Use of biometrics for regeneration of cancelable post-quantum crypto-biometric keys

Supervisors : Bernadette Dorizzi
Dijana Petrovska-Delacrétaz

PhD student : Mohamed Amine HMANI

TELECOM SudParis

IP PARIS

INSTITUT
POLYTECHNIQUE
DE PARIS

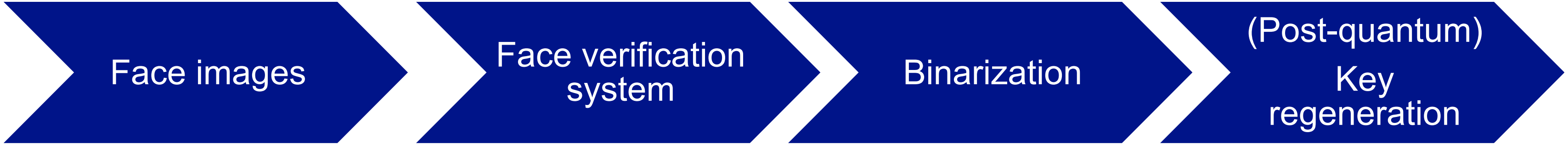
Objective

- Create cryptographic keys from biometric data that are resistant to quantum computing.

Motivation

- Advances in Quantum computing
- Non-repudiation
- Revocability

Plan


Face images

Face verification system

Binarization

(Post-quantum) Key regeneration

+ Easily accessible
+ Publicly available large datasets
- Can not be used as encryption keys
- high variability

- High FAR → low entropy
- High FRR → low probability of key successful regeneration

➔ Need for high accuracy

- State of the are face recognition systems use real representation ➔Need for binary format
- Binarization must not degrade the performance of the face verification system

- Need for stable bit-string input
- Revocable
- Symmetric encryption

Face verification system: Contributions

IMPLEMENTATION IN THE H2020 SPEECHXRAYS PROJECT AND TESTED ON 2000 USERS

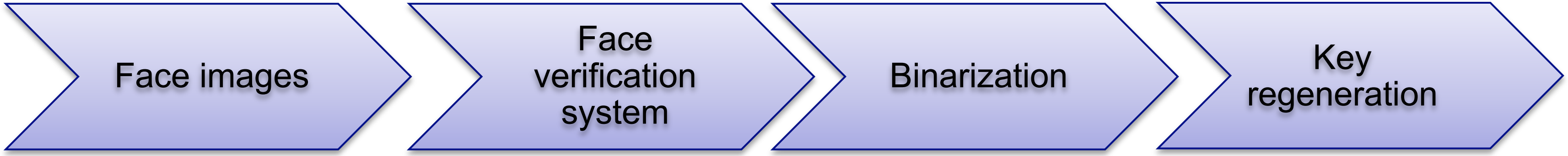
+

CANCELABLE VERSION

IMPLEMENTATION IN THE H2020 EMPATHIC PROJECT

PARTICIPATION IN THE NIST SRE'19 MULITIMEDIA CHALLENGE (BEST SINGLE SYSTEM ON FACE)

Results



Face images

Face verification system

Binarization

Key regeneration

- DNN Based on Facenet
- Triplet Loss
- 99.8% Accuracy on LFW
- 1% HTER on Mobio

- DNN based binarization
- Auto-encoder with triplet loss
- Variable length binary embeddings from 128 bits to 8012 bits
- 99% Accuracy on LFW
- 1% Accuracy on Mobio

- Fuzzy commitment
- Use BCH-encoding
- Use of a cohort
- 528-bit symmetric keys
- 1% FRR on Mobio
- 0.3 % FAR on Mobio