IAIK TU Graz

KNOW Center

TU Graz
SCIENCE
PASSION
TECHNOLOGY

Datenschutz durch Technikgestaltung

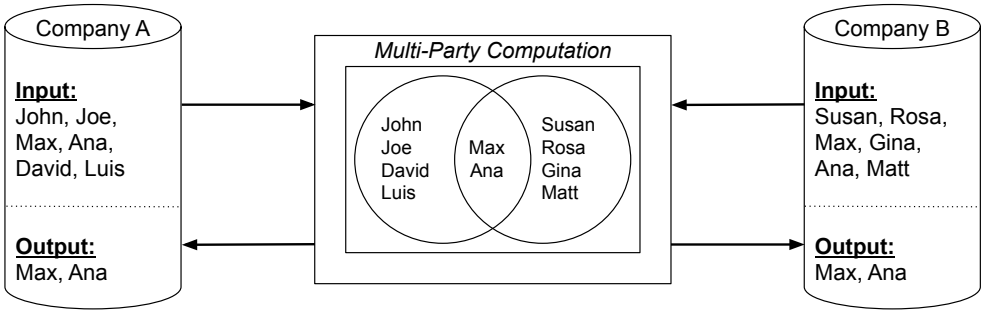
Multi-Party Computation unter der DSGVO
Fallbeispiel Standortdaten

Lukas Helminger

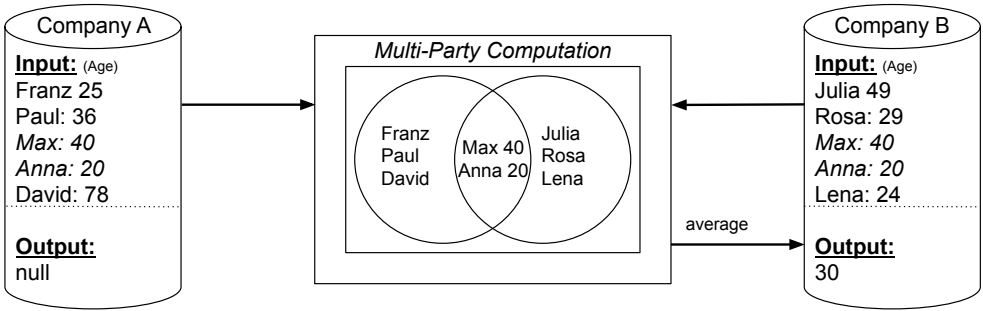
31.03.2022

Multi-Party Computation ist

- eine Technologie zur Verbesserung des Datenschutzes
- sie erlaubt Daten während einer Berechnung zu schützen
- mit ähnlichen Sicherheitsgarantien wie Verschlüsselungen.



MPC schützt Daten während einer Berechnung (Verschlüsselung).



MPC schützt Daten während einer Berechnung (Verschlüsselung).

Kryptographen sind sich einig, dass MPC zu einem besseren Datenschutz beiträgt, aber

Gibt es auch rechtliche Vorteile für Verantwortliche die MPC einsetzen?

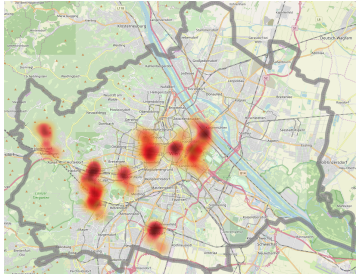
Wo haben sich Corona-Patienten im Ansteckungszeitraum aufgehalten?

Behörde(Positive)

Paul	0043 664 1234567
Lena	0043 664 2354334
Lisa	0043 664 1219928
⋮	⋮

Telekomm.(Standort)

Paul	0043 664 1234567
Anna	0043 664 7654321
Lisa	0043 664 1219928
⋮	⋮



Mögliche (technische) Lösungen

Lösung	MPC	Beschreibung	Problem
1	nein	T sendet Daten zu B	Standortdaten von "allen"

Mögliche (technische) Lösungen

Lösung	MPC	Beschreibung	Problem
1	nein	T sendet Daten zu B	Standortdaten von "allen"
2	nein	B sendet Liste zu T	T erfährt wer positiv

Mögliche (technische) Lösungen

Lösung	MPC	Beschreibung	Problem
1	nein	T sendet Daten zu B	Standortdaten von "allen"
2	nein	B sendet Liste zu T	T erfährt wer positiv
3	ja	B sendet verschlüsselte Liste zu T	keine

Fazit

- MPC hilft das Dilemma von Datenanalyse und Datenschutz zu lösen.
- Es gibt rechtliche Vorteile wenn man MPC nützt.
- MPC genießt noch nicht die nötige Aufmerksamkeit die es verdient. (z.B.: Verhaltensregeln, Standardisierung).