Modes of operations for computing on encrypted data

Dragos Rotaru, N.P. Smart, and Martijn Stam

KU Leuven, University of Bristol
Multiparty computation hijacks FSE’18

Goal: Compute $F(a, b, c)$
What is the problem?
What is the problem?
What is the problem?

Enc + Enc + Enc = 42
What is the problem?

Enc(42)
What is the problem?

Enc(42)
What is the problem?

Enc(42) → Tag(E(42))
What is the problem?

For free: detect malicious encryption keys.

Enc(42) Tag(E(42))
Prior work – PRFs in MPC (CCS’16)

Enc(42) \quad \text{Tag}(\text{Enc}(42))

- MiMC
- Legendre PRF
Prior work – PRFs in MPC (CCS’16)

Enc(42) \textbf{Tag(Enc(42))}

M[1]

Enc
Prior work – PRFs in MPC (CCS’16)

Enc(42) Tag(Enc(42))
Prior work – PRFs in MPC (CCS’16)

Enc(42) \ Tag(Enc(42))
Prior work – PRFs in MPC (CCS’16)

Enc(42) \ Tag(Enc(42))
What we have done

- Analyze AE in Multiparty Computation (MPC).
- Useful MPC happens in $\mathbb{F}_p$ => Need AE and PRFs modp.
- Look for parallel AE: CTR+PMAC, OTR.
The story

This Photo by Unknown Author is licensed under CC BY-NC-ND
The story

‘You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe.

You take the red pill—you stay in Wonderland, and I show you how deep the rabbit hole goes.’
‘You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe.

You take the *red* pill—you stay in Wonderland, and I show you how deep the rabbit hole goes.’
Down the rabbit hole - MPC with Secret Sharing

\[ x = x_1 + \cdots + x_n \]

Each \( P_i \) has \([x] \leftarrow x_i\)
MPC Preprocessing Phase

Generate triples

\[ c = [a][b] \]
MPC Preprocessing Phase

Generate triples

\[ [c] = [a][b] \]
MPC Preprocessing Phase
MPC Preprocessing Phase
MPC Online Phase

Use Triples.
MPC Online Phase
MPC Circuit Evaluation
MPC Circuit Evaluation
MPC Circuit Evaluation
MPC Circuit Evaluation
MPC Circuit Evaluation

3 triples.
2 comm. rounds
Tweak your encryption to MPC
Tweak your encryption to MPC
Tweak your encryption to MPC
How-to compute PMAC

\[ \tilde{E}_k^{1,0} \] \[ \tilde{E}_k^{2,0} \] \[ \tilde{E}_k^{3,0} \] \[ \tilde{E}_k^{\ell-1,0} \] \[ \tilde{E}_k^{p-1,0} \]

\[ m_1 \] \[ m_2 \] \[ m_3 \] \[ m_{\ell-1} \] \[ m_{\ell} \]

\[ + \] \[ + \] \[ + \] \[ + \]

Tag
Let’s do AE with CTR+pPMAC

\[ \tilde{N} \leftrightarrow \tilde{E}_{k} \rightarrow \tilde{E}_{k} \rightarrow \tilde{E}_{k} \rightarrow \cdots \rightarrow \tilde{E}_{k} \rightarrow m_{1} \rightarrow c_{1} \rightarrow \cdots \rightarrow m_{\ell} \rightarrow c_{\ell} \]
Let’s do AE with CTR+pPMAC
When ideal meets real
When ideal meets real – surprise!
When ideal meets real – surprise!

![Graph showing latency vs. message blocks for Legendre and MiMC methods.](image-url)
## Other competitive modes

<table>
<thead>
<tr>
<th>PRF</th>
<th>Mode</th>
<th>Online cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Rounds (Enc/Dec)</td>
</tr>
<tr>
<td>Leg</td>
<td>CTR+pPMAC</td>
<td>7/6</td>
</tr>
<tr>
<td>MiMC</td>
<td>CTR+pPMAC</td>
<td>221/147</td>
</tr>
<tr>
<td>Leg</td>
<td>CTR+HtMAC</td>
<td>5/4</td>
</tr>
<tr>
<td>MiMC</td>
<td>CTR+HtMAC</td>
<td>148/75</td>
</tr>
<tr>
<td>Leg</td>
<td>OTR</td>
<td>6/9</td>
</tr>
<tr>
<td>MiMC</td>
<td>OTR</td>
<td>220/295</td>
</tr>
</tbody>
</table>
## Other competitive modes

<table>
<thead>
<tr>
<th>PRF</th>
<th>Mode</th>
<th>Online cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Rounds (Enc/Dec)</td>
</tr>
<tr>
<td>Leg</td>
<td>CTR+pPMAC</td>
<td>7/6</td>
</tr>
<tr>
<td>MiMC</td>
<td>CTR+pPMAC</td>
<td>221/147</td>
</tr>
<tr>
<td>Leg</td>
<td>CTR+HtMAC</td>
<td>5/4</td>
</tr>
<tr>
<td>MiMC</td>
<td>CTR+HtMAC</td>
<td>148/75</td>
</tr>
<tr>
<td>Leg</td>
<td>OTR</td>
<td>6/9</td>
</tr>
<tr>
<td>MiMC</td>
<td>OTR</td>
<td>220/295</td>
</tr>
</tbody>
</table>
Some open problems

- Preprocessing scales linearly in terms of number of message blocks - roughly n PRFs for n messages.
- Number of rounds of a cipher vs. multiplicative depth in MPC.
Thank you!
Thank you!

• Questions?