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

ATHENE
National Research Center
for Applied Cybersecurity

– Master-/Bachelor Thesis –

Post-Quantum Protection for Biometric Systems

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

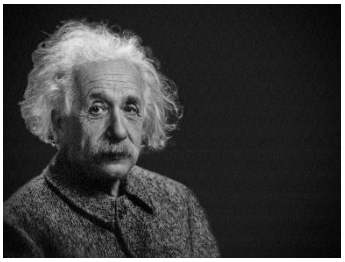
Biometric data is considered sensitive personal and can be used to identify individuals over long periods of time. Therefore, long-term protection is required to secure biometric templates. In terms of cryptographic algorithms, applying post-quantum cryptography yields protection of the biometric data even if an attacker had access to a quantum computer. This protection is vital as of today, as it is also feasible for an attacker to record classically protected biometric templates today, and reverse them later using a quantum computer.

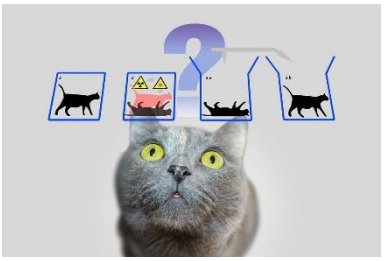
Tasks

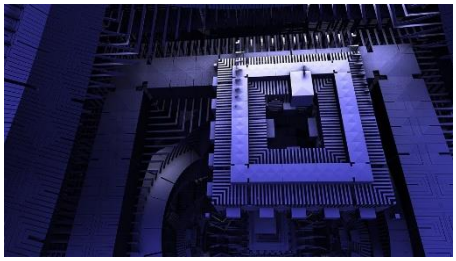
- Select a post-quantum algorithm
- Upgrade a classically protected system to post-quantum security
- Benchmark computational efficiency

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