**Secure Multi-Party Computation**

**Fairness**

<table>
<thead>
<tr>
<th>Composition schemes</th>
<th>Minimum of ranks</th>
<th>Maximize the minimum of the preferences each party assigned to its inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Side condition</td>
<td>( c \in (N \cup \ldots \cup N) ) Common input</td>
</tr>
<tr>
<td></td>
<td>Sum of ranks</td>
<td>Maximize the sum of the preferences each party assigned to its inputs</td>
</tr>
</tbody>
</table>

**SMC User Studies**

- Experiment execution
- Prototype development
- Study life cycle
- Subject recruitment
- Study areas
- Privacy / Security
- SMC protocols
- Security models
- Usability

**Join us!**

- Participation & Registration
  - What to expect
  - What you have to do

- Optimization
  - Precomputation
  - Computation of set operations in parallel
  - Caching of keying material

**Usability**

- Usability
  - Simplicity
  - Natural Mappings

**Efficiency**

<table>
<thead>
<tr>
<th>Minimum of ranks, n=5, keysize=1024</th>
<th>Run time</th>
<th>Number of inputs</th>
<th>Initial MR vs. MR-opt, n=5, keysize=1024</th>
<th>Run time</th>
<th>Number of inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Number of parties</td>
<td></td>
<td></td>
<td>Number of parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum of ranks</td>
<td></td>
<td></td>
<td>Minimum of ranks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sum of ranks, n=5, keysize=1024</td>
<td></td>
<td></td>
<td>Sum of ranks, n=5, keysize=1024</td>
</tr>
</tbody>
</table>

**Mobile Applications**

- iPhone App
  - Scheduling dates
  - Two-party setting
  - Secure bluetooth connection
- Android App
  - Scheduling dates
  - Multi-party setting
  - Secure channels via SSL

**Framework SMC-MuSe**

- **Scheduling dates**
- **Two-party setting**
- **Secure channels via SSL**

**Privacy / Security**

- Homomorphic encryption
- Privacy-preserving set operations
- Multiset union
- Multiset reduction
- Computable grammar

**System model**

- Multi-party setting
  - SSL connection
  - Keyserver
  - Relay Server
- Two-party setting
  - No server needed
  - Limited communication range

**Secure Multi-Party Computation on Smartphones: A Field Study**

Georg Neugebauer, Dominik Teubert, Philipp Siebenkotten, Samuel Schüppen, Christian Bien, Ulrike Meyer

Research Group IT Security, RWTH Aachen University, Germany