Threshold Cryptography in MP-SPDZ
MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 2023

Marcel Keller

CSIRO’s Data61

26 September 2023
Imagine a Magic Black Box Between a Set of Parties

\[ a + b = c \]

Parties
- Have handles to values
- Don’t know the values
- Can input values
- Can agree on computations creating new values
- Can agree on outputting values
Secure Multiparty Computation: Black Box as Protocol

Wanted: \( f(x, y, z) \)

- Computation on secret inputs
- Replace black box
- Central questions in MPC
  - How many honest parties?
  - Dishonest parties still follow the protocol?
- MP-SPDZ supports > 40 protocol variants across all properties
Unifying MPC: Basic Operations

<table>
<thead>
<tr>
<th>Communication</th>
<th>Addition</th>
<th>Multiplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shamir/Replicated</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>SPDZ/TinyOT</td>
<td>Add shares</td>
<td>Reshare</td>
</tr>
<tr>
<td></td>
<td>Add shares/MACs</td>
<td>Beaver</td>
</tr>
</tbody>
</table>
Unified C++ Interface

```cpp
for (int i = 0; i < n; i++)
    sum[i] = a[i] + b[i];

protocol.init_mul();
for (int i = 0; i < n; i++)
    protocol.prepare_mul(a[i], b[i]);
protocol.exchange();
for (int i = 0; i < n; i++)
    product[i] = protocol.finalize_mul();
```

- Addition is straightforward
- Similar for multiplication would lead to sequential execution
- Prepare/exchange/finalize minimal interface for parallel execution
C++ Templating

- Share type defines protocol variant
- Share types are templated on domain
- Maximal code reuse across variants

```cpp
Rep3<Rep3Share<Z2<64>>> proto;
Rep3<Rep3Share<gfp_<0, 2>>> proto;
Shamir<ShamirShare<gfp_<0, 2>>> proto;
Shamir<ShamirShare<gf2n>>> proto;
Beaver<SemiShare<Z2<64>>> proto;
Beaver<SemiShare<gfp_<0, 2>>> proto;
Beaver<LowGearShare<gfp_<0, 2>>> proto;
Beaver<HighGearShare<gfp_<0, 2>>> proto;
```
Threshold ECDSA with Black-Box MPC

ECDSA Signature

\[ s = k^{-1}(H(M) + sk \cdot r_x) \]

where

- \( k \) secret randomness in \( \mathbb{Z}_p \)
- \( r_x \) a coordinate of \( kG \) in group of order \( p \)

Black-Box MPC

- Use black box for secret key \( sk \) and \( k \)
- Need to publish \( kG \) but not \( k \)
- Secret sharing scheme over \( \mathbb{Z}_p \) implies one over the group with local conversion
MP-SPDZ Domain Interface for EC Group

- Uses OpenSSL for EC functionality
- 200 lines of code
- 7 static members, 10 overloaded operators, 4 constructors, (de)serialization

```cpp
P256Element P256Element::operator +(const P256Element& other) const
{
    P256Element res;
    assert(EC_POINT_add(curve, res.point, point, other.point, 0) != 0);
    return res;
}
```
ECDSA in MP-SPDZ (Simplified)

\[ s = k^{-1}(H(M) + sk \cdot r_x) \]

Scalar hash = hash_to_scalar(message);
Share<Scalar> k, b, c;
get_random_triple(k, b, c);
Share<Scalar> k_inv = b / open(c);
Scalar r_x = open(Share<P256Element>(k)).x();
Scalar s = open(mul(k_inv, hash + sk * rx));
## Supported Protocols

<table>
<thead>
<tr>
<th>Name</th>
<th>Honest</th>
<th>Majority</th>
<th>Malicious</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rep3</td>
<td>Y</td>
<td>N</td>
<td></td>
<td><a href="https://ia.cr/2016/768">https://ia.cr/2016/768</a></td>
</tr>
<tr>
<td>Mal-Rep3</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td><a href="https://ia.cr/2017/816">https://ia.cr/2017/816</a></td>
</tr>
<tr>
<td>Shamir</td>
<td>Y</td>
<td>N</td>
<td></td>
<td><a href="https://ia.cr/2000/037">https://ia.cr/2000/037</a></td>
</tr>
<tr>
<td>Mal-Shamir</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td><a href="https://ia.cr/2017/816">https://ia.cr/2017/816</a></td>
</tr>
<tr>
<td>Semi</td>
<td>N</td>
<td>N</td>
<td></td>
<td><a href="https://ia.cr/2016/505">https://ia.cr/2016/505</a></td>
</tr>
<tr>
<td>MASCOT</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="https://ia.cr/2016/505">https://ia.cr/2016/505</a></td>
</tr>
<tr>
<td>ATLAS</td>
<td>N</td>
<td>N</td>
<td></td>
<td><a href="https://ia.cr/2021/833">https://ia.cr/2021/833</a></td>
</tr>
<tr>
<td>Rep4</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="https://ia.cr/2020/1330">https://ia.cr/2020/1330</a></td>
</tr>
</tbody>
</table>