USING STATE-OF-THE-ART ENCRYPTION TO GAIN NEW INSIGHTS FROM VIDEO GAME DATA

Supervisors: Prof Alex Wade & Prof Delaram Kahrobaei
Student: Dewi Jones
WHAT IS ENCRYPTION?

Plaintext: Here’s my private data

Encrypt

Key

Ciphertext: U2sdGVkX1o KSus91yVnP

Decrypt

Key

Plaintext: Here’s my private data
FULLY HOMOMORPHIC ENCRYPTION?

What?

\[ E(x) + E(y) = E(x + y) \]
\[ E(x) \cdot E(y) = E(xy) \]

How?

Why?
FULLY HOMOMORPHIC ENCRYPTION?

What?

\[ E(x) + E(y) = E(x + y) \]

\[ E(x) \cdot E(y) = E(xy) \]

How?

Why?
THE PROJECT - OVERVIEW

E(DATA) → E(F(x)) → F(x)

E(F(x)) → F()?
### THE PROJECT - DATABASE

<table>
<thead>
<tr>
<th>AccountID</th>
<th>GameID</th>
<th>ELO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100023</td>
<td>1014</td>
</tr>
<tr>
<td>3</td>
<td>150035</td>
<td>1203</td>
</tr>
<tr>
<td>9</td>
<td>108412</td>
<td>990</td>
</tr>
<tr>
<td>6</td>
<td>301234</td>
<td>1400</td>
</tr>
<tr>
<td>3</td>
<td>578917</td>
<td>894</td>
</tr>
<tr>
<td>1</td>
<td>127593</td>
<td>1500</td>
</tr>
</tbody>
</table>
## THE PROJECT - DATABASE

<table>
<thead>
<tr>
<th>AccountID</th>
<th>GameID</th>
<th>ELO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1278648736</td>
<td>29376948475</td>
<td>937980981</td>
</tr>
<tr>
<td>2983749823</td>
<td>38093287423</td>
<td>239479382</td>
</tr>
<tr>
<td>2374928347</td>
<td>39274928347</td>
<td>293472934</td>
</tr>
<tr>
<td>1394872947</td>
<td>23849723987</td>
<td>023238473</td>
</tr>
<tr>
<td>1987394875</td>
<td>23984793847</td>
<td>293847924</td>
</tr>
<tr>
<td>3294872498</td>
<td>29834729834</td>
<td>2394872235</td>
</tr>
</tbody>
</table>
THE PROJECT - EXAMPLE

Operations: 
+/-  
X

<table>
<thead>
<tr>
<th>AccountID</th>
<th>GameID</th>
<th>ELO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1278648736</td>
<td>29376948475</td>
<td>937980981</td>
</tr>
<tr>
<td>2983749823</td>
<td>38093287423</td>
<td>239479382</td>
</tr>
<tr>
<td>2374928347</td>
<td>39274928347</td>
<td>293472934</td>
</tr>
<tr>
<td>1394872947</td>
<td>23849723987</td>
<td>023238473</td>
</tr>
<tr>
<td>1987394875</td>
<td>23984793847</td>
<td>293847924</td>
</tr>
<tr>
<td>3294872498</td>
<td>29834729834</td>
<td>2394872235</td>
</tr>
</tbody>
</table>
## THE PROJECT - EXAMPLE

<table>
<thead>
<tr>
<th>ELO</th>
</tr>
</thead>
<tbody>
<tr>
<td>937980981</td>
</tr>
<tr>
<td>239479382</td>
</tr>
<tr>
<td>293472934</td>
</tr>
<tr>
<td>02328473</td>
</tr>
<tr>
<td>293847924</td>
</tr>
<tr>
<td>2394872235</td>
</tr>
</tbody>
</table>
THE PROJECT - EXAMPLE

Sum of ELO

816214871628
<table>
<thead>
<tr>
<th>Sum of ELO</th>
</tr>
</thead>
<tbody>
<tr>
<td>7001</td>
</tr>
<tr>
<td>AccountID</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
THE PROJECT – PROOF OF CONCEPT

CORRELATION BETWEEN

SLOPE OF THE FIRST 10 GAMES

&

SUM OF THE LAST 10 GAMES (PER USER)
THE PROJECT – CHALLENGES

DIVISION

CONDITIONAL BRANCHING

```csharp
public void PerformOp(string operationName) {
    if (operationName == "Op1") {
        // something
    } else if (operationName == "Op2") {
        // something else
    } else {
        // default path
    }
}
```
THE PROJECT – DIVISION

DECIMAL EQUIVALENTS

\[
\frac{2}{10} = 2 \times \frac{1}{10} = 2 \times 0.1
\]

NEWTON-RAPHSON METHOD

\[
\log(a) - \log(b) = \log\left(\frac{a}{b}\right)
\]

\[
\frac{2}{x} = 2 \times \frac{1}{x} \approx 2 \times y
\]

where
\[
y_{i+1} = y_i + y_i(1-xy_i)
\]

LOGARITHMS
THE PROJECT – CONDITIONAL BRANCHING

FERMAT’S LITTLE THEOREM

\[ a^{p-1} \equiv 1 \mod p \]
\[ \text{e.g. } a^6 \equiv 1 \mod 7 \]

CREATES A 1 OR 0

\[ (x_1 - x_2)^{p-1} \equiv 1 \mod p \]
\[ \text{e.g. } (1D - \text{Entry})^6 \equiv 1 \mod 7 \]

SUM += COEFFICIENT * SUMMAND
WHAT NEXT?

Solidify the division alternatives

Implement more algorithms

Create packages for different languages and programs
THANK YOU!