Attribute-Based Encryption for Circuits of Unbounded Depth from Lattices

謝耀慶
(Yao-Ching Hsieh)

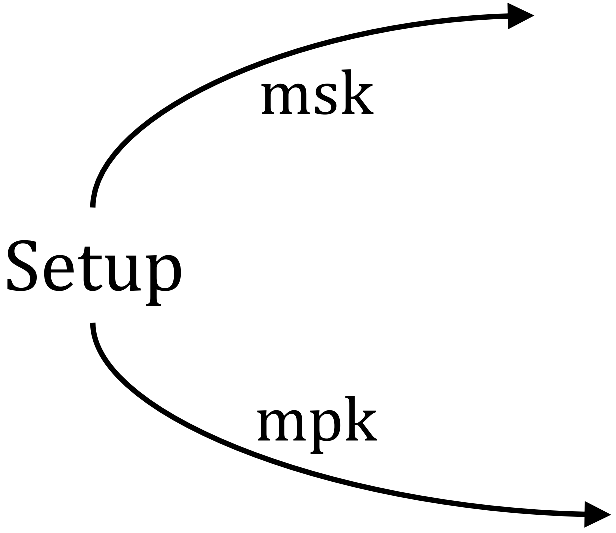
Rachel Lin

罗辑
(Ji Luo)

UNIVERSITY *of* WASHINGTON

Attribute-Based Encryption [GPSW]

Attribute-Based Encryption [GPSW]

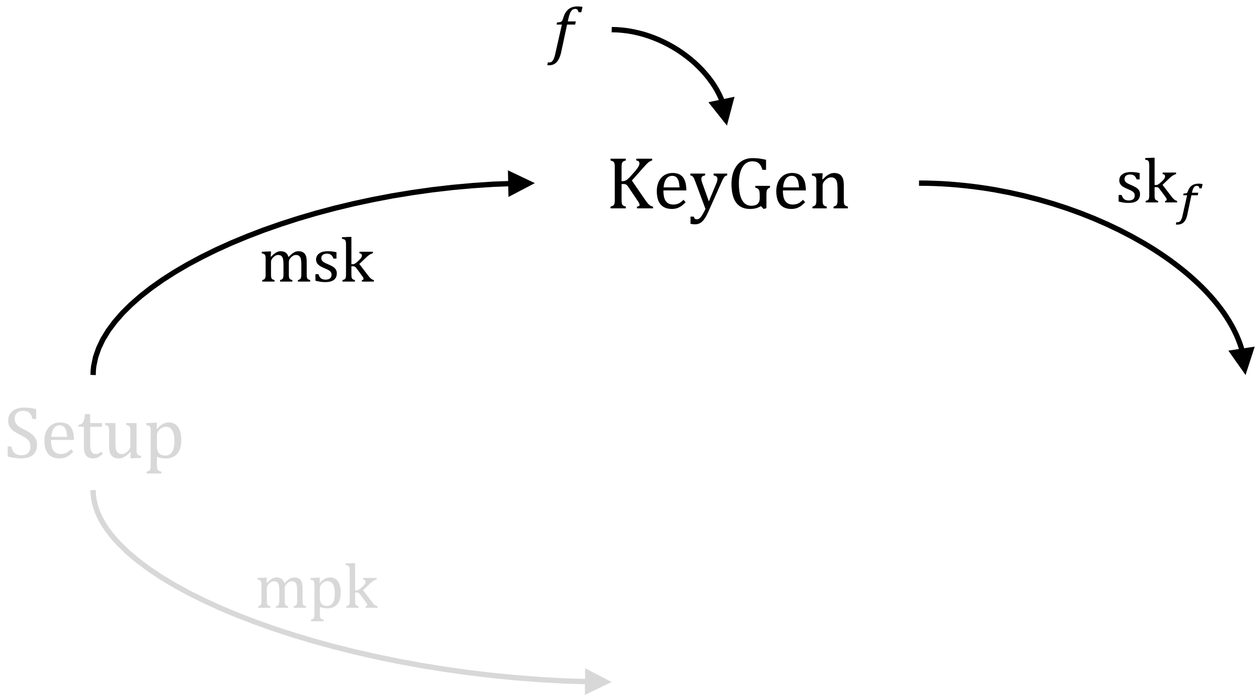


msk

Setup

mpk

Attribute-Based Encryption [GPSW]



f

KeyGen

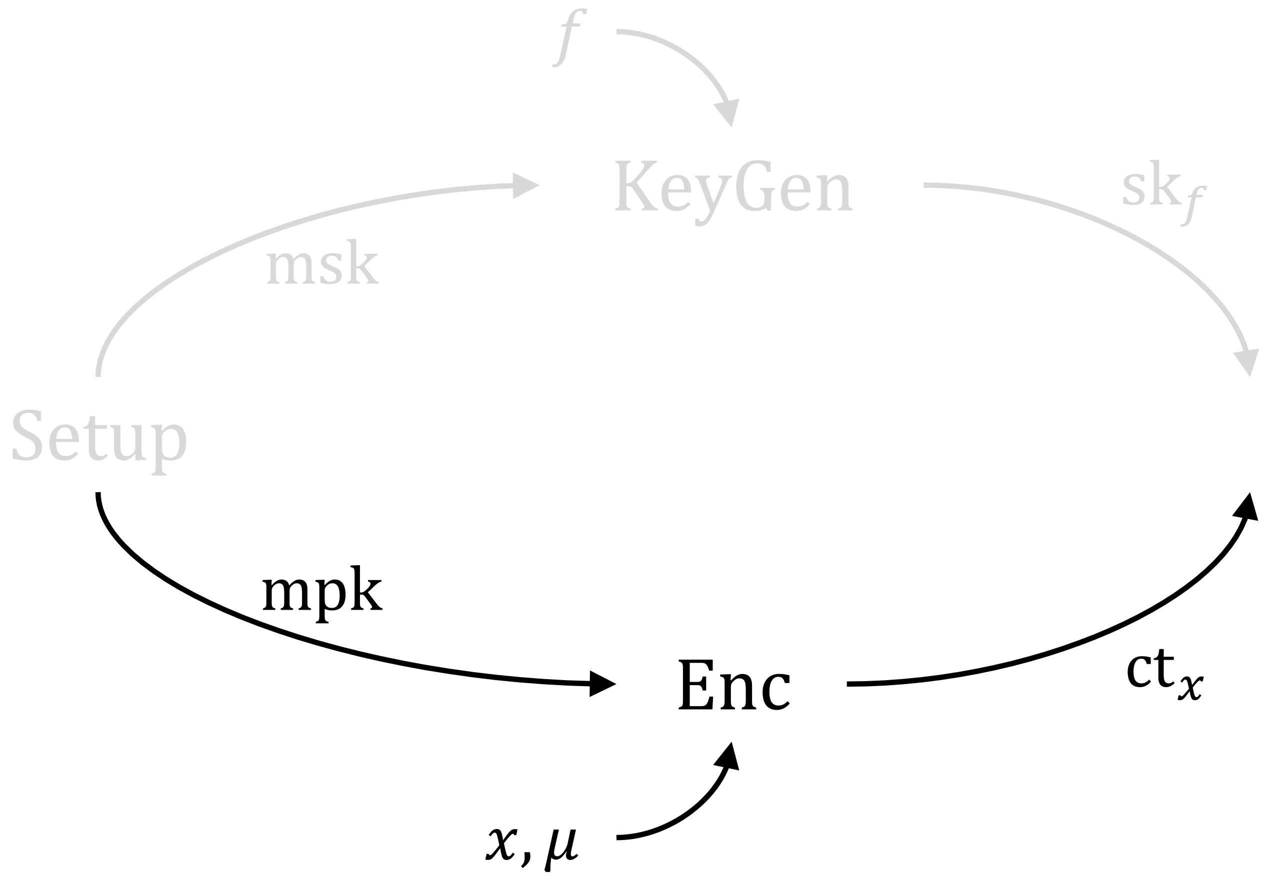
sk_f

msk

Setup

mpk

Attribute-Based Encryption [GPSW]



f

KeyGen

sk_f

msk

Setup

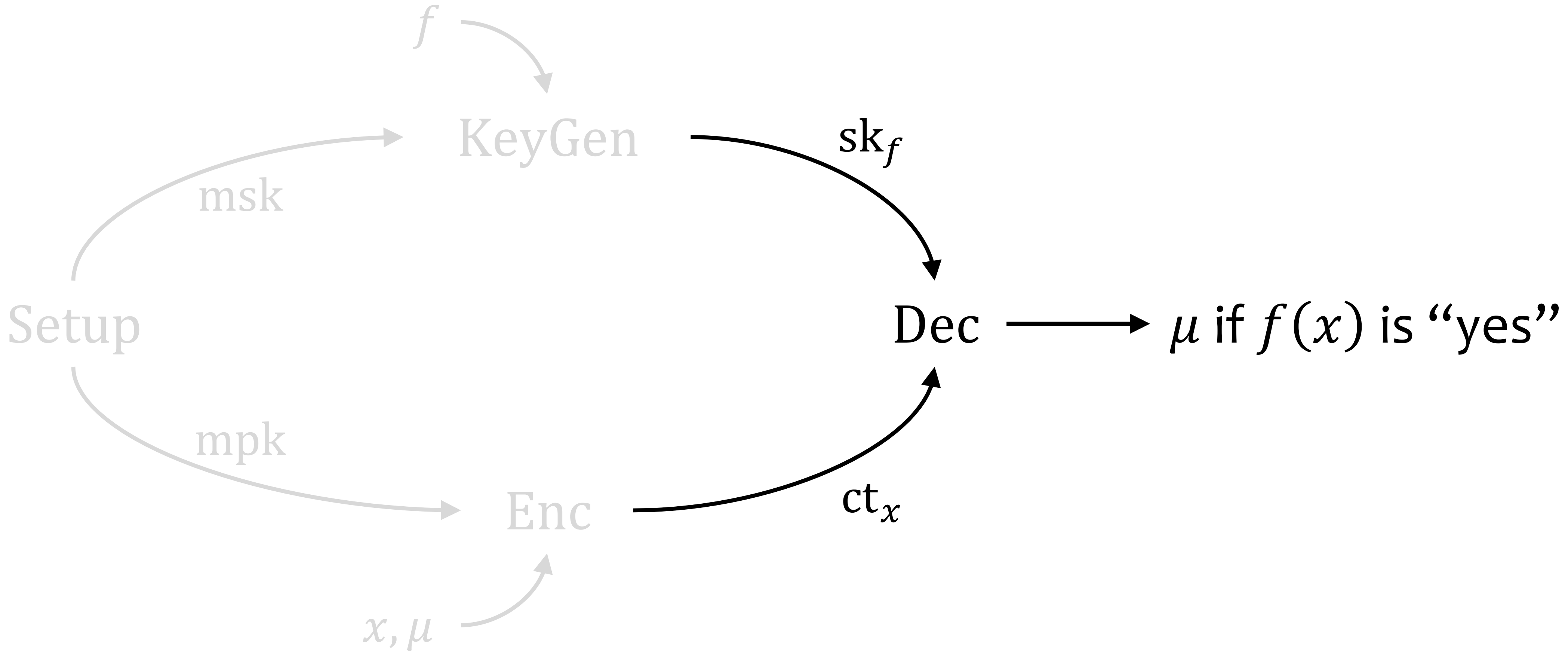
mpk

Enc

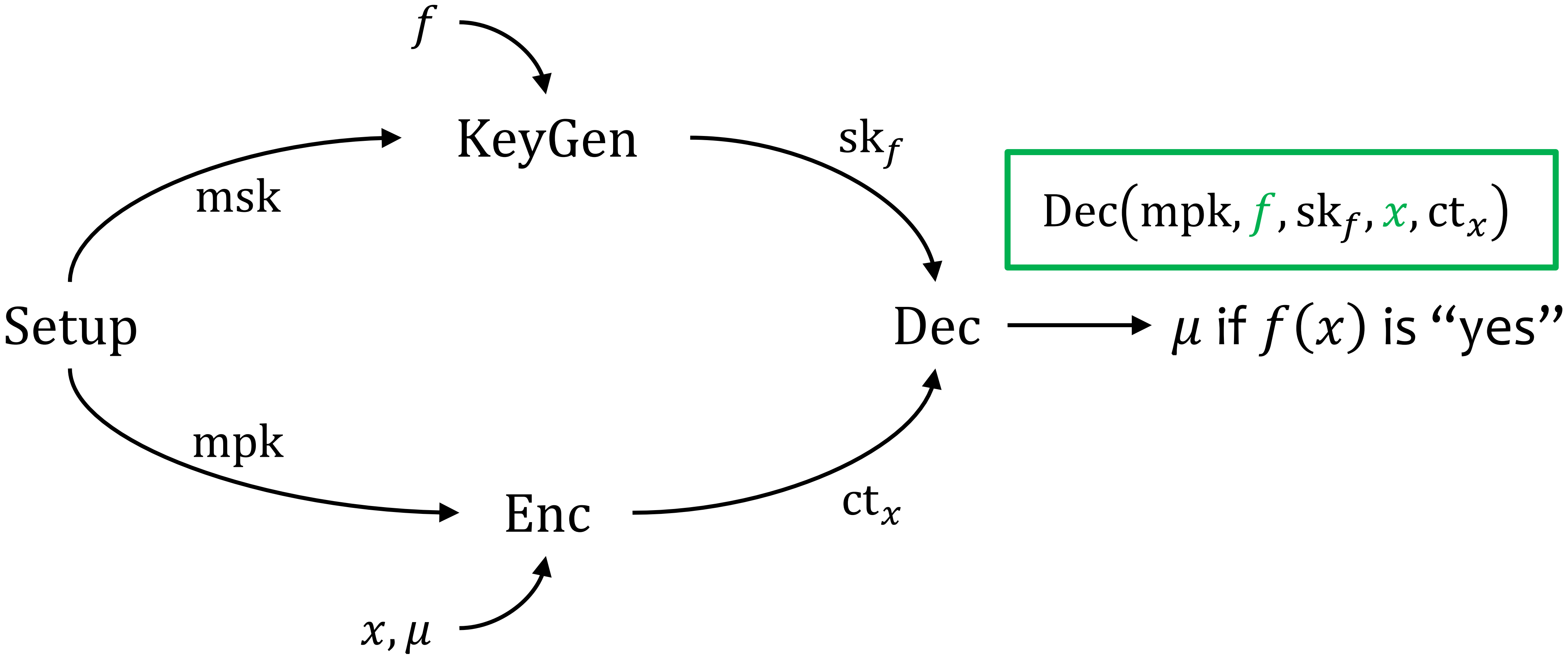
ct_x

x, μ

Attribute-Based Encryption [GPSW]



Attribute-Based Encryption [GPSW]



f

KeyGen

sk_f

msk

Setup

Dec

μ if $f(x)$ is “yes”

$\mathrm{Dec}(\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x)$

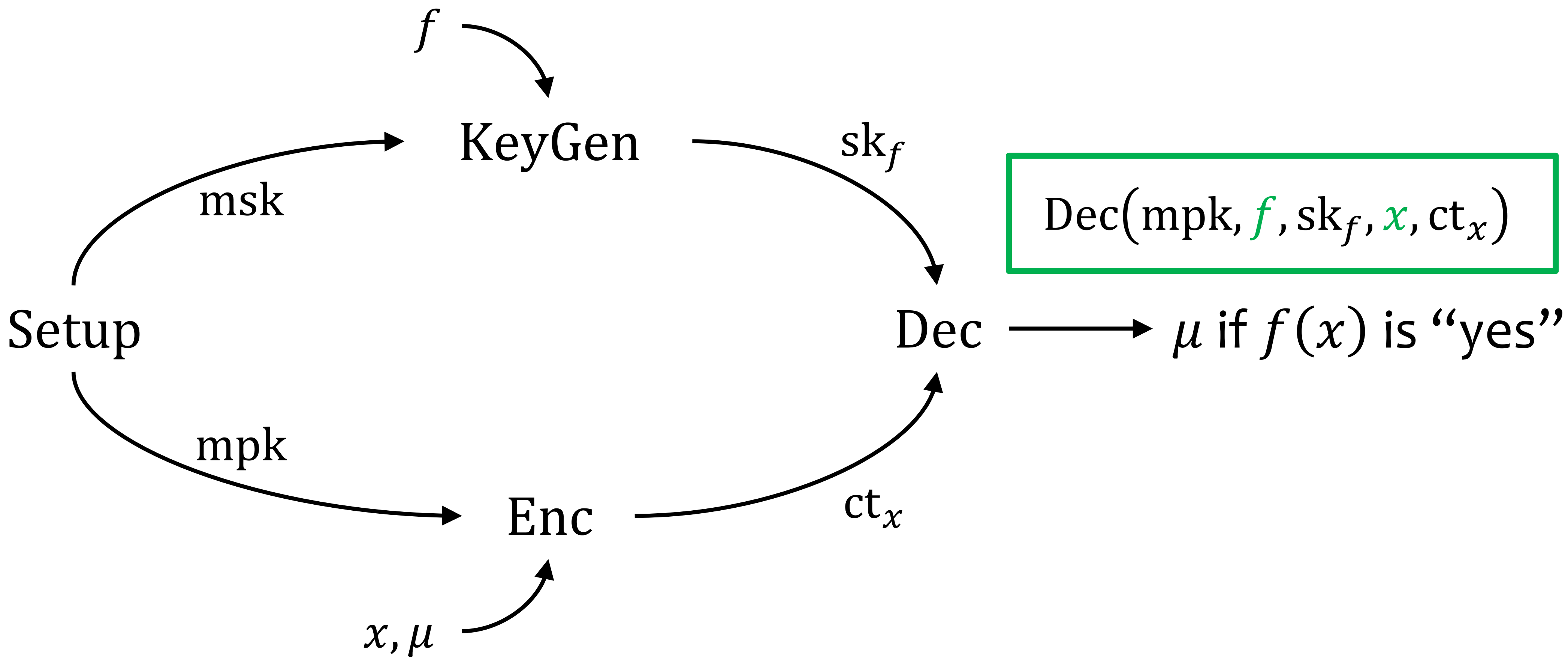
mpk

Enc

ct_x

x, μ

Attribute-Based Encryption [GPSW]



f

KeyGen

sk_f

msk

$\mathrm{Dec}\big(\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x\big)$

Setup

Dec

μ if $f(x)$ is “yes”

mpk

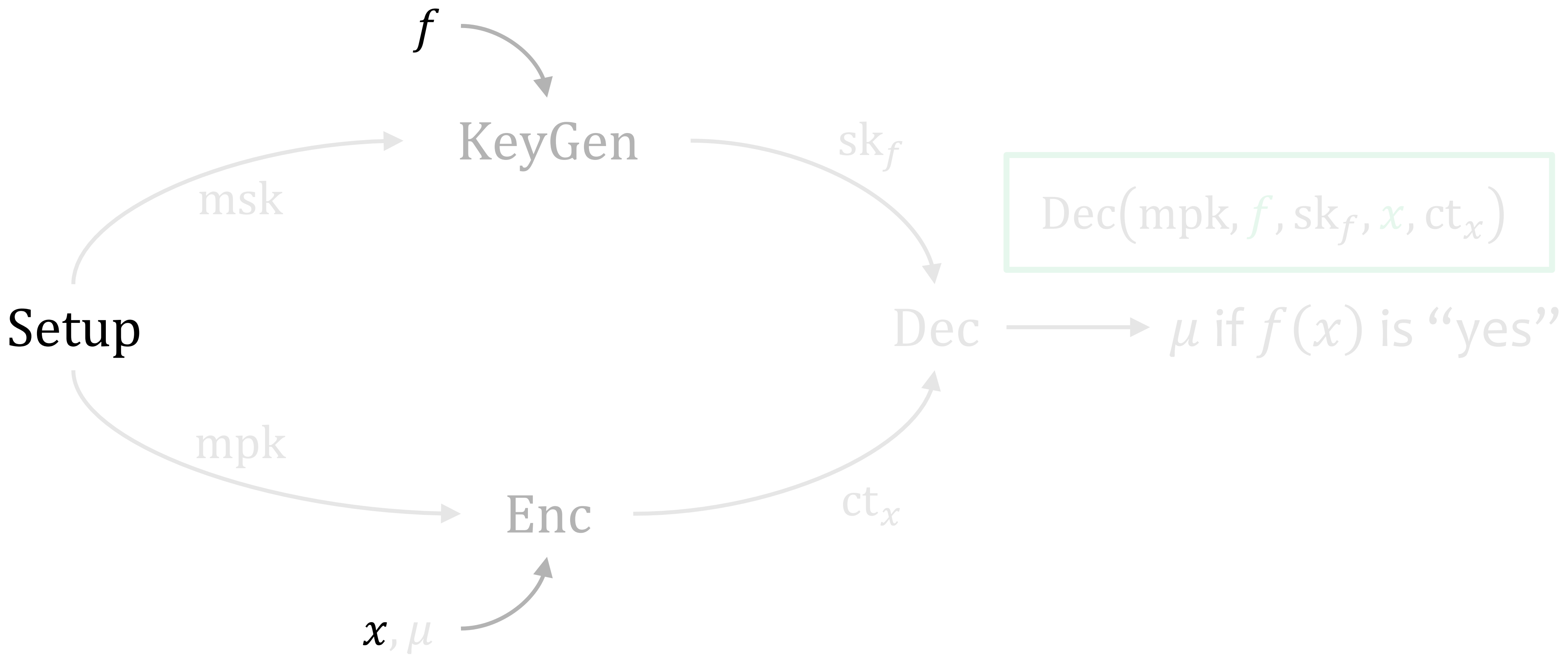
Enc

ct_x

x, μ

Security. $\mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(0) \approx \mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Bounded and Unbounded



f

KeyGen

msk

sk_f

$\boxed{\text{Dec}(\text{mpk}, f, \text{sk}_f, x, \text{ct}_x)}$

Setup

Dec $\longrightarrow$ μ if $f(x)$ is "yes"

mpk

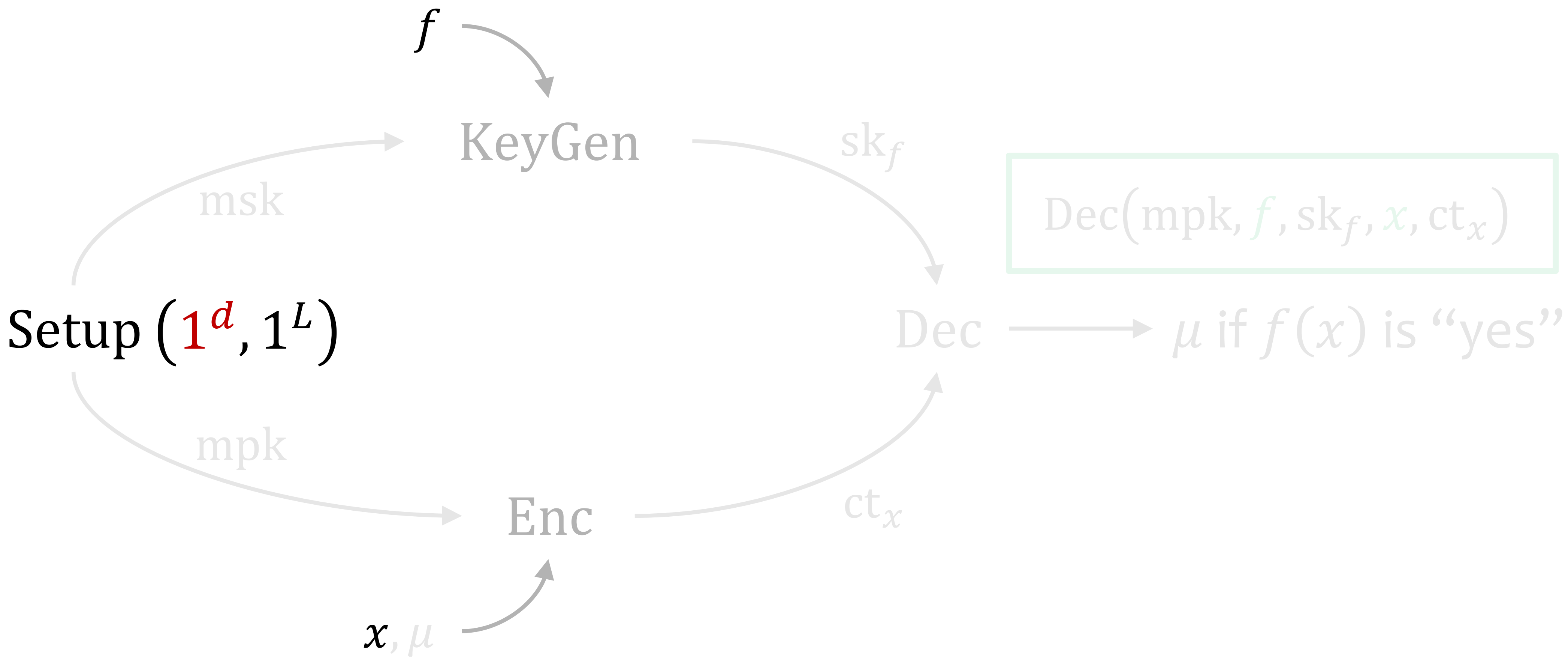
Enc

ct_x

x, μ

Security. $\text{mpk}, \{\text{sk}_j\}_{j\in[J]}, \text{ct}_x(0) \approx \text{mpk}, \{\text{sk}_j\}_{j\in[J]}, \text{ct}_x(1)$ if $f_j(x)$ is "no" for all $j \in [J]$

Bounded and Unbounded



f

KeyGen

sk_f

msk

$\mathsf{Dec}(\mathsf{mpk}, f, \mathsf{sk}_f, x, \mathsf{ct}_x)$

$\mathsf{Setup}\left(1^d, 1^L\right)$

Dec

μ if $f(x)$ is “yes”

mpk

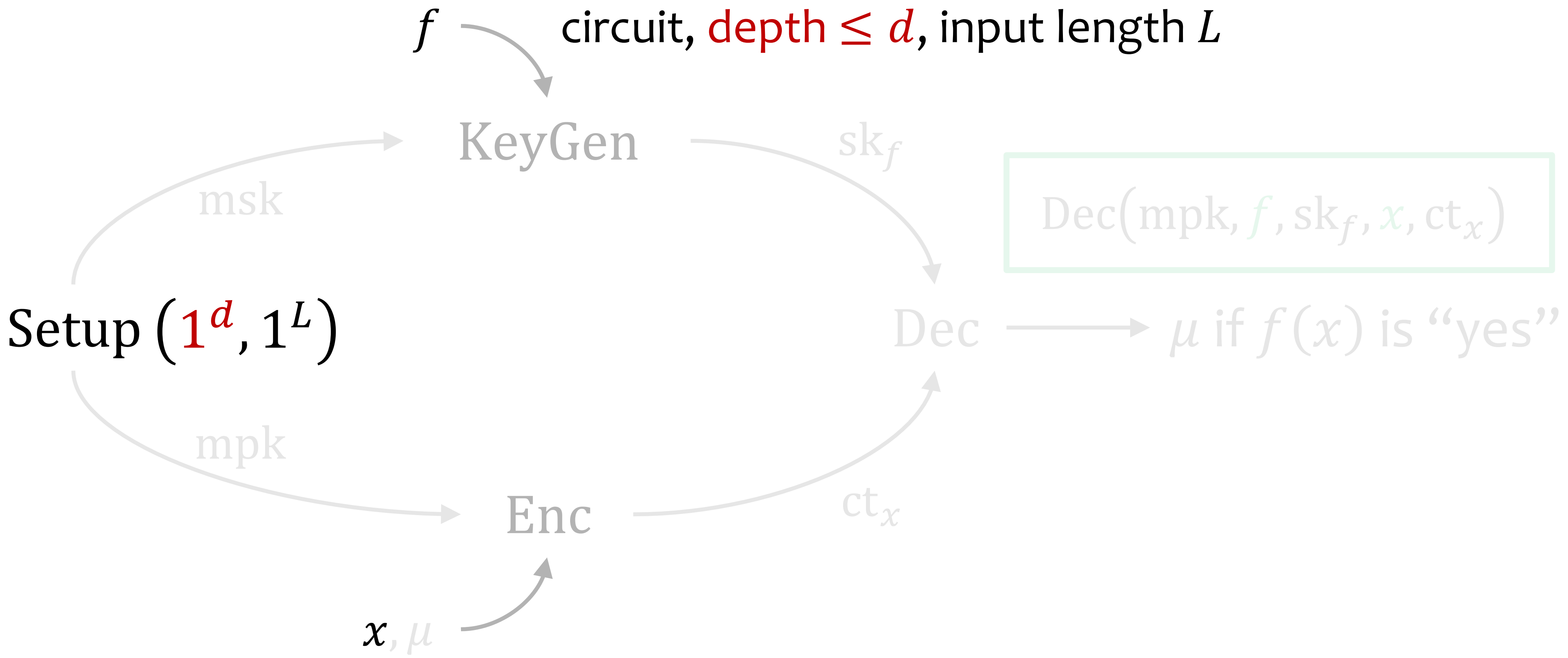
Enc

ct_x

x, μ

Security. $\mathsf{mpk}, \{\mathsf{sk}_j\}_{j\in[J]}, \mathsf{ct}_x(0) \approx \mathsf{mpk}, \{\mathsf{sk}_j\}_{j\in[J]}, \mathsf{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Bounded and Unbounded



f circuit, depth $\leq d$, input length L

KeyGen

msk

sk_f

$\mathrm{Dec}(\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x)$

$\mathrm{Setup}\left(1^d, 1^L\right)$

Dec

μ if $f(x)$ is “yes”

mpk

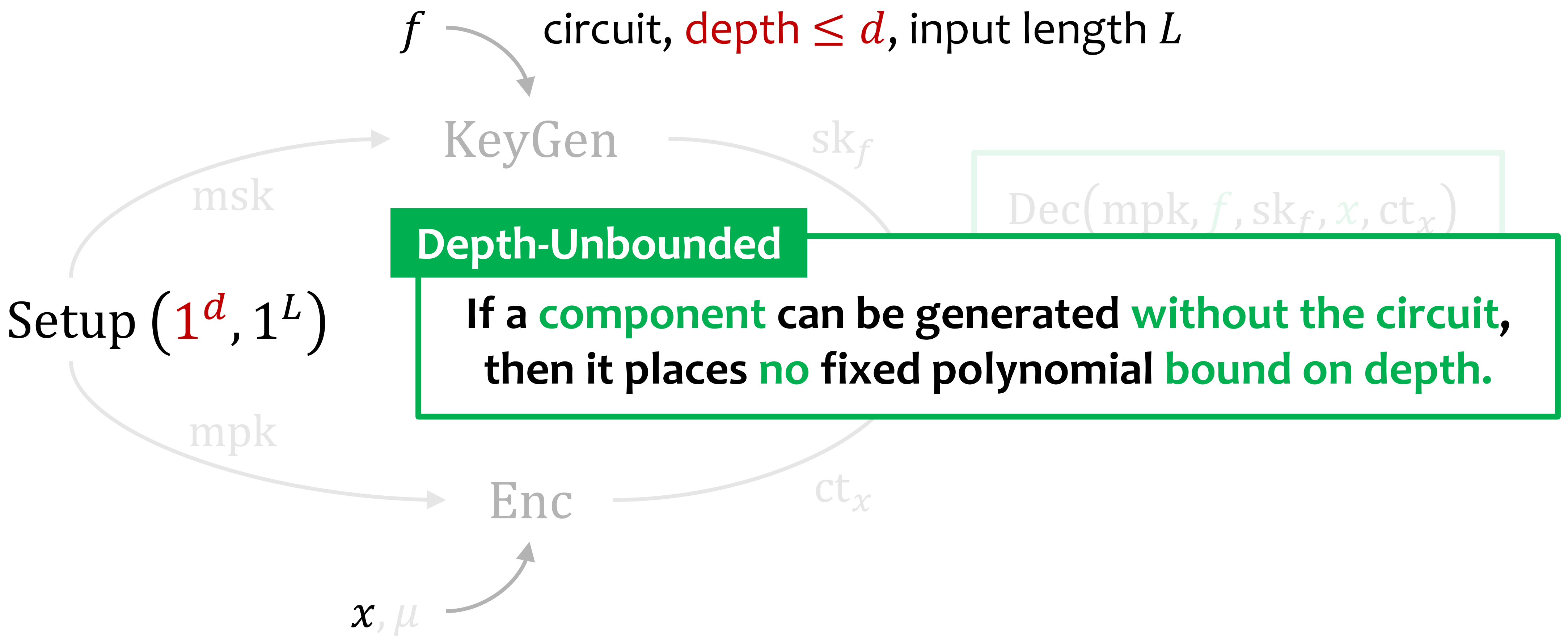
Enc

ct_x

x, μ

Security. $\mathrm{mpk}, \{\mathrm{sk}_j\}_{j \in [J]}, \mathrm{ct}_x(0) \approx \mathrm{mpk}, \{\mathrm{sk}_j\}_{j \in [J]}, \mathrm{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Bounded and Unbounded



f circuit, depth $\leq d$, input length L

KeyGen

sk_f

$\mathrm{Dec}(\mathsf{mpk}, f, \mathsf{sk}_f, x, \mathsf{ct}_x)$

msk

Setup $(1^d, 1^L)$

mpk

Enc

ct_x

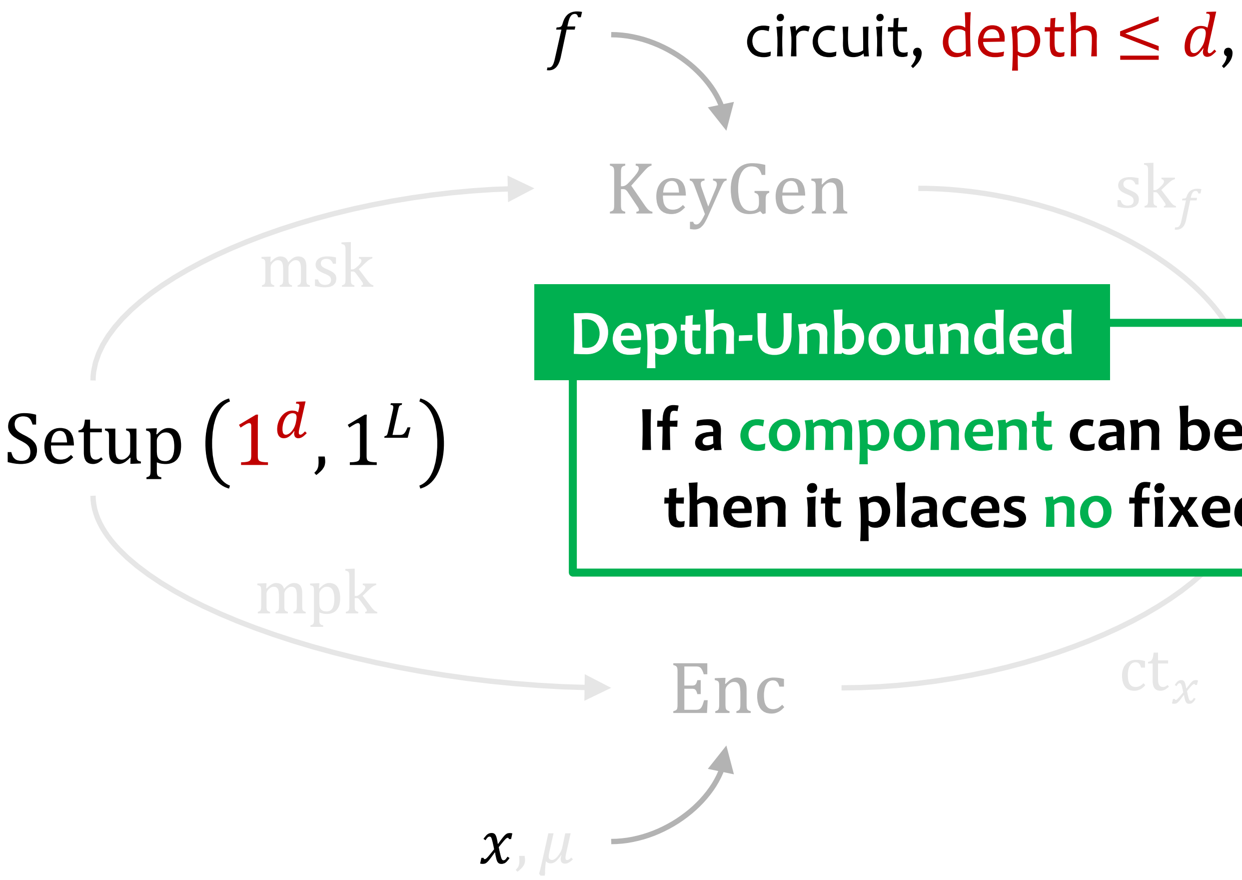
x, μ

Depth-Unbounded

If a component can be generated without the circuit, then it places no fixed polynomial bound on depth.

Security. $\mathsf{mpk}, \{\mathsf{sk}_j\}_{j\in[J]}, \mathsf{ct}_x(0) \approx \mathsf{mpk}, \{\mathsf{sk}_j\}_{j\in[J]}, \mathsf{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Bounded and Unbounded



f circuit, depth $\leq d$, input length L

KeyGen

msk

sk_f

Setup $(1^d, 1^L)$

mpk

Enc

ct_x

x, μ

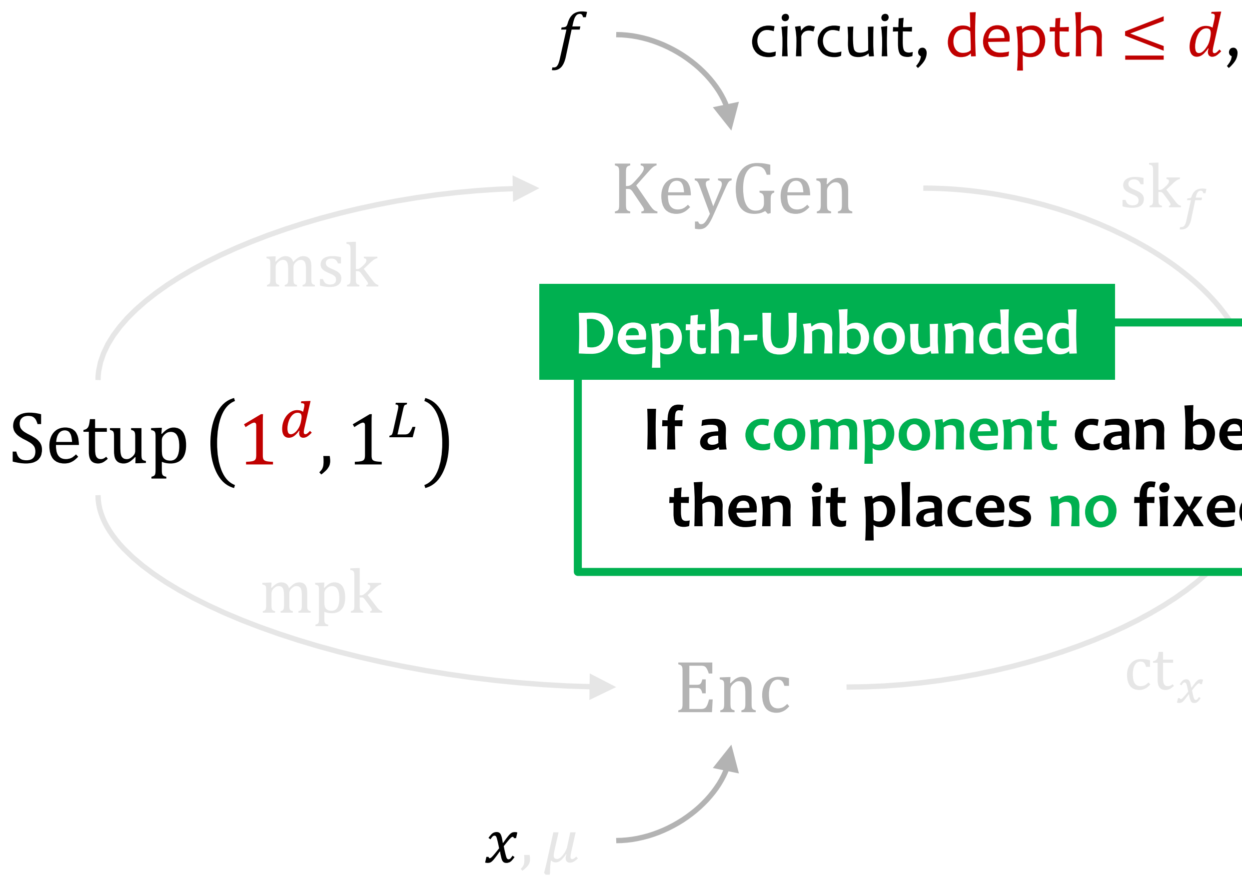
cf. non-leveled FHE

Depth-Unbounded

If a component can be generated without the circuit, then it places no fixed polynomial bound on depth.

Security. $\mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(0) \approx \mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Bounded and Unbounded


f circuit, depth $\leq d$, input length L

KeyGen

sk_f

msk

Setup $(1^d, 1^L)$

mpk

Enc

ct_x

x, μ

cf. non-leveled FHE

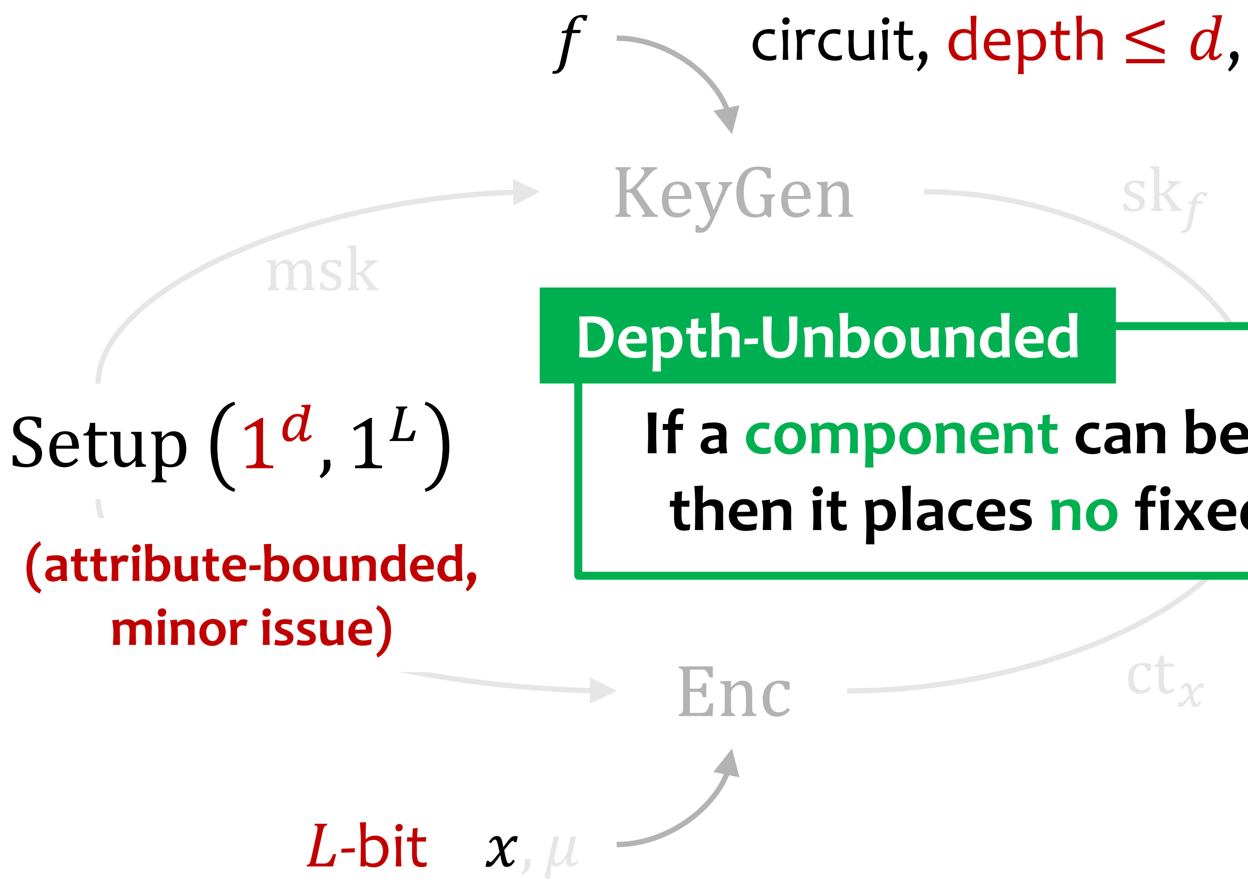
Depth-Unbounded

If a component can be generated without the circuit, then it places no fixed polynomial bound on depth.

concept **separate** from whether size grows with d

Security. $\mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(0) \approx \mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Bounded and Unbounded



cf. non-leveled FHE

Depth-Unbounded

If a component can be generated without the circuit, then it places no fixed polynomial bound on depth.

concept **separate** from whether size grows with d

Security. $\mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(0) \approx \mathrm{mpk}, \{\mathrm{sk}_j\}_{j\in[J]}, \mathrm{ct}_x(1)$ if $f_j(x)$ is “no” for all $j \in [J]$

Old Landscape of Lattice-Based Schemes

depth-unbounded

depth-independent component sizes

Old Landscape of Lattice-Based Schemes

depth-unbounded	**depth-independent component sizes**
✓ FHE – circular LWE [G, BV, GSW]	✓

Old Landscape of Lattice-Based Schemes

	depth-unbounded	**depth-independent component sizes**
✓	FHE – circular LWE [G, BV, GSW]	✓
✗	ABE – even 1-key	
✗	predicate encryption	
✗	constrained PRF	
✗	homomorphic signatures	
✗	laconic function evaluation	
✗	1-key functional encryption	

Old Landscape of Lattice-Based Schemes

depth-unbounded	**depth-independent component sizes**
✓ FHE – circular LWE [G, BV, GSW]	✓
✗ ABE – even 1-key	
✗ predicate encryption	
✗ constrained PRF	
✗ homomorphic signatures	
✗ laconic function evaluation	
✗ 1-key functional encryption	✗ pk of reusable garbling

Old Landscape of Lattice-Based Schemes

depth-unbounded	depth-independent component sizes
✓ FHE – circular LWE [G, BV, GSW]	✓
✗ ABE – even 1-key	sk – [CW] or with pairing [LLL]
✗ predicate encryption	
✗ constrained PRF	
✗ homomorphic signatures	
✗ laconic function evaluation	
✗ 1-key functional encryption	✗ pk of reusable garbling

Old Landscape of Lattice-Based Schemes

depth-unbounded	depth-independent component sizes
✓ FHE – circular LWE [G, BV, GSW]	✓
✗ ABE – even 1-key	sk – [CW] or with pairing [LLL]
✗ predicate encryption	
✗ constrained PRF	
✗ homomorphic signatures	
✗ laconic function evaluation	**was only salvaged in obfustopia [. . . , KNTY, JLL, DGM]**
✗ 1-key functional encryption	✗ pk of reusable garbling

Old Landscape of Lattice-Based Schemes

	depth-unbounded		**depth-independent component sizes**
✓	FHE – circular LWE [G, BV, GSW]	✓	
✗	ABE – even 1-key		sk – [CW] or with pairing [LLL]
✗	predicate encryption		
✗	constrained PRF		
✗	homomorphic signatures		
✗	laconic function evaluation		
✗	1-key functional encryption	✗	pk of reusable garbling

Despite connections to [GSW] homomorphic structures!

was only salvaged in obfustopia [. . . , KNTY, JLL, DGM]

Results (Unbounded, Bounded, Efficiency Improvement)

Results (Unbounded, Bounded, Efficiency Improvement)

from circular security:

LFE:

$$|\mathrm{crs}| = O(L),\ |\mathrm{digest}_C| = O(1),\ T_{\mathrm{Enc}} = O(L)$$

Results (Unbounded, Bounded, Efficiency Improvement)

from circular security: **previous**

LFE:

$|\mathrm{crs}| = O(L),\ |\mathrm{digest}_C| = O(1),\ T_{\mathrm{Enc}} = O(L)$

$i\mathcal{O}$: $O(1)$

LWE: $d^{\Theta(1)}$

Results (Unbounded, Bounded, Efficiency Improvement)

from circular security: **previous**

LFE: $i\mathcal{O}$: $O(1)$

$|\mathrm{crs}| = O(L),\ |\mathrm{digest}_C| = O(1),\ T_{\mathrm{Enc}} = O(L)$ LWE: $d^{\Theta(1)}$

1-key FE for $\{0,1\}^L \to \{0,1\}^{L'}$: (sel. sim.-secure) $i\mathcal{O}$: $O(1) + L'$

$|\mathrm{mpk}|, |\mathrm{ct}| = O(L + L'),\ |\mathrm{sk}_C| = O(L')$ LWE: $d^{\Theta(1)} \cdot L'$

Results (Unbounded, Bounded, Efficiency Improvement)

from circular security: **previous**

LFE: $i\mathcal{O}$: $O(1)$
$|\mathrm{crs}| = O(L),\ |\mathrm{digest}_C| = O(1),\ T_{\mathrm{Enc}} = O(L)$ LWE: $d^{\Theta(1)}$

1-key FE for $\{0,1\}^L \to \{0,1\}^{L'}$: (sel. sim.-secure) $i\mathcal{O}$: $O(1) + L'$
$|\mathrm{mpk}|, |\mathrm{ct}| = O(L + L'),\ |\mathrm{sk}_C| = O(L')$ LWE: $d^{\Theta(1)} \cdot L'$

reusable garbled circuits: (hides x, not C) $i\mathcal{O}$: $O(1)$
$|\hat{C}| = O(1),\ |\mathrm{pk}|, |\hat{x}| = O(L)$ LWE: $d^{\Theta(1)}$

Results (Unbounded, Bounded, Efficiency Improvement)

from circular security: **previous**

LFE:
$|\mathrm{crs}| = O(L),\ |\mathrm{digest}_C| = O(1),\ T_{\mathrm{Enc}} = O(L)$

$i\mathcal{O}$: $O(1)$
LWE: $d^{\Theta(1)}$

1-key FE for $\{0,1\}^L \to \{0,1\}^{L'}$: (sel. sim.-secure)
$|\mathrm{mpk}|, |\mathrm{ct}| = O(L + L'),\ |\mathrm{sk}_C| = O(L')$

$i\mathcal{O}$: $O(1) + L'$
LWE: $d^{\Theta(1)} \cdot L'$

reusable garbled circuits: (hides x, not C)
$|\hat{C}| = O(1),\ |\mathrm{pk}|, |\hat{x}| = O(L)$

$i\mathcal{O}$: $O(1)$
LWE: $d^{\Theta(1)}$

plus variant of evasive LWE:

KP-ABE:
$|\mathrm{mpk}|, |\mathrm{ct}| = O(L),\ \mathrm{sk}_C = O(1)$

$i\mathcal{O}$: $|\mathrm{mpk}|, |\mathrm{ct}|, |\mathrm{sk}| = O(1)$
LWE: $|\mathrm{mpk}|, |\mathrm{ct}| = d^{\Theta(1)} \cdot L$
$|\mathrm{sk}| = O(1)$

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is **small Gaussian** and **encrypted bit-by-bit**.

(roughly speaking)

Circular Small-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is
(roughly speaking) **small Gaussian** and **encrypted bit-by-bit**.

$$\overline{\boldsymbol{A}}_{\mathrm{fhe}} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\mathrm{fhe}} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{m}$$

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is
(roughly speaking) **small Gaussian** and **encrypted bit-by-bit**.

$$\overline{\boldsymbol{A}}_{\text{fhe}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\text{fhe}} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^{m}$$

$$\boldsymbol{A}_{\text{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\text{fhe}} \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}_{\text{fhe}} + \boldsymbol{e}_{\text{fhe}}^{\top} \end{pmatrix},$$

[GSW] public key

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is
(roughly speaking) **small Gaussian** and **encrypted bit-by-bit**.

$$\overline{\boldsymbol{A}}_{\mathrm{fhe}} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\mathrm{fhe}} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{m} \qquad \boldsymbol{s} \leftarrow (\boldsymbol{r}^{\top}, -1)^{\top}$$

$$\boldsymbol{R} \overset{\$}{\leftarrow} \{0,1\}^{m\times \mathrm{len}(\boldsymbol{s})m}$$

$$\boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^{\top} \end{pmatrix},$$

[GSW] public key

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is **small Gaussian** and **encrypted bit-by-bit**.

(roughly speaking)

$$\overline{\boldsymbol{A}}_{\text{fhe}} \xleftarrow{\$} \mathbb{Z}_q^{n \times m} \qquad \boldsymbol{r} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\text{fhe}} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^{m} \qquad \boldsymbol{s} \leftarrow (\boldsymbol{r}^{\top}, -1)^{\top}$$

$$\boldsymbol{R} \xleftarrow{\$} \{0,1\}^{m \times \text{len}(\boldsymbol{s})m}$$

$$\boldsymbol{A}_{\text{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\text{fhe}} \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}_{\text{fhe}} + \boldsymbol{e}_{\text{fhe}}^{\top} \end{pmatrix}, \quad \boldsymbol{S} = \boldsymbol{A}_{\text{fhe}}\boldsymbol{R} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G},$$

[GSW] public key

circular ciphertext

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is **small Gaussian** and **encrypted bit-by-bit**.

(roughly speaking)

$$\overline{\boldsymbol{A}}_{\mathrm{fhe}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\mathrm{fhe}} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma}^{m} \qquad \boldsymbol{s} \leftarrow (\boldsymbol{r}^{\top}, -1)^{\top}$$

$$\overline{\boldsymbol{A}}' \xleftarrow{\$} \mathbb{Z}_q^{n\times m'} \qquad \boldsymbol{e}' \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},\sigma'}^{m'} \qquad \boldsymbol{R} \xleftarrow{\$} \{0,1\}^{m\times \mathrm{len}(\boldsymbol{s})m}$$

$$\boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^{\top} \end{pmatrix}, \quad \boldsymbol{S} = \boldsymbol{A}_{\mathrm{fhe}}\boldsymbol{R} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G}, \quad \begin{matrix} \overline{\boldsymbol{A}}', \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}' + (\boldsymbol{e}')^{\top} \end{matrix}$$

[GSW] public key **circular ciphertext** **extra LWE samples**

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is **small Gaussian** and **encrypted bit-by-bit**.

(roughly speaking)

$$\overline{\boldsymbol{A}}_{\text{fhe}} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\text{fhe}} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{m} \qquad \boldsymbol{s} \leftarrow (\boldsymbol{r}^\top, -1)^\top$$

$$\overline{\boldsymbol{A}}' \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m'} \qquad \boldsymbol{e}' \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma'}^{m'} \qquad \boldsymbol{R} \overset{\$}{\leftarrow} \{0,1\}^{m\times \text{len}(\boldsymbol{s})m}$$

$$\boldsymbol{A}_{\text{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\text{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\text{fhe}} + \boldsymbol{e}_{\text{fhe}}^\top \end{pmatrix}, \quad \boldsymbol{S} = \boldsymbol{A}_{\text{fhe}} \boldsymbol{R} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G}, \quad \begin{matrix} \overline{\boldsymbol{A}}', \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}' + (\boldsymbol{e}')^\top \end{matrix} \quad \approx \quad \$.$$

[GSW] public key **circular ciphertext** **extra LWE samples**

Circular **S**mall-Secret LWE

One-Liner. [GSW] FHE is **circularly secure** when secret key is
(roughly speaking) **small Gaussian** and **encrypted bit-by-bit**.

$$\overline{\boldsymbol{A}}_{\mathrm{fhe}} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\mathrm{fhe}} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{m} \qquad \boldsymbol{s} \leftarrow (\boldsymbol{r}^\top, -1)^\top$$

$$\overline{\boldsymbol{A}}' \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m'} \qquad \boldsymbol{e}' \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma'}^{m'} \qquad \boldsymbol{R} \overset{\$}{\leftarrow} \{0,1\}^{m\times \mathrm{len}(\boldsymbol{s})m}$$

Assume $q/\sigma, q/\sigma' \geq 2^{n^{\Omega(1)}}$ (though a certain $2^{\log^c n}$ suffices).

$$\boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^\top \end{pmatrix}, \quad \boldsymbol{S} = \boldsymbol{A}_{\mathrm{fhe}} \boldsymbol{R} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G}, \quad \begin{matrix} \overline{\boldsymbol{A}}', \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}' + (\boldsymbol{e}')^\top \end{matrix} \approx \$.$$

[GSW] public key **circular ciphertext** **extra LWE samples**

Circular **S**mall-Secret LWE

bootstraps [GSW] FHE

One-Liner. [GSW] FHE is **circularly secure** when secret key is
(roughly speaking) **small Gaussian** and **encrypted bit-by-bit**.

$$\overline{\boldsymbol{A}}_{\text{fhe}} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m} \qquad \boldsymbol{r} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{n} \qquad \boldsymbol{e}_{\text{fhe}} \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma}^{m} \qquad \boldsymbol{s} \leftarrow (\boldsymbol{r}^{\top}, -1)^{\top}$$

$$\overline{\boldsymbol{A}}' \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m'} \qquad \boldsymbol{e}' \overset{\$}{\leftarrow} \mathcal{D}_{\mathbb{Z},\sigma'}^{m'} \qquad \boldsymbol{R} \overset{\$}{\leftarrow} \{0,1\}^{m\times \text{len}(\boldsymbol{s})m}$$

Assume $q/\sigma\,, q/\sigma' \geq 2^{n^{\Omega(1)}}$ (though a certain $2^{\log^c n}$ suffices).

$$\boldsymbol{A}_{\text{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\text{fhe}} \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}_{\text{fhe}} + \boldsymbol{e}_{\text{fhe}}^{\top} \end{pmatrix}, \quad \boldsymbol{S} = \boldsymbol{A}_{\text{fhe}}\boldsymbol{R} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G}, \quad \begin{matrix} \overline{\boldsymbol{A}}', \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}' + (\boldsymbol{e}')^{\top} \end{matrix} \quad \approx \quad \$.$$

[GSW] public key — circular ciphertext — extra LWE samples

Evasive **C**ircular **S**mall-Secret LWE

One-Liner. Evasive LWE holds when
augmented with circular ciphertext and encoding.

Evasive **C**ircular **S**mall-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

Evasive **C**ircular **S**mall-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \overset{\$}{\leftarrow} \mathcal{S}$$

Evasive Circular Small-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \xleftarrow{\$} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \xleftarrow{\$} \mathrm{TrapGen}$$

Evasive Circular Small-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \xleftarrow{\$} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \xleftarrow{\$} \mathrm{TrapGen}$$

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top \overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top \boldsymbol{B}},\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \mathrm{aux}\ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \mathrm{aux}.$$

Evasive **C**ircular **S**mall-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \text{aux}) \xleftarrow{\$} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \xleftarrow{\$} \text{TrapGen}$$

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top \overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top \boldsymbol{B}},\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \text{aux} \ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \text{aux}.$$

〰 = noisy

Evasive Circular Small-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \xleftarrow{\$} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n \times m}, \tau_{\boldsymbol{B}}\right) \xleftarrow{\$} \mathrm{TrapGen}$$

low-norm K such that $BK = P$

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top \overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top \boldsymbol{B}},\ \boxed{\boldsymbol{B}^{-1}(\boldsymbol{P}),}\ \mathrm{aux} \ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \mathrm{aux}.$$

$\sim$ = noisy

Evasive **C**ircular **S**mall-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \xleftarrow{\$} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \xleftarrow{\$} \mathrm{TrapGen}$$

if

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top\overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top\boldsymbol{B}},\ \utilde{\boldsymbol{r}^\top\boldsymbol{P}},\ \mathrm{aux} \ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \$,\ \mathrm{aux}.$$

then

low-norm K such that $BK = P$

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top\overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top\boldsymbol{B}},\ \boxed{\boldsymbol{B}^{-1}(\boldsymbol{P})},\ \mathrm{aux} \ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \mathrm{aux}.$$

$\sim$ = noisy

Evasive **C**ircular **S**mall-Secret LWE

Recap

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \xleftarrow{\$} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \xleftarrow{\$} \mathrm{TrapGen}$$

if ❶ ≈ ❷

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top\overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top\boldsymbol{B}},\ \utilde{\boldsymbol{r}^\top\boldsymbol{P}},\ \mathrm{aux} \ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \$,\ \mathrm{aux}.$$

then ❸ ≈ ❹

low-norm K such that $BK = P$

$$\boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \utilde{\boldsymbol{r}^\top\overline{\boldsymbol{A}}'},\ \utilde{\boldsymbol{r}^\top\boldsymbol{B}},\ \boxed{\boldsymbol{B}^{-1}(\boldsymbol{P}),}\ \mathrm{aux} \ \approx\ \boldsymbol{B},\ \overline{\boldsymbol{A}}',\ \boldsymbol{P},\ \$,\ \$,\ \boldsymbol{B}^{-1}(\boldsymbol{P}),\ \mathrm{aux}.$$

$\sim$ = noisy

Evasive Circular Small-Secret LWE (cont'd)

One-Liner. Evasive LWE holds when
augmented with circular ciphertext and encoding.

$$(\boldsymbol{A}_{\mathrm{circ}}, \overline{\boldsymbol{A}}', \boldsymbol{P}, \mathrm{aux}) \overset{\$}{\leftarrow} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \overset{\$}{\leftarrow} \mathrm{TrapGen}$$

if

❶, $\approx$ ❷,

then

❸, $\approx$ ❹,

Evasive Circular Small-Secret LWE (cont'd)

One-Liner. Evasive LWE holds when augmented with circular ciphertext and encoding.

$$(\mathbf{A}_{\text{circ}}, \overline{\mathbf{A}}', \mathbf{P}, \text{aux}) \overset{\$}{\leftarrow} \mathcal{S} \qquad \left(\mathbf{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\mathbf{B}}\right) \overset{\$}{\leftarrow} \text{TrapGen} \qquad \overline{\mathbf{A}}_{\text{fhe}}, \mathbf{e}_{\text{fhe}}, \mathbf{R}$$

if

[GSW] public key,
circular ciphertext

❶, $\boxed{\mathbf{A}_{\text{fhe}}, \ \mathbf{S},}$ $\approx$ ❷,

then

❸, $\approx$ ❹,

Evasive Circular Small-Secret LWE (cont'd)

One-Liner. Evasive LWE holds when
augmented with circular ciphertext and encoding.

$$(\boldsymbol{A}_{\text{circ}}, \overline{\boldsymbol{A}}', \boldsymbol{P}, \text{aux}) \overset{\$}{\leftarrow} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \overset{\$}{\leftarrow} \text{TrapGen} \qquad \overline{\boldsymbol{A}}_{\text{fhe}}, \boldsymbol{e}_{\text{fhe}}, \boldsymbol{R}$$

if

[GSW] public key,
circular ciphertext

$$❶, \boxed{\boldsymbol{A}_{\text{fhe}}, \ \boldsymbol{S},} \ \boldsymbol{A}_{\text{circ}}, \ \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}_{\text{circular [BGG}^{+}\text{] encoding}} \approx ❷,$$

then

$$❸, \qquad \approx ❹,$$

Evasive Circular Small-Secret LWE (cont'd)

One-Liner. Evasive LWE holds when
augmented with circular ciphertext and encoding.

$$(\boldsymbol{A}_{\text{circ}}, \overline{\boldsymbol{A}}', \boldsymbol{P}, \text{aux}) \overset{\$}{\leftarrow} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \overset{\$}{\leftarrow} \text{TrapGen} \qquad \overline{\boldsymbol{A}}_{\text{fhe}}, \boldsymbol{e}_{\text{fhe}}, \boldsymbol{R}$$

if

[GSW] public key,
circular ciphertext

$$❶, \boxed{\boldsymbol{A}_{\text{fhe}}, \ \boldsymbol{S},} \ \boldsymbol{A}_{\text{circ}}, \ \boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}) \quad \approx \quad ❷, \ \$, \ \$, \ \boldsymbol{A}_{\text{circ}}, \ \$.$$

circular [BGG+] encoding

then

$$❸, \qquad \approx \quad ❹,$$

Evasive Circular Small-Secret LWE (cont'd)

One-Liner. Evasive LWE holds when
augmented with circular ciphertext and encoding.

$$(\boldsymbol{A}_{\text{circ}}, \overline{\boldsymbol{A}}', \boldsymbol{P}, \text{aux}) \overset{\$}{\leftarrow} \mathcal{S} \qquad \left(\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}, \tau_{\boldsymbol{B}}\right) \overset{\$}{\leftarrow} \text{TrapGen} \qquad \overline{\boldsymbol{A}}_{\text{fhe}}, \boldsymbol{e}_{\text{fhe}}, \boldsymbol{R}$$

if

[GSW] public key,
circular ciphertext

$$❶,\ \boxed{\boldsymbol{A}_{\text{fhe}},\ \ \boldsymbol{S},}\ \ \boldsymbol{A}_{\text{circ}},\ \ \underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})} \quad \approx \quad ❷,\ \ \$,\ \ \$,\ \ \boldsymbol{A}_{\text{circ}},\ \ \$.$$

circular [BGG+] encoding

then

$$❸,\ \boldsymbol{A}_{\text{fhe}},\ \ \boldsymbol{S},\ \ \boldsymbol{A}_{\text{circ}},\ \ \underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})} \quad \approx \quad ❹,\ \ \$,\ \ \$,\ \ \boldsymbol{A}_{\text{circ}},\ \ \$.$$

Unbounded Homomorphic Evaluation

Unbounded Homomorphic Evaluation

$$\boldsymbol{A}_{\text{attr}}, \boldsymbol{A}_{\text{circ}} \xrightarrow[C(\boldsymbol{x}) \in \{0,1\}]{\text{UEvalC}} \boldsymbol{A}_C$$

Unbounded Homomorphic Evaluation

$$\boldsymbol{A}_{\text{attr}}, \boldsymbol{A}_{\text{circ}} \xrightarrow[C(\boldsymbol{x}) \in \{0,1\}]{\text{UEvalC}} \boldsymbol{A}_C$$

$$\boldsymbol{c}_{\text{attr}}^{\top} = \underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{attr}} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G})}$$

$$\boldsymbol{c}_{\text{circ}}^{\top} = \underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$$

Unbounded Homomorphic Evaluation

$$\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}} \xrightarrow[C(\boldsymbol{x}) \in \{0,1\}]{\mathrm{UEvalC}} \boldsymbol{A}_C$$

$$\boldsymbol{c}_{\mathrm{attr}}^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G})}$$

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$$

$$\begin{matrix} \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \\ \boldsymbol{c}_{\mathrm{attr}}, \boldsymbol{c}_{\mathrm{circ}}, \\ \boldsymbol{x}, \boldsymbol{S} \end{matrix} \xrightarrow[\text{circuit } C]{\mathrm{UEvalCX}} \boldsymbol{c}_C^{\top}$$

Unbounded Homomorphic Evaluation

$$\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}} \xrightarrow[C(\boldsymbol{x}) \in \{0,1\}]{\mathrm{UEvalC}} \boldsymbol{A}_C$$

$$\boldsymbol{c}_{\mathrm{attr}}^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G})}$$

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$$

$$\begin{matrix} \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \\ \boldsymbol{c}_{\mathrm{attr}}, \boldsymbol{c}_{\mathrm{circ}}, \\ \boldsymbol{x}, \boldsymbol{S} \end{matrix} \xrightarrow[\text{circuit } C]{\mathrm{UEvalCX}} \boldsymbol{c}_C^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})}$$

(w.h.p.) ↑ noise magnitude
independent of depth of C

Unbounded Homomorphic Evaluation

$$\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}} \xrightarrow[C(\boldsymbol{x}) \in \{0,1\}]{\mathrm{UEvalC}} \boldsymbol{A}_C$$

$$\boldsymbol{c}_{\mathrm{attr}}^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G})}$$

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$$

LWE secret is **triply** used!

1. FHE key (in $\boldsymbol{S}$)
2. FHE plaintext (in $\boldsymbol{S}$)
3. encoding secret (in $\boldsymbol{c}$'s)

$$\begin{array}{c}\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \\ \boldsymbol{c}_{\mathrm{attr}}, \boldsymbol{c}_{\mathrm{circ}}, \\ \boldsymbol{x}, \boldsymbol{S}\end{array} \xrightarrow[\text{circuit } C]{\mathrm{UEvalCX}} \boldsymbol{c}_C^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})}$$

(w.h.p.) ↑ noise magnitude **independent** of depth of C

Recap: [BGG⁺, BTVW] Attribute Encoding

$$\boldsymbol{A} \xrightarrow[C(\boldsymbol{x}) \in \mathbb{Z}_q^{(n+1)\times m}]{\text{MEvalC}}$$

$$\boldsymbol{c}^\top = \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}$$

$$\boldsymbol{A}, \boldsymbol{x} \xrightarrow[\text{circuit } C]{\text{MEvalCX}}$$

Recap: [BGG+, BTVW] Attribute Encoding

$$\boldsymbol{A} \xrightarrow[C(\boldsymbol{x}) \in \mathbb{Z}_q^{(n+1)\times m}]{\text{MEvalC}} \boldsymbol{H}_C$$

$$\boldsymbol{A}_C = \boldsymbol{A}\boldsymbol{H}_C$$

$$\boldsymbol{c}^\top = \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}$$

$$\boldsymbol{A}, \boldsymbol{x} \xrightarrow[\text{circuit } C]{\text{MEvalCX}}$$

Recap: [BGG+, BTVW] Attribute Encoding

$$\begin{tikzcd} \boldsymbol{A} \arrow[r, "\mathrm{MEvalC}", "C(\boldsymbol{x}) \in \mathbb{Z}_q^{(n+1)\times m}"'] & \boldsymbol{H}_C \end{tikzcd}$$

$$\boldsymbol{A}_C = \boldsymbol{A}\boldsymbol{H}_C$$

$$\boldsymbol{c}^\top = \uwave{\boldsymbol{s}^\top(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}$$

$$\begin{tikzcd} \boldsymbol{A}, \boldsymbol{x} \arrow[r, "\mathrm{MEvalCX}", "\text{circuit } C"'] & \boldsymbol{H}_{C,\boldsymbol{x}} \end{tikzcd}$$

$$(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})\boldsymbol{H}_{C,\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{H}_C - C(\boldsymbol{x})$$

Recap: [BGG$^+$, BTVW] Attribute Encoding

$$\boldsymbol{A} \xrightarrow[C(\boldsymbol{x}) \in \mathbb{Z}_q^{(n+1)\times m}]{\text{MEvalC}} \boldsymbol{H}_C$$

$$\boldsymbol{A}_C = \boldsymbol{A}\boldsymbol{H}_C$$

$$\boldsymbol{c}^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})} \qquad \boldsymbol{c}_C^\top = \boldsymbol{c}^\top \boldsymbol{H}_{C,\boldsymbol{x}} = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}))}$$

$$\boldsymbol{A}, \boldsymbol{x} \xrightarrow[\text{circuit } C]{\text{MEvalCX}} \boldsymbol{H}_{C,\boldsymbol{x}}$$

$$(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})\boldsymbol{H}_{C,\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{H}_C - C(\boldsymbol{x})$$

Recap: [BGG⁺, BTVW] Attribute Encoding

$$\boldsymbol{A} \xrightarrow[C(\boldsymbol{x}) \in \mathbb{Z}_q^{(n+1)\times m}]{\text{MEvalC}} \boldsymbol{H}_C$$

$$\boldsymbol{A}_C = \boldsymbol{A}\boldsymbol{H}_C$$

$$\boldsymbol{c}^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})} \qquad \boldsymbol{c}_C^\top = \boldsymbol{c}^\top \boldsymbol{H}_{C,\boldsymbol{x}} = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}))}$$

$$\boldsymbol{A}, \boldsymbol{x} \xrightarrow[\text{circuit } C]{\text{MEvalCX}} \boldsymbol{H}_{C,\boldsymbol{x}}$$

$\boxed{\text{usual version: } C(\boldsymbol{x}) \in \{\boldsymbol{0}, \boldsymbol{G}\}}$

$$(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})\boldsymbol{H}_{C,\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{H}_C - C(\boldsymbol{x})$$

Recap: [BGG$^+$, BTVW] Attribute Encoding

$$\boldsymbol{A} \xrightarrow[C(\boldsymbol{x}) \in \mathbb{Z}_q^{(n+1)\times m}]{\mathrm{MEvalC}} \boldsymbol{H}_C$$

$$\boldsymbol{A}_C = \boldsymbol{A}\boldsymbol{H}_C$$

$$\boldsymbol{c}^\top = \boldsymbol{s}^\top(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G}) \qquad \boldsymbol{c}_C^\top = \boldsymbol{c}^\top \boldsymbol{H}_{C,\boldsymbol{x}} = \boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}))$$

noise growth $\|\boldsymbol{H}\| \leq m^{\Theta(d)}$

$$\boldsymbol{A}, \boldsymbol{x} \xrightarrow[\text{circuit } C]{\mathrm{MEvalCX}} \boldsymbol{H}_{C,\boldsymbol{x}}$$

usual version: $C(\boldsymbol{x}) \in \{\boldsymbol{0}, \boldsymbol{G}\}$

$$(\boldsymbol{A} - \boldsymbol{x}^\top \otimes \boldsymbol{G})\boldsymbol{H}_{C,\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{H}_C - C(\boldsymbol{x})$$

Inspirations from FHE

Rounding

Bootstrapping

Inspirations from FHE

Rounding

$$\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top$$

Bootstrapping

Inspirations from FHE

Rounding

$$\left\lfloor \frac{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\mathrm{large}}^\top}{M} \right\rceil$$

Bootstrapping

Inspirations from FHE

Rounding

$$\left\lfloor \frac{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x})\cdot\boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top}{M} \right\rceil = \boldsymbol{s}^\top\big(\boldsymbol{A}_{C,\text{small}} - C(\boldsymbol{x})\cdot\boldsymbol{G}_{\text{small}}\big) + \underbrace{\boldsymbol{e}_{\text{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{\text{large}}^\top}{M} \right\rceil}_{\boldsymbol{e}_{\text{small}}^\top}$$

Bootstrapping

Inspirations from FHE

Rounding

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x})\cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top\left(\boldsymbol{A}_{C,\text{small}} - C(\boldsymbol{x})\cdot\boldsymbol{G}_{\text{small}}\right) + \underbrace{\boldsymbol{e}_{\text{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{\text{large}}^\top}{M}\right\rceil}_{\boldsymbol{e}_{\text{small}}^\top} \right)$$

$$\bmod \frac{q}{M}$$

Bootstrapping

Inspirations from FHE

Rounding

$|e|$ **goes down**, but $|e|/\text{modulus}$ **is unchanged**

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x})\cdot\boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top(\boldsymbol{A}_{C,\text{small}} - C(\boldsymbol{x})\cdot\boldsymbol{G}_{\text{small}}) + \underbrace{\boldsymbol{e}_{\text{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{\text{large}}^\top}{M} \right\rceil}_{\boldsymbol{e}_{\text{small}}^\top} \right)$$

$$\bmod \frac{q}{M}$$

Bootstrapping

Inspirations from FHE

Rounding

$|e|$ **goes down**, but $|e|/\text{modulus}$ **is unchanged**

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top\left(\boldsymbol{A}_{C,\text{small}} - C(\boldsymbol{x}) \cdot \boldsymbol{G}_{\text{small}}\right) + \underbrace{\boldsymbol{e}_{\text{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{\text{large}}^\top}{M} \right\rceil}_{\boldsymbol{e}_{\text{small}}^\top} \right) \bmod \frac{q}{M}$$

Bootstrapping

Inspirations from FHE

Rounding

$|e|$ **goes down**, but $|e|/\text{modulus}$ **is unchanged**

$$\left\lfloor \frac{\left(\mathbf{s}^\top(\mathbf{A}_C - C(\mathbf{x})\cdot\mathbf{G}) + \mathbf{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\mathbf{s}^\top\left(\mathbf{A}_{C,\text{small}} - C(\mathbf{x})\cdot\mathbf{G}_{\text{small}}\right) + \underbrace{\mathbf{e}_{\text{round}}^\top + \left\lfloor \frac{\mathbf{e}_{\text{large}}^\top}{M} \right\rceil}_{\mathbf{e}_{\text{small}}^\top} \right) \bmod \frac{q}{M}$$

Bootstrapping

$\text{hct}_{\text{large}} = \text{hct}(x)$ circular $\text{hct}_{\text{fresh}}(\text{hsk})$

Inspirations from FHE

Rounding

$|e|$ **goes down**, but $|e|/\text{modulus}$ **is unchanged**

$$\left\lfloor \frac{\left(\mathbf{s}^\top(\mathbf{A}_C - C(\mathbf{x})\cdot \mathbf{G}) + \mathbf{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\mathbf{s}^\top \left(\mathbf{A}_{C,\text{small}} - C(\mathbf{x})\cdot \mathbf{G}_{\text{small}}\right) + \underbrace{\mathbf{e}_{\text{round}}^\top + \left\lfloor \frac{\mathbf{e}_{\text{large}}^\top}{M}\right\rceil}_{\mathbf{e}_{\text{small}}^\top} \right) \bmod \frac{q}{M}$$

Bootstrapping

$\text{hct}_{\text{large}} = \text{hct}(x)$ circular $\text{hct}_{\text{fresh}}(\text{hsk})$

$$\text{HEval}\left(\text{Dec}(\cdot, \text{hct}_{\text{large}}), \text{hct}_{\text{fresh}}(\text{hsk})\right)$$

Inspirations from FHE

Rounding

$|e|$ **goes down**, but $|e|/\text{modulus}$ **is unchanged**

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top\left(\boldsymbol{A}_{C,\text{small}} - C(\boldsymbol{x}) \cdot \boldsymbol{G}_{\text{small}}\right) + \underbrace{\boldsymbol{e}_{\text{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{\text{large}}^\top}{M} \right\rceil}_{\boldsymbol{e}_{\text{small}}^\top} \right) \bmod \frac{q}{M}$$

Bootstrapping

$\text{hct}_{\text{large}} = \text{hct}(x)$ circular $\text{hct}_{\text{fresh}}(\text{hsk})$

$$\text{HEval}\left(\text{Dec}(\cdot, \text{hct}_{\text{large}}), \text{hct}_{\text{fresh}}(\text{hsk})\right) = \text{hct}_{\text{small}}\left(\text{Dec}(\text{hsk}, \text{hct}_{\text{large}})\right)$$

Inspirations from FHE

Rounding $|e|$ **goes down**, but $|e|/\text{modulus}$ **is unchanged**

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top (\boldsymbol{A}_C - C(\boldsymbol{x})\cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top (\boldsymbol{A}_{C,\text{small}} - C(\boldsymbol{x})\cdot \boldsymbol{G}_{\text{small}}) + \underbrace{\boldsymbol{e}_{\text{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{\text{large}}^\top}{M}\right\rceil}_{\boldsymbol{e}_{\text{small}}^\top} \right) \bmod \frac{q}{M}$$

Bootstrapping output $|e|$ bound **independent** of $\text{hct}_{\text{large}}$

$\text{hct}_{\text{large}} = \text{hct}(x)$ circular $\text{hct}_{\text{fresh}}(\text{hsk})$

$$\text{HEval}\left(\text{Dec}(\cdot, \text{hct}_{\text{large}}), \text{hct}_{\text{fresh}}(\text{hsk})\right) = \text{hct}_{\text{small}}\left(\text{Dec}(\text{hsk}, \text{hct}_{\text{large}})\right) = \text{hct}_{\text{small}}(x)$$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\text{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\mathrm{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\mathrm{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\mathrm{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\mathrm{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$
3. evaluate $C'(\boldsymbol{s}) = \mathrm{Dec}\left(\cdot, \boldsymbol{c}_{\mathrm{large}}\right) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\mathrm{circ}}^{\top}$

$$\boldsymbol{c}_{\mathrm{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}$$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\text{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\text{circ}}^{\top} = \underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$
3. evaluate $C'(\boldsymbol{s}) = \text{Dec}\left(\cdot, \boldsymbol{c}_{\text{large}}\right) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\text{circ}}^{\top}$

$$\boldsymbol{c}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} = \boldsymbol{s}^{\top}\Big(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - C'(\boldsymbol{s})\Big) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}$$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\text{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\text{circ}}^{\top} = \underset{\sim\sim\sim}{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$
3. evaluate $C'(\boldsymbol{s}) = \text{Dec}\left(\cdot, \boldsymbol{c}_{\text{large}}\right) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\text{circ}}^{\top}$

$$
\begin{aligned}
\boldsymbol{c}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} &= \boldsymbol{s}^{\top}\Big(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - C'(\boldsymbol{s})\Big) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - \text{Dec}\left(\boldsymbol{s}, \boldsymbol{c}_{\text{large}}\right) \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}
\end{aligned}
$$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\text{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\text{circ}}^{\top} = \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$
3. evaluate $C'(\boldsymbol{s}) = \text{Dec}\left(\cdot, \boldsymbol{c}_{\text{large}}\right) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\text{circ}}^{\top}$

$$
\begin{aligned}
\boldsymbol{c}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} &= \boldsymbol{s}^{\top}\Big(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - C'(\boldsymbol{s})\Big) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - \text{Dec}\left(\boldsymbol{s}, \boldsymbol{c}_{\text{large}}\right) \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - C(\boldsymbol{x}) \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}
\end{aligned}
$$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\mathrm{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\mathrm{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$
3. evaluate $C'(\boldsymbol{s}) = \mathrm{Dec}\left(\cdot, \boldsymbol{c}_{\mathrm{large}}\right) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\mathrm{circ}}^{\top}$

$$
\begin{aligned}
\boldsymbol{c}_{\mathrm{circ}}^{\top} \boldsymbol{H}_{C',\boldsymbol{s}} &= \boldsymbol{s}^{\top}\Big(\boldsymbol{A}_{\mathrm{circ}} \boldsymbol{H}_{C'} - C'(\boldsymbol{s})\Big) + \boldsymbol{e}_{\mathrm{circ}}^{\top} \boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\mathrm{circ}} \boldsymbol{H}_{C'} - \mathrm{Dec}\left(\boldsymbol{s}, \boldsymbol{c}_{\mathrm{large}}\right) \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{\mathrm{circ}}^{\top} \boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\mathrm{circ}} \boldsymbol{H}_{C'} - C(\boldsymbol{x}) \cdot \boldsymbol{G}\right) + \boxed{\boldsymbol{e}_{\mathrm{circ}}^{\top} \boldsymbol{H}_{C',\boldsymbol{s}}}
\end{aligned}
$$

bound independent of $\boldsymbol{e}_{\mathrm{large}}$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\text{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\text{circ}}^{\top} = \uwave{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$
3. evaluate $C'(\boldsymbol{s}) = \text{Dec}(\cdot, \boldsymbol{c}_{\text{large}}) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\text{circ}}^{\top}$

$$
\begin{aligned}
\boldsymbol{c}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} &= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - C'(\boldsymbol{s})\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - \text{Dec}(\boldsymbol{s}, \boldsymbol{c}_{\text{large}}) \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}} \\
&= \boldsymbol{s}^{\top}\left(\boxed{\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'}} - C(\boldsymbol{x}) \cdot \boldsymbol{G}\right) + \boxed{\boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}}
\end{aligned}
$$

C' hardwires $\boldsymbol{c}_{\text{large}}$

(cannot KeyGen in ABE)

bound independent of $\boldsymbol{e}_{\text{large}}$

Problems with Naïve Bootstrapping

1. regard $\boldsymbol{c}_{\text{large}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{C} - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^{\top}$ as ciphertext of $C(\boldsymbol{x})$ under $\boldsymbol{s}$
2. provide $\boldsymbol{c}_{\text{circ}}^{\top} = \uwave{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ}} - \text{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$ ✗
3. evaluate $C'(\boldsymbol{s}) = \text{Dec}(\cdot, \boldsymbol{c}_{\text{large}}) \cdot \boldsymbol{G}$ on $\boldsymbol{c}_{\text{circ}}^{\top}$

$$\boldsymbol{c}_{\text{circ}}^{\top}\boxed{\boldsymbol{H}_{C',\boldsymbol{s}}} = \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - C'(\boldsymbol{s})\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}$$

must know $\boldsymbol{s}$ for evaluation **(no security)**

$$= \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'} - \text{Dec}(\boldsymbol{s}, \boldsymbol{c}_{\text{large}}) \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}$$

$$= \boldsymbol{s}^{\top}\left(\boxed{\boldsymbol{A}_{\text{circ}}\boldsymbol{H}_{C'}} - C(\boldsymbol{x}) \cdot \boldsymbol{G}\right) + \boxed{\boldsymbol{e}_{\text{circ}}^{\top}\boldsymbol{H}_{C',\boldsymbol{s}}}$$

C' hardwires $\boldsymbol{c}_{\text{large}}$ **(cannot KeyGen in ABE)**

bound independent of $\boldsymbol{e}_{\text{large}}$

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{(\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\mathrm{large}}^{\top}) \bmod q}{M} \right\rceil$$

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top (\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\mathrm{large}}^\top\right) \bmod q}{M} \right\rceil$$

$$= \left(\left\lfloor \frac{\left(\boldsymbol{s}^\top \boldsymbol{A}_C + \boldsymbol{e}_{\mathrm{large}}^\top\right) \bmod q}{M} \right\rceil - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}} \right) \bmod \frac{q}{M}$$

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rceil$$

(M is power of two, ignore small part of $\boldsymbol{G}$)

$$= \left(\left\lfloor \frac{(\boldsymbol{s}^\top \boldsymbol{A}_C + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rceil - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \bmod \frac{q}{M}$$

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rfloor$$

(M is power of two, ignore small part of $\boldsymbol{G}$)

$$= \left(\left\lfloor \frac{(\boldsymbol{s}^\top \boldsymbol{A}_C + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rfloor - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \bmod \frac{q}{M}$$

(w.h.p)

$$= \left(\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_C \bmod q}{M} \right\rfloor - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \bmod \frac{q}{M}$$

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rceil$$

(M is power of two, ignore small part of $\boldsymbol{G}$)

$$= \left(\left\lfloor \frac{(\boldsymbol{s}^\top \boldsymbol{A}_C + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rceil - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \bmod \frac{q}{M}$$

(w.h.p)

$$= \left(\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_C \bmod q}{M} \right\rceil - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \boxed{\bmod \frac{q}{M}}$$

multiply by M to restore modulus

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x})\cdot\boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rceil$$

(M is power of two, ignore small part of $\boldsymbol{G}$)

$$= \left(\left\lfloor \frac{(\boldsymbol{s}^\top \boldsymbol{A}_C + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rceil - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \bmod \frac{q}{M}$$

(w.h.p)

$$= \left(\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_C \bmod q}{M} \right\rceil - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \boxed{\bmod \frac{q}{M}}$$

multiply by M to restore modulus

$$\to \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_C \bmod q}{M} \right\rceil M - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top M \boldsymbol{G}_{\text{small}}$$

Step 1: Noise Removal

noiseless rounding inspired by learning with rounding (LWR)

$$\left\lfloor \frac{(\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rfloor$$

(M is power of two, ignore small part of $\boldsymbol{G}$)

$$= \left(\left\lfloor \frac{(\boldsymbol{s}^\top \boldsymbol{A}_C + \boldsymbol{e}_{\text{large}}^\top) \bmod q}{M} \right\rfloor - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \bmod \frac{q}{M}$$

(w.h.p)

$$= \left(\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_C \bmod q}{M} \right\rfloor - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\text{small}} \right) \boxed{\bmod \frac{q}{M}}$$

multiply by M to restore modulus

$$\to \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_C \bmod q}{M} \right\rfloor M - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top M \boldsymbol{G}_{\text{small}}$$

not all of $\boldsymbol{G}$

Step 1: Noise Removal (cont’d)

$$\boldsymbol{G} = (\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}})\boldsymbol{Q}$$

$$\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})}$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

$$\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\underset{}{\boldsymbol{Q}} \quad \text{permutation}$$

$$\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}})$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

$$\left\lfloor \frac{\uwave{\boldsymbol{s}^{\top}(\boldsymbol{A}_{C} - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rfloor$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q}$$ permutation

$$\left\lfloor \frac{\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{C} - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix}$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

$$\left\lfloor \frac{\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

Left. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

$$\left\lfloor \frac{\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

Step 1: Noise Removal (cont’d)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q}$$ permutation

Left. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q}$$ permutation

Left. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$= \left\lfloor \frac{\utilde{\boldsymbol{s}^\top\boldsymbol{A}_C}\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q} - C(\boldsymbol{x}) \cdot \boldsymbol{s}^\top\boldsymbol{G}$$

Step 1: Noise Removal (cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q}$$ permutation

Left. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M}\cdot\boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M}\cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\uwave{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x})\cdot\boldsymbol{G})}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$= \boxed{\left\lfloor \frac{\uwave{\boldsymbol{s}^{\top}\boldsymbol{A}_C}\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}} - C(\boldsymbol{x})\cdot\boldsymbol{s}^{\top}\boldsymbol{G}$$

$\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})$ = ↑ without noise

Step 1: Noise Removal (cont'd cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

Left. $\frac{\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$= \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s}) - C(\boldsymbol{x}) \cdot \boldsymbol{s}^{\top}\boldsymbol{G} \qquad \text{(w.h.p.)}$$

Step 1: Noise Removal (cont'd cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

Left. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\uwave{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$= \boxed{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})} - C(\boldsymbol{x}) \cdot \boldsymbol{s}^{\top}\boldsymbol{G} \qquad \text{(w.h.p.)}$$

- low-depth – **linear, rounding, linear.**

Step 1: Noise Removal (cont'd cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q} \quad \text{permutation}$$

Left. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$= \boxed{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})} - C(\boldsymbol{x}) \cdot \boldsymbol{s}^{\top}\boldsymbol{G} \qquad \text{(w.h.p.)}$$

- **low-depth – linear, rounding, linear.**
- **further homomorphic evaluation?**

Step 1: Noise Removal (cont'd cont'd)

$$\boldsymbol{G} = (\overset{< M}{\boldsymbol{G}_{\mathrm{L}}}, \underset{\geq M}{\boldsymbol{G}_{\mathrm{R}}})\boldsymbol{Q}$$ permutation

Left. $\frac{\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

Right. $\frac{\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

$$\left\lfloor \frac{\boldsymbol{s}^{\top}(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$= \boxed{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})} - C(\boldsymbol{x}) \cdot \boldsymbol{s}^{\top}\boldsymbol{G} \qquad \text{(w.h.p.)}$$

- **low-depth – linear, rounding, linear.**
- **further homomorphic evaluation?**

wanted $\boldsymbol{s}^{\top}\boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})$

Recap: [GSW] FHE

$$\mathrm{hpk} = \boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^\top \end{pmatrix}$$

$$\mathrm{hsk} = \boldsymbol{s}^\top = (\boldsymbol{r}^\top, -1)^\top$$

$$\mathrm{hct}(\boldsymbol{x}) = \boldsymbol{A}_{\mathrm{fhe}} \boldsymbol{R} - \boldsymbol{x}^\top \otimes \boldsymbol{G}$$

Recap: [GSW] FHE

$$\mathrm{hpk} = \boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^\top \end{pmatrix}$$

$$\mathrm{hsk} = \boldsymbol{s}^\top = (\boldsymbol{r}^\top, -1)^\top$$

$$f : \boldsymbol{x} \mapsto \boldsymbol{f}^\top$$

$$\mathrm{hct}(\boldsymbol{x}) = \boldsymbol{A}_{\mathrm{fhe}} \boldsymbol{R} - \boldsymbol{x}^\top \otimes \boldsymbol{G}$$

Recap: [GSW] FHE

$$\mathrm{hpk} = \boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^\top \end{pmatrix}$$

$$\mathrm{hsk} = \boldsymbol{s}^\top = (\boldsymbol{r}^\top, -1)^\top$$

$$f: \boldsymbol{x} \mapsto \boldsymbol{f}^\top \xrightarrow[\hat{f} = \mathrm{HEval}(f, \cdot)]{} \hat{f}$$

$$\mathrm{hct}(\boldsymbol{x}) = \boldsymbol{A}_{\mathrm{fhe}} \boldsymbol{R} - \boldsymbol{x}^\top \otimes \boldsymbol{G}$$

Recap: [GSW] FHE

$$\mathrm{hpk} = \boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^\top \end{pmatrix} \qquad \mathrm{hsk} = \boldsymbol{s}^\top = (\boldsymbol{r}^\top, -1)^\top$$

$$f\colon \boldsymbol{x} \mapsto \boldsymbol{f}^\top \xrightarrow[\hat{f} = \mathrm{HEval}(f,\cdot)]{} \hat{f}$$

$$\mathrm{hct}(\boldsymbol{x}) = \boldsymbol{A}_{\mathrm{fhe}}\boldsymbol{R} - \boldsymbol{x}^\top \otimes \boldsymbol{G} \xrightarrow[\text{apply } \hat{f}]{} \boldsymbol{A}_{\mathrm{fhe}}\boldsymbol{R}_f - \begin{pmatrix} \boldsymbol{0} \\ \boldsymbol{f}^\top \end{pmatrix}$$

Recap: [GSW] FHE

$$\mathrm{hpk} = \boldsymbol{A}_{\mathrm{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\mathrm{fhe}} \\ \boldsymbol{r}^{\top}\overline{\boldsymbol{A}}_{\mathrm{fhe}} + \boldsymbol{e}_{\mathrm{fhe}}^{\top} \end{pmatrix} \qquad \mathrm{hsk} = \boldsymbol{s}^{\top} = (\boldsymbol{r}^{\top}, -1)^{\top}$$

$$f : \boldsymbol{x} \mapsto \boldsymbol{f}^{\top} \xrightarrow[\hat{f} \,=\, \mathrm{HEval}(f, \cdot)]{\hspace{6em}} \hat{f} \ \text{ with } \boldsymbol{s}^{\top}\hat{f}\big(\mathrm{hct}(\boldsymbol{x})\big) = f(\boldsymbol{x}) = \boldsymbol{f}^{\top}$$

$$\mathrm{hct}(\boldsymbol{x}) = \boldsymbol{A}_{\mathrm{fhe}}\boldsymbol{R} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G} \xrightarrow[\text{apply } \hat{f}]{\hspace{6em}} \boldsymbol{A}_{\mathrm{fhe}}\boldsymbol{R}_f - \begin{pmatrix} \boldsymbol{0} \\ \boldsymbol{f}^{\top} \end{pmatrix}$$

Recap: [GSW] FHE

$$\text{hpk} = \boldsymbol{A}_{\text{fhe}} = \begin{pmatrix} \overline{\boldsymbol{A}}_{\text{fhe}} \\ \boldsymbol{r}^\top \overline{\boldsymbol{A}}_{\text{fhe}} + \boldsymbol{e}_{\text{fhe}}^\top \end{pmatrix} \qquad \text{hsk} = \boldsymbol{s}^\top = (\boldsymbol{r}^\top, -1)^\top$$

$$f : \boldsymbol{x} \mapsto \boldsymbol{f}^\top \xrightarrow[\hat{f} = \text{HEval}(f, \cdot)]{} \hat{f} \text{ with } \boldsymbol{s}^\top \hat{f}\big(\text{hct}(\boldsymbol{x})\big) = \uwave{f(\boldsymbol{x})} = \uwave{\boldsymbol{f}}^\top$$

$$\boxed{\hat{d} = d \cdot \text{poly}(\lambda)}$$

$$\text{hct}(\boldsymbol{x}) = \boldsymbol{A}_{\text{fhe}} \boldsymbol{R} - \boldsymbol{x}^\top \otimes \boldsymbol{G} \xrightarrow[\text{apply } \hat{f}]{} \boldsymbol{A}_{\text{fhe}} \boldsymbol{R}_f - \begin{pmatrix} \boldsymbol{0} \\ \boldsymbol{f}^\top \end{pmatrix}$$

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\underline{\boldsymbol{s}^{\top}\boldsymbol{A}'_{C} - \mathrm{RndPad}_{\boldsymbol{A}_{C}}(\boldsymbol{s})}$

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\utilde{\boldsymbol{s}^\top \boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

circular ciphertext $\boldsymbol{S} = \mathrm{hct}(\boldsymbol{s})$

circular encoding $\boldsymbol{c}_{\mathrm{circ}}^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\underline{\boldsymbol{s}^\top \boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

[<u>GSW</u>] $\boldsymbol{s}^\top \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\mathrm{hct}(\boldsymbol{s})) = \underline{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

circular ciphertext $\boldsymbol{S} = \mathrm{hct}(\boldsymbol{s})$

circular encoding $\boldsymbol{c}_{\mathrm{circ}}^\top = \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$

$$\Big\downarrow$$

[<u>BGG⁺</u>, <u>BTVW</u>] evaluate $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}$ on input $\boldsymbol{S}$

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\underline{\boldsymbol{s}^\top \boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

[GSW] $\boldsymbol{s}^\top\, \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\mathrm{hct}(\boldsymbol{s})) = \underline{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

circular ciphertext $\quad \boldsymbol{S} = \mathrm{hct}(\boldsymbol{s})$

circular encoding $\quad \boldsymbol{c}_{\mathrm{circ}}^\top = \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$

$\downarrow$ [BGG⁺, BTVW] evaluate $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}$ on input $\boldsymbol{S}$

$$\boldsymbol{c}_{\mathrm{circ}}^\top \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}, \boldsymbol{S}} = \underline{\boldsymbol{s}^\top \left(\boldsymbol{A}_{\mathrm{circ}} \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}} - \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\boldsymbol{S})\right)}$$

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\boldsymbol{s}^\top \boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})$

$$\boxed{[\underline{\text{GSW}}]\ \boldsymbol{s}^\top\, \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\mathrm{hct}(\boldsymbol{s})) = \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$$

circular ciphertext $\boldsymbol{S} = \mathrm{hct}(\boldsymbol{s})$

circular encoding $\boldsymbol{c}_{\mathrm{circ}}^\top = \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})$

[BGG⁺, BTVW] ↓ evaluate $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}$ on input $\boldsymbol{S}$

$= \boldsymbol{A}'_C$, only depends on C

$$\boldsymbol{c}_{\mathrm{circ}}^\top \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C},\boldsymbol{S}} = \boldsymbol{s}^\top\left(\boxed{\boldsymbol{A}_{\mathrm{circ}}\boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}}} - \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\boldsymbol{S})\right)$$

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\underline{\boldsymbol{s}^\top \boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

$\boxed{[\text{GSW}]\ \boldsymbol{s}^\top\, \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\mathrm{hct}(\boldsymbol{s})) = \underline{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}}$

circular ciphertext $\boldsymbol{S} = \mathrm{hct}(\boldsymbol{s})$

circular encoding $\boldsymbol{c}_{\mathrm{circ}}^\top = \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$

$$\Big\downarrow$$

[BGG+, BTVW] evaluate $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}$ on input $\boldsymbol{S}$

$$\boldsymbol{c}_{\mathrm{circ}}^\top \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}, \boldsymbol{S}} = \underline{\boxed{\boldsymbol{s}^\top}\left(\overset{= \boldsymbol{A}'_C\text{, only depends on } C}{\boxed{\boldsymbol{A}_{\mathrm{circ}} \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}}}} - \boxed{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\boldsymbol{S})}\right)}$$

↖ **automagic decryption** ↗ $= \underline{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

(dual-use technique [BTVW])

Step 2: Bootstrapping (Restore Encoding Format)

Goal. $\underline{\boldsymbol{s}^\top \boldsymbol{A}'_C - \mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

$$\boxed{[\underline{\text{GSW}}]\ \boldsymbol{s}^\top\, \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\mathrm{hct}(\boldsymbol{s})) = \underline{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}}$$

circular ciphertext $\boldsymbol{S} = \mathrm{hct}(\boldsymbol{s})$

circular encoding $\boldsymbol{c}_{\mathrm{circ}}^\top = \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$

[BGG+, BTVW] $\downarrow$ evaluate $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}$ on input $\boldsymbol{S}$

Low Output Noise

depths of $\mathrm{RndPad}_{\boldsymbol{A}_C}$ and $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}$ independent of C

$$\boldsymbol{c}_{\mathrm{circ}}^\top \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}, \boldsymbol{S}} = \underline{\boxed{\boldsymbol{s}^\top}\left(\overset{= \boldsymbol{A}'_C\text{, only depends on } C}{\boxed{\boldsymbol{A}_{\mathrm{circ}} \boldsymbol{H}_{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}}}} - \boxed{\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_C}(\boldsymbol{S})}\right)}$$

↖ **automagic decryption** ↗ $= \underline{\mathrm{RndPad}_{\boldsymbol{A}_C}(\boldsymbol{s})}$

(dual-use technique [BTVW])

Summary of UEvalC$[X]$ (Fresh, Small, Large)

for every gate $x_3 = x_3(x_1, x_2)$ in C:

$$\boldsymbol{c}_1^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})}$$

$$\boldsymbol{c}_2^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})}$$

Summary of $\mathrm{UEvalC}[X]$ (Fresh, Small, Large)

for every gate $x_3 = x_3(x_1, x_2)$ in C:

$$\begin{matrix} \boldsymbol{c}_1^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})} \\ \boldsymbol{c}_2^\top = \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})} \end{matrix} \xrightarrow[\text{for } x_3]{[\underline{\text{BGG}^+}, \underline{\text{BTVW}}]} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})}$$

Summary of $\mathrm{UEvalC}[X]$ (Fresh, Small, Large)

for every gate $x_3 = x_3(x_1, x_2)$ in C:

$$\begin{tikzcd}
\begin{array}{l} \boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) \\ \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) \end{array} \arrow[r, "{[\underline{\mathrm{BGG}^+}, \underline{\mathrm{BTVW}}]}", "\text{for } x_3"'] & \boldsymbol{s}^\top(\boldsymbol{A}'_3 - x_3\boldsymbol{G}) \arrow[d, "\textbf{remove noise}"] \\
 & \mathrm{RndPad}_{\boldsymbol{A}'_3}(\boldsymbol{s}) - x_3\boldsymbol{s}^\top\boldsymbol{G}
\end{tikzcd}$$

Summary of UEvalC$[X]$ (Fresh, Small, Large)

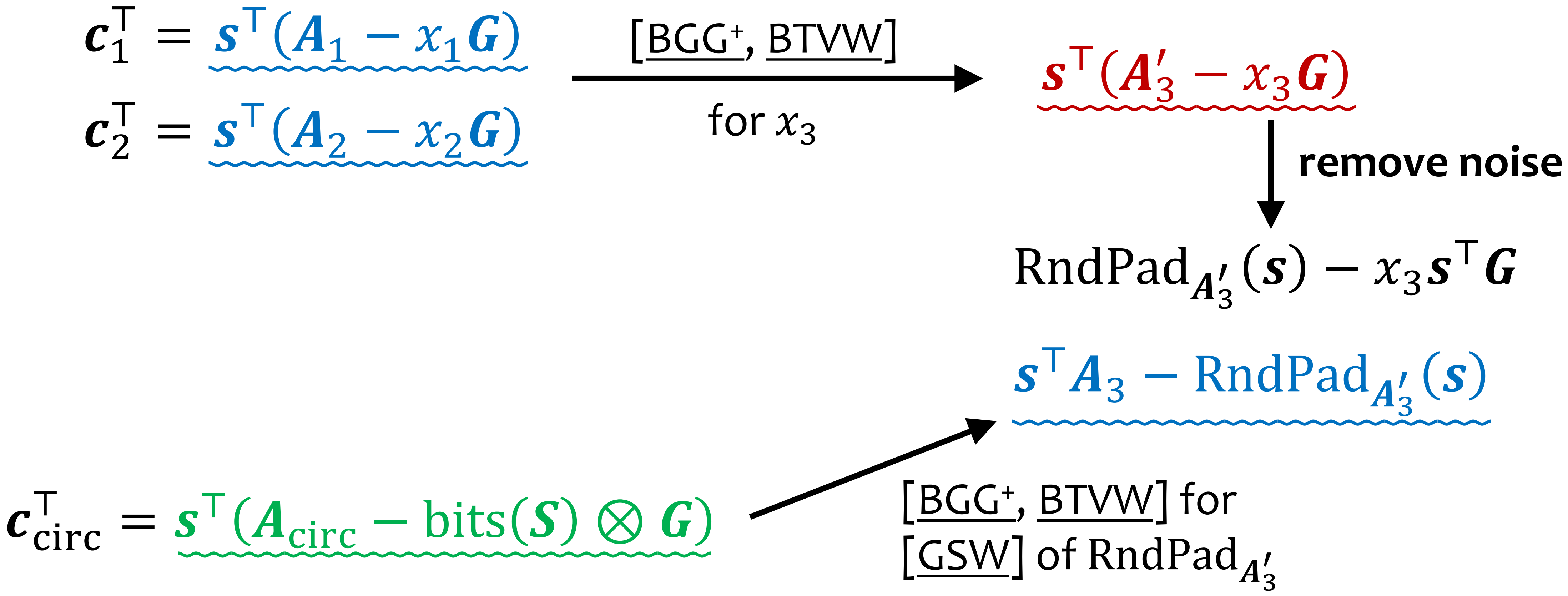
for every gate $x_3 = x_3(x_1, x_2)$ in C:

$$\begin{tikzcd}
\begin{array}{l} \boldsymbol{c}_1^\top = \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})} \\ \boldsymbol{c}_2^\top = \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})} \end{array} \arrow[r, "\text{[\underline{BGG}^+, \underline{BTVW}]}", "\text{for } x_3"'] & \uwave{\boldsymbol{s}^\top(\boldsymbol{A}'_3 - x_3\boldsymbol{G})} \arrow[d, "\textbf{remove noise}"] \\
 & \mathrm{RndPad}_{\boldsymbol{A}'_3}(\boldsymbol{s}) - x_3\boldsymbol{s}^\top\boldsymbol{G}
\end{tikzcd}$$

$$\boldsymbol{c}_{\mathrm{circ}}^\top = \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}$$

Summary of $\mathrm{UEvalC}[X]$ (Fresh, Small, Large)

for every gate $x_3 = x_3(x_1, x_2)$ in C:



$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})$$

$$\boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})$$

[BGG+, BTVW] for x_3

$$\boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})$$

remove noise

$$\mathrm{RndPad}_{\boldsymbol{A}_3'}(\boldsymbol{s}) - x_3\boldsymbol{s}^\top\boldsymbol{G}$$

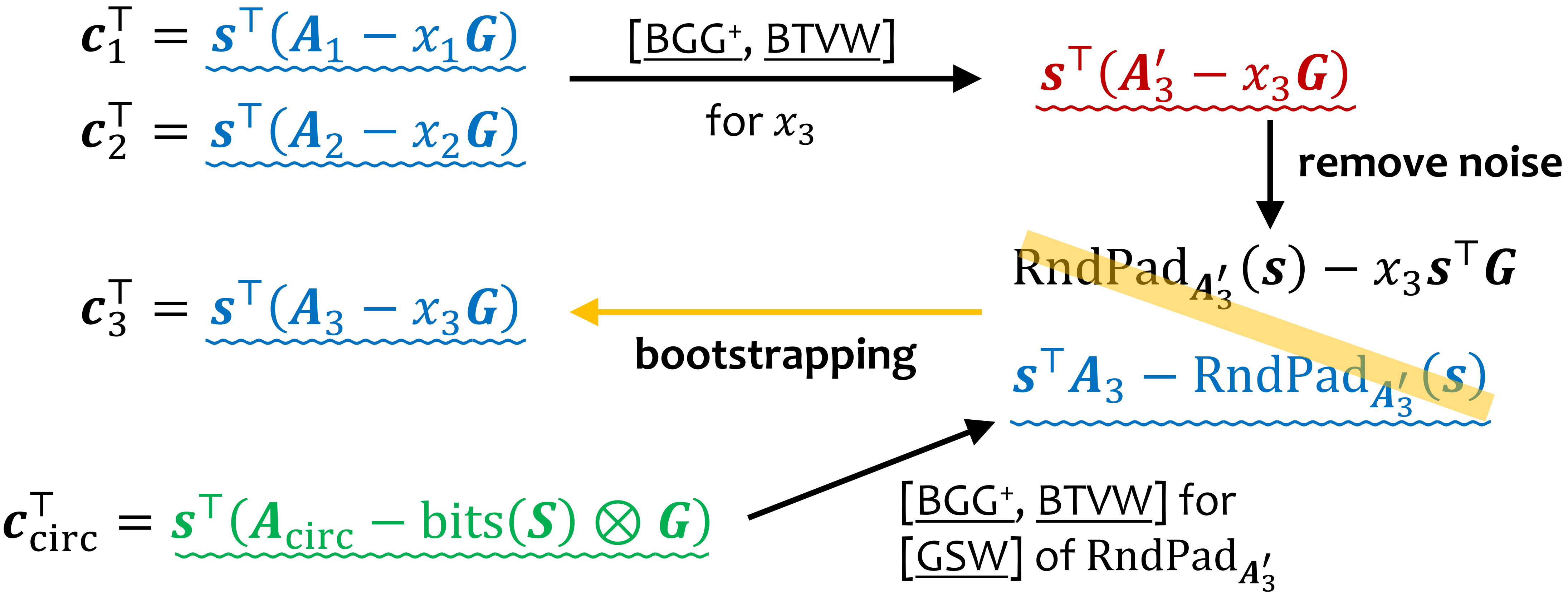
$$\boldsymbol{s}^\top\boldsymbol{A}_3 - \mathrm{RndPad}_{\boldsymbol{A}_3'}(\boldsymbol{s})$$

$$\boldsymbol{c}_{\mathrm{circ}}^\top = \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})$$

[BGG+, BTVW] for
[GSW] of $\mathrm{RndPad}_{\boldsymbol{A}_3'}$

Summary of $\mathrm{UEvalC}[X]$ (Fresh, Small, Large)

for every gate $x_3 = x_3(x_1, x_2)$ in C:



$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})$

$\boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})$

[BGG+, BTVW]

for x_3

$\boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})$

remove noise

$\mathrm{RndPad}_{\boldsymbol{A}_3'}(\boldsymbol{s}) - x_3\boldsymbol{s}^\top\boldsymbol{G}$

$\boldsymbol{s}^\top\boldsymbol{A}_3 - \mathrm{RndPad}_{\boldsymbol{A}_3'}(\boldsymbol{s})$

bootstrapping

$\boldsymbol{c}_3^\top = \boldsymbol{s}^\top(\boldsymbol{A}_3 - x_3\boldsymbol{G})$

$\boldsymbol{c}_{\mathrm{circ}}^\top = \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})$

[BGG+, BTVW] for
[GSW] of $\mathrm{RndPad}_{\boldsymbol{A}_3'}$

Subtlety of Correctness

$$\mathrm{RndPad}_{\boldsymbol{A}}(\boldsymbol{s}) = \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$\overset{?}{=} \left\lfloor \frac{\utilde{\boldsymbol{s}^\top \boldsymbol{A}}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

Subtlety of Correctness

$$\mathrm{RndPad}_{\boldsymbol{A}}(\boldsymbol{s}) = \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$\overset{?}{=} \left\lfloor \frac{\underbrace{\boldsymbol{s}^\top \boldsymbol{A}}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

OK when $\boldsymbol{s}^\top \boldsymbol{A}\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}})$ is **far from carry/borrow boundaries.**

Intuition. entries of $\boldsymbol{s}^\top \boldsymbol{A}\boldsymbol{G}^{-1}(\cdots)$ marginally random

Subtlety of Correctness

$$\mathrm{RndPad}_{\boldsymbol{A}}(\boldsymbol{s}) = \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$\overset{?}{=} \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

OK when $\boldsymbol{s}^\top \boldsymbol{A}\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}})$ is **far from carry/borrow boundaries.**

Intuition. entries of $\boldsymbol{s}^\top \boldsymbol{A}\boldsymbol{G}^{-1}(\cdots)$ marginally random

Problem. $\boldsymbol{A}\boldsymbol{G}^{-1}(\cdots) = \boldsymbol{A}_{\mathrm{circ}}\boldsymbol{H}_{C(\boldsymbol{A}_{\mathrm{circ}})}\boldsymbol{G}^{-1}(\cdots)$ adversarial
could make product specific value!

Subtlety of Correctness

$$\mathrm{RndPad}_{\boldsymbol{A}}(\boldsymbol{s}) = \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

$$\overset{?}{=} \left\lfloor \frac{\underline{\boldsymbol{s}^\top \boldsymbol{A}}\, \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}}) \bmod q}{M} \right\rceil \begin{pmatrix} \boldsymbol{I} & \\ & M\boldsymbol{I} \end{pmatrix} \boldsymbol{Q}$$

OK when $\boldsymbol{s}^\top \boldsymbol{A}\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}})$ is **far from carry/borrow boundaries.**

Intuition. entries of $\boldsymbol{s}^\top \boldsymbol{A}\boldsymbol{G}^{-1}(\cdots)$ marginally random

Problem. $\boldsymbol{A}\boldsymbol{G}^{-1}(\cdots) = \boldsymbol{A}_{\mathrm{circ}}\boldsymbol{H}_{C(\boldsymbol{A}_{\mathrm{circ}})}\boldsymbol{G}^{-1}(\cdots)$ adversarial could make product specific value!

Solution 1. circuit-selective correctness from csLWE

Solution 2. add (pseudo-)random shift before rounding

AB-LFE Syntax and Security

$$\mathrm{crsGen}(1^L) \to \mathrm{crs}$$

AB-LFE Syntax and Security

$$\mathrm{crsGen}(1^L) \to \mathrm{crs}$$

$$\mathrm{Compress}(\mathrm{crs}, C) \to \mathrm{digest}_C$$

AB-LFE Syntax and Security

$$\mathrm{crsGen}(1^L) \rightarrow \mathrm{crs}$$

$$\mathrm{Compress}(\mathrm{crs}, C) \rightarrow \mathrm{digest}_C$$

$$\mathrm{Enc}(\mathrm{crs}, \mathrm{digest}_C, \boldsymbol{x}, \mu) \rightarrow \mathrm{ct}_{C,\boldsymbol{x}}$$

AB-LFE Syntax and Security

$$\mathrm{crsGen}(1^L) \to \mathrm{crs}$$

$$\mathrm{Compress}(\mathrm{crs}, C) \to \mathrm{digest}_C$$

$$\mathrm{Enc}(\mathrm{crs}, \mathrm{digest}_C, \boldsymbol{x}, \mu) \to \mathrm{ct}_{C,\boldsymbol{x}}$$

$$\mathrm{Dec}(\mathrm{crs}, C, \boldsymbol{x}, \mathrm{ct}_{C,\boldsymbol{x}}) \to \mu \text{ if } C(\boldsymbol{x}) \text{ is “yes”}$$

AB-LFE Syntax and Security

$$\mathrm{crsGen}(1^L) \to \mathrm{crs}$$

$$\mathrm{Compress}(\mathrm{crs}, C) \to \mathrm{digest}_C$$

$$\mathrm{Enc}(\mathrm{crs}, \mathrm{digest}_C, \boldsymbol{x}, \mu) \to \mathrm{ct}_{C,\boldsymbol{x}}$$

$\mathrm{Dec}(\mathrm{crs}, C, \boldsymbol{x}, \mathrm{ct}_{C,\boldsymbol{x}}) \to \mu$ if $C(\boldsymbol{x})$ is “yes”

Security. $\mathrm{crs}, \mathrm{ct}_{C,\boldsymbol{x}}(\mu) \approx \mathrm{crs}, \mathrm{Sim}(\mathrm{crs}, C, \boldsymbol{x})$ if $C(\boldsymbol{x})$ is “no”

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \right.$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_{C} = \boldsymbol{A}_{C} \text{ from UEvalC}$$

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{ll} & \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ & \end{array} \right.$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{ll} & \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ & \utilde{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{ll} & \left.\begin{array}{l} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array}\right\} \xrightarrow{\mathrm{UEvalCX}} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \\ \boldsymbol{S}, & \\ & \utilde{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = {\color{blue}\boldsymbol{A}_C} \text{ from UEvalC}$$

if ${\color{blue}C(\boldsymbol{x}) = 0}$ (yes), then
cancel **one-time pad**

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{ll} & \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \\ \quad\;\; \utilde{\boldsymbol{s}^\top {\color{blue}\boldsymbol{A}_C} \boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

if $C(\boldsymbol{x}) = 0$ (yes), then cancel **one-time pad**

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{rl} & \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^{\top} \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\text{UEvalCX}} \utilde{\boldsymbol{s}^{\top}(\boldsymbol{A}_C \cancel{- C(\boldsymbol{x}) \cdot \boldsymbol{G}})} \\ \qquad \utilde{\boldsymbol{s}^{\top}\boldsymbol{A}_C\boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

AB-LFE for Circuits of Unbounded Depth

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

if $C(\boldsymbol{x}) = 0$ (yes), then cancel **one-time pad**

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{ll} & \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underline{\boldsymbol{s}^\top(\boldsymbol{A}_C \cancel{- C(\boldsymbol{x}) \cdot \boldsymbol{G}})} \\ \qquad \boxed{\underline{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})}} + \mu \cdot \lfloor q/2 \rceil \qquad\qquad\qquad\qquad \cdot \boldsymbol{G}^{-1}(\boldsymbol{u}) \end{array} \right.$$

AB-LFE Scheme Security

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

when $C(\boldsymbol{x}) = 1$ (no)

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{ll} & \left.\begin{array}{l} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array}\right\} \xrightarrow{\text{UEvalCX}} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} = \boldsymbol{c}_C^\top \\ \boldsymbol{S}, & \\ & \utilde{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

AB-LFE Scheme Security

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{l} \left.\begin{array}{l} \qquad\underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array}\right\} \\ \qquad\boxed{\underline{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})}} + \mu \cdot \lfloor q/2 \rceil \end{array}\right.$$

when $C(\boldsymbol{x}) = 1$ (no)

$$\xrightarrow{\mathtt{UEvalCX}} \underline{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})}$$

$$= \boldsymbol{c}_C^\top$$

$$\boldsymbol{c}_C^\top \boldsymbol{G}^{-1}(\boldsymbol{u}) + \underbrace{1}_{C(\boldsymbol{x})} \cdot \underline{\boldsymbol{s}^\top \boldsymbol{u}}$$

AB-LFE Scheme Security

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \boldsymbol{S},\ \begin{array}{l} \left.\begin{array}{l} \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G}), \\ \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}), \end{array}\right\} \xrightarrow{\mathrm{UEvalCX}} \boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G}) = \boldsymbol{c}_C^\top \\ \boxed{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

when $C(\boldsymbol{x}) = 1$ (no)

$$\boldsymbol{c}_C^\top \boldsymbol{G}^{-1}(\boldsymbol{u}) + \underbrace{1}_{C(\boldsymbol{x})} \cdot \boldsymbol{s}^\top \boldsymbol{u}$$

N.B. Security relies on UEvalCX correctness.

AB-LFE Scheme Security

$$\mathrm{crs} = (\boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{digest}_C = \boldsymbol{A}_C \text{ from UEvalC}$$

when $C(\boldsymbol{x}) = 1$ (no)

$$\mathrm{ct}_{C,\boldsymbol{x}} = \left\{ \begin{array}{ll} & \left.\begin{array}{l} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array}\right\} \xrightarrow{\text{UEvalCX}} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} = \boldsymbol{c}_C^\top \\ \boldsymbol{S}, & \\ & \boxed{\utilde{\boldsymbol{s}^\top \boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u})}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

$$\boldsymbol{c}_C^\top \boldsymbol{G}^{-1}(\boldsymbol{u}) + \underbrace{1}_{C(\boldsymbol{x})} \cdot \utilde{\boldsymbol{s}^\top \boldsymbol{u}}$$

N.B. Security relies on UEvalCX correctness.

$\mathrm{ct}_{C,\boldsymbol{x}} \approx \$$ under csLWE

ABE for Circuits of Unbounded Depth

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{ll} & \left.\begin{array}{l} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \\ \boldsymbol{S}, & \\ & \end{array} \right.$$

ABE for Circuits of Unbounded Depth

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \boldsymbol{S},\ \left.\begin{array}{l} \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array}\right\} \xrightarrow{\mathtt{UEvalCX}} \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x})\cdot\boldsymbol{G})} \right.$$

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE for Circuits of Unbounded Depth

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{r} \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, \;\; \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underline{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \\ \underline{\boldsymbol{s}^\top \boldsymbol{B}}, \;\; \underline{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

“another layer of indirection”

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE for Circuits of Unbounded Depth

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{r} \underline{\boldsymbol{s}^\top (\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, \ \underline{\boldsymbol{s}^\top (\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underline{\boldsymbol{s}^\top (\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \\ \underline{\boldsymbol{s}^\top \boldsymbol{B}}, \ \ \underline{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

“another layer of indirection”

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE for Circuits of Unbounded Depth

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{sk}_C = \boldsymbol{u}_C,\ \ \boldsymbol{B}^{-1}(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C) + \boldsymbol{u})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{r} \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \underline{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underline{\boldsymbol{s}^\top(\boldsymbol{A}_C - C(\boldsymbol{x}) \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(\boldsymbol{u}_C) \\ \underline{\boldsymbol{s}^\top \boldsymbol{B}},\ \ \underline{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

“another layer of indirection”

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE for Circuits of Unbounded Depth

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{sk}_C = \boldsymbol{u}_C,\ \ \boldsymbol{B}^{-1}(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C) + \boldsymbol{u})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \qquad \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top \boldsymbol{B}},\ \ \utilde{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right. \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \begin{array}{r} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - \cancel{C(\boldsymbol{x})} \cdot \boldsymbol{G})} \\ \cdot\, \boldsymbol{G}^{-1}(\boldsymbol{u}_C) \end{array}$$

“another layer of indirection”

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE for Circuits of Unbounded Depth

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{sk}_C = \boldsymbol{u}_C,\ \ \boldsymbol{B}^{-1}(\cancel{\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C)} + \boldsymbol{u})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \qquad \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top \boldsymbol{B}},\ \ \utilde{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right. \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \utilde{\boldsymbol{s}^\top(\cancel{\boldsymbol{A}_C} - \cancel{C(\boldsymbol{x})} \cdot \boldsymbol{G})} \cdot \cancel{\boldsymbol{G}^{-1}(\boldsymbol{u}_C)}$$

“another layer of indirection”

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE for Circuits of Unbounded Depth

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{sk}_C = \boldsymbol{u}_C,\ \ \boldsymbol{B}^{-1}(\cancel{\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C)} + \cancel{\boldsymbol{u}})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \left. \begin{array}{l} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \utilde{\boldsymbol{s}^\top(\cancel{\boldsymbol{A}_C} - \cancel{C(\boldsymbol{x})} \cdot \boldsymbol{G})} \cancel{\cdot \boldsymbol{G}^{-1}(\boldsymbol{u}_C)} \\ \utilde{\boldsymbol{s}^\top \boldsymbol{B}},\ \ \utilde{\cancel{\boldsymbol{s}^\top \boldsymbol{u}}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

“another layer of indirection”

- $\boldsymbol{A}_C$ unknown at Enc time
- security against multiple C’s

ABE Scheme Security

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

$$\mathrm{sk}_C = \boldsymbol{u}_C,\ \ \boldsymbol{B}^{-1}(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C) + \boldsymbol{u})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \qquad \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \utilde{\boldsymbol{s}^\top \boldsymbol{B}},\ \ \utilde{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right. \left. \begin{array}{l} \\ \\ \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \utilde{\boldsymbol{s}^\top(\boldsymbol{A}_C - \overbrace{C(\boldsymbol{x})}^{1} \cdot \boldsymbol{G})}$$

ABE Scheme Security

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

evcsLWE precondition

$$\mathrm{sk}_C = \boldsymbol{u}_C, \quad \boldsymbol{s}^\top(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C) + \boldsymbol{u})$$

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{c} \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G}), \\ \boldsymbol{S}, \quad \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}), \\ \boldsymbol{s}^\top\boldsymbol{B}, \quad \boldsymbol{s}^\top\boldsymbol{u} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

$$\left. \begin{array}{c} \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G}), \\ \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}), \end{array} \right\} \xrightarrow{\mathtt{UEvalCX}} \boldsymbol{s}^\top(\boldsymbol{A}_C - \overbrace{C(\boldsymbol{x})}^{1} \cdot \boldsymbol{G})$$

ABE Scheme Security

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

evcsLWE precondition

$$\mathrm{sk}_C = \boldsymbol{u}_C, \quad \underbrace{\boxed{\boldsymbol{s}^\top(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C))} + \boldsymbol{u})}$$

≈ \$ like in AB-LFE proof

$$\mathrm{ct}_{\boldsymbol{x}} = \left\{ \begin{array}{l} \qquad \underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, \;\; \underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \underset{\sim\sim\sim}{\boldsymbol{s}^\top\boldsymbol{B}}, \;\; \boxed{\underset{\sim\sim\sim}{\boldsymbol{s}^\top\boldsymbol{u}}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right.$$

hides message

$$\left.\begin{array}{l} \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G}), \\ \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}), \end{array}\right\} \xrightarrow{\mathrm{UEvalCX}} \underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_C - \overbrace{C(\boldsymbol{x})}^{1} \cdot \boldsymbol{G})}$$

ABE Scheme Security

$$\mathrm{mpk} = (\boldsymbol{B}, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \boldsymbol{u})$$

evcsLWE precondition

$$\mathrm{sk}_C = \boldsymbol{u}_C, \quad \uwave{\boxed{\boldsymbol{s}^\top(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C)} + \boldsymbol{u})}$$

≈ $ like in AB-LFE proof

$$\mathrm{ct}_{\boldsymbol{x}} = \begin{cases} \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - \boldsymbol{x}^\top \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, \ \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \uwave{\boldsymbol{s}^\top \boldsymbol{B}}, \ \boxed{\uwave{\boldsymbol{s}^\top \boldsymbol{u}}} + \mu \cdot \lfloor q/2 \rceil \end{cases}$$

$$\left.\begin{matrix} \\ \\ \end{matrix}\right\} \xrightarrow{\mathtt{UEvalCX}} \uwave{\boldsymbol{s}^\top(\boldsymbol{A}_C - \overbrace{C(\boldsymbol{x})}^{1} \cdot \boldsymbol{G})}$$

hides message

No evcsLWE? Use generic pairing group to compute $[\![\boldsymbol{s}^\top(\boldsymbol{A}_C \boldsymbol{G}^{-1}(\boldsymbol{u}_C) + \boldsymbol{u})]\!]$.

[LLL]

bootstrapping attribute encoding for unbounded homomorphic evaluation

bootstrapping attribute encoding for unbounded homomorphic evaluation

$\Longrightarrow$ **depth-unbounded**
LFE, 1-key FE, reusable GC, ABE
from lattices

bootstrapping attribute encoding for unbounded homomorphic evaluation

$\Longrightarrow$ **depth-unbounded**
LFE, 1-key FE, reusable GC, ABE
from lattices

?

- perfect correctness (e.g., by detection?)
- ABE security from non-knowledge-type assumption
- non-circular version of bootstrapping

bootstrapping attribute encoding for unbounded homomorphic evaluation

$\Longrightarrow$ **depth-unbounded**
LFE, 1-key FE, reusable GC, ABE
from lattices

?

- perfect correctness (e.g., by detection?)
- ABE security from non-knowledge-type assumption
- non-circular version of bootstrapping

Thank you!

`https://luoji.bio/`
`luoji@cs.washington.edu`