h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

fbi
FACHBEREICH INFORMATIK

ATHENE
National Research Center
for Applied Cybersecurity

– Master-/Bachelor Thesis –
Multi-Party Computation for Biometrics

da/sec

da/sec is the biometrics and Internet security research group and is affiliated with University of Applied Sciences Darmstadt and the National Research Center for Applied Cybersecurity (ATHENE). The group is led by Prof. Dr. Christoph Busch. The focus of the group is on highly innovative and applied IT security research in the special fields of biometrics and internet security. Read more on www.dasec.h-da.de.

Motivation & Goal

Biometric data is considered sensitive personal information by the GDPR and therefore needs to be protected. Multi-Party Computation (MPC) is a cryptographic protocol that enables the evaluation of public functions on private inputs. The goal of this project is to investigate how MPC can assist in protecting biometric information.

Tasks

- Implement biometric comparison using MPC
- Assess security and privacy properties according to ISO/IEC 24745
- Benchmark computational performance

We offer

- Incentives for the student to work on this project (work within scientific context, international collaboration, work on project in collaboration with companies)

Requirements

- High motivation and creativity
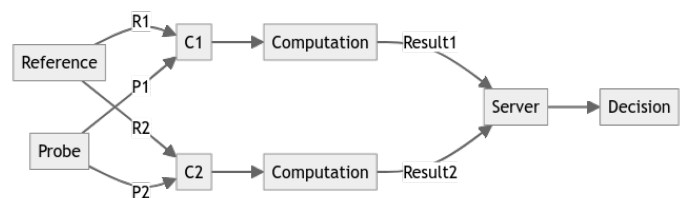- Analytical and programming skills
- Strong interest in research

By Date

By now / by appointment

Contact

Florian Bayer
florian.bayer@h-da.de

h_da
Faculty of
Computer Science

ATHENE–National Research Center for Applied Cybersecurity
da/sec – biometrics and internet security research group
Schöfferstraße 8b
64295 Darmstadt