Industry Adoption and Standardization Efforts by the MPC Alliance and its Members

www.mpcalliance.org
Andrei Lapets

NIST Special Topics on Privacy and Public Auditability — Event 6
July 25, 2023
Agenda

- Secure Multi-Party Computation (MPC)
- Members and Areas of Focus
- Events and Activities
- Standardization: Necessity, Opportunities, and Challenges
Secure Multi-Party Computation (MPC)

- Two or more parties
  - Multi-party
  - Two-party
  - Outsourced

- **Input** privacy for any function
  - Malicious
  - Honest-but-curious

- Information-theoretic security

- Can be costly or can scale well
  - Bandwidth usage can be high
  - But, even browser solutions exist!
MPC Alliance: Members and Areas of Focus

<table>
<thead>
<tr>
<th>Security</th>
<th>Mix/Other</th>
<th>Data Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Custody</td>
<td>● Infrastructure</td>
<td>● Analytics</td>
</tr>
<tr>
<td>● Threshold signatures</td>
<td>● Frameworks</td>
<td>● Matching</td>
</tr>
<tr>
<td>● Blockchain</td>
<td></td>
<td>● ML</td>
</tr>
</tbody>
</table>

50+ members

- Americas
- Europe
- Asia
MPC Alliance: Events and Activities

- Event organization and support/participation
- Member organization contributions to standards efforts
- Support/feedback for guidance materials and legislation
MPC Alliance: Events and Activities

- Reference/guidance document survey
  - 28 documents considered
  - 20 organizations or groups (UN, ISO/IEC, UK Royal Society, NIST, etc.)
  - No report is comprehensive
  - Choose any 2 of 3
    - comprehensive
    - good guidance on choosing
    - deployments/use cases
  - Little coverage of some topics
    - cost of MPC
    - legal aspects of MPC
    - comparisons (for key protection)
Standardization: Necessity

- Prerequisite for solution adoption in application domains
  - Healthcare
  - Finance
  - Identity/authentication

- Interoperability

- Integration with other privacy-enhancing technologies
Standardization: Opportunities

● Industries evaluating MPC, with some deploying right now

● At what layer is standardization useful/possible today?
  ○ Low-level primitives and core protocols
  ○ Common abstractions/interfaces
  ○ High-level applicability/fitness criteria (security, threat model, etc.) within use cases, domains, and industries

● Examples from digital advertising: IPA, OPJA, and PAIR
  ○ Interoperable Private Attribution – Meta (member) and Mozilla
  ○ Open Private Join & Activation – IAB Tech Lab, Magnite (member), et al.
  ○ Publisher Advertiser Identity Reconciliation (PAIR) – Google
Standardization: Opportunities

**IPA from Meta (member) and Mozilla for determining when online ads lead to purchases**

**OPJA from IAB Tech Lab, Magnite (member), et al. and PAIR from Google for identifying audiences eligible for targeted online ads**

**https://services.google.com/fh/files/misc/pair_visual_final_10242022.pdf**

**https://github.com/patcg-individual-drafts/ipa/blob/main/IPA-End-to-End.md**

**https://iabtechlab.com/datacleanrooms/**

**https://iabtechlab.com/datacleanrooms/OPJA from IAB Tech Lab, Magnite (member), et al. and PAIR from Google for identifying audiences eligible for targeted online ads**

**https://services.google.com/fh/files/misc/pair_visual_final_10242022.pdf**

**https://github.com/patcg-individual-drafts/ipa/blob/main/IPA-End-to-End.md**

**https://iabtechlab.com/datacleanrooms/OPJA from IAB Tech Lab, Magnite (member), et al. and PAIR from Google for identifying audiences eligible for targeted online ads**

**https://services.google.com/fh/files/misc/pair_visual_final_10242022.pdf**

**https://github.com/patcg-individual-drafts/ipa/blob/main/IPA-End-to-End.md**
Standardization: Challenges

● How will MPC capabilities be packaged and delivered?
  ○ *Analogy*: DB engine and compiler features/interfaces *took decades*
  ○ What will be the relational algebra or the MapReduce (or any other analogous paradigm) for MPC?
  ○ How to craft standards before the above is known?

● How do multiple *organizations* agree to work together?
  ○ Identification, outreach, and negotiation
  ○ Legal guidelines/frameworks
  ○ Multi-party contracts and SLAs (nothing analogous exists today)

● How will standards interact with (or satisfy) regulations?
Thank You!
www.mpcalliance.org