PhD topic for Oubaida Chouchane: Cryptographic primitives for GDPR compliant Biometric applications

Biometrics recognition technology has revolutionised traditional person recognition technologies which rely on tokens or passwords. Whereas the latter can be lost, stolen, or easily forgotten, biometrics technology relies on biological and/or behavioural traits to infer identity [1]. Such activities must be regulated and monitored in order to ensure they do not violate the right to privacy and related rights. The new European general data protection regulation (GDPR) demands stringent provisions for privacy preservation in biometric applications. Due to the fact that the link between individuals and their biometric characteristics, e.g. fingerprints or iris, is strong and permanent, biometric reference data (templates) need to be protected in order to safeguard individuals' privacy and biometric system security. Unprotected storage of biometric reference templates poses severe privacy threats, e.g. identity theft, cross-matching, or limited renewability. In fact, biometric data are defined as sensitive data within the European Union (EU) GDPR 2016/679, which means that the use of these data is subjected to the right of privacy preservation.

In order to comply with the General Data Protection Regulation (GDPR), biometric operations should be performed without disclosing any sensitive information. Homomorphic encryption [2] and secure multi-party computation [3] can be considered as suitable cryptographic tools for the design of novel primitives as they allow some functions to be evaluated by one or multiple parties without discovering any information than what is needed. Nevertheless, the integration of these tools, while delivering privacy protection, may impact on systems' operation/performance. Some complex operations cannot be supported by existing practical tools and therefore may need to be approximated by simpler operations. It is critical, however, that these approximations do not degrade security. The PhD candidate will research privacy preserving biometric identification and authentication primitives by leveraging such advanced cryptographic techniques, while minimizing computational, memory and bandwidth costs and accuracy degradation.

Research plan

The objectives of this PhD study are as follows:

1. Study existing biometric systems and their main building blocks, and identify the privacy, security and performance challenges, accordingly.
2. Get familiar with advanced cryptographic primitives including homomorphic encryption and secure mutli-party computation.
3. Propose new privacy preserving biometric authentication solutions: Since most of these solutions make use of neural networks, the goal is to develop their privacy preserving variants using advanced cryptographic tools such as homomorphic encryption and/or secure multi-party computation. The student will first study existing privacy preserving neural network solutions such as [4,5] and further propose new mechanisms suitable to biometric recognition.
4. Evaluate the proposed solutions in terms of privacy, security and performance. Indeed, solutions should deliver an acceptable trade-off between security, privacy, computational efficiency, and communication and memory overhead.

References

[1] A. K. Jain, A. Ross and S. Prabhakar, An introduction to biometric recognition, in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004

[2] C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, Stanford University and IBM Watson, 2009

[3] U. Maurer, Secure Multi-party Computation made simple, 2002

[4] S. Wagh et al., FALCON: Honest-Majority Maliciously Secure Framework for Private Deep Learning, PETS 2021

[5] F. Bourse et al., Fast Homomorphic Evaluation of Deep Discretized Neural Networks, CRYPTO 2018