Quel est le prix du chiffrement fonctionnel ?

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

Aayush Jain

Rachel Lin

罗辑 (Ji Luo)

Carnegie Mellon University

UNIVERSITY of WASHINGTON

Eurocrypt 2023
Partially Hiding Functional Encryption

Setup → mpk, msk
Partially Hiding Functional Encryption

Setup → mpk, msk

Enc(mpk, x, y) → ct_x(y)
Partially Hiding Functional Encryption

Setup $\rightarrow$ mpk, msk
KeyGen(msk, $f$) $\rightarrow$ sk$_f$

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

public/private inputs
Partially Hiding Functional Encryption

Setup $\rightarrow mpk, msk$

KeyGen($msk, f$) $\rightarrow sk_f$

$mpk, f, sk_f$

Enc($mpk, x, y$) $\rightarrow ct_x(y)$

public/private inputs

Dec($mpk, f, sk_f, x, ct_x$) $\rightarrow f(x, y)$

$x, ct_x$

correctness
Partially Hiding Functional Encryption

Setup $\rightarrow$ mpk, msk
KeyGen(msk, $f$) $\rightarrow$ sk$_f$

mpk, $f$, sk$_f$

$f, x$ are always provided in the clear.

Enc(mpk, $x, y$) $\rightarrow$ $ct_x(y)$
Public/private inputs

Dec(mpk, $f, sk_f, x, ct_x$) $\rightarrow$ $f(x, y)$
Correctness
PHFE Security

Setup → mpk, msk

KeyGen(msk, f) → sk_f

mpk, f, sk_f

Enc(mpk, x, y) → ct_x(y)

x, ct_x

Security. Hides all information about y beyond f(x, y).
PHFE Security: **Collusion Resistance**

**Setup** → mpk, msk

**KeyGen(msk, $f_q$)** → $sk_{f_q}$

$mpk, \{f_q, sk_{f_q}\}$

**Enc(mpk, $x, y$)** → $ct_x(y)$

$x, ct_x$

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

4 / 23
PHFE Security: Collusion Resistance

Setup → mpk, msk
KeyGen(msk, $f_q$) → $sk_{f_q}$

Given arbitrarily many keys, information revealed about $y$ is exactly the computation results.

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

Enc(mpk, $x$, $y$) → $ct_x(y)$

$x$, $ct_x$
PHFE Security: IND-CPA

\[ \text{Exp}^b_{\text{PHFE}} \]
PHFE Security: **IND-CPA**

\[
\text{Exp}_b^{\text{PHFE}}
\]
PHFE Security: IND-CPA

\[ \text{Exp}_{\text{PHFE}}^b \]

\[ \text{mpk} \]

\[ f_q \]

\[ \text{sk}_{f_q} \]
PHFE Security: IND-CPA

$\text{Exp}_{PHFE}^b$
PHFE Security: IND-CPA

\[ \text{Exp}_{\text{PHFE}}^b \]

\[ \text{mpk} \]

\[ f_q \]

\[ \text{sk}_{f_q} \]

\[ x, y_0, y_1 \]

\[ \text{ct}_x(y_b) \]}
PHFE Security: **IND-CPA**

\[ \text{Exp}_{\text{PHFE}}^b \]

\[ \text{mpk} \]

\[ f_q \]

\[ \text{sk}_{f_q} \]

\[ x, y_0, y_1 \]

\[ \text{ct}_x (y_b) \]

\[ f_q \]

\[ \text{sk}_{f_q} \]
PHFE Security: **IND-CPA**

\[
\begin{align*}
\text{Exp}_{\text{PHFE}}^b & \quad \text{mpk} \\
& \quad f_q \\
& \quad \text{sk}_{f_q} \\
& \quad x, y_0, y_1 \\
& \quad \text{ct}_x(y_b) \\
& \quad f_q \\
& \quad \text{sk}_{f_q} \\
\:
\end{align*}
\]

\[
\text{Exp}_{\text{PHFE}}^0 \approx \text{Exp}_{\text{PHFE}}^1 \quad \text{if } |y_0| = |y_1| \quad \text{and} \quad \forall q: f_q(x, y_0) = f_q(x, y_1)
\]

5 / 23
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
- ★ short keys / ciphertexts
- ★ fast decryption

supports RAM computation with unbounded output length
What do we want for a PHFE?

★ expressive functionality supports RAM computation with unbounded output length

★ short keys / ciphertexts

\[ |\text{sk}_f| = \text{poly}(|f|) \]
\[ |\text{ct}_x(y)| = \text{poly}(|x|, |y|) \]

★ fast decryption

\[ T_{\text{Dec}} = \text{poly}(|f|, |x|, |y|, T) \]
What do we want for a PHFE?

★ expressive functionality 

supports RAM computation with unbounded output length

★ short keys / ciphertexts

$$|sk_f| = \text{poly}(|f|)$$
$$|ct_x(y)| = \text{poly}(|x|, |y|)$$

★ fast decryption

$$T_{\text{Dec}} = \text{poly}(|f|, |x|, |y|, T)$$
What do we want for a PHFE? (continued)

★ expressive functionality supports **RAM** computation with **unbounded output length**

★ short keys / ciphertexts

\[
|sk_f| = O(1)
\]

\[
|ct_x(y)| = |y| + O(1)
\]

★ fast decryption

\[
T_{Dec} = O(T)
\]
What do we want for a PHFE? (continued)

★ expressive functionality supports RAM computation with unbounded output length

★ short keys / ciphertexts

\[ |\text{sk}_f| = O(1) \]

\[ |\text{ct}_x(y)| = |y| + O(1) \]

★ fast decryption

\[ T_{\text{Dec}} = O(T) \]

★ adaptive security & minimal assumption
What do we want for a PHFE? (continued)

★ expressive functionality supports RAM computation with unbounded output length

★ short keys / ciphertexts

\[ |sk_f| = O(1) \]
\[ |ct_x(y)| = |y| + O(1) \]

★ fast decryption

\[ T_{Dec} = O(T) \]

★ 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

\[ |\text{mpk}| = O(1), \quad |\text{sk}_f| = O(1), \quad |\text{ct}_{x}(y)| = 2|y| + O(1), \]
\[ T_{\text{KeyGen}} = O(|f|), \quad T_{\text{Enc}} = O(|x| + |y|), \]
\[ T_{\text{Dec}} = O(T + |f| + |x| + |y|). \]
Our Results: Nearly Optimal PHFE for RAM

(weakly selective 1-key FE with $T_{\text{Enc}} = |f|^{1-\varepsilon}$ for circuits)

“obfuscation-minimum” FE

$\implies$ polynomially secure FE for circuits

$\implies$ adaptively secure PHFE for RAM with

- $|\text{mpk}| = O(1)$,
- $|\text{sk}_f| = O(1)$,
- $|\text{ct}_x(y)| = 2|y| + O(1)$,
- $T_{\text{KeyGen}} = O(|f|)$,
- $T_{\text{Enc}} = O(|x| + |y|)$,
- $T_{\text{Dec}} = O(T + |f| + |x| + |y|)$. 
Our Results: Nearly Optimal PHFE for RAM

(weakly selective 1-key FE with $T_{\text{Enc}} = |f|^{1-\varepsilon}$ for circuits)

“obfuscation-minimum” FE [long line of prior works]

$\implies$ polynomially secure FE for circuits

$\implies$ adaptively secure PHFE for RAM with

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

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

$T_{\text{Dec}} = O(T + |f| + |x| + |y|)$
Our Results: Nearly Optimal PHFE for RAM

(weakly selective 1-key FE with $T_{Enc} = |f|^{1-\varepsilon}$ for circuits)

“obfuscation-minimum” FE [long line of prior works]

$\implies$ polynomially secure FE for circuits

$\implies$ adaptively secure PHFE for RAM with

$|mpk| = O(1)$, $|sk_f| = O(1)$, $|ct_x(y)| = 2|y| + O(1)$,

$T_{KeyGen} = O(|f|)$, $T_{Enc} = O(|x| + |y|)$, $T_{Dec} = O(T + |f| + |x| + |y|)$

necessary / barrier
Select Related Works on FE

| for     | adaptive | $|sk_f|$ | $|ct_x(y)|$ | $T_{Dec}$ | assumptions |
|---------|----------|--------|-----------|-----------|-------------|
| RAM     | this     | 0(1)   | 2$|y|$ + 0(1) | 0($T + |f| + |x| + |y|$) | FE          |
| long output |          |        |           |           |             |
Select Related Works on FE

| for                  | adaptive | $|sk_f|$  | $|ct_x(y)|$  | $T_{Dec}$                                  | assumptions       |
|----------------------|----------|----------|--------------|-------------------------------------------|-------------------|
| RAM long output      | this     | $0(1)$   | $2|y| + 0(1)$ | $O(T + |f| + |x| + |y|)$                       | FE                |
| RAM                  | ACFQ     | poly($|f|$) | poly($|y|$)   | $T \text{ poly}(|f|)$                  | PK-DE-PIR + FE    |
## Select Related Works on FE

| for         | adaptive | $|sk_f|$       | $|ct_x(y)|$               | $T_{Dec}$                       | assumptions                        |
|-------------|----------|--------------|-------------------------|-------------------------------|-----------------------------------|
| RAM long output | this     | $0(1)$       | $2|y| + 0(1)$            | $0(T + |f| + |x| + |y|)$ | FE                                |
| RAM         | ACFQ     | $\text{poly}(|f|)$ | $\text{poly}(|y|)$ | $T\text{ poly}(|f|)$ | PK-DE-PIR + FE                    |
| TM          | AS       | $\text{poly}(|f|)$ | $\text{poly}(|y|)$ | $T\text{ poly}(|f|, |y|)$ | $iO$                              |
|             | AJS      | $c|f| + 0(1)$ | $c|y| + 0(1)$           | $T\text{ poly}(|f|, |y|)$ | subexp $iO$                       |
|             | AM       | $\text{poly}(|f|)$ | $O(|y|)$                | $T\text{ poly}(|f|, |y|)$ | dist. ind. FE                     |
|             | KNTY     | $\text{poly}(|f|)$ | $\text{poly}(|y|)$ | $T\text{ poly}(|f|, |y|)$ | 1-key sel. FE                     |
### Select Related Works on FE

| for         | adaptive | $|sk_f|$ | $|ct_x(y)|$ | $T_{Dec}$                              | assumptions                                      |
|-------------|----------|---------|-------------|----------------------------------------|--------------------------------------------------|
| RAM long output | this     | $O(1)$  | $2|y| + O(1)$ | $O(T + |f| + |x| + |y|)$ | FE                                               |
| RAM         | ACFQ     | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|)$ | PK-DE-PIR + FE                                    |
| TM          | AS       | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|, |y|)$ | $iO$                                            |
| TM          | AJS      | $c|f| + O(1)$ | $c|y| + O(1)$ | $T \text{ poly}(|f|, |y|)$ | subexp $iO$                                      |
| TM          | AM       | poly($|f|$) | $O(|y|)$   | $T \text{ poly}(|f|, |y|)$ | dist. ind. FE                                    |
| TM          | KNTY     | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|, |y|)$ | 1-key sel. FE                                    |
| circuit     | GGHRSW   | poly($|C|$) | poly($|y|$) | poly($|C|$) | $iO$                                            |
| circuit     | KNTY     | poly($|C|$) | poly($|y|$) | poly($|C|$) | 1-key sel. FE                                    |
| circuit     | GWZ      | poly($|C|$) | $|y| + O(1)$ | poly($|C|$) | $iO$                                            |
### Significant Improvement and “Two Clouds”

| for | adaptive | $|sk_f|$ | $|ct_x(y)|$ | $T_{Dec}$ | assumptions |
|-----|----------|--------|--------|----------|-------------|
| RAM long output | **this** | 0(1) | $2|y| + 0(1)$ | $O(T + |f| + |x| + |y|)$ | FE |
| RAM | ACFQ | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|)$ | PK-DE-PIR + FE |
| TM | AS | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|, |y|)$ | $i\Omega$ |
|  | AJS | $\sqrt[\frac{1}{2}]{|y|}$ | poly($|y|$) | $T \text{ poly}(|f|, |y|)$ | subexp $i\Omega$ |
|  | AM | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|, |y|)$ | dist. ind. FE |
|  | KNTY | poly($|f|$) | poly($|y|$) | $T \text{ poly}(|f|, |y|)$ | 1-key sel. FE |
| circuit | GGHRSW | poly($|C|$) | poly($|y|$) | poly($|C|$) | $i\Omega$ |
|  | KNTY | **this** | poly($|C|$) | poly($|y|$) | poly($|C|$) | 1-key sel. FE |
|  | GWZ | poly($|C|$) | $|y| + O(1)$ | poly($|C|$) | $i\Omega$ |

**improvement from polynomial to nearly optimal efficiency**
## Significant Improvement and “Two Clouds”

### Table: Adaptive Security and Efficiency

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RAM long output</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adaptive</td>
<td>$</td>
<td>sk_f</td>
</tr>
<tr>
<td><strong>this</strong></td>
<td>$O(1)$</td>
<td>$2</td>
</tr>
<tr>
<td>$T_{Dec}$</td>
<td>$O(T +</td>
<td>f</td>
</tr>
<tr>
<td><strong>assumptions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FE</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>ACFQ</td>
<td>$T \ poly(</td>
</tr>
<tr>
<td>AS</td>
<td>$\checkmark$</td>
<td>$T \ poly(</td>
</tr>
<tr>
<td>AM</td>
<td>$\checkmark$</td>
<td>$T \ poly(</td>
</tr>
<tr>
<td>KNTY</td>
<td>$\checkmark$</td>
<td>$T \ poly(</td>
</tr>
<tr>
<td><strong>improvement from polynomial to nearly optimal efficiency</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KNTY</td>
<td>GGHRSW</td>
<td>$T \poly(</td>
</tr>
<tr>
<td>circuit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GWZ</td>
<td>$\checkmark$</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

> ✓ obtainable if abandoning adaptive security & long output

---

### Footnotes

- Improvement from polynomial to nearly optimal efficiency
- ✓ obtainable if abandoning adaptive security & long output
## Significant Improvement and “Two Clouds”

| for          | adaptive | $|sk_f|$    | $|ct_x(y)|$    | $T_{Dec}$                        | assumptions |
|--------------|----------|------------|---------------|----------------------------------|-------------|
| RAM          | this     | $O(1)$     | $2|y| + O(1)$  | $O(T + |f| + |x| + |y|)$  | ?           |
| long output  |          |            |               |                                  |             |
| RAM          | ACFQ     | poly($|f|$) | poly($|y|$)   | $T$ poly($|f|$)                  | PK-DE-PIR + FE |
| TM           | AS       | poly($|f|$) | poly($|y|$)   | $T$ poly($|f|, |y|$)            | $iO$        |
|              | AJS      | poly($|f|$) | poly($|y|$)   | $T$ poly($|f|, |y|$)            | subexp $iO$ |
|              | AM       | poly($|f|$) | poly($|y|$)   | $T$ poly($|f|, |y|$)            | dist. ind. FE |
|              | KNTY     | poly($|f|$) | poly($|y|$)   | $T$ poly($|f|, |y|$)            | 1-key sel. FE |
| circuit      | GGHRSW   | poly($|C|$) | poly($|y|$)   | poly($|C|$)                      | $iO$        |
|              | KNTY     | poly($|C|$) | poly($|y|$)   | poly($|C|$)                      | 1-key sel. FE |
|              | GWZ      | poly($|C|$) | $|y| + O(1)$  | poly($|C|$)                      | $iO$        |

**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

For FE or PHFE for RAM, if

\[ |sk_f| = 0(|f|^A), \quad T_{Dec} = (T + |f|^B + |y|) \Omega(|x|^C) \]

then \( A \geq 1 \) or \( B \geq 1 \).
Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

For FE or PHFE for RAM, if

\[ |sk_f| = O(|f|^A), \quad T_{\text{Dec}} = (T + |f|^B + |y|) O(|x|^C) \]

then \( A \geq 1 \) or \( B \geq 1 \).

For PHFE for RAM, if

\[ |ct_{x}(y)| = O(|x|^A |y|^C), \quad T_{\text{Dec}} = (T + |f| + |x|^B) O(|y|^C) \]

then \( A \geq 1 \) or \( B \geq 1 \).
Results: **Unconditional** Space-Time Trade-Offs for (PH-)FE

For FE or PHFE for RAM, if

\[ |sk_f| = O(|f|^A), \quad T_{\text{Dec}} = (T + |f|^B + |y|) O(|x|^C) \]

then \( A \geq 1 \) or \( B \geq 1 \).

For PHFE for RAM, if

\[ |ct_x(y)| = O(|x|^A |y|^C), \quad T_{\text{Dec}} = (T + |f| + |x|^B) O(|y|^C) \]

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**

For FE or PHFE for RAM, if

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

then \( A \geq 1 \) or \( B \geq 1 \).

For PHFE for RAM, if

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

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**

For FE or PHFE for RAM, if

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

then \( A \geq 1 \) or \( B \geq 1 \).

For PHFE for RAM, if

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

then \( A \geq 1 \) or \( B \geq 1 \).

\[ \text{“Component size and decryption time cannot both be sublinear in } f, x. \text{”} \]

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

\[ y? \text{ Linear-size components? Optimal decryption time? Connections to DE-PIR.} \]
Doubly Efficient Private Information Retrieval

DE-PIR \( D \)
Doubly Efficient Private Information Retrieval

DE-PIR $D$ Process $\tilde{D}$

$k$
Doubly Efficient Private Information Retrieval

DE-PIR $D \xrightarrow{\text{Process}} \tilde{D} \\
\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad k \xrightarrow{\text{Query}(i)} ct$
Doubly Efficient Private Information Retrieval

DE-PIR

\(D\xrightarrow{\text{Process}} \tilde{D} \xrightarrow{\text{Resp}} D[i]\)

\(D\)

\(k\)

\(\text{ct}\)

\(\text{Query}(i)\)
Doubly Efficient Private Information Retrieval

\[
\begin{align*}
\text{DE-PIR} & \quad D \xrightarrow{\text{Process}} \tilde{D} \xrightarrow{\text{Resp}} D[i] \\
\text{client efficiency} & \quad |k| = O(1) \text{ and } T_{\text{Query}} = O(|D|^{1-\varepsilon}) \\
\text{server efficiency} & \quad T_{\text{Resp}} = O(|D|^{1-\varepsilon})
\end{align*}
\]
Doubly Efficient Private Information Retrieval

\[ |k| = O(1) \text{ and } T_{\text{Query}} = O(|D|^{1-\varepsilon}) \]

\[ T_{\text{Resp}} = O(|D|^{1-\varepsilon}) \]

security \( \tilde{D}, \{\text{ct}(i_q)\} \) hides \( \{i_q\} \)
Doubly Efficient Private Information Retrieval

\[
\text{DE-PIR} \quad D \xrightarrow{\text{Process}} \tilde{D} \xrightarrow{\text{Resp}} D[i]
\]

- **client efficiency**: \(|k| = O(1) \text{ and } T_{\text{Query}} = O(|D|^{1-\varepsilon})\)
- **server efficiency**: \(T_{\text{Resp}} = O(|D|^{1-\varepsilon})\)
- **security**: \(\tilde{D}, \{\text{ct}(i_q)\} \text{ hides } \{i_q\}\)
- **dream efficiency**: \(|\tilde{D}| = O(|D|) \text{ and } T_{\text{Query}}, T_{\text{Resp}} = O(1)\)
Doubly Efficient Private Information Retrieval

DE-PIR $D$ Process $\tilde{D}$ 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** $\tilde{D}, \{\text{ct}(i_q)\} \text{ hides } \{i_q\}$
- **dream efficiency** $|\tilde{D}| = O(|D|)$ 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 \textbf{sufficiently} expressive secure PHFE with

\[ |ct_x(y)| = |x|^A \text{poly}(|y|), \quad T_{\text{Dec}} = |x|^B \text{poly}(T, |f|, |y|), \]

or

\[ |ct_x(y)| = |y|^A \text{poly}(|x|), \quad T_{\text{Dec}} = |y|^B \text{poly}(T, |f|, |x|) \]

for \( B < 1 \), then there exists \textbf{secret-key} DE-PIR with

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

essentially also proven in ACFQ
Results: Optimal Decryption Time Implies DE-PIR

Assuming mildly expressive secure PHFE with

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

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

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

Assuming sufficiently expressive secure PHFE with

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

or

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

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

$$|\tilde{D}| = |D| + O(|D|^A), \quad T_{\text{Query}} = O(1), \quad T_{\text{Resp}} = O(|D|^B).$$
Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

\[ \text{subexp. secure FE for circuits} \]

\[ \Rightarrow \text{subexp. secure } i\mathcal{O} \text{ for RAM with} \]

\[ |\tilde{M}| = 2|M| + \text{poly}(|D|) \]
Results: Constant-Overhead $i\mathcal{O}$ & ABE for RAM

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

$\Rightarrow$ subexp. secure Fe for circuits

$|\tilde{M}| = 2|M| + \text{poly}(|D|)$
Results: Constant-Overhead $iO$ & ABE for RAM

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

$\Rightarrow$ subexp. secure $iO$ for RAM with $|\tilde{M}| = 2|M| + \text{poly}(|D|)$

| ABE for RAM   | $|sk_f|$ | $|ct_x|$ | $T_{Dec}$ |
|---------------|---------|---------|----------|
| from PHFE     | $O(1)$  | $O(1)$  | $O(T + |f| + |x|)$ |
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

$\Rightarrow$ subexp. secure $i\mathcal{O}$ for RAM with $|\tilde{M}| = 2|M| + \text{poly}(|D|)$

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

can move between size and time

(adaptive, based on FE for circuits)
Results: Constant-Overhead $iO$ & ABE for RAM

| ABE for RAM          | $|\text{sk}_f|$ | $|\text{ct}_x|$ | $T_{\text{Dec}}$ |
|----------------------|----------------|----------------|-----------------|
| from PHFE            | $0(1)$         | $0(1)$         | $0(T + |f| + |x|)$ |
| $|f| + 0(1)$          | $0(1)$         | $0(T + |x|)$   |
| minor tweaks         | $0(1)$         | $|x| + 0(1)$   | $0(T + |f|)$    |
| $|f| + 0(1)$          | $|x| + 0(1)$   | $0(T')$        |

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

$\Rightarrow$ subexp. secure $iO$ for RAM with $|\tilde{M}| = 2|M| + \text{poly}(|D|)$

4 new! ABE for RAM

(can move between size and time)

(adaptive, based on FE for circuits)
Results: Constant-Overhead $iO$ & ABE for RAM

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

⇒ subexp. secure $iO$ for RAM with $|\tilde{M}| = 2|M| + \text{poly}(|D|)$

| ABE for RAM | $|sk_f|$ | $|ct_x|$ | $T_{Dec}$ |
|--------------|---------|---------|-----------|
| from PHFE    | $0(1)$  | $0(1)$  | $0(T + |f| + |x|)$ |
| minor tweaks | $|f| + 0(1)$ | $0(1)$  | $0(T + |x|)$ |
|              | $0(1)$  | $|x| + 0(1)$ | $0(T + |f|)$ |
|              | $|f| + 0(1)$ | $|x| + 0(1)$ | $0(T)$ (X) |

(can move between size and time)

(adaptive, based on FE for circuits)
Where we stand now: \((\text{PH-})\text{FE}\)

\[
y\text{-independent Dec}
\]

\[
\begin{array}{c}
\uparrow \\
morally \\
\downarrow \\
\text{DE-PIR}
\end{array}
\]
Where we stand now: \((PH-)FE\)

\(y\)-independent Dec

↑
morally

↓
DE-PIR

size exponent

1

0

time exponent

1

dependency on \(f\) or \(x\)

characterized by this work
Where we stand now: \((\text{PH-)FE}\)

\[y\text{-independent Dec} \uparrow \text{morally} \downarrow \text{DE-PIR}\]

dependency on \(f\) or \(x\) characterized by this work
Where we stand now: (PH-)FE

\[ \begin{aligned}
\text{y-independent Dec} & \quad \uparrow \text{morally} \quad \downarrow \\
\text{DE-PIR} &
\end{aligned} \]

1. size exponent

\[ \begin{aligned}
0 & \quad \square \quad \times \quad \checkmark \\
1 &
\end{aligned} \]

1. time exponent

dependency on \( f \) or \( x \)

classified by this work
Where we stand now: \((PH-)\text{FE}\)

\[ y \text{-independent Dec} \]

\[
\begin{align*}
\uparrow & \quad \text{morally} \\
\downarrow & \\
\text{DE-PIR}
\end{align*}
\]

DE-PIR dependency on \(f\) or \(x\) characterized by this work

impossible

\[ \text{achieved} \]

size exponent

\[ \text{time exponent} \]

dependency on \(f\) or \(x\)

characterized by this work

characterized by this work

dependency on \(f\) or \(x\)

characterized by this work

dependency on \(f\) or \(x\)

characterized by this work

dependency on \(f\) or \(x\)

characterized by this work
Where we stand now: ABE

dependency on $f$ or $x$

$T_{Dec} = O(T + \cdots)$
Where we stand now: ABE

dependency on $f$ or $x$

$T_{\text{Dec}} = O(T + \cdots)$
Where we stand now: ABE

dependency on $f$ or $x$

$$T_{Dec} = O(T + \cdots)$$
Where we stand now: ABE

\[
T_{\text{Dec}} = O(T + \cdots)
\]
Proof Sketch of \textbf{Unconditional} Lower Bound

\[ |sk_f| = |f|^A, \quad T_{\text{Dec}} = T + |f|^B + |x| + |y|, \quad A, B < 1. \]
Proof Sketch of **Unconditional** Lower Bound

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

\[
f = R \in \{0,1\}^N, \quad x = \bot, \quad y_0 = (I, w), \quad y_1 = z.\]
Proof Sketch of **Unconditional** Lower Bound

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

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

\[ z \in \{0,1\}^n \]

\[ I \subseteq [N] \text{ is of size } n \quad w \in \{0,1\}^n \]
Proof Sketch of **Unconditional** Lower Bound

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

\[ f = R \in \{0,1\}^N, \quad I \subseteq [N] \text{ is of size } n \quad \text{w} \in \{0,1\}^n \]

\[ x = \bot, \quad y_0 = (I, w), \quad y_1 = z. \]

\[ f(x, y) = \begin{cases} R[I] \oplus w, & y = (I, w); \\ z, & y = z. \end{cases} \quad z \in \{0,1\}^n \]
Proof Sketch of Unconditional Lower Bound

$$|sk_f| = |f|^A,$$

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

$$= N^A \ll n$$  

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

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

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

$$x = \bot, \quad y_0 = (I,w), \quad y_1 = z.$$ 

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

\[ |\text{sk}_f| \ll n, \quad T_{\text{Dec}} \ll N. \]

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

\[ |\text{sk}_f| \ll n, \quad T_{\text{Dec}} \ll N. \]

How much of \( R[I] \) does \( \text{Dec}^R(\text{sk}_f, ct) \) 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)

\[ |\text{sk}_f| \ll n, \quad T_{\text{Dec}} \ll N. \]

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

- \((\text{sk}_f, \text{ct})\) 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 \(z = R[I] \oplus w\)

How much of \(R[I]\) does \(\text{Dec}^R(\text{sk}_f, \text{ct})\) read?
Unconditional Lower Bound (continued)

|sk_f| ≪ n, \quad T_{Dec} ≪ N.

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

(\(sk_f, ct\)) contains \(|n|\) bits of \(R[I]\) (\(|n|\) bits)
must read **almost all** of \(R[I]\) (**incompressibility argument**)

When \(y = y_1 = z\):
behavior of \(Dec^R(\sk_f, ct)\) **independent** of \(I\)
can only read \(|I| \cdot \frac{T_{Dec}}{N} \ll n\) 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 \textbf{DE-PIR}

\[ |\text{sk}_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{poly}(T, |x|, |y|), \quad B < 1. \]
Proof Sketch of Technical Barrier of DE-PIR

\[ |\text{sk}_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{poly}(T, |x|, |y|), \quad B < 1. \]

\[ f = D, \quad x = \bot, \quad y = i, \quad f_D(x, y) = D[i]. \]
Proof Sketch of Technical Barrier of DE-PIR

\[ |sk_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{poly}(T, |x|, |y|), \quad B < 1. \]

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

Preprocessing. \[ \tilde{D} = (D, \text{fes} \ f_f), \quad k = \text{fempk}. \]

\[ |\tilde{D}| = |D| + |D|^A \]
Proof Sketch of Technical Barrier of DE-PIR

\[ |\text{sk}_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{poly}(T, |x|, |y|), \quad B < 1. \]

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

Preprocessing. \[ \tilde{D} = (D, \text{fesk}_f), \quad k = \text{fempk}. \]

\[ |\tilde{D}| = |D| + |D|^A \]

Querying. \[ \text{ct} = \text{fect}(i). \quad T_{\text{Query}} = O(1) \]
Proof Sketch of Technical Barrier of \textbf{DE-PIR}

\[ |sk_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{poly}(T, |x|, |y|), \quad B < 1. \]

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

\textbf{Preprocessing.} \quad \tilde{D} = (D, \text{fesk}_f), \quad k = \text{fempk}.

\[ |\tilde{D}| = |D| + |D|^A \]

\textbf{Querying.} \quad ct = \text{fect}(i). \quad \quad T_{\text{Query}} = O(1)

\textbf{Responding.} \quad \text{Dec}^D(\text{fesk}_f, \text{fect}). \quad \quad T_{\text{Resp}} = |D|^B
Proof Sketch of Technical Barrier of DE-PIR

\[ |\text{sk}_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{ poly}(T, |x|, |y|), \quad B < 1. \]

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

Preprocessing. \[ \tilde{D} = (D, \text{fes}k_f), \quad k = \text{fempk}. \]
\[ |\tilde{D}| = |D| + |D|^A \]

Querying. \[ \text{ct} = \text{fect}(i). \]

Responding. \[ \text{Dec}^D(\text{fes}k_f, \text{fect}). \]

\[ T_{\text{Query}} = O(1) \]
\[ T_{\text{Resp}} = |D|^B \]

⚠️ IND-secure, selective, non-output-hiding, (if SK) non-database-hiding.
Proof Sketch of Technical Barrier of **DE-PIR**

\[ |\text{sk}_f| = |f|^A, \quad T_{\text{Dec}} = |f|^B \text{poly}(T, |x|, |y|), \quad B < 1. \]

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

**Preprocessing.** \[ \tilde{D} = (D, \text{fesk}_f), \quad k = \text{fempk}. \]
\[ |\tilde{D}| = |D| + |D|^A \]

**Querying.** \[ \text{ct} = \text{fect}(i). \quad T_{\text{Query}} = O(1) \]

**Responding.** \[ \text{Dec}^D(\text{fesk}_f, \text{fect}). \quad T_{\text{Resp}} = |D|^B \]

⚠️ **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.

- $(f)$ input tape
- $(D)$ input tape
- Working tape

(step circuit) (for universal RAM)
Core of PHFE: Laconic Garbled (Multi-Tape) RAM

Step 1: Formulate the right definition.

Step 2: Achieve it.

(f) input tape

(D) input tape

working tape

old state

previous read

step circuit
(for universal RAM)

new state

next read/write

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

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

**Step 2:** Achieve it.

---

(f) input tape

(D) input tape

working tape

old state

previous read

new state

next read/write

output

<table>
<thead>
<tr>
<th>step circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td>(for universal RAM)</td>
</tr>
</tbody>
</table>
Core of PHFE: **Laconic Garbled (Multi-Tape) RAM**

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

Step 2: **Achieve it.**

\[
\begin{align*}
\text{(f) input tape} & & \cdots & & \text{Compress} & & \text{Digest}_1 \\
\text{(D) input tape} & & \cdots & & \text{Compress} & & \text{Digest}_2 \\
\text{working tape} & & \cdots & & \text{step circuit} \\
& & & & \text{new state} & & \text{output} \\
& & & & \text{old state} & & \text{previous read}
\end{align*}
\]

\[|\text{digest}| = O(1)\]
Core of PHFE: Laconic Garbled (Multi-Tape) RAM

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

Step 2: **Achieve it.**

(f) input tape

(D) input tape

working tape

<table>
<thead>
<tr>
<th>step circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td>(for universal RAM)</td>
</tr>
</tbody>
</table>

Compress \( \Rightarrow \) digest\(_1\) \( \Rightarrow \) \( \hat{M} \)

Compress \( \Rightarrow \) digest\(_2\)

| digest| = \(O(1)\)

Garble

\( T_{Garble} = poly(|M|) \)
Core of PHFE: Laconic Garbled (Multi-Tape) RAM

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

Step 2: **Achieve it.**

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

\[ M^{f,D}() \]

\[ \text{Eval}^{f,D} \]

\[ |\text{digest}| = O(1) \]

Compress

digest\(_1\)

\(\widehat{M}\)

Compress

digest\(_2\)

\[ T_{\text{Garble}} = \text{poly}(|M|) \]

\[ \text{Garble} \]

\( (f) \) input tape

... 

... 

\( (D) \) input tape

\[ \text{step circuit} \] (for universal RAM)

new state

next read/write

output

old state

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

Step 1: Formulate the right definition.

Step 2: Achieve it.

\( (f) \) input tape

\( (D) \) input tape

working tape

\( \text{step circuit} \)
(for universal RAM)

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

Security is IND-based, not SIM-based.

\[ M^{f,D}() \]

\( \text{Eval}^{f,D} \)

\( \widehat{M} \)

\( |\text{digest}| = O(1) \)

\[ T_{\text{Garble}} = \text{poly}(|M|) \]
Core of PHFE: Laconic Garbled (Multi-Tape) RAM

Step 1: Formulate the right definition.

Step 2: Achieve it.

Security is IND-based, not SIM-based.

important for nearly optimal efficiency

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

\[ M^{f,D}() \]

Eval^{f,D} \rightarrow \hat{M}

\[ |\text{digest}| = O(1) \]

\[ T_{\text{Garble}} = \text{poly}(|M|) \]

(f) input tape

(D) input tape

working tape

step circuit (for universal RAM)

compress

compress

compress

new state

next read/write

output

old state

previous read

reusable

digest_1

digest_2
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 $T_{\text{Dec}}$ from/and dream DE-PIR.
2. **Achieve** rate-1 in $y$ with adaptive security and/or long output.
3. **Tight relation** between optimal $T_{\text{Dec}}$ and DE-PIR.

FE for circuits + **PK-DE-PIR** $\Rightarrow (x, y)$-optimal Dec time $\Rightarrow$ **SK-DE-PIR**.
FE for circuits + **SK-DE-PIR** $\Rightarrow$ ...?
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** $\Rightarrow$ (x, y)-optimal Dec time $\Rightarrow$ **SK-DE-PIR**.
   
   FE for circuits + **SK-DE-PIR** $\Rightarrow$ ...?
4. **Pin down** the exact Pareto frontier of efficiency.
   
   Demystify the **stripe area**.
Thanks!

ePrint 2022/1317 (revision coming soon)