MULTI-PARTY COMPUTATION IN THE MOBILITY AS A SERVICE INDUSTRY

Marina Wiemers
m.c.f.wiemers@student.tudelft.nl

Zekeriya Erkin
Supervisor & Responsible Professor
z.erkin@tudelf.nl

1 BACKGROUND

Multi-Party Computation (MPC)
privacy enhancing technology that allows for sharing and processing of secret input data

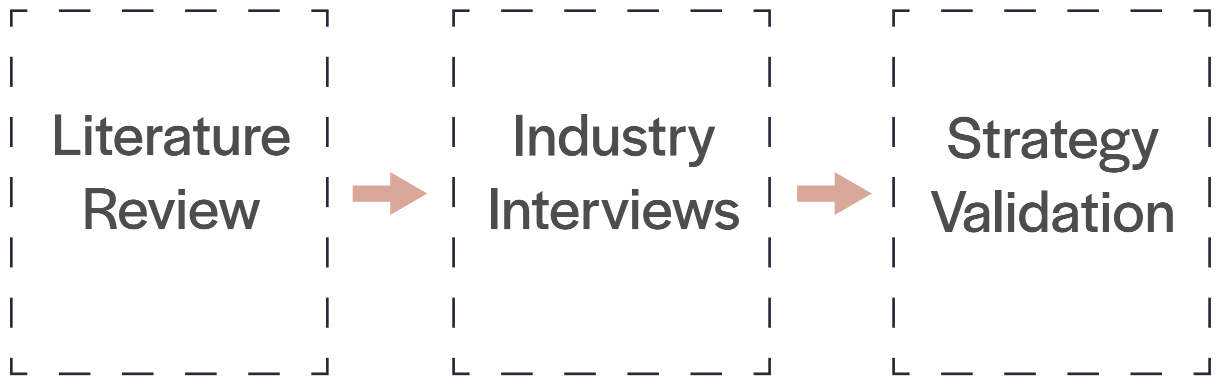
Mobility as a Service (MaaS)
shift from privately owned means of travel to collaborative transport

General Data Protection Regulation (GDPR)
law of data protection and privacy within the EU

2 RESEARCH QUESTION

How can Multi-Party Computation enable secret, secure, and GDPR-compliant sharing of mobility data?

3 METHOD



Literature Review → Industry Interviews → Strategy Validation

Investigate and understand existing applications of MPC in the industry to use as a basis for interviews with mobility providers whose results are used to validate and evaluate the devised suggestions

4 RESULTS

INDUSTRY INSIGHTS

- lack of MPC or other PETs among mobility providers
- lack of pedestrian, GDPR compliant data
- unwillingness of logistics companies to share data
- [waiting for more interviews]

POSSIBLE SOLUTION/STRATEGY

[high-level architecture]

[roles: (input, computation, result parties) to (mobility provider, 3rd party, municipal authority)]

[chosen protocol]

[graphic to show architecture & basic protocol]

5 CONCLUSION

[TBA]

- evaluate against different criteria (e.g. feasibility, robustness, number of adversaries/security,...)

- validate against insights from interviews

- show how mobility data can be used to improve traffic management in inner cities

SHARING PRIVATE DATA FOR IMPROVED TRAFFIC MANAGEMENT

An Investigation of Applications of Multi-Party Computation to Share and Process Mobility Data

Marina Wiemers
m.c.f.wiemers@student.tudelft.nl

Zekeriya Erkin
Supervisor & Responsible Professor
z.erkin@tudelf.nl

Multi-Party Computation (MPC)
privacy enhancing technology that allows for sharing and processing of secret input data

Mobility as a Service (MaaS)
shift from privately owned means of travel to collaborative transport

General Data Protection Regulation (GDPR)
law of data protection and privacy within the EU

How can Multi-Party Computation enable secret, secure, andt GDPR-compliant sharing of mobility data?

Literature Review → Industry Interviews → Strategy Validation

Investigate and understand existing applications of MPC in the industry to use as a basis for interviews with mobility providers whose results are used to validate and evaluate the devised suggestions

INDUSTRY INSIGHTS

- lack of MPC or other PETs among mobility providers
- lack of pedestrian, GDPR compliant data
- unwillingness of logistics companies to share data
- [waiting for more interviews]

POSSIBLE SOLUTION/STRATEGY

[high-level architecture]

[roles: (input, computation, result parties) to (mobility provider, 3rd party, municipal authority)]

[chosen protocol]

[graphic to show architecture & basic protocol]

[TBA]

- evaluate against different criteria (e.g. feasibility, robustness, number of adversaries/security,...)
- validate against insights from interviews
- show how mobility data can be used to improve traffic management in inner cities

SHARING PRIVATE DATA FOR IMPROVED TRAFFIC MANAGEMENT

An Investigation of Multi-Party Computation to Share and Process Mobility Data

Marina Wiemers
m.c.f.wiemers@student.tudelft.nl

Zekeriya Erkin
Supervisor & Responsible Professor
z.erkin@tudelft.nl

1 STATUS QUO

Mobility as a Service (MaaS)

MaaS describes the concept of the fusion of different modes of transportation into one **integrated system**. For instance, travel advice can be given based on current traffic, and users can shift from privately owned vehicles to **shared solutions**, such as ride-sourcing, carpooling, and e-scooters.

Infrastructure Governing

Sourcing data from all kinds of mobility providers allows municipal authorities **facilitated decision-making** for traffic and infrastructure management. By providing **dependable sources**, reports and strategies to optimise aspects such as emissions, safety, sustainability , and accessability. can be made.

Data Barriers: GDPR and Competition

Nevertheless, considerably little data is actually shared by mobility providers with governing institutions. For one, the EU's General Data Protection Regulation (GDPR) introduced new measures to **protect identifiable data** with concepts such as Privacy by Design, impeding possibilities of data sharing. Simultaneously, due to the competitive nature of the MaaS market, companies within the industry are likely **unwilling to share data openly** with their competitors.

2 MPC AS A SOLUTION?

Secure Multi-Party Computation (MPC)

MPC is a **privacy enhancing technology** that allows for safe and secure processing and sharing of data. Using cryptographic protocols, MPC enables computations, such as statistical aggregation or voting systems, without revealing only the output of the analysis, i.e. the **input data remains hidden.**

Thus, MPC enables companies or data owners to **collaborate on statistics** and results of aggregated data with each other without sharing any explicit data.

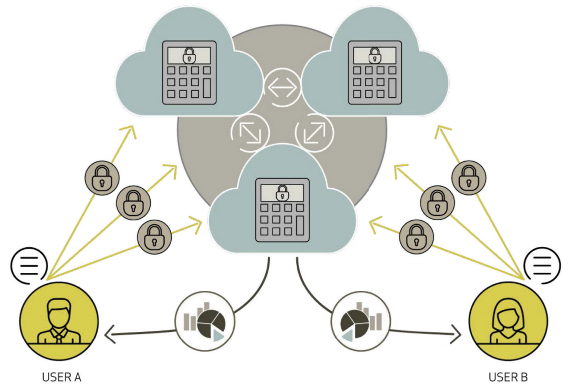


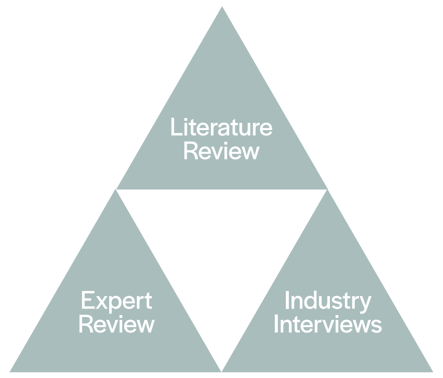
Figure 1. *Multi-Party Computation: User A and B provide data for a joint statistical analysis without revelaing their inputs.*
[Source: Archer et al., 2018]

How can MPC enable personal, geo-locational data to be shared with policy-makers in a secure and GDPR-compliant way?

3 GAINING INDUSTRY INSIGHTS

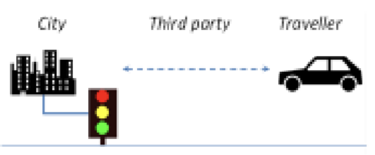
Elicitation

- *Literature Review*: existing applications and implementations of MPC, GDPR implications, data security in MaaS
- *Expert Review*: data requirements, formats, and regulations, insight into needs and applications of data
- *Industry Interviews*: awareness of MPC, state of data collaboration, barriers and limiting factors

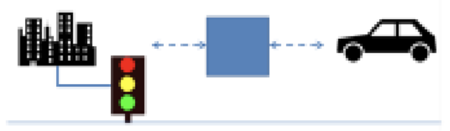


Conception

VEHICLE to INFRASTRUCTURE



PROVIDER to INFRASTRUCTURE



Validation

- Comparison to existing APIs and Mobility Data Standards, such as TOMP-API and CDS-M
- Requirements and Decision Criteria: Legality, Usability, Feasibility, Security, Data Availability, Infrastructure

4 A SECURE SOLUTION

[Use Case Specific Solution]

[Results of devised strategy and evaluation against different criteria, i.e. Feasibility, Robustness, Communication and Management Overhead,...]

[Graphic of Final Devised Architecture]

5 OUTLOOK: MPC AND MAAS

Feasibility of MPC within the MaaS Sector

[TBA]

Limiting Factors and Potential Barriers of Employing MPC

[TBA]

Potential further applications of MPC within MaaS

[TBA]

Next steps,..

[TBA]