AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Wie moderne Kryptographie neue Kooperationsmethoden ermöglicht.

Thomas Lorünser
Center for Digital Safety & Security

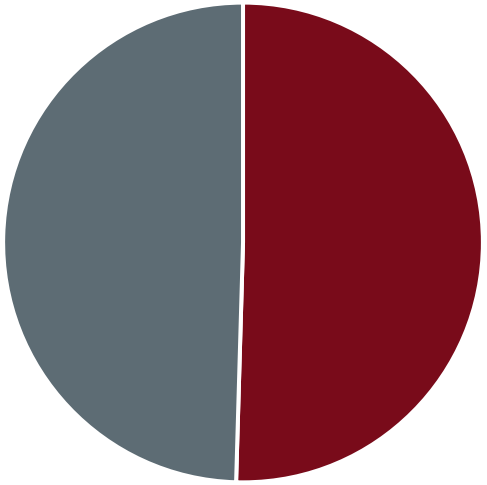
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

OWNERSHIP STRUCTURE

49.54 %

FEDERATION OF AUSTRIAN INDUSTRIES
(through VFFI)



50.46 %

REPUBLIC OF AUSTRIA
Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology

~1500

EMPLOYEES

182,9 m EUR

TOTAL REVENUES
as of YE 2022

103 m EUR	Contract research revenues (incl. grants)
53,7 m EUR	BMK funding
26,2 m EUR	Other operating income, incl. Nuclear Engineering Seibersdorf
4,3 m EUR (2021)	Profactor (51%)

CRYPTO TOPIC OVERVIEW

Long-term & post-quantum security

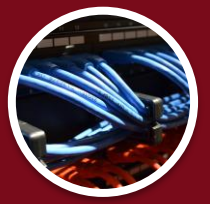
- Post-quantum cryptography incl. NIST competitions
- Forward & post-compromise security
- Application cases

Hybridization with QKD

- Key management systems
- Development of PQ-QKD hybrid protocols
- Secure architectures

Privacy-enhancing technologies

- Primitives (e.g., zkSNARKs)
- Anonymous authentication
- Privacy-friendly use of biometrics



Federated processing on sensitive data

- Secure Multi-Party Computation
- End-to-end verifiability for auctions and data markets

COMP4DRONES

TeamaWare

PETRUS

QCAT

SUNRISE

Cyber Security for Europe

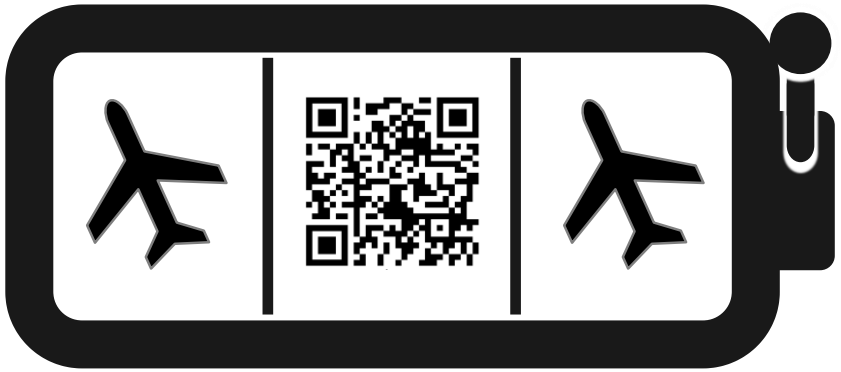
KRAKEN

FAEST Signature Algorithm

PICNIC

PRESENT

Project SLOTMACHINE

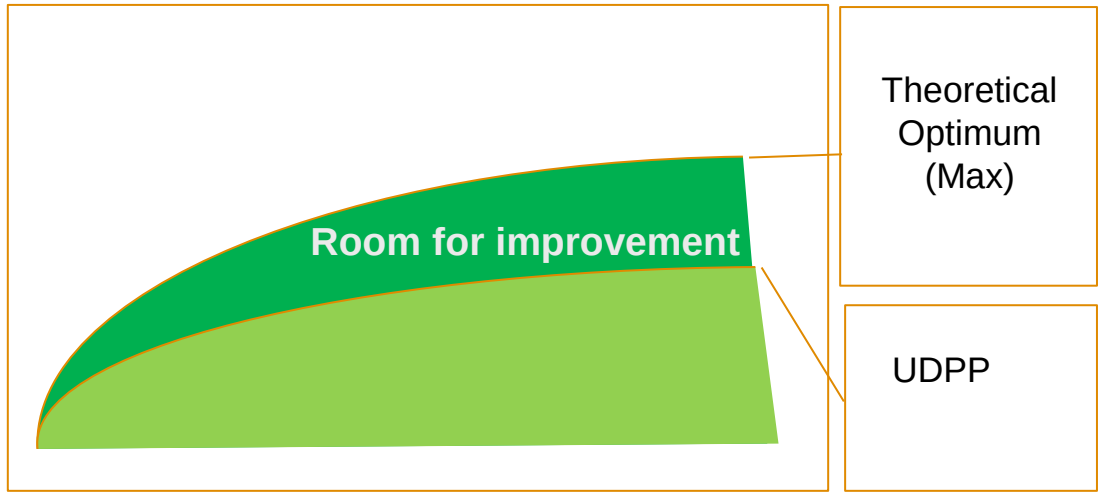


A Marketplace for more cost-efficient flight prioritization

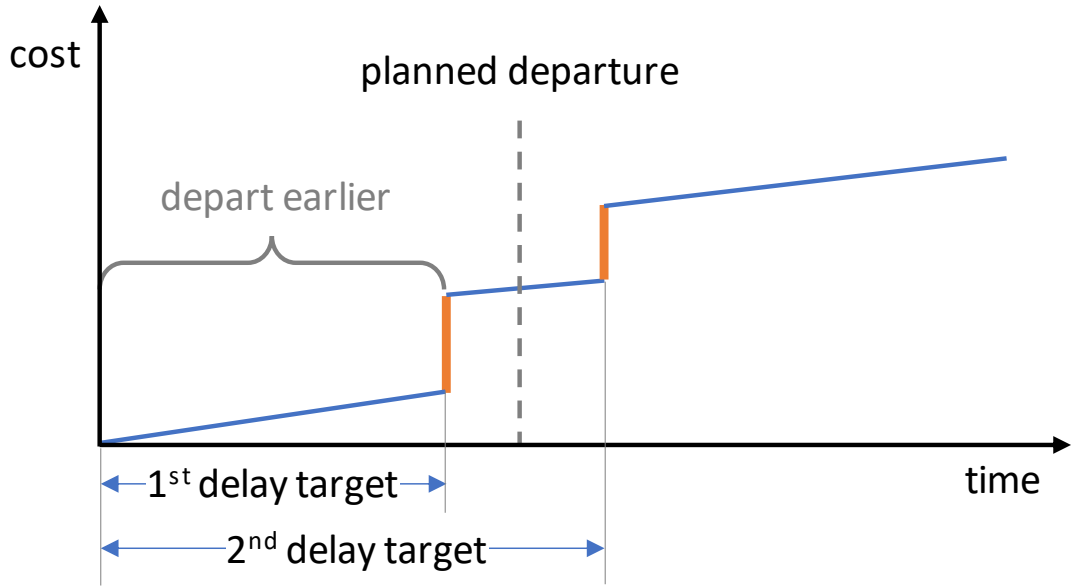
- FREQUENTIS AG (Coordinator)
- AIT – Austrian Institute of Technology GmbH
- EUROCONTROL
- JKU – Johannes Keppler University of Linz
- SWISS – Swiss International Air Lines AG

THE POWER OF COLLABORATION

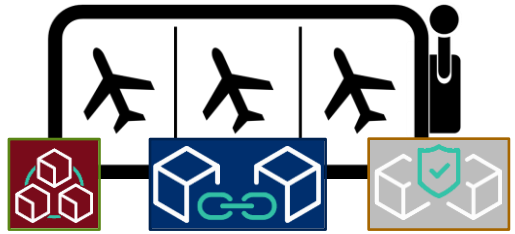
- In case of ATFM regulation, UDPP allows each AU to reduce cost of delays within own flights.
- Further optimisation is possible with increased flexibility across AUs.



- Non-linear cost functions for each flight
- If delay targets are missed, the costs for the delay increase disproportionately



SLOTMACHINE RESULTS

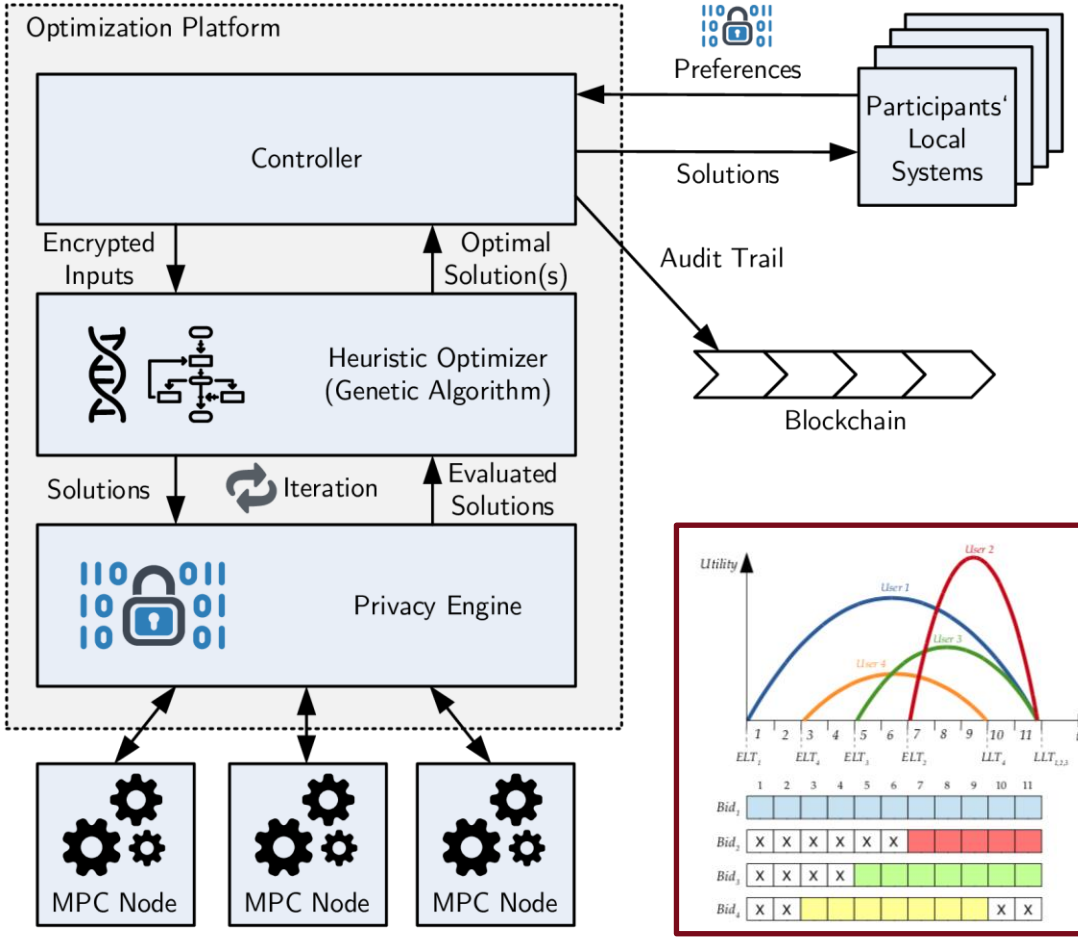


AUSTRIAN INSTITUTE OF TECHNOLOGY

- A new privacy-preserving collaboration platform for ATFM
- Data are encrypted at end-user
- Data collected from different users are collected at the platform
- Oblivious computation on joint data set is performed and only result revealed
- Ideally verifiability is added

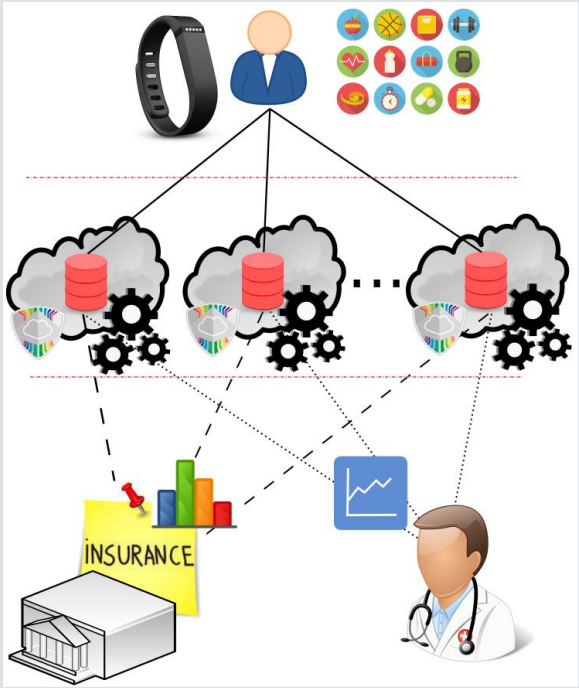
Benefit: Solves privacy vs. utility trade-off

Challenge: Computation speed

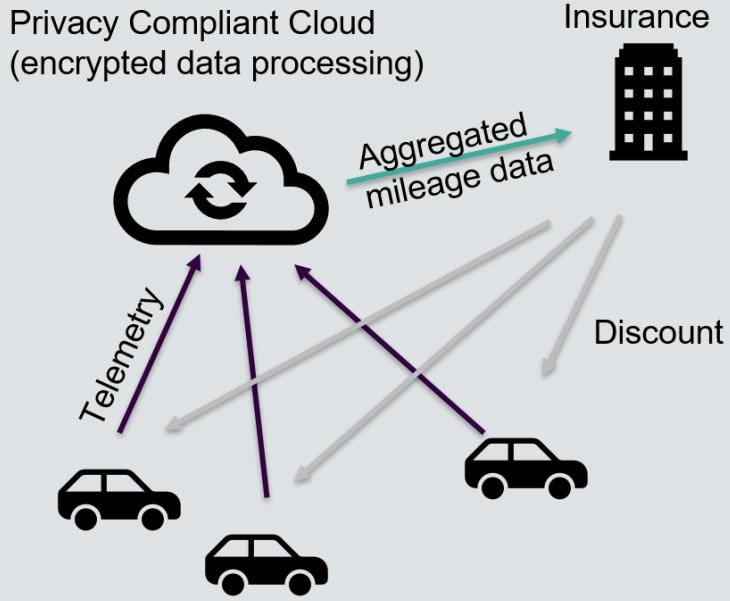


COLLABORATION ON ENCRYPTED DATA: A GENERAL PATTERN

- For more agility new solutions for computing on encrypted data have emerged
- New technologies:
  - Fully homomorphic encryption (FHE)
  - Multiparty computation (MPC)
  - TEE
- Applications
  - Secure auctions
  - Privacy preserving data mining
  - Collaborative machine learning
  - …



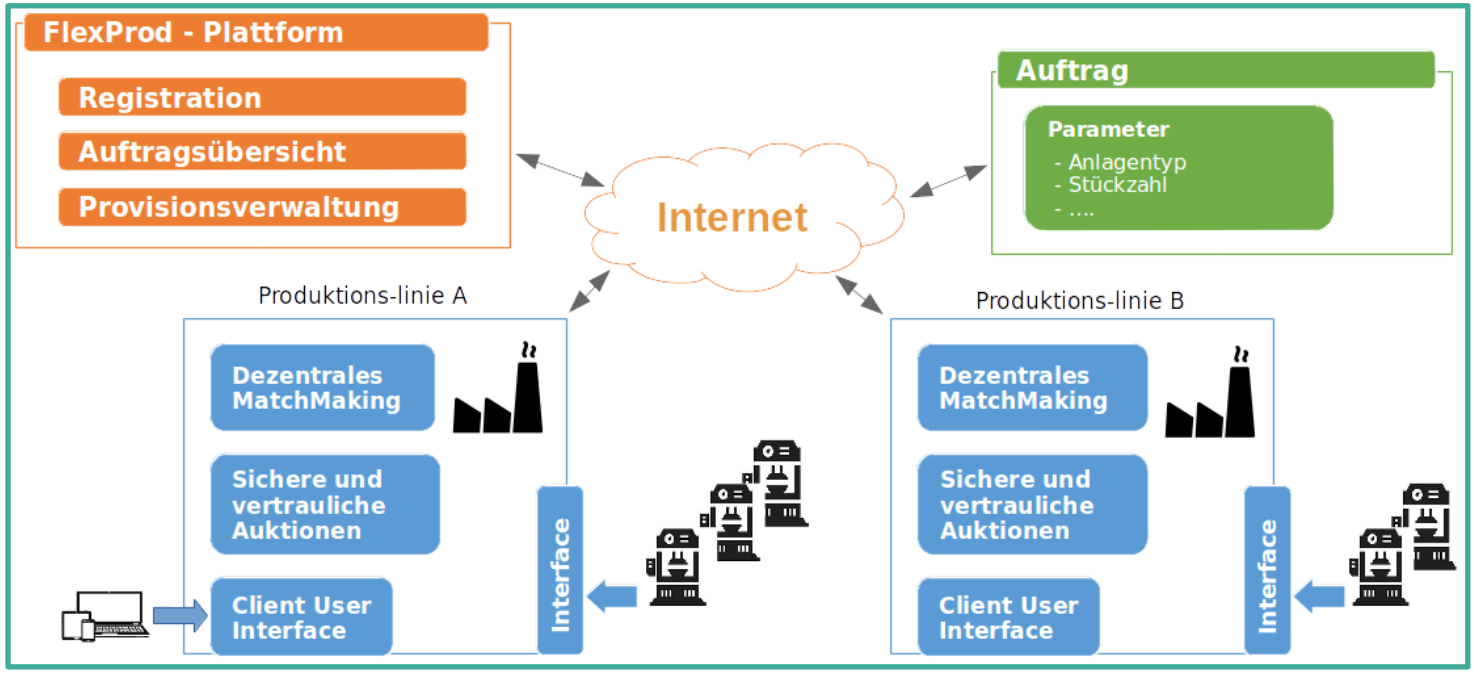
IoT Pattern



Use Case

SICHERE AUKTIONSPLATTFORM FÜR I4.0

- Decentralized system for contracting and outsourcing of manufacturing capacities => **Decentralized**
- Development of a (Cloud-)based secure auction platform for industry 4.0 => **Secure by Design**
- Critical business data is protected but still assured authentic => **E2E Verifiability**



https://www.catch.direct/

CHALLENGES AHEAD

Collaboration in Data Spaces: How can (decentralized) cryptography help to increase collaboration?

How are the geopolitical changes affecting your view on IT: How save is your data in hyperscaler infrastructures?

Digital Sovereignty more important than ever: Local Infrastructure vs. Cryptography?

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Thomas Lorünser

AIT Austrian Institute of Technology
Giefinggasse 4 | 1210 Wien
Thomas.Loruenser@ait.ac.at