A Facial Authentication System Using Post-Quantum-Secure Data Generated on Mobile Devices

Paula López-González†, Rosario Arjona, Roberto Román, Iluminada Baturone
Instituto de Microelectrónica de Sevilla (IMSE-CNM)
Universidad de Sevilla, CSIC
Seville, Spain
{paula,arjona,roman,lumi}@imse-cnm.csic.es

ABSTRACT

This paper describes a demonstrator of a post-quantum-secure facial authentication system distributed between a mobile device acting as a client and a remote computer acting as an authentication server. Homomorphic encryption based on Classic McEliece, one of the fourth-round candidates of the NIST post-quantum standardization process, is carried out by the client for protecting the biometric data extracted from the users' faces at enrollment and verification. The remote computer only stores and compares the received protected data, thus preserving user privacy. An Android App and a Graphical User Interface (GUI) were implemented at the client and the server, respectively, to show the system performance in terms of computation and security.

CCS CONCEPTS

•Security and privacy •Security services •Privacy-preserving protocols •Pseudonymity, anonymity and untraceability •Biometrics •Public key encryption •Client-server architectures

KEYWORDS

Biometric template protection, homomorphic encryption, post-quantum security, distributed and mobile architectures.

ACM Reference format:

Paula López-González, Rosario Arjona, Roberto Román and Iluminada Baturone. 2022. A Facial Authentication System Using Post-Quantum-Secure Data Generated on Mobile Devices. In *The 28th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '22), October 17-21, 2022, Sydney, NSW, Australia, 2 pages.* https://doi.org/10.1145/3495243.3558761

1 Introduction

Biometric authentication systems have become very popular in the last decade, especially after being included in common smartphones. In these systems, generally, two phases have to be performed: enrollment and verification. At the enrollment phase, biometric captures are acquired and biometric features are extracted and stored as templates. At the verification phase, fresh biometric features are extracted and compared with those stored. If the comparison result satisfies a threshold, the authentication is successful. These systems can have a device-centric or a distributed architecture. In a device-centric architecture, all operations are performed on the device, usually a mobile device. Meanwhile, in a distributed architecture, acquisition and feature extraction are performed on the mobile device, but storage, comparison and decision are performed externally. The advantage of the distributed architecture is that there is external evidence because the remote computer compares biometric features. However, the extracted features, which are sensitive data, must be protected.

Among biometric template protection schemes, homomorphic encryption has the capability to perform mathematical operations on encrypted data, resulting in the same way as performing operations on plaintext. With the advent of quantum computers, post-quantum cryptography should be considered in biometric template protection schemes. In addition, security should be supported by standards. One of the fourth-round candidates of the NIST Post-Quantum Cryptography Standardization process [1] in the category of Public-key Encryption algorithms is Classic McEliece [2]. The security of the McEliece cryptosystem has remained stable for over 40 years and it is based on the hardness of decoding random binary linear codes.

This work is the demonstration of a distributed and post-quantum-secure system for facial authentication based on homomorphic encryption and Classic McEliece. This paper is organized as follows. The proposed distributed and post-quantum-secure facial authentication system is summarized in Section 2. Section 3 presents the main features of the demonstrator and the experimental results obtained. Finally, Section 4 shows the conclusions.

2. Proposed system

It is assumed that a user needs authentication to gain access to a service provided by a remote server (for example, of a bank or a fuel station) and the user only wears a mobile device (for example, a smartphone). In our proposed system, a mobile device client, using a camera, detects the user's face

ACM MobiCom '22, October 17–21, 2022, Sydney, NSW, Australia

ACM ISBN 978-1-4503-9181-8/22/10…$15.00
https://doi.org/10.1145/3495243.3558761

with a convolutional network (CNN) called BlazeFace [3] and extracts facial features from the detected face with the Facenet CNN [4]. The extracted features, also called embeddings, have 128 floating-point data. Subsequently, they are quantized and binarized by applying the Linearly Separable Subcode (LSSC) algorithm [5]. Then, they are conveniently padded and encrypted using the Classic McEliece encryption algorithm and the public key of the authentication server of the particular service needed by the user. Finally, they are sent to the remote computer, at the enrollment phase to be stored as protected template, and at the verification phase to be matched with the stored one. It has to be noticed that the enrollment has to be done once, typically when the user hires the service, and in a controlled scenario. On the other side, the verification phase can be done many times, at any place and conditions.

It is convenient that each user has an associated ID. This way, the authentication server stores the protected template indexed by the ID at the enrollment. At verification, the server retrieves the protected template with the received ID and computes its encrypted similarity with the fresh encrypted data received. Using the Classic McEliece decoding algorithm and its private key, the server decodes the encrypted similarity, and if it satisfies a prefixed threshold, the user is authenticated.

3. Realization of the demonstrator

An Android application (App) has been implemented as a client on a Huawei P40 smartphone. The App, which uses the frontal camera to capture facial images, was developed in Java using Android Studio. BlazeFace and Facenet Tensor Flow Lite models were included to detect and extract facial features, respectively. The ClassicMcEliece6688128 parameter set was selected to provide a security of 256 bits. The Classic McEliece code, programmed in C, was included using the Java Native Interface (JNI). The authentication server was developed on a computer with an Intel Core i5-9400F processor and Ubuntu 20.04 as operating system. On the authentication server, a Python program was developed that includes the Classic McEliece C library. The smartphone takes around 60 ms to generate the protected data, meanwhile the computer takes 85 ms to compare protected data and make the authentication decision.

In order to illustrate the proposed system, a Graphical User Interface (GUI) was developed in Python using tkinter to simulate the servers of two different services, one of a bank and another of a fuel station. Both the servers and the Android App employ an event log in which all the operations performed are shown in a step-by-step mode.

(a) (b)

Figure 1: (a) Android App authenticating a user and (b) Authentication Server GUI after an authentication

An adversarial scenario is shown in this demonstrator, where a malicious authentication server tries to get information about the protected data. It is seen how the malicious server fails in its decoding trials, since the protected data are created so that they cannot be decoded.

The demonstration also illustrates that the proposed system satisfies the security requirements of irreversibility, revocability and unlinkability established in the ISO/IEC 24745 standard [6], in addition to a stolen-device scenario where an attacker employs the smartphone of an enrolled user. Fig. 1 shows the Android App and an authentication server GUI illustrating the main steps of the proposed system.

4. Conclusions

A demonstrator has been developed to show the performance of the proposed distributed and post-quantum-secure facial authentication scheme based on Facenet CNN, homomorphic encryption and Classic McEliece. It is composed of an Android App, which acts as a client, and a Python program, which acts as an authentication server on a remote computer. Authentication is performed at real time, with a total computation time of 145 ms. Security is of 256 bits, resistant to stolen-device attacks and satisfying irreversibility, revocability, and unlinkability requirements.

ACKNOWLEDGMENTS

This research was conducted thanks to Grant PDC2021-121589-I00 funded by MCIN/AEI/10.13039/501100011033 and the "European Union NextGenerationEU/PRTR", and Grant PID2020-119397RB-I00 funded by MCIN/AEI/ 10.13039/501100011033. The work of Roberto Román was supported by VI Plan Propio de Investigación y Transferencia through the University of Seville.

REFERENCES

[1] NIST Post-quantum Cryptography fourth-round submissions. Accessed: Aug 08, 2022. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

[2] Classic McEliece NIST finalist. Accessed: Jul 01, 2022. [Online]. Available: https://classic.mceliece.org/.

[3] BlazeFace model available. Accessed: Jul. 01, 2022. [Online]. Available: https://github.com/tensorflow/tfjs-models/tree/master/blazeface.

[4] David Sanberg's Facenet model. Accessed: Jul. 01, 2022. [Online]. Available: https://drive.google.com/file/d/0B5MzpY9kBtDVZ2RpVDYwWmxoSUk/edit?resourcekey=0-xi62SLMG3gMyC6wTkl9Q0A

[5] M. Lim, and A. B. J. Teoh, "A Novel Encoding Scheme for Effective Biometric Discretization: Linearly Separable Subcode," in IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 2, Feb. 2013, pp. 300-313, doi: 10.1109/TPAMI.2012.122.

[6] Information security, cybersecurity and privacy protection — Biometric information protection, document ISO/IEC 24745:2022, 2022.