Quel est le prix du chiffrement fonctionnel ?

On the Optimal Succinctness and Efficiency of Functional Encryption and Attribute-Based Encryption

Aayush Jain

Carnegie Mellon University

Rachel Lin

罗辑 (Ji Luo)

UNIVERSITY of WASHINGTON

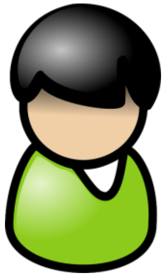
Partially Hiding Functional Encryption

$\mathsf{Setup} \rightarrow \mathsf{mpk}, \mathsf{msk}$

Partially Hiding Functional Encryption

Setup $\rightarrow$ mpk, msk

mpk



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

public/private inputs

Partially Hiding Functional Encryption

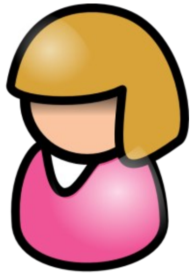
$\mathrm{Setup} \to \mathrm{mpk}, \mathrm{msk}$

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

function

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

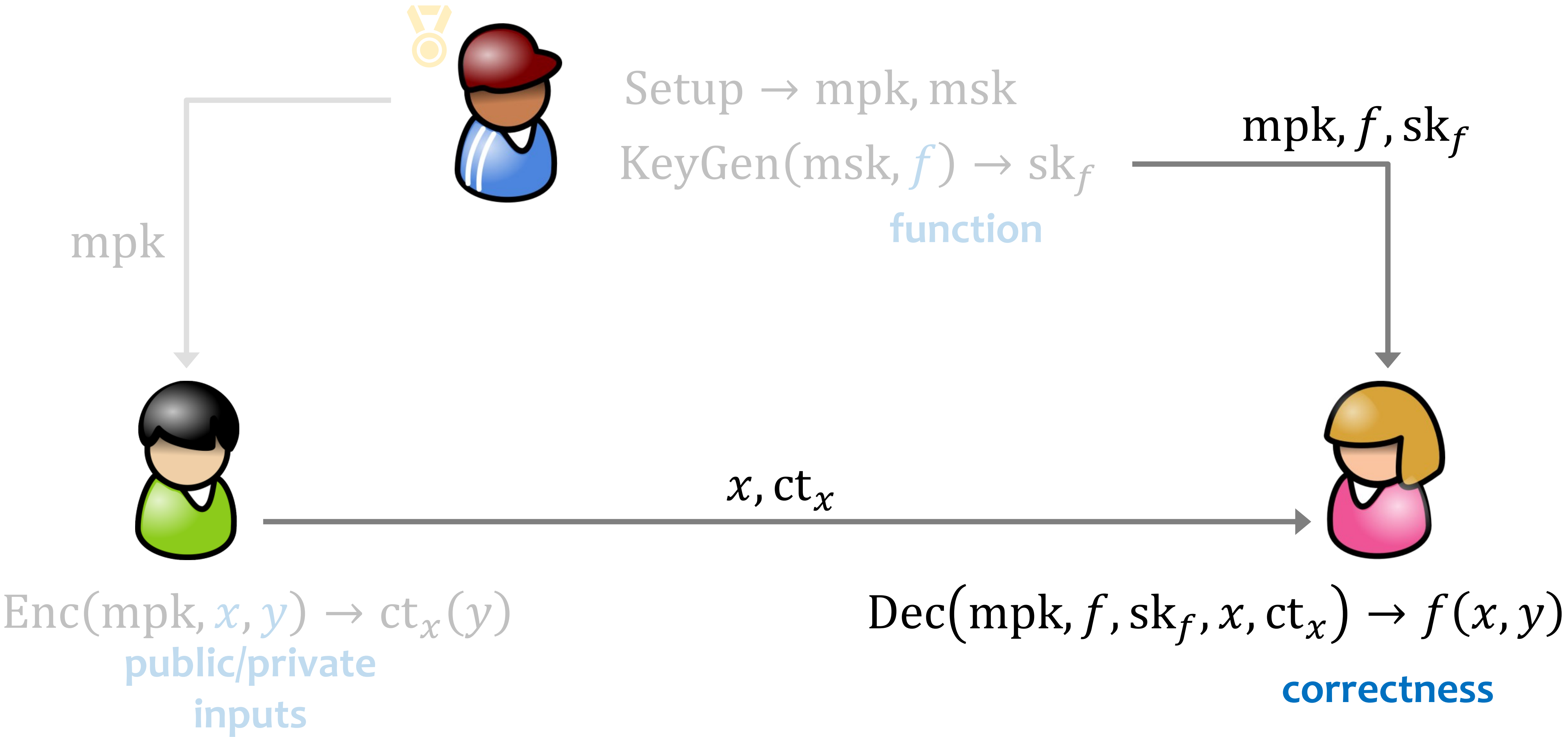
mpk



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

public/private inputs

Partially Hiding Functional Encryption



Partially Hiding Functional Encryption

Setup $\rightarrow$ mpk, msk

KeyGen(msk, f) $\rightarrow$ sk_f

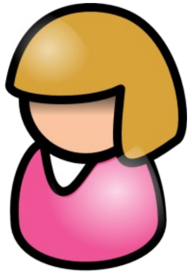
function

mpk

mpk, f, sk_f

f, x are always provided in the clear.

x, ct_x



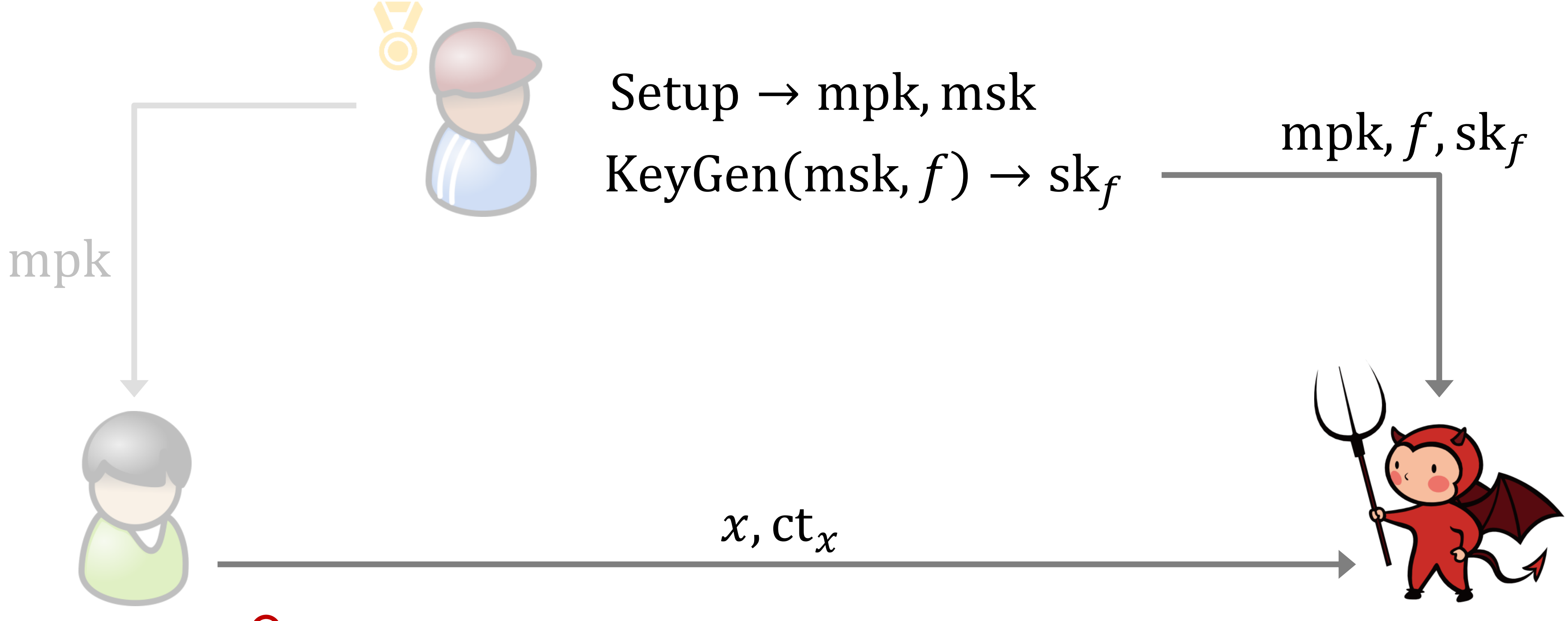
Enc(mpk, x, y) $\rightarrow$ $\mathrm{ct}_x(y)$

public/private inputs

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

correctness

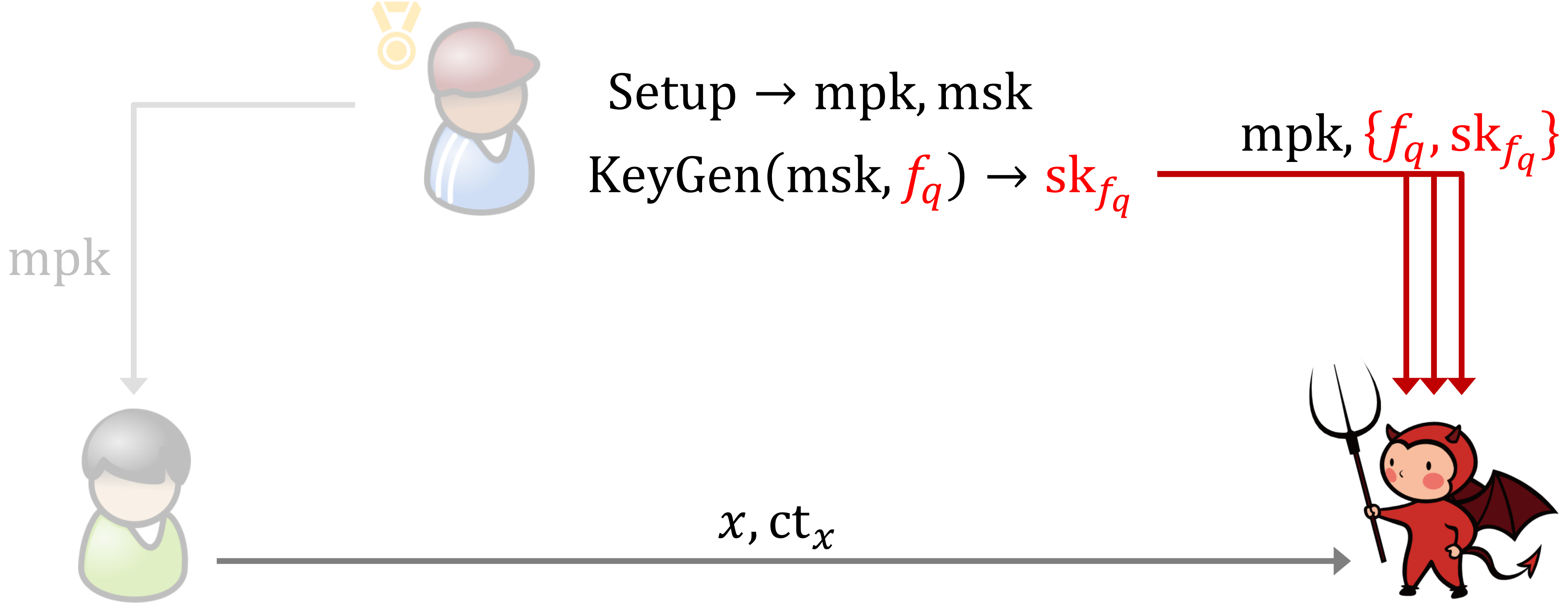
PHFE Security



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

Security. Hides all information about y beyond $f(x, y)$.

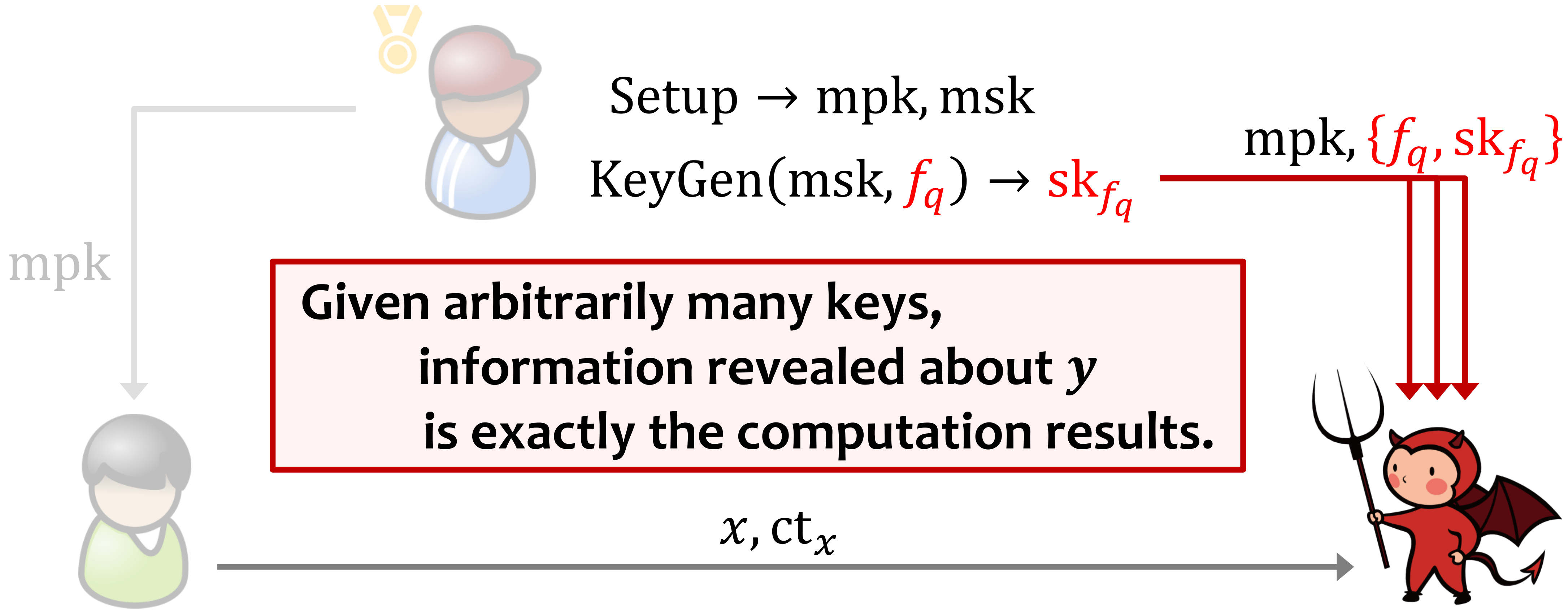
PHFE Security: Collusion Resistance



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

Security. Hides all information about y beyond $\{f_q(x, y)\}$.

PHFE Security: Collusion Resistance



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

Security. Hides all information about y beyond $\{f_q(x, y)\}$.

PHFE Security: **IND-CPA**

$\mathrm{Exp}^{b}_{\mathrm{PHFE}}$

PHFE Security: **IND-CPA**

$$\xrightarrow{\mathrm{mpk}}$$

$\mathrm{Exp}^{b}_{\mathrm{PHFE}}$

PHFE Security: **IND-CPA**

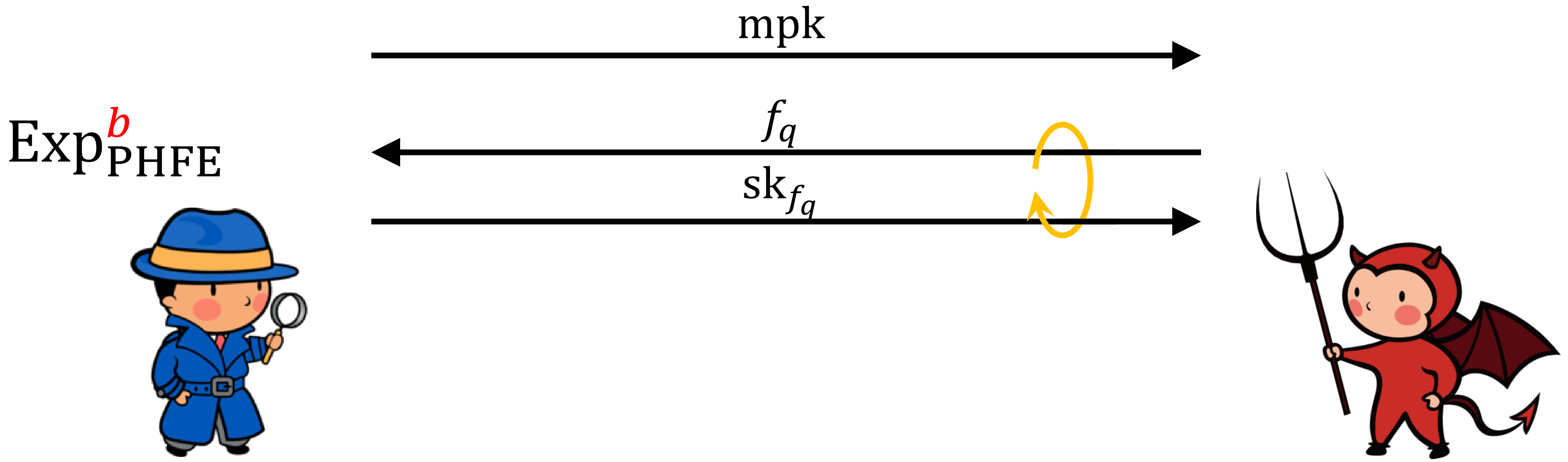
$\mathrm{Exp}^{b}_{\mathrm{PHFE}}$

$\xrightarrow{\mathrm{mpk}}$

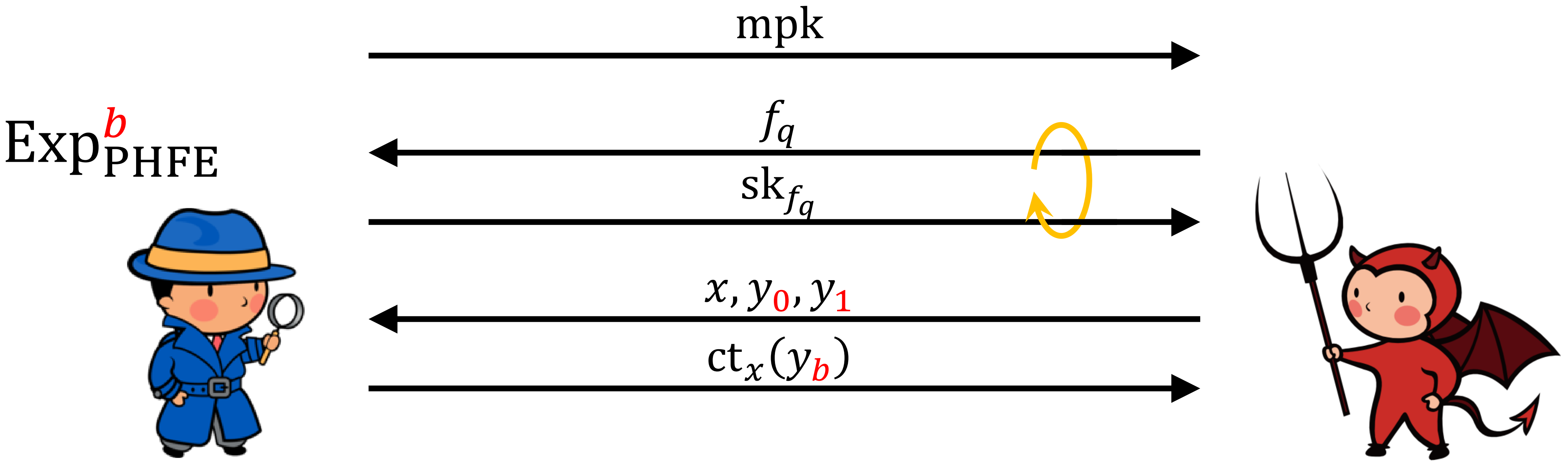
$\xleftarrow{f_q}$

$\xrightarrow{\mathrm{sk}_{f_q}}$

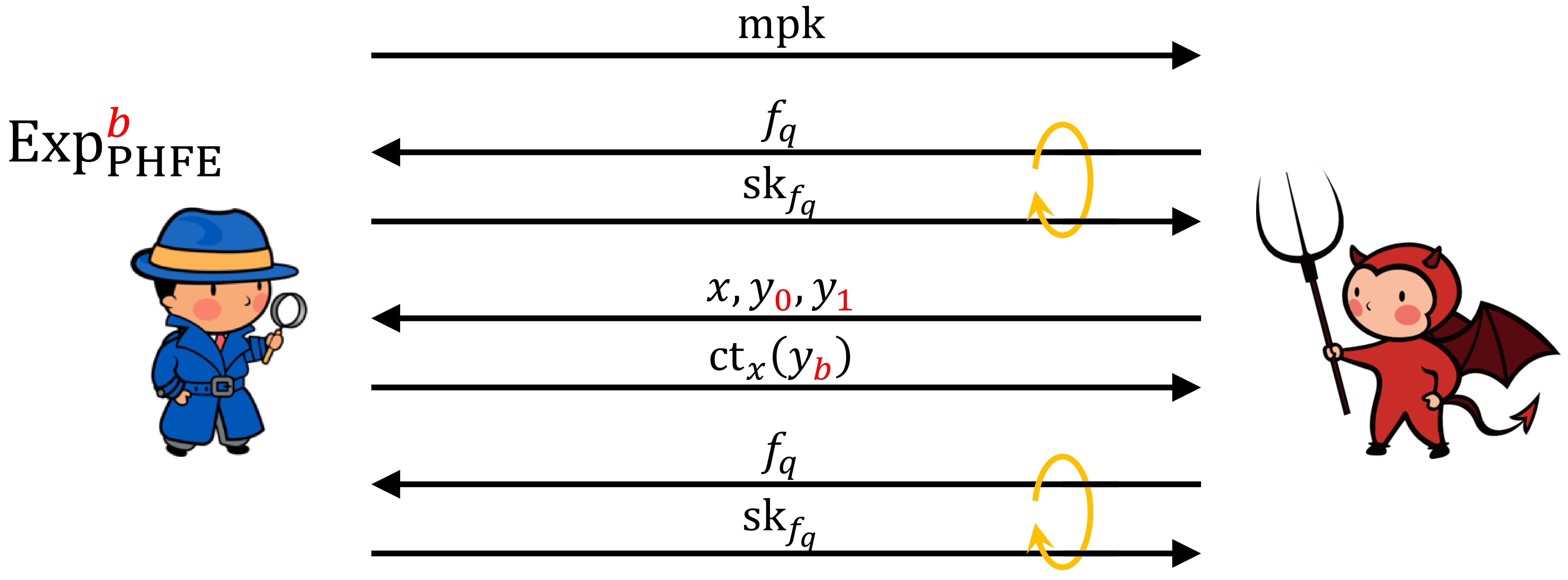
PHFE Security: **IND-CPA**



PHFE Security: **IND-CPA**



PHFE Security: **IND-CPA**



PHFE Security: IND-CPA

$\mathrm{Exp}^{b}_{\mathrm{PHFE}}$

$\xrightarrow{\mathrm{mpk}}$

$\xleftarrow{f_q}$

$\xrightarrow{\mathrm{sk}_{f_q}}$

$\xleftarrow{x, y_0, y_1}$

$\xrightarrow{\mathrm{ct}_x(y_b)}$

$\xleftarrow{f_q}$

$\xrightarrow{\mathrm{sk}_{f_q}}$

$\mathrm{Exp}^{0}_{\mathrm{PHFE}} \approx \mathrm{Exp}^{1}_{\mathrm{PHFE}}$ **if** $|y_0| = |y_1|$ **and** $\forall q\colon f_q(x, y_0) = f_q(x, y_1)$

What do we want for a PHFE?

★ expressive functionality

What do we want for a PHFE?

- ★ expressive functionality
- ★ short keys / ciphertexts
- ★ fast decryption

What do we want for a PHFE?

- ★ expressive functionality

  supports **RAM** computation
  with **unbounded output length**

- ★ short keys / ciphertexts

- ★ fast decryption

What do we want for a PHFE?

- ★ expressive functionality

  supports **RAM** computation with **unbounded output length**

- ★ short keys / ciphertexts

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

- ★ fast decryption

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

What do we want for a PHFE?

- ★ expressive functionality

  supports **RAM** computation with **unbounded output length**

- ★ short keys / ciphertexts

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

- ★ fast decryption

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

What do we want for a PHFE? (continued)

★ expressive functionality

supports **RAM** computation with **unbounded output length**

★ short keys / ciphertexts

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

ideal

★ fast decryption

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

ideal

What do we want for a PHFE? (continued)

★ expressive functionality

supports **RAM** computation
with **unbounded output length**

★ short keys / ciphertexts

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

ideal

★ fast decryption

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

ideal

★ adaptive security & minimal assumption

What do we want for a PHFE? (continued)

★ expressive functionality

supports **RAM computation**
with **unbounded output length**

★ short keys / ciphertexts

$$|\mathsf{sk}_f| = O(1)$$
$$|\mathsf{ct}_x(y)| = |y| + O(1)$$

ideal

★ fast decryption

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

ideal

★ adaptive security & minimal assumption

Motivation / Questions

Motivation / Questions

What is the **best-possible efficiency** of PHFE?

Motivation / Questions

What is the **best-possible efficiency** of PHFE?

Are there **trade-offs** among different aspects of efficiency?

Motivation / Questions

What is the **best-possible efficiency** of PHFE?

Are there **trade-offs** among
different aspects of efficiency?

(From what assumptions)
Can we **construct** optimally efficient PHFE?

Our Results: **Nearly Optimal PHFE for RAM**

polynomially secure FE for circuits

$\Longrightarrow$ **adaptively secure PHFE for RAM with**

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

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

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

Our Results: **Nearly Optimal PHFE for RAM**

(weakly selective 1-key FE with $T_{\mathrm{Enc}}=|f|^{1-\varepsilon}$ for circuits)
"obfuscation-minimum" FE [long line of prior works]

$\Longrightarrow$ **polynomially secure FE for circuits**

$\Longrightarrow$ **adaptively secure PHFE for RAM with**

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

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

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

Our Results: **Nearly Optimal PHFE for RAM**

(weakly selective 1-key FE with $T_{\mathsf{Enc}}=|f|^{1-\varepsilon}$ for circuits)
"obfuscation-minimum" FE [long line of prior works]

$\Longrightarrow$ **polynomially secure FE for circuits**

$\Longrightarrow$ **adaptively secure PHFE for RAM with**

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

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

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

Our Results: **Nearly Optimal PHFE for RAM**

(weakly selective 1-key FE with $T_{\mathrm{Enc}}=|f|^{1-\varepsilon}$ for circuits)
"obfuscation-minimum" FE [long line of prior works]

$\Longrightarrow$ **polynomially secure FE for circuits**

$\Longrightarrow$ **adaptively secure PHFE for RAM with**

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

?

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

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

?

necessary / barrier

Select Related Works on FE

for	adaptive	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	assumptions
RAM long output	this ✓	$O(1)$	$2\lvert y\rvert + O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert + \lvert y\rvert)$	FE

Select Related Works on FE

for	adaptive	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	assumptions
RAM long output	**this** ✓	$O(1)$	$2\lvert y \rvert + O(1)$	$O(T + \lvert f \rvert + \lvert x \rvert + \lvert y \rvert)$	**FE**
RAM	ACFQ	$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert)$	PK-DE-PIR + FE

Select Related Works on FE

for		adaptive	$\lvert\mathrm{sk}_f\rvert$	$\lvert\mathrm{ct}_x(y)\rvert$	T_{Dec}	assumptions
RAM long output	**this**	✓	$O(1)$	$2\lvert y\rvert + O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert + \lvert y\rvert)$	**FE**
RAM	ACFQ		$\mathrm{poly}(\lvert f\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert)$	PK-DE-PIR + FE
TM	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

Select Related Works on FE

for		adaptive	$\lvert\mathrm{sk}_f\rvert$	$\lvert\mathrm{ct}_x(y)\rvert$	T_{Dec}	assumptions
RAM long output	**this**	✓	$O(1)$	$2\lvert y\rvert + O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert + \lvert y\rvert)$	**FE**
RAM	ACFQ		$\mathrm{poly}(\lvert f\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert)$	PK-DE-PIR + FE
TM	AS	✓	$\mathrm{poly}(\lvert f\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert, \lvert y\rvert)$	$i\mathcal{O}$
TM	AJS	✓	$c\lvert f\rvert + O(1)$	$c\lvert y\rvert + O(1)$	$T\,\mathrm{poly}(\lvert f\rvert, \lvert y\rvert)$	subexp $i\mathcal{O}$
TM	AM	✓	$\mathrm{poly}(\lvert f\rvert)$	$O(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert, \lvert y\rvert)$	dist. ind. FE
TM	KNTY		$\mathrm{poly}(\lvert f\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert, \lvert y\rvert)$	1-key sel. FE
circuit	GGHRSW		$\mathrm{poly}(\lvert C\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$\mathrm{poly}(\lvert C\rvert)$	$i\mathcal{O}$
circuit	KNTY	✓	$\mathrm{poly}(\lvert C\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$\mathrm{poly}(\lvert C\rvert)$	1-key sel. FE
circuit	GWZ		$\mathrm{poly}(\lvert C\rvert)$	$\lvert y\rvert + O(1)$	$\mathrm{poly}(\lvert C\rvert)$	$i\mathcal{O}$

Significant Improvement and "Two Clouds"

for		adaptive	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	assumptions
RAM long output	**this**	✓	$O(1)$	$2\lvert y \rvert + O(1)$	$O(T + \lvert f \rvert + \lvert x \rvert + \lvert y \rvert)$	**FE**
RAM	ACFQ		$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert)$	PK-DE-PIR + FE
TM	AS	✓	$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	$i\mathcal{O}$
	AJS	✓			$, \lvert y \rvert)$	subexp $i\mathcal{O}$
	AM	✓			$, \lvert y \rvert)$	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
circuit	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		$\mathrm{poly}(\lvert C \rvert)$	$\lvert y \rvert + O(1)$	$\mathrm{poly}(\lvert C \rvert)$	$i\mathcal{O}$

improvement from polynomial to *nearly optimal* efficiency

Significant Improvement and "Two Clouds"

for		adaptive	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	assumptions
RAM long output	**this**	✓	$O(1)$	$2\lvert y \rvert + O(1)$	$O(T + \lvert f \rvert + \lvert x \rvert + \lvert y \rvert)$	**FE**
RAM	ACFQ		$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert)$	PK-DE-PIR + FE
TM	AS	✓	$\mathrm{poly}(\lvert f \rvert)$	$\mathrm{poly}(\lvert y \rvert)$	$T\,\mathrm{poly}(\lvert f \rvert, \lvert y \rvert)$	$i\mathcal{O}$
	AJS	✓			$, \lvert y \rvert)$	subexp $i\mathcal{O}$
	AM	✓			$, \lvert y \rvert)$	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
circuit	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		$\mathrm{poly}(\lvert C \rvert)$	$\lvert y \rvert + O(1)$	$\mathrm{poly}(\lvert C \rvert)$	$i\mathcal{O}$

improvement from polynomial to *nearly optimal* efficiency

✓ **obtainable if abandoning adaptive security & long output**

Significant Improvement and “Two Clouds”

for		adaptive	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x(y) \rvert$	T_{Dec}	assumptions
RAM long output	**this**	✓	$O(1)$	$2\lvert y\rvert + O(1)$	$O(T + \boxed{\lvert f\rvert + \lvert x\rvert + \lvert y\rvert})$?	**FE**
RAM	ACFQ		$\mathrm{poly}(\lvert f\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert)$	PK-DE-PIR + FE
TM	AS	✓	$\mathrm{poly}(\lvert f\rvert)$	$\mathrm{poly}(\lvert y\rvert)$	$T\,\mathrm{poly}(\lvert f\rvert, \lvert y\rvert)$	$i\mathcal{O}$
	AJS	✓			$, \lvert y\rvert)$	subexp $i\mathcal{O}$
	AM	✓			$, \lvert y\rvert)$	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
circuit	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		$\mathrm{poly}(\lvert C\rvert)$	$\lvert y\rvert + O(1)$	$\mathrm{poly}(\lvert C\rvert)$	$i\mathcal{O}$

improvement from polynomial to *nearly optimal* efficiency

✓ **obtainable if abandoning adaptive security & long output**

Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

first space-time efficiency trade-offs for (PH-)FE

Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

first space-time efficiency trade-offs for (PH-)FE

For FE or PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

first space-time efficiency trade-offs for (PH-)FE

For FE or PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

For PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

first space-time efficiency trade-offs for (PH-)FE

For FE or PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

For PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

"Component size and decryption time cannot both be sublinear in f, x."

Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

first space-time efficiency trade-offs for (PH-)FE

For FE or PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

For PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

"Component size and decryption time cannot both be sublinear in f, x."

Both hold for very **selective 1-sk 1-ct secret-key** scheme (a.k.a. **garbling**) supporting **simple** functions.

Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

first space-time efficiency trade-offs for (PH-)FE

For FE or PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

For PHFE for RAM, if

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

then $A \geq 1$ or $B \geq 1$.

"Component size and decryption time cannot both be sublinear in f, x."

Both hold for very **selective 1-sk 1-ct secret-key** scheme (a.k.a. **garbling**) supporting **simple** functions.

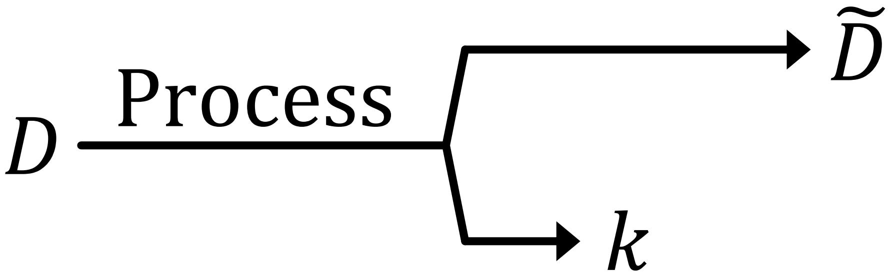
y? Linear-size components? Optimal decryption time? Connections to DE-PIR.

Doubly Efficient Private Information Retrieval

DE-PIR D

Doubly Efficient Private Information Retrieval

DE-PIR



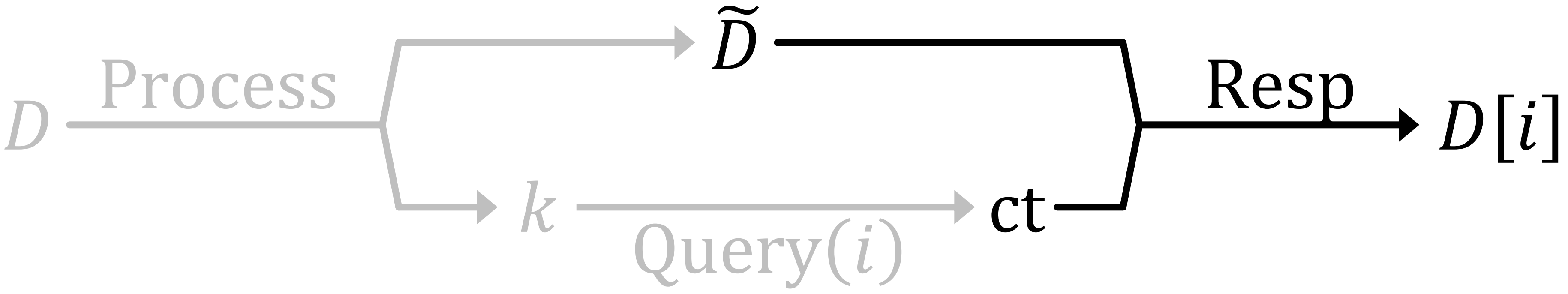
Doubly Efficient Private Information Retrieval

DE-PIR

$$D \xrightarrow{\text{Process}} \begin{cases} \widetilde{D} \\ k \xrightarrow[\text{Query}(i)]{} \text{ct} \end{cases}$$

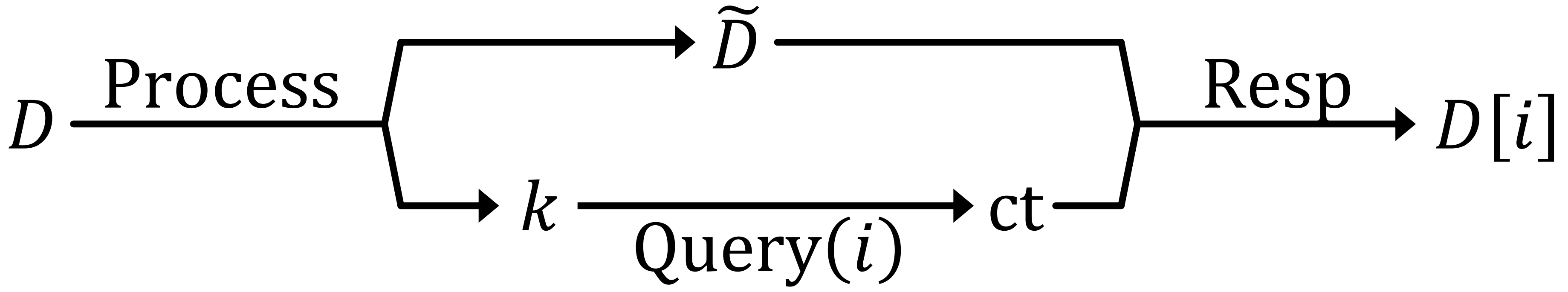
Doubly Efficient Private Information Retrieval

DE-PIR



Doubly Efficient Private Information Retrieval

DE-PIR

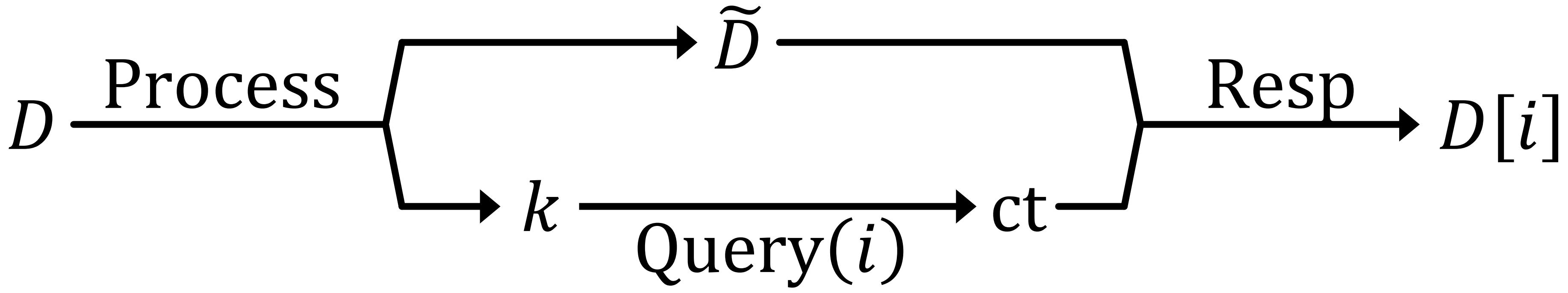


client efficiency $|k| = O(1)$ **and** $T_{\text{Query}} = O(|D|^{1-\varepsilon})$

server efficiency $T_{\text{Resp}} = O(|D|^{1-\varepsilon})$

Doubly Efficient Private Information Retrieval

DE-PIR



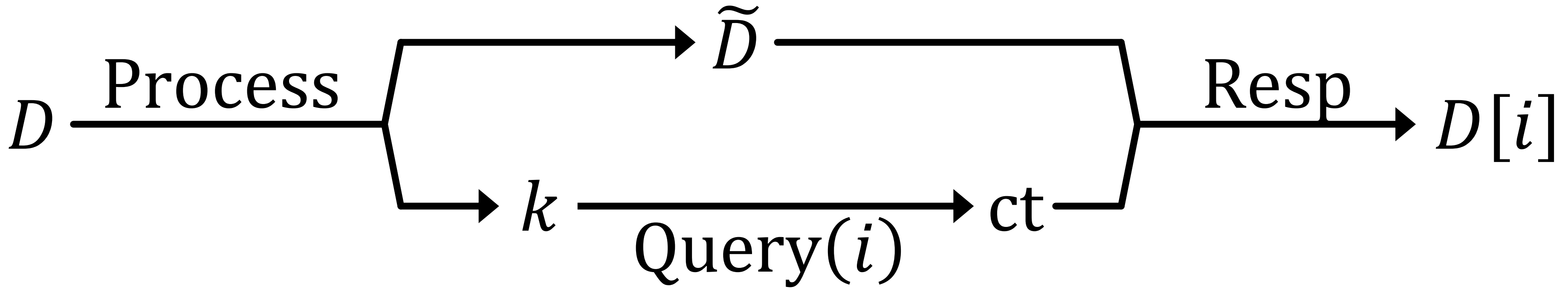
client efficiency $|k| = O(1)$ **and** $T_{\text{Query}} = O(|D|^{1-\varepsilon})$

server efficiency $T_{\text{Resp}} = O(|D|^{1-\varepsilon})$

security $\widetilde{D}, \{\text{ct}(i_q)\}$ **hides** $\{i_q\}$

Doubly Efficient Private Information Retrieval

DE-PIR



client efficiency $|k| = O(1)$ **and** $T_{\text{Query}} = O(|D|^{1-\varepsilon})$

server efficiency $T_{\text{Resp}} = O(|D|^{1-\varepsilon})$

security $\widetilde{D}, \{\text{ct}(i_q)\}$ **hides** $\{i_q\}$

dream efficiency $|\widetilde{D}| = O(|D|)$ **and** $T_{\text{Query}}, T_{\text{Resp}} = O(1)$

Doubly Efficient Private Information Retrieval

DE-PIR

$$D \xrightarrow{\text{Process}} \widetilde{D},\ k \qquad k \xrightarrow{\text{Query}(i)} \text{ct} \qquad \widetilde{D},\ \text{ct} \xrightarrow{\text{Resp}} D[i]$$

client efficiency $|k| = O(1)$ **and** $T_{\text{Query}} = O(|D|^{1-\varepsilon})$

server efficiency $T_{\text{Resp}} = O(|D|^{1-\varepsilon})$

security $\widetilde{D}, \{\text{ct}(i_q)\}$ **hides** $\{i_q\}$

dream efficiency $|\widetilde{D}| = O(|D|)$ **and** $T_{\text{Query}}, T_{\text{Resp}} = O(1)$

Is it known?

Results: Optimal Decryption Time Implies **DE-PIR**

Results: Optimal Decryption Time Implies **DE-PIR**

Assuming **sufficiently** expressive secure PHFE with

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

or

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

for $B < 1$, then there exists **secret-key** DE-PIR with

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

essentially also proven in ACFQ

Results: Optimal Decryption Time Implies **DE-PIR**

Assuming **mildly** expressive secure PHFE with

new in this work

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

for $B < 1$, then there exists **public-key** DE-PIR with

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

Assuming **sufficiently** expressive secure PHFE with

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

or

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

for $B < 1$, then there exists **secret-key** DE-PIR with

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

essentially also proven in ACFQ

Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

subexp. secure FE for circuits

$\Longrightarrow$ subexp. secure $i\mathcal{O}$ for RAM with

$$|\widetilde{M}| = 2|M| + \mathrm{poly}(|D|)$$

Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

new! previously only known for circuits [BV] with LWE / TM [AJS]

subexp. secure FE for circuits

$\Longrightarrow$ subexp. secure $i\mathcal{O}$ for RAM with

$$|\widetilde{M}| = 2|M| + \mathrm{poly}(|D|)$$

Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

new! previously only known for circuits [BV] with LWE / TM [AJS]

subexp. secure FE for circuits
$\Longrightarrow$ subexp. secure $i\mathcal{O}$ for RAM with
$|\widetilde{M}| = 2|M| + \mathrm{poly}(|D|)$

ABE for RAM	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x \rvert$	T_{Dec}
from PHFE	$O(1)$	$O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert)$

Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

new! previously only known for circuits [BV] with LWE / TM [AJS]

subexp. secure FE for circuits
$\Longrightarrow$ subexp. secure $i\mathcal{O}$ for RAM with
$|\widetilde{M}| = 2|M| + \text{poly}(|D|)$

4 new!

ABE for RAM	$\lvert\text{sk}_f\rvert$	$\lvert\text{ct}_x\rvert$	T_{Dec}
from PHFE	$O(1)$	$O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert)$
minor tweaks	$\lvert f\rvert + O(1)$	$O(1)$	$O(T + \lvert x\rvert)$
	$O(1)$	$\lvert x\rvert + O(1)$	$O(T + \lvert f\rvert)$
	$\lvert f\rvert + O(1)$	$\lvert x\rvert + O(1)$	$O(T)$

can move between size and time

(adaptive, based on FE for circuits)

Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

new! previously only known for circuits [BV] with LWE / TM [AJS]

subexp. secure FE for circuits
$\Longrightarrow$ subexp. secure $i\mathcal{O}$ for RAM with
$|\widetilde{M}| = 2|M| + \mathrm{poly}(|D|)$

4 new!

ABE for RAM	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x \rvert$	T_{Dec}
from PHFE	$O(1)$	$O(1)$	$O(T + \lvert f \rvert + \lvert x \rvert)$
minor tweaks	$\lvert f \rvert + O(1)$	$O(1)$	$O(T + \lvert x \rvert)$
	$O(1)$	$\lvert x \rvert + O(1)$	$O(T + \lvert f \rvert)$
	$\lvert f \rvert + O(1)$	$\lvert x \rvert + O(1)$	$O(T)$

can move between size and time

(adaptive, based on FE for circuits)

Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

new! previously only known for circuits [BV] with LWE / TM [AJS]

subexp. secure FE for circuits
$\Longrightarrow$ subexp. secure $i\mathcal{O}$ for RAM with
$|\widetilde{M}| = 2|M| + \mathrm{poly}(|D|)$

4 new!

ABE for RAM	$\lvert \mathrm{sk}_f \rvert$	$\lvert \mathrm{ct}_x \rvert$	T_{Dec}
from PHFE	$O(1)$	$O(1)$	$O(T + \lvert f\rvert + \lvert x\rvert)$
minor tweaks	$\lvert f\rvert + O(1)$	$O(1)$	$O(T + \lvert x\rvert)$
	$O(1)$	$\lvert x\rvert + O(1)$	$O(T + \lvert f\rvert)$
	$\lvert f\rvert + O(1)$	$\lvert x\rvert + O(1)$	$O(T)$

can move between size and time

Luo22

(adaptive, based on FE for circuits)

Where we stand now: **(PH-)FE**

$$y\text{-independent Dec}$$

$$\Uparrow$$

morally

$$\Downarrow$$

DE-PIR

Where we stand now: **(PH-)FE**

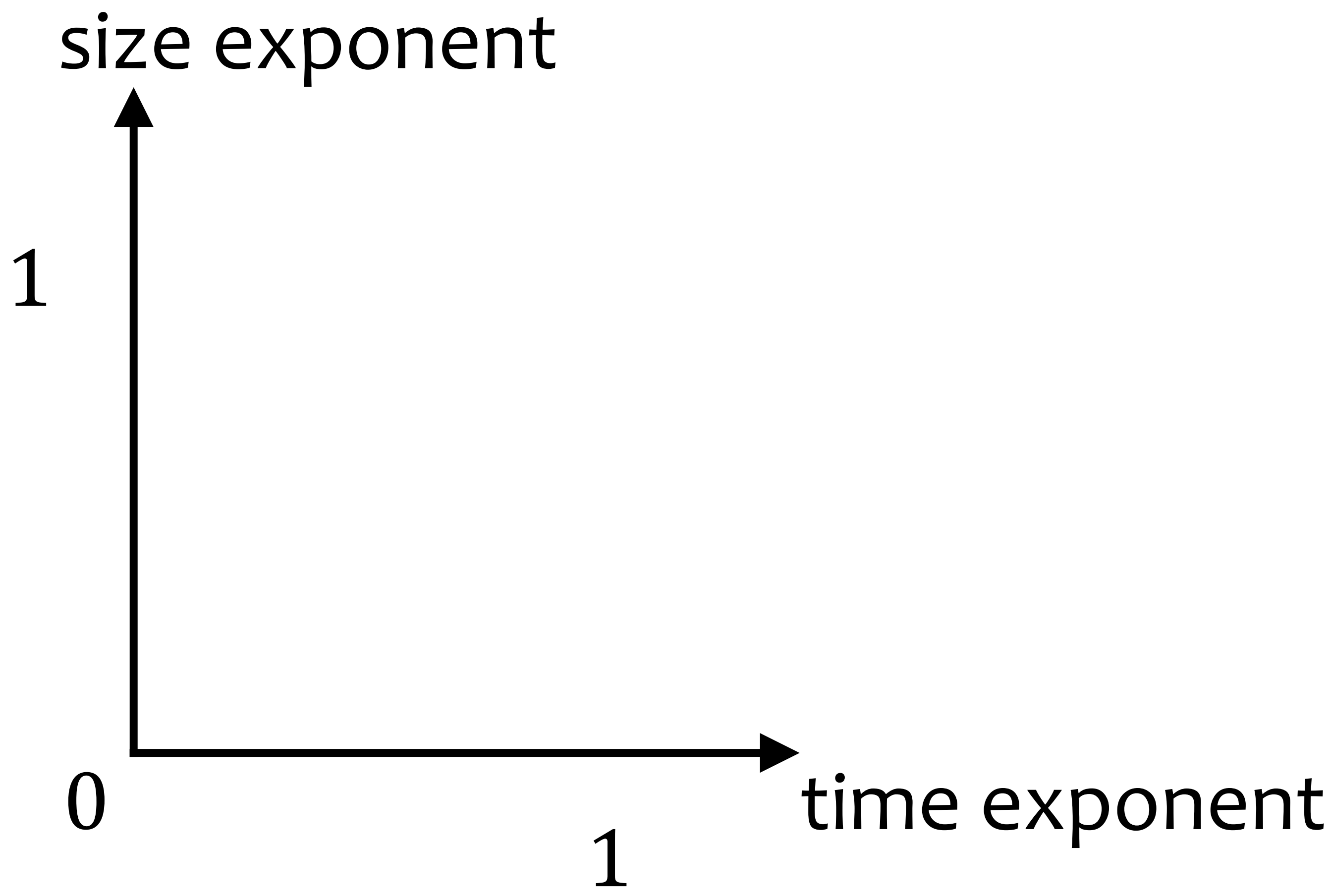
y-independent Dec

$\Uparrow$

morally

$\Downarrow$

DE-PIR



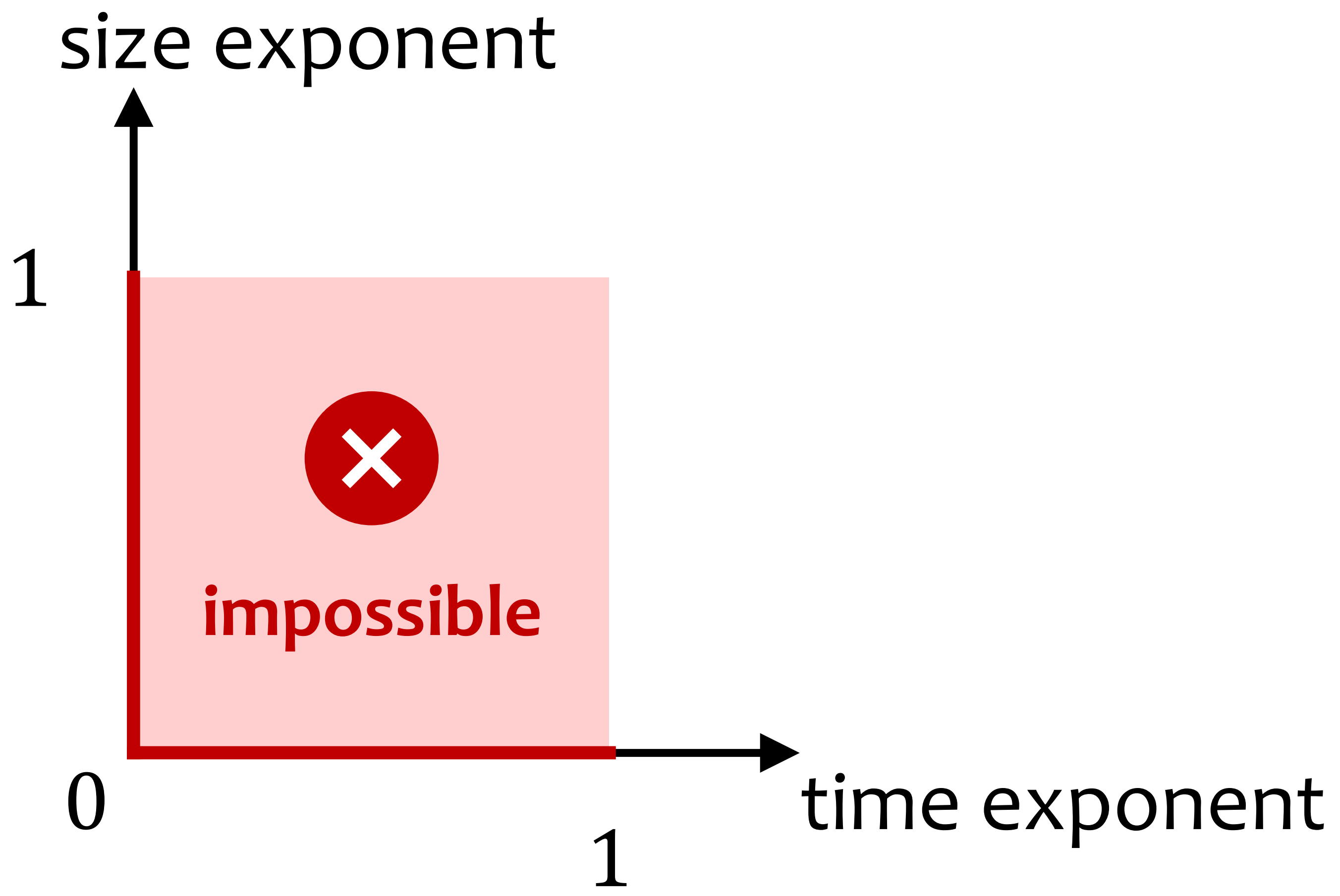
dependency on f or x
characterized by this work

Where we stand now: **(PH-)FE**

y-independent Dec

$\Uparrow$ **morally** $\Downarrow$

DE-PIR



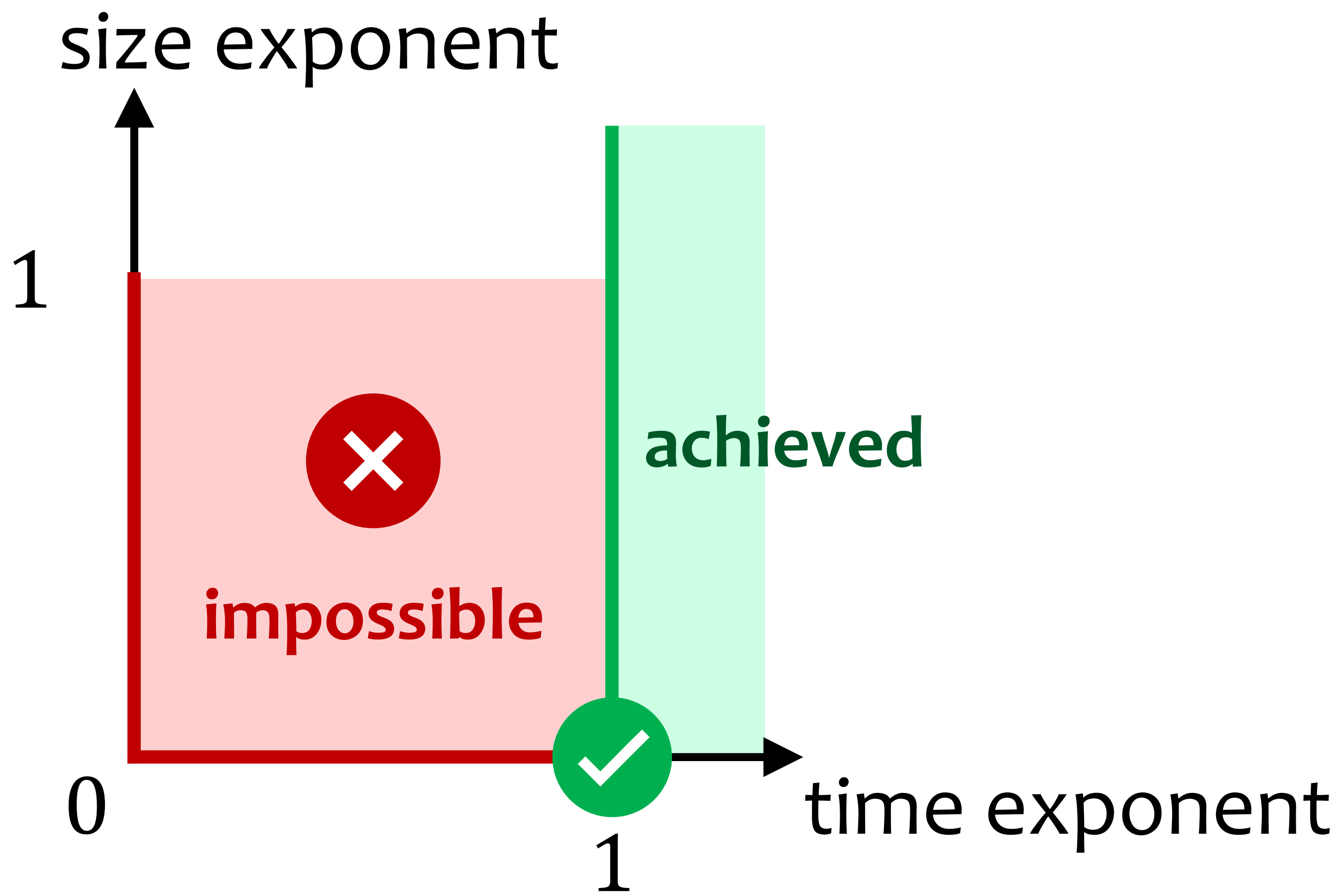
dependency on f or x characterized by this work

Where we stand now: **(PH-)FE**

y-independent Dec

$\Updownarrow$ **morally**

DE-PIR



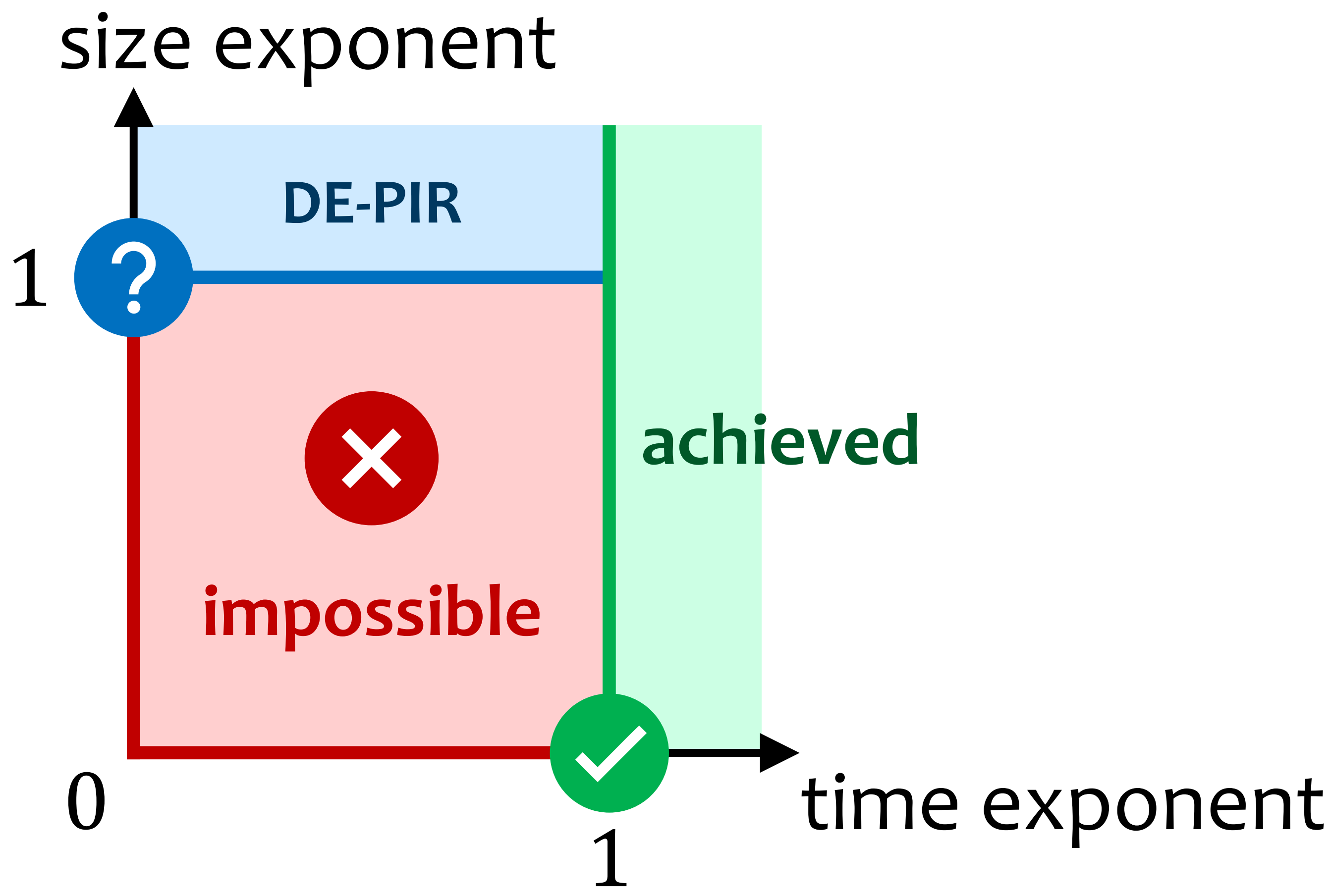
dependency on f or x
characterized by this work

Where we stand now: **(PH-)FE**

y-independent Dec

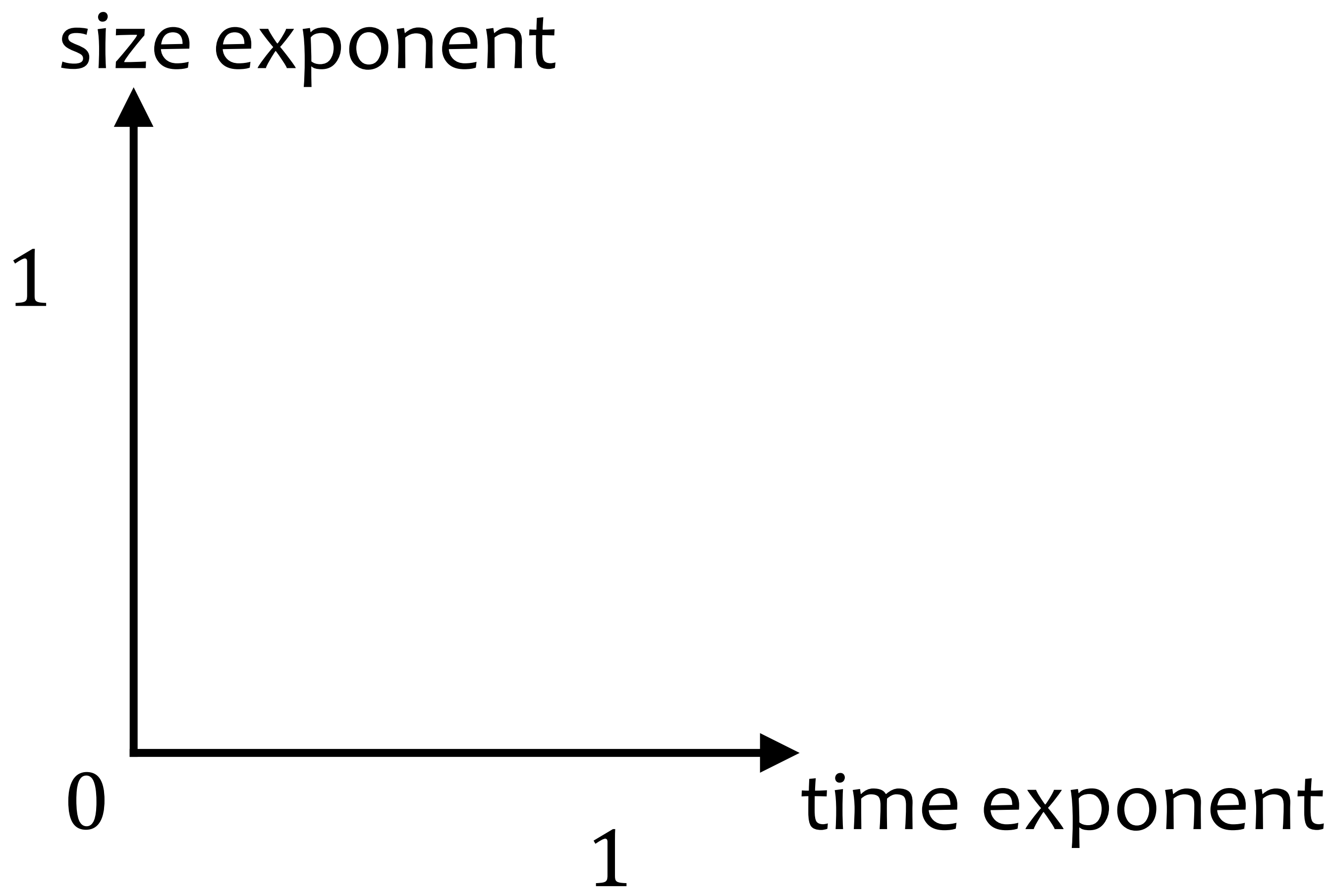
$\Uparrow$
morally
$\Downarrow$

DE-PIR



dependency on f or x
characterized by this work

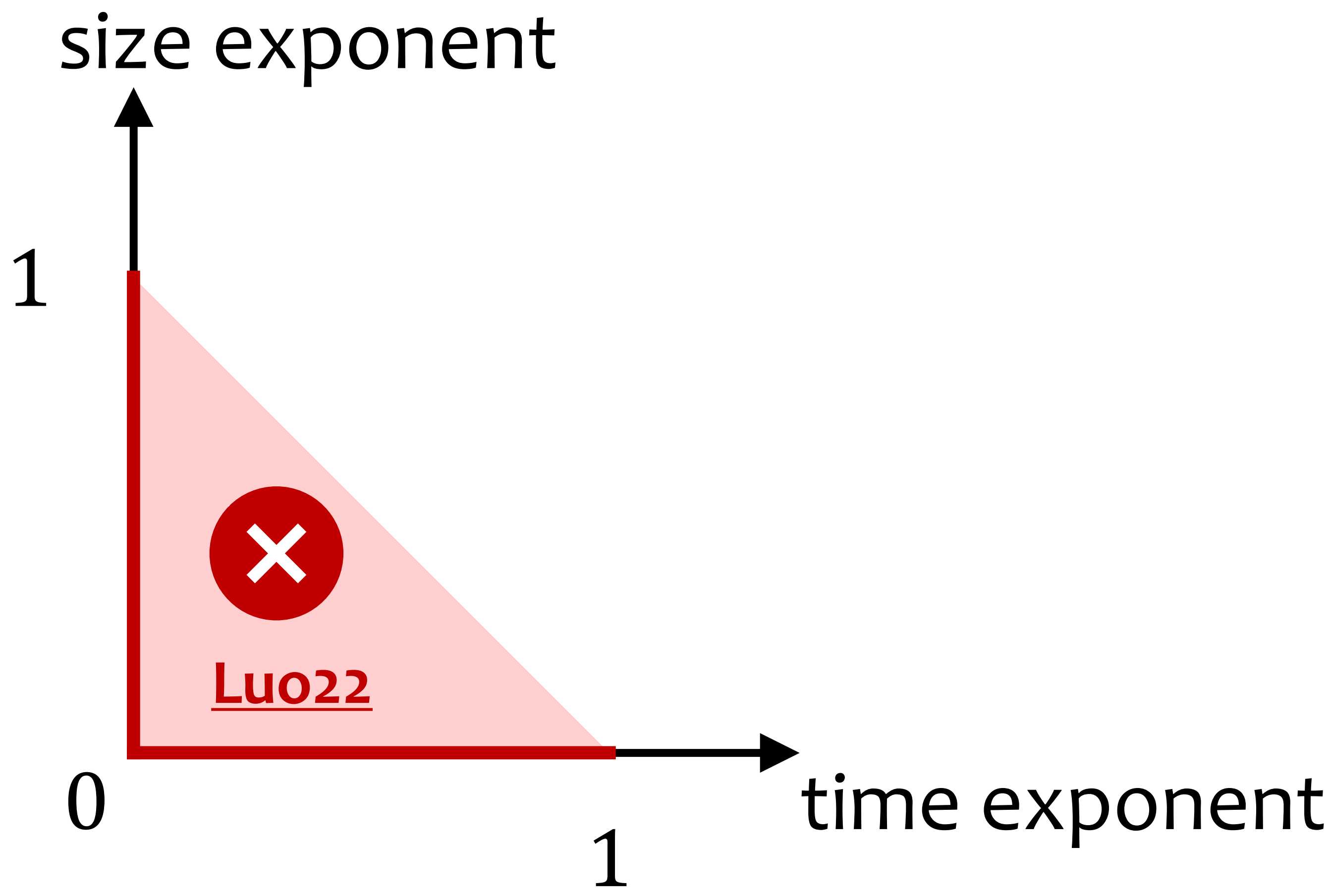
Where we stand now: **ABE**



dependency on f or x

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

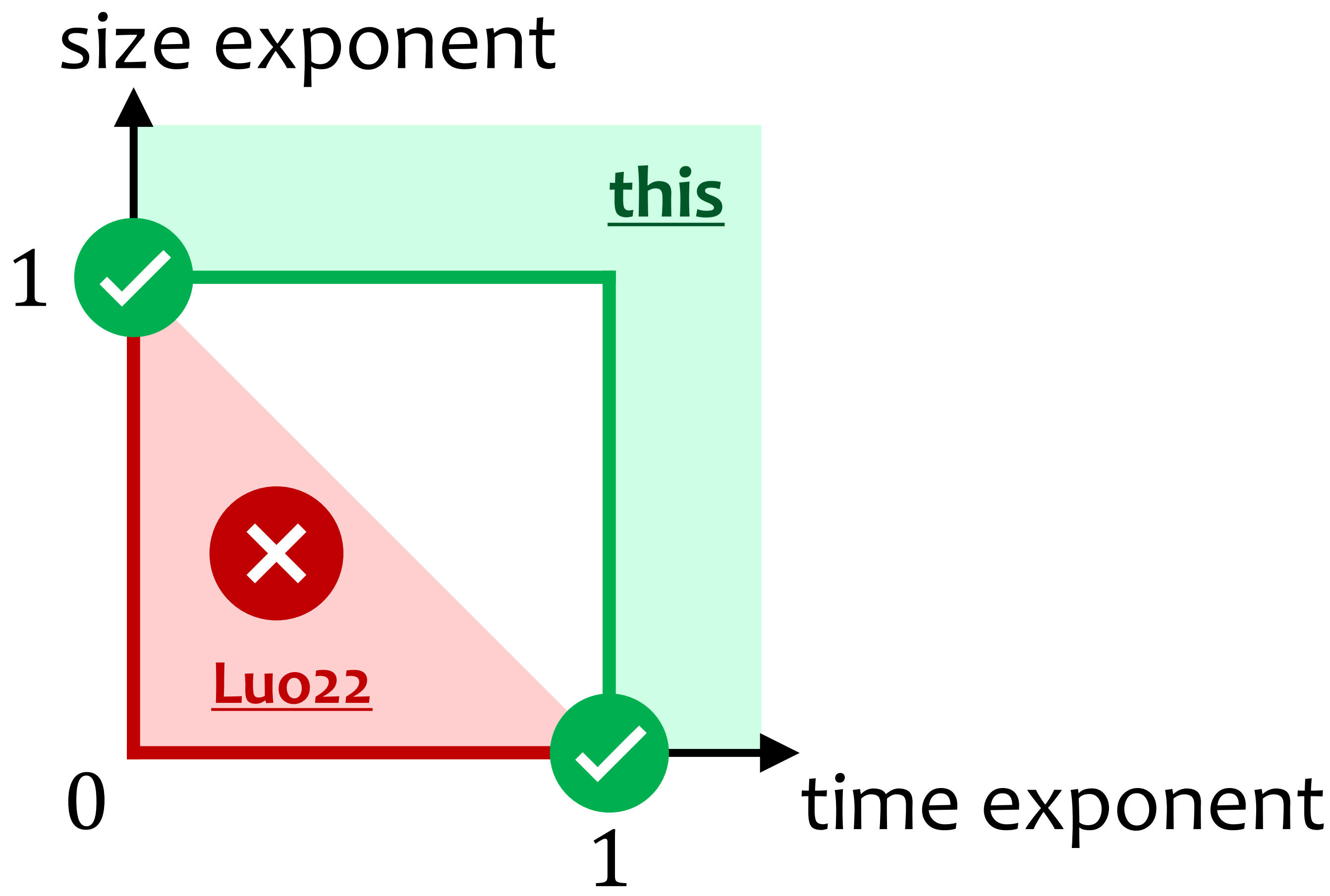
Where we stand now: **ABE**



dependency on f or x

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

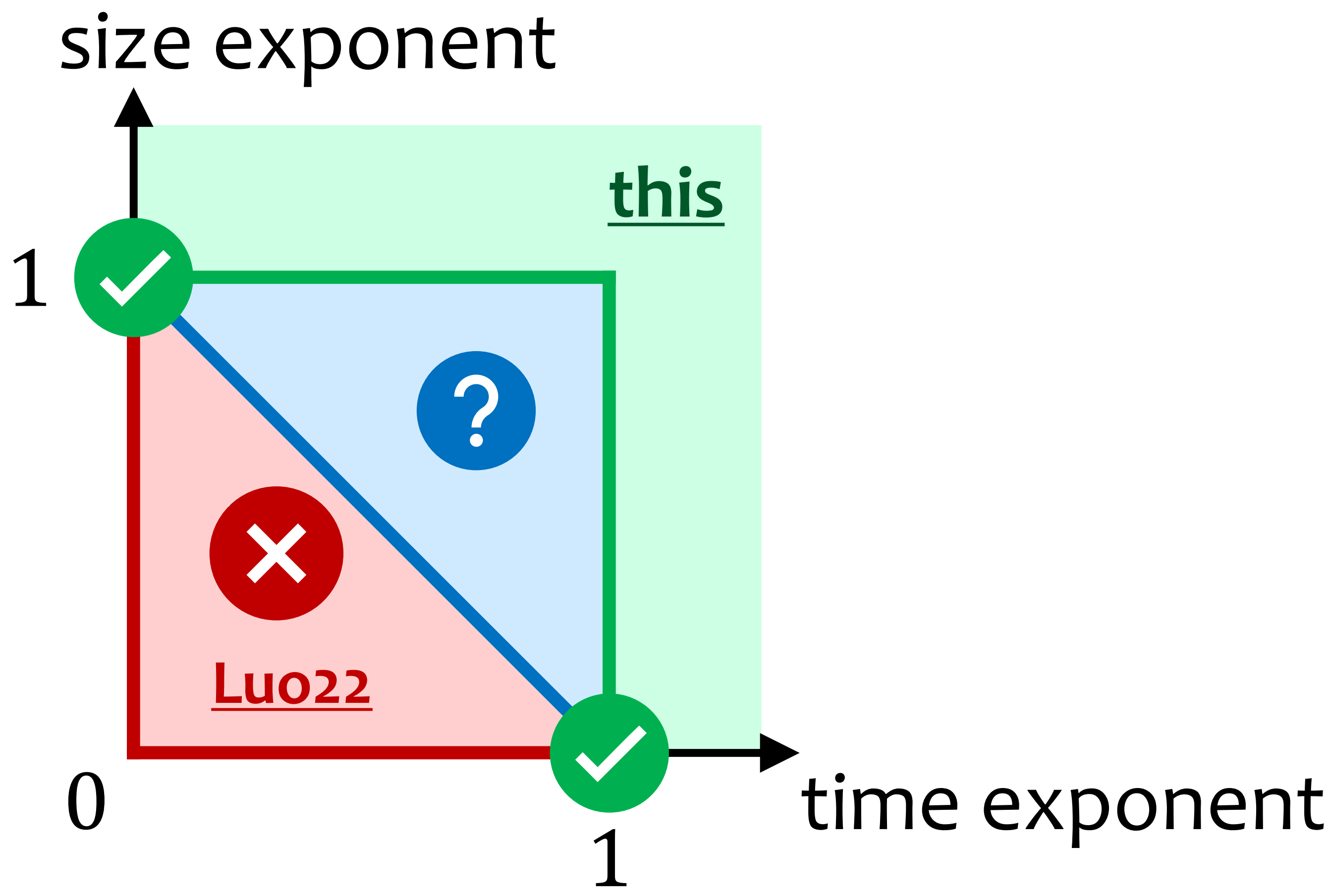
Where we stand now: **ABE**



dependency on f or x

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

Where we stand now: **ABE**



dependency on f or x

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

Proof Sketch of **Unconditional** Lower Bound

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

Proof Sketch of **Unconditional** Lower Bound

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

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

Proof Sketch of **Unconditional** Lower Bound

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

$I \subseteq [N]$ is of size n $\quad w \in \{0,1\}^n$

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

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

Proof Sketch of **Unconditional** Lower Bound

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

$I \subseteq [N]$ is of size n $\quad w \in \{0,1\}^n$

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

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

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

Proof Sketch of **Unconditional** Lower Bound

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

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

make $N^A, N^B \ll n \ll N$

$I \subseteq [N]$ is of size n $\quad w \in \{0,1\}^n$

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

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

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

Unconditional Lower Bound (continued)

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

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

Unconditional Lower Bound (continued)

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

How much of $R[I]$ does $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ read?

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

choose random I, w and $z = R[I] \oplus w$

Unconditional Lower Bound (continued)

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

How much of $R[I]$
does $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ read?

When $y = y_0 = (I, w)$:

$(\mathrm{sk}_f, \mathrm{ct})$ contains $\ll n$ bits of $R[I]$ (n bits)

must read **almost all** of $R[I]$ **(incompressibility argument)**

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

choose random I, w
and $z = R[I] \oplus w$

Unconditional Lower Bound (continued)

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

How much of $R[I]$ does $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ read?

When $y = y_0 = (I, w)$:

$(\mathrm{sk}_f, \mathrm{ct})$ contains $\ll n$ bits of $R[I]$ (n bits)

must read **almost all** of $R[I]$ (incompressibility argument)

When $y = y_1 = z$:

behavior of $\mathrm{Dec}^R(\mathrm{sk}_f, \mathrm{ct})$ **independent** of I

can **only** read $|I| \cdot \frac{T_{\mathrm{Dec}}}{N} \ll n$ bits from $R[I]$ **(hypergeometric distribution)**

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

choose random I, w and $z = R[I] \oplus w$

Proof Sketch of Technical Barrier of **DE-PIR**

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

Proof Sketch of Technical Barrier of **DE-PIR**

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

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

Proof Sketch of Technical Barrier of **DE-PIR**

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

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

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

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

Proof Sketch of Technical Barrier of **DE-PIR**

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

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

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

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

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

Proof Sketch of Technical Barrier of **DE-PIR**

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

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

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

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

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

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

Proof Sketch of Technical Barrier of **DE-PIR**

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

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

Preprocessing. $\widetilde{D} = (D, \mathrm{fesk}_f)$, $\quad k = \mathrm{fempk}.$

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

Querying. $\mathrm{ct} = \mathrm{fect}(i)\,.$ $\quad T_{\mathrm{Query}} = O(1)$

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

⚠ **IND-secure, selective, non-output-hiding, (if SK) non-database-hiding.**

Proof Sketch of Technical Barrier of **DE-PIR**

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

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

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

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

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

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

⚠ **IND-secure, selective, non-output-hiding, (if SK) non-database-hiding.**

Generic efficiency-preserving transformation for SIM-secure, adaptive, output-hiding, (if SK) database-hiding. ✓

Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

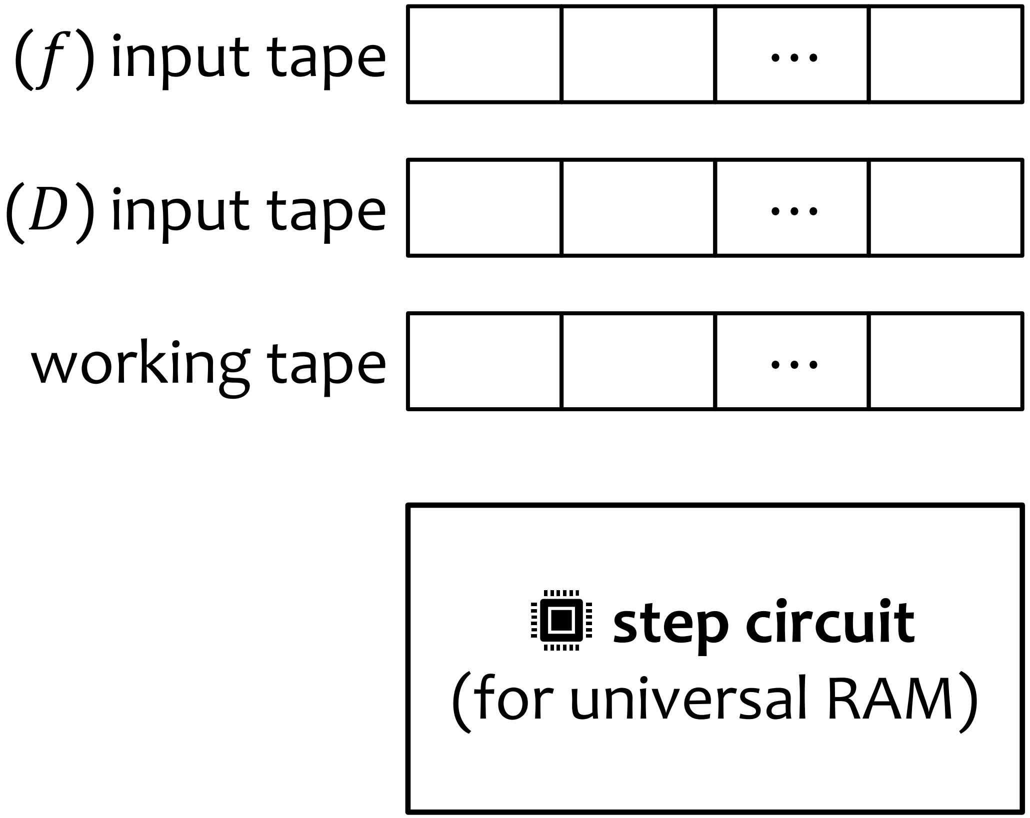
Step 1: **Formulate the right definition.**

Step 2: **Achieve it.**

Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

Step 1: **Formulate the right definition.**

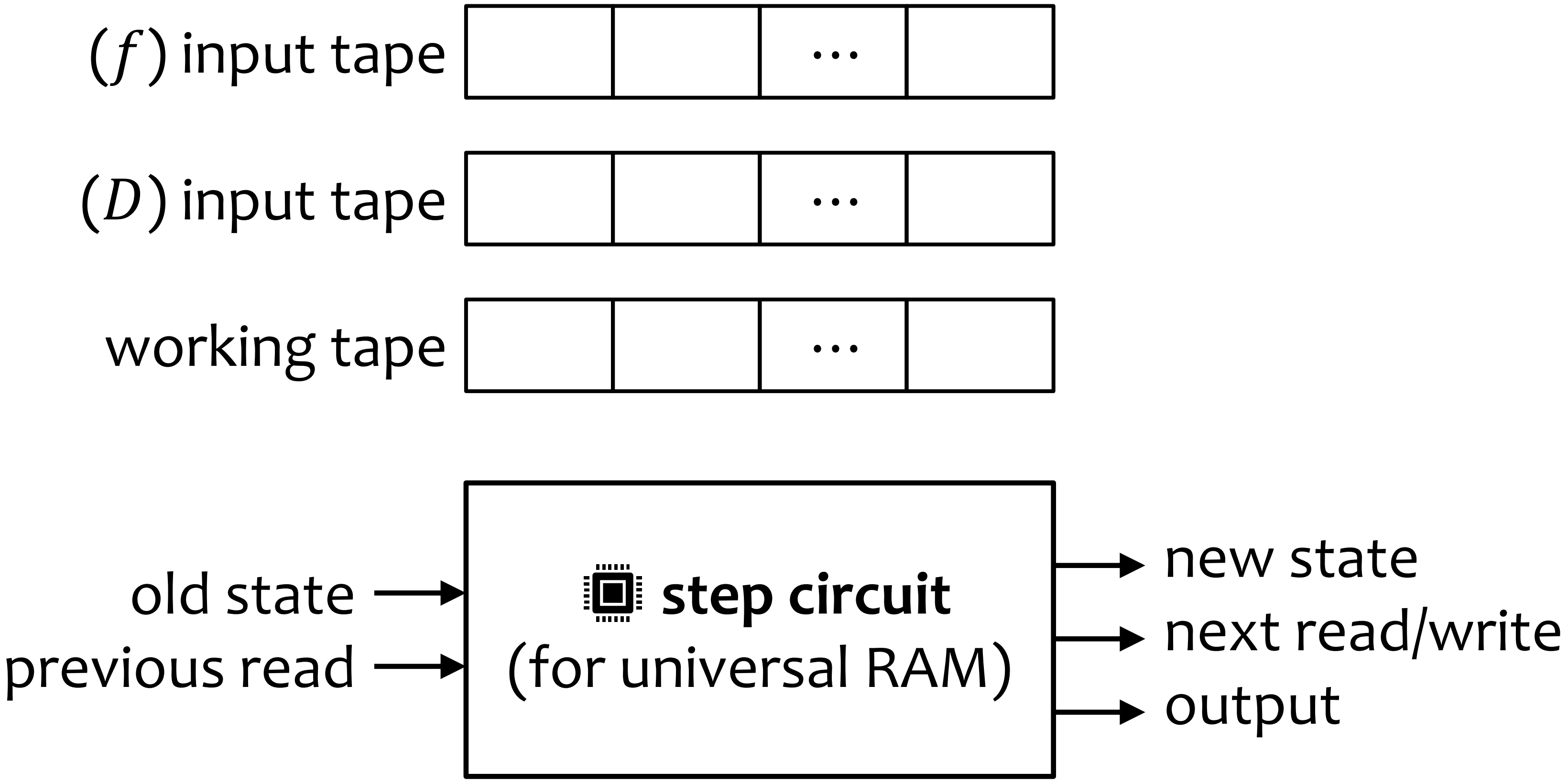
Step 2: **Achieve it.**



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

Step 1: **Formulate the right definition.**

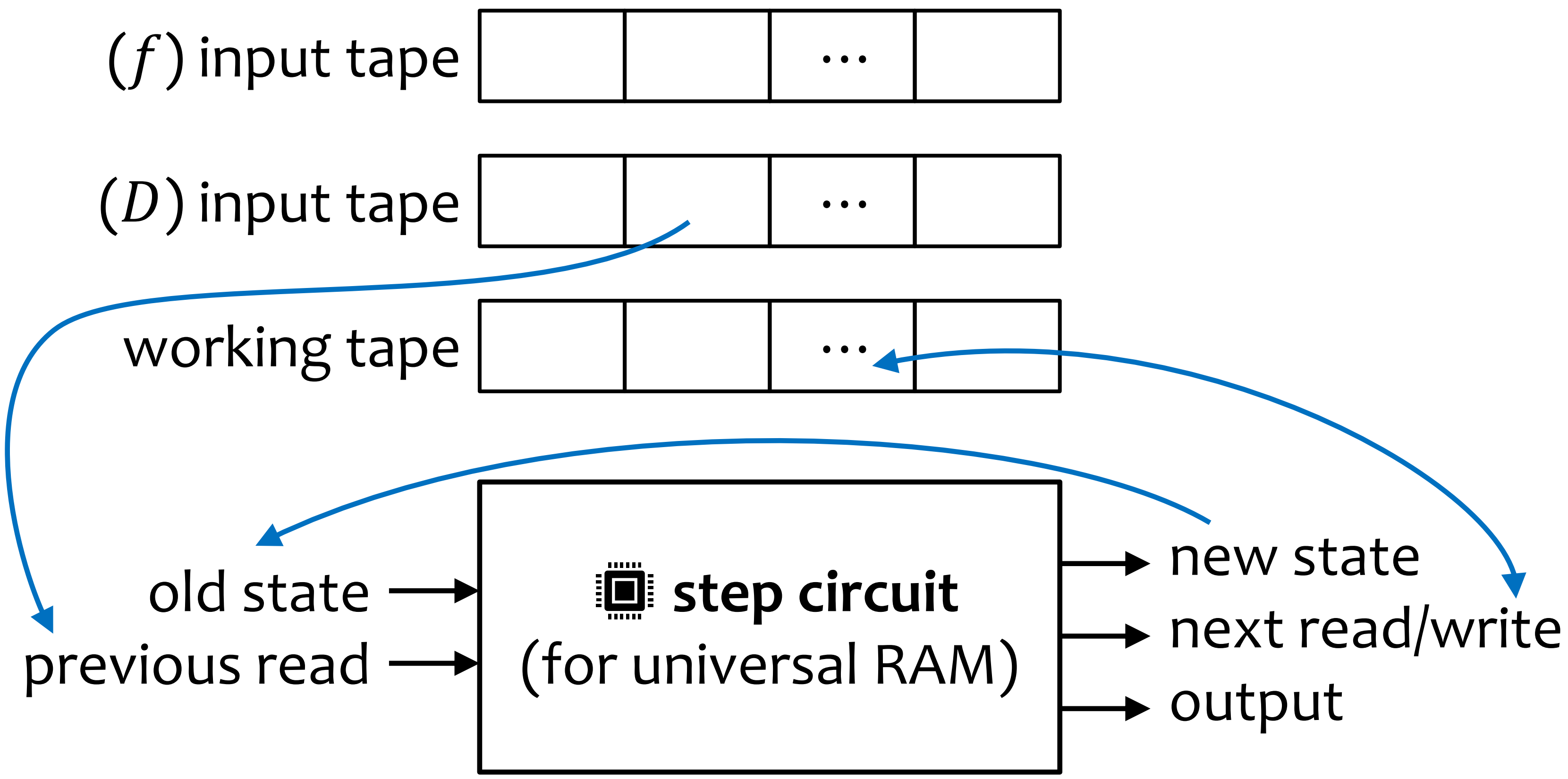
Step 2: **Achieve it.**



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

Step 1: **Formulate the right definition.**

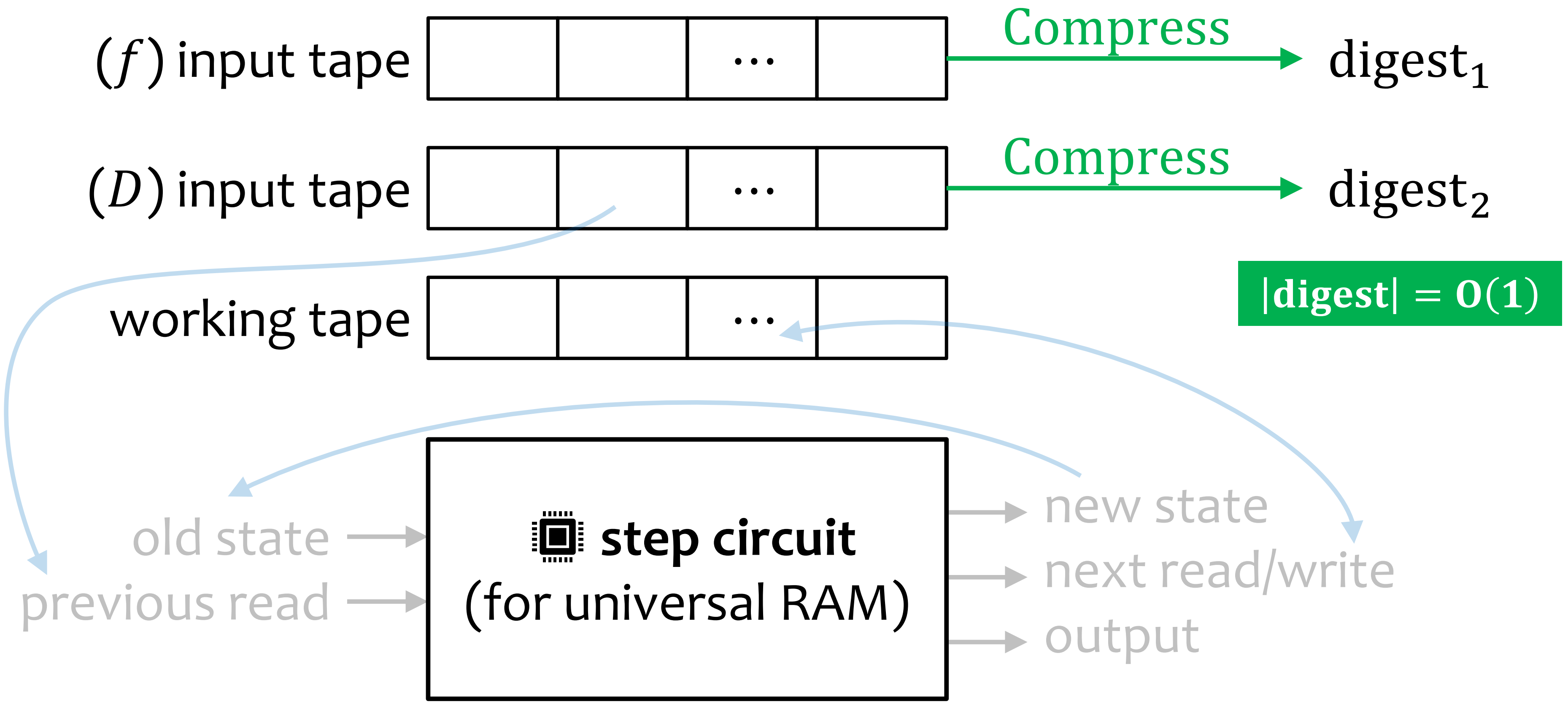
Step 2: **Achieve it.**



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

Step 1: **Formulate the right definition.**

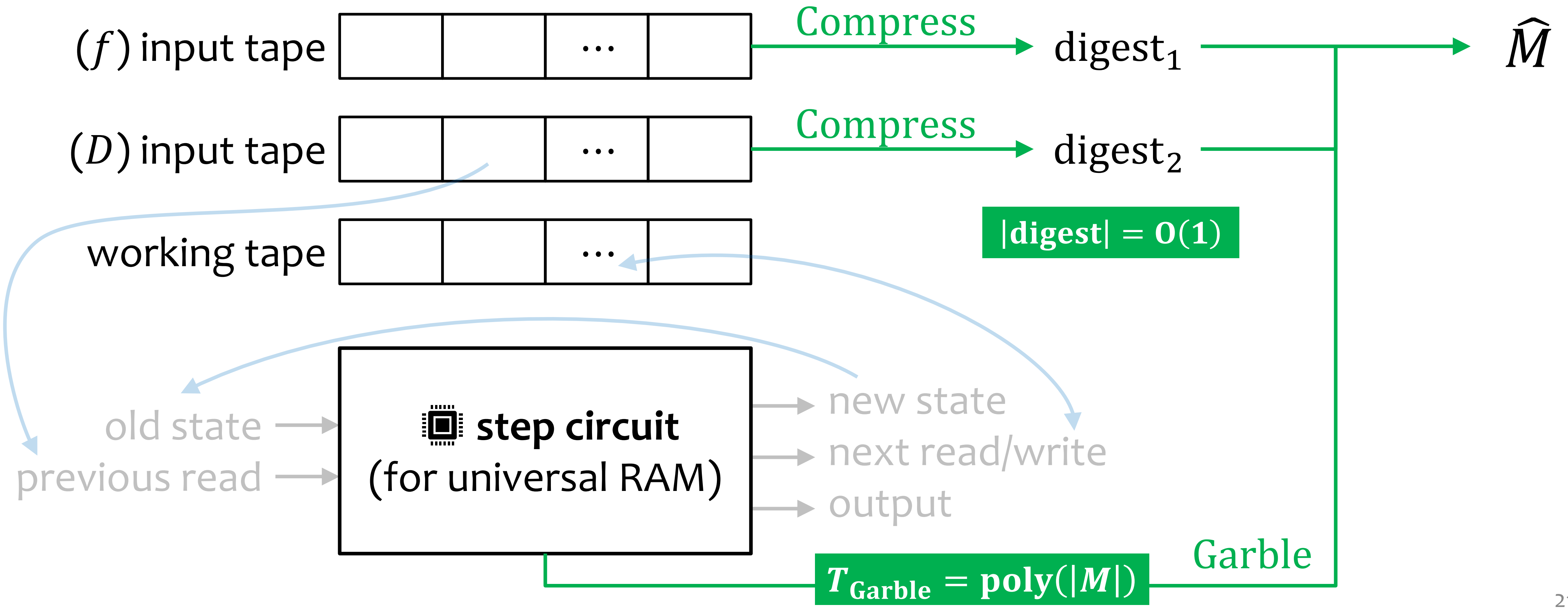
Step 2: **Achieve it.**



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

Step 1: **Formulate the right definition.**

Step 2: **Achieve it.**



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

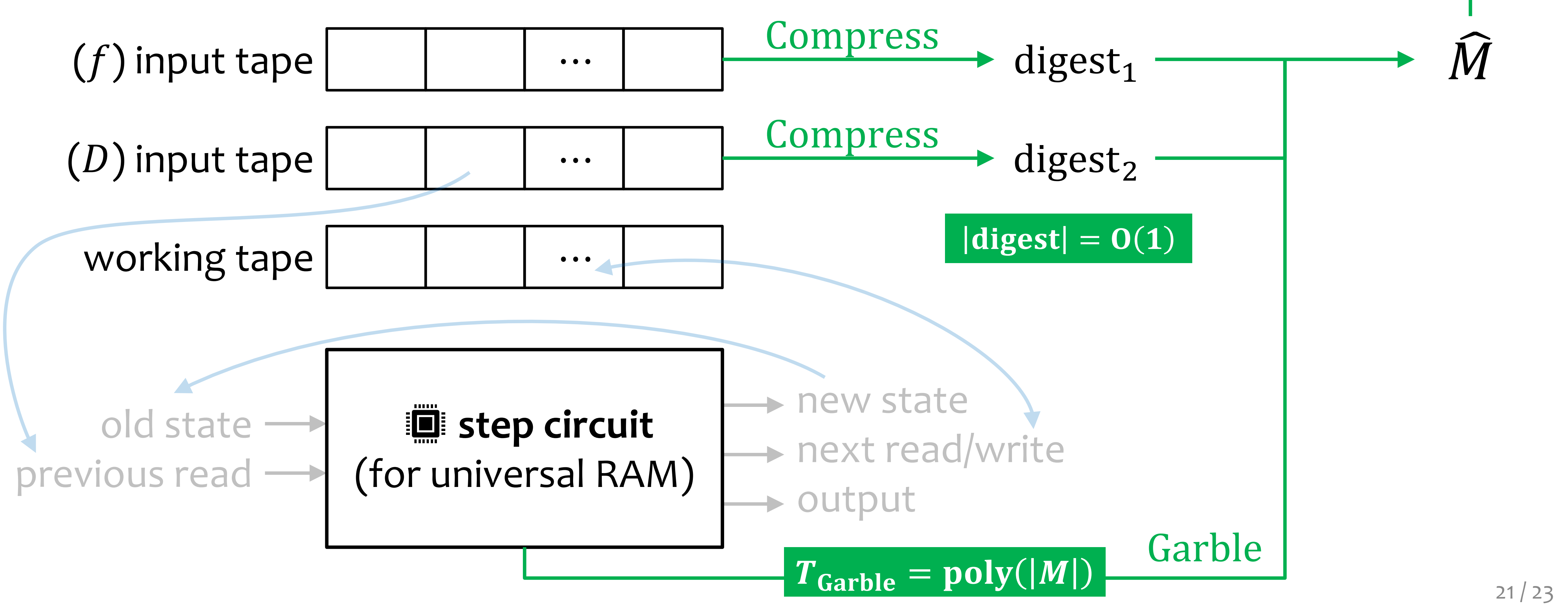
$T_{\mathrm{Eval}} = (T + |f| + |D|)\,\mathrm{poly}(|M|)$

Step 1: **Formulate the right definition.**

Step 2: **Achieve it.**

$M^{f,D}()$

$\mathrm{Eval}^{f,D}$



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

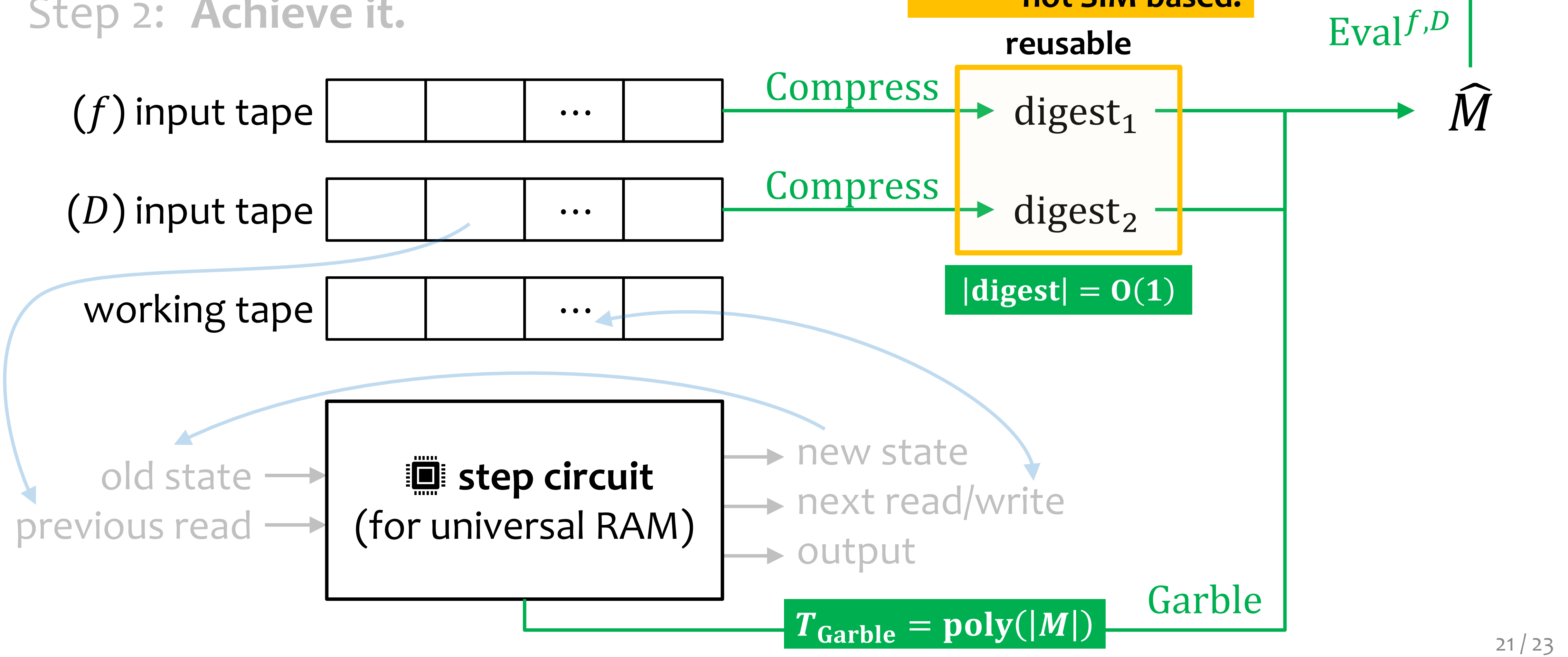
$T_{\text{Eval}} = (T + |f| + |D|)\,\text{poly}(|M|)$

Step 1: **Formulate the right definition.**

Step 2: **Achieve it.**

Security is IND-based, not SIM-based.

$M^{f,D}()$



Core of PHFE: **Laconic** Garbled **(Multi-Tape)** RAM

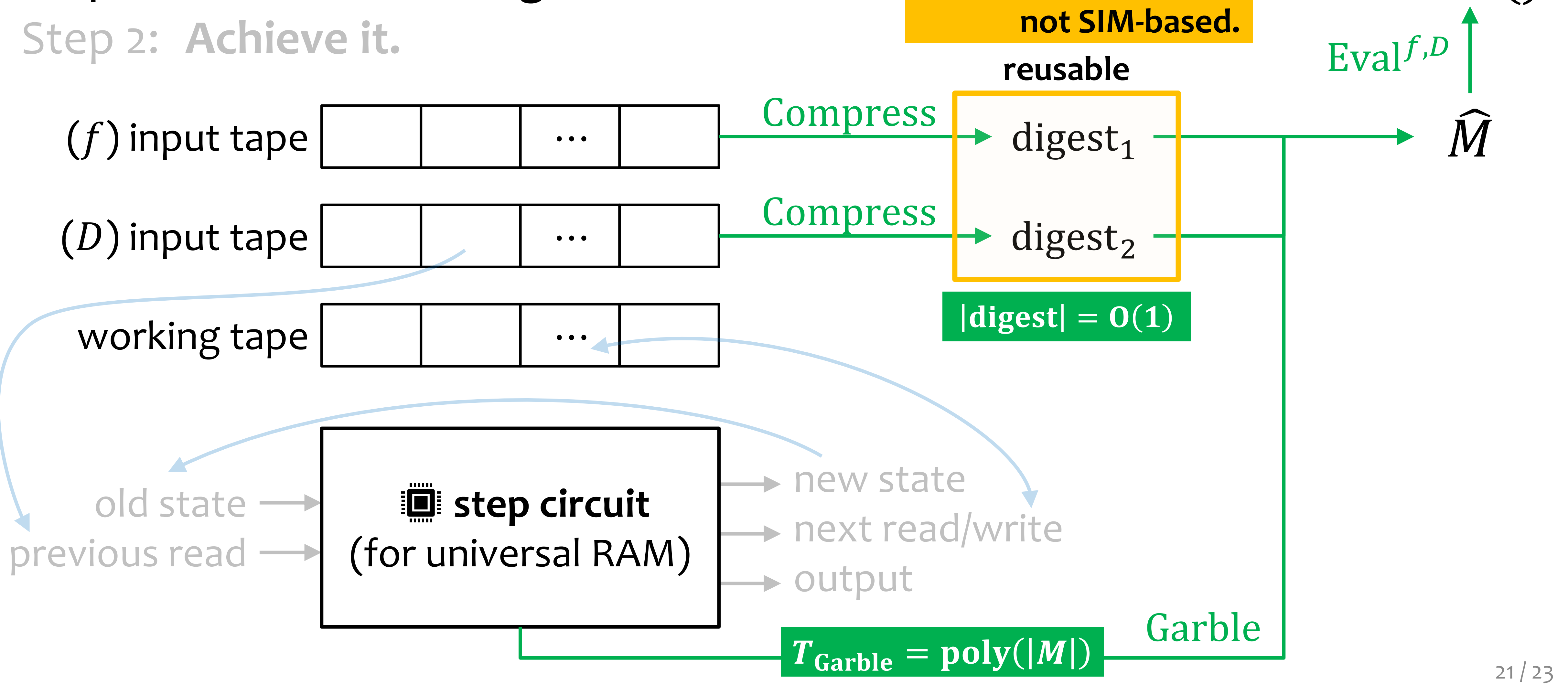
important for nearly optimal efficiency

$T_{\mathrm{Eval}} = (T + |f| + |D|)\,\mathrm{poly}(|M|)$

Step 1: **Formulate the right definition.**

Step 2: **Achieve it.**

Security is IND-based, not SIM-based.



Open Questions: **What's next for (PH-)FE/ABE?**

1. **Construct** PHFE with optimal T_{Dec} from/and dream DE-PIR.
2. **Achieve** rate-1 in y with adaptive security and/or long output.

Open Questions: **What's next for (PH-)FE/ABE?**

1. **Construct** PHFE with optimal T_{Dec} from/and dream DE-PIR.
2. **Achieve** rate-1 in y with adaptive security and/or long output.
3. **Tight relation** between optimal T_{Dec} and DE-PIR.

   FE for circuits + **PK**-DE-PIR $\Longrightarrow$ (x, y)-optimal Dec time $\Longrightarrow$ **SK**-DE-PIR.
   FE for circuits + **SK**-DE-PIR $\Longrightarrow$ … ?

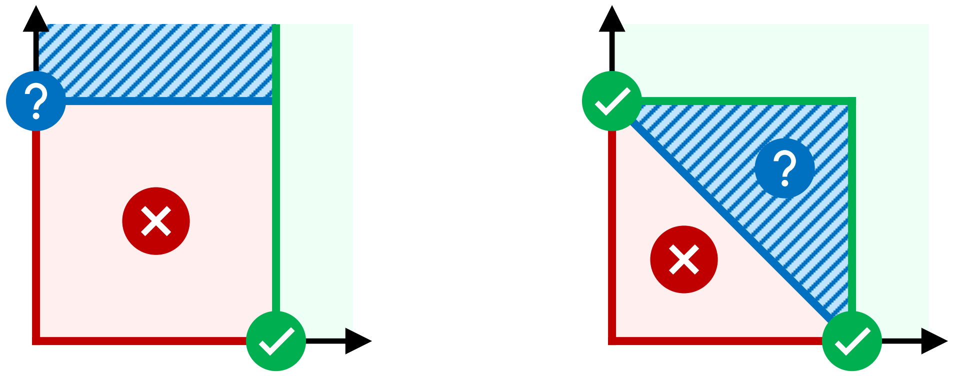
Open Questions: **What's next for (PH-)FE/ABE?**

1. **Construct** PHFE with optimal T_{Dec} from/and dream DE-PIR.
2. **Achieve** rate-1 in y with adaptive security and/or long output.
3. **Tight relation** between optimal T_{Dec} and DE-PIR.

   FE for circuits + **PK**-DE-PIR $\Longrightarrow$ (x, y)-optimal Dec time $\Longrightarrow$ **SK**-DE-PIR.
   FE for circuits + **SK**-DE-PIR $\Longrightarrow$ $\ldots$?

4. **Pin down** the exact Pareto frontier of efficiency.

   Demystify the **stripe area**.



Thanks!

ePrint 2022/1317 (revision coming soon)