h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

ATHENE
National Research Center
for Applied Cybersecurity

– Master-/Bachelor Thesis –

Multi-Party Computation for Biometric Information Protection

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. Harald Baier and Prof. Dr. Christoph Busch. The focus of the group is on highly innovative and applied IT security research in the special fields of biometrics, internet security, and digital forensics. Read more on www.dasec.h-da.de.

Motivation & Goal

Biometric data is considered sensitive personal data both by the GDPR and the ISO/IEC 24745 standard on biometric information protection- Therefore, it requires adequate protection. Multi-Party Computation (MPC) protocols are cryptographic protocols that allow several parties to jointly evaluate an arbitrary function without revealing the input data to one another. Thereby, they can be used to securely compute biometric distance computations and compare biometric templates securely.

Tasks

- Select a suitable MPC protocol
- Prepare biometric templates for the use in MPC
- Benchmark computational efficiency

Requirements

- High motivation and creativity
- Strong interest in research
- Programming experience




Start Date

By appointment

Contact

Pia Bauspieß
pia.bauspiess@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