simula@uib

General information

Simula@UiB – Forskningssenteret for Informasjons-og kommunikasjonssikkerhet

Contacts –

- **Håvard Raddum** haavardr@simula.no
- **Øyvind Ytrehus** oyvindy@simula.no
- **Kjell Jørgen Hole** hole@simula.no

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	Y
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms	Y
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	N
○ Authenticated encrypted token research for mobile payment solution	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

simula@uib

Competencies

- *Organisation competencies/Skills we can bring:*
  - Cryptography and cryptanalysis
  - Information and coding theory
  - Software security

- *Organisation experience in the European project:*
  - As company: Limited (new company, started June 1)
  - Have been partners in NESSIE, ECRYPT, Marie Curie, other projects…

simula@uib

Project idea

- *Functional encryption for cloud databases*
  - Main components: Functional encryption, Efficient implementation, Privacy-preservation , Quantum safe cryptography, Automated proof techniques for FE
  - Simula@UiB, UoB, RU Bochum, U Graz, INRIA
- *List of the complementary skills you need for your consortium*
  - Development to technology readiness level 3-5
  - Stakeholders: regulators, users

simula@uib

Functional Encryption for Cloud Databases

Goal: Implement useful Functional Encryption schemes for cloud computing

Research:

- **Functional Encryption, realisations**
- **Fully Homomorphic Encryption schemes, efficiency and security**
- **Privacy-preserving mechanisms in a cloud computing environment**

simula@uib

Want to be quantum safe

Intend to implement solution(s) using quantum safe crypto:

- **Lattice based and coding based crypto**
- **Encryption schemes based on MQ problem**
- **Ring Learning With Errors**

simula@uib

Consortium

We have:

- **Academic partners with high expertise in cryptography research (TU Graz, RU Bochum, INRIA, UoBergen)**

We need:

- **Partner(s) with expertise in implementing advanced cryptography (industry)**
- **Stakeholder/end-user(s) who would benefit from a functional encryption solution**