured description)

NI-CTE FROM LWE

1st ingredient:

$(G,+)$ ← large group

$H=\langle h\rangle$ ← hidden cyclic subgroup

$g \xleftarrow{\$} G$ looks like $g \xleftarrow{\$} H$

2nd ingredient:

lossy trapdoor function f (unstructured description)

SURJECTIVE MODE

LOSSY MODE

NI-CTE FROM LWE

1st ingredient:

$(G,+) \leftarrow$ large group

$H = \langle h \rangle \leftarrow$ hidden cyclic subgroup

$g \xleftarrow{\$} G$ looks like $g \xleftarrow{\$} H$

2nd ingredient:

lossy trapdoor function f (unstructured description)

SURJECTIVE MODE $\rightarrow$ f outputs random elements in G

LOSSY MODE

NI-CTE FROM LWE

1st ingredient:

$(G,+)$ ← large group

$H = \langle h \rangle$ ← hidden cyclic subgroup

$g \xleftarrow{\$} G$ looks like $g \xleftarrow{\$} H$

2nd ingredient:

lossy trapdoor function f (unstructured description)

SURJECTIVE MODE → f outputs random elements in G

LOSSY MODE → f outputs random elements in H

NI-CTE FROM LWE

$G \leftarrow$ large group $\quad H = \langle h \rangle \leftarrow$ hidden cyclic subgroup

$$f : \{0,1\}^{L} \longrightarrow G$$

ALICE $\qquad$ BOB

NI-CTE FROM LWE

$G \leftarrow$ large group $\qquad H = \langle h \rangle \leftarrow$ hidden cyclic subgroup

$$f : \{0,1\}^L \longrightarrow G$$

ALICE $\qquad\qquad\qquad\qquad$ BOB

$$x_A \xleftarrow{\$} \{0,1\}^L$$

$$x_B \xleftarrow{\$} \{0,1\}^L$$

NI-CTE FROM LWE

$G \leftarrow$ large group $H = \langle h \rangle \leftarrow$ hidden cyclic subgroup

$$f : \{0,1\}^L \longrightarrow G$$

ALICE   BOB

$$\text{ALICE} \xrightarrow{x_A \xleftarrow{\$} \{0,1\}^L} \text{BOB}$$

$$\text{ALICE} \xleftarrow[x_B \xleftarrow{\$} \{0,1\}^L]{} \text{BOB}$$

$\mathcal{F}_n \longrightarrow f_A, f_B, \alpha$

NI-CTE FROM LWE

$G \leftarrow$ large group $H = \langle h \rangle \leftarrow$ hidden cyclic subgroup

$$f : \{0,1\}^\ell \longrightarrow G$$

ALICE BOB

$$x_A \xleftarrow{\$} \{0,1\}^\ell$$

$$\longrightarrow$$

$$\longleftarrow$$

$$x_B \xleftarrow{\$} \{0,1\}^\ell$$

$\mathcal{F}_n \longrightarrow f_A, f_B, \alpha$

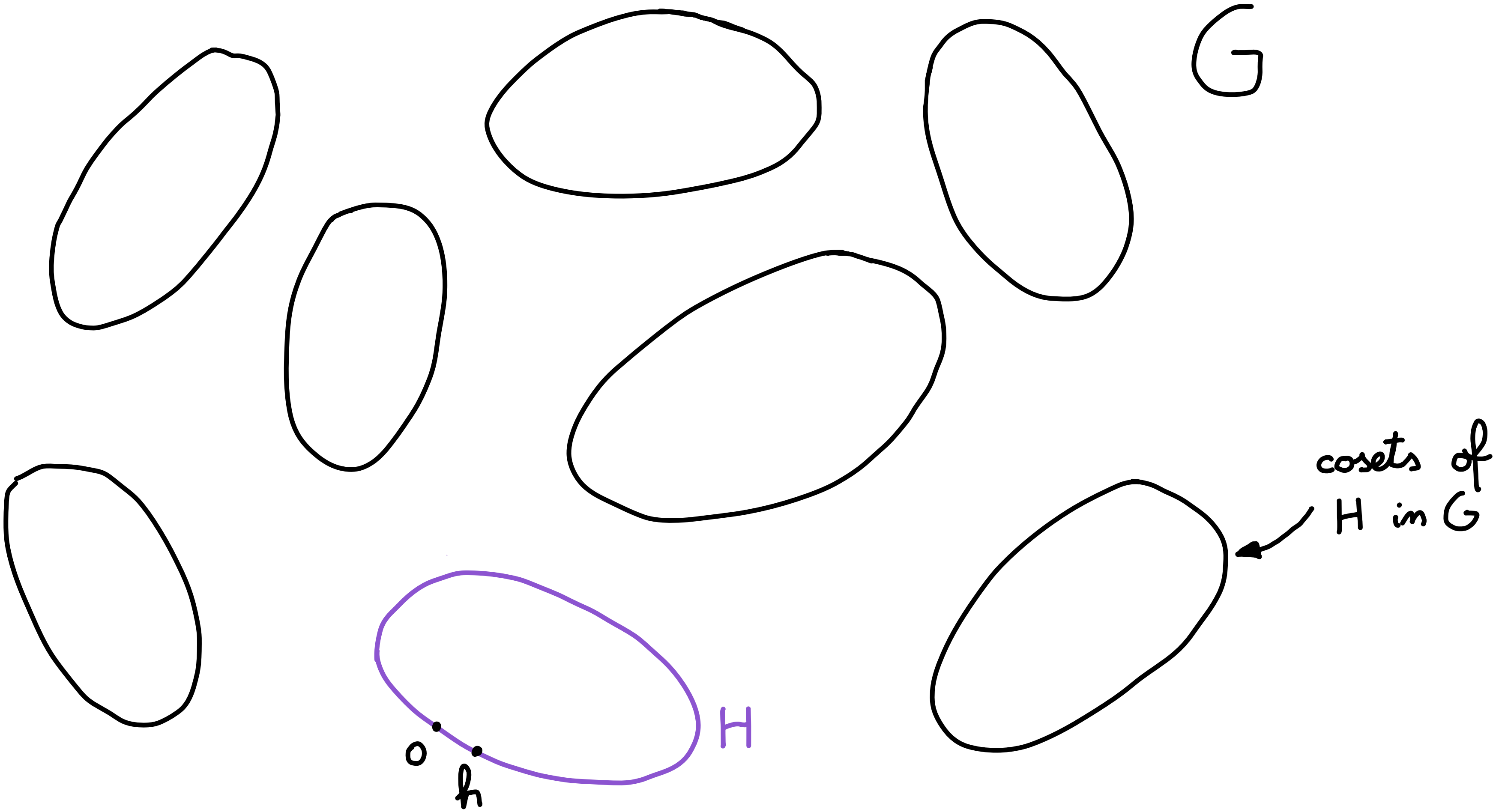
$$\boxed{\text{Output } \; f_A(x_A) + f_B(x_B) + \alpha \cdot h}$$

NI-CTE FROM LWE

f_A ← SURJECTIVE

f_B ← LOSSY

$$\boxed{\text{Output } \; f_A(x_A) + f_B(x_B) + \alpha \cdot h}$$

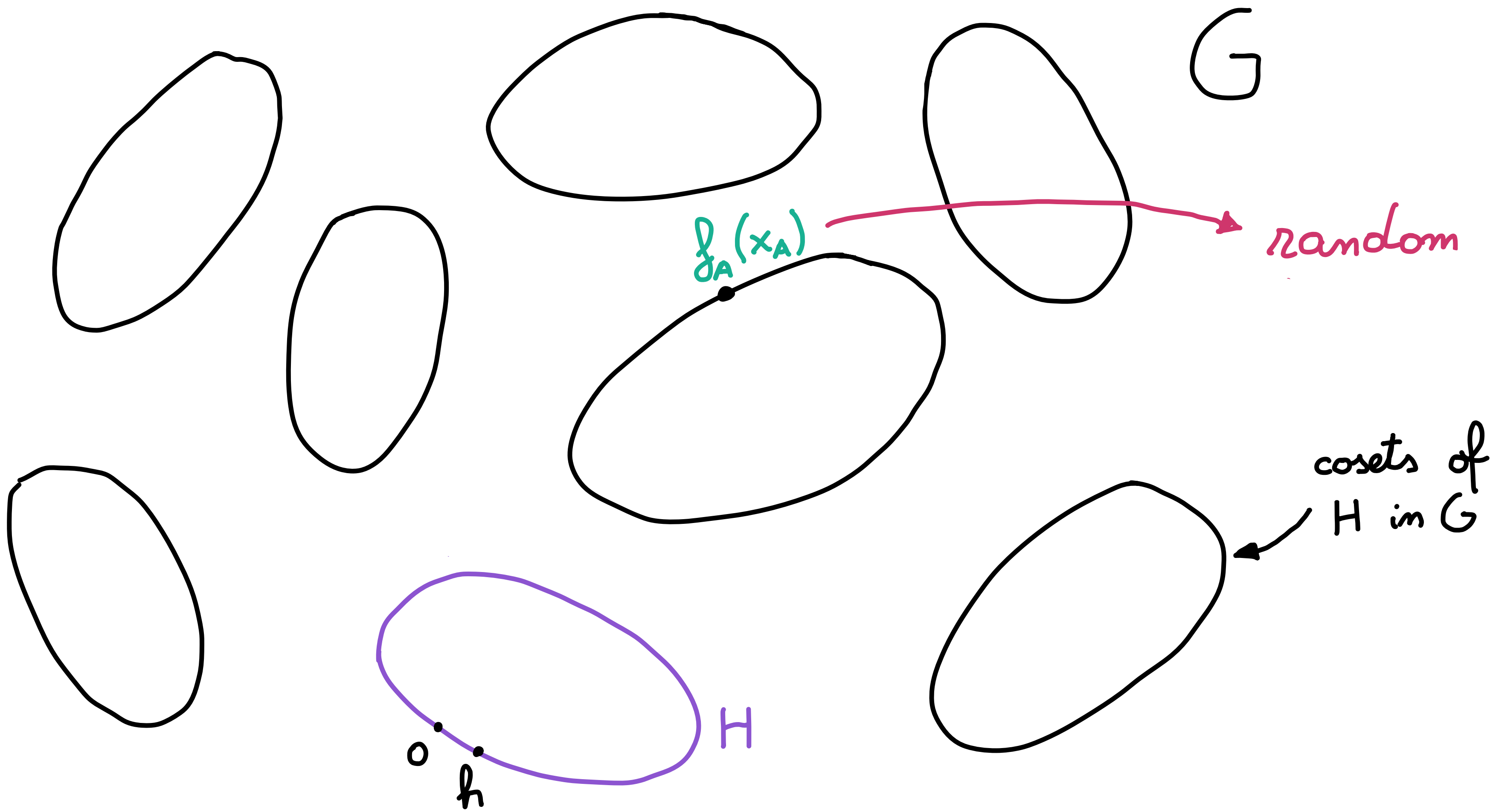


NI-CTE FROM LWE

$f_A \leftarrow$ SURJECTIVE

$f_B \leftarrow$ LOSSY

$\boxed{\text{Output } f_A(x_A) + f_B(x_B) + \alpha \cdot h}$



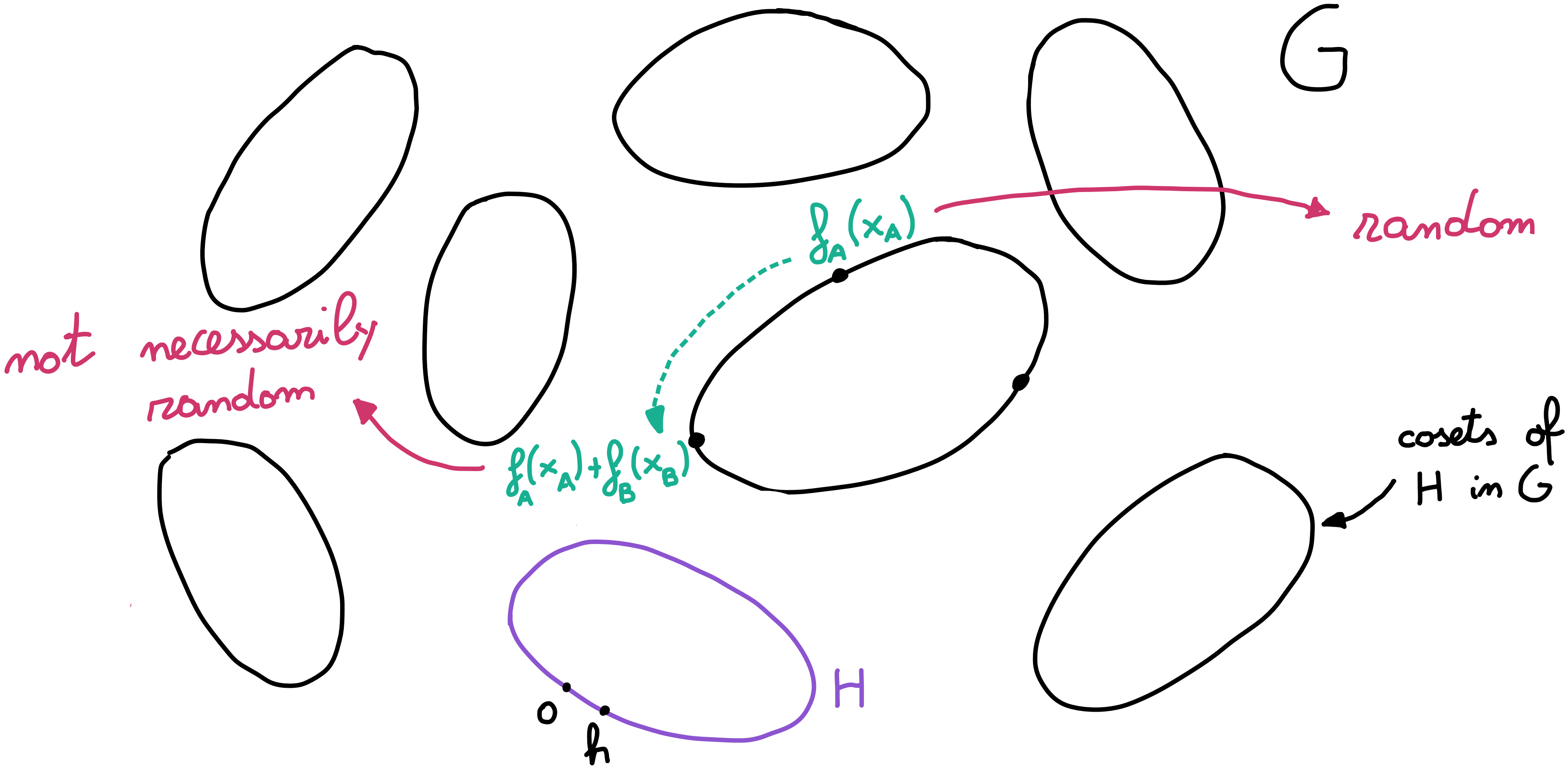
NI-CTE FROM LWE

$f_A \leftarrow$ SURJECTIVE

$f_B \leftarrow$ LOSSY

in H

$$\boxed{\text{Output} \quad f_A(x_A) + f_B(x_B) + \alpha \cdot h}$$



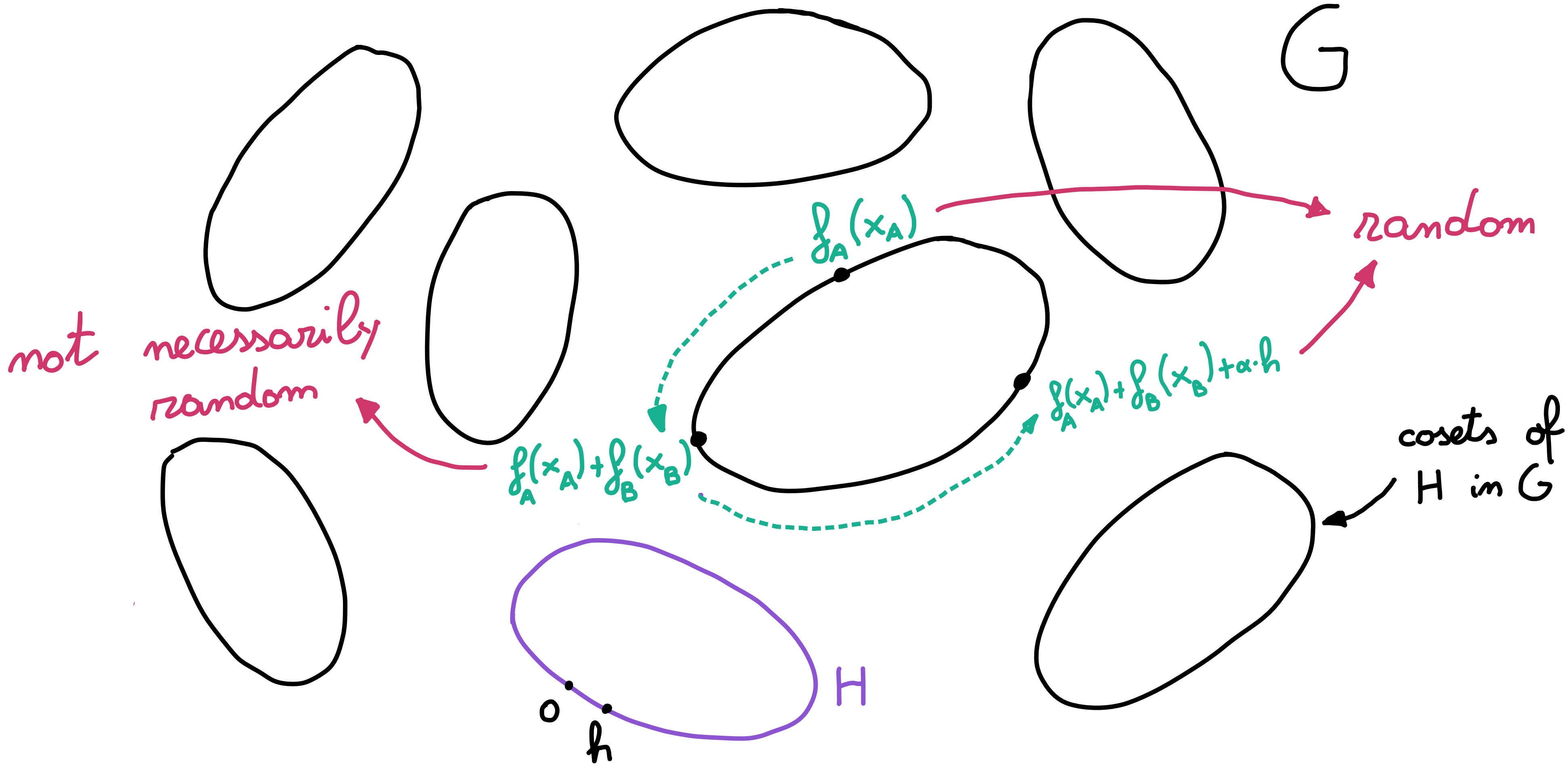
NI-CTE FROM LWE

$f_A \leftarrow$ SURJECTIVE

$f_B \leftarrow$ LOSSY

in H

$\boxed{\text{Output } f_A(x_A) + f_B(x_B) + \alpha \cdot h}$ $\rightarrow$ random in H



NI-CTE FROM LWE

$G = \mathbb{Z}_q^{k+T}$

NI-CTE FROM LWE

$G = \mathbb{Z}_q^{K+T}$

$H = \{ (\underbrace{v_1}_{K}, \underbrace{v_2}_{T}) \mid v_2 = S \cdot v_1 \}$ $\quad S \xleftarrow{\$} \mathbb{Z}_q^{T \times K}$

secret

NI-CTE FROM LWE

$G = \mathbb{Z}_q^{K+T}$

$H = \{ (\underbrace{v_1}_{K}, \underbrace{v_2}_{T}) \mid v_2 = S \cdot v_1 \}$ $\quad \underset{\text{secret}}{S} \xleftarrow{\$} \mathbb{Z}_q^{T \times K}$

SURJECTIVE MODE

$g \rightsquigarrow M \xleftarrow{\$} \mathbb{Z}_q^{(K+T) \times W}$

NI-CTE FROM LWE

$G = \mathbb{Z}_q^{K+T}$

$H = \{ (\underbrace{v_1}_{K}, \underbrace{v_2}_{T}) \mid v_2 = S \cdot v_1 \}$ $\quad S \xleftarrow{\$} \mathbb{Z}_q^{T \times K}$

secret

SURJECTIVE MODE

$f \rightsquigarrow M \xleftarrow{\$} \mathbb{Z}_q^{(K+T) \times W}$

$f(x) = M \cdot x'$

view x
as randomness
for discrete Gaussian

NI-CTE FROM LWE

$G = \mathbb{Z}_q^{K+T}$ $\qquad H = \{ (\underbrace{v_1}_{K}, \underbrace{v_2}_{T}) \mid v_2 = S \cdot v_1 \}$ $\qquad \underset{\uparrow}{S} \xleftarrow{\$} \mathbb{Z}_q^{T \times K}$

secret

SURJECTIVE MODE

$f \rightsquigarrow M \xleftarrow{\$} \mathbb{Z}_q^{(K+T) \times W}$ $\qquad f(x) = M \cdot x'$ $\leftarrow$ view x as randomness for discrete Gaussian

LOSSY MODE

$f \rightsquigarrow \begin{pmatrix} M_1 \\ S \cdot M_1 + E \end{pmatrix}$ $\qquad M_1 \xleftarrow{\$} \mathbb{Z}_q^{K \times W}$

$E \xleftarrow{\$} \chi^{T \times W}$

NI-CTE FROM LWE

$G = \mathbb{Z}_q^{K+T}$

$H = \{ (\underbrace{v_1}_{K}, \underbrace{v_2}_{T}) \mid v_2 = S \cdot v_1 \}$ $\quad S \xleftarrow{\$} \mathbb{Z}_q^{T \times K}$

secret

SURJECTIVE MODE

$f \rightsquigarrow M \xleftarrow{\$} \mathbb{Z}_q^{(K+T) \times W}$

$f(x) = M \cdot x'$ ← view x as randomness for discrete Gaussian

LOSSY MODE

$f \rightsquigarrow \begin{pmatrix} M_1 \\ S \cdot M_1 + E \end{pmatrix}$ $\quad \begin{array}{l} M_1 \xleftarrow{\$} \mathbb{Z}_q^{K \times W} \\ E \xleftarrow{\$} \chi^{T \times W} \end{array}$ ← looks random under LWE

NI-CTE FROM LWE

$$G = \mathbb{Z}_q^{K+T} \qquad H = \{(\underbrace{v_1}_{K}, \underbrace{v_2}_{T}) \mid v_2 = S \cdot v_1\} \qquad S \xleftarrow{\$} \mathbb{Z}_q^{T \times K}$$

secret

SURJECTIVE MODE

$$f \rightsquigarrow M \xleftarrow{\$} \mathbb{Z}_q^{(K+T) \times W} \qquad f(x) = M \cdot x'$$

view x as randomness for discrete Gaussian

LOSSY MODE

$$f \rightsquigarrow \begin{pmatrix} M_1 \\ S \cdot M_1 + E \end{pmatrix} \qquad M_1 \xleftarrow{\$} \mathbb{Z}_q^{K \times W} \qquad E \xleftarrow{\$} \chi^{T \times W}$$

looks random under LWE

close to H

$$f(x) = \begin{pmatrix} M_1 \cdot x' \\ S \cdot M_1 \cdot x' + E \cdot x' \end{pmatrix} \approx \begin{pmatrix} y_1 \\ S \cdot y_1 \end{pmatrix} \qquad y_1 := M_1 \cdot x'$$

NI-CTE FROM LWE

$$\boxed{\text{Output } \underbrace{f_A(x_A)}_{\text{random in } G} + \underbrace{f_B(x_B)}_{\text{close to } H} + \underbrace{\alpha \cdot h}_{\text{random in } H}}$$

$$H = \{ (v_1, v_2) \in \underbrace{\mathbb{Z}_q^{K}}_{\text{not cyclic}} \times \mathbb{Z}_q^{T} \mid v_2 = S \cdot v_1 \}$$

NI-CTE FROM LWE

$$\boxed{\text{Output } f_A(x_A) + f_B(x_B) + \alpha \cdot h}$$

random in G   close to H   random in H

$$H = \{ (v_1, v_2) \in \mathbb{Z}_q^k \times \mathbb{Z}_q^T \mid v_2 = S \cdot v_1 \}$$

not cyclic

PROBLEM:

how to sample at random in H ?

NI-CTE FROM LWE

$$\boxed{\text{Output} \quad f_A(x_A) + f_B(x_B) + D\cdot e}$$

random in G — close to H — close to random element in H

$\mathcal{F}_n \xrightarrow{\$} f_A, f_B, D, e$

$$H = \{ (v_1, v_2) \in \mathbb{Z}_q^K \times \mathbb{Z}_q^T \mid v_2 = S \cdot v_1 \}$$

not cyclic

PROBLEM:

how to sample at random in H?

Let $\mathcal{F}_n$ give $\sim K \cdot \log q$ vectors close to H (matrix D) and gaussian vector e. Output $D\cdot e$ ← close to random element in H

NB: $|e| \ll$ output size

$K \log q \ll (K+T) \log q$

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?

  Round down the last τ entries of the output

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?

  Round down the last τ entries of the output

- the stretch is negative!

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?
  Round down the last T entries of the output
- the stretch is negative!
  Run the protocol L times reusing f_A, f_B and D!

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?
  Round down the last T entries of the output
- the stretch is negative!
  Run the protocol L times reusing f_A, f_B and D!
  [$\mathcal{I}_n$ needs to generate L gaussian vectors $e_1, \dots, e_L \sim L \cdot K \cdot \log q$ bits.
  ALL GOOD: the output is $L \cdot (K+T) \cdot \log q$ bits!]

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?
  Round down the last T entries of the output
- the stretch is negative!
  Run the protocol L times reusing δ_A, δ_B and D!
  [$\mathcal{F}_m$ needs to generate L gaussian vectors $e_1, \dots, e_L \sim L \cdot K \cdot \log q$ bits.
  ALL GOOD: the output is $L \cdot (K+T) \cdot \log q$ bits!]
- the output of $\mathcal{F}_m$ is linear in #parties N!

NI-CTE FROM LWE

OTHER PROBLEMS:

- how to deal with the noise?
  Round down the last T entries of the output
- the stretch is negative!
  Run the protocol L times reusing f_A, f_B and D!
  [$\mathcal{F}_n$ needs to generate L gaussian vectors $e_1, \dots, e_L \sim L \cdot K \cdot \log q$ bits.
  ALL GOOD: the output is $L \cdot (K+T) \cdot \log q$ bits!]
- the output of $\mathcal{F}_n$ is linear in #parties N!
  Using GSW13-based techniques, we can make it $O(\log N)$!

SUMMARY

MAGIC BUTTON

$\tilde{\mathcal{F}}_{\omega(\log\lambda)}$

ASSUMPTION	OUTPUT FUNCTIONALITY	# ROUNDS	MODEL	ADAPTIVE CORRUPTION
OWF	any m $r \xleftarrow{\$} \{0,1\}^m$	$O(\#\text{parties})$	standalone	?
coin tossing with identifiable abort	any m $r \xleftarrow{\$} \{0,1\}^m$	$O(\#\text{parties})$	it depends...	it depends...
DDH / Paillier / class groups	any m $r \xleftarrow{\$} \{0,1\}^m$	1	UC + reusable CRS	NO
LWE with $\omega(\lambda^{\log\lambda})$ modulus-noise ratio	any m $r \xleftarrow{\$} \{0,1\}^m$	1	UC	YES
iO + indistinguishability preserving distributed samplers	$R \xleftarrow{\$} D(1^\lambda)$	1	UC + reusable CRS	NO

LOWER BOUND: R-round statistical CTE with black-box simulation has $O(R \cdot \log\lambda)$ stretch!

EXPLAINABLE EXTRACTOR: for entropy sources $S(1^\lambda) \xrightarrow{\$} (x_1, \ldots, x_n)$

$\exists i$, PPT $\mathcal{A}$ s.t. $x_i \xleftarrow{\$} \{0,1\}^L$, $(x_j)_{j \neq i} \xleftarrow{\$} \mathcal{A}(1^\lambda, x_i)$