Open Source Framework for Hybrid Homomorphic Encryption

Lukas Helminger, Daniel Kales, Christian Rechberger, Roman Walch
FSE 2020 Rump Session

www.iaik.tugraz.at
Hybrid Homomorphic Encryption

- Evaluate symmetric ciphers under homomorphic encryption

- Why?
  - Ciphertext expansion prevention
  - See also Dasta talk from Monday

- Relevant metrics:
  - Multiplicative depth (AND-depth)
  - ANDs per encrypted bit
HHE Schemes

- So far:
  - Many candidate schemes
  - Many different HE libraries
  - But: No meaningful comparison done/possible

- Which scheme is best suited for
  - ... which metric?
  - ... which HE library?
  - ... which use case afterwards?
Benchmarking Framework

- No meaningful comparison done/possible → until now!
- We build a open-source Framework:
  - **Compares** candidate schemes in different libraries
  - **Benchmarks** use cases afterwards
  - **Easy integration** of new designs
- Small use cases from Privacy-Preserving Machine Learning
  - E.g. linear regression to identify handwritten digits

\[
\gamma = \beta \cdot \chi + \epsilon
\]
Benchmarks Framework – Status

- So far:
  - Implementations of candidate ciphers in three different libraries
  - Small benchmarks

<table>
<thead>
<tr>
<th></th>
<th>SEAL</th>
<th>HElib</th>
<th>TFHE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rasta</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Agrasta</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dasta</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>FiLIP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Kreyvium</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LowMC</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Benchmarking Framework – Status (cont.)

- Up next:
  - Implement missing ciphers
  - Extensive Benchmarks
  - Compare to orthogonal approach
    - E.g. LWEs $\rightarrow$ RLWE [CDKS20]
  - Publish Code
    - Will be available at https://github.com/IAIK/hybrid-HE-framework
Open Source Framework for Hybrid Homomorphic Encryption

Lukas Helminger, Daniel Kales, Christian Rechberger, Roman Walch
FSE 2020 Rump Session
Bibliography I


