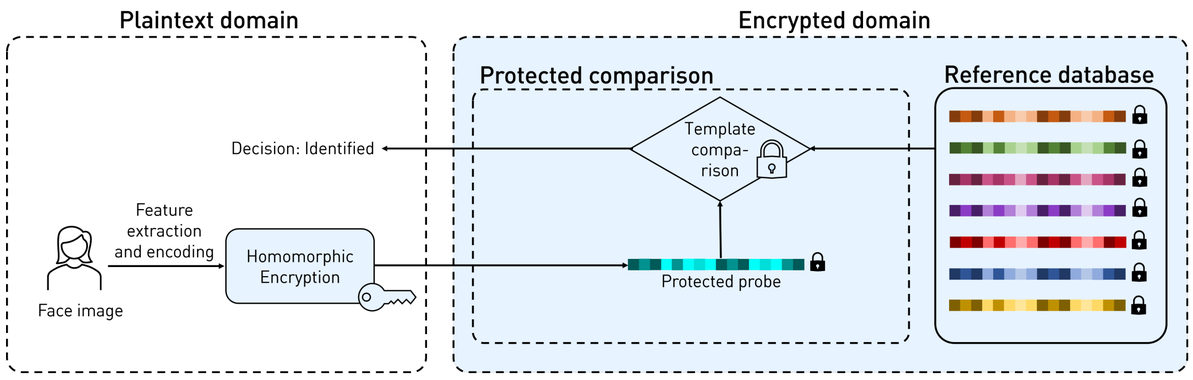
Efficient Privacy Protection for Biometric Identification Systems

NTNU

Objective

- The PhD project aims at contributing new solutions to efficient and secure biometric identification systems using homomorphic encryption and other privacy-preserving computation techniques.
- Encryption techniques applied for biometric information protection introduce an additional computational workload.
- Therefore, a key focus of the PhD project is improving the efficiency of protected biometric systems.



Homomorphically encrypted biometric identification

Research Questions

- Which privacy-preserving computation techniques are best suited for biometric information protection? How do different approaches to biometric information protection compare in terms of their security and efficiency?
- How can computational workload reduction be applied to improve the efficiency of homomorphic encryption in biometric identification systems?
- How can biometric systems be secured against quantum adversaries? In particular, which quantum adversary models need to be considered for biometric systems?

Approach

- State-of-the-art encryption techniques are evaluated and applied practically to secure biometric templates of different modalities.
- The designed systems are evaluated in terms of recognition accuracy, computation efficiency and security.
- Computational workload reduction techniques such as feature transformation or preselection are transferred to the encrypted domain while maintaining the security of the baseline system.
- The practical long-term security of biometric data will be investigated by applying and evaluating post-quantum cryptography for biometric systems.

NTNU

ATHENE
National Research Center for Applied Cybersecurity

Pia Bauspieß
pia.bauspiess@ntnu.no

Prof Dr. Christoph Busch
christoph.busch@ntnu.no

Dr. Anamaria Costache
anamaria.costache@ntnu.no

Norwegian University of Science and Technology – Norwegian Biometrics Lab