泛函加密，代价几何？

谈泛函加密、属性加密的最优时空效率

Aayush Jain

Carnegie Mellon University

Rachel Lin
林蕙佳

罗辑

UNIVERSITY of WASHINGTON

报告大纲

- 偏泛函加密　　定义、目标
- 动机、问题
- 成果介绍

- 必要之繁　　时空效率下界证明一瞥
- 技巧匮乏　　与 DE-PIR 的联系
- 偏泛函加密　　定义细节
- 核心工具　　凝练乱码 RAM
- 未解问题

部分保密的泛函加密 (partially hiding functional encryption)

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

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

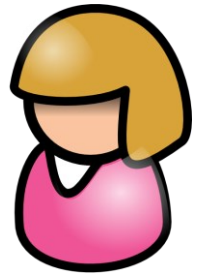
函数

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

mpk

总是明文提供 f, x 本身

x, ct_x



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

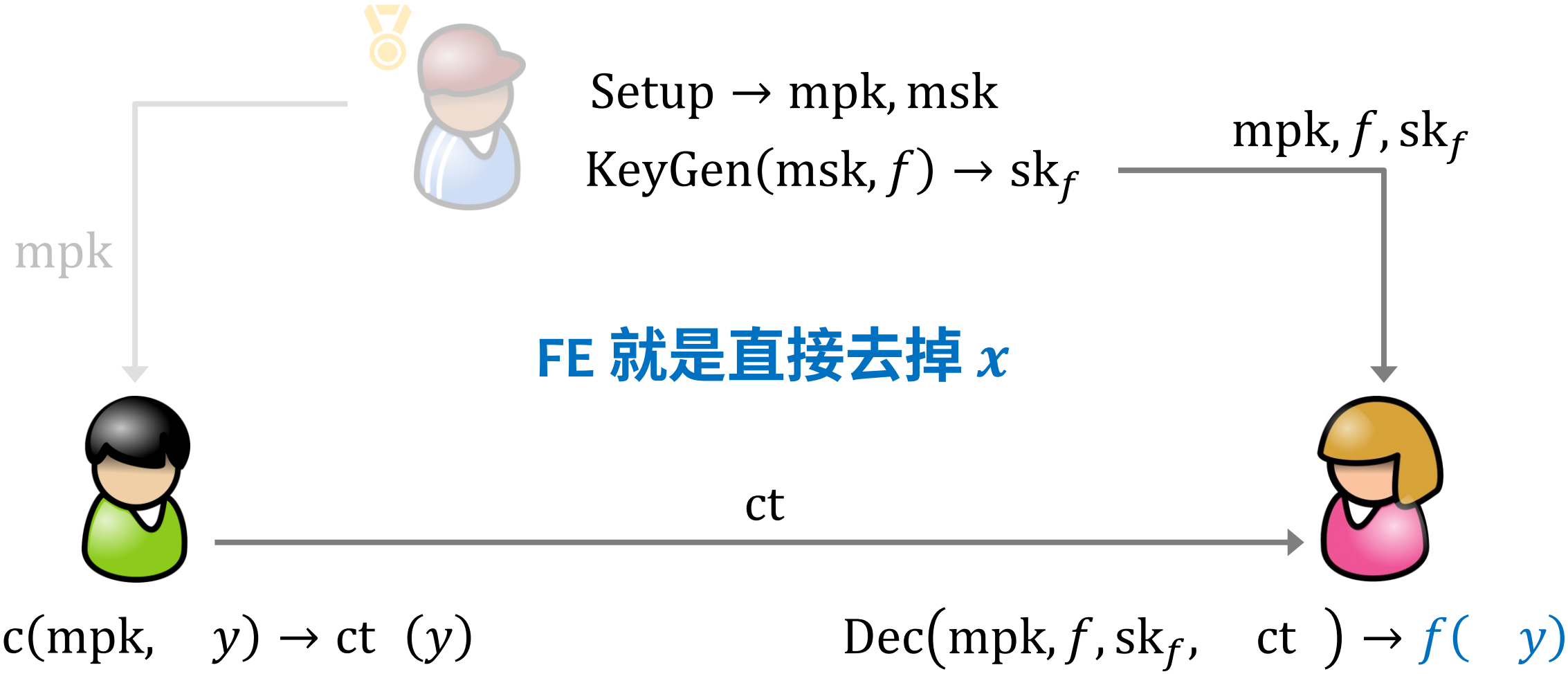
公开 / 秘密

输入

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

正确性要求

偏泛函加密实现泛函加密 (functional encryption)



偏泛函加密实现**属性加密** (attribute-based encryption)

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

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

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

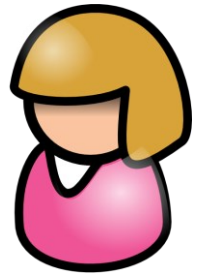
mpk

ABE 中 f 的形式仅限于

$$f(x,y) = \begin{cases} y, & \text{若 } P(x) = 1; \\ \perp, & \text{若 } P(x) = 0. \end{cases}$$

其中 P 是“访问策略”

x, ct_x



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

x = 属性

y = 消息

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

当 $P(x) = 1$ 时

解密可得 y

偏泛函加密的安全性

$\text{Setup} \to \text{mpk}, \text{msk}$

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

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

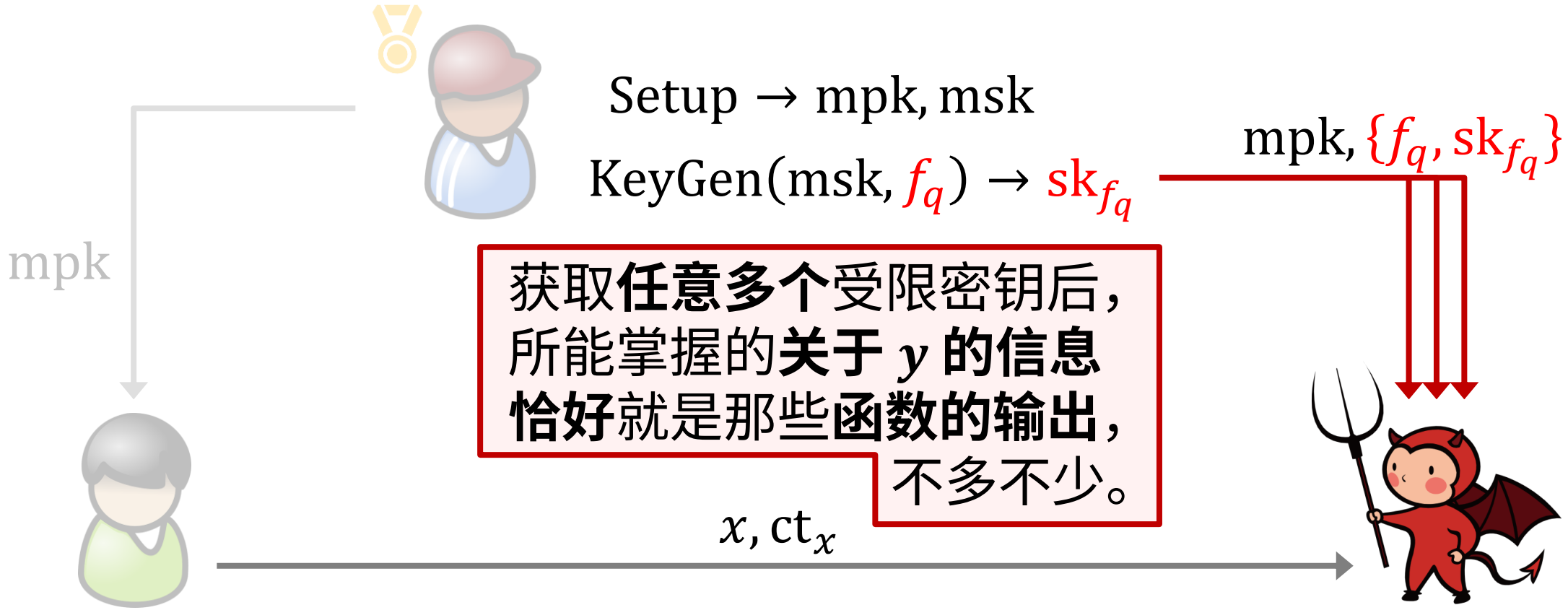
mpk

x, ct_x

$\text{Enc}(\text{mpk}, x, y) \to \text{ct}_x(y)$

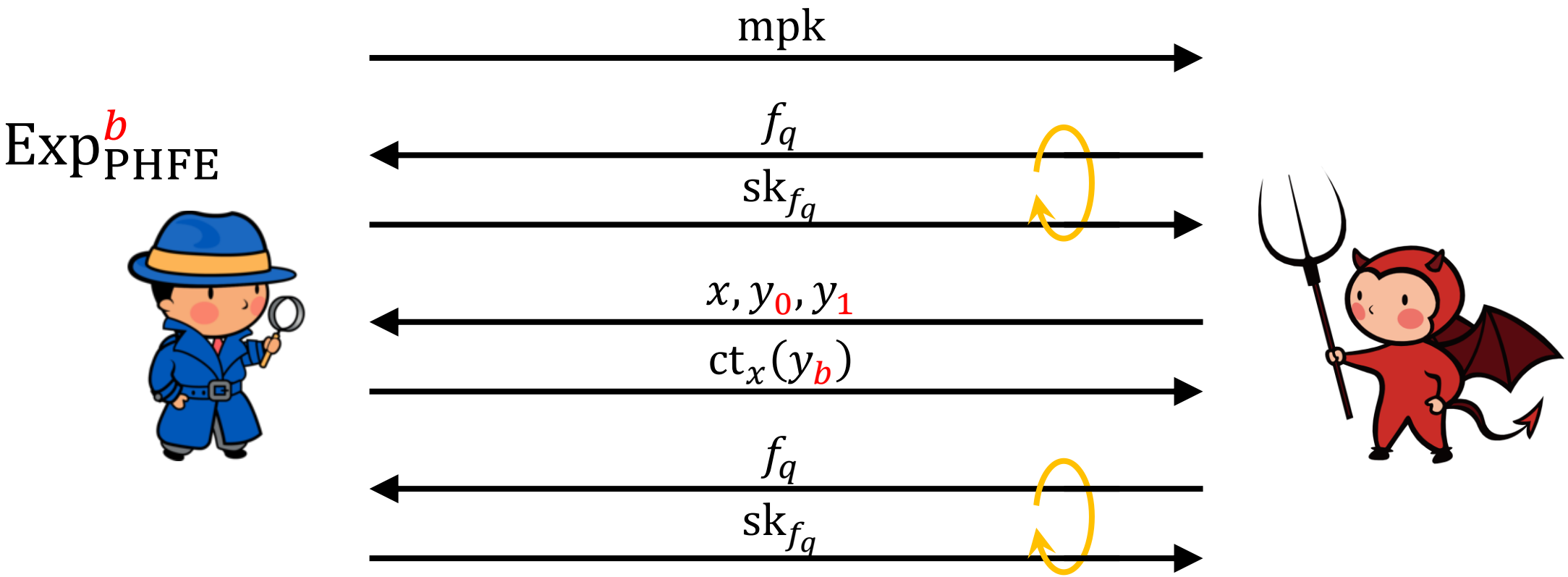
安全性．除了 $f(x, y)$ 之外，
一切关于 y 的信息都隐藏。

偏泛函加密的安全性：抗乌合 (collusion resistance)



安全性．除了 $\{f_q(x, y)\}$ 之外，
一切关于 y 的信息都隐藏。

选择明文攻击下密文不可区分 (IND-CPA)



若 $|y_0| = |y_1|$ **且** $\forall q: f_q(x, y_0) = f_q(x, y_1)$ **则** $\mathrm{Exp}^{0}_{\mathrm{PHFE}} \approx \mathrm{Exp}^{1}_{\mathrm{PHFE}}$

多快好省

★ 多：支持各种复杂函数

支持**输出长度无限制**、
random-access machine
用**随机访问机**表示的函数

★ 省：短密钥、短密文

$$|\mathrm{sk}_f| = \mathrm{poly}(|f|)$$
$$|\mathrm{ct}_x(y)| = \mathrm{poly}(|x|, |y|)$$

★ 快：快速解密

$$T_{\mathrm{Dec}} = \mathrm{poly}(|f|, |x|, |y|, T)$$

多快好省（续）

★ 多：支持各种复杂函数

支持**输出长度无限制**、
random-access machine
用**随机访问机**表示的函数

★ 省：短密钥、短密文

$$|\mathrm{sk}_f| = \mathrm{O}(1)$$

$$|\mathrm{ct}_x(y)| = |y| + \mathrm{O}(1)$$

理想标的

★ 快：快速解密

$$T_{\mathrm{Dec}} = \mathrm{O}(T)$$

理想标的

★ 好：适应性安全、基于弱假设

动机与问题

偏泛函加密**能有多高效**?

不同效率参数间是否
“**鱼与熊掌，不可兼得**”?

（基于何种假设、）
如何构造**效率最优**的偏泛函加密?

本作成果：**近最优偏泛函加密**

（适用于电路、选择性安全、单密钥 FE，满足 $T_{\mathrm{Enc}}=|f|^{1-\varepsilon}$）

“能用来实现程序混淆”的 FE [前人之述备矣]

$\Longrightarrow$ **多项式安全、适用于电路的 FE**

$\Longrightarrow$ **适应性安全、适用于 RAM 的 PHFE，效率：**

$$|\mathrm{mpk}| = \mathrm{O}(1),\quad |\mathrm{sk}_f| = \mathrm{O}(1),\quad |\mathrm{ct}_x(y)| = 2|y| + \mathrm{O}(1),$$

$$T_{\mathrm{KeyGen}} = \mathrm{O}(|f|),\quad T_{\mathrm{Enc}} = \mathrm{O}(|x| + |y|),$$

$$T_{\mathrm{Dec}} = \mathrm{O}(T + |f| + |x| + |y|)$$

？ ？

必要之繁 / 技巧匮乏

几项 FE 方面的相关工作

支持		适应性安全	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	需要的假设
RAM 输出长度无限制	**本作**	✓	$O(1)$	$2\lvert y \rvert + O(1)$	$O(T + \lvert f \rvert + \lvert x \rvert + \lvert y \rvert)$	**FE**
RAM	ACFQ		$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert)$	PK-DE-PIR + FE
Turing 机	AS	✓	$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	$i\mathcal{O}$
	AJS	✓	$c\lvert f \rvert + O(1)$	$c\lvert y \rvert + O(1)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	subexp $i\mathcal{O}$
	AM	✓	$\mathrm{poly}(\lvert f \rvert)$	$O(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	dist. ind. FE
	KNTY		$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	1-key sel. FE
电路	GGHRSW		$\mathrm{poly}(\lvert C \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$\mathrm{poly}(\lvert C \rvert)$	$i\mathcal{O}$
	KNTY	✓	$\mathrm{poly}(\lvert C \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$\mathrm{poly}(\lvert C \rvert)$	1-key sel. FE
	GWZ		$\mathrm{poly}(\lvert C \rvert)$	$\lvert y \rvert + O(1)$	$\mathrm{poly}(\lvert C \rvert)$	$i\mathcal{O}$

效率大幅改进、“两朵乌云”

支持		适应性安全	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	需要的假设
RAM 输出长度无限制	本作	✓	$O(1)$	$2\lvert y \rvert + O(1)$	$O(T + \lvert f \rvert + \lvert x \rvert + \lvert y \rvert)$?	FE
RAM	ACFQ		$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert)$	PK-DE-PIR + FE
Turing 机	AS	✓	$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	$i\mathcal{O}$
	AJS	✓	$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	subexp $i\mathcal{O}$
	AM	✓	$\mathrm{poly}(\lvert f \rvert)$	$O(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	dist. ind. FE
	KNTY		$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	1-key sel. FE
电路	GGHRSW		$\mathrm{poly}(\lvert C \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$\mathrm{poly}(\lvert C \rvert)$	$i\mathcal{O}$
	KNTY	✓	$\mathrm{poly}(\lvert C \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$\mathrm{poly}(\lvert C \rvert)$	1-key sel. FE
	GWZ		$\mathrm{poly}(\lvert C \rvert)$	$\lvert y \rvert + O(1)$	$\mathrm{poly}(\lvert C \rvert)$	$i\mathcal{O}$

多项式效率改进到**近最优效率**

✓ 可以得到：**放弃适应性安全**且**限制输出长度**

本作成果：(PH-)FE 时空效率下界（无条件成立）

首个 (PH-)FE 时空效率权衡下界

对任意适用于 RAM 的 FE 和 PHFE，若

$$|\mathrm{sk}_f| = \mathrm{O}(|f|^A),\quad T_{\mathrm{Dec}} = (T + |f|^B + |y|)\,\mathrm{O}(|x|^C)$$

则 $A \geq 1$ 或 $B \geq 1$.

对任意适用于 RAM 的 PHFE，若

$$|\mathrm{ct}_x(y)| = \mathrm{O}(|x|^A |y|^C),\quad T_{\mathrm{Dec}} = (T + |f| + |x|^B)\,\mathrm{O}(|y|^C)$$

则 $A \geq 1$ 或 $B \geq 1$.

“密钥密文长度、解密时间不能同时关于 f, x 次线性。”

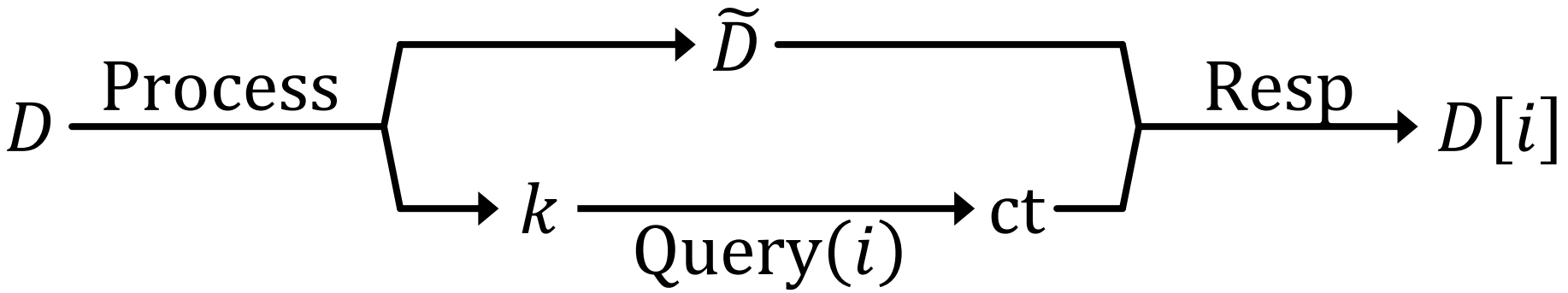
y 呢？又若考虑**线性长度**，可以得到**最优解密时间**吗？答案与 **DE-PIR** 有关.

这两个下界对极**选择性安全**、**单密钥**、**单密文**、**私钥**方案（即**乱码化**（garbling）也成立，而且只用到**相当简单**的函数.

doubly efficient private information retrieval

双重高效隐私信息检索

DE-PIR



客户端高效 $|k| = \mathrm{O}(1)$ **且** $T_{\mathrm{Query}} = \mathrm{O}(|D|^{1-\varepsilon})$

服务端高效 $T_{\mathrm{Resp}} = \mathrm{O}(|D|^{1-\varepsilon})$

安全 $\widetilde{D}, \{\mathrm{ct}(i_q)\}$ **隐藏** $\{i_q\}$

效率理想型 $|\widetilde{D}| = \mathrm{O}(|D|)$ **且** $T_{\mathrm{Query}}, T_{\mathrm{Resp}} = \mathrm{O}(1)$

这能构造出吗?

本作成果：最速解密蕴涵着 DE-PIR

若 PHFE 满足

本作新结论

$$|\mathrm{sk}_f| = \mathrm{O}(|f|^A),\quad T_{\mathrm{Dec}} = |f|^B\,\mathrm{poly}(T,|x|,|y|),$$

其中 $B < 1$，则存在着如下效率的**公钥** DE-PIR：

$$|\widetilde{D}| = |D| + \mathrm{O}(|D|^A),\quad T_{\mathrm{Query}} = \mathrm{O}(1),\quad T_{\mathrm{Resp}} = \mathrm{O}(|D|^B).$$

若 PHFE 满足

$$|\mathrm{ct}_x(y)| = |x|^A\,\mathrm{poly}(|y|),\quad T_{\mathrm{Dec}} = |x|^B\,\mathrm{poly}(T,|f|,|y|),$$

或

$$|\mathrm{ct}_x(y)| = |y|^A\,\mathrm{poly}(|x|),\quad T_{\mathrm{Dec}} = |y|^B\,\mathrm{poly}(T,|f|,|x|),$$

其中 $B < 1$，则存在着如下效率的**私钥** DE-PIR：

$$|\widetilde{D}| = |D| + \mathrm{O}(|D|^A),\quad T_{\mathrm{Query}} = \mathrm{O}(1),\quad T_{\mathrm{Resp}} = \mathrm{O}(|D|^B).$$

ACFQ 也证明了

本作成果：适用于 RAM、常数额外开销的 $i\mathcal{O}$ 和 ABE

新结论！ 此前只有
电路 [BV]$_{\text{外加 LWE}}$ / Turing 机 [AJS] 的版本

$\Longrightarrow$ 亚指数安全、适用于电路的 FE
亚指数安全、适用于 RAM 的 $i\mathcal{O}$，效率：
$|\widetilde{M}| = 2|M| + \mathrm{poly}(|D|)$

四个新结论！

适用于 RAM 的 ABE	$\lvert\mathrm{sk}_f\rvert$	$\lvert\mathrm{ct}_x\rvert$	T_{Dec}
PHFE 的直接推论	$O(1)$	$O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert)$
微调一下构造	$\lvert f\rvert + O(1)$	$O(1)$	$O(T + \lvert x\rvert)$
	$O(1)$	$\lvert x\rvert + O(1)$	$O(T + \lvert f\rvert)$
	$\lvert f\rvert + O(1)$	$\lvert x\rvert + O(1)$	$O(T)$ ✗

（适应性安全，基于电路 FE）

时空开销可互换

[Luo22] 证明了
$|\mathrm{ct}| \cdot T_{\mathrm{Dec}} = \Omega(|x|)$

目前的知识边界：(PH-)FE

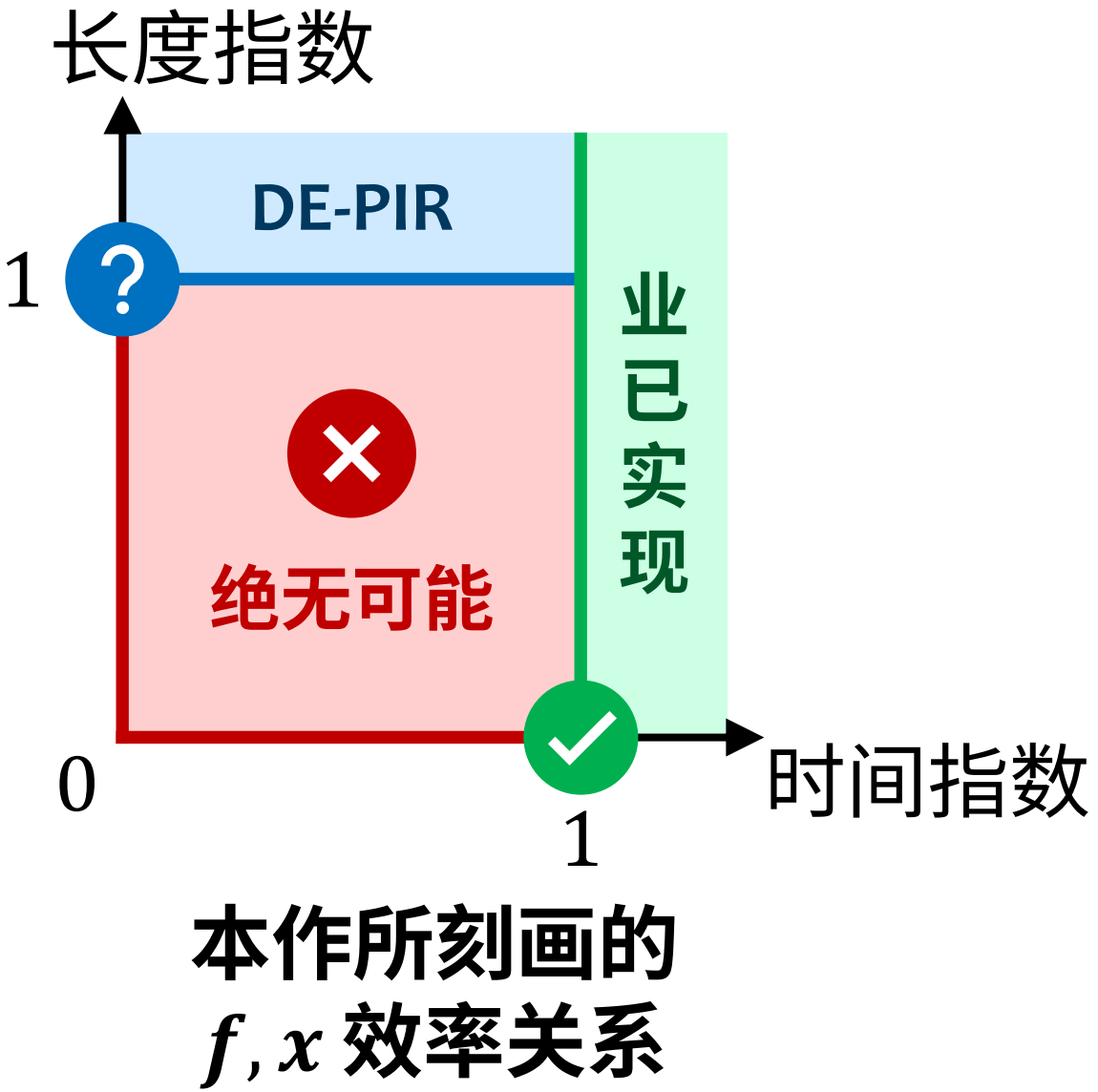
与 y 无关的 Dec

⇑

基本上

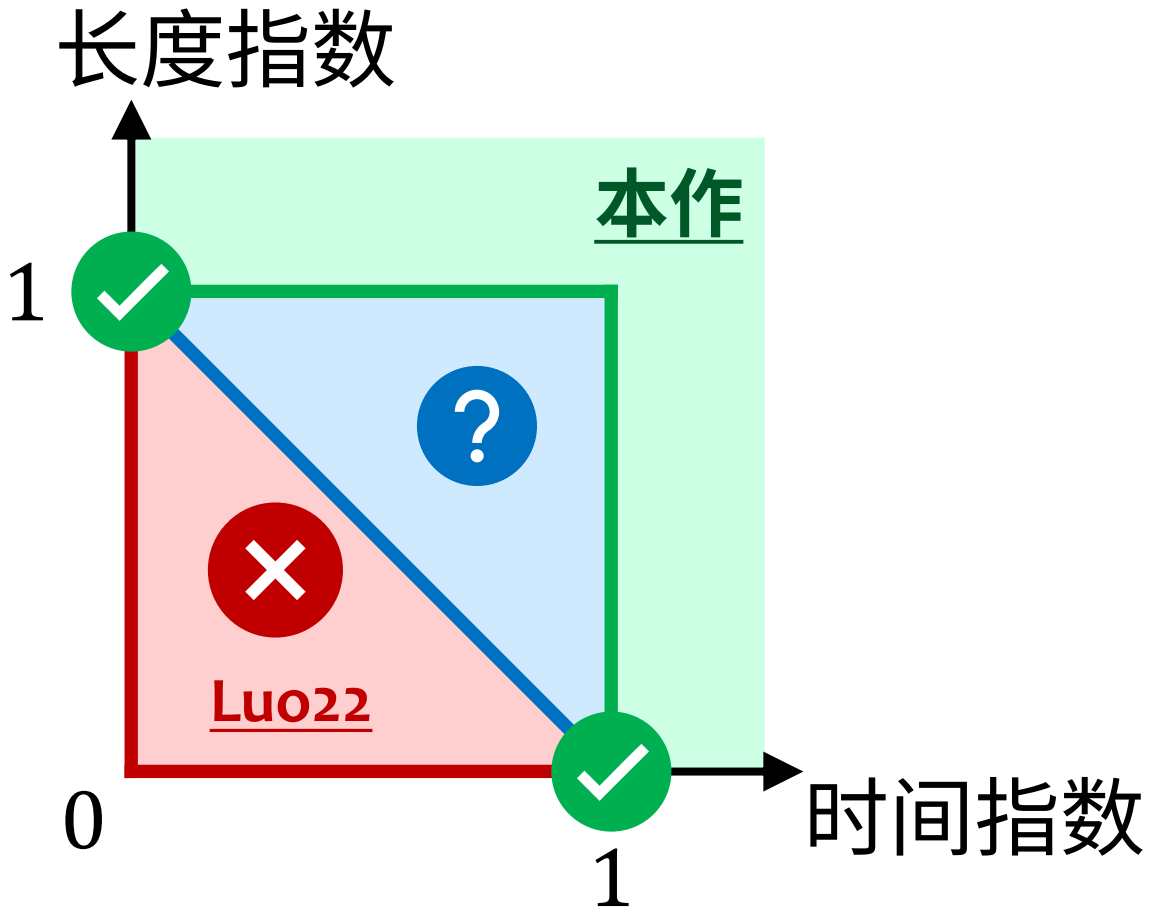
⇓

DE-PIR



本作所刻画的
f, x 效率关系

目前的知识边界：ABE



$T_{\mathrm{Dec}} = \mathrm{O}(T + \cdots)$ 中 f, x 的效率关系

休息，
休息一会儿！

画面上缺少两个形象，是什么？
答案：一休、晴天娃娃.

报告大纲（回顾）

- 偏泛函加密　　定义、目标
- 动机、问题
- 成果介绍

- 必要之繁　　时空效率下界证明一瞥
- 技巧匮乏　　与 DE-PIR 的联系
- 偏泛函加密　　定义细节
- 核心工具　　凝练乱码 RAM
- 未解问题

时空权衡下界证明一瞥：参数设置

$|\mathrm{sk}_f| = |f|^A,$ $T_{\mathrm{Dec}} = T + |f|^B + |x| + |y|,$ $A, B < 1.$

$= N^A \ll n$ $= n + N^B + 0 + n \approx n \ll N$

令 $N^A, N^B \ll n \ll N$

$I \subseteq [N]$ 是 n 个下标 $w \in \{0,1\}^n$

$f = R \in \{0,1\}^N,$ $x = \perp,$ $y_0 = (I, w),$ $y_1 = z.$

$z \in \{0,1\}^n$

$$f\ (x, y) = \begin{cases} R[I] \oplus w, & y = (I, w); \\ z, & y = z. \end{cases}$$

时空权衡下界证明一瞥：直观想法（情况一）

$|\mathrm{sk}_f| \ll n,$ $T_{\mathrm{Dec}} \ll N.$

运行 $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ 时
解密算法大量读取 $R[I]$ 吗?

若加密的是 $y = y_0 = (I, w)$：

运行 $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct}) \oplus w$ 会得到 $R[I]$，这有 n 位信息
但 $\mathrm{sk}_f, \mathrm{ct}, w$ 只含 $|\mathrm{sk}_f| \ll n$ 位（很少）关于 $R[I]$ 的信息
解密算法必须**大量读取** $R[I]$

$$f_R(x, y) = \begin{cases} R[I] \oplus w, & y = y_0 = (I, w); \\ z, & y = y_1 = z. \end{cases}$$

选择随机的 I, w
并令 $z = R[I] \oplus w$

时空权衡下界证明一瞥：直观想法（情况二）

$|\mathrm{sk}_f| \ll n,$ $T_{\mathrm{Dec}} \ll N.$

运行 $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ 时
解密算法大量读取 $R[I]$ 吗？

若加密的是 $y = y_1 = z$：

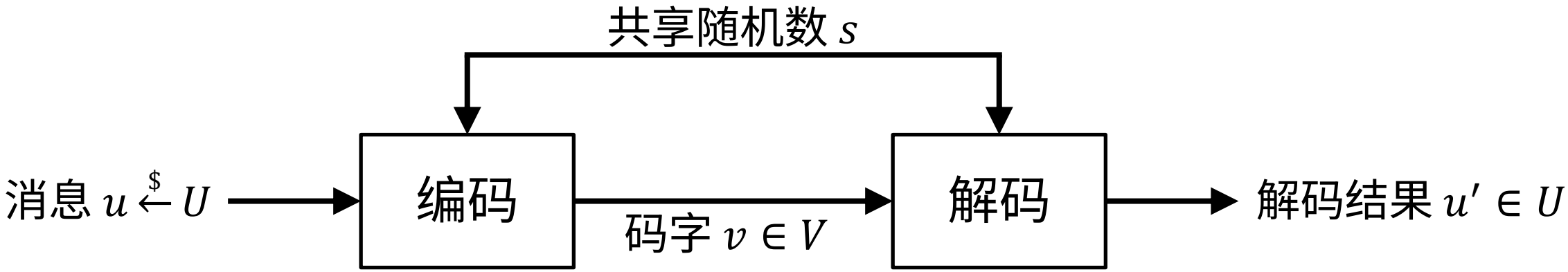
注意 I 在 $R, \mathrm{sk}_f, \mathrm{ct}$ 里**只出现**在明文 $z = R[I] \oplus w$ 中
一次性密钥 w 完美掩盖了 I
所以 $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ 的行为和 I 独立
由于时间限制，最多读取 R 中的 $T_{\mathrm{Dec}} \ll N$ 位
因此大部分 $R[I]$ 都**没读取**（不放回抽样、超几何分布）

根据解密算法读取 $R[I]$ 的多少区分！

$$f_R(x, y) = \begin{cases} R[I] \oplus w, & y = y_0 = (I, w); \\ z, & y = y_1 = z. \end{cases}$$

选择随机的 I, w
并令 $z = R[I] \oplus w$

证明工具：信息不可压缩



“编码长度不能小于消息长度”的定量版本

引理. 若 $\log_2|V| \leq -\lambda + \log_2|U|$ 则

$$\Pr_{\substack{u \xleftarrow{\$} U \\ s \xleftarrow{\$} S}} [D(E(u,s),s) = u] \leq 2^{-\lambda}.$$

compression argument

时空权衡下界证明一瞥：压缩论证（情况一）

回顾. $f_R(I,w) = R[I] \oplus w$

- sk 与 $R \in \{0,1\}^N$ 关联
- ct 加密了 (I,w)，其中 $|I| = n,\ w \in \{0,1\}^n$
- $|\mathrm{sk}_f| \ll n$（暂设为定长）

欲证. $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ 以 $> 99\%$ 的概率读取 $R[I]$ 的 $\geq (n - |\mathrm{sk}_f| - 6)$ 位

反证. 假设此算法以 $\geq 1\%$ 的概率只读取 $\leq (n - |\mathrm{sk}_f| - 7)$ 位

共享随机数 $s = \big(I, w, R[\notin I],$ 密码算法所需要的随机数$\big)$

消息 $u \in \{0,1\}^n$　　编码 v 长度是 $|\mathrm{sk}_f| + (n - |\mathrm{sk}_f| - 7) = n - 7$

编码方法.

1. 令 $R[I] = u$，
   结合 s 中的 $R[\notin I]$，
   则 R 已经完全定义
2. 使用 s 中的随机数计算 $\mathrm{sk}_f, \mathrm{ct}$
3. 把 sk_f 作为 v 的第一部分
4. 运行 $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$，每次算法
   读取 $R[I]$ 中新的一位时，
   把这一位放入 v 的第二部分
5. 在尾部填充或截断 v 使
   它的长度恰好是 $(n-7)$ 位

compression argument

时空权衡下界证明一瞥：压缩论证（续）

回顾. $f_R(I,w) = R[I] \oplus w$

- sk 与 $R \in \{0,1\}^N$ 关联
- ct 加密了 (I,w)，其中 $|I| = n,\ w \in \{0,1\}^n$
- $|\mathrm{sk}_f| \ll n$（暂设为定长）

欲证. $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ 以 $> 99\%$ 的概率读取 $R[I]$ 的 $\geq (n - |\mathrm{sk}_f| - 6)$ 位

反证. 假设此算法以 $\geq 1\%$ 的概率只读取 $\leq (n - |\mathrm{sk}_f| - 7)$ 位

共享随机数 $s = (I, w, R[\notin I],$ 密码算法所需要的随机数$)$

消息 $u \in \{0,1\}^n$　　编码 $v = (\mathrm{sk}_f,$ 解密所读取 $R[I]$ 的部分$) \in \{0,1\}^{n-7}$

解码方法.

1. 使用 s 中的随机数重新计算 ct
2. 从 s 读取 w，从 v 读取 sk_f
3. 运行 $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$，
   读取 R 的处理见右侧
   i. $R[\notin I]$ 从 s 中读取
   ii. $R[I]$ 中新的一位从 v 中读取
   iii. $R[I]$ 重复读取时不必“消耗” v
4. 解密结果记作 z，输出 $z \oplus w$

读取 $\leq (n - |\mathrm{sk}_f| - 7)$ 位 $\implies$ v 未曾截断 $\implies$ 解码结果是 $(R[I] \oplus w) \oplus w = u$

compression argument

时空权衡下界证明一瞥：压缩论证（完）

回顾. $f_R(I,w) = R[I] \oplus w$

- sk 与 $R \in \{0,1\}^N$ 关联
- ct 加密了 (I,w)，其中 $|I| = n,\ w \in \{0,1\}^n$
- $|\mathrm{sk}_f| \ll n$（暂设为定长）

欲证. $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ 以 $> 99\%$ 的概率读取 $R[I]$ 的 $\geq (n - |\mathrm{sk}_f| - 6)$ 位

反证. 假设此算法以 $\geq 1\%$ 的概率只读取 $\leq (n - |\mathrm{sk}_f| - 7)$ 位

共享随机数 $s = (I, w, R[\notin I],$ 密码算法所需要的随机数$)$

消息 $u \in \{0,1\}^n$　　编码 $v = (\mathrm{sk}_f,$ 解密所读取 $R[I]$ 的部分$) \in \{0,1\}^{n-7}$

引理表明

$$\frac{1}{128} = 2^{-7} \geq \Pr[\text{正确解码}] \geq \Pr[\text{读取} \leq (n - |\mathrm{sk}_f| - 7) \text{ 位}] \geq 0.01 = \frac{1}{100}.$$

读取 $\leq (n - |\mathrm{sk}_f| - 7)$ 位 $\implies$ v 未曾截断 $\implies$ 解码结果是 $(R[I] \oplus w) \oplus w = u$

时空权衡下界证明一瞥：论证收尾

$|\mathrm{sk}_f| \ll n,$ $\quad\quad$ $T_{\mathrm{Dec}} \ll N.$

若加密的是 $y = y_0 = (I, w)$：

$$\Pr[\text{读取} \geq n/2] \geq \Pr[\text{读取} \geq (n - |\mathrm{sk}_f| - 6)] > 99\%$$

若加密的是 $y = y_1 = z$：

$$\mathbb{E}[\text{读取}] \leq \frac{|I| \cdot T_{\mathrm{Dec}}}{N} \leq \frac{n}{200}$$，由 Markov 不等式

$$\Pr[\text{读取} \geq n/2] \leq \frac{1/200}{1/2} = 1\%$$

时空权衡下界证明一瞥：结论

$$|\mathrm{sk}_f| = |f|^A, \qquad T_{\mathrm{Dec}} = T + |f|^B + |x| + |y|, \qquad A, B < 1.$$

这样的 (PH-)FE 不可能安全！

最速解密蕴涵 DE-PIR

$$|\mathrm{sk}_f| = |f|^A, \qquad T_{\mathrm{Dec}} = |f|^B \,\mathrm{poly}(T, |x|, |y|), \qquad B < 1.$$

$$f = D, \qquad x = \perp, \qquad y = i, \qquad f_D(x, y) = D[i].$$

预处理. $\widetilde{D} = (D, \mathrm{fesk}_f), \qquad k = \mathrm{fempk}.$

$$|\widetilde{D}| = |D| + |D|^A$$

查询. $\mathrm{ct} = \mathrm{fect}(i)$. $\qquad T_{\mathrm{Query}} = \mathrm{O}(1)$

答复. $\mathrm{Dec}^D(\mathrm{fesk}_f, \mathrm{fect})$. $\qquad T_{\mathrm{Resp}} = |D|^B$

⚠ 不可区分安全性、选择性安全、不隐藏查询结果、（私钥方案）不隐藏数据库

✓ 选择性安全蕴含着适应性安全
保高效的一般变换：模拟安全性、隐藏查询结果、（私钥方案）隐藏数据库

保高效的一般变换

隐藏查询结果（查两次）

要处理数据库 D（长度 n），去处理 $D' = D\overline{D}$

查询 $D[i]$ 时随机选一种：

- 先查询 $D'[i]$ 再查询 $D'[n+i]$
- 先查询 $D'[n+i]$ 再查询 $D'[i]$

查询结果等概率为 01 或 10

收到回复后保留 $D'[i]$ 即可

查询结果隐藏时，不可区分安全性蕴含着模拟安全性

隐藏数据库（加密）

要处理 D：

- 生成 PRF 密钥 k_{PRF}
- 去处理 $D' = D \oplus \mathrm{PRF}(k_{\mathrm{PRF}}, \cdots)$
- 把 k_{PRF} 放入 DE-PIR 客户端私钥 k 中

查询 $D[i]$ 时查询 $D'[i]$

收到回复后计算 $D[i] = D'[i] \oplus \mathrm{PRF}(k_{\mathrm{PRF}}, i)$

为什么在“外部”变换
而不直接用 (PH-)FE “内部”实现？
为了让证明所需要的 (PH-)FE **尽可能弱**.

制造密码学对象的三个步骤

1. 给它下恰当的定义
2. 用合适的工具构造它
3. 证明这一构造正确且安全

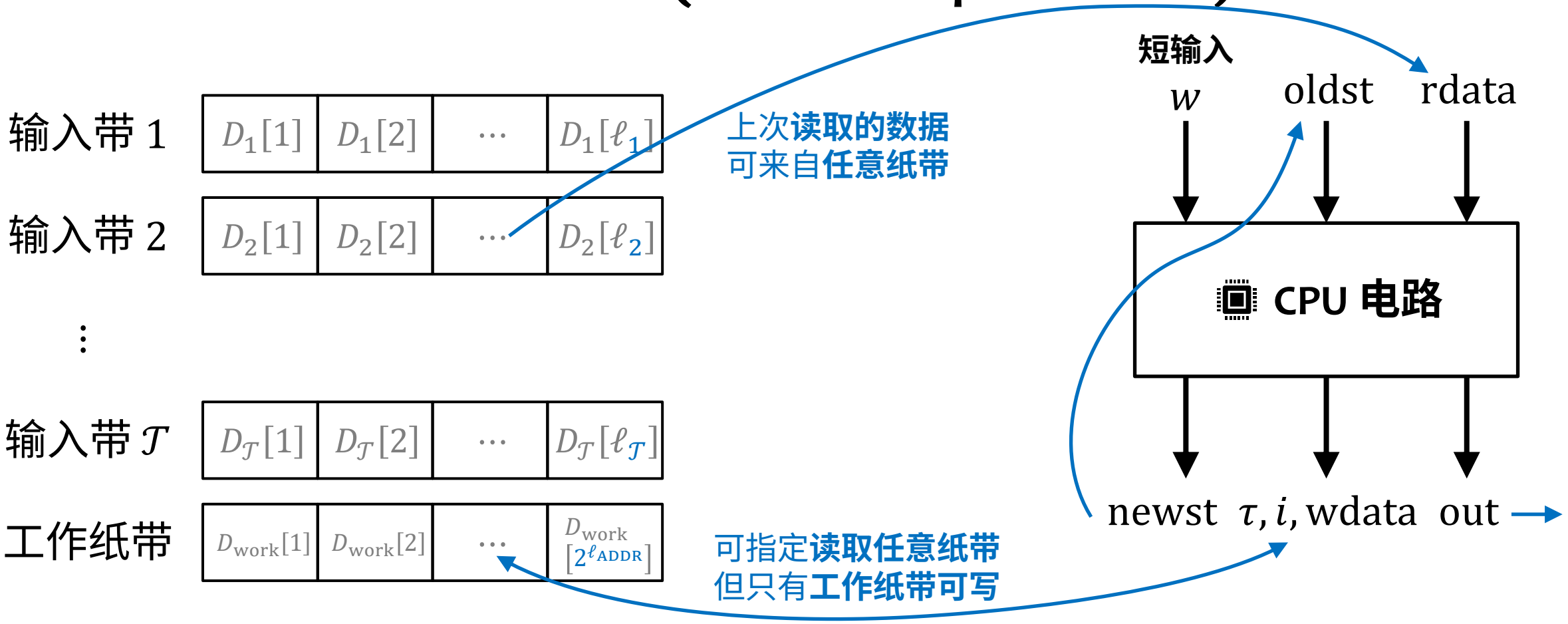
要把大象装冰箱，总共分几步？

要把长颈鹿装冰箱，总共分几步？

发明和使用工具的四个步骤

1. 根据需求给工具下恰当的定义
2. 用合适的底层工具构造它
3. 证明这一构造正确且安全
4. 用工具构造产品

多重纸带随机访问机 (multi-tape RAM)



$M^{D_1,\ldots,D_{\mathcal{T}}}(w)$ 的输出序列 $\text{outS}(M, D_1, \ldots, D_{\mathcal{T}}, w) = (\text{out}_1, \ldots, \text{out}_{T-1})$

偏泛函加密：准确定义

适用于 $\Phi = \{\varphi: F_\varphi \times X_\varphi \times Y_\varphi \to \{\perp\} \cup (\mathbb{N}_+ \times Z_\varphi)\}$ 的偏泛函加密

- $\varphi(f, x, y) = (T, z)$ 表示计算时间是 T 且输出是 z
- $\varphi(f, x, y) = \perp$ 表示计算不作定义

排除不停机的情况

T 代表“无密码学参与”时的计算时间，可作为 T_{Dec} 和安全定义可证伪性的基准

算法.

- $\mathrm{Setup}(\varphi \in \Phi) \to (\mathrm{mpk}, \mathrm{msk})$
- $\mathrm{KeyGen}(\mathrm{msk}, f \in F_\varphi) \to \mathrm{sk}_f$
- $\mathrm{Enc}(\mathrm{mpk}, x \in X_\varphi, y \in Y_\varphi) \to \mathrm{ct}_x$
- $\mathrm{Dec}^{\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x}() \to z'$

可进一步加强定义，如本作实现的是 $(T + |f| + |x| + |y|)\,\mathrm{poly}(|\varphi|)$

正确性. 若 $\varphi(f, x, y) = (T, z)$ 则 $z = z'$ 且 Dec 在 $\mathrm{poly}(|\varphi|, |f|, |x|, |y|, T)$ 步内停机

偏泛函加密：准确定义（续）

适用于 $\Phi = \{\varphi: F_\varphi \times X_\varphi \times Y_\varphi \to \{\perp\} \cup (\mathbb{N}_+ \times Z_\varphi)\}$ 的偏泛函加密

- $\varphi(f, x, y) = (T, z)$ 表示计算时间是 T 且输出是 z
- $\varphi(f, x, y) = \perp$ 表示计算不作定义

排除不停机的情况

T 代表“无密码学参与”时的计算时间，可作为 T_{Dec} 和**安全定义可证伪性**的基准

falsifiability

算法.

- $\mathrm{Setup}(\varphi \in \Phi) \to (\mathrm{mpk}, \mathrm{msk})$
- $\mathrm{KeyGen}(\mathrm{msk}, f \in F_\varphi) \to \mathrm{sk}_f$
- $\mathrm{Enc}(\mathrm{mpk}, x \in X_\varphi, y \in Y_\varphi) \to \mathrm{ct}_x$
- $\mathrm{Dec}^{\mathrm{mpk}, f, \mathrm{sk}_f, x, \mathrm{ct}_x}() \to z'$

确保运算时间是多项式级别

——高效验证“**无法通过既定功能区分**”的约束

安全性. 要求使坏者额外输出 $1^{\bar{T}}$，且选择的 $\varphi, \{f_q\}_q, x, y_0, y_1$ 满足

$$\varphi(f_q, x, y_0) = \varphi(f_q, x, y_1) = (T_q, z_q) \neq \perp \text{ 且 } T_q \leq \bar{T}$$

偏泛函加密：适用于 RAM 的 PHFE

令

$$\varphi_{M,T_{\max}}(f,x,y) = \begin{cases} (T, \mathrm{outS}(M,f,xy,\varepsilon)), & \text{若 } T = \mathrm{time}(M,f,xy,\varepsilon) \le T_{\max}; \\ \perp, & \text{其他情况.} \end{cases}$$

实际使用时 M 应选为**通用 RAM**（universal RAM）并令 $T_{\max} = 2^{\lambda}$

（f 理解为汇编代码而 xy 理解为输入）

其中

- M 可以取任何**双**输入纸带、**无短输入**的 RAM
- $T_{\max}$ 可以取任何正整数

且 $\varphi_{M,T_{\max}}$ 的描述长度是 $(|M| + \lceil \log_2 T_{\max} \rceil)$

对定义的**形式化可行性**、
实现**短密钥短密文**至关重要

偏泛函加密：电路 FE（工具）

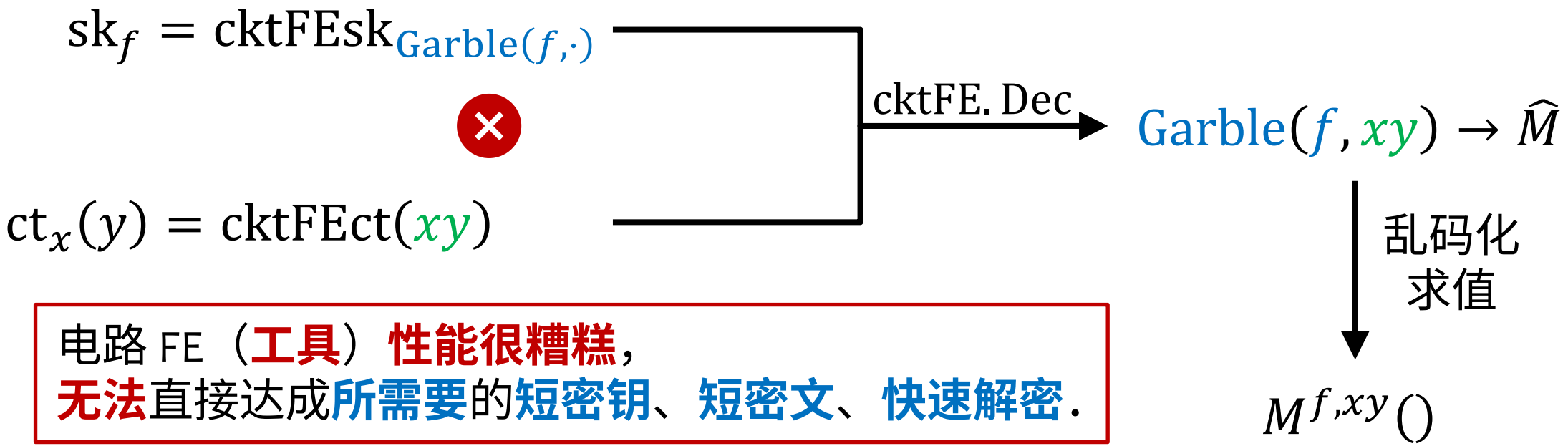
令

$$\varphi_{\ell,s}(f,x,y) = \begin{cases} (1, f(y)), & f \text{ 是输入长度为 } \ell \text{ 规模为 } s \text{ 的电路且 } x = \perp, y \in \{0,1\}^{\ell}; \\ \perp, & \text{其他情况.} \end{cases}$$

其中 $s \geq \ell$ 可取任何正整数且 $\varphi_{\ell,s}$ 的描述长度是 $(\ell + s)$

所有算法都可以有
关于 ℓ, s **任意糟糕的多项式**复杂度

RAM 乱码化 (garbling) + 电路 FE $\Longrightarrow$ 适用于 RAM 的 PHFE



电路 FE（**工具**）**性能很糟糕**，
无法直接达成**所需要**的**短密钥**、**短密文**、**快速解密**.

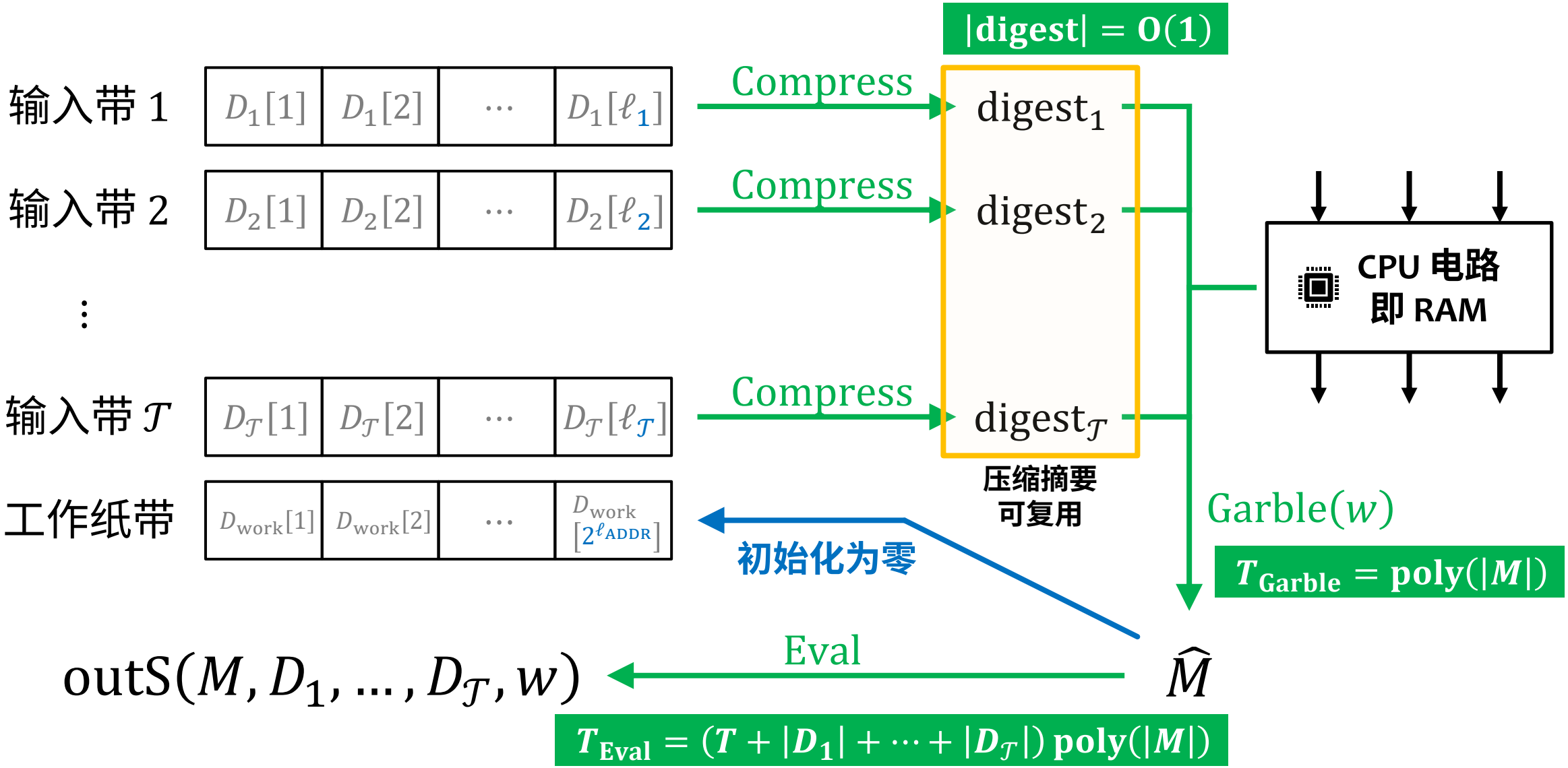
寻求 RAM 乱码化算法恰当的定义
——无需依赖电路 FE 性能

laconic garbled RAM

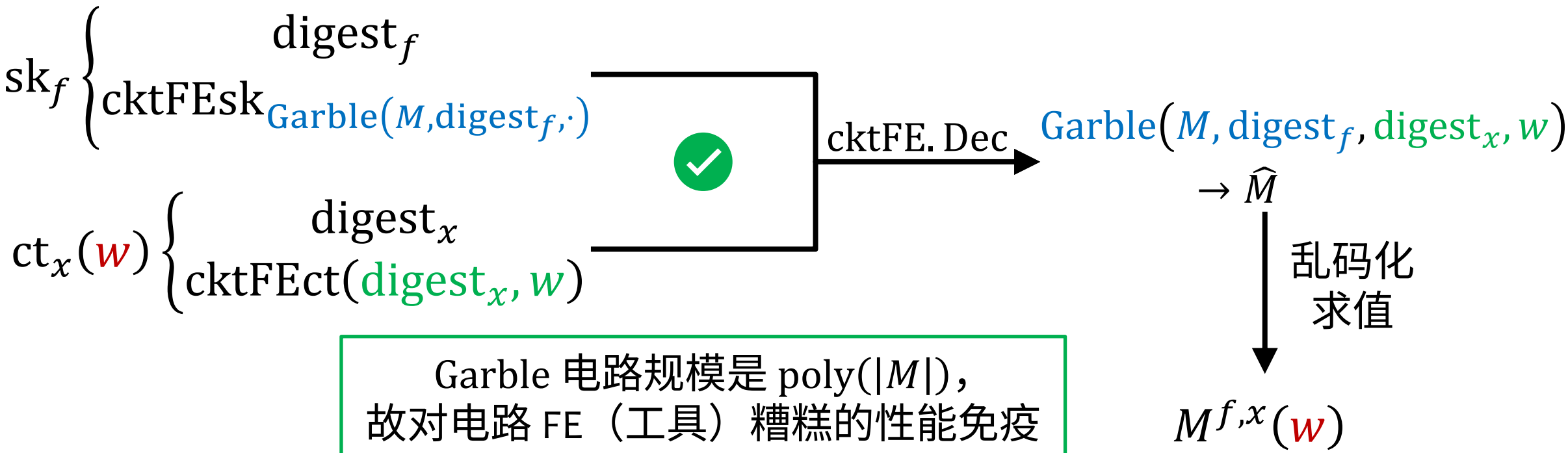
核心工具：凝练乱码 RAM

考虑不可区分安全性
（不考虑模拟安全性）

对效率至关重要！



凝练乱码 RAM + 电路 FE



Garble 电路规模是 $\mathrm{poly}(|M|)$，
故对电路 FE（工具）糟糕的性能免疫

? y 呢？w 很短且与 w 相关的性能参数很差

用 w 加密 y，密文放入 x，RAM 内解密计算
需要用 [NY] 双加密法（y 码率为 2 的源头）

未解问题：(PH-)FE、ABE 路在何方？

1. 构造**最速解密**的 PHFE 以及（或者仅利用）DE-PIR 的效率理想型.

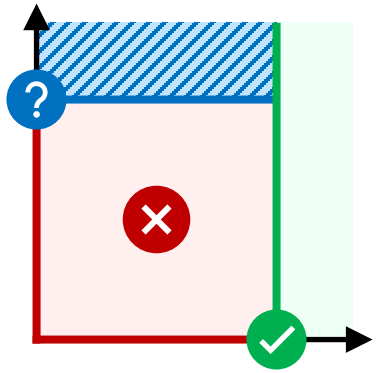
2. 达成 y **码率为 1** 和适应性安全、无限制输出长度（之一）.

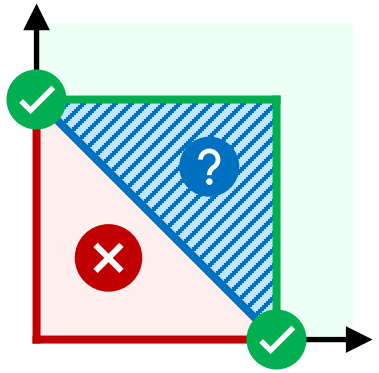
3. 探究最速解密和 DE-PIR 类型之间的**紧关系**.

   电路 FE + **公**钥 DE-PIR $\Longrightarrow$ (x, y)-最速解密 $\Longrightarrow$ **私**钥 DE-PIR.[ACFQ]
   电路 FE + **私**钥 DE-PIR $\Longrightarrow$ ...？

4. 完全刻画它们的 **Pareto 效率前沿**.

   即解答**阴影区域**的情况.





谢谢！

ia.cr/2022/1317（修订在即）

哔哩哔哩 BV1qs4y1Q7G9

luoji@cs.washington.edu / luoji.bio