Lightweight FHE-based Protocols
Achieving Results Consistency
for Data Encrypted under Different Keys

Marina Checri, Jean-Paul Bultel, Renaud Sirdey, Aymen Boudguiga

Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France
{marina.checri, jean-paul.bultel, renaud.sirdey, aymen.boudguiga}@cea.fr

October 17, 2023
The Need for Homomorphic Encryption Protocols

What are we talking about?

\[ x + y \approx x^y \approx x^y \]

What for?

Data confidentiality during calculations

Typically, for Cloud Computing
The Need for Homomorphic Encryption Protocols

What are we talking about?

Data confidentiality during calculations

Typically, for Cloud Computing
What are we talking about?

\[ [x] + [y] \rightarrow [x + y] \]
\[ [x] \times [y] \rightarrow [x \times y] \]
The Need for Homomorphic Encryption Protocols

What are we talking about?

\[ x + y \rightarrow x + y \]
\[ x \times y \rightarrow x \times y \]

\[ m \xrightarrow{f} f(m) \]
The Need for Homomorphic Encryption Protocols

What are we talking about?

\[ x + y \rightarrow x + y \]
\[ x \times y \rightarrow x \times y \]

\[ m \xrightarrow{f} f(m) \]

Data confidentiality during calculations

Typically, for Cloud Computing

Marina Checri
What are we talking about?

\[
\begin{align*}
[x] + [y] & \rightarrow [x + y] \\
[x] \times [y] & \rightarrow [x \times y]
\end{align*}
\]

\[
\begin{align*}
m & \xrightarrow{f} f(m) \\
[m] & \xrightarrow{\text{Eval}(f, [m])} [f(m)]
\end{align*}
\]
What are we talking about?

\[
[x] + [y] \rightarrow [x + y] \\
[x] \times [y] \rightarrow [x \times y]
\]
The Need for Homomorphic Encryption Protocols

What are we talking about?

\[
\begin{align*}
[x] + [y] &\rightarrow [x + y] \\
[x] \times [y] &\rightarrow [x \times y]
\end{align*}
\]

What for?

Data confidentiality during calculations

Typically, for Cloud Computing

Marina Checri

FHE-based multi-user protocols

October 17, 2023
The Need for Homomorphic Encryption Protocols

What are we talking about?

\[
\begin{align*}
[x] + [y] &\rightarrow [x + y] \\
[x] \times [y] &\rightarrow [x \times y]
\end{align*}
\]

What for?

Data confidentiality during calculations

Typically, for Cloud Computing

Marina Checri
The Need for Homomorphic Encryption Protocols

What are we talking about?

\[ [x] + [y] \rightarrow [x + y] \]

\[ [x] \times [y] \rightarrow [x \times y] \]

What for?

Data confidentiality *during* calculations

Typically, for Cloud Computing
Did you say **multi-user**?
Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...
A Multi-user / Multi-key Framework

Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

Medical secrecy
Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user → Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

Medical secrecy

Financial domain
Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...
Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user → Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...
How can users detect those encrypted messages intended for them?
How can users detect those encrypted messages intended for them?

Detect key inconsistency with a padding of zeroes
How can users detect those encrypted messages intended for them?

Detect key inconsistency with a padding of zeroes

- Decrypting zero with a wrong key yields a random number
- Zero padding makes it possible to sort valid results from random ones
- Assuming a uniform distribution over $\mathbb{F}_q$
  - When decrypting $[00 \cdots 0]$, the probability of a false positive is $\frac{1}{q^\ell}$
A Use Case: Regulate Accesses to Secured Rooms

The server:

- grants or denies room access, according to user’s accreditation.
- must learn nothing about the admission policy or room attendance.
An Incremental Approach: Scenarii 1 and 2

- Produce consistent results derived only from data encrypted under the requester’s key.

- Avoid transmissions of evks by the contributors.
An Incremental Approach: Scenario 3

Scenario 3 for \( \alpha = 0 \)

- Result compactness
- No need for post-decryption padding verification for the requester
Our Use Case is Addressed by Scenario 3

(a) Use case

\[
\sum [d \leq T]_{D_1} = [1]_{D_1}
\]

\[
[d(c, X_2) \leq T]_{D_1} = [1]_{D_1}
\]

\[
[d(c, X_0) \leq T]_{D_1} = [0]_{D_1}
\]

\[
\ldots
\]

\[
\sum_{i \text{ such that } \text{chk}([0], [0])} \sum_{i} f(x_i, y_i) \leftarrow \sum_{i} \text{chk}([0], [0]) \cdot f(x_i, y_i) + [0]
\]

(b) Scenario 3 - last scenario

\[
[b] \cdot [m] : [\alpha] \iff ([m] - [\alpha]) \cdot [b] + [\alpha] = \begin{cases} [m] & \text{if } b = 1 \\ [\alpha] & \text{if } b = 0 \end{cases}
\]
Key Forcing Subtility with TFHE

FHE and noise
- add noise for security

Homomorphic operations
- increase the noise

Bootstrapping
- to reduce the noise
  = homomorphic decryption

TFHE Bootstrapping key
- Bootstrapping key = evaluation key
- Bootstrapping key = encryption of the private key

Multi-user framework
- The encryption key used does not always match the bootstrapping key.
TFHE is not natively designed for multi-user operations.
FHE and noise

<table>
<thead>
<tr>
<th>FHE encryption</th>
<th>add noise for security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homomorphic operations</td>
<td>increase the noise</td>
</tr>
<tr>
<td>Bootstrapping</td>
<td>to reduce the noise</td>
</tr>
<tr>
<td></td>
<td>= homomorphic decryption</td>
</tr>
</tbody>
</table>
Key Forcing Subtlety with TFHE

**FHE and noise**

- **FHE encryption** → add noise for security
- **Homomorphic operations** → increase the noise
- **Bootstrapping** → to reduce the noise
  = homomorphic decryption

**TFHE Bootstrapping key**

- Bootstrapping key = evaluation key
- Bootstrapping key = encryption of the private key
Key Forcing Subtlety with TFHE

FHE and noise

- FHE encryption → add noise for security
- Homomorphic operations → increase the noise
- Bootstrapping → to reduce the noise
  = homomorphic decryption

TFHE Bootstrapping key

- Bootstrapping key = evaluation key
- Bootstrapping key = encryption of the private key

Multi-user framework

→ The encryption key used does not always match the bootstrapping key.
Key Forcing Subtlety with TFHE

\[
JFK(\hat{\otimes}_{bk_{RK}}, [a]_{pk_{RK}}, [b]_{pk_{RK}}) \\
= [a]_{pk_{RK}} \hat{\otimes}_{bk_{RK}} ([1]_{pk_{RK}} \&_{bk_{RK}} [b]_{pk_{RK}}) \\
= [a \otimes b]_{pk_{RK}}
\]

\[
JFK(\hat{\otimes}_{bk_{RK}}, [a]_{pk_{RK}}, [b]_{pk_{WK}}) \\
= [a]_{pk_{RK}} \hat{\otimes}_{bk_{RK}} ([1]_{pk_{RK}} \&_{bk_{RK}} [b]_{pk_{WK}}) \\
= [a \otimes b]_{pk_{RK}} \\
= [\$]_{pk_{RK}}
\]
Time Analysis of Scenarii 1 and 2

![Graph showing time analysis for Scenarios 1 and 2.]

**Scenario 1**
- **Evaluations**
- **Decryptions**

**Scenario 2**
- **Evaluations**
- **Decryptions**

**Number of database records**
- 5
- 10
- 50
- 100

**Time (min:sec)**
- 00:00
- 00:05
- 00:10
- 00:15
- 00:20
- 00:25
- 00:30
- 00:35
- 00:40
- 00:45
- 00:50
- 00:55
- 01:00
- 01:05
- 01:10
- 01:15
- 01:20
- 01:25

Marina Checri
FHE-based multi-user protocols
October 17, 2023
Time Analysis of Scenario 3

Scenario 3 - TFHE

![Chart showing time analysis for Scenario 3 with different numbers of database records and bits of padding. The chart indicates that the time increases with the number of records and padding size.]

Number of database records:
- Yellow: 5 records
- Orange: 10 records
- Red: 50 records
- Purple: 100 records

Bits of padding:
- 8
- 16
- 32
- 64
Key Takeaways

- Scenarii of increasing practical relevance and usefulness
- Lightweight multi-user setting (one requester per request)
- Calculations on data from different contributors under different keys
- Data and results confidentiality
- Results consistency
- Untraceability of contributors by requesters
Thank you for your kind attention!