lattice circuits of unbounded depth attribute-based encryption

基于格构造支持不限深度的电路的属性加密

最优规模乱码电路、凝练的函数求值等

garbled circuits laconic function evaluation

Yao-Ching Hsieh
謝耀慶

Rachel Lin
林蕙佳

Ji Luo
罗辑

大纲（综述部分）

- 预备概念
  - 同态加密 (HE) 与属性加密 (ABE)
  - 受限 (bounded) 与不限 (unbounded)
- 成果介绍
  - 先前同态原语 (primitive) 的状况
  - 格相关的假设
  - 本作新结果
- 核心：不限深度的公钥、属性编码 (attribute encoding) 同态
- 应用
- 未解问题

同态加密 (homomorphic encryption) [RAD78]

$$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$$

$$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$$

同态加密 (homomorphic encryption) [RAD78]

$$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$$

$$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$$

$$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$$

同态加密 (homomorphic encryption) [RAD78]

$$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$$

$$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$$

$$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$$

- 支持**任意**电路 f
- $|\mathrm{pk}| = \mathrm{poly}(\lambda) = O(1)$ 与 f **无关**
- $|\mathrm{hct}| = O(|明文|)$ 与 f **无关**

同态加密 (homomorphic encryption) [RAD78]

fully 全同态加密	vs.	leveled 定层同态加密
$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$		$\mathrm{Gen}(1^d) \to (\mathrm{pk}, \mathrm{sk})$
$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$		—"—
$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$		$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$

- 支持**任意**电路 f
- $|\mathrm{pk}| = \mathrm{poly}(\lambda) = O(1)$ 与 f **无关**
- $|\mathrm{hct}| = O(|明文|)$ 与 f **无关**

同态加密 (homomorphic encryption) [RAD78]

fully
全同态加密

vs.

leveled
定层同态加密

$$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$$

$$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$$

$$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$$

- 支持**任意**电路 f
- $|\mathrm{pk}| = \mathrm{poly}(\lambda) = O(1)$ 与 f **无关**
- $|\mathrm{hct}| = O(|明文|)$ 与 f **无关**

$$\mathrm{Gen}(1^d) \to (\mathrm{pk}, \mathrm{sk})$$

—"—

$$\mathrm{HEval}(\underbrace{f}_{\boxed{深度 \leq d}}, \boxed{x}) \to \boxed{f(x)}$$

- 仅支持**预先以多项式界定**的深度

同态加密 (homomorphic encryption) [RAD78]

fully
全同态加密

vs.

leveled
定层同态加密

$$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$$

$$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$$

$$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$$

- 支持**任意**电路 f
- $|\mathrm{pk}| = \mathrm{poly}(\lambda) = O(1)$ 与 f **无关**
- $|\mathrm{hct}| = O(|明文|)$ 与 f **无关**

$$\mathrm{Gen}(1^d) \to (\mathrm{pk}, \mathrm{sk})$$

—"—

$$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$$

深度 $\le d$

- 仅支持**预先以多项式界定**的深度
- $|\mathrm{pk}| = \mathrm{poly}(d)$ 随**深度上界**增加
- $|\mathrm{hct}| = |明文| \cdot \mathrm{poly}(d)$

同态加密 (homomorphic encryption) [RAD78]

fully
全同态加密

$$\mathrm{Gen}() \to (\mathrm{pk}, \mathrm{sk})$$

$$\mathrm{Enc}(\mathrm{pk}, x) \to \mathrm{hct}(x) = \boxed{x}$$

$$\mathrm{HEval}(f, \boxed{x}) \to \boxed{f(x)}$$

- 支持**任意**电路 f
- $|\mathrm{pk}| = \mathrm{poly}(\lambda) = O(1)$ 与 f **无关**
- $|\mathrm{hct}| = O(|明文|)$ 与 f **无关**

- 需要**循环** (circular) **LWE**

vs.

leveled
定层同态加密

$$\mathrm{Gen}(1^d) \to (\mathrm{pk}, \mathrm{sk})$$

—"—

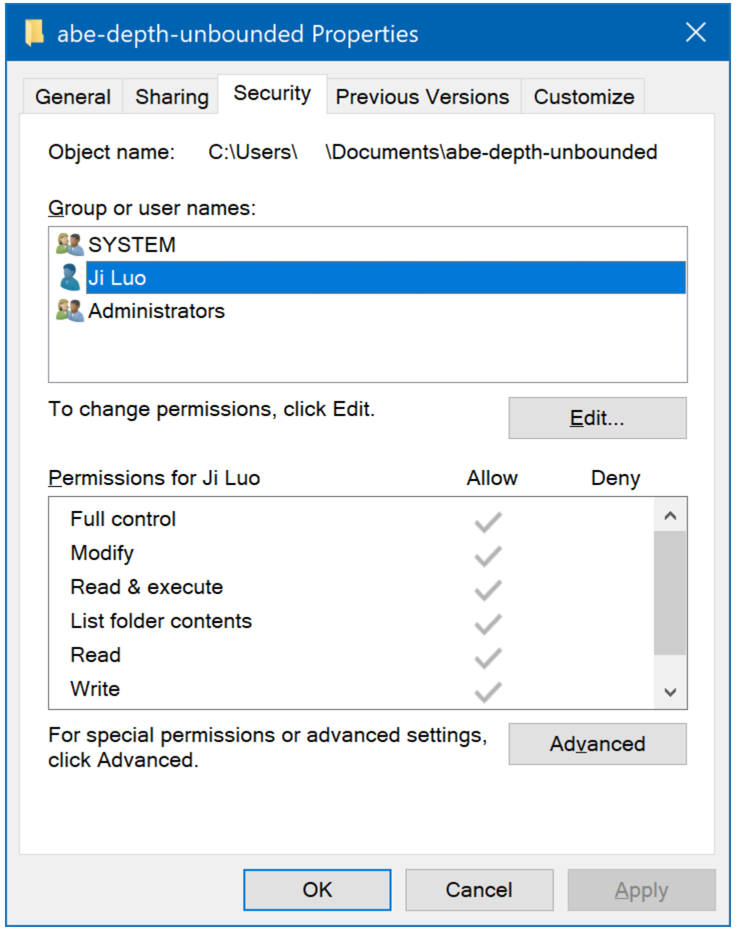
$$\underbrace{\mathrm{HEval}(f,}_{\boxed{\text{深度} \le d}} \boxed{x}) \to \boxed{f(x)}$$

- 仅支持**预先以多项式界定**的深度
- $|\mathrm{pk}| = \mathrm{poly}(d)$ 随**深度上界**增加
- $|\mathrm{hct}| = |明文| \cdot \mathrm{poly}(d)$

- 可基于 **LWE** 构造

属性加密 (attribute-based encryption) [GPSW06]

“用密码学而不是简单的 if 实现权限控制”



Windows NTFS 访问控制列表：

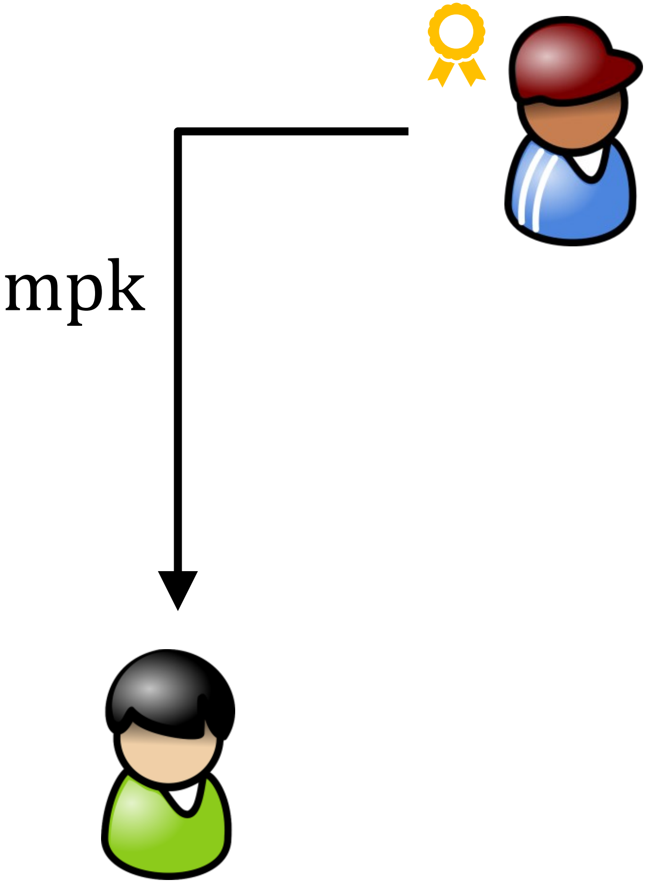
有且只有 **Alice 和不是 Bob 的管理员**可以访问

属性加密：语法、正确性

$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$

属性加密：语法、正确性

$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$



$\mathrm{Enc}(\mathrm{mpk}, {\color{blue}x}, {\color{red}\mu}) \to \mathrm{ct}_{\color{blue}x}({\color{red}\mu})$

属性 x **消息** $\mu \in \{0,1\}$

属性加密：语法、正确性

$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$

$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$

策略 $f: x \mapsto$ 可/否

mpk

$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

属性 x **消息** $\mu \in \{0,1\}$

属性加密：语法、正确性

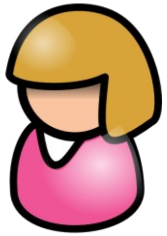
$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$

$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$

策略 $f : x \mapsto$ 可/否

mpk

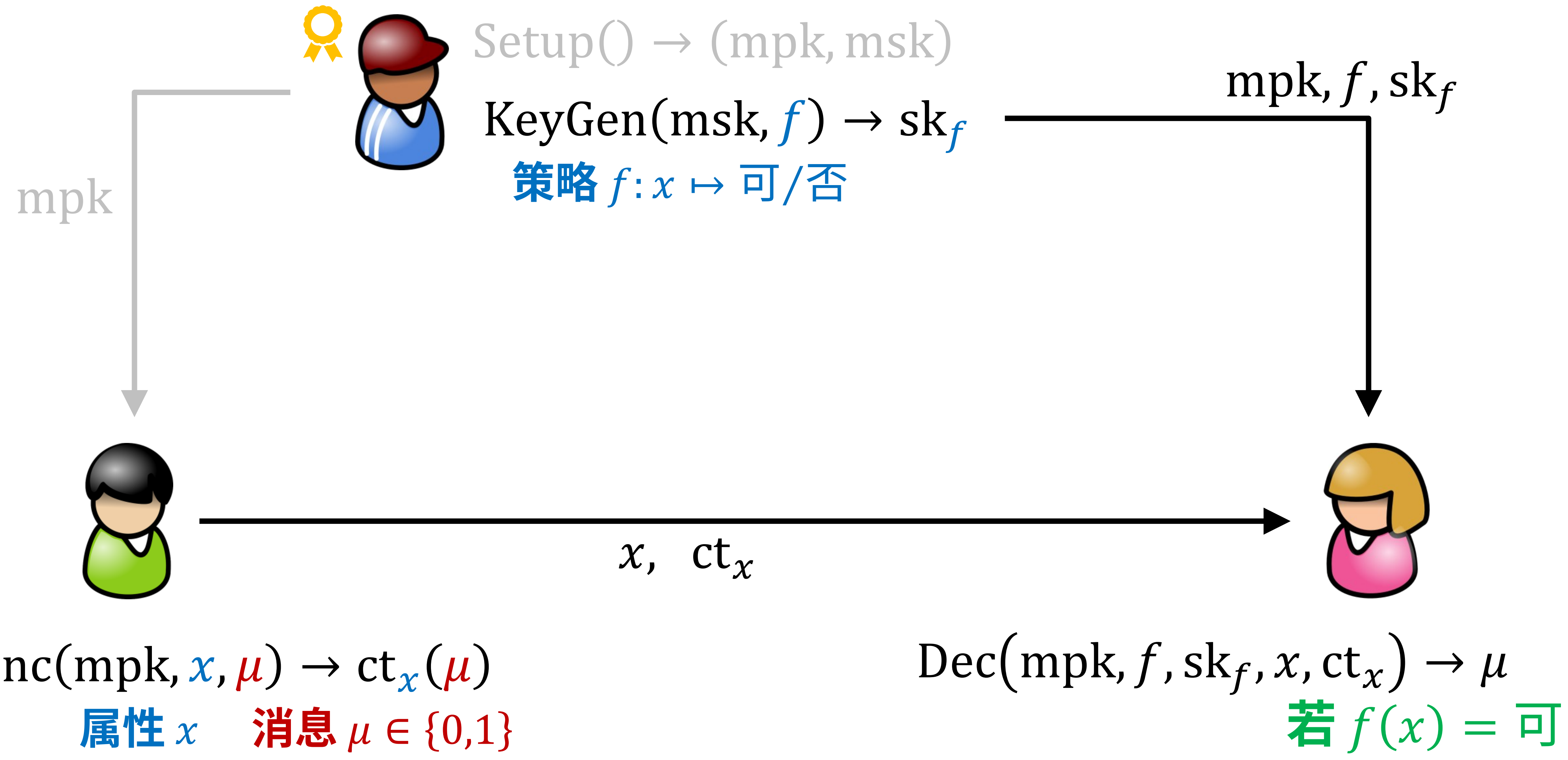
$\mathrm{mpk}, f, \mathrm{sk}_f$



$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

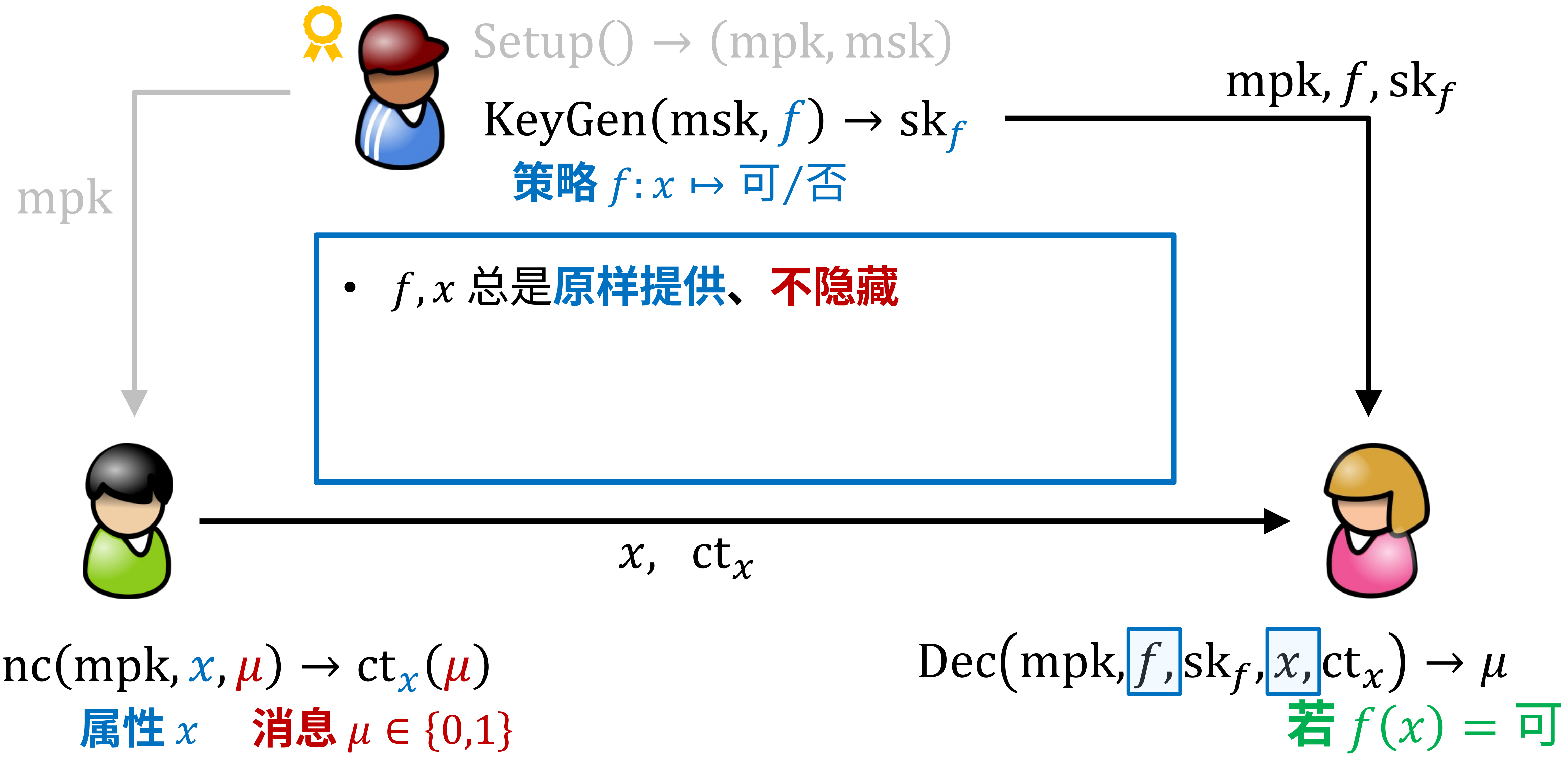
属性 x **消息** $\mu \in \{0,1\}$

属性加密：语法、正确性



$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$
$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$
策略 $f: x \mapsto$ 可/否
$\mathrm{mpk}, f, \mathrm{sk}_f$
mpk
$x,\ \mathrm{ct}_x$
$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$
属性 x 消息 $\mu \in \{0,1\}$
$\mathrm{Dec}(\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x) \to \mu$
若 $f(x) =$ 可

属性加密：语法、正确性



$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$
$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$
策略 $f: x \mapsto$ 可/否
$\mathrm{mpk}, f, \mathrm{sk}_f$
mpk
• f, x 总是原样提供、不隐藏
$x,\ \ \mathrm{ct}_x$
$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$
属性 x 消息 $\mu \in \{0,1\}$
$\mathrm{Dec}(\mathrm{mpk}, \boxed{f}, \mathrm{sk}_f, \boxed{x}, \mathrm{ct}_x) \to \mu$
若 $f(x) =$ 可

属性加密：语法、正确性

$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$

$\mathrm{mpk}, f, \mathrm{sk}_f$

$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$

策略 $f: x \mapsto$ 可/否

mpk

- f, x 总是**原样提供**、**不隐藏**
- $\mathrm{sk}_f, \mathrm{ct}_x$ 与 f, x **绑定**
  - 可以想成散列 (hash)、签名、消息认证码 (MAC)
  - 甚至可能有 $|\mathrm{sk}_f| < |f|$ 和 $|\mathrm{ct}_x| < |x|$

$x, \ \mathrm{ct}_x$

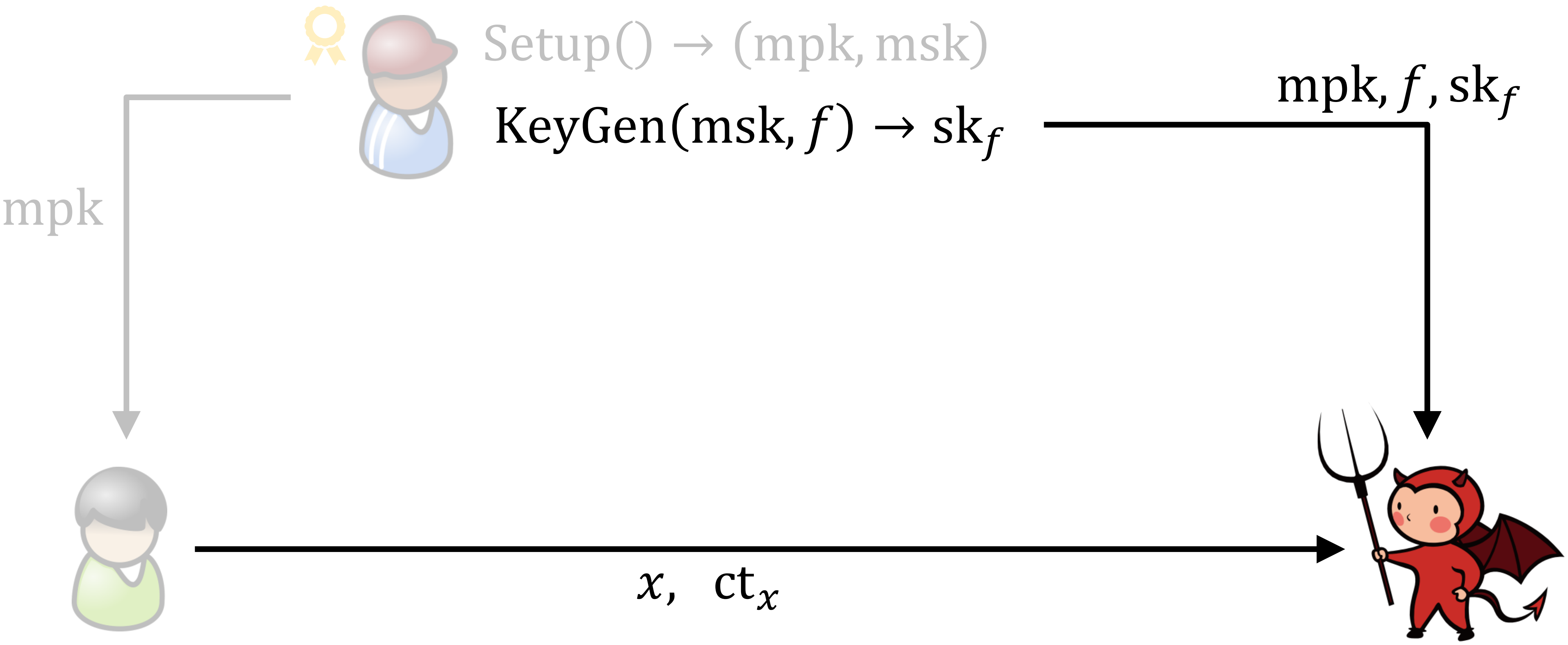
$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

属性 x **消息** $\mu \in \{0,1\}$

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

若 $f(x) =$ 可

属性加密：安全性

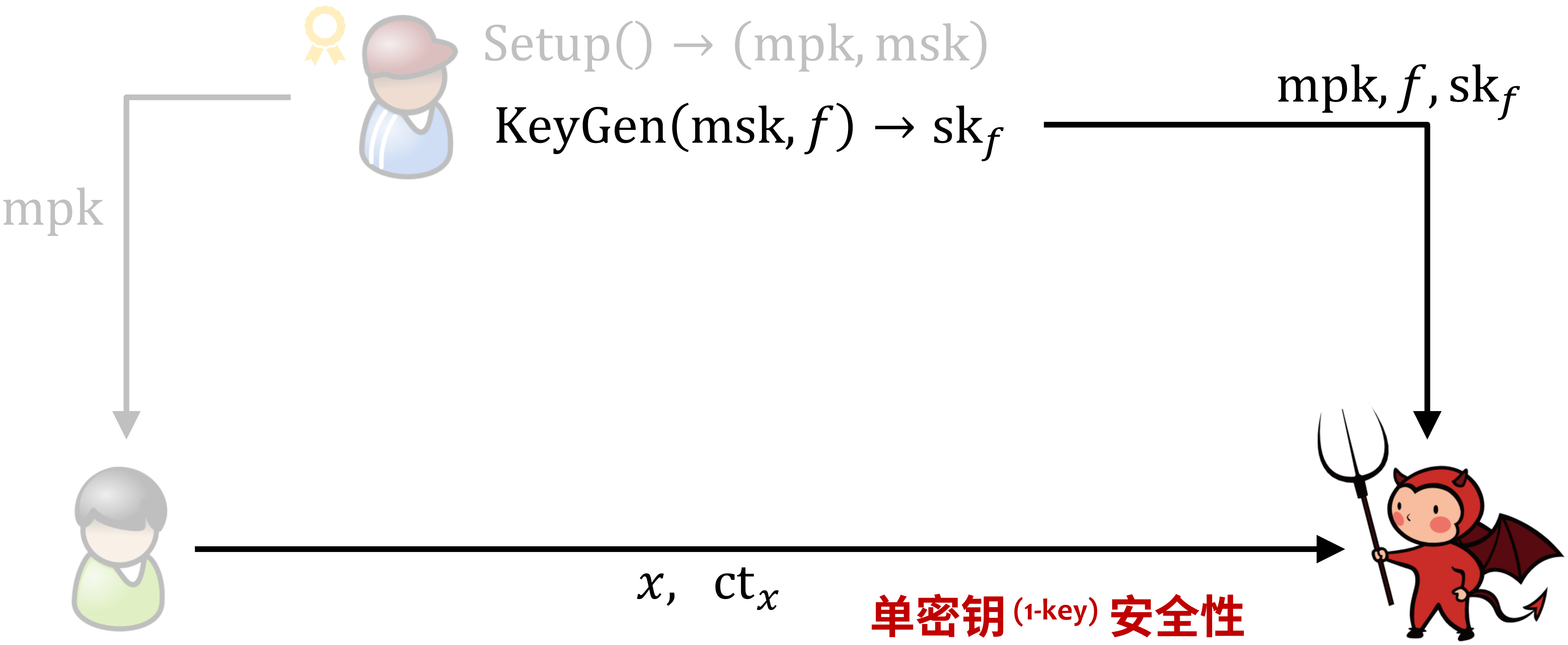


$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

$\big(\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x(0)\big) \approx \big(\cdots, \mathrm{ct}_x(1)\big)$

若 $f(x) =$ 否

属性加密：安全性



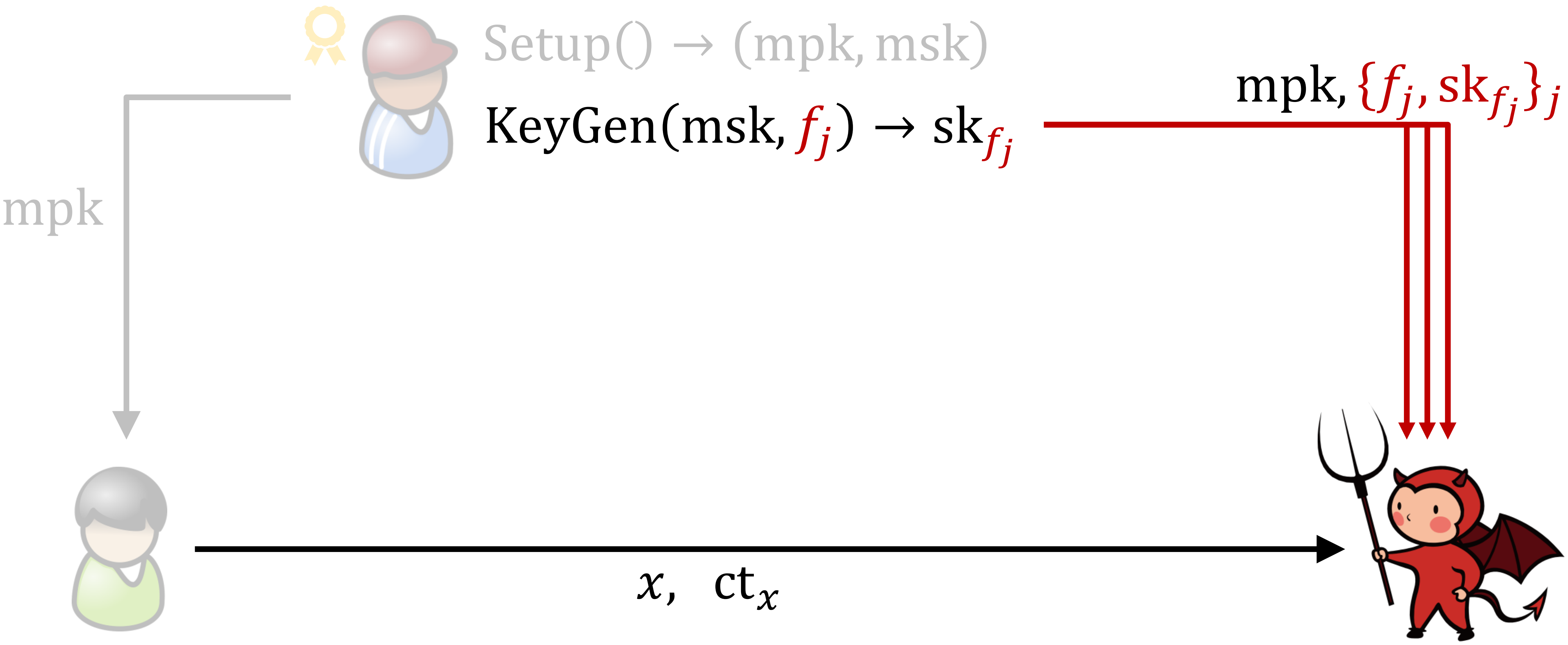
单密钥 (1-key) 安全性

$\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x(\mu)$

$$\left(\mathsf{mpk}, \boxed{f, \mathsf{sk}_f,} x, \mathsf{ct}_x(0)\right) \approx \left(\cdots, \mathsf{ct}_x(1)\right)$$

若 $f(x) =$ 否

属性加密：安全性（续）



$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

$$\left(\mathrm{mpk}, \{f_j, \mathrm{sk}_{f_j}\}_j, x, \mathrm{ct}_x(0)\right) \approx \left(\cdots, \mathrm{ct}_x(1)\right)$$

若 $f_j(x) =$ 否 **对所有** j

属性加密：安全性（续）

$\mathsf{Setup}() \to (\mathsf{mpk}, \mathsf{msk})$

$\mathsf{KeyGen}(\mathsf{msk}, f_j) \to \mathsf{sk}_{f_j}$

$\mathsf{mpk}, \{f_j, \mathsf{sk}_{f_j}\}_j$

mpk

collusion resistance

- **抗沆瀣一气**

$x, \ \mathsf{ct}_x$

$\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x(\mu)$

$$\big(\mathsf{mpk}, \{f_j, \mathsf{sk}_{f_j}\}_j, x, \mathsf{ct}_x(0)\big) \approx \big(\cdots, \mathsf{ct}_x(1)\big)$$

若 $f_j(x) =$ 否 **对所有** j

属性加密：安全性（续）

$\mathrm{Setup}() \to (\mathrm{mpk}, \mathrm{msk})$

$\mathrm{KeyGen}(\mathrm{msk}, f_j) \to \mathrm{sk}_{f_j}$

$\mathrm{mpk}, \{f_j, \mathrm{sk}_{f_j}\}_j$

mpk

collusion resistance

- **抗沆瀣一气**

adaptive　selective　static

- 不同强度：适应性、选择性、**静态**
  - **非常选择性**是指 $\{f_j\}_j, x$ 在最开始就一次性选好

very selective

x, ct_x

$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

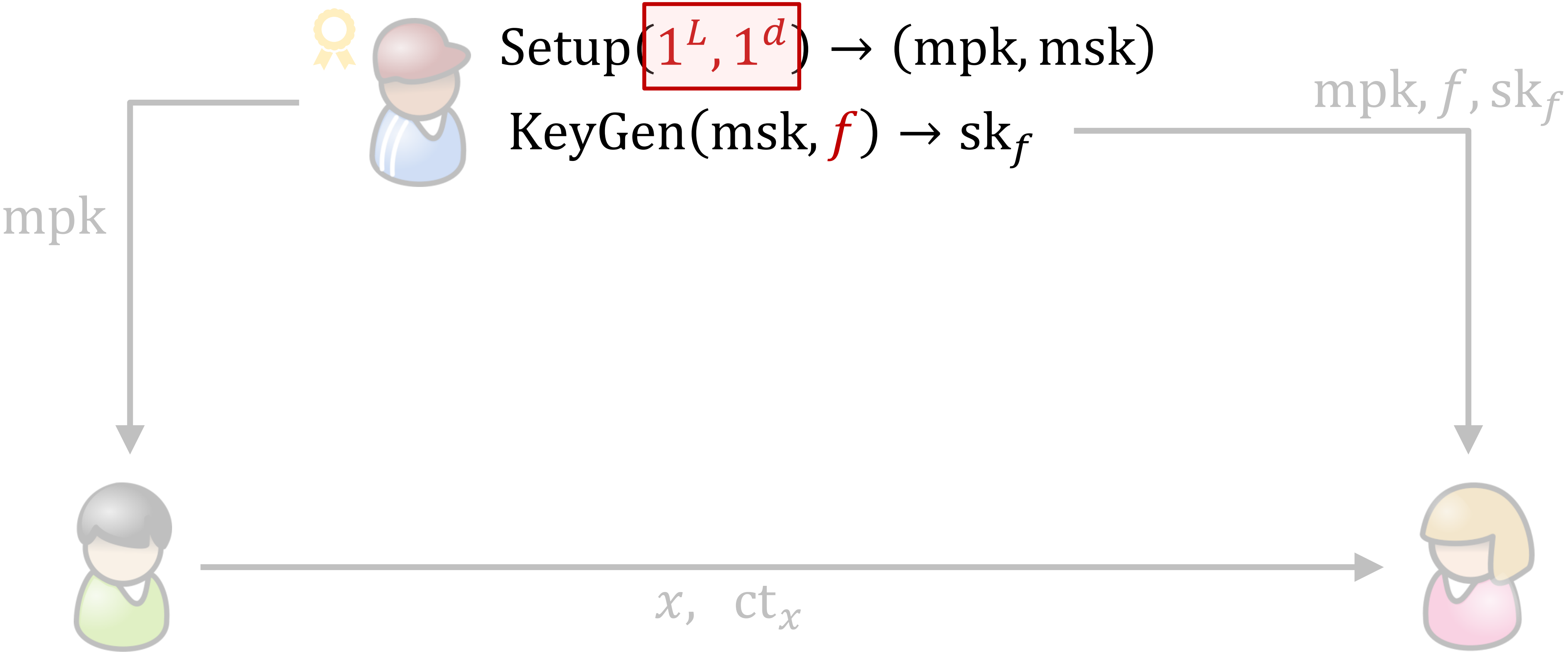
$\left(\mathrm{mpk}, \{f_j, \mathrm{sk}_{f_j}\}_j, x, \mathrm{ct}_x(0)\right) \approx \left(\cdots, \mathrm{ct}_x(1)\right)$

若 $f_j(x) =$ 否 **对所有** j

属性加密：受限 (bounded) 与不限 (unbounded)

$\mathrm{Setup}(\boxed{1^L, 1^d}) \to (\mathrm{mpk}, \mathrm{msk})$

$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$



$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

属性加密：受限 (bounded) 与不限 (unbounded)

$\mathsf{Setup}(\boxed{1^L, 1^d}) \to (\mathsf{mpk}, \mathsf{msk})$

$\boxed{f \text{ 深度} \leq d}$ $\mathsf{KeyGen}(\mathsf{msk}, f) \to \mathsf{sk}_f$

$\mathsf{mpk}, f, \mathsf{sk}_f$

mpk

$x, \ \mathsf{ct}_x$

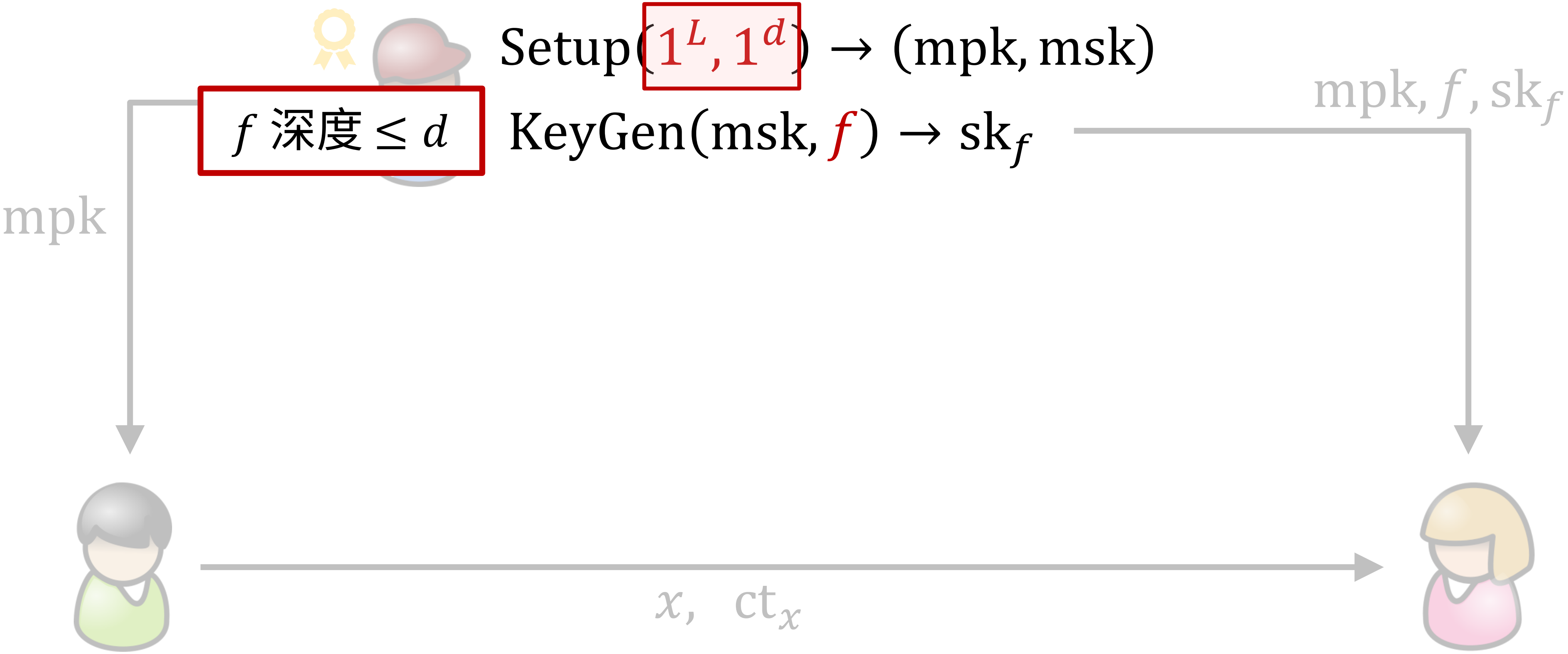
$\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x(\mu)$

$\boxed{|x| = L}$

属性加密：受限 (bounded) 与不限 (unbounded)

$\mathrm{Setup}(\boxed{1^L, 1^d}) \to (\mathrm{mpk}, \mathrm{msk})$

$\boxed{f \text{ 深度} \le d}$ $\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$



$\mathrm{Enc}(\mathrm{mpk}, x, \mu) \to \mathrm{ct}_x(\mu)$

$\boxed{|x| = L}$ ← 容易解决，暂且不谈

先前同态原语 (primitive) 的状况

laconic function evaluation
凝练的函数求值

同态签名

commitment
同态封笺

reusable garbled circuits
可复用的乱码电路

同态加密

constrained PRF
约束伪随机函数

属性加密

lockable obfuscation
可上锁混淆

- 全部：可基于 LWE 构造**深度受限**、**尺寸随深度增加**的版本

先前同态原语 (primitive) 的状况

laconic function evaluation
凝练的函数求值

同态签名

commitment
同态封笺

reusable garbled circuits
可复用的乱码电路

同态加密

lockable obfuscation
可上锁混淆

constrained PRF
约束伪随机函数

属性加密

循环 LWE $\Longrightarrow$ 深度不限

- 全部：可基于 LWE 构造**深度受限**、**尺寸随深度增加**的版本
- **某一些**：可基于**循环 LWE** 构造**深度不限**版本

先前同态原语 (primitive) 的状况

laconic function evaluation
凝练的函数求值

同态签名

commitment
同态封笺

reusable garbled circuits
可复用的乱码电路

同态加密

lockable obfuscation
可上锁混淆

constrained PRF
约束伪随机函数

属性加密

循环 LWE $\Longrightarrow$ 深度不限

- 全部：可基于 LWE 构造**深度受限**、**尺寸随深度增加**的版本
- **某一些**：可基于**循环 LWE** 构造**深度不限**版本
- **另一些**：暂时需要**不可区分混淆** ($i\mathcal{O}$)

先前同态原语 (primitive) 的状况

laconic function evaluation
凝练的函数求值

同态签名

commitment
同态封笺

reusable garbled circuits
可复用的乱码电路

同态加密

lockable obfuscation
可上锁混淆

constrained PRF
约束伪随机函数

属性加密

循环 LWE $\Longrightarrow$ 深度不限

- 全部：可基于 LWE 构造**深度受限、尺寸随深度增加**的版本
- **某一些**：可基于**循环 LWE** 构造**深度不限**版本
- **另一些**：暂时需要**不可区分混淆** ($i\mathcal{O}$)

结构类似 [GSW13]，为何有些受限、有些不限？

本作新结果

laconic function evaluation
凝练的函数求值

reusable garbled circuits
可复用的乱码电路

属性加密

♥ **基于格、深度不限**

同态签名

同态加密

lockable obfuscation
可上锁混淆

commitment
同态封笺

constrained PRF
约束伪随机函数

本作新结果

laconic function evaluation
凝练的函数求值

reusable garbled circuits
可复用的乱码电路

属性加密

同态签名

同态加密

lockable obfuscation
可上锁混淆

commitment
同态封笺

constrained PRF
约束伪随机函数

♥ 基于格、深度不限

循环 LWE ⟹ 深度不限
♥ 适用范围扩大

LWE 假设 [R05]

$$\boxed{\overline{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}}, \quad \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top}\,\boxed{\overline{\boldsymbol{A}}} + \boxed{\boldsymbol{e}^\top}$$

LWE 假设 [R05]

$$\boxed{\overline{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}}, \quad \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top}\ \boxed{\overline{\boldsymbol{A}}} + \boxed{\boldsymbol{e}^\top}$$

$$\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^n$$

LWE 假设 [R05]

$$\overline{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \quad \boldsymbol{c}^\top = \boldsymbol{r}^\top \overline{\boldsymbol{A}} + \boldsymbol{e}^\top$$

$\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^n$

$\boldsymbol{e} \xleftarrow{\$} \chi^m$ 满足 $\|\boldsymbol{e}\|_\infty \leq B$

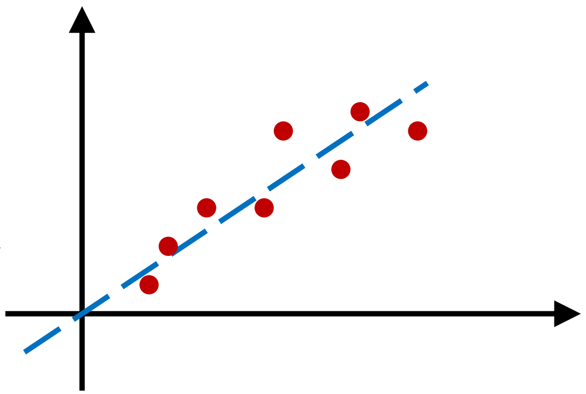
LWE 假设 [R05]

$\overline{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, $\boldsymbol{c}^\top = \boldsymbol{r}^\top \overline{\boldsymbol{A}} + \boldsymbol{e}^\top$

$\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^{n}$

$\boldsymbol{e} \xleftarrow{\$} \chi^m$ 满足 $\|\boldsymbol{e}\|_\infty \le B$

LWE 样本

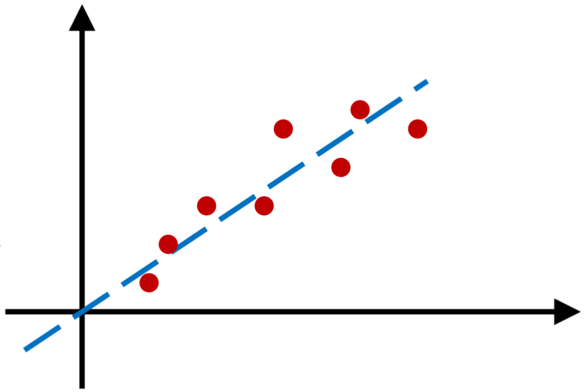


LWE 假设 [R05]

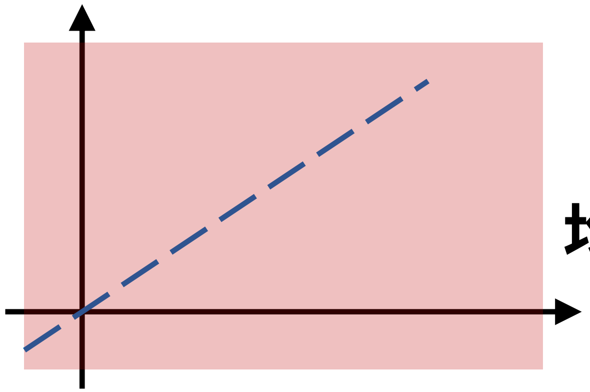
$$\boxed{\bar{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}},\quad \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top}\ \boxed{\bar{\boldsymbol{A}}} + \boxed{\boldsymbol{e}^\top} \approx \bar{\boldsymbol{A}}, \$$$

$$\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^n \qquad \boldsymbol{e} \xleftarrow{\$} \chi^m \text{ 满足 } \|\boldsymbol{e}\|_\infty \le B$$

LWE 样本



$\approx$



均匀随机样本

LWE 假设 [R05]

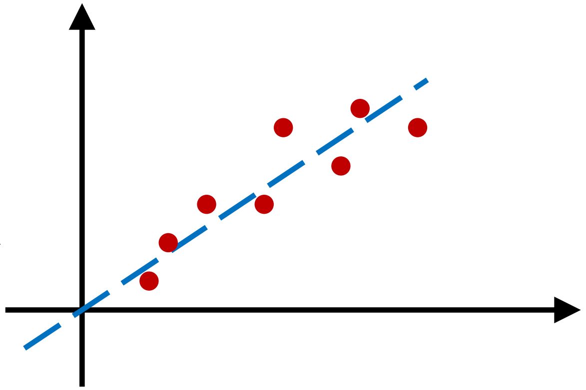
$$\boxed{\bar{\boldsymbol{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}}, \quad \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top}\ \boxed{\bar{\boldsymbol{A}}} + \boxed{\boldsymbol{e}^\top} \approx \bar{\boldsymbol{A}}, \$$$

$\cancel{\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^n}$

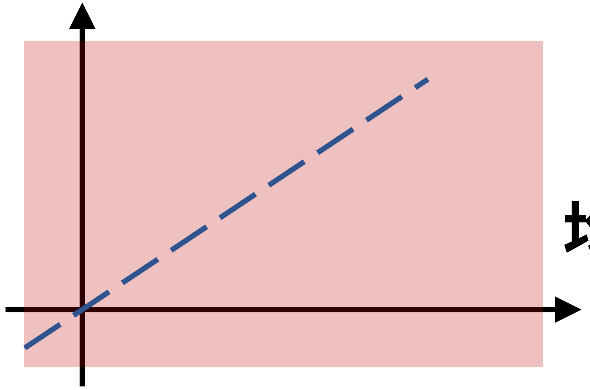
$\boldsymbol{r} \xleftarrow{\$} \chi^n$

$\boldsymbol{e} \xleftarrow{\$} \chi^m$ 满足 $\|\boldsymbol{e}\|_\infty \le B$

LWE 样本



$\approx$



均匀随机样本

循环 LWE 假设

$$\overline{\boldsymbol{A}},\ \ \boldsymbol{c}^\top = \boldsymbol{r}^\top\overline{\boldsymbol{A}} + \boldsymbol{e}^\top + \boldsymbol{f}(\boldsymbol{r}) \quad \approx \quad \overline{\boldsymbol{A}},\ \ \$$$

循环 LWE 假设

$$\overline{\boldsymbol{A}},\ \ \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top}\,\overline{\boldsymbol{A}} + \boldsymbol{e}^\top + \boldsymbol{f}(\boldsymbol{r}) \quad \approx \quad \overline{\boldsymbol{A}},\ \ \$$$

私钥

循环 LWE 假设

encryption randomness
加密算法的随机数

one-time pad
一次性密钥

$$\boxed{\bar{\boldsymbol{A}},}\ \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top \bar{\boldsymbol{A}} + \boldsymbol{e}^\top} + \boldsymbol{f}(\boldsymbol{r}) \quad \approx \quad \bar{\boldsymbol{A}},\ \$$$

私钥

循环 LWE 假设

encryption randomness
加密算法的随机数

one-time pad
一次性密钥

$$\underbrace{\boxed{\overline{\boldsymbol{A}},}\ \boldsymbol{c}^{\top} = \boxed{\boldsymbol{r}^{\top}\overline{\boldsymbol{A}} + \boldsymbol{e}^{\top}} + \boldsymbol{f}(\boldsymbol{r})}_{\text{用私钥 } \boldsymbol{r} \text{ 加密 } \boldsymbol{f}(\boldsymbol{r}) \text{ 的密文}} \approx \overline{\boldsymbol{A}},\ \$$$

私钥

循环 LWE 假设

encryption randomness
加密算法的随机数

one-time pad
一次性密钥

$$\underbrace{\boxed{\overline{\boldsymbol{A}},}\ \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top}\boxed{\overline{\boldsymbol{A}} + \boldsymbol{e}^\top} + \boldsymbol{f}(\boldsymbol{r})}_{\text{用私钥 } \boldsymbol{r} \text{ 加密 } \boldsymbol{f}(\boldsymbol{r}) \text{ 的密文}} \approx \overline{\boldsymbol{A}},\ \$$$

私钥

- LWE 蕴含**某些** $\boldsymbol{f}$ 的版本

循环 LWE 假设

encryption randomness
加密算法的随机数

one-time pad
一次性密钥

私钥

$$\underbrace{\boxed{\overline{\boldsymbol{A}},}\ \boldsymbol{c}^\top = \boxed{\boldsymbol{r}^\top \overline{\boldsymbol{A}} + \boldsymbol{e}^\top} + \boldsymbol{f}(\boldsymbol{r})}_{\text{用私钥 } \boldsymbol{r} \text{ 加密 } \boldsymbol{f}(\boldsymbol{r}) \text{ 的密文}} \approx \overline{\boldsymbol{A}},\ \$$$

- LWE 蕴含**某些** $\boldsymbol{f}$ 的版本
- FHE 所用版本，**不知**如何归约为 LWE

循环 LWE 假设

encryption randomness
加密算法的随机数

one-time pad
一次性密钥

$$\underbrace{\boxed{\bar{\boldsymbol{A}},}\ \boldsymbol{c}^\top = \boxed{\underbrace{\boldsymbol{r}}_{\text{私钥}}{}^\top\bar{\boldsymbol{A}} + \boldsymbol{e}^\top} + \boldsymbol{f}(\boldsymbol{r})}_{\text{用私钥 } \boldsymbol{r} \text{ 加密 } \boldsymbol{f}(\boldsymbol{r}) \text{ 的密文}} \approx \bar{\boldsymbol{A}},\ \$$$

- LWE 蕴含**某些** $\boldsymbol{f}$ 的版本
- FHE 所用版本，**不知**如何归约为 LWE
- 研究虽尚不透彻，姑且还算**标准**假设

循环 LWE 假设

$$\underbrace{\boxed{\overset{\text{encryption randomness}}{\underset{}{\text{加密算法的随机数}}}\ \overline{\boldsymbol{A}},}\ \boldsymbol{c}^\top = \underset{\text{私钥}}{\boxed{\boldsymbol{r}^\top}}\overline{\boldsymbol{A}} + \boldsymbol{e}^\top + \boldsymbol{f}(\boldsymbol{r})}_{\text{用私钥 } \boldsymbol{r} \text{ 加密 } \boldsymbol{f}(\boldsymbol{r}) \text{ 的密文}} \approx \overline{\boldsymbol{A}},\ \$$$

(one-time pad / 一次性密钥: $\boldsymbol{r}^\top\overline{\boldsymbol{A}} + \boldsymbol{e}^\top$)

- LWE 蕴含**某些** $\boldsymbol{f}$ 的版本
- FHE 所用版本，**不知**如何归约为 LWE
- 研究虽尚不透彻，姑且还算**标准**假设

- 本作所用版本即 FHE 所用版本

凝练的函数求值 (LFE)

$f:\{0,1\}^L \rightarrow \{0,1\}$

$x \in \{0,1\}^L$

$f(x)$

凝练的函数求值 (LFE)

$$\mathrm{crs} \xleftarrow{\$} \mathrm{crsGen}(\cdots)$$

$f: \{0,1\}^L \to \{0,1\}$

$x \in \{0,1\}^L$

$f(x)$

凝练的函数求值 (LFE)

$$\mathrm{crs} \stackrel{\$}{\leftarrow} \mathrm{crsGen}(\cdots)$$

$f: \{0,1\}^L \to \{0,1\}$

$x \in \{0,1\}^L$

$$\mathrm{digest}_f \leftarrow \mathrm{Compress}(\mathrm{crs}, f)$$

$f(x)$

凝练的函数求值 (LFE)

$$\mathrm{crs} \xleftarrow{\$} \mathrm{crsGen}(\cdots)$$

$f : \{0,1\}^L \to \{0,1\}$

$$\mathrm{digest}_f \leftarrow \mathrm{Compress}(\mathrm{crs}, f)$$

$$\mathrm{ct}_f(x) \xleftarrow{\$} \mathrm{Enc}\left(\mathrm{crs}, \mathrm{digest}_f, x\right)$$

$x \in \{0,1\}^L$

$f(x)$

凝练的函数求值 (LFE)

$$\mathrm{crs} \xleftarrow{\$} \mathrm{crsGen}(\cdots)$$

$f : \{0,1\}^L \to \{0,1\}$

$x \in \{0,1\}^L$

$$\xrightarrow{\mathrm{digest}_f \leftarrow \mathrm{Compress}(\mathrm{crs}, f)}$$

$$\xleftarrow{\mathrm{ct}_f(x) \xleftarrow{\$} \mathrm{Enc}(\mathrm{crs}, \mathrm{digest}_f, x)}$$

$f(x) \leftarrow \mathrm{Dec}(\mathrm{crs}, f, \mathrm{ct}_f)$

凝练的函数求值 (LFE)

$$\mathsf{crs} \xleftarrow{\$} \mathsf{crsGen}(\cdots)$$

$f:\{0,1\}^L \to \{0,1\}$

$\mathsf{digest}_f \leftarrow \mathsf{Compress}(\mathsf{crs}, f)$

$\boxed{\mathsf{ct}_f(x)} \xleftarrow{\$} \mathsf{Enc}(\mathsf{crs}, \mathsf{digest}_f, x)$

$x \in \{0,1\}^L$

$f(x) \leftarrow \mathsf{Dec}(\mathsf{crs}, f, \mathsf{ct}_f)$

只透露 $f(x)$ 而隐藏 x

$(\mathsf{crs}, \mathsf{digest}_f, \mathsf{Enc}(\cdots)) \approx (\cdots, \mathsf{Sim}(\mathsf{crs}, f, f(x)))$

凝练的函数求值 (LFE)

$$\mathrm{crs} \xleftarrow{\$} \mathrm{crsGen}(\cdots)$$

$f:\{0,1\}^L \to \{0,1\}$

$x \in \{0,1\}^L$

$\mathrm{digest}_f \leftarrow \mathrm{Compress}(\mathrm{crs}, f)$

$\boxed{\mathrm{ct}_f(x)} \xleftarrow{\$} \mathrm{Enc}(\mathrm{crs}, \mathrm{digest}_f, x)$

$f(x) \leftarrow \mathrm{Dec}(\mathrm{crs}, f, \mathrm{ct}_f)$

只透露 $f(x)$ 而隐藏 x

$(\mathrm{crs}, \mathrm{digest}_f, \mathrm{Enc}(\cdots)) \approx (\cdots, \mathrm{Sim}(\mathrm{crs}, f, f(x)))$

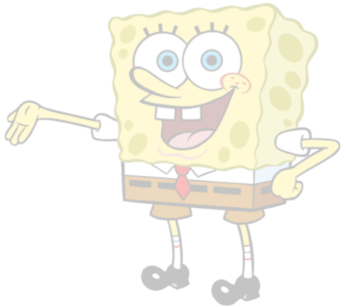
	深度	$\lvert\mathrm{crs}\rvert$	$\lvert\mathrm{digest}_f\rvert$	$\lvert\mathrm{ct}\rvert$	假设
[QWW18]	受限 ✘	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE
本作	不限 ✔	$O(L)$	$O(1)$	$O(L)$	循环 LWE

凝练的**属性**函数求值(**AB**-LFE)

$$\mathrm{crs} \xleftarrow{\$} \mathrm{crsGen}(\cdots)$$

$f:\{0,1\}^L \rightarrow \{可, 否\}$

$x \in \{0,1\}^L, \quad \mu \in \{0,1\}$



$$\mathrm{digest}_f \leftarrow \mathrm{Compress}(\mathrm{crs}, f) \longrightarrow$$

$$\mathrm{ct}_{f,x}(\mu) \xleftarrow{\$} \mathrm{Enc}\big(\mathrm{crs}, \mathrm{digest}_f, x, \mu\big) \longleftarrow$$

$\mu \leftarrow \mathrm{Dec}\big(\mathrm{crs}, f, x, \mathrm{ct}_{f,x}\big)$

若 $f(x) =$ 可

凝练的属性函数求值 (AB-LFE)

$$\mathrm{crs} \xleftarrow{\$} \mathrm{crsGen}(\cdots)$$

$f: \{0,1\}^L \to \{可, 否\}$

$x \in \{0,1\}^L, \quad \mu \in \{0,1\}$

$\mathrm{digest}_f \leftarrow \mathrm{Compress}(\mathrm{crs}, f)$

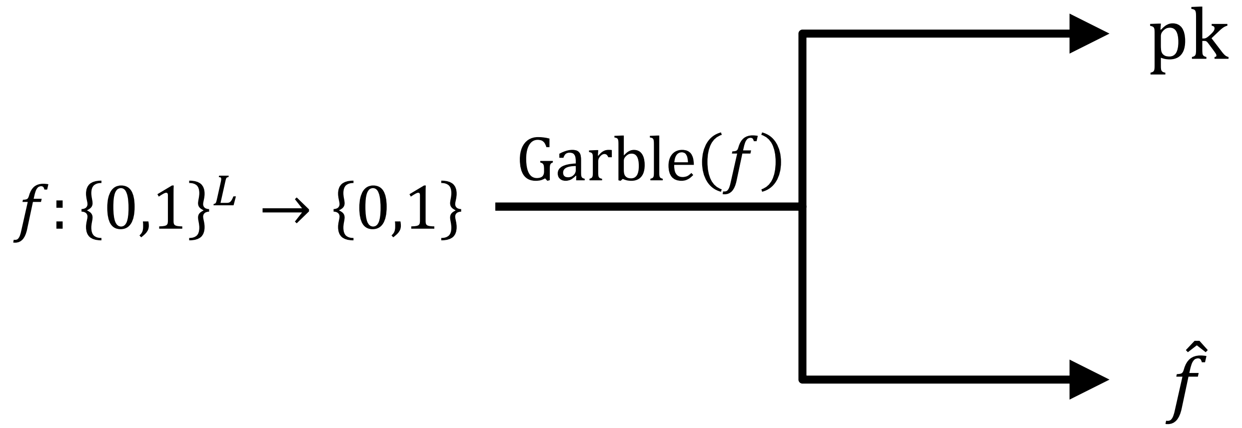
$\boxed{\mathrm{ct}_{f,x}(\mu)} \xleftarrow{\$} \mathrm{Enc}\big(\mathrm{crs}, \mathrm{digest}_f, x, \mu\big)$

若 $f(x) =$ 否，则隐藏 μ

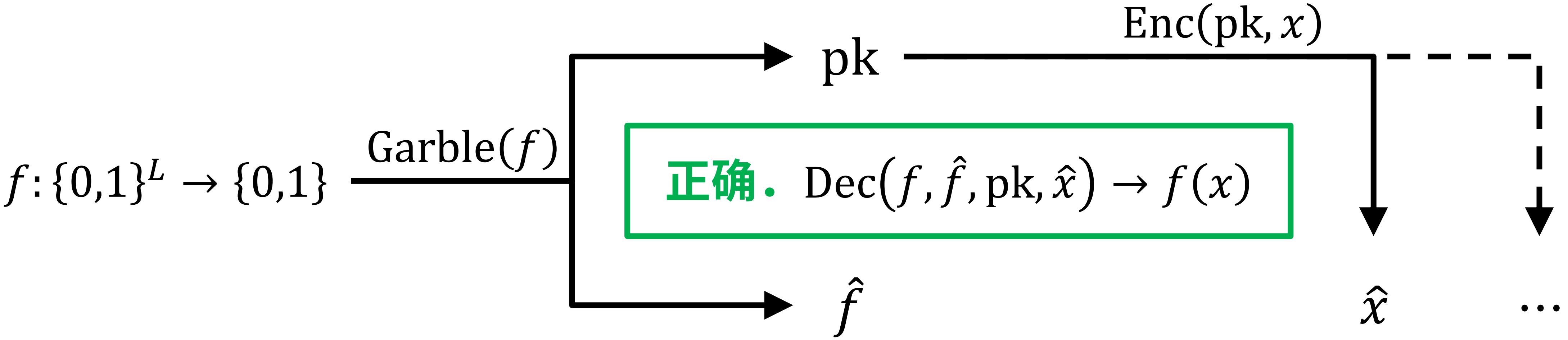
$\mu \leftarrow \mathrm{Dec}\big(\mathrm{crs}, f, x, \mathrm{ct}_{f,x}\big)$

若 $f(x) =$ 可

可复用的乱码电路（单密钥泛函加密）



可复用的乱码电路（单密钥泛函加密）



可复用的乱码电路（单密钥泛函加密）

$f:\{0,1\}^L \to \{0,1\}$ $\xrightarrow{\mathrm{Garble}(f)}$ pk, $\hat{f}$

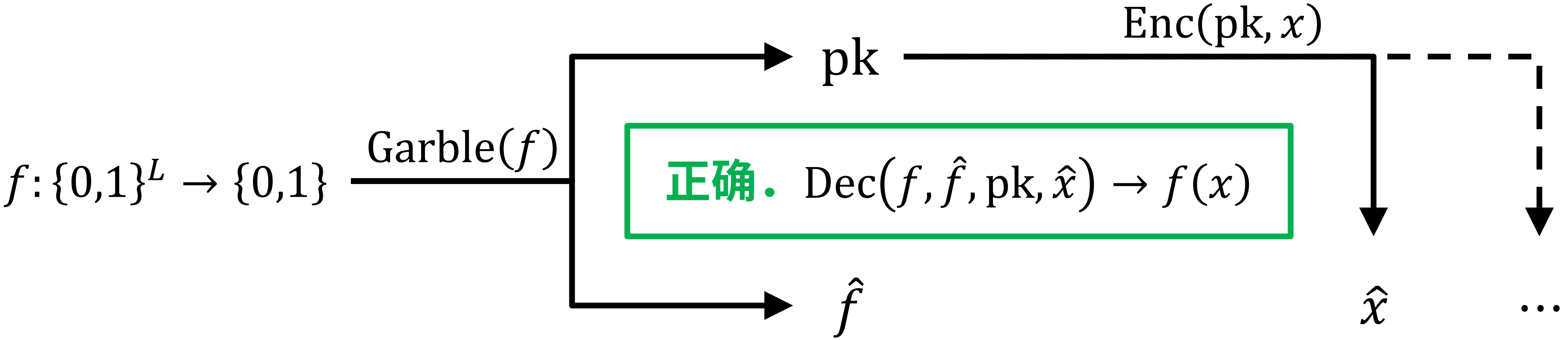
$\mathrm{pk} \xrightarrow{\mathrm{Enc}(\mathrm{pk},x)} \hat{x}$ $\cdots$

正确. $\mathrm{Dec}\big(f,\hat{f},\mathrm{pk},\hat{x}\big) \to f(x)$

安全. 只透露 $f(x)$ 而隐藏 x，即

$$\big(f,\hat{f},\mathrm{pk},\mathrm{Enc}(\cdots)\big) \approx \big(\cdots,\mathrm{Sim}\big(f,\hat{f},\mathrm{pk},f(x)\big)\big)$$

可复用的乱码电路（单密钥泛函加密）



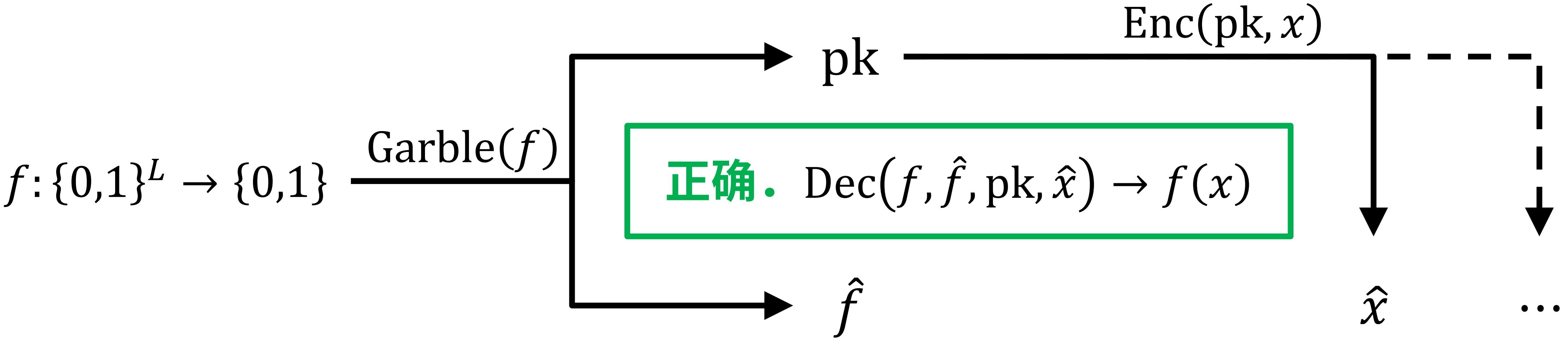
正确. $\mathrm{Dec}\left(f, \hat{f}, \mathrm{pk}, \hat{x}\right) \to f(x)$

安全. 只透露 $f(x)$ 而隐藏 x，即

$$\left(f, \hat{f}, \mathrm{pk}, \mathrm{Enc}(\cdots)\right) \approx \left(\cdots, \mathrm{Sim}\left(f, \hat{f}, \mathrm{pk}, f(x)\right)\right)$$

	$\lvert\mathrm{pk}\rvert$	$\lvert\hat{f}\rvert$	$\lvert\hat{x}\rvert$	假设
[GKPVZ12]	$L \cdot \mathrm{poly}(d)$	$\mathrm{poly}(d)$	$L \cdot \mathrm{poly}(d)$	LWE
本作	$O(L)$	$O(1)$	$O(L)$	循环 LWE

可复用的乱码电路（单密钥泛函加密）



首次不用程序混淆
达成 O(1) 规模乱码电路

安全． 只透露 $f(x)$ 而隐藏 x，即
$$\big(f,\hat{f},\mathrm{pk},\mathrm{Enc}(\cdots)\big) \approx \big(\cdots,\mathrm{Sim}\big(f,\hat{f},\mathrm{pk},f(x)\big)\big)$$

	$\lvert\mathrm{pk}\rvert$	$\lvert\hat{f}\rvert$	$\lvert\hat{x}\rvert$	假设
[GKPVZ12]	$L\cdot\mathrm{poly}(d)$	$\mathrm{poly}(d)$	$L\cdot\mathrm{poly}(d)$	LWE
本作	$O(L)$	$O(1)$	$O(L)$	循环 LWE

属性加密

$f:\{0,1\}^L \to \{可,否\}$

	深度	$\lvert\mathrm{mpk}\rvert$	$\lvert\mathrm{sk}_f\rvert$	$\lvert\mathrm{ct}_x\rvert$	假设
[BGGHNSVV14]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$\mathrm{poly}(d)$	$L \cdot \mathrm{poly}(d)$	LWE
[LLL22]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE + 双线性群 + GGM
[CW23]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE
本作	不限 ✓	$O(L)$	$O(1)$	$O(L)$	循环 LWE + 闪避 LWE

属性加密

$f:\{0,1\}^L \to \{可, 否\}$

evasive

闪避 LWE。新晋 [W22, T22] 假设

- **知识**假设 (**knowledge** assumption)
- 用于 LWE 的**一般模型** (**generic** model)

	深度	$\lvert\mathrm{mpk}\rvert$	$\lvert\mathrm{sk}_f\rvert$	$\lvert\mathrm{ct}_x\rvert$	假设
[BGGHNSVV14]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$\mathrm{poly}(d)$	$L \cdot \mathrm{poly}(d)$	LWE
[LLL22]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE + 双线性群 + GGM
[CW23]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE
本作	不限 ✓	$O(L)$	$O(1)$	$O(L)$	循环 LWE + 闪避 LWE

属性加密

$f : \{0,1\}^L \to \{$可, 否$\}$

evasive
闪避 LWE. 新晋 [W22, T22] 假设
- **知识**假设 (**knowledge** assumption)
- 用于 LWE 的**一般模型** (**generic model**)
- 处理**陷门** (**trapdoor**) 下 LWE 样本的伪随机性

	深度	$\lvert\mathbf{mpk}\rvert$	$\lvert\mathbf{sk}_f\rvert$	$\lvert\mathbf{ct}_x\rvert$	假设
[BGGHNSVV14]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$\mathrm{poly}(d)$	$L \cdot \mathrm{poly}(d)$	LWE
[LLL22]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE + 双线性群 + GGM
[CW23]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE
本作	不限 ✓	$O(L)$	$O(1)$	$O(L)$	循环 LWE + 闪避 LWE

属性加密

$f:\{0,1\}^L \to \{可,否\}$

cryptanalytic

“逃过了已知的密码分析技巧”

evasive

闪避 LWE. 新晋 [W22, T22] 假设

- **知识**假设 (knowledge assumption)
- 用于 LWE 的**一般模型** (generic model)
- 处理**陷门** (trapdoor) 下 LWE 样本的伪随机性

	深度	$\lvert\mathbf{mpk}\rvert$	$\lvert\mathbf{sk}_f\rvert$	$\lvert\mathbf{ct}_x\rvert$	假设
[BGGHNSVV14]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$\mathrm{poly}(d)$	$L \cdot \mathrm{poly}(d)$	LWE
[LLL22]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE + 双线性群 + GGM
[CW23]	受限 ✗	$L \cdot \mathrm{poly}(d)$	$O(1)$	$L \cdot \mathrm{poly}(d)$	LWE
本作	不限 ✓	$O(L)$	$O(1)$	$O(L)$	循环 LWE + 闪避 LWE

中场提问

“上场事，上场毕！”

大纲（技术部分）

- 预备概念
- 成果介绍

- 核心：不限深度的公钥、属性编码 (attribute encoding) 同态
  - 引子、复习 [BGGHNSVV14]
  - 思路、工具 [GSW13, BTVW17]、构造
- 应用
  - AB-LFE
  - 闪避 LWE 与 ABE
- 未解问题

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f:\{0,1\}^L \to \{0,1\}$ 绑定

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f\colon\{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \dots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \dots, \mathrm{pk}_{f_{L'}}\right)$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f\colon\{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \dots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \dots, \mathrm{pk}_{f_{L'}}\right)$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

"无穷个"非独立 pk
通过同态运算相联系

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f:\{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \dots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \dots, \mathrm{pk}_{f_{L'}}\right)$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

"无穷个" 非独立 pk
通过同态运算相联系

公钥同态运算 $\mathrm{EvalC}(g, \mathrm{pk}_f) = \mathrm{pk}_{g \circ f}$

g 输入长度 = f 输出长度

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f\colon\{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \ldots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \ldots, \mathrm{pk}_{f_{L'}}\right)$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

“无穷个”非独立 pk
通过同态运算相联系

公钥同态运算 $\mathrm{EvalC}\left(g, \mathrm{pk}_f\right) = \mathrm{pk}_{g\circ f}$

g 输入长度 = f 输出长度

密文同态运算 $\mathrm{EvalCX}\left(g, y, \mathrm{Enc}\left(\mathrm{pk}_f, y, \mu\right)\right) \to \mathrm{Enc}\left(\mathrm{pk}_{g\circ f}, g(y), \mu\right)$

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f:\{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \ldots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \ldots, \mathrm{pk}_{f_{L'}}\right)$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

“无穷个” 非独立 pk
通过同态运算相联系

公钥同态运算 $\mathrm{EvalC}\left(g, \mathrm{pk}_f\right) = \mathrm{pk}_{g \circ f}$

g 输入长度 = f 输出长度

密文同态运算 $\mathrm{EvalCX}\left(g, y, \boxed{\mathrm{Enc}\left(\mathrm{pk}_f, y, \mu\right)}\right) \to \mathrm{Enc}\left(\mathrm{pk}_{g \circ f}, g(y), \mu\right)$

属性 x 满足 $f(x) = y$

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f: \{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \dots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = (\mathrm{pk}_{f_1}, \dots, \mathrm{pk}_{f_{L'}})$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

"无穷个"非独立 pk
通过同态运算相联系

公钥同态运算 $\mathrm{EvalC}(g, \mathrm{pk}_f) = \mathrm{pk}_{g \circ f}$

g 输入长度 = f 输出长度

密文同态运算 $\mathrm{EvalCX}(g, y, \boxed{\mathrm{Enc}(\mathrm{pk}_f, y, \mu)}) \to \boxed{\mathrm{Enc}(\mathrm{pk}_{g \circ f}, g(y), \mu)}$

属性 x 满足 $f(x) = y$

属性 x 满足
$(g \circ f)(x) = g(y)$

密钥同态 (key-homomorphic) 加密 [BGGHNSVV14]

pk_f 与 $f:\{0,1\}^L \to \{0,1\}$ 绑定

若 $f = (f_1, \dots, f_{L'})$ 输出有多位，
则记 $\mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \dots, \mathrm{pk}_{f_{L'}}\right)$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

"无穷个"非独立 pk
通过同态运算相联系

公钥同态运算 $\mathrm{EvalC}\left(g, \mathrm{pk}_f\right) = \mathrm{pk}_{g\circ f}$

g 输入长度 = f 输出长度

密文同态运算 $\mathrm{EvalCX}\left(g, y, \mathrm{Enc}\left(\mathrm{pk}_f, y, \mu\right)\right) \to \mathrm{Enc}\left(\mathrm{pk}_{g\circ f}, g(y), \mu\right)$

属性 x 满足 $f(x) = y$

属性 x 满足 $(g \circ f)(x) = g(y)$

私钥 sk_f 可以解密 $\mathrm{Enc}\left(\mathrm{pk}_f, 0, \mu\right)$ 且不能解密 $\mathrm{Enc}\left(\mathrm{pk}_f, 1, \mu\right)$

$f(x) = 0 =$ 可

密钥同态(key-homomorphic)加密 [BGGHNSVV14]

pk_f 与 $f:\{0,1\}^L \to \{0,1\}$ 绑定

“无穷个”非独立 pk
通过同态运算相联系

$\boxed{\text{若 } f = (f_1, \dots, f_{L'}) \text{ 输出有多位，则记 } \mathrm{pk}_f = \left(\mathrm{pk}_{f_1}, \dots, \mathrm{pk}_{f_{L'}}\right)}$

$\mathrm{mpk} = \mathrm{pk}_{\mathrm{id}}$

公钥同态运算 $\mathrm{EvalC}\left(g, \mathrm{pk}_f\right) = \mathrm{pk}_{g \circ f}$

$\boxed{g \text{ 输入长度} = f \text{ 输出长度}}$

密文同态运算 $\mathrm{EvalCX}\left(g, y, \boxed{\mathrm{Enc}\left(\mathrm{pk}_f, y, \mu\right)}\right) \to \boxed{\mathrm{Enc}\left(\mathrm{pk}_{g \circ f}, g(y), \mu\right)}$

属性 x 满足 $f(x) = y$

属性 x 满足 $(g \circ f)(x) = g(y)$

私钥 sk_f 可以解密 $\mathrm{Enc}\left(\mathrm{pk}_f, 0, \mu\right)$ 且不能解密 $\mathrm{Enc}\left(\mathrm{pk}_f, 1, \mu\right)$

$\boxed{f(x) = 0 = \text{可}}$

ABE 密文就是 $\mathrm{Enc}(\mathrm{mpk}, x, \mu) = \mathrm{Enc}(\mathrm{pk}_{\mathrm{id}}, \mathrm{id}(x), \mu)$

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

“$f(x) = y$” 编码为 $\boldsymbol{c}_f^\top = \boldsymbol{s}^\top(\boldsymbol{A}_f - y\boldsymbol{G}) + \boldsymbol{e}_f^\top$

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

"$f(x) = y$" 编码为 $\boldsymbol{c}_f^\top = \boldsymbol{s}^\top\left(\boldsymbol{A}_f - y\boldsymbol{G}\right) + \boldsymbol{e}_f^\top$

例. 初始编码 $\boldsymbol{c}_\ell^\top = \boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G}) + \boldsymbol{e}_\ell^\top$

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

"$f(x) = y$" 编码为 $\boldsymbol{c}_f^\top = \boldsymbol{s}^\top\left(\boldsymbol{A}_f - y\boldsymbol{G}\right) + \boldsymbol{e}_f^\top$

例. 初始编码 $\boldsymbol{c}_\ell^\top = \boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G}) + \boldsymbol{e}_\ell^\top$

$$\boldsymbol{G} = \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & 2 & 4 & 8 & \cdots \end{pmatrix} = \boldsymbol{I}_{n+1} \otimes \underbrace{(1,2,4,8,\dots)}_{m/(n+1)}$$

$\mathbb{Z}_q$ 元素都可写成 $\frac{m}{n+1} = \Theta(\log q)$ 位**二进制**数

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

"$f(x) = y$" 编码为 $\boldsymbol{c}_f^\top = \boldsymbol{s}^\top(\boldsymbol{A}_f - y\boldsymbol{G}) + \boldsymbol{e}_f^\top$

例. 初始编码 $\boldsymbol{c}_\ell^\top = \boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G}) + \boldsymbol{e}_\ell^\top$

$$\boldsymbol{G} = \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & 2 & 4 & 8 & \cdots \end{pmatrix} = \boldsymbol{I}_{n+1} \otimes \underbrace{(1,2,4,8,\ldots)}_{m/(n+1)}$$

记号. $\boldsymbol{G}^{-1}\left(\boldsymbol{v} \in \mathbb{Z}_q^{n+1}\right) \in \{0,1\}^m$ 为 $\boldsymbol{v}$ 各分量**二进制分解**依序列位

$\mathbb{Z}_q$ 元素都可写成 $\frac{m}{n+1} = \Theta(\log q)$ 位**二进制**数

公钥、属性编码同态：打开抽象

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$

$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

"$f(x) = y$" 编码为 $\boldsymbol{c}_f^\top = \boldsymbol{s}^\top(\boldsymbol{A}_f - y\boldsymbol{G}) + \boldsymbol{e}_f^\top$

例. 初始编码 $\boldsymbol{c}_\ell^\top = \boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell\boldsymbol{G}) + \boldsymbol{e}_\ell^\top$

$$\boldsymbol{G} = \begin{pmatrix} 1 & 2 & 4 & 8 & \cdots & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & 2 & 4 & 8 & \cdots \end{pmatrix} = \boldsymbol{I}_{n+1} \otimes \underbrace{(1,2,4,8,\dots)}_{m/(n+1)}$$

记号. $\boldsymbol{G}^{-1}\left(\boldsymbol{v} \in \mathbb{Z}_q^{n+1}\right) \in \{0,1\}^m$ 为 $\boldsymbol{v}$ 各分量**二进制分解**依序列位

按列分块作用于矩阵，$\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(\boldsymbol{V}) = \boldsymbol{V}$

$\mathbb{Z}_q$ 元素都可写成 $\frac{m}{n+1} = \Theta(\log q)$ 位**二进制**数

公钥、属性编码同态：快速上手前作

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$ $+ \boldsymbol{e}_f^\top$

简记. x_1, x_2 表示任意两个门，不一定是输入

gates

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

公钥、属性编码同态：快速上手前作

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$　　$\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

gates

简记．x_1, x_2 表示任意两个门，不一定是输入

$+ \boldsymbol{e}_f^\top$

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$$x_+ = x_1 + x_2$$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)}_{\boldsymbol{e}_+}{}^\top$$

公钥、属性编码同态：快速上手前作

$\mathsf{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（属性编码的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$ $+ \boldsymbol{e}_f^\top$

gates

简记. x_1, x_2 表示任意两个门，不一定是输入

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$$x_+ = x_1 + x_2$$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)}_{\boldsymbol{e}_+}{}^\top$$

$$x_\times = x_1 x_2$$

$$\boldsymbol{c}_\times^\top = \boldsymbol{c}_1^\top \boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1 \boldsymbol{c}_2^\top$$

公钥、属性编码同态：快速上手前作

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（属性编码的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

简记. x_1, x_2 表示任意两个门，不一定是输入
gates

$+ \boldsymbol{e}_f^\top$

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$$x_+ = x_1 + x_2$$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top\big(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}\big) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)^\top}_{\boldsymbol{e}_+}$$

$$x_\times = x_1 x_2$$

$$\begin{aligned}\boldsymbol{c}_\times^\top &= \boldsymbol{c}_1^\top \boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1 \boldsymbol{c}_2^\top \\ &= \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2) \\ &\quad + x_1 \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) \\ &\quad + \boldsymbol{e}_1^\top \boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1 \boldsymbol{e}_2^\top\end{aligned}$$

公钥、属性编码同态：快速上手前作

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$ $+ \boldsymbol{e}_f^\top$

简记. x_1, x_2 表示任意两个$\overset{\text{gates}}{\text{门}}$，不一定是输入

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$$x_+ = x_1 + x_2$$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)}_{\boldsymbol{e}_+}{}^\top$$

$$x_\times = x_1 x_2$$

$$\begin{aligned}
\boldsymbol{c}_\times^\top &= \boldsymbol{c}_1^\top \boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{c}_2^\top \\
&= \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2) \\
&\qquad + x_1\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) \\
&\qquad + \boldsymbol{e}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{e}_2^\top \\
&= \boldsymbol{s}^\top(\underbrace{\boldsymbol{A}_1\boldsymbol{G}^{-1}(\boldsymbol{A}_2)}_{\boldsymbol{A}_\times} - x_\times\boldsymbol{G}) + \boldsymbol{e}_\times^\top
\end{aligned}$$

公钥、属性编码同态：快速上手前作

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（**属性编码**的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$ $+\ \boldsymbol{e}_f^\top$

gates

简记. x_1, x_2 表示任意两个门，不一定是输入

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$x_+ = x_1 + x_2$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)}_{\boldsymbol{e}_+}{}^\top$$

$x_\times = x_1 x_2$

编码同态运算要用到属性本身

$$\begin{aligned}\boldsymbol{c}_\times^\top &= \boldsymbol{c}_1^\top \boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{c}_2^\top \\ &= \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2) \\ &\quad + x_1\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) \\ &\quad + \boldsymbol{e}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{e}_2^\top \\ &= \boldsymbol{s}^\top(\underbrace{\boldsymbol{A}_1\boldsymbol{G}^{-1}(\boldsymbol{A}_2)}_{\boldsymbol{A}_\times} - x_\times\boldsymbol{G}) + \boldsymbol{e}_\times^\top\end{aligned}$$

公钥、属性编码同态：噪幅增长、受限

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（属性编码的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$ $+\, \boldsymbol{e}_f^\top$

$\boxed{\text{简记. } x_1, x_2 \text{ 表示任意两个门（gates），不一定是输入}}$

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$$x_+ = x_1 + x_2$$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top\big(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}\big) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)^\top}_{\boldsymbol{e}_+}$$

$$x_\times = x_1 x_2$$

$\boxed{\text{编码同态运算要用到属性本身}}$

$$\begin{aligned}\boldsymbol{c}_\times^\top &= \boldsymbol{c}_1^\top \boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{c}_2^\top \\ &= \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2) \\ &\quad + x_1\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) \\ &\quad + \boldsymbol{e}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{e}_2^\top \\ &= \boldsymbol{s}^\top\big(\underbrace{\boldsymbol{A}_1\boldsymbol{G}^{-1}(\boldsymbol{A}_2)}_{\boldsymbol{A}_\times} - x_\times\boldsymbol{G}\big) + \boldsymbol{e}_\times^\top\end{aligned}$$

公钥、属性编码同态：噪幅增长、受限

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（属性编码的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

简记. x_1, x_2 表示任意两个$\overset{\text{gates}}{门}$，不一定是输入 $+\ \boldsymbol{e}_f^\top$

$$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \qquad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$$

$$x_+ = x_1 + x_2$$

$$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - \overbrace{(x_1 + x_2)}^{x_+}\boldsymbol{G}) + \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)^\top}_{\boldsymbol{e}_+}$$

$$\boxed{\|\boldsymbol{e}_+\| \le \|\boldsymbol{e}_1\| + \|\boldsymbol{e}_2\|}$$

$$x_\times = x_1 x_2$$

编码同态运算要用到属性本身

$$\boldsymbol{c}_\times^\top = \boldsymbol{c}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{c}_2^\top$$

$$= \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2)$$

$$+ x_1\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})$$

$$+ \boldsymbol{e}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{e}_2^\top$$

$$= \boldsymbol{s}^\top(\boldsymbol{A}_1\boldsymbol{G}^{-1}(\boldsymbol{A}_2) - x_\times\boldsymbol{G}) + \boldsymbol{e}_\times^\top$$

$$\boxed{\|\boldsymbol{e}_\times\| \le \|\boldsymbol{e}_1\| \cdot m + 1 \cdot \|\boldsymbol{e}_2\|}$$

公钥、属性编码同态：噪幅增长、受限

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（属性编码的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

gates

简记. x_1, x_2 表示任意两个门，不一定是输入 $+\, \boldsymbol{e}_f^\top$

$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top,$ $\boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$

$x_+ = x_1 + x_2$

$x_\times = x_1 x_2$

编码同态运算要用到属性本身

$\|\boldsymbol{e}_f\| \le m^{\Theta(d)} \cdot \|\boldsymbol{e}_{\mathrm{initial}}\|$

$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$

$(\boldsymbol{A}_2) + x_1\boldsymbol{c}_2^\top$

$- x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2)$

$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - (x_1 + x_2)\boldsymbol{G})$

$+ x_1\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})$

$+ \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)}_{\boldsymbol{e}_+}^\top$

$+ \boldsymbol{e}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{e}_2^\top$

$= \boldsymbol{s}^\top(\boldsymbol{A}_1\boldsymbol{G}^{-1}(\boldsymbol{A}_2) - x_\times\boldsymbol{G}) + \boldsymbol{e}_\times^\top$

$\|\boldsymbol{e}_+\| \le \|\boldsymbol{e}_1\| + \|\boldsymbol{e}_2\|$

$\|\boldsymbol{e}_\times\| \le \|\boldsymbol{e}_1\| \cdot m + 1 \cdot \|\boldsymbol{e}_2\|$

公钥、属性编码同态：噪幅增长、受限

$\mathrm{pk}_f = \boldsymbol{A}_f \in \mathbb{Z}_q^{(n+1)\times m}$ $\quad \boldsymbol{s} = (\boldsymbol{r}^\top, -1)^\top \in \mathbb{Z}_q^{n+1}$ 为加密随机数（属性编码的 LWE 秘密）

mpk 里 $\boldsymbol{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}$

$\boxed{\text{简记. } x_1, x_2 \text{ 表示任意两个门（gates），不一定是输入}}$ $+ \boldsymbol{e}_f^\top$

$\boldsymbol{c}_1^\top = \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) + \boldsymbol{e}_1^\top, \quad \boldsymbol{c}_2^\top = \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) + \boldsymbol{e}_2^\top$

$x_+ = x_1 + x_2$

$\boldsymbol{c}_+^\top = \boldsymbol{c}_1^\top + \boldsymbol{c}_2^\top$

$= \boldsymbol{s}^\top(\overbrace{(\boldsymbol{A}_1 + \boldsymbol{A}_2)}^{\boldsymbol{A}_+} - (x_1 + x_2)\boldsymbol{G})$

$+ \underbrace{(\boldsymbol{e}_1 + \boldsymbol{e}_2)^\top}_{\boldsymbol{e}_+}$

$\boxed{\|\boldsymbol{e}_+\| \le \|\boldsymbol{e}_1\| + \|\boldsymbol{e}_2\|}$

$x_\times = x_1 x_2$

$\boxed{\text{编码同态运算要用到属性本身}}$

$(\boldsymbol{A}_2) + x_1\boldsymbol{c}_2^\top$

$- x_1\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{A}_2)$

$+ x_1\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})$

$+ \boldsymbol{e}_1^\top\boldsymbol{G}^{-1}(\boldsymbol{A}_2) + x_1\boldsymbol{e}_2^\top$

$= \boldsymbol{s}^\top(\boldsymbol{A}_1\boldsymbol{G}^{-1}(\boldsymbol{A}_2) - x_\times\boldsymbol{G}) + \boldsymbol{e}_\times^\top$

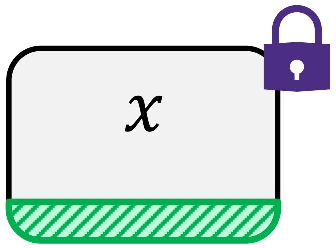
$\boxed{\|\boldsymbol{e}_\times\| \le \|\boldsymbol{e}_1\| \cdot m + 1 \cdot \|\boldsymbol{e}_2\|}$

$$\|\boldsymbol{e}_f\| \le m^{\Theta(d)} \cdot \|\boldsymbol{e}_{\text{initial}}\|$$

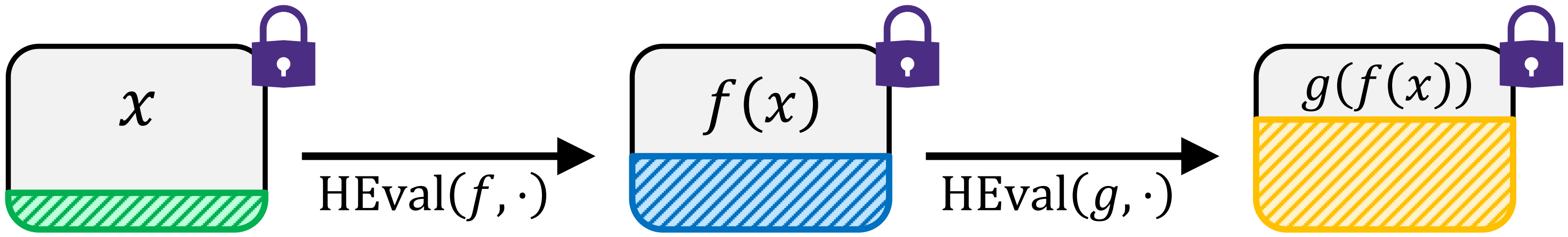
初始化选定 q 将约束

$$d \le \log_m q \le \log q$$

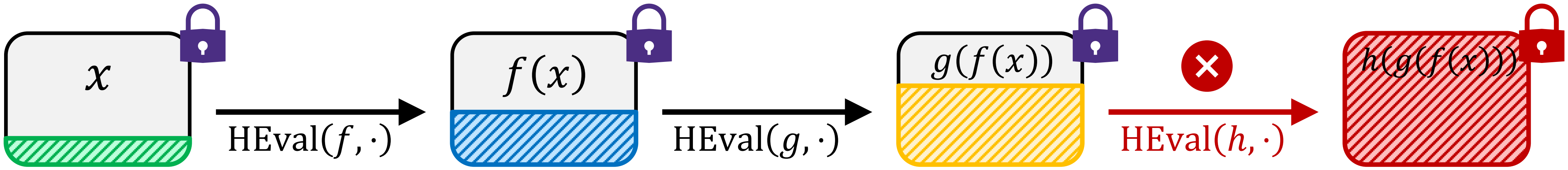
回顾：FHE 降噪、自举 (bootstrapping)



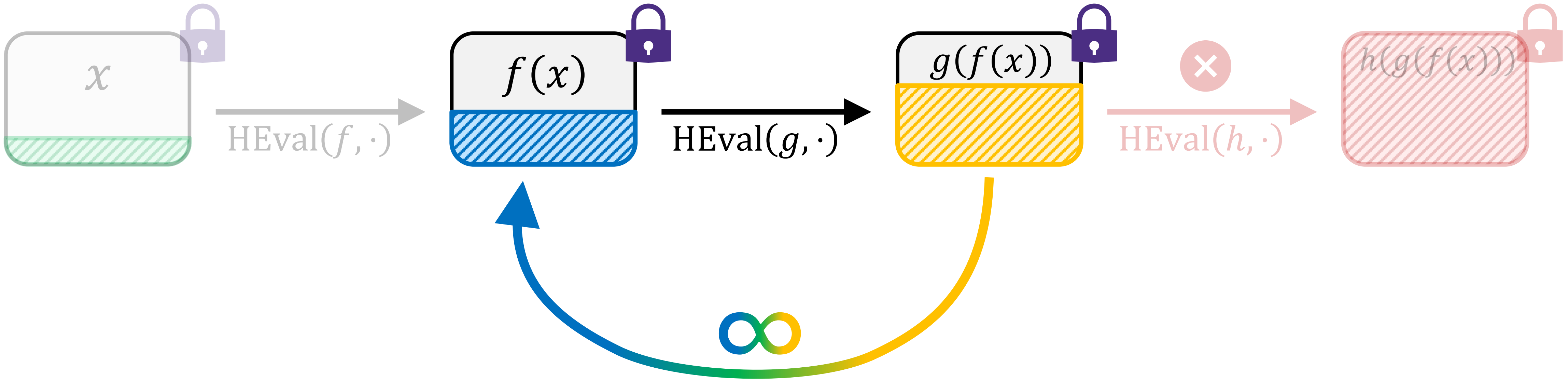
回顾：FHE 降噪、自举 (bootstrapping)



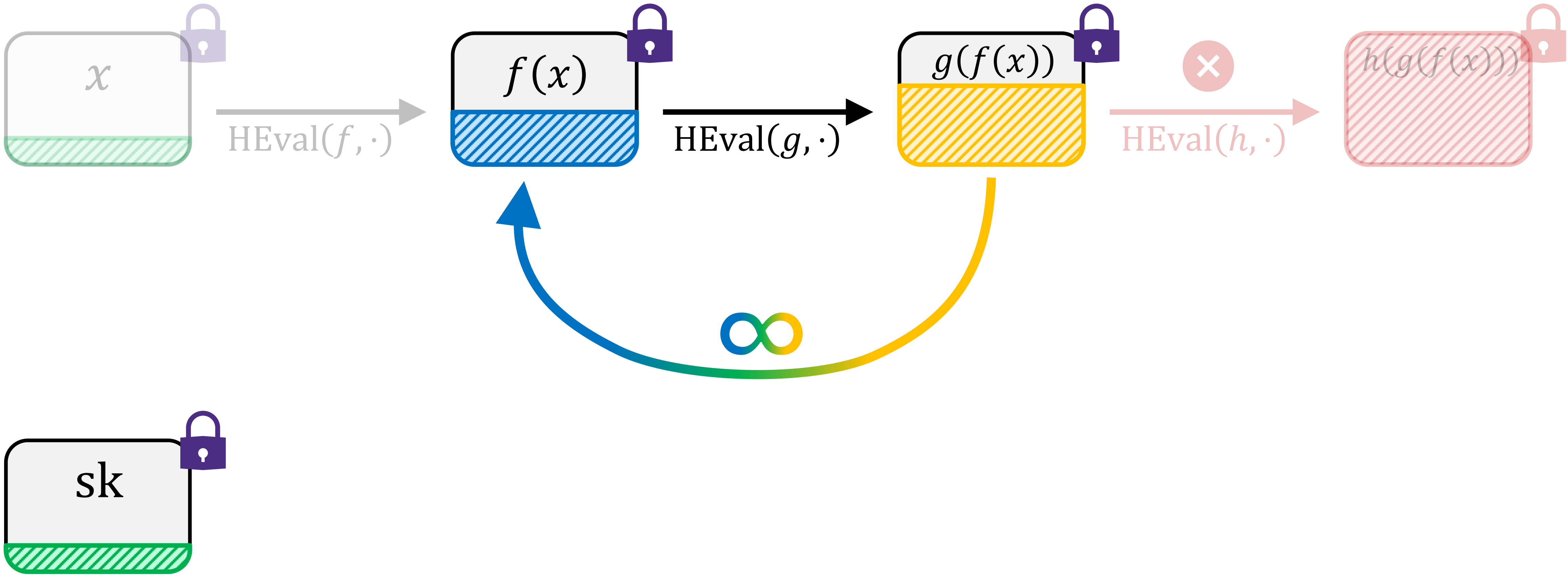
回顾：FHE 降噪、自举 (bootstrapping)



回顾：FHE 降噪、自举 (bootstrapping)

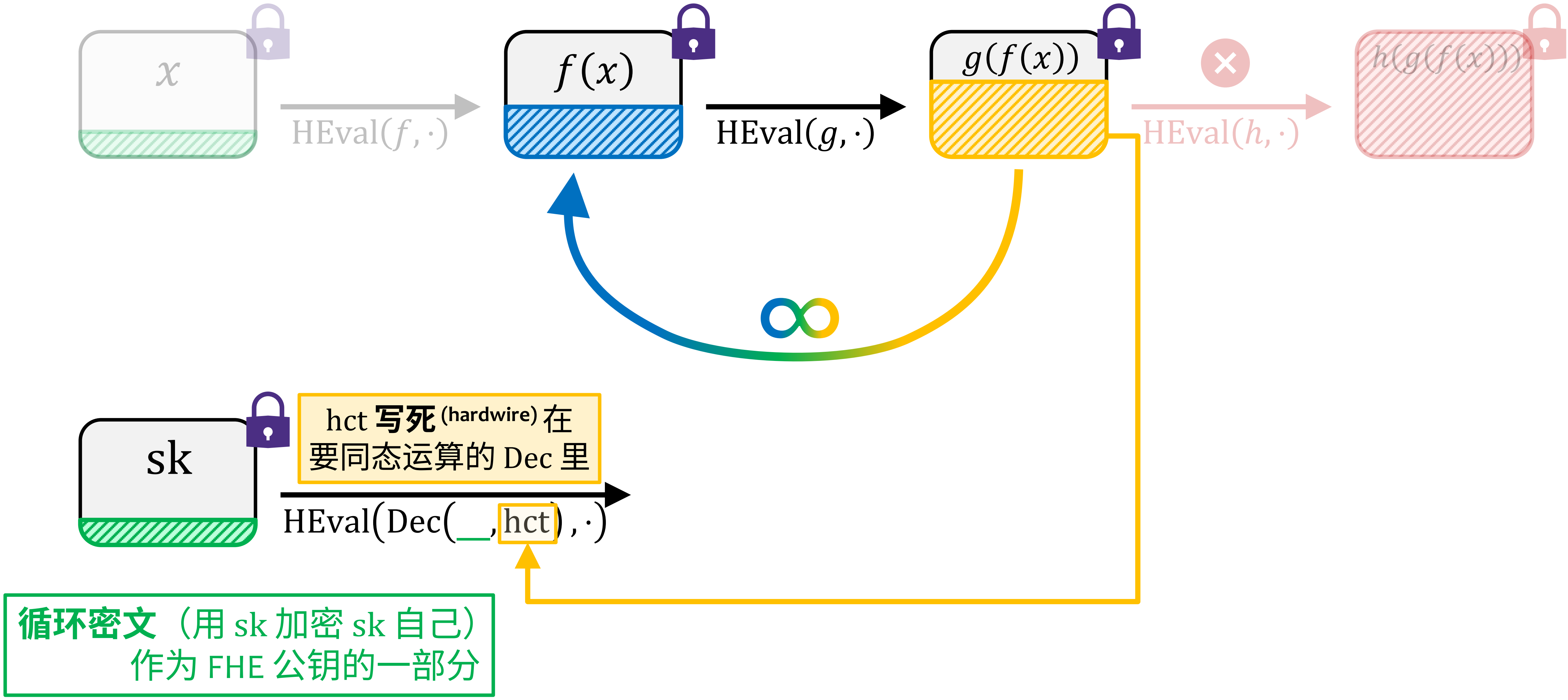


回顾：FHE 降噪、自举 (bootstrapping)

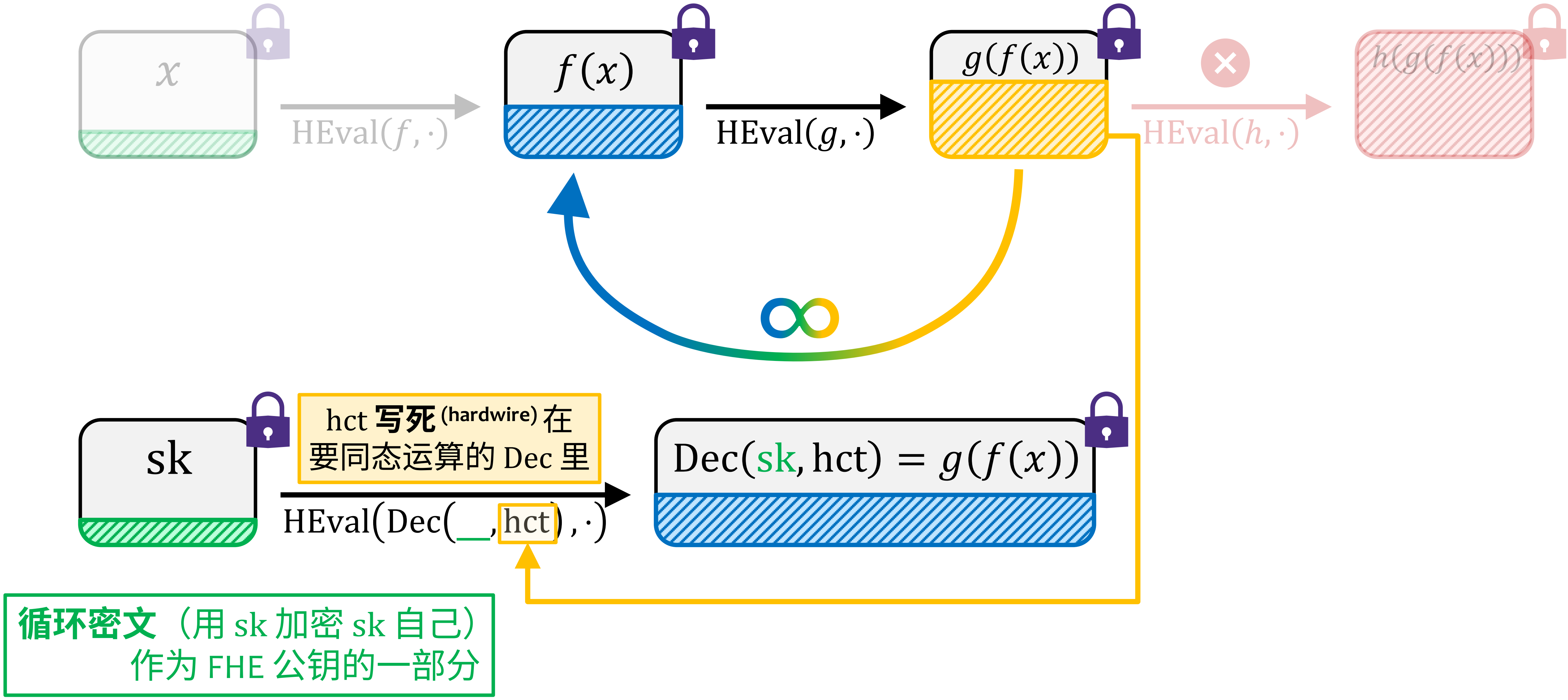


循环密文（用 sk 加密 sk 自己）
作为 FHE 公钥的一部分

回顾：FHE 降噪、自举 (bootstrapping)



回顾：FHE 降噪、自举 (bootstrapping)



朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ},1} - \mathrm{bits}(\boldsymbol{s})\,[1] \cdot \boldsymbol{G},\ \ \boldsymbol{A}_{\mathrm{circ},2} - \mathrm{bits}(\boldsymbol{s})\,[2] \cdot \boldsymbol{G},\ \ \ldots) + \boldsymbol{e}_{\mathrm{circ}}^{\top}$
$= \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})$ 波浪线表示噪点

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ},1} - \mathrm{bits}(\boldsymbol{s})[1] \cdot \boldsymbol{G},\ \ \boldsymbol{A}_{\mathrm{circ},2} - \mathrm{bits}(\boldsymbol{s})[2] \cdot \boldsymbol{G},\ \ \ldots) + \boldsymbol{e}_{\mathrm{circ}}^{\top}$

   $= \underset{\sim\sim\sim}{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})}$ 波浪线表示噪点

3. 令 $f'(\_\_) = \mathrm{AttrDec}\left(\_\_, \boldsymbol{A}_{f,\mathrm{LARGE}}, \boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}\right)$ 并对 $\boldsymbol{c}_{\mathrm{circ}}^{\top}$ 做 f' 的属性同态

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} \xrightarrow{\mathrm{EvalCX}(f', \boldsymbol{s}, \_\_)}$$

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}\left(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ},1} - \mathrm{bits}(\boldsymbol{s})[1] \cdot \boldsymbol{G},\ \boldsymbol{A}_{\mathrm{circ},2} - \mathrm{bits}(\boldsymbol{s})[2] \cdot \boldsymbol{G},\ \ldots) + \boldsymbol{e}_{\mathrm{circ}}^{\top}$

$= \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})$ 波浪线表示噪点

3. 令 $f'(\_\_) = \mathrm{AttrDec}\left(\_\_, \boldsymbol{A}_{f,\mathrm{LARGE}}, \boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}\right)$ 并对 $\boldsymbol{c}_{\mathrm{circ}}^{\top}$ 做 f' 的属性同态

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} \xrightarrow{\mathrm{EvalCX}(f', \boldsymbol{s}, \_\_)} \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - f'(\boldsymbol{s}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{f'}^{\top}$$

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ},1} - \mathrm{bits}(\boldsymbol{s})[1] \cdot \boldsymbol{G},\ \boldsymbol{A}_{\mathrm{circ},2} - \mathrm{bits}(\boldsymbol{s})[2] \cdot \boldsymbol{G},\ \ldots) + \boldsymbol{e}_{\mathrm{circ}}^{\top}$

   $= \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})$ 波浪线表示噪点

3. 令 $f'(\_\_) = \mathrm{AttrDec}(\_\_, \boldsymbol{A}_{f,\mathrm{LARGE}}, \boldsymbol{c}_{f,\mathrm{LARGE}}^{\top})$ 并对 $\boldsymbol{c}_{\mathrm{circ}}^{\top}$ 做 f' 的属性同态

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} \xrightarrow{\mathrm{EvalCX}(f', \boldsymbol{s}, \_\_)} \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - f'(\boldsymbol{s}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{f'}^{\top}$$

$$\boldsymbol{c}_{f,\mathrm{small}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - \qquad y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f'}^{\top}$$

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\text{LARGE}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\text{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\text{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\text{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\text{circ},1} - \text{bits}(\boldsymbol{s})[1] \cdot \boldsymbol{G},\ \boldsymbol{A}_{\text{circ},2} - \text{bits}(\boldsymbol{s})[2] \cdot \boldsymbol{G},\ \ldots) + \boldsymbol{e}_{\text{circ}}^{\top}$

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

波浪线表示噪点

3. 令 $f'(\_\_) = \text{AttrDec}(\_\_, \boldsymbol{A}_{f,\text{LARGE}}, \boldsymbol{c}_{f,\text{LARGE}}^{\top})$ 并对 $\boldsymbol{c}_{\text{circ}}^{\top}$ 做 f' 的属性同态

$$\boldsymbol{c}_{\text{circ}}^{\top} \xrightarrow{\text{EvalCX}(f', \boldsymbol{s}, \_\_)} \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - f'(\boldsymbol{s}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{f'}^{\top}$$

$$\boldsymbol{c}_{f,\text{small}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - y \cdot \boldsymbol{G}) + \boxed{\boldsymbol{e}_{f'}^{\top}}$$

噪幅取决于 f' 深度（**固定**）
与 $\boldsymbol{c}_{f,\text{LARGE}}^{\top}$ **无关**

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ},1} - \mathrm{bits}(\boldsymbol{s})[1] \cdot \boldsymbol{G},\ \boldsymbol{A}_{\mathrm{circ},2} - \mathrm{bits}(\boldsymbol{s})[2] \cdot \boldsymbol{G},\ \ldots) + \boldsymbol{e}_{\mathrm{circ}}^{\top}$

$= \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})$ 波浪线表示噪点

3. 令 $f'(\_\_) = \mathrm{AttrDec}(\_\_, \boldsymbol{A}_{f,\mathrm{LARGE}}, \boxed{\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}})$ 并对 $\boldsymbol{c}_{\mathrm{circ}}^{\top}$ 做 f' 的属性同态

f' 的描述包含**具体编码值** $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}$

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} \xrightarrow{\mathrm{EvalCX}(f', \boldsymbol{s}, \_\_)} \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - f'(\boldsymbol{s}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{f'}^{\top}$$

$$\boldsymbol{c}_{f,\mathrm{small}}^{\top} = \boldsymbol{s}^{\top}(\boxed{\boldsymbol{A}_{f'}} - y \cdot \boldsymbol{G}) + \boxed{\boldsymbol{e}_{f'}^{\top}}$$

噪幅取决于 f' 深度（**固定**）
与 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}$ **无关**

与具体编码值 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}$ 有关
（ABE 中 KeyGen 时不知道）

朴素尝试：用“循环编码”降噪

1. 把 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$ 看作 y 在 $\boldsymbol{s}$ 下的密文

2. 提供 $\boldsymbol{c}_{\mathrm{circ}}^{\top} = \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ},1} - \mathrm{bits}(\boldsymbol{s})[1] \cdot \boldsymbol{G},\ \ \boldsymbol{A}_{\mathrm{circ},2} - \mathrm{bits}(\boldsymbol{s})[2] \cdot \boldsymbol{G},\ \ \ldots) + \boldsymbol{e}_{\mathrm{circ}}^{\top}$

$$= \boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{s}) \otimes \boldsymbol{G})$$ 波浪线表示噪点

3. 令 $f'(\_\_) = \mathrm{AttrDec}(\_\_, \boldsymbol{A}_{f,\mathrm{LARGE}}, \boxed{\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}})$ 并对 $\boldsymbol{c}_{\mathrm{circ}}^{\top}$ 做 f' 的属性同态

做此运算要**明文用到 $\boldsymbol{s}$**（无安全性）

f' 的描述包含**具体编码值** $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}$

$$\boldsymbol{c}_{\mathrm{circ}}^{\top} \xrightarrow{\mathrm{EvalCX}(f', \boxed{\boldsymbol{s},} \_\_)} \boldsymbol{s}^{\top}(\boldsymbol{A}_{f'} - f'(\boldsymbol{s}) \cdot \boldsymbol{G}) + \boldsymbol{e}_{f'}^{\top}$$

$$\boldsymbol{c}_{f,\mathrm{small}}^{\top} = \boldsymbol{s}^{\top}(\boxed{\boldsymbol{A}_{f'}} - \quad y \cdot \boldsymbol{G}) + \boxed{\boldsymbol{e}_{f'}^{\top}}$$

噪幅取决于 f' 深度（**固定**）
与 $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}$ **无关**

与**具体编码值** $\boldsymbol{c}_{f,\mathrm{LARGE}}^{\top}$ 有关
（ABE 中 KeyGen 时不知道）

另一常见技巧：舍入、取整(rounding)

$$\boldsymbol{s}^{\top}\left(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}$$

另一常见技巧：舍入、取整(rounding)

$$\left\lfloor \frac{\boldsymbol{s}^{\top}\left(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}}{M} \right\rceil$$

另一常见技巧：舍入、取整 (rounding)

$$\left\lfloor \frac{\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top}{M} \right\rceil = \boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\mathrm{small}} - y \cdot \boldsymbol{G}\right) + \underbrace{\boldsymbol{e}_{\mathrm{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{f,\mathrm{LARGE}}^\top}{M} \right\rceil}_{\boldsymbol{e}_{f,\mathrm{small}}^\top}$$

另一常见技巧：舍入、取整 (rounding)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{LARGE}} - y\cdot\boldsymbol{G}) + \boldsymbol{e}^\top_{f,\mathrm{LARGE}}\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{small}} - y\cdot\boldsymbol{G}) + \underbrace{\boldsymbol{e}^\top_{\mathrm{round}} + \left\lfloor \frac{\boldsymbol{e}^\top_{f,\mathrm{LARGE}}}{M} \right\rceil}_{\boldsymbol{e}^\top_{f,\mathrm{small}}}\right) \bmod \frac{q}{M}$$

另一常见技巧：舍入、取整 (rounding)

$\boxed{\|\boldsymbol{e}\| \text{ 降低但 } \|\boldsymbol{e}\|/\text{模数 不变}}$

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{LARGE}} - y\cdot\boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{small}} - y\cdot\boldsymbol{G}) + \underbrace{\boldsymbol{e}_{\mathrm{round}}^\top + \left\lfloor \frac{\boldsymbol{e}_{f,\mathrm{LARGE}}^\top}{M} \right\rceil}_{\boldsymbol{e}_{f,\mathrm{small}}^\top}\right) \bmod \frac{q}{M}$$

另一常见技巧：舍入、取整 (rounding)

$\|\boldsymbol{e}\|$ **降低但** $\|\boldsymbol{e}\|/$模数 **不变**

M **足够大时可彻底消去**

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{LARGE}} - y\cdot\boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{small}} - y\cdot\boldsymbol{G}) + \underbrace{\boldsymbol{e}_{\mathrm{round}}^\top + \boxed{\left\lfloor \frac{\boldsymbol{e}_{f,\mathrm{LARGE}}^\top}{M} \right\rceil}}_{\boldsymbol{e}_{f,\mathrm{small}}^\top}\right) \bmod \frac{q}{M}$$

另一常见技巧：舍入、取整 (rounding)

$\|\boldsymbol{e}\|$ **降低但** $\|\boldsymbol{e}\|$/模数 **不变**

M **足够大时可彻底消去**

源自 $\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}}{M} \right\rceil \to \boldsymbol{s}^\top \left\lfloor \frac{\boldsymbol{A}}{M} \right\rceil$

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\text{LARGE}} - y \cdot \boldsymbol{G}\right) + \boldsymbol{e}_{f,\text{LARGE}}^\top\right) \bmod q}{M} \right\rceil = \left(\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\text{small}} - y \cdot \boldsymbol{G}\right) + \underbrace{\boxed{\boldsymbol{e}_{\text{round}}^\top} + \boxed{\left\lfloor \frac{\boldsymbol{e}_{f,\text{LARGE}}^\top}{M} \right\rceil}}_{\boldsymbol{e}_{f,\text{small}}^\top}\right) \bmod \frac{q}{M}$$

另一常见技巧：舍入、取整 (rounding)

$\|e\|$ 降低但 $\|e\|$/模数 不变

源自 $\left\lfloor \frac{s^\top A}{M} \right\rceil \to s^\top \left\lfloor \frac{A}{M} \right\rceil$

M 足够大时可彻底消去

$$\left\lfloor \frac{\left(s^\top (A_{f,\text{LARGE}} - y \cdot G) + e_{f,\text{LARGE}}^\top\right) \bmod q}{M} \right\rceil = \left(s^\top (A_{f,\text{small}} - y \cdot G) + \underbrace{\boxed{e_{\text{round}}^\top} + \boxed{\left\lfloor \frac{e_{f,\text{LARGE}}^\top}{M} \right\rceil}}_{e_{f,\text{small}}^\top} \right) \bmod \frac{q}{M}$$

思路． 不把 s 从取整函数里拿出来？

另一常见技巧：舍入、取整 (rounding)

$\|e\|$ 降低但 $\|e\|$/模数 不变

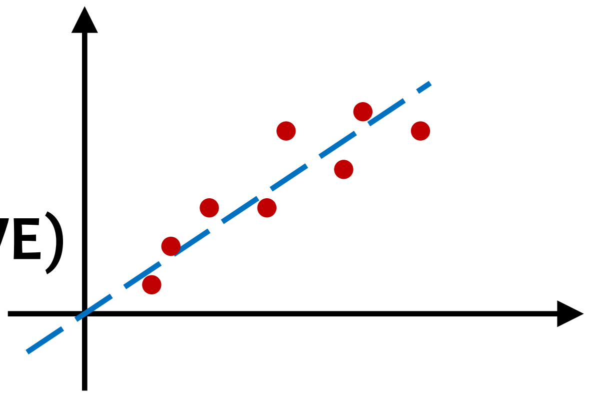
源自 $\left\lfloor \frac{s^\top A}{M} \right\rceil \to s^\top \left\lfloor \frac{A}{M} \right\rceil$

M 足够大时可彻底消去

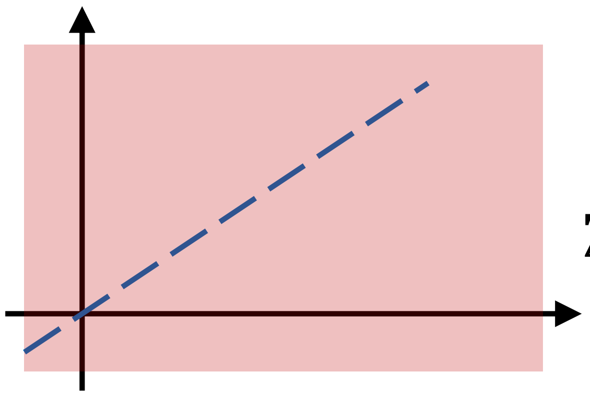
$$\left\lfloor \frac{\left(s^\top\left(A_{f,\mathrm{LARGE}} - y\cdot G\right) + e^\top_{f,\mathrm{LARGE}}\right) \bmod q}{M} \right\rceil = \left(s^\top\left(A_{f,\mathrm{small}} - y\cdot G\right) + \underbrace{\boxed{e^\top_{\mathrm{round}}} + \left\lfloor \frac{e^\top_{f,\mathrm{LARGE}}}{M} \right\rceil}_{e^\top_{f,\mathrm{small}}} \right) \bmod \frac{q}{M}$$

思路. 不把 s 从取整函数里拿出来?

$s^\top A + e^\top$ (LWE)



$\approx$



$\mathbb{Z}_q$ 随机

另一常见技巧：舍入、取整 (rounding)

$\|e\|$ 降低但 $\|e\|/$模数 不变

源自 $\left\lfloor \frac{s^\top A}{M} \right\rceil \to s^\top \left\lfloor \frac{A}{M} \right\rceil$

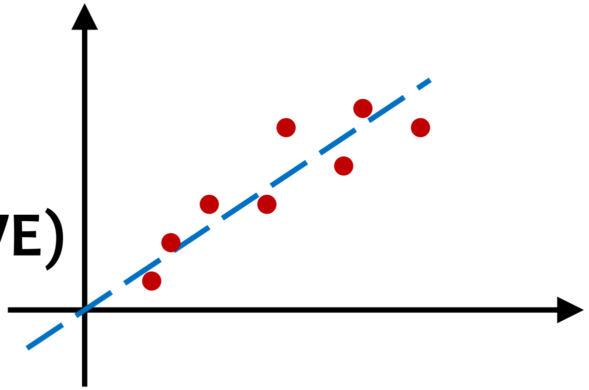
M 足够大时可彻底消去

$$\left\lfloor \frac{\left(s^\top (A_{f,\mathrm{LARGE}} - y \cdot G) + e^\top_{f,\mathrm{LARGE}}\right) \bmod q}{M} \right\rceil = \left(s^\top (A_{f,\mathrm{small}} - y \cdot G) + \underbrace{\boxed{e^\top_{\mathrm{round}}} + \boxed{\left\lfloor \frac{e^\top_{f,\mathrm{LARGE}}}{M} \right\rceil}}_{e^\top_{f,\mathrm{small}}} \right) \bmod \frac{q}{M}$$

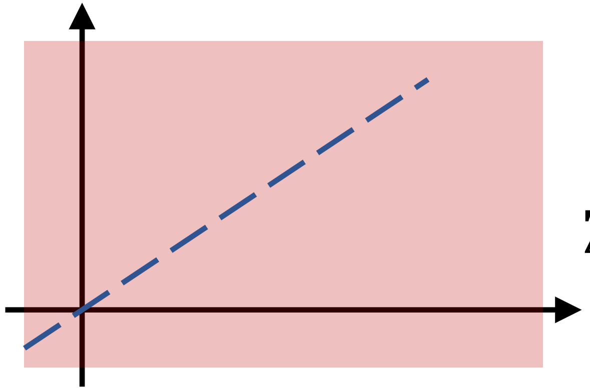
思路. 不把 s 从取整函数里拿出来?

s 之外的随机性，有时难以处理

$s^\top A + \boxed{e^\top}$ (LWE)



$\approx$



$\mathbb{Z}_q$ 随机

舍入取整学习 (learning with rounding) 的启发

$\|e\|$ 降低但 $\|e\|/$模数 不变

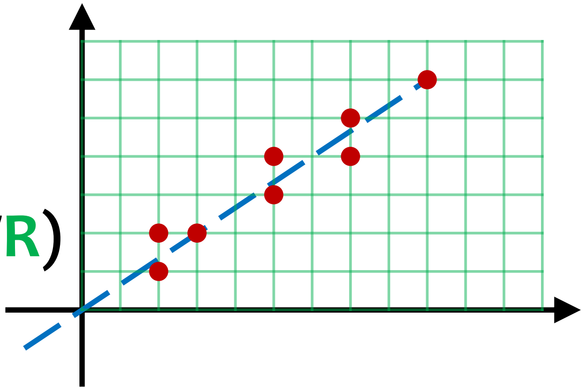
源自 $\left\lfloor \frac{s^\top A}{M} \right\rceil \to s^\top \left\lfloor \frac{A}{M} \right\rceil$

M 足够大时可彻底消去

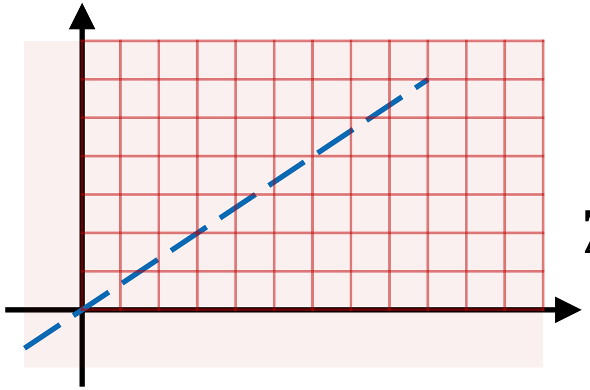
$$\left\lfloor \frac{\left(s^\top (A_{f,\mathrm{LARGE}} - y \cdot G) + e^\top_{f,\mathrm{LARGE}}\right) \bmod q}{M} \right\rceil = \left(s^\top (A_{f,\mathrm{small}} - y \cdot G) + \underbrace{\boxed{e^\top_{\mathrm{round}}} + \left\lfloor \frac{e^\top_{f,\mathrm{LARGE}}}{M} \right\rceil}_{e^\top_{f,\mathrm{small}}} \right) \bmod \frac{q}{M}$$

思路． 不把 s 从取整函数里拿出来？

$\lfloor s^\top A/M \rceil$ (LWR)



$\approx$



$\mathbb{Z}_{q/M}$ 随机

舍入取整学习 (learning with rounding) 的启发

$\|e\|$ 降低但 $\|e\|$/模数 不变

源自 $\left\lfloor \frac{s^\top A}{M} \right\rceil \to s^\top \left\lfloor \frac{A}{M} \right\rceil$

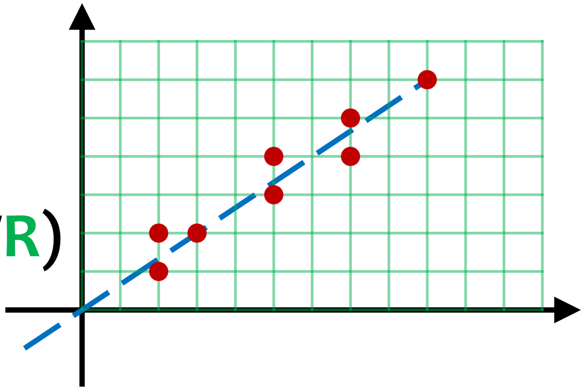
M 足够大时可彻底消去

$$\left\lfloor \frac{\left(s^\top (A_{f,\mathrm{LARGE}} - y \cdot G) + e^\top_{f,\mathrm{LARGE}}\right) \bmod q}{M} \right\rceil = \left(s^\top (A_{f,\mathrm{small}} - y \cdot G) + \underbrace{\boxed{e^\top_{\mathrm{round}}} + \left\lfloor \frac{e^\top_{f,\mathrm{LARGE}}}{M} \right\rceil}_{e^\top_{f,\mathrm{small}}} \right) \bmod \frac{q}{M}$$

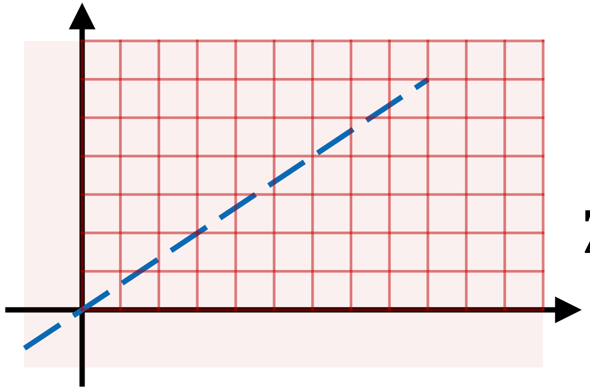
思路． 不把 s 从取整函数里拿出来?

LWR 可以想成**噪点被 s, A 决定**（易于处理）

$\lfloor s^\top A / M \rceil$ (LWR)



$\approx$



$\mathbb{Z}_{q/M}$ 随机

第一步： 除噪 (noise removal)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top (\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil$$

第一步： 除噪 (noise removal)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top (\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil$$

$$= \left(\left\lfloor \frac{\left(\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil - y \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}} \right) \bmod \frac{q}{M}$$

第一步：除噪 (noise removal)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{LARGE}} - y\cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil$$

M 是 2 的乘方，暂且忽略 $\boldsymbol{G}$ 中较小的部分

$$= \left(\left\lfloor \frac{\left(\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil - y \cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}} \right) \bmod \frac{q}{M}$$

第一步： 除噪 (noise removal)

$$\left\lfloor \frac{\left(\boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}\right) \bmod q}{M} \right\rceil$$

M 是 2 的乘方，暂且忽略 $\boldsymbol{G}$ 中较小的部分

$$= \left(\left\lfloor \frac{\left(\boldsymbol{s}^{\top}\boldsymbol{A}_{f,\mathrm{LARGE}} + \boldsymbol{e}_{f,\mathrm{LARGE}}^{\top}\right) \bmod q}{M} \right\rceil - y \cdot \boldsymbol{s}^{\top}\boldsymbol{G}_{\mathrm{small}} \right) \bmod \frac{q}{M}$$

（高概率成立，**无噪**）

$$= \left(\left\lfloor \frac{\boldsymbol{s}^{\top}\boldsymbol{A}_{f,\mathrm{LARGE}} \bmod q}{M} \right\rceil - y \cdot \boldsymbol{s}^{\top}\boldsymbol{G}_{\mathrm{small}} \right) \bmod \frac{q}{M}$$

第一步：除噪 (noise removal)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{LARGE}} - y\cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil$$

M 是 2 的乘方，暂且忽略 $\boldsymbol{G}$ 中较小的部分

$$= \left(\left\lfloor \frac{\left(\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil - y\cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}}\right) \bmod \frac{q}{M}$$

（高概率成立，**无噪**）

$$= \left(\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} \bmod q}{M} \right\rceil - y\cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}}\right) \boxed{\bmod \frac{q}{M}}$$

直接乘 M 恢复模数

$$\to \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} \bmod q}{M} \right\rceil M - y\cdot \boldsymbol{s}^\top M \boldsymbol{G}_{\mathrm{small}} \pmod q$$

第一步：除噪 (noise removal)

$$\left\lfloor \frac{\left(\boldsymbol{s}^\top(\boldsymbol{A}_{f,\mathrm{LARGE}} - y\cdot \boldsymbol{G}) + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil$$

M 是 2 的乘方，暂且

忽略 $\boldsymbol{G}$ 中较小的部分

$$= \left(\left\lfloor \frac{\left(\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} + \boldsymbol{e}_{f,\mathrm{LARGE}}^\top\right) \bmod q}{M} \right\rceil - y\cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}}\right) \bmod \frac{q}{M}$$

（高概率成立，**无噪**）

$$= \left(\left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} \bmod q}{M} \right\rceil - y\cdot \boldsymbol{s}^\top \boldsymbol{G}_{\mathrm{small}}\right) \boxed{\bmod \frac{q}{M}}$$

直接乘 M 恢复模数

$$\to \left\lfloor \frac{\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{LARGE}} \bmod q}{M} \right\rceil M - y\cdot \boldsymbol{s}^\top \boxed{M\boldsymbol{G}_{\mathrm{small}}} \pmod q$$

不是完整的 $\boldsymbol{G}$

第一步：除噪（续）

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

$$\boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G})$$

第一步：除噪（续）

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

$$\boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G})$$

第一步：除噪（续）

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

$$\underline{\boldsymbol{s}^{\top}(\boldsymbol{A}_{f,\mathrm{LARGE}} - y \cdot \boldsymbol{G})} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}}, \boldsymbol{G}_{\mathrm{R}})$$

第一步：除噪（续）

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

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

第一步：除噪（续）

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

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

第一步：除噪（续）

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

左. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

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

第一步：除噪（续）

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

左. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

第一步：除噪（续）

$$\boldsymbol{G} = (\underbrace{\boldsymbol{G}_{\mathrm{L}}}^{<M}, \underbrace{\boldsymbol{G}_{\mathrm{R}}}_{\geq M})\boldsymbol{Q}$$ 置换矩阵

左. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

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

第一步：除噪（续）

$$\boldsymbol{G} = (\underbrace{\boldsymbol{G}_{\mathrm{L}}}_{<M}, \underbrace{\boldsymbol{G}_{\mathrm{R}}}_{\geq M})\boldsymbol{Q}$$ 置换矩阵

左. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

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

$\mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})$ = ↑ 但不加噪点

第一步：除噪（终）

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

左. $\left\lfloor \frac{\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

$$= \mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s}) - y \cdot \boldsymbol{s}^\top \boldsymbol{G}$$ （高概率成立）

第一步：除噪（终）

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

左. $\left\lfloor \frac{\boldsymbol{G}\cdot \boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G}\cdot \boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

$$= \boxed{\mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})} - y \cdot \boldsymbol{s}^{\top}\boldsymbol{G}$$ （高概率成立）

- 被 $\boldsymbol{A}_{f,\mathrm{LARGE}}$ 描述（和 x 无关）
- 深度低（线性、取整、线性）

第一步：除噪（终）

$$\boldsymbol{G} = (\underbrace{\boldsymbol{G}_{\mathrm{L}}}_{<M}, \underbrace{\boldsymbol{G}_{\mathrm{R}}}_{\geq M})\boldsymbol{Q}$$ 置换矩阵

左. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

$$= \boxed{\mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})} - y \cdot \boldsymbol{s}^{\top}\boldsymbol{G}$$ （高概率成立）

- **被 $\boldsymbol{A}_{f,\mathrm{LARGE}}$ 描述**（和 x 无关）
- **深度低**（线性、取整、线性）
- **无法继续用于属性同态**

第一步：除噪（终）

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

$\boldsymbol{G}_{\mathrm{L}}$: $< M$；$\boldsymbol{G}_{\mathrm{R}}$: $\geq M$；$\boldsymbol{Q}$: 置换矩阵

左. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(M\boldsymbol{G}_{\mathrm{L}})}{M} \right\rceil \cdot \boldsymbol{I} = \boldsymbol{G}_{\mathrm{L}}$

右. $\left\lfloor \frac{\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{G}_{\mathrm{R}})}{M} \right\rceil \cdot M\boldsymbol{I} = \boldsymbol{G}_{\mathrm{R}}$

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

$$= \boxed{\mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})} - y\cdot\boldsymbol{s}^\top\boldsymbol{G}$$

（高概率成立）

- **被 $\boldsymbol{A}_{f,\mathrm{LARGE}}$ 描述**（和 x 无关）
- **深度低**（线性、取整、线性）
- **无法继续用于属性同态**

需要. $\boldsymbol{s}^\top\boldsymbol{A}_{f,\mathrm{small}} - \mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})$

工具：[GSW13] 同态加密

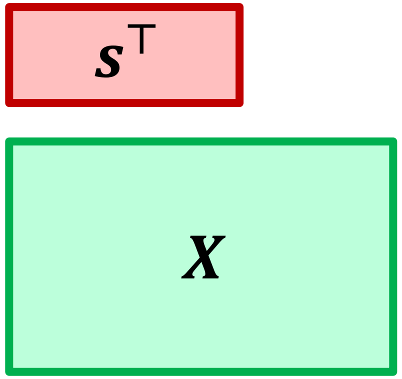
$$\mathrm{sk} = \boldsymbol{s}^\top \in \mathbb{Z}_q^{1\times(n+1)}$$

$\boxed{\boldsymbol{s}^\top}$

工具：[GSW13] 同态加密

$$\mathrm{sk} = \boldsymbol{s}^\top \in \mathbb{Z}_q^{1\times(n+1)}$$

$$\mathrm{hct}(x) = \boldsymbol{X} \in \mathbb{Z}_q^{(n+1)\times m}$$

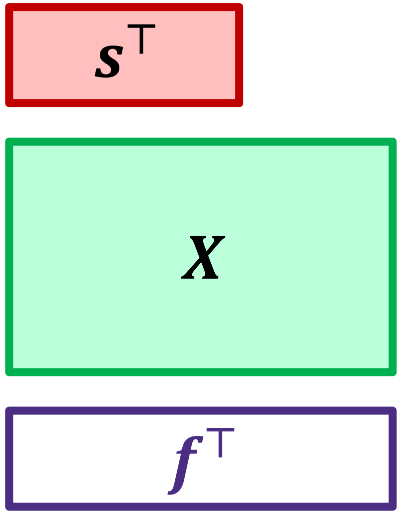


工具：[GSW13] 同态加密

$$\mathrm{sk} = \boldsymbol{s}^{\top} \in \mathbb{Z}_q^{1\times(n+1)}$$

$$\mathrm{hct}(x) = \boldsymbol{X} \in \mathbb{Z}_q^{(n+1)\times m}$$

$$\boldsymbol{f}^{\top}: \{0,1\}^{L'} \to \mathbb{Z}_q^{1\times m}$$



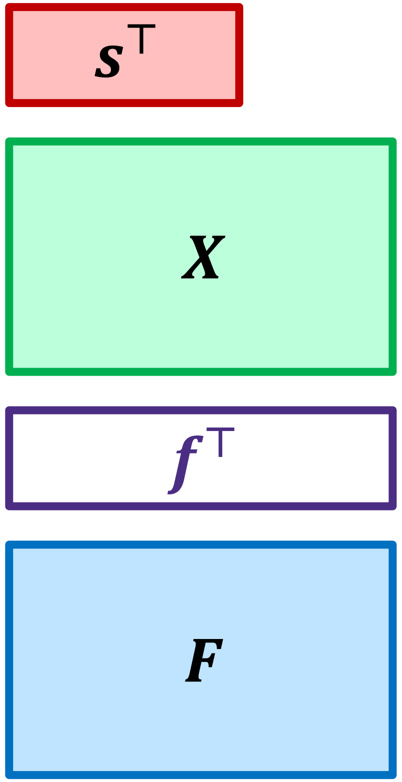
工具：[GSW13] 同态加密

$$\mathrm{sk} = \boldsymbol{s}^\top \in \mathbb{Z}_q^{1\times(n+1)}$$

$$\mathrm{hct}(x) = \boldsymbol{X} \in \mathbb{Z}_q^{(n+1)\times m}$$

$$\boldsymbol{f}^\top : \{0,1\}^{L'} \to \mathbb{Z}_q^{1\times m}$$

$$\mathrm{HEval}\left(\boldsymbol{f}^\top, \{\boldsymbol{X}_\ell\}_{\ell\in[L']}\right) = \boldsymbol{F} \in \mathbb{Z}_q^{(n+1)\times m}$$



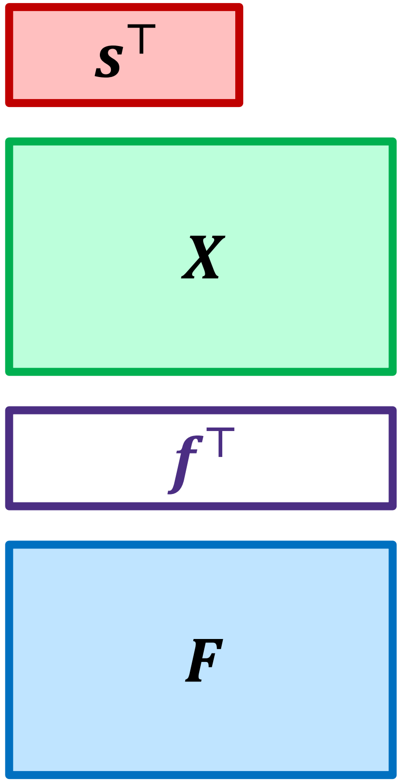
工具：[GSW13] 同态加密

$$\mathrm{sk} = \boldsymbol{s}^\top \in \mathbb{Z}_q^{1\times(n+1)}$$

$$\mathrm{hct}(x) = \boldsymbol{X} \in \mathbb{Z}_q^{(n+1)\times m}$$

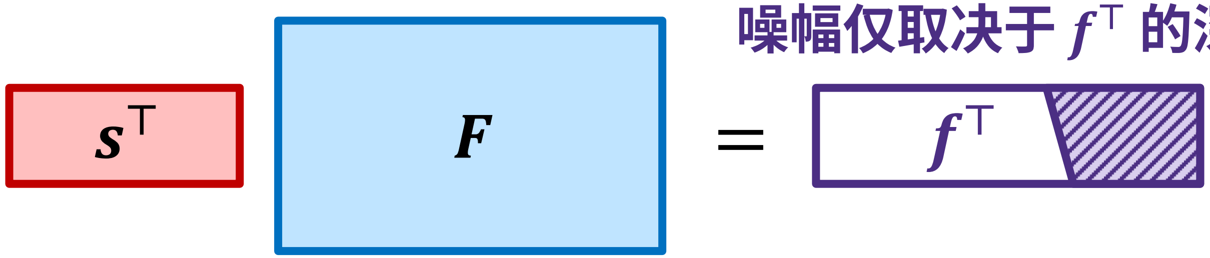
$$\boldsymbol{f}^\top : \{0,1\}^{L'} \to \mathbb{Z}_q^{1\times m}$$

$$\mathrm{HEval}\left(\boldsymbol{f}^\top, \{\boldsymbol{X}_\ell\}_{\ell\in[L']}\right) = \boldsymbol{F} \in \mathbb{Z}_q^{(n+1)\times m}$$



$$\boldsymbol{s}^\top \boldsymbol{F} = \boldsymbol{f}^\top + \boldsymbol{e}^\top$$

噪幅仅取决于 $f^\top$ 的深度



工具：[BTVW17] 矩阵值函数同态

回忆． 布尔值函数 $f(x) \in \{0,1\}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathsf{EvalC}(f,\_)} \boldsymbol{A}_f,$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathsf{EvalCX}(f,x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_f - f(x)\cdot \boldsymbol{G}).$$

工具：[BTVW17] 矩阵值函数同态

回忆. 布尔值函数 $f(x) \in \{0,1\}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{EvalC}(f,\_)} \boldsymbol{A}_f,$$

$$\{\underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})}\} \xrightarrow{\mathrm{EvalCX}(f,x,\_)} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}.$$

扩展. 矩阵值函数 $\boldsymbol{F}(x) \in \mathbb{Z}_q^{(n+1)\times m}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{MEvalC}(\boldsymbol{F},\_)} \boldsymbol{A}_{\boldsymbol{F}},$$

$$\{\underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})}\} \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},x,\_)} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(x))}.$$

工具：[BTVW17] 矩阵值函数同态

回忆. 布尔值函数 $f(x) \in \{0,1\}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{EvalC}(f,\_)} \boldsymbol{A}_f,$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathrm{EvalCX}(f,x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G}).$$

扩展. 矩阵值函数 $\boldsymbol{F}(x) \in \mathbb{Z}_q^{(n+1)\times m}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{MEvalC}(\boldsymbol{F},\_)} \boldsymbol{A}_{\boldsymbol{F}},$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(x)).$$

输出噪幅仅取决于 $\boldsymbol{F}$ 深度

工具：[BTVW17] 一搭两用 (dual use) 技巧

一搭两用.

- 函数 $\boldsymbol{F}(\_) = \mathrm{HEval}(\boldsymbol{f}^\top, \_)$ 输出矩阵
- 属性 $\boldsymbol{X} = \mathrm{ct}(x)$ 是 [GSW13] 密文，密钥、属性编码用**同一个** $\boldsymbol{s}$

扩展. 矩阵值函数 $\boldsymbol{F}(x) \in \mathbb{Z}_q^{(n+1)\times m}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{MEvalC}(\boldsymbol{F},\_)} \boldsymbol{A}_{\boldsymbol{F}},$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(x)).$$

输出噪幅仅取决于 $\boldsymbol{F}$ 深度

工具：[BTVW17] 一搭两用 (dual use) 技巧

一搭两用.

- 函数 $\boldsymbol{F}(\_) = \mathrm{HEval}(\boldsymbol{f}^\top, \_)$ 输出矩阵
- 属性 $\boldsymbol{X} = \mathrm{ct}(x)$ 是 [GSW13] 密文，密钥、属性编码用**同一个** $\boldsymbol{s}$

$$\boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{X}} - \mathrm{bits}(\boldsymbol{X}) \otimes \boldsymbol{G}) \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},\boldsymbol{X},\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(\boldsymbol{X}))$$

扩展. 矩阵值函数 $\boldsymbol{F}(x) \in \mathbb{Z}_q^{(n+1)\times m}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{MEvalC}(\boldsymbol{F},\_)} \boldsymbol{A}_{\boldsymbol{F}},$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(x)).$$

$\boxed{\text{输出噪幅仅取决于 } \boldsymbol{F} \text{ 深度}}$

工具：[BTVW17] 一搭两用 (dual use) 技巧

一搭两用.

- 函数 $\boldsymbol{F}(\_) = \mathrm{HEval}(\boldsymbol{f}^\top, \_)$ 输出矩阵
- 属性 $\boldsymbol{X} = \mathrm{ct}(x)$ 是 [GSW13] 密文，**密钥、属性编码用同一个 $\boldsymbol{s}$**

$$\boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{X}} - \mathrm{bits}(\boldsymbol{X}) \otimes \boldsymbol{G}) \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},\boldsymbol{X},\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(\boldsymbol{X}))$$

$$(\boldsymbol{F}\text{ 的定义}) \quad = \boldsymbol{s}^\top \boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{s}^\top \mathrm{HEval}(\boldsymbol{f}^\top, \boldsymbol{X})$$

扩展. 矩阵值函数 $\boldsymbol{F}(x) \in \mathbb{Z}_q^{(n+1)\times m}$ 的属性同态：

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{MEvalC}(\boldsymbol{F},\_)} \boldsymbol{A}_{\boldsymbol{F}},$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(x)).$$

$\boxed{\text{输出噪幅仅取决于 } \boldsymbol{F} \text{ 深度}}$

工具：[BTVW17] 一搭两用 (dual use) 技巧

一搭两用.

- 函数 $F(\_) = \mathrm{HEval}(f^\top, \_)$ 输出矩阵
- 属性 $X = \mathrm{ct}(x)$ 是 [GSW13] 密文，密钥、属性编码用**同一个 s**

$$s^\top(A_X - \mathrm{bits}(X) \otimes G) \xrightarrow{\mathrm{MEvalCX}(F,X,\_)} s^\top(A_F - F(X))$$

（F 的定义） $= s^\top A_F - s^\top \mathrm{HEval}(f^\top, X)$

"自动解密" $= s^\top A_F - f^\top(x)$

automagic decryption

扩展. 矩阵值函数 $F(x) \in \mathbb{Z}_q^{(n+1)\times m}$ 的属性同态：

$$\{A_\ell\} \xrightarrow{\mathrm{MEvalC}(F,\_)} A_F,$$

$$\{s^\top(A_\ell - x_\ell G)\} \xrightarrow{\mathrm{MEvalCX}(F,x,\_)} s^\top(A_F - F(x)).$$

$\boxed{\text{输出噪幅仅取决于 } F \text{ 深度}}$

工具：[BTVW17] 一搭两用 (dual use) 技巧

一搭两用.

- 函数 $\boldsymbol{F}(\_) = \mathrm{HEval}(\boldsymbol{f}^\top, \_)$ 输出矩阵
- 属性 $\boldsymbol{X} = \mathrm{ct}(x)$ 是 [GSW13] 密文，**密钥、属性编码用同一个 $\boldsymbol{s}$**

$$\boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{X}} - \mathrm{bits}(\boldsymbol{X}) \otimes \boldsymbol{G}) \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},\boldsymbol{X},\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(\boldsymbol{X}))$$

（F 的定义） $= \boldsymbol{s}^\top \boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{s}^\top \mathrm{HEval}(\boldsymbol{f}^\top, \boldsymbol{X})$

"自动解密" $= \boldsymbol{s}^\top \boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{f}^\top(x)$

automagic decryption

扩展. 矩阵值函数 $\boldsymbol{F}(x) \in \mathbb{Z}_q^{(n+1)\times m}$

两部分噪点（F 属性同态、同态加密的解密），总噪幅仅取决于 $f^\top$ 深度

$$\{\boldsymbol{A}_\ell\} \xrightarrow{\mathrm{MEvalC}(\boldsymbol{F},\_)} \boldsymbol{A}_{\boldsymbol{F}},$$

$$\{\boldsymbol{s}^\top(\boldsymbol{A}_\ell - x_\ell \boldsymbol{G})\} \xrightarrow{\mathrm{MEvalCX}(\boldsymbol{F},x,\_)} \boldsymbol{s}^\top(\boldsymbol{A}_{\boldsymbol{F}} - \boldsymbol{F}(x)).$$

输出噪幅仅取决于 F 深度

第二步：恢复编码格式 (bootstrapping)

目标． 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{small}} - \mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})$

第二步：恢复编码格式 (bootstrapping)

目标. 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$

循环密文 $\boldsymbol{S} = \text{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\text{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\boldsymbol{c}_{\text{circ}}^\top = \overbrace{\boldsymbol{s}}^{\text{属性编码秘密}}{}^\top(\boldsymbol{A}_{\text{circ}} - \overbrace{\text{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

第二步：恢复编码格式 (bootstrapping)

目标． 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{small}} - \mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})$

循环密文 $\quad \boldsymbol{S} = \mathrm{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\mathrm{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\quad \boldsymbol{c}_{\mathrm{circ}}^\top = \overbrace{\boldsymbol{s}}^{\text{属性编码秘密}}{}^\top (\boldsymbol{A}_{\mathrm{circ}} - \overbrace{\mathrm{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

属性同态 $\quad \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\_) = \mathrm{HEval}(\mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}, \_)$

$$\boldsymbol{s}^\top \left(\boldsymbol{A}_{f,\mathrm{small}} - \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{S})\right)$$

第二步：恢复编码格式 (bootstrapping)

目标. 计算 $\underline{\boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})}$

循环密文 $\quad \boldsymbol{S} = \text{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\text{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\quad \boldsymbol{c}_{\text{circ}}^\top = \overbrace{\boldsymbol{s}^\top}^{\text{属性编码秘密}} (\boldsymbol{A}_{\text{circ}} - \overbrace{\text{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

属性同态 $\quad \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\_) = \text{HEval}(\text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}, \_)$

$$\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\text{small}} - \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})\right)$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \boldsymbol{s}^\top \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})$$

第二步：恢复编码格式 (bootstrapping)

目标. 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{small}} - \mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})$

循环密文 $\boldsymbol{S} = \mathrm{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\mathrm{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\boldsymbol{c}_{\mathrm{circ}}^\top = \overbrace{\boldsymbol{s}^\top}^{\text{属性编码秘密}} (\boldsymbol{A}_{\mathrm{circ}} - \overbrace{\mathrm{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

属性同态 $\downarrow$ $\widehat{\mathrm{RndPad}}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\_) = \mathrm{HEval}(\mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}, \_)$

$$\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\mathrm{small}} - \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{S})\right)$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{small}} - \boldsymbol{s}^\top \widehat{\mathrm{RndPad}}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{S})$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\mathrm{small}} - \mathrm{RndPad}_{\boldsymbol{A}_{f,\mathrm{LARGE}}}(\boldsymbol{s})$$

第二步：恢复编码格式(bootstrapping)

目标. 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$

✓ 函数完全由 $\boldsymbol{A}_{f,\text{LARGE}}$ 描述，和 x、具体编码值无关

循环密文 $\boldsymbol{S} = \text{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\text{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\boldsymbol{c}_{\text{circ}}^\top = \overbrace{\boldsymbol{s}^\top}^{\text{属性编码秘密}} (\boldsymbol{A}_{\text{circ}} - \overbrace{\text{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

属性同态 $\widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\_) = \text{HEval}(\text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}, \_)$

$$\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\text{small}} - \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})\right)$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \boldsymbol{s}^\top \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$$

第二步：恢复编码格式 (bootstrapping)

目标. 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$

- ✓ 函数完全由 $\boldsymbol{A}_{f,\text{LARGE}}$ 描述，和 x、具体编码值无关
- ✓ 函数深度低、固定、和 f 无关

循环密文 $\boldsymbol{S} = \text{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\text{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\boldsymbol{c}_{\text{circ}}^\top = \overbrace{\boldsymbol{s}^\top}^{\text{属性编码秘密}} (\boldsymbol{A}_{\text{circ}} - \overbrace{\text{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

属性同态 $\widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\_) = \text{HEval}(\text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}, \_)$

$$\boldsymbol{s}^\top(\boldsymbol{A}_{f,\text{small}} - \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S}))$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \boldsymbol{s}^\top \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$$

第二步：恢复编码格式 (bootstrapping)

目标. 计算 $\boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$

- ✓ 函数完全由 $\boldsymbol{A}_{f,\text{LARGE}}$ 描述，和 x、具体编码值无关
- ✓ 函数深度低、固定、和 f 无关
- ✓ 属性同态运算只用 $\boldsymbol{S}$ 不用 $\boldsymbol{s}$

循环密文 $\boldsymbol{S} = \text{hct}(\underbrace{\boldsymbol{s}}_{\text{密钥}}, \underbrace{\text{bits}(\boldsymbol{s})}_{\text{明文}})$

循环编码 $\boldsymbol{c}_{\text{circ}}^\top = \overbrace{\boldsymbol{s}^\top}^{\text{属性编码秘密}} (\boldsymbol{A}_{\text{circ}} - \overbrace{\text{bits}(\boldsymbol{S})}^{\text{被编码的属性}} \otimes \boldsymbol{G})$

属性同态 $\widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\_) = \text{HEval}(\text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}, \_)$

$$\boldsymbol{s}^\top\left(\boldsymbol{A}_{f,\text{small}} - \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})\right)$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \boldsymbol{s}^\top \widehat{\text{RndPad}}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{S})$$

$$= \boldsymbol{s}^\top \boldsymbol{A}_{f,\text{small}} - \text{RndPad}_{\boldsymbol{A}_{f,\text{LARGE}}}(\boldsymbol{s})$$

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

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

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

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

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

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

$$\xrightarrow[\text{[BGGHNSVV14]}]{\textbf{属性同态}} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})}$$

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

$$\begin{aligned} \boldsymbol{c}_1^\top &= \boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G}) \\ \boldsymbol{c}_2^\top &= \boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G}) \end{aligned} \quad \xrightarrow[\text{[BGGHNSVV14]}]{\textbf{属性同态}} \quad \boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})$$

$$\Big\downarrow \ \textbf{除噪}$$

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

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

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

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

$\xrightarrow[\text{[BGGHNSVV14]}]{\text{属性同态}}$ $\underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})}$

$\Big\downarrow$ 除噪

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

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

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

$$\boldsymbol{c}_1^\top = \underbrace{\boldsymbol{s}^\top(\boldsymbol{A}_1 - x_1\boldsymbol{G})}$$
$$\boldsymbol{c}_2^\top = \underbrace{\boldsymbol{s}^\top(\boldsymbol{A}_2 - x_2\boldsymbol{G})}$$

$\xrightarrow[\text{[BGGHNSVV14]}]{\text{属性同态}}$ $\underbrace{\boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})}$

$\big\downarrow$ **除噪**

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

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

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

属性同态 [GSW13, BGGHNSVV14, BTVW17]

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

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

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

$$\xrightarrow[\text{[BGGHNSVV14]}]{\text{属性同态}} \boldsymbol{s}^\top(\boldsymbol{A}_3' - x_3\boldsymbol{G})$$

$$\Big\downarrow \text{除噪}$$

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

$$\boldsymbol{c}_3^\top = \boldsymbol{s}^\top(\boldsymbol{A}_3 - x_3\boldsymbol{G}) \xleftarrow{\text{恢复编码格式}} \cancel{\boldsymbol{s}^\top\boldsymbol{A}_3 - \mathrm{RndPad}_{\boldsymbol{A}_3'}(\boldsymbol{s})}$$

$$\boldsymbol{c}_{\mathrm{circ}}^\top = \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}) \longrightarrow \boldsymbol{s}^\top\boldsymbol{A}_3 - \mathrm{RndPad}_{\boldsymbol{A}_3'}(\boldsymbol{s})$$

属性同态 [GSW13, BGGHNSVV14, BTVW17]

降噪 = 除噪 + 恢复编码格式（小中大噪幅）

$x_3 = x_3(x_1, x_2)$ 是电路中的一个门

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

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

属性同态 [BGGHNSVV14] →

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

↓ 除噪

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

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

← 恢复编码格式

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

∞

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

属性同态 [GSW13, BGGHNSVV14, BTVW17]

接口：深度不限的属性同态运算

$$\mathrm{UEvalC}(f, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}) \to \boldsymbol{A}_f$$

接口：深度不限的属性同态运算

$$\mathrm{UEvalC}(f, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}) \to \boldsymbol{A}_f$$

$$\mathrm{UEvalCX}\begin{pmatrix} f, x, \boldsymbol{S}, \\ \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \\ \boldsymbol{c}_{\mathrm{attr}}^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{c}_{\mathrm{circ}}^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})} \end{pmatrix} \to \boldsymbol{c}_f^{\top} = \underbrace{\boldsymbol{s}^{\top}(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}$$

接口：深度不限的属性同态运算

$$\mathrm{UEvalC}(f, \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}) \to \boldsymbol{A}_f$$

$$\mathrm{UEvalCX}\begin{pmatrix} f, x, \boldsymbol{S}, \\ \boldsymbol{A}_{\mathrm{attr}}, \boldsymbol{A}_{\mathrm{circ}}, \\ \boldsymbol{c}_{\mathrm{attr}}^{\top} = \underset{\sim\sim\sim}{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{c}_{\mathrm{circ}}^{\top} = \underset{\sim\sim\sim}{\boldsymbol{s}^{\top}(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})} \end{pmatrix} \to \boldsymbol{c}_f^{\top} = \underset{\sim\sim\sim}{\boldsymbol{s}^{\top}(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}$$

噪点（仅）以高概率足够小

深度不限的电路的 AB-LFE

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

深度不限的电路的 AB-LFE

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

$$\mathrm{ct}_{f,x} = \left\{ \vphantom{\begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix}} \right.$$

深度不限的电路的 AB-LFE

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

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

深度不限的电路的 AB-LFE

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

$$\mathrm{ct}_{f,x} = \begin{cases} & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ & \underset{\sim}{\boldsymbol{s}^\top \boldsymbol{A}_f \boldsymbol{G}^{-1}(\boldsymbol{u})} + \mu \cdot \lfloor q/2 \rceil \end{cases}$$

深度不限的电路的 AB-LFE

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

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

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

深度不限的电路的 AB-LFE

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

$f(x) = 0 =$ 可 时
消去**一次性密钥**

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

深度不限的电路的 AB-LFE

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

$f(x) = 0 =$ 可时
消去**一次性密钥**

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

$$\cdot\, \boldsymbol{G}^{-1}(\boldsymbol{u})$$

深度不限的电路的 AB-LFE 安全性

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

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

$f(x) = 1 =$ 否 时

深度不限的电路的 AB-LFE 安全性

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

$f(x) = 1 = $ 否 时

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

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

$$\boldsymbol{s}^\top \boldsymbol{A}_f \boldsymbol{G}^{-1}(\boldsymbol{u}) = \boldsymbol{c}_f^\top \boldsymbol{G}^{-1}(\boldsymbol{u}) + \underbrace{1}_{f(x)} \cdot \boldsymbol{s}^\top \boldsymbol{u}$$

深度不限的电路的 AB-LFE 安全性

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

$$f(x) = 1 = \text{否 时}$$

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

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

注意. 安全证明依赖于正确性（$\boldsymbol{c}_f^\top$ 噪幅小）

深度不限的电路的 AB-LFE 安全性

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

$$\mathrm{digest}_f = \boldsymbol{A}_f \leftarrow \mathrm{UEvalC}$$

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

$f(x) = 1 =$ 否 时

$$\boldsymbol{c}_f^\top \boldsymbol{G}^{-1}(\boldsymbol{u}) + \underbrace{1}_{f(x)} \cdot \underset{\sim}{\boldsymbol{s}^\top \boldsymbol{u}}$$

注意. 安全证明依赖于正确性（$\boldsymbol{c}_f^\top$ 噪幅小）

$\mathrm{ct}_{f,x} \approx \$$ 归约为循环 LWE

深度不限的电路的 ABE

$$\mathrm{ct}_x = \left\{ \begin{array}{ll} & \underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ & \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underset{\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}$$

深度不限的电路的 ABE

$$\mathrm{ct}_x = \left\{ \begin{array}{ll} & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ & \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}$$

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

$$\mathrm{ct}_x = \left\{\begin{array}{ll} & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \underset{\sim}{\boldsymbol{s}^\top\boldsymbol{B}}, & \underset{\sim}{\boldsymbol{s}^\top\boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array}\right. \Bigg\} \xrightarrow{\mathtt{UEvalCX}} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}$$

indirection
"再加一层中转"

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

$$\mathrm{ct}_x = \begin{cases} \qquad \underset{\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{S},\ \ \underset{\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \underset{\sim\sim\sim}{\boldsymbol{s}^\top\boldsymbol{B}},\quad \underset{\sim\sim\sim}{\boldsymbol{s}^\top\boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{cases} \xrightarrow{\mathrm{UEvalCX}} \underset{\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - f(x) \cdot \boldsymbol{G})}$$

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

短向量 $\boldsymbol{k} = \boldsymbol{B}^{-1}(\boldsymbol{p})$ 满足 $\boldsymbol{B}\boldsymbol{k} = \boldsymbol{p}$
（可用 $\boldsymbol{B}$ 的陷门高效生成）

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

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

短向量 $\boldsymbol{k} = \boldsymbol{B}^{-1}(\boldsymbol{p})$ 满足 $\boldsymbol{B}\boldsymbol{k} = \boldsymbol{p}$
（可用 $\boldsymbol{B}$ 的陷门高效生成）

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

$$\left.\begin{matrix} \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G}), \\ \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}), \end{matrix}\right\} \xrightarrow{\mathrm{UEvalCX}} \boldsymbol{s}^\top(\boldsymbol{A}_f - \cancel{f(x)} \cdot \boldsymbol{G})$$

$$\boldsymbol{s}^\top \boldsymbol{B} \cdot \boldsymbol{k} = \boldsymbol{s}^\top \boldsymbol{p}$$

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

短向量 $\boldsymbol{k} = \boldsymbol{B}^{-1}(\boldsymbol{p})$ 满足 $\boldsymbol{B}\boldsymbol{k} = \boldsymbol{p}$
（可用 $\boldsymbol{B}$ 的陷门高效生成）

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

$\boldsymbol{s}^\top\boldsymbol{B} \cdot \boldsymbol{k} = \boldsymbol{s}^\top\boldsymbol{p}$

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE

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

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

短向量 $\boldsymbol{k} = \boldsymbol{B}^{-1}(\boldsymbol{p})$ 满足 $\boldsymbol{B}\boldsymbol{k} = \boldsymbol{p}$
（可用 $\boldsymbol{B}$ 的陷门高效生成）

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

$\boldsymbol{s}^\top \boldsymbol{B} \cdot \boldsymbol{k} = \boldsymbol{s}^\top \boldsymbol{p}$

indirection
“再加一层中转”

- Enc 不知道 $\boldsymbol{A}_f$
- 多个 sk_f 下安全

深度不限的电路的 ABE：闪避 LWE 概要

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

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

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

$$\xrightarrow{\mathrm{UEvalCX}} \boldsymbol{s}^\top(\boldsymbol{A}_f - \overbrace{f(x)}^{1} \cdot \boldsymbol{G})$$

$\boldsymbol{B}$ 有陷门时
LWE 不成立！

深度不限的电路的 ABE：闪避 LWE 概要

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

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

没有 $\boldsymbol{B}$ 的**完整陷门**，
有关于 $\boldsymbol{B}$ 的**一些陷门原像**，
如何处理？

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

$$\xrightarrow{\mathrm{UEvalCX}} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - \overbrace{f(x)}^{1} \cdot \boldsymbol{G})}$$

$\boldsymbol{B}$ 有陷门时
LWE 不成立！

深度不限的电路的 ABE：闪避 LWE 概要

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

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

没有 $\boldsymbol{B}$ 的**完整陷门**，
有关于 $\boldsymbol{B}$ 的**一些陷门原像**，
如何处理？

$$\mathrm{ct}_x = \left\{ \begin{array}{ll} & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G})}, \\ \boldsymbol{S}, & \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G})}, \\ \boxed{\underset{\sim}{\boldsymbol{s}^\top\boldsymbol{B}},} & \underset{\sim}{\boldsymbol{s}^\top\boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right\} \xrightarrow{\mathrm{UEvalCX}} \underset{\sim}{\boldsymbol{s}^\top(\boldsymbol{A}_f - \overbrace{f(x)}^{1} \cdot \boldsymbol{G})}$$

$\boldsymbol{B}$ 有陷门时
LWE 不成立！

闪避 LWE。 同时给出 $\underset{\sim}{\boldsymbol{s}^\top\boldsymbol{B}}, \boldsymbol{B}^{-1}(\boldsymbol{P})$ **差不多等效于**同时给出 $\underset{\sim}{\boldsymbol{s}^\top\boldsymbol{B}}, \underset{\sim}{\boldsymbol{s}^\top\boldsymbol{P}}$，
外加处理一些循环加密的有的没的的……（非常不严谨的说法）

深度不限的电路的 ABE：安全性概要

失去陷门

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

利用闪避 LWE

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

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

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

深度不限的电路的 ABE：安全性概要

失去陷门

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

利用闪避 LWE

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

$\approx \$$ 理同 AB-LFE

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

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

深度不限的电路的 ABE：安全性概要

失去陷门

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

利用闪避 LWE

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

$\approx \$$ 理同 AB-LFE

$$\mathrm{ct}_x = \left\{ \begin{array}{l} \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{attr}} - x \otimes \boldsymbol{G}), \\ \boldsymbol{S}, \quad \boldsymbol{s}^\top(\boldsymbol{A}_{\mathrm{circ}} - \mathrm{bits}(\boldsymbol{S}) \otimes \boldsymbol{G}), \\ \boldsymbol{s}^\top \boldsymbol{B}, \quad \boxed{\boldsymbol{s}^\top \boldsymbol{u}} + \mu \cdot \lfloor q/2 \rceil \end{array} \right. \left. \vphantom{\begin{array}{l} a \\ b \end{array}} \right\} \xrightarrow{\mathrm{UEvalCX}} \boldsymbol{s}^\top(\boldsymbol{A}_f - \overbrace{f(x)}^{1} \cdot \boldsymbol{G})$$

隐藏了消息

深度不限的电路的 ABE：安全性概要

失去陷门

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

利用闪避 LWE

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

$\approx \$$ 理同 AB-LFE

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

隐藏了消息

另法. 用双线性群计算 OTP，用 GGM 完成证明 [LLL22]

属性编码自举

实现**不限深度**的属性同态

属性编码自举

实现**不限深度**的属性同态

$\Longrightarrow$ **基于格、不限深度的**

LFE、单密钥 FE、可复用 GC、ABE

属性编码自举
实现**不限深度**的属性同态

$\Longrightarrow$ **基于格、不限深度的**

LFE、单密钥 FE、可复用 GC、ABE

?

- 其他同态原语
- 完美正确性

属性编码自举
实现**不限深度**的属性同态

$\Longrightarrow$ **基于格、不限深度的**

LFE、单密钥 FE、可复用 GC、ABE

?

- 其他同态原语
- 完美正确性
- 非知识型 (knowledge-type) 假设下证明 ABE 安全性
- 多项式大小的模噪比 (modulus-to-noise ratio)

属性编码自举
实现**不限深度**的属性同态

$\Longrightarrow$ **基于格、不限深度的**
LFE、单密钥 FE、可复用 GC、ABE

?

- 其他同态原语
- 完美正确性
- 非知识型 (knowledge-type) 假设下证明 ABE 安全性
- 多项式大小的模噪比 (modulus-to-noise ratio)
- 非循环的自举

属性编码自举
实现**不限深度**的属性同态

$\Longrightarrow$ **基于格、不限深度的**
LFE、单密钥 FE、可复用 GC、ABE

?
- 其他同态原语
- 完美正确性
- 非知识型 (knowledge-type) 假设下证明 ABE 安全性
- 多项式大小的模噪比 (modulus-to-noise ratio)
- 非循环的自举

谢谢！

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

https://ia.cr/2023/1716

提问 1

有一些从循环安全性得到 $i\mathcal{O}$ 的工作 [BDGM20a, GP20, BDGM20b, WW20]，但是这些假设已经有攻击 [HJL21]，那么：

- 循环安全假设里密钥泄露 (leakage) 到多少就不安全了?
- 为什么这项工作里的循环安全假设可以认为靠谱?

提问 1 与回答 1.1

有一些从循环安全性得到 $i\mathcal{O}$ 的工作 [BDGM20a, GP20, BDGM20b, WW20]，但是这些假设已经有攻击 [HJL21]，那么：

- **循环安全假设里密钥泄露 (leakage) 到多少就不安全了?**
- 为什么这项工作里的循环安全假设可以认为靠谱?

回答. 我不太熟悉从循环安全性得到 $i\mathcal{O}$ 的系列工作，不过我的感觉是那些工作需要“条件解密”：

- 可以在一类既定的同态运算（电路求值）之后解密，
- 但又不允许在同态运算之前解密（从而得到电路本身），

即“对（密钥泄露部分的）解密能力有精细的控制”，这通常是出问题的地方.

提问 1 与回答 1.2

有一些从循环安全性得到 $i\mathcal{O}$ 的工作 [BDGM20a, GP20, BDGM20b, WW20]，但是这些假设已经有攻击 [HJL21]，那么：

- 循环安全假设里密钥泄露 (leakage) 到多少就不安全了?
- **为什么这项工作里的循环安全假设可以认为靠谱?**

回答. 至于这项工作为什么可以觉得靠谱，是因为：

- 这个假设和用于自举超多项式模噪比的 [GSW13] 是同一个假设；
- 本作的应用的安全性里，没有任何时刻可以发生解密，因此不需要"对解密能力的精细控制".

这种情况下暂时还**不**知道循环**不**安全性.

提问 2

可否用陷门采样的技巧，如 [MP12]，来避免“闪避 LWE”?

提问 2 和回答 2（事后有补充）

可否用陷门采样的技巧，如 [MP12]，来避免“闪避 LWE”？

回答. [MP12] 是本作方案里真实算法会用到的.
要解答这个问题，得深入 [BGGHNSVV14] 的具体操作，用本次报告的符号来说，彼作在安全证明中设置

$$\boldsymbol{A}_{\text{attr}} = \boldsymbol{B}\boldsymbol{R}_{\text{attr}} + x \otimes \boldsymbol{G}.$$

这样做可以让 $\boldsymbol{B}$ 失去陷门、以 $\boldsymbol{R}_{\text{attr}}$ 作为“部分挖去” (punctured) 的陷门，同时依然正常生成 sk_f 中的陷门原像——挖去的正好是使坏者所不能查询的（可以解密的）密钥. 然而这种嵌入、挖去的技巧不总是奏效，本作的证明暂时要用更强的假设.

提问 3

第二节开头，同态作用与复合函数?

提问 3 与回答 3.1

第二节开头，同态作用与复合函数?

回答. 同态作用时，下面两对数据是绑定的:

- 作用的函数 $\leftrightarrow$ pk;
- 得到的函数值 $\leftrightarrow$ 密文的 y.

例如，$f(x_1)=0$、$f(x_2)=1$，又 $g(y)=0$，那么

$$\mathrm{EvalCX}\big(g, f(x_1), \mathrm{Enc}\big(\mathrm{pk}_f, f(x_1), \mu\big)\big) \to \mathrm{Enc}\big(\mathrm{pk}_{g\circ f}, 0, \mu\big),$$

$$\mathrm{EvalCX}\big(g, f(x_2), \mathrm{Enc}\big(\mathrm{pk}_f, f(x_2), \mu\big)\big) \to \mathrm{Enc}\big(\mathrm{pk}_{g\circ f}, 0, \mu\big).$$

但是 $\mathrm{sk}_{g\circ f}$ 本应能够解密两者，没有矛盾.

提问 3 与回答 3.2（事后补充）

第二节开头，同态作用与复合函数?

回答. 同态作用时，下面两对数据是绑定的：

- 作用的函数 $\leftrightarrow$ pk；
- 得到的函数值 $\leftrightarrow$ 密文的 y.

例如，$f(x_1) = 0$、$f(x_2) = 1$，又 $g(y) = 0$，那么

$$\mathrm{EvalCX}\big(g, f(x_1), \mathrm{Enc}\big(\mathrm{pk}_f, f(x_1), \mu\big)\big) \to \mathrm{Enc}\big(\mathrm{pk}_{g \circ f}, 0, \mu\big),$$

$$\mathrm{EvalCX}\big(g, f(x_2), \mathrm{Enc}\big(\mathrm{pk}_f, f(x_2), \mu\big)\big) \to \mathrm{Enc}\big(\mathrm{pk}_{g \circ f}, 0, \mu\big).$$

若只有 sk_f，则**可以**解密**绿色**密文、**不能**解密**蓝色**密文，也没有矛盾.

提问 3 与回答 3.3（事后补充）

第二节开头，同态作用与复合函数?

回答. 同态作用时，下面两对数据是绑定的：

- 作用的函数 $\leftrightarrow \mathrm{pk}$;
- 得到的函数值 $\leftrightarrow$ 密文的 y.

例如，$f(x_1) = 0$、$f(x_2) = 1$，又 $g(y) = 0$，那么

$$\mathrm{EvalCX}\big(g, f(x_1), \mathrm{Enc}\big(\mathrm{pk}_f, f(x_1), \mu\big)\big) \to \mathrm{Enc}\big(\mathrm{pk}_{g\circ f}, 0, \mu\big),$$

$$\mathrm{EvalCX}\big(g, f(x_2), \mathrm{Enc}\big(\mathrm{pk}_f, f(x_2), \mu\big)\big) \to \mathrm{Enc}\big(\mathrm{pk}_{g\circ f}, 0, \mu\big).$$

又若分别进一步以 g 同态作用，则 sk_f 和**黄色**密文的公钥不对应，**无法**从属性同态**得出或否定**原来 pk_f 下**密文**的安全性.

提问 3 与回答 3.4（事后补充）

第二节开头，同态作用与复合函数?

回答. 同态运算多次复合，在 FHE 文献中叫“多跳”(multi-hop)，属性同态的多跳也有应用，如

[T19] Fully Secure Attribute-Based Encryption for t-CNF from LWE.