•Secure Machine Learning in the Cloud

•

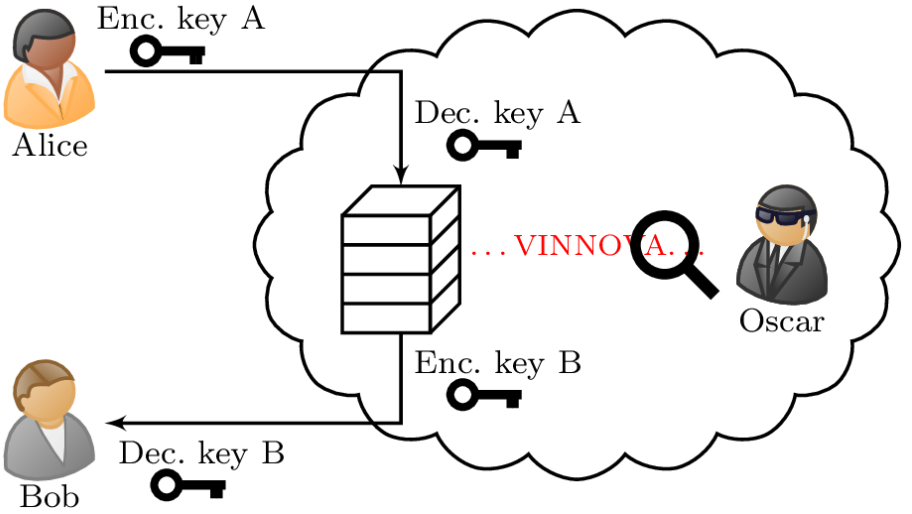
Roland Hostettler

- Department of Electrical Engineering
- Uppsala University
- E-Mail: roland.hostettler@angstrom.uu.se

UPPSALA UNIVERSITET

Background

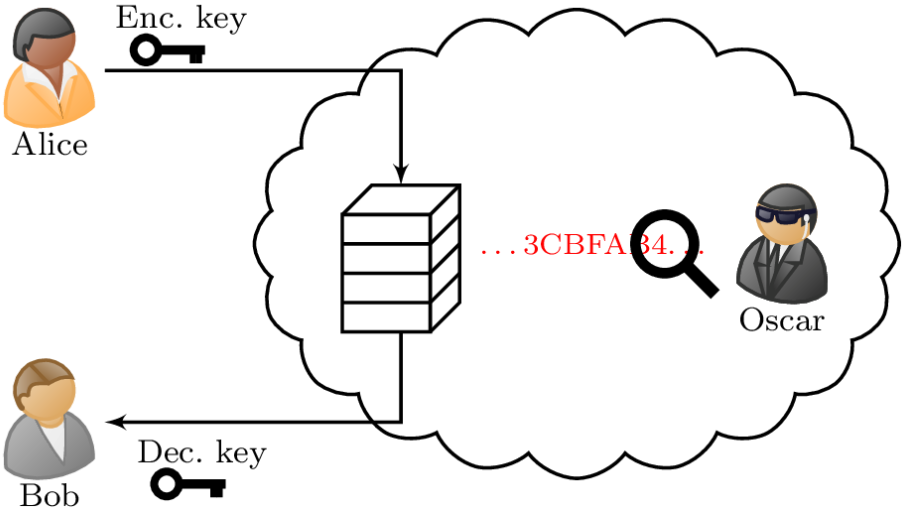
- Machine learning:
  - Key in industry (process, automotive, healthcare, ...)
- Cloud/edge computing (MLaaS):
  - Scalable and flexible
  - Subject to provider's security measures
  - Local legislation
- Data sharing:
  - Cyberattacks
  - Privacy concerns
  - Industrial or governmental espionage
- Federated learning:
  - Often only shares derived data



UPPSALA UNIVERSITET

Goals

1. Data security:
    - Machine learning using homomorphic encryption
2. Integrity preservation:
    - Machine learning using differential privacy
3. Application platform requirements & demonstration



Partners

UPPSALA
UNIVERSITET

SKYDOME

intel®

UPPSALA
UNIVERSITET

Collaboration Opportunities

- Research
- Industrial stakeholders
  - Use-cases
  - Reference group
- Verification and auditing

UPPSALA
UNIVERSITET

•Contact Information

•

Roland Hostettler

• Project Leader

• Department of Electrical Engineering

• Uppsala University

• E-Mail: roland.hostettler@angstrom.uu.se

UPPSALA
UNIVERSITET