Post-quantum cryptographic methods for protection of information and matching of secure information, including biometric data and responses from behavioural and physical unclonable functions

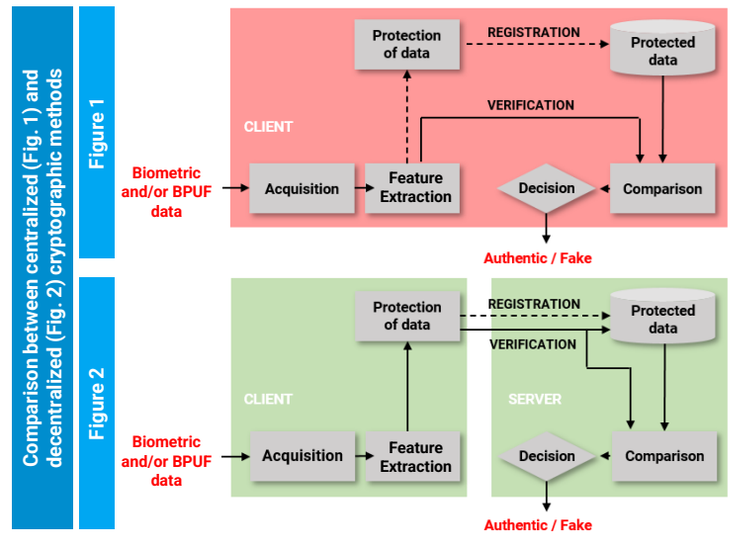
The Problem

With the daily growth in the number of e-transactions and the increasing adoption of Internet, not only by people but also by things (IoT), it is essential to ensure and prove that only the authentic people and IoT devices are accessing to online services. Biometric data (from faces, vein patterns,...) are employed to represent a person univocally. The responses from electronic **Physical Unclonable Functions (PUFs)** are employed to represent an electronic device univocally. There are two main problems with biometric data and PUF responses: (1) they are not exactly the same but are somewhat noisy, even provided by the authentic people or thing, and (2) they can be copied if employed in unprotected domains. Due to the first problem, standard cryptographic methods cannot be employed for biometric and PUF data. Due to the second problem, the biometric and PUF data are only employed in a device-centric topology (Fig. 1), in which the acquisition, processing and the storage of the biometric and PUF data are performed locally in a presumably secure device, for example, a smartphone. Therefore, the person is who the smartphone says he/she is or, in the absence of person, the device authenticates itself, with no third-party verifiers being able to prove that the person or device truly presented their data. **Researchers from University of Seville have developed cryptographic methods to protect noisy data** (such as biometric and PUF data) and match those protected data, without revealing sensitive information, as in Fig. 2. This can be employed in decentralized topologies, from the typical client-server scheme to the peer-to-peer scheme of recent blockchains. **These methods are resistant to attacks from quantum computers, so that they offer long-term security**. Since the use of multi-modal biometric data (combinations of faces, vein patterns, ...) is more secure than the use of only one kind of data, the researchers from University of Seville have developed **Behavioral and Physical Unclonable Functions (BPUFs)**, which are more secure than currently employed PUFs.

Technology description

The researchers have developed **post-quantum cryptographic methods for protecting sensitive information and matching the protected information**. Sensitive information can be represented by noisy data, such as biometric data and BPUF responses. The methods can be employed by architectures centered in a client as well as distributed and decentralized architectures with one or more parties besides the client, all of them protecting the sensitive information extracted by the client and allowing secure electronic transactions carried out by the client. In the case of architectures with three or more parties, the methods preserve the privacy of the client. A BPUF can exploit some intrinsic hardware of the device (its SRAM, for example) or can be added as a dedicated hardware block in the device.

There are many applications for the methods and the BPUFs related to people and device authentication and identification and the establishment of secure communication channels. Particularly, decentralized applications using blockchain technologies to ensure the external verification of digital credentials and to allow their traceability.



Benefits

This novel technology provides many benefits:

- The **cryptographic methods offer post-quantum security** and satisfy irreversibility, privacy, revocability and unlinkability properties. The sensitive information protected with these methods will remain protected even when quantum computers become a reality.
- The cryptographic methods are **based on proven post-quantum algorithms** (NIST 3-round post-quantum cryptography finalists).
- The client providing authentic but somewhat noisy information (biometric and/or BPUF data) can perform **secure electronic transactions, without the need of storing cryptographic keys**.
- There are external evidences (proofs) of the protected data provided by the person and/or device, which **can be employed for legal or forensics purposes**.
- **Security is achieved not only at software level but also at physical level**: at biometric level for people and at hardware level for devices.
- The **use of BPUFs reduce the risk of modelling and physical attacks to PUFs** as they consider dynamic in addition to static behaviour. Hence, counterfeit devices are better avoided and detected with BPUFs.

Stage of development

The cryptographic methods for protection of sensitive information and matching of protected information were successfully verified by considering code-based cryptography (Classic McEliece), facial biometrics and the implementation in a smartphone acting as a client device. The security level can be of 256 bits, false rejections are preserved with respect to the unprotected scheme and false acceptances can be 0, memory requirements of the protected information is very low, and recognition is carried out at real time.

The BPUFS were analysed experimentally using SRAMs of 90-nm CMOS technology. The highest probability of a successful attack was evaluated experimentally as 1.5e-34, considering changes in the operating conditions (power supply voltage, temperature, and aging). BPUFs have also been analysed experimentally using SRAMs in microcontrollers and Ring Oscillators in FPGAs of 90 nm and 28 nm.

Intellectual property
European Patent Application submitted in July of 2019 with application number EP 19382623.7. European Patent Application submitted in April of 2022 with application number EP 22382418.6

Represented Institution and inventor:

The researchers behind the innovation belong to Seville Institute of Microelectronics (IMSE-CNM), an R+D+i joint center of the University of Seville and the Spanish National Research Council (CSIC), which together with its counterpart institutes in Barcelona and Madrid, forms part of the National Microelectronics Center (CNM) in Spain. The research group has extensive experience in cybersecurity, working with worldwide renowned IT companies and organizations. Other projects they are currently working on include "Mas+Cara: Proof of concept of a decentralized and private facial recognition scheme with post-quantum security", and "HardWallet: Trusted and post-quantum secure hardware for wallets of decentralized identities using bio and device metrics".

Objective of the collaboration:

The represented institution is looking for a collaboration that leads to commercial exploitation of the presented invention. The ideal scenario would be to reach an agreement in order to transfer the technology by a license (exclusive or non-exclusive) of the patented procedure, or a co-development. However, the form, terms, and conditions of the collaboration can be openly discussed if the presented technology is of interest.

Contact: Iluminada Baturone, Univ. of Seville, Seville Institute of Microelectronics
lumi@imse-cnm.csic.es