MPC ALLIANCE

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

www.mpcalliance.org

Andrei Lapets

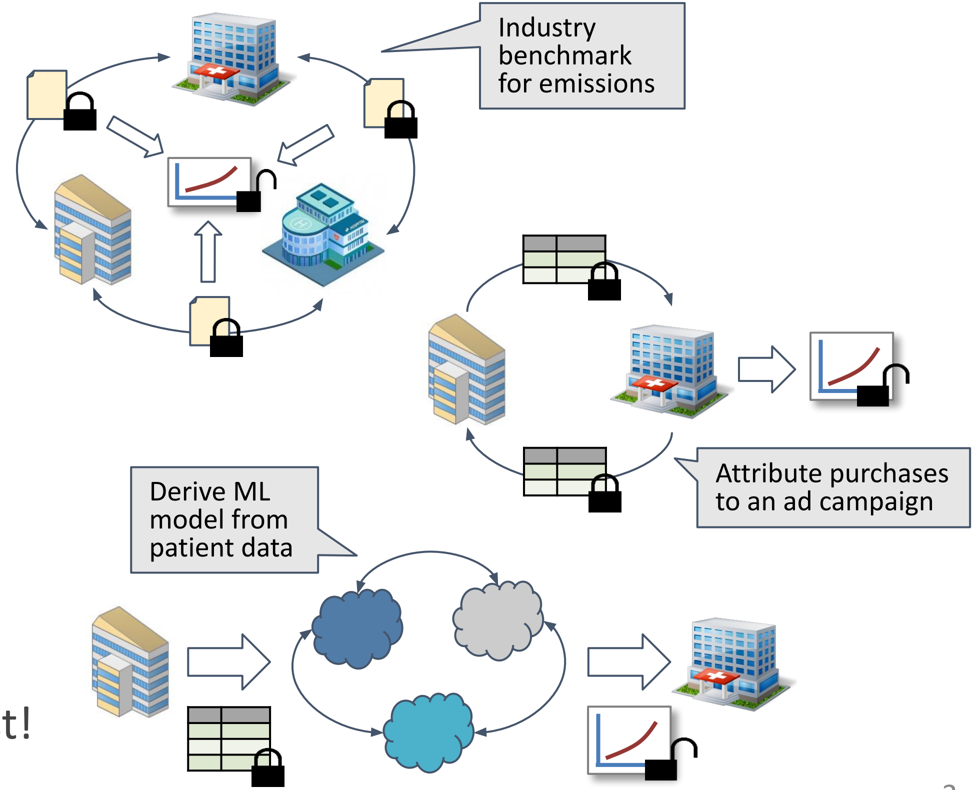
NIST Special Topics on Privacy and Public Auditability — Event 6
July 25, 2023

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!

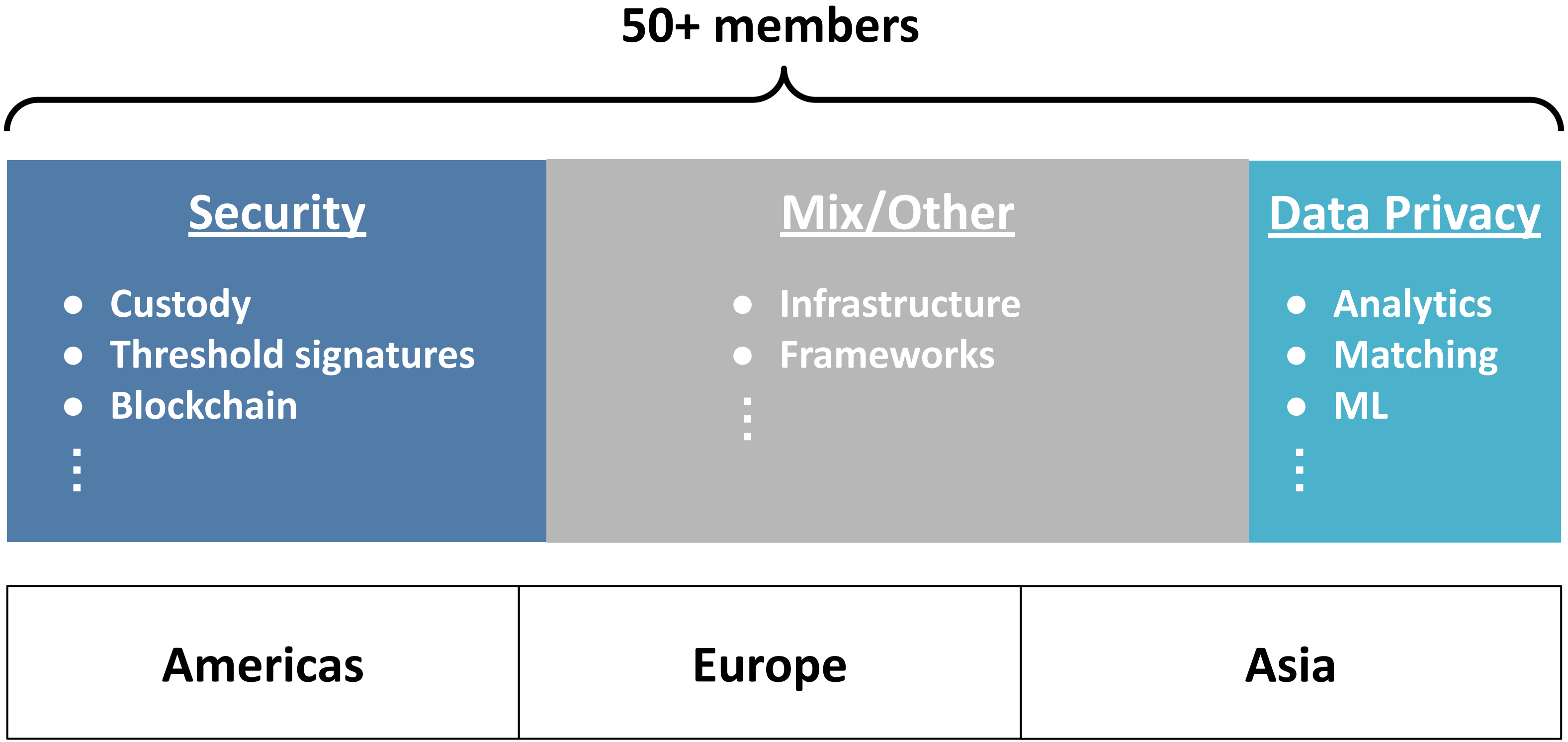


Industry benchmark for emissions

Attribute purchases to an ad campaign

Derive ML model from patient data

MPC Alliance: Members and Areas of Focus



50+ members

Security

- Custody
- Threshold signatures
- Blockchain

⋮

Mix/Other

- Infrastructure
- Frameworks

⋮

Data Privacy

- Analytics
- Matching
- ML

⋮

Americas	Europe	Asia

MPC Alliance: Events and Activities

- Event organization and support/participation

MPC DATA PRIVACY & SECURITY CONFERENCE BY THE MPC ALLIANCE

MPC DIGITAL ASSET SECURITY SUMMIT BY THE MPC ALLIANCE

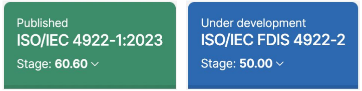
MPC DATA PRIVACY SUMMIT BY THE MPC ALLIANCE

PRIVACY-ENHANCING TECHNOLOGY SUMMIT EUROPE

DeCompute 2023

- Member organization contributions to standards efforts

CYBERNETICA → ISO



Published
ISO/IEC 4922-1:2023
Stage: 60.60

Under development
ISO/IEC FDIS 4922-2
Stage: 50.00

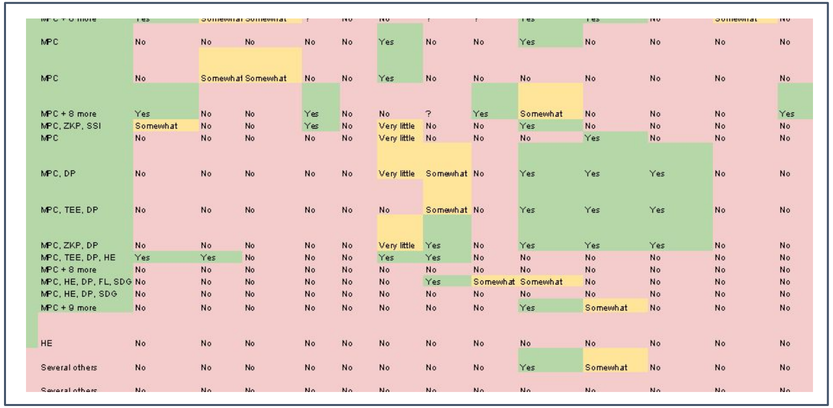
Magnite → iab. TECH LAB

- Support/feedback for guidance materials and legislation

MPC ALLIANCE → UNITED STATES CONGRESS, ico. Information Commissioner's Office

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)



MPC + 8 more	Yes	Somewhat	Somewhat	?	No	No	?	?	Yes	Yes	No	Somewhat	No
MPC	No	No	No	No	No	Yes	No	No	Yes	No	No	No	No
MPC	No	Somewhat	Somewhat	No	No	Yes	No	No	No	No	No	No	No
MPC + 8 more	Yes	No	No	Yes	No	No	?	Yes	Somewhat	No	No	No	Yes
MPC, ZKP, SSI	Somewhat	No	No	Yes	No	Very little	No	No	Yes	No	No	No	No
MPC	No	No	No	No	No	Very little	No	No	No	Yes	No	No	No
MPC, DP	No	No	No	No	No	Very little	Somewhat	No	Yes	Yes	Yes	No	No
MPC, TEE, DP	No	No	No	No	No	No	Somewhat	No	Yes	Yes	Yes	No	No
MPC, ZKP, DP	No	No	No	No	No	Very little	Yes	No	Yes	Yes	Yes	No	No
MPC, TEE, DP, HE	Yes	Yes	No	No	No	Yes	Yes	No	No	No	No	No	No
MPC + 8 more	No	No	No	No	No	No	No	No	No	No	No	No	No
MPC, HE, DP, FL, SDG	No	No	No	No	No	No	Yes	Somewhat	Somewhat	No	No	No	No
MPC, HE, DP, SDG	No	No	No	No	No	No	No	No	No	No	No	No	No
MPC + 9 more	No	No	No	No	No	No	No	No	Yes	Somewhat	No	No	No
HE	No	No	No	No	No	No	No	No	No	No	No	No	No
Several others	No	No	No	No	No	No	No	No	Yes	Somewhat	No	No	No
Several others	No	No	No	No	No	No	No	No	No	No	No	No	No

Standardization: Necessity

- Prerequisite for solution adoption in application domains
  - Healthcare
  - Finance
  - Identity/authentication
- Interoperability
- Integration with other privacy-enhancing technologies

WORLD ECONOMIC FORU

Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows

BRIEFING PAPER

JANUARY 2023

THE PET GUIDE

THE UNITED NATIONS GUIDE ON PRIVACY-ENHANCING TECHNOLOGIES FOR OFFICIAL STATISTICS.

2023

United Nations BigData

NIST

Information Tech

COMPUTE

PUBLICATIONS

NISTIR 8214C (Draft)

NIST First Call for Multi-Party Threshold Schemes

Date Published: January 25, 2023
Comments Due: April 10, 2023
Email Comments to: nistir-8214C-comments@nist.gov

Author(s)
Luís T. A. N. Brandão (Strativia), Rene Peralta (NIST)

Announcement

NIST requests public comments on NIST IR 8214C ipd (initial public draft), *NIST First Call for Multi-Party Threshold Schemes*, for primitives organized into two categories:

1. Cat1: selected NIST-specified primitives
2. Cat2: other primitives not specified by NIST

The report specifies the various categories, subcategories, and requirements for a successful submission, including security characterization, technical description, open-source implementation, and performance evaluation. The process intends to help the NIST cryptographic technology group collect reference material to promote a public analysis of the viability of threshold schemes and related primitives. This will support the NIST multi-party threshold cryptography and privacy-enhancing cryptography projects in developing future recommendations.

DECEMBER 05, 2022

tatement of the Trade nology Council

ROOM ▸ STATEMENTS AND RELEASES

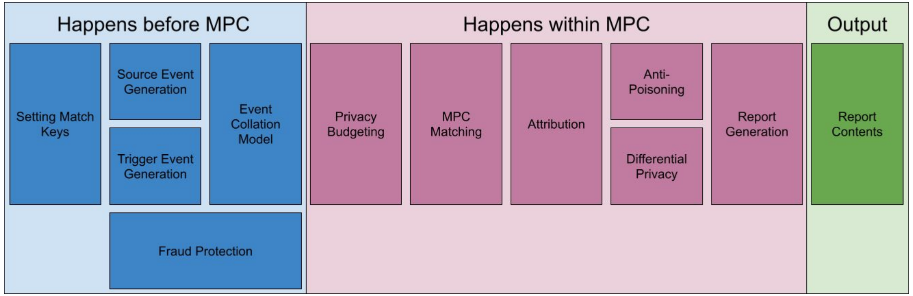
The U.S.-EU Trade and Technology Council (TTC) met outside Washington, D.C., on December 5, 2022. The meeting was co-chaired by U.S. Secretary of State Antony Blinken, U.S. Secretary of Commerce Gina Raimondo, U.S. Trade Representative Katherine Tai, European Commission Executive Vice President Margrethe Vestager, and European Commission Executive Vice President Valdis Dombrovskis, joined by U.S. Deputy Under Secretary of Labor Thea Lee, Jamaica Minister for Information Communication Technology Floyd Green, and Kenya Cabinet Secretary for Information, Communication and the Digital Economy Eliud Owalo.

The TTC is a key mechanism to support stronger transatlantic relations and to deliver concrete outcomes. We reaffirm that international rules-based

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

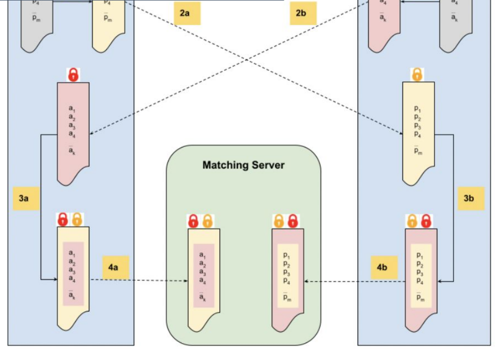
Standardization: Opportunities



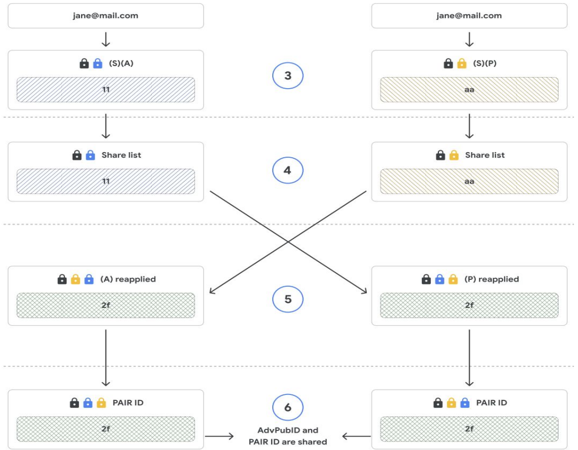
https://github.com/patcg-individual-drafts/ipa/blob/main/IPA-End-to-End.md

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://iabtechlab.com/datacleanrooms/



PAIR IDs shared by counterparty in step 6 are compared against PAIR IDs created in step 5 to determine match rate

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

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?

MPC
ALLIANCE

Thank You!

www.mpcalliance.org