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

ATHENE
National Research Center
for Applied Cybersecurity

– Master-/Bachelor Thesis –

Homomorphic Encryption 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 data and requires to be stored irreversible, unlinkable, and renewable according to the standard ISO/IEC 24745 on biometric information protection. Homomorphic encryption allows to perform operations on the ciphertext that directly effect the plaintext. This can be used to compute the distance between two biometric templates in the encrypted domain without revealing the sensitive data.

Tasks

- Select a suitable encryption scheme
- Prepare biometric templates for encryption
- Benchmark computational efficiency in the encrypted domain

Requirements

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




By 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