Technik statt Recht zum Schutz der Privatsphäre

2. Dezember 2022

Dr. sc. ETH David M. Sommer

Zürich - Karl der Grosse

Definitionen

personenbezogen

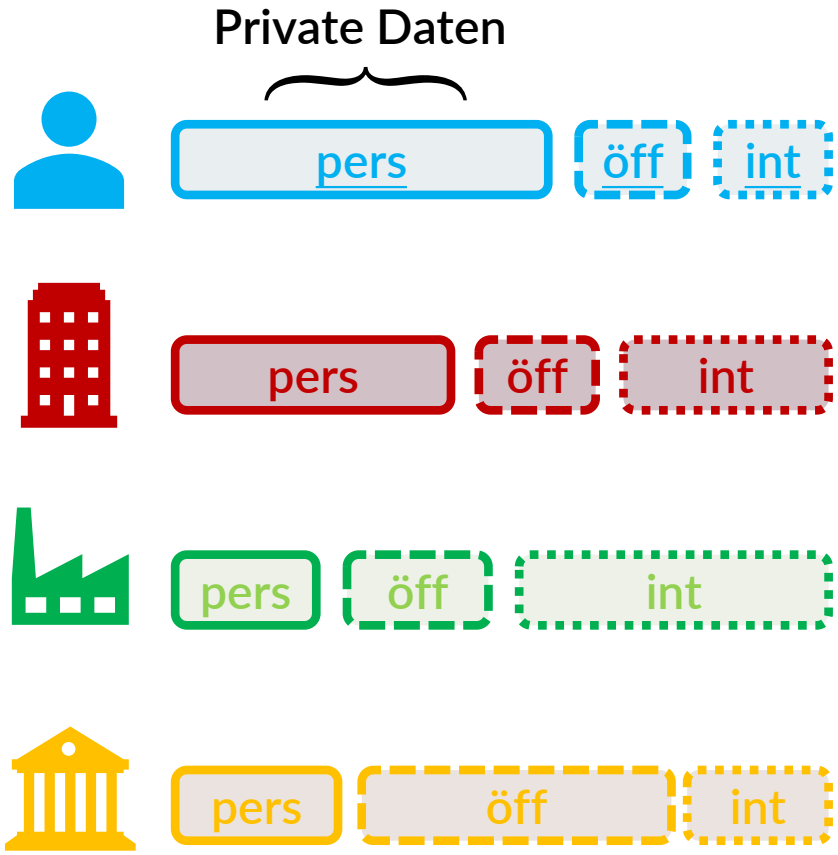
- Kundendaten
- Verhaltensdaten
- Photos ..

öffentlich

- Geo-Daten
- BFS-Statistiken
- ...

intern

- unternehmensbezogen
- Verwaltungsinformationen
- ...



Kann man Daten kombinieren, ohne sie zentral zu sammeln?

Datn, Datn, Watn?

- Ziel: Bessere / schnellere / biligere Entscheidungen
- Hoffnung
  - Bessere Produktplatzierung
  - Schnellere Arbeitszyklen
  - “Sicht in die Zukunft”
  - Informiertere Öffentlichkeit
  - Generell: bessere Lösungen
- Vernetzung
  - Vorteil steigt überproportional mit Menge an Daten
- Datennutzung endet oft an Unternehmensgrenzen
  - Datenschutzgesetze
  - Wettbewerbsvorteile

Quelle: TRFN / Limit Records Official video for Daft Punk’s "Harder Better Faster Stronger" from the album Discovery.

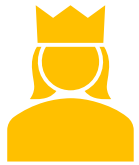
Privacy Enhancing Technologies (PETs)

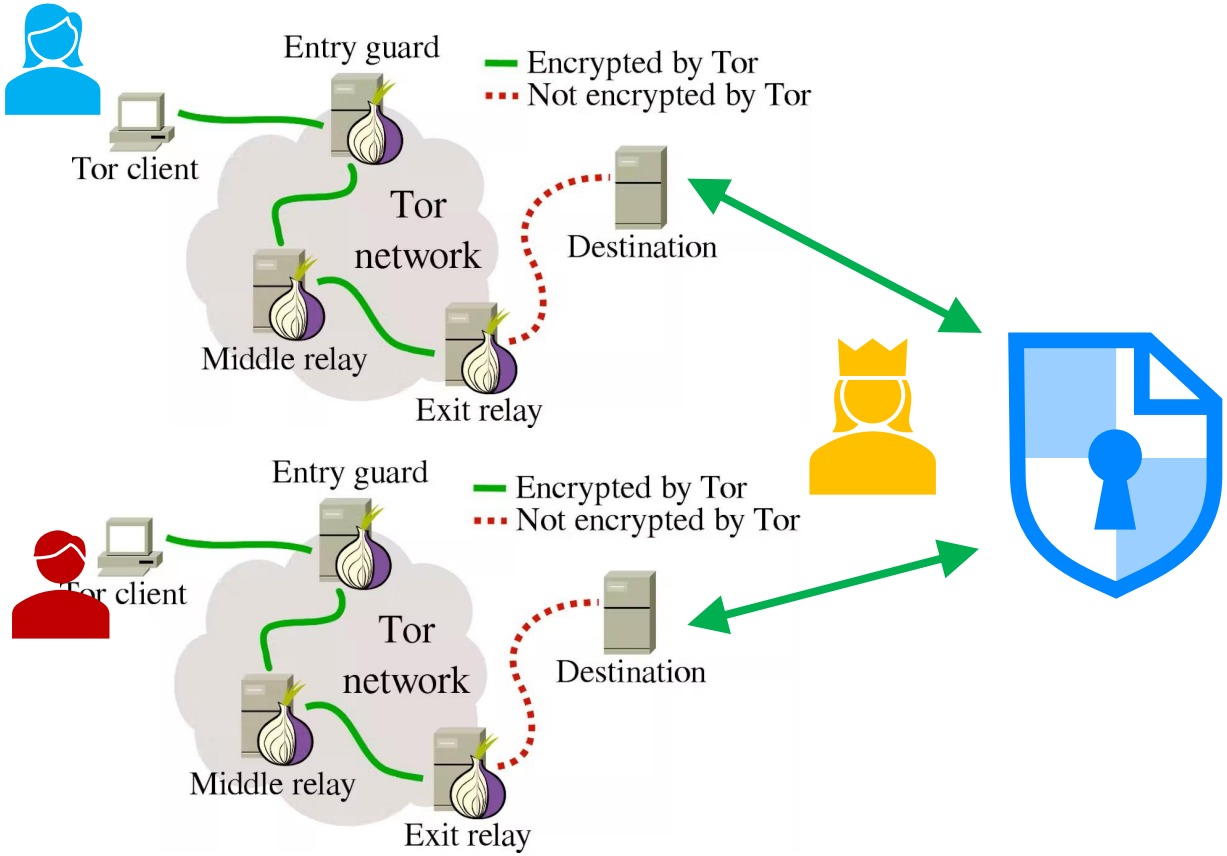
- PETS: Gesamtlösungen
  - Bsp.: Tor, Signal, CryptPad
- Ziel: Funktionalität bei maximaler Wahrung der Privatsphäre
  - Minimale Rückschlüsse auf Benutzung und Inhalt
    - Vertraulichkeit und Unverbindbarkeit (confidentiality, unlinkability)
  - Evtl. auch Ununterscheidbarkeit, Unbeobachtbarkeit, Abstreitbarkeit
    - (indistinguishability, unobservability, deniability)
- Privacy vs. Privatsphäre
  - Privacy = Privatsphäre + die Kontrolle über die Verteilung der Informationen
  - Privacy ~ Privatheit
- Kern des Problems: Freiheit und Macht
  - Minimierung von Informationen: Privacy nur Mittel-zum-Zweck / Methode

Beispiel: PETs im Arbeitskampf

- Gewerkschaftsvertretende

- Direktorin mit hochkarätigen Freunden





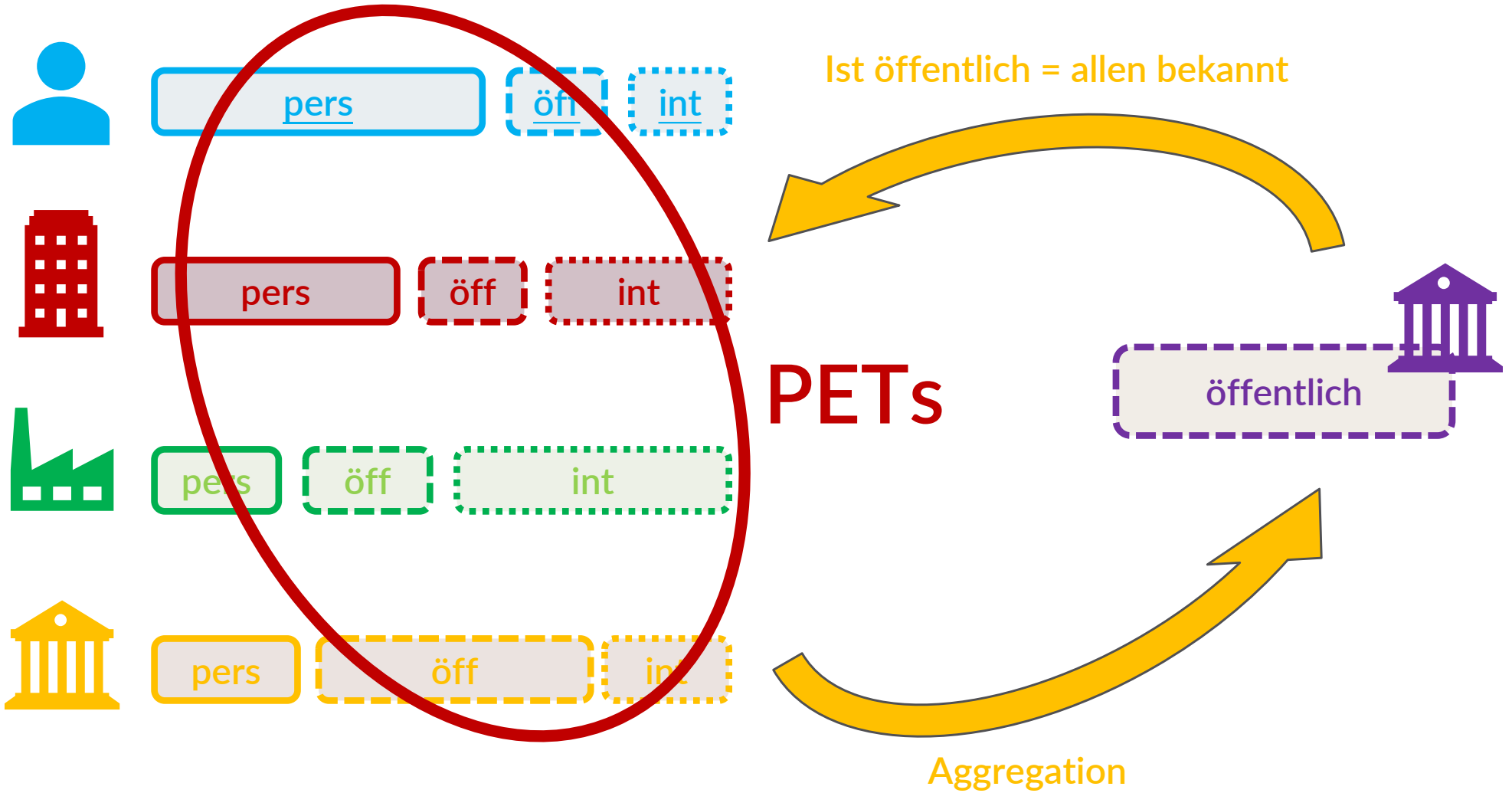
Privacy Enhancing Technologies II

- PETs bestehen aus vielen verschiedenen Komponenten
- Technisch gut analysierte «building blocks»
  - Kryptographische Strukturen
  - Kommunikationsmuster
  - Resultatsgarantieen
  - ..
- PETs: Primär für Daten innerhalb der Kontrolle des Produzenten (Personen, Institutionen, ..)
  - Fokus aber auf Personen als Produzenten
  - Kundendaten oder Verhaltensdaten bereits zentral gesammelt: zu spät

PETs für Data-Sharing

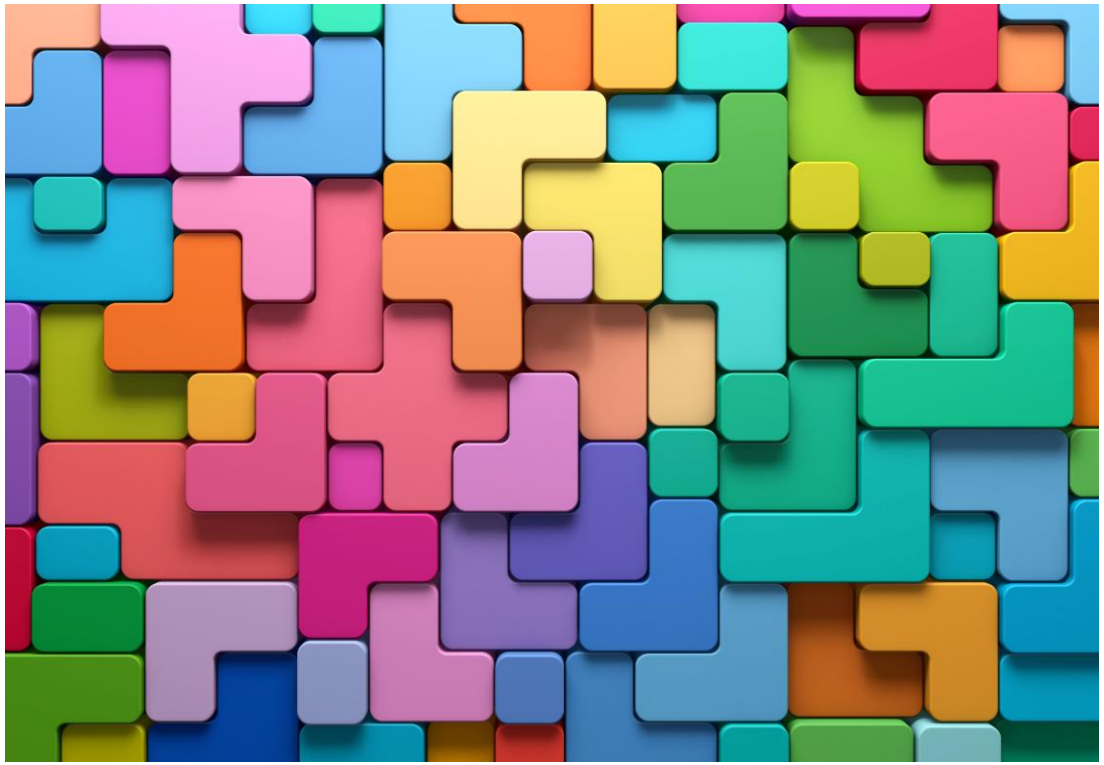
- Andere Voraussetzungen für Data-Sharing
  - Im B2B-Setting: Kooperation ist oft bekannt
    - Weniger wichtig: unlinkability, indistinguishability, unobservability, or deniability
  - Dafür:
    - Stärkere Garantien der Fairness
    - Compliance-Aspekte (Z.B. Datenschutzgesetze, Bankgeheimnis)
    - Vertrauen von gleichgestellten Kooperationspartner
  - Einzelne Personen können auch mit Firmen kooperieren
    - Attribute werden wieder interessant: unlinkability, indistinguishability, unobservability, or deniability
- Gleiche «building blocks»
  - Design-Erfahrungen sowie Building-Blocks können wiederverwendet werden
- Ziel: Daten gemeinsam verwenden, ohne die Daten preiszugeben oder Kopieren zu ermöglichen

Datenflüsse mit PETs



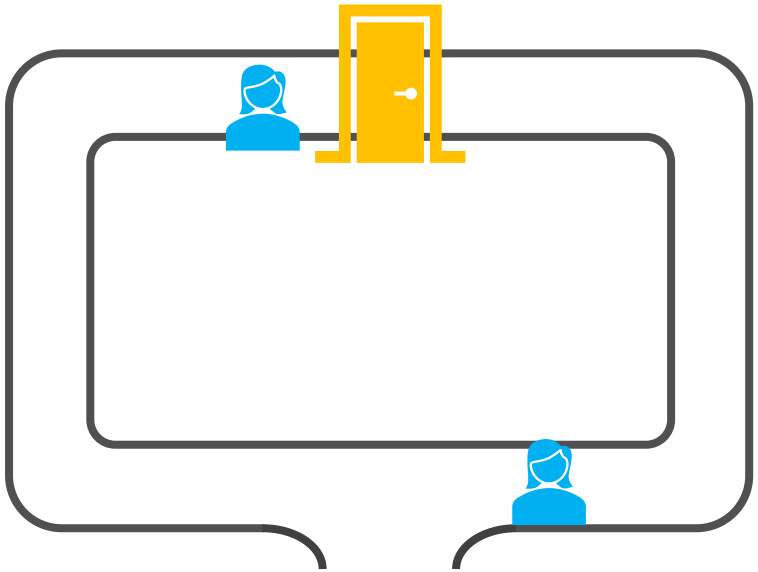
B.. B.. Building Blocks

- Kenntnis beweisen
  - Zero Knowledge Proofs
- Zusammen berechnen
  - Multi-Party Computation (MPC)
  - Homomorphic Encryption (HE)
  - Trusted Execution Environment (TEE)
- Aggregation
  - Differential Privacy



Zero-Knowledge Proofs

- Kenntnis beweisen ohne Geheimnis zu zeigen
- Einzige Information: «Statement is true»
- Oft commitment-basiert
  - Oft interaktiv
- Nützlich für
  - Zugangsberechtigungen
  - Altersbeweise

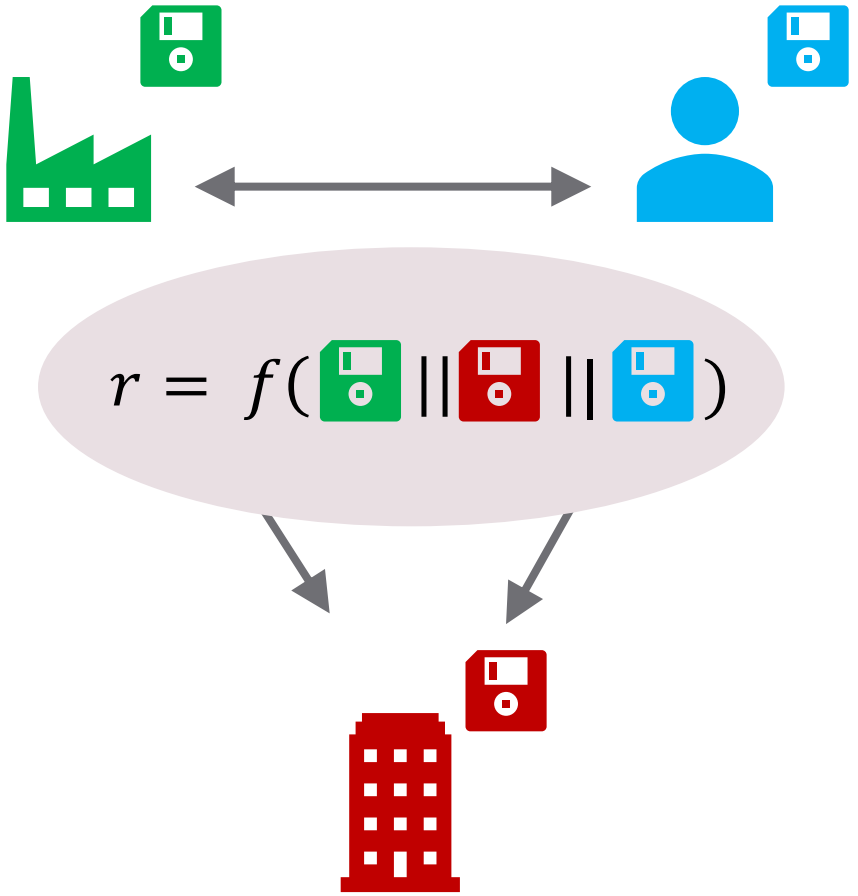


Betrugswahrscheinlichkeit $\Pr_n^{cheat} = \frac{1}{2^n}$

Bsp.: $\Pr_{20}^{cheat} = 0.00000095..$

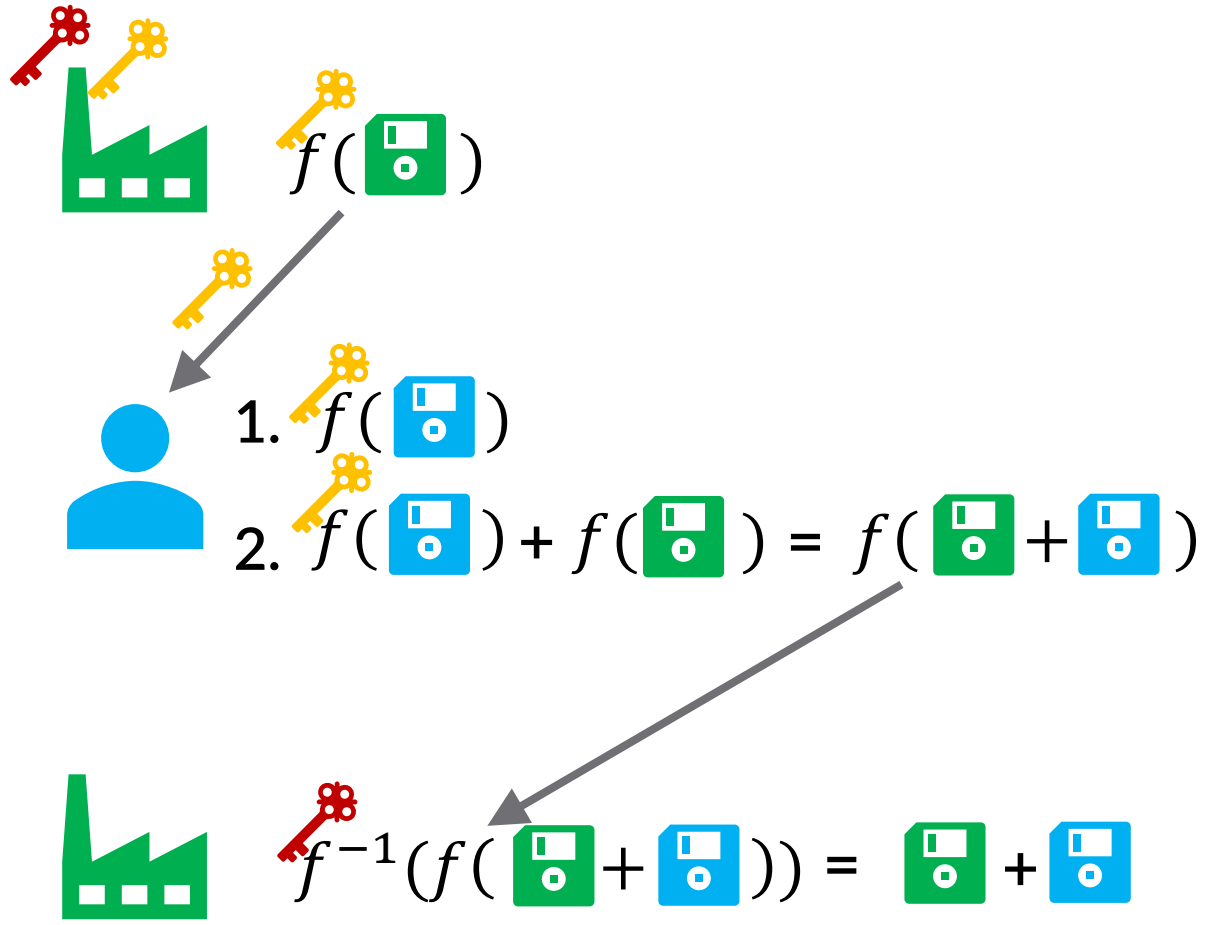
Multi-Party-Computation (MPC)

- Gemeinsames Berechnen von f
  - Input bleibt privat
  - Garantiertes Erhalten des Outputs
  - Keine «trusted third party»
- Synchron («Online-Zwang»)
- Nützlich für:
  - Risikoabschätzung bei Versicherungen
  - Gesundesheitsdaten-Zusammenführung



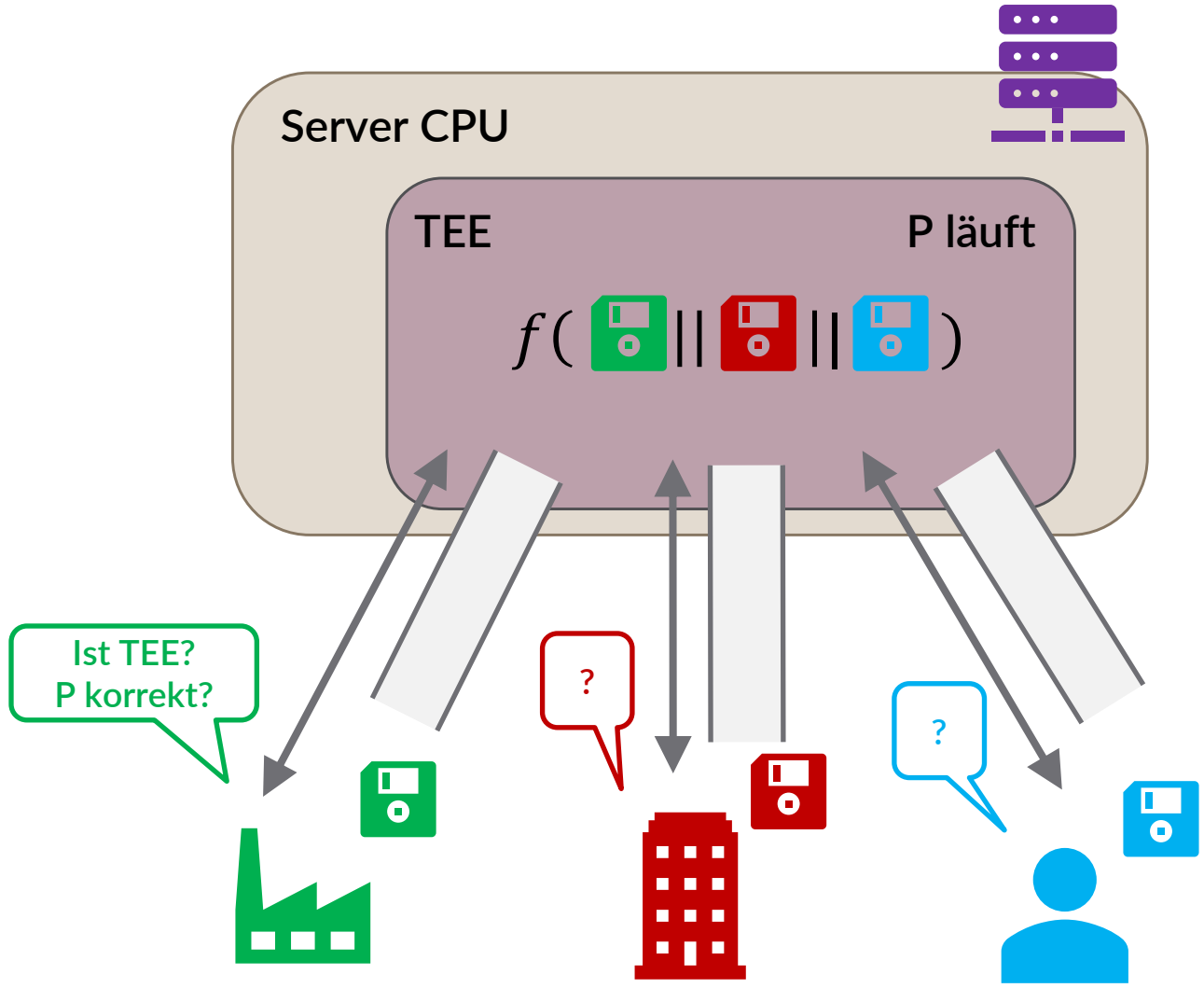
Homomorphe Verschlüsselung (HE)

- Zahlen verschlüsselt verrechnen
  - enc(a) + enc(b) = enc(a+b)
- Unterschiede MPC
  - Asynchron (kein «Online-Zwang»)
  - Keine Garantie für Resultat
- Nützlich für
  - E-Voting (0 oder 1 addieren)
  - Verschlüsseltes Machine-Learning



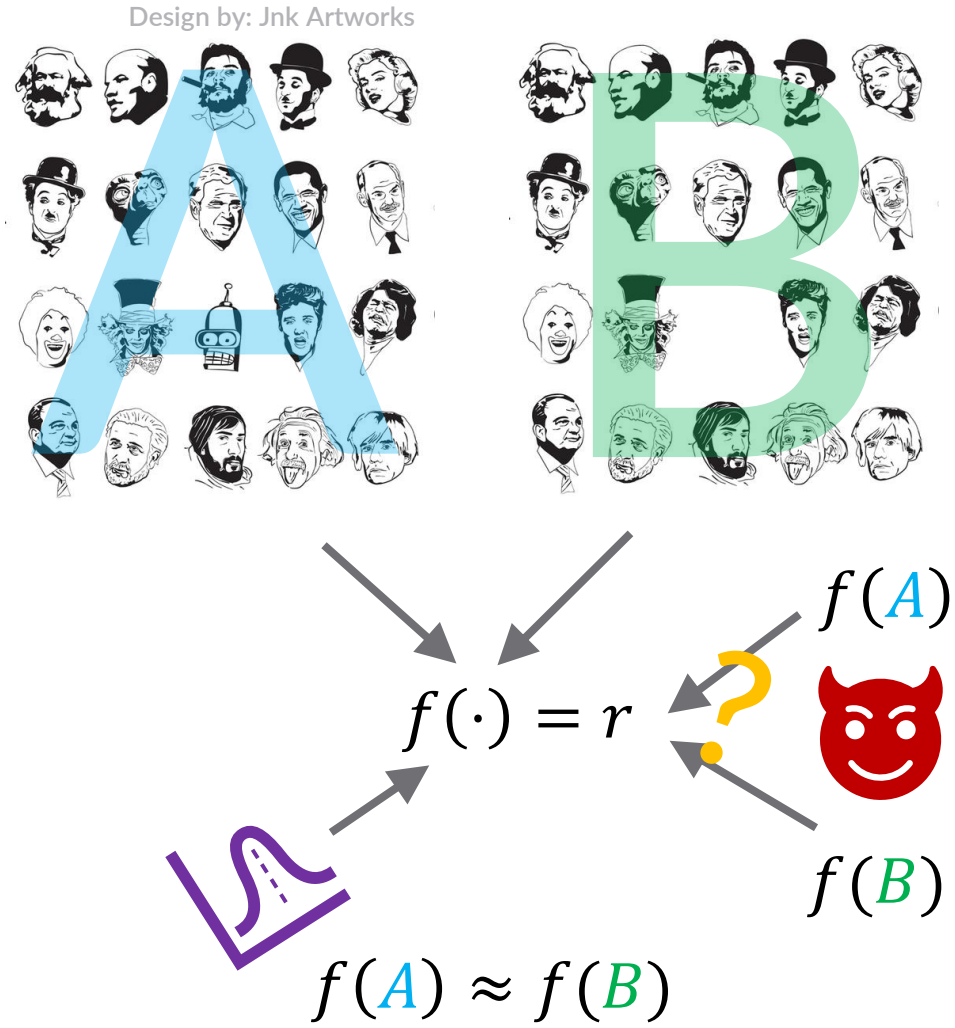
Trusted Execution Environment (TEE)

- Abgeschirmter Raum für Berechnungen
  - Via Hardwaremodul
- Vertrauen bei Hardware-Hersteller
  - Garantiert Vertraulichkeit und Integrität
  - Garantiert korrekter Hash zu Programm P
- Vorteil
  - Einfach zu implementieren
- Nützlich für
  - Verarbeitung von Umfrage-Antworten
  - Verarbeitung von persönlichen Daten



Differential Privacy (DP)

- Verrauschen von aggregierten Daten
- Ziel: Nachweisbarkeit des Einfluss individueller Datenpunkte beschränken
  - War Datenpunkt X Teil des Datensets? Ja – Nein
- Akademischer Gold-Standard
  - Sehr mächtiges Attacker-Modell
- Kombinierbar mit MPC, HE, TEE etc
- Personenbezogene Daten?
  →DP-Aggregation veröffentlichbar
- Nützlich für
  - Volkszählungen
  - Veröffentlichung von Umfrage-Ergebnissen



Conclusion

- Datensparsamkeit
  - Vorhandene Daten werden gebraucht/missbraucht
  - Unklare zukünfitge Verwendung
  - Regelmässige Daten-Leaks
- Keine zentrale Datensammlung nötig
  - Funktionalität auch so möglich
- Jedes Problem benötigt eigene Lösung
  - Erhöhter Engineering-Aufwand
- Aktive gesellschaftliche Entscheidung

Backup-Slides

Weiterführende Links

- Vertrauenswürdige Datenräume
  unter Berücksichtigung der
  digitalen Selbstbestimmung
  Studie zu zentralen Herausforderungen, Grundprinzipien und
  Voraussetzungen, konkreten Beispielen sowie Kernelementen
  eines Modells vertrauenswürdiger Datenräume im Auftrag
  des BAKOM
  Patrizio Collovà, Michael Marti, Daniel Schwarz, Flurina Wäspi und Nicolai Wenger
  Bern, 22.07.2021

Synthetic Data & Agregation

- Eg.g. use DP

Was ist dieser Talk nicht about

- Geschäftsmodelle
- Platformregulierung

I need more content

- Netzwerk- und Lock-in-Effekte
- Die Datansammlung beruht die Bereitschaft zur Datenbekanntgabe in der aktuellen Big-Data-Ökonomie
  nicht auf der Basis von Transparenz und Vertrauen, sondern ist letztlich eine Folge der schwachen Marktstellung der Konsument*innen gegenüber den Unternehmen

Beispiel PET: Tor

- Gewerkschaftsvertreter

Building Blocks:

- Verschlüsslung
- Absenden Verrauschen
- Vertrauen
- Indistingusihability (tor bridges aus china)