Securing Minutia Cylinder Codes for Fingerprints through Physically Unclonable Functions: An Exploratory Study

R. Arjona, M. A. Prada-Delgado, I. Baturone
Instituto de Microelectrónica de Sevilla (IMSE-CNM)
Universidad de Sevilla (US), Consejo Superior de
Investigaciones Científicas (CSIC)
Seville, Spain
{arjona, prada, lumi}@imse-cnm.csic.es

A. Ross
Department of Computer Science and Engineering
Michigan State University (MSU)
East Lansing, USA
rossarun@cse.msu.edu

***Abstract*—A number of personal devices, such as smartphones, have incorporated fingerprint recognition solutions for user authentication purposes. This work proposes a dual-factor fingerprint matching scheme based on P-MCCs (Protected Minutia Cylinder-Codes) generated from fingerprint images and PUFs (Physically Unclonable Functions) generated from device SRAMs (Static Random Access Memories). Combining the fingerprint identifier with the device identifier results in a secure template satisfying the discriminability, irreversibility, revocability, and unlinkability properties, which are strongly desired for data privacy and security. Experiments convey the benefits of the proposed dual-factor authentication mechanism in enhancing the security of personal devices that utilize biometric authentication schemes.**

Keywords- Fingerprint recognition; Minutia Cylinder Codes (MCCs); Physically Unclonable Functions (PUFs); Two-factor recognition; Biometric template protection; Cancelable biometrics

I. INTRODUCTION

Biometrics is the science of recognizing individuals based on their physical, behavioral or physiological attributes such as fingerprints, gait and heartbeat [1]. Biometric data should be protected because they are vulnerable to various types of adversarial attacks [2][3]. According to the data protection regulation of many countries, biometric data are categorized as sensitive data [4]. Thus, they can only be used in specific situations and privacy protection is required. Furthermore, biometric data should be replaceable (also known as renewable or cancelable or revocable) in case they are compromised [5]. In some cases, protection is extended by performing matching in the encrypted domain [6]. In addition to revocability, the resulting template[1] should satisfy the properties of irreversibility, unlinkability and discriminability [7]. A protected template is irreversible if it is computationally difficult to recover the original data from the protected template. Unlinkability ensures that it is possible to generate different versions of protected templates by incorporating different auxiliary data so that they cannot be linked to a specific individual. Discriminability ensures that the template protection scheme does not degrade the recognition accuracy of the biometric system.

Several biometric template protection schemes proposed in the literature are based on the use of a secret key to create geometric transforms, random projections, convolutions with random kernels or random permutations [8]. In invertible transformations, where the original template can be reconstructed if the secret key is known, the security depends on the secrecy of the key. The use of a secret key is also considered as a second factor in the recognition process since it also provides distinctive information. The "what you know" factor is replaced by the "what you have" factor in the technique known as Biohashing, originally proposed in [9]. It is based on a token, defined as a physical device that stores human-chosen passwords or pseudo-random sequences. The token provides a different password at different times or for a different challenge. The advantage of this solution is that passwords can be longer because they do not have to be remembered by the user. The disadvantage is that passwords should be stored in highly secure non-volatile memories, which are more expensive than standard memories, since, otherwise, passwords can be recovered from the token by attacking the memory [10] and the original template can be reconstructed.

Increasingly, the biometric data of an individual is being associated with the specific device in possession of the individual. For example, the incorporation of biometric verification mechanisms in smartphones [7] is highlighting the need to authenticate both the individual ("who you are") as well as the device ("what you have"). The highest level of security in electronic authentication as defined by the digital identity guidelines of the NIST SP 800-63 [11] is based on the possession of an authenticator device, authentication of the individual, authentication of the device which the individual owns, application of template protection techniques and performing the entire authentication operation on the same device.

An approach to increase the security of the "what you have" factor at low cost is to exploit the intrinsic hardware identity of the device through Physically Unclonable Functions (PUFs). PUFs are unique, distinctive and unpredictable identifiers extracted from intrinsic features of the hardware produced by the manufacturing process variability [12]. The device with PUFs cannot be cloned

[1] The biometric data of a subject that is stored in a gallery database, either as raw data or as a condensed feature set, is referred to as the *template* of that individual.

physically because the manufacturing process introduces variations that are specific to each device. The PUF identifiers are not stored but, rather, are generated on the fly. Therefore, adversarial attacks are expected to be more complex since they should be performed during operation of the device. Among the various electronic circuits employed as PUFs (SRAMs, latches, D Flip-Flops, arbiters, ring oscillators, etc.), in this work we use SRAM PUFs since no additional circuitry is needed [13]. Commonly, SRAMs are readily present in popular devices. For example, many parts of a smartphone include memories: Bluetooth chips, inertial sensors, pedometers, cameras, etc. The use of SRAMs as PUFs involves reading the start-up values when the memory is switched on and no data are written.

Since sequences provided by PUFs are binary and non-predictable, the XOR fusion operator is very suitable to combine them with biometric information and to obfuscate biometric data efficiently (which ensures irreversibility). Discriminability is ensured with PUFs because, on the one hand, PUF sequences generated from different devices are quite different due to the random variability of the manufacturing process, and, on the other hand, PUF sequences generated from the same source are very similar. Finally, many sequences can be provided by a PUF (for example, low-cost SRAMs contain tens, hundreds or thousands of kilobits). Hence, revocability and unlinkability are achieved even when using the same device.

However, the XOR operation requires biometric features to be represented as binary, ordered and fixed-length vectors. The work presented in [14] employs a level-1 fingerprint feature based on a directional image window centered at the convex core point to create a compact representation composed of a fixed number of binary ordered elements. Several samples and several fingers are considered, and the feature vectors are combined with PUF data created by simulations with the parameters determined in [13]. In this work, we utilize a level-2 fingerprint feature known as Minutia Cylinder Codes (MCCs) whose representation is based on cylinders that encode spatial and directional relationships between each minutia and its neighborhood [15]. MCCs have been employed for fingerprint identification as well as for indexing applications [16]. The vector obtained for each cylinder is invariant, fixed-length and bit-oriented. The P-MCC variant is more suitable for template protection since it is a non-invertible and protected MCC representation [17].

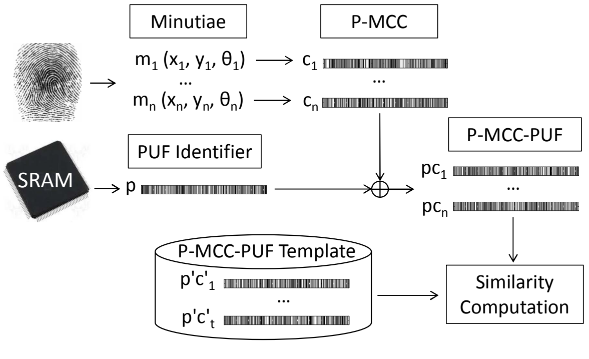


Figure 1: Dual-factor recognition scheme based on P-MCC-PUFs.

Dual-factor recognition based on MCCs [18] and P-MCCs [19] have been proposed in the literature by using permutations of the cylinder elements determined by a secret key. In our approach, the fusion with PUFs considers P-MCCs that do not include minutia information, unlike the case of templates based on MCCs. Thus, all the information from the P-MCC template is fused with the PUF data. In addition to dual-factor recognition (imparted by the discriminability of P-MCC and PUF identifiers), the fusion of P-MCCs and PUFs results in a dual-factor template protection mechanism (the protected MCCs are obfuscated by the information given by PUFs).

This paper is structured as follows. Section 2 includes a brief description of the representation and matching using MCCs and P-MCCs. The extraction process of PUF-based identifiers from SRAMs is described in Section 3. Details of how P-MCCs and PUF-based identifiers are fused are provided in Section 4. The proposal is evaluated in Section 5 in terms of recognition performance and security analysis, and is compared to other proposals in the literature. Finally, conclusions are presented in Section 6.

II. Fingerprint Identifiers from MCCs

MCCs, proposed in [15], are fingerprint features based on minutiae which are suitable for template protection [19]. Cylinders offer the advantages of being invariant to translation and rotation, tolerant to noise, and suitable for fixed-length and bit-based representations. Furthermore, the accuracy of MCCs is slightly better than some of the most accurate commercial algorithms evaluated in the context of the FVC-onGoing competition [20].

A cylinder is created for each minutia in a fingerprint by encoding spatial and directional relationships between the minutia and its neighborhood. According to the ISO/IEC 19794-2 template format, minutiae are represented by their locations and directions in the range $[0, 2\pi)$. The cylinder, which is created with a predefined radius and a height of 2π, is inside a cuboid centered at the minutia location and whose base is aligned with the minutia direction. The cuboid is discretized into N_S x N_S x N_D cells, where N_S is the number of cells along the cylinder diameter (associated with the spatial distances to the cylinder minutia) and N_D is the number of cylinder sections (associated with the directional distances to the cylinder minutia). The value of a cell represents the likelihood of finding minutiae with locations and directions that are close to the cell location and direction. The numerical value of a cell is calculated by accumulating the spatial and directional contributions from each minutia belonging to a predefined neighborhood around the cell center. For a bit-based MCC representation, a unit step function compares the accumulated contributions with a predefined threshold to assign the value 0 or 1 (or invalid) to each cell.

TABLE I. COMPARISON OF PROPOSALS BASED ON MCCS

	FVC 2002 DB2a		FVC 2002 DB3a	
Proposal	EER	FMR$_0$	EER	FMR$_0$
MCC16b	0.64	1.57	5.90	17.50
P-MCC32	5.37	15.57	14.72	66.21
P-MCC-PUF32	4.05	11.57	8.77	41.64
P-MCC64	2.54	8.75	9.81	47.18
P-MCC-PUF64	1.45	2.82	4.76	24.71
P-MCC128	1.53	2.89	6.62	29.82
P-MCC-PUF128	0.75	1.54	3.07	9.57
P-MCC256	1.03	1.57	5.68	22.14
P-MCC-PUF256	0.46	0.46	0.99	3.64
P-MCC512	0.92	1.43	4.34	19.29
P-MCC-PUF512	0.43	0.57	1.17	1.32
P-MCC1024	1.13	1.79	4.93	15.14
P-MCC-PUF1024	0.39	0.39	0.81	0.82
MCC16d2048 [18]	0.42	-	3.84	-
2P-MCC64 [19]	1.1	1.4	4.4	11.8

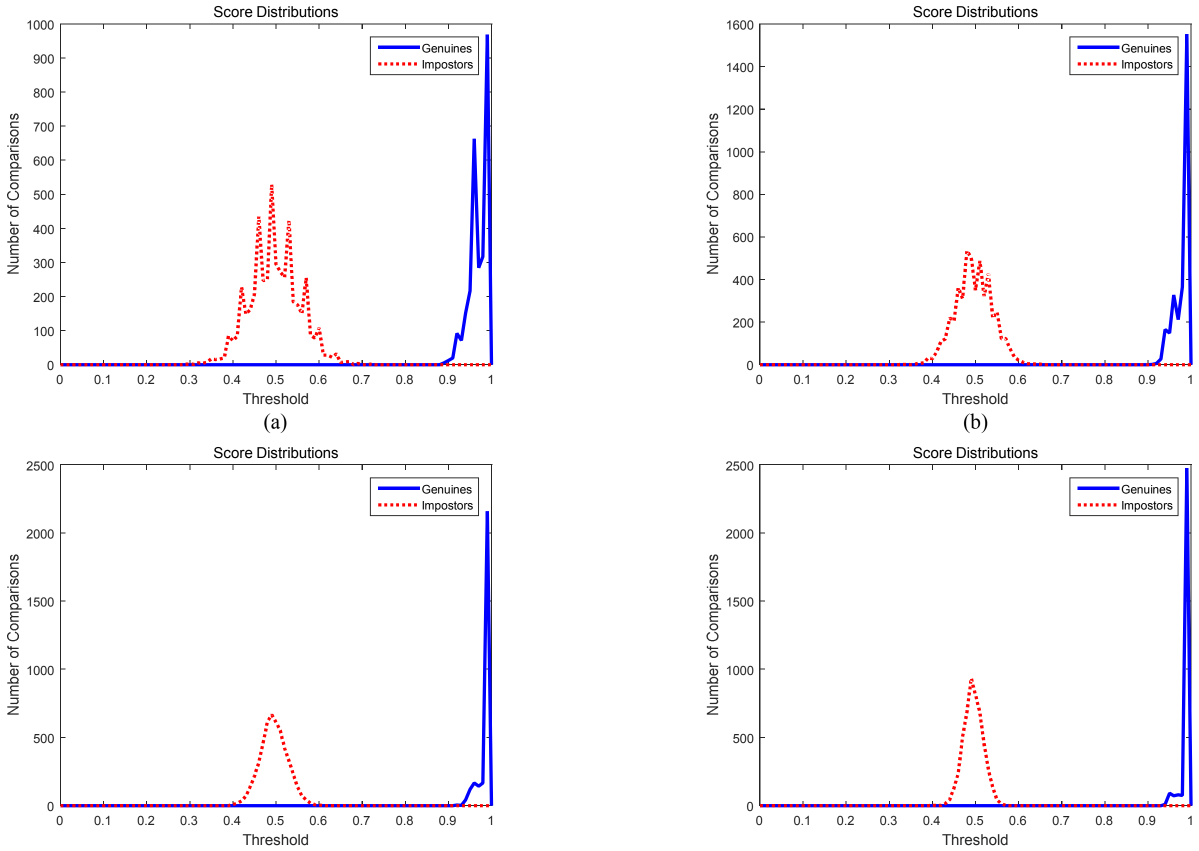
EER and FMR$_0$ are expressed in %

The noninvertible P-MCC representation [17] is created by the application of a dimensionality reduction operation based on Karhunen-Loeve (K-L) projection followed by a binarization step. In this representation, each cell takes the value 0 or 1 (the invalid value is substituted with 0 for simplicity). In contrast to the MCC representation, which usually includes minutia information to allow matching at global level based on the relative placement and directional differences of minutiae, P-MCC identifiers do not store minutiae. Thus, the comparison between two P-MCC identifiers is only performed in the transformed space. This comparison requires a first step to compute the local similarities between two protected cylinders followed by the computation of a global similarity.

The local similarity between two cylinders is based on the application of an XOR operation as in (1), where c_A and c_B are the bit vectors generated from two cylinders A and B, respectively, L is the length of the bit vectors, and $\|\cdot\|_1$ is the 1-norm (that is the number of bits with value 1 in a bit vector). This is equivalent to calculate the Hamming Distance between c_A and c_B. The similarity result is in the range [0, 1], with 0 indicating no similarity and 1 indicating maximum similarity.

$$\gamma(c_A,c_B)=1-\frac{\left\|XOR(c_A,c_B)\right\|_1}{L}\,. \qquad (1)$$

In this work, the global similarity between two P-MCC identifiers is based on Local Greedy Similarity (LGS) [17]. In general terms, LGS combines the local similarities into an overall score as the average similarity of a predefined number of cylinders pairs with the largest similarity, but discarding pairs that contain an already selected cylinder.



(a)

(b)

(c)

(d)

Figure 2: Impostor and genuine score distributions for PUF-based identifiers extracted with (a) 128, (b) 256, (c) 512, and (d) 1024 bits.

III. Device Identifiers from SRAM PUFs

Physically Unclonable Functions from SRAMs (SRAM PUFs) are based on extracting the start-up values of the memory cells. When the memory is powered up and no data are written, each memory cell takes the value ‘0’ or ‘1’, and this information is lost when the memory is powered down. If the tendency of the memory cells to take ‘0’ or ‘1’ depends on the manufacturing process variability, those values are difficult to predict, to model mathematically and to clone physically. Standard SRAM cells are composed of two cross-coupled inverters. Ideally, both inverters should behave identically. However, the variability of the manufacturing process can make inverters behave differently and the cell has a trend towards a particular start-up value [13].

If for several power-ups a memory cell tends to have the same value, it is a stable cell. Otherwise, it is an unstable cell. Stable cells are the best memory cells to generate identifiers or feature vectors for devices [13]. Although some bit flipping is unavoidable, identifiers generated by the same memory are quite different to identifiers generated by other memories. An important criteria to create unpredictable identifiers is that the start-up values considered should contain the same number of 1’s and 0’s. Thus, it is crucial to create identifiers without bias.

The general procedure to extract feature vectors from SRAM PUFs requires the generation of masks that classify the cells as stable and unstable and that apply debiasing. In order to remove the possible bias in identifiers, the von Neumann debiasing technique can be applied as described in [21]. This stage is the registration or enrollment of the memory (similar to the fingerprint enrollment process). The SRAM is powered down and up several times, the start-up values are compared, the cells that take the same values are classified as stable cells and the others as unstable cells, and the non-biased stable cells are identified. The mask is stored to be employed in the generation process of the device identifier. The masks can be public because they do not reveal any sensitive information about the device.

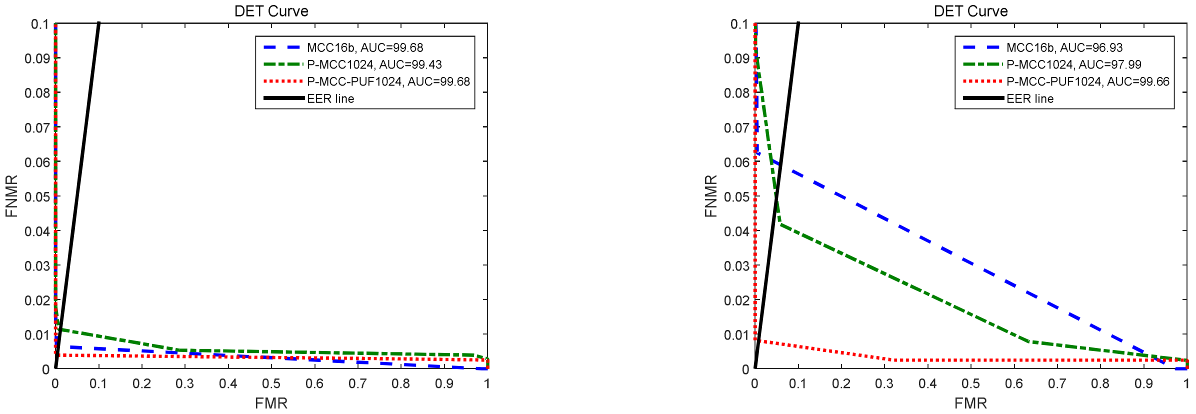
In order to generate the device identifier, the SRAM is powered up and its associated mask is applied to the start-up values obtained. It must be noted that the identifier (the sensitive information) is not stored. Hence, the generation process is repeated whenever the device identifier is required. Security is increased because the identifier is generated on the fly at the operation level. This is more secure than using a seed stored in the token as in [9].

Since PUF-based identifiers are binary, the Hamming Distance is employed to compare two device identifiers. Thus, the similarity score expressed by (1) is suitable for the comparison of PUF-based device identifiers. Ideally, identifiers from the same memory should have a similarity score of 1. However, some bit flipping is unavoidable among different measurements from the same memory. Also, if identifiers are debiased, PUF-based identifiers from different memories will have a similarity score of 0.5 [13]. In contrast to biometrics, where distinctiveness is commonly used instead of uniqueness [7], uniqueness is achieved with SRAM PUF-based identifiers.

IV. Fingerprint and Device Identifiers Fusion

Fusion of identifiers can be accomplished at different levels, including feature, score and decision levels [22]. In feature level fusion, the feature sets are combined before the comparison operation. The fusion at feature level is more restrictive since it requires compatible feature sets, in contrast to scores at score level or decisions at decision level. However, in our case, feature level fusion is possible for P-MCCs and PUF-based identifiers since both features are composed of binary values.

Feature vectors can be either concatenated or combined using the XOR operator. From a security point of view, XOR-based fusion is preferred since the random nature of the PUF-based identifier ensures that the biometric information is obfuscated and cannot be easily recovered. Thus, there is double template protection: from the protected MCCs (P-MCCs) and from the application of the XOR



(a) (b)

Figure 3: DET curves and AUC values for MCC16b, P-MCC1024 and P-MCC-PUF1024-based recognition in two databases: (a) FVC 2002 DB2a and (b) FVC 2002 DB3a.

TABLE II. COMPARISON OF BIOMETRIC RECOGNITION WITH RESPECT TO DUAL-FACTOR RECOGNITION IN THE STOLEN-TOKEN SCENARIO

	FVC 2002 DB2a		FVC 2002 DB3a	
Proposal	**EER**	**FMR_0**	**EER**	**FMR_0**
P-MCC1024	1.13	1.79	4.93	15.14
P-MCC64 [17]	1.76	5.46	7.78	20.71
P-MCC-PUF1024	1.23	2.29	4.97	17.79
2P-MCC64 [19]	1.8	5.5	7.8	20.7

EER and FMR_0 are expressed in %

operation with random data.

P-MCCs are composed of invariant and fixed-length cylinders. However, the number of cylinders is variable and depends on the number of minutiae detected. Another issue is that cylinders are not ordered. Therefore, the same PUF-based identifier should be fused with each cylinder of the P-MCC template.

The recognition process based on the fusion of P-MCC and PUF features is illustrated in Fig. 1. Once the fingerprint is registered by obtaining its P-MCC and the SRAM is registered by obtaining its cell mask, it is possible to perform the P-MCC-PUF enrollment and recognition processes. The P-MCC cylinders (c'_i, with i=1…t at enrollment, and c_j, with j=1…n at recognition) are obtained from the minutiae extracted from the fingerprint image. Each minutia has an associated cylinder, and the number of minutiae can be different for each sample captured. In the example in Fig. 1, t and n minutiae are extracted during the enrollment and recognition stages, respectively. Fig. 1 denotes the minutiae obtained at recognition as m_1,...,m_n, with the location and orientation values (x_j and y_j, and θ_j, respectively). The PUF-based identifier (p' at enrollment and p at recognition) generated by the SRAM is fused with each cylinder. The P-MCC-PUF identifier obtained at recognition is composed of the bit vectors $\{pc_1,…,pc_n\}$. The P-MCC-PUF template obtained during enrollment is composed of the bit vectors $\{p'c'_1,…,p'c'_t\}$.

In addition to produce a protected identifier (both device and fingerprint), matching is also performed in the protected domain. The similarity score is the result of the comparison of the extracted query P-MCC-PUF feature with the stored template P-MCC-PUF. Once the query feature vectors are fused to obtain $\{pc_1,…,pc_n\}$ as shown in Fig. 1, they are XOR-ed with the template feature vector $\{p'c'_1,…,p'c'_t\}$ to obtain a noisy version of XOR($p'c'_i$, pc_j). The noisy data are employed to perform the P-MCC matching: firstly, by computing the local similarities as in (1), and then by applying the Local Greedy Similarity algorithm to obtain an overall score as commented in Section 2.

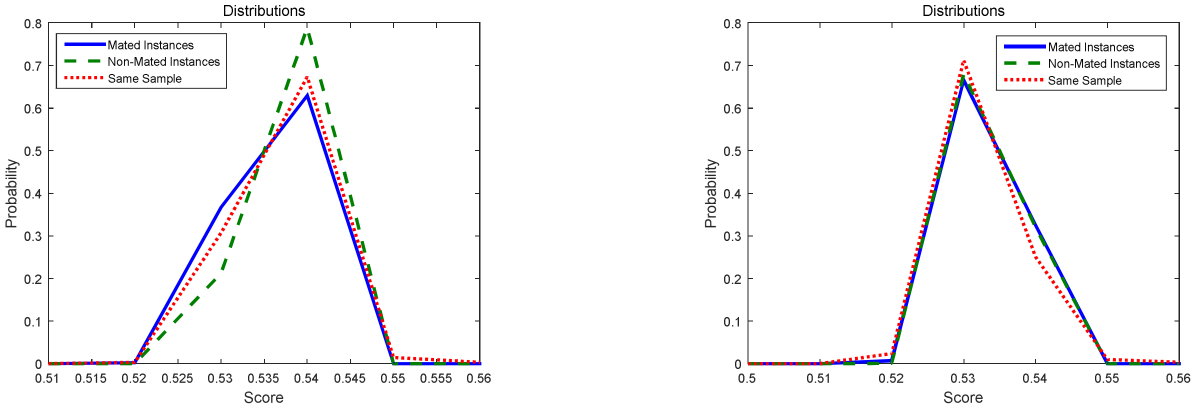
V. RECOGNITION AND SECURITY PERFORMANCE

In order to take into account a database with information from individuals and devices, we created a virtual database where real fingerprints (from public databases) are associated with real SRAM values (from measurements performed on commercial devices).

The biometric part was evaluated by considering the public databases from the Fingerprint Verification Competition (FVC). In order to compare the results with other proposals in the literature, the databases selected were FVC 2002 DB2a and DB3a. These databases contain 100 individuals and 8 fingerprint samples for each individual. Fingerprints are acquired with two types of sensors: optical for FVC 2002 DB2a, and capacitive for FVC 2002 DB3a.

The recognition results were obtained by evaluating EER, FMR_0 and AUC indicators, FMR and FNMR curves, DET curve, and score distributions. Matching experiments were conducted according to the FVC protocol. Genuine comparisons were made between every pair of samples corresponding to the same subject (in total, 2800 comparisons). Impostor comparisons were made between the first sample of a subject and the first sample of the rest of the subjects (in total, 4950 comparisons).

Minutiae were extracted by using the commercial software Innovatrics, which was one of the algorithms with better tradeoff between accuracy and speed in the most recent NIST Fingerprint Vendor Technology Evaluation [23]. This software provides ISO/IEC 19794-2 minutia templates to be processed by the Minutia Cylinder-Code SDK [24]. The parameters employed for the extraction and comparison of MCC features were proposed in [20]



(a) (b)

Figure 4: Score distributions for the evaluation of revocability and unlinkability in two databases: (a) FVC 2002 DB2a and (b) FVC 2002 DB3a.

according to the baseline MCC configuration tuned over the large BioSec-Baseline dataset.

Since different parameters for the KL projection were considered for P-MCCs, different lengths of P-MCC feature vectors were obtained: 32, 64, 128, 256, 512 and 1024 bits. In general, longer feature vectors are more accurate, as shown in Table I. However, template security is lower for P-MCC feature vectors with longer lengths. As the P-MCC representation becomes less compact, it becomes less secure because it is easier to recover the cylinder information and, thus, to reconstruct minutiae. Our approach is not influenced by this issue because additional protection is extended by the PUF-based identifier.

The evaluation of SRAM PUF-based identifiers was performed with a database created from the start-up values of SRAMs found in commercial Texas Instruments CC2541 Bluetooth Low Energy chips, measured under nominal operation conditions [21]. Ten CC2541 devices were analyzed and 40 measurements were carried out for each device. The measurements were obtained by a specific firmware that powered down and up the SRAM in each device. The first 20 measurements were employed to create the cell mask for each SRAM and the database was created with the other 20 measurements for each of the 10 devices.

After registering each device, as summarized in Section 3, non-biased 14,758 bits from stable cells were obtained from each measurement during recognition. The number of stable cells is different for each device, but this value was adjusted so that each measurement had the same number of bits. Instead of considering 10 14,758-bit PUF-based identifiers (corresponding to 10 devices), in this work we grouped the stable cells from all the devices to obtain the following sets of PUF-based identifiers: 4,610 with 32 bits, 2,300 with 64 bits, 1,150 with 128 bits, 570 with 256 bits, 280 with 512 bits, and 140 with 1,024 bits. This can be done since no correlation was found among the cells of the same SRAM. The database of PUF-based identifiers considers the first 100 identifiers of these sets, and the first 8 measurements (the measurements are slightly different between them due to bit flipping). Following the FVC protocol for computing the genuine and impostor distributions, the EER obtained was equal to 0% (except for the 32-bit PUF-based identifiers whose value was 0.12%). There is a total separation between the impostor and genuine score distributions (except for the 32-bit identifiers). For identifiers with larger lengths, the distributions are more ideal because their dispersions are smaller: the impostor distributions are more centered at 0.5 and the genuine distributions are closer to 1. In Fig. 2, score distributions are shown for 128-bit, 256-bit, 512-bit and 1024-bit PUF-based identifiers.

In our dual-factor approach, the combination of P-MCCs and PUFs, named as P-MCC-PUFs, was evaluated with several feature vector lengths, as shown in Table I. By considering this dual-factor approach, accuracy is increased with respect to P-MCCs. For P-MCC-PUF1024, performance is also improved with respect to the MCC16b unprotected approach (whose cylinders are composed of 1280 elements from 16 x 16 x 5 binary cells, as proposed in [20]). The DET curves are illustrated in Fig. 3 (a) and (b) for FVC 2002 DB2a and DB3a, respectively. The AUC values are also indicated.

In the literature, there are other dual-factor recognition proposals which apply permutations based on secret keys to MCCs [18] and P-MCCs [19]. Performance of these proposals is included in Table I. The work in [18] employs a 2048-element secret key and MCCs are created with 2048 elements (16 x 16 x 8 double-valued cells). In the comparison included in Table I, this approach is named as MCC16d2048. The template in [18] is not completely protected because the dual factor is applied to the cylinders of MCCs and some minutia information is required for the matching operation. The proposal in [19] creates a revocable feature vector from P-MCCs. Several lengths for P-MCCs and secret keys are considered. In [17], the best tradeoff between accuracy and security is obtained by using P-MCCs with a length of 64 and secret keys with 64 elements. In the comparison included in Table I, this approach is named as 2P-MCC64. Our proposed P-MCC-PUF1024 increases the performance.

Regarding irreversibility, the difficulty to recover the original template from the P-MCC-PUF template depends on the difficulty to obtain the PUF-based identifier. The PUF-based identifier information is not stored anywhere, but it is generated when the identifier is required, so that an attack to obtain the identifier has to be carried out when the device is in operation. In the case of a brute force attack to guess the identifier employed, the difficulty depends on the length of the identifier. As an example, for P-MCC-PUF1024, there are 2^{1024} possibilities. Finally, if the PUF-based identifier is discovered, the security depends on the irreversibility of the P-MCC feature vector [17].

In order to evaluate unlinkability, we applied the framework proposed recently in [25] by considering the distributions composed of (a) mated instances, that is, scores are computed from the comparisons of templates extracted from different samples of the same instance by using different keys (in our case, hardware identifiers), and (b) non-mated instances, that is, scores are computed from the comparisons of templates extracted from samples of different instances by using different keys (in our case, hardware identifiers). If both distributions coincide, the unlinkability of a scenario is proven. The revocability property is satisfied if different protected templates can be generated from the same sample by using different keys (in our case, hardware identifiers) [25]. The results from our proposal are viewed in Fig. 4. They show that the three distributions overlap extensively and, therefore, the revocability and unlinkability of our proposal are established because the resulting scores from protected templates generated by using different hardware identifiers from the same sample and different samples are comparable to the resulting scores from protected templates generated from different fingers.

Another attack is when the token is stolen. In other proposals in the literature, the stolen-token scenario refers to the secret key (or the seed to generate it) which is known by an attacker (because this information is recovered from its storage) [19]. In our proposal, it is not possible to recover the stored hardware identifier because it is not stored anywhere. The only way to recover the hardware identifier is to access the PUF when it is operating or to physically steal the token so that an impostor can use it. Basically, in this scenario, the evaluation results only correspond to the biometric recognition component. Although PUF-based identifiers generated by the same device are not exactly equal (because some fit flipping is unavoidable), these differences are low. The results are included in Table II.

VI. CONCLUSIONS

A dual-factor recognition scheme based on feature level fusion of P-MCCs and SRAM PUF-based identifiers has been proposed, resulting in a secure identifier named as P-MCC-PUFs. The best performance was obtained using P-MCC-PUF1024 which considers 1024-bit feature vectors. The approach provides revocability and unlinkability to P-MCCs and also stronger template protection because the biometric information stored is obfuscated by sequences of random bits provided by SRAM PUFs.

ACKNOWLEDGMENT

This work was supported by TEC2014-57971-R project from Ministerio de Economía y Competitividad of the Spanish Government (with support from the PO FEDER-FSE), 201750E010 (HW-SEEDS) project from CSIC, and US National Science Foundation (NSF) Award No. 1617466. The work of R. Arjona was supported by VI Plan Propio de Investigación through the University of Seville. The work of M. A. Prada-Delgado was supported by V Plan Propio de Investigación through the University of Seville.

REFERENCES

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to Biometrics: A Textbook. Springer Publishers, 2011.

[2] A. K. Jain, K. Nandakumar and A. Nagar, “Biometric Template Security”, EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, vol. 2008, no. 113. Hindawi Publishing Corporation, 2008.

[3] P. Campisi, Security and Privacy in Biometrics. Springer, 2013.

[4] E. J. Kindt, Privacy and Data Protection Issues of Biometric Applications. Springer, 2013.

[5] N. Ratha, J. Connell, and R. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems”, IBM Systems Journal, vol. 40, no. 3. IEEE, 2001, pp. 614–634.

[6] A. Nagar, K. Nandakumar and A. K. Jain, “A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates”, Pattern Recognition Letters, vol. 31, no. 8. Elsevier, 2010, pp. 733–741.

[7] A. K. Jain, K. Nandakumar, and A. Ross, “50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities”, Pattern Recognition Letters, vol. 79. Elsevier, 2016, pp. 80–105.

[8] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable Biometrics: A Review”, IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 54–65, 2015.

[9] A. T. B. Jin, D. N. C. Ling, and A. Goh, “Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number”, Pattern Recognition, vol. 37, no. 11. Elsevier, 2004, pp. 2245–2255.

[10] D. Samyde, S. Skorobogatov, R. Anderson, and J.-J. Quisquater, “On a New Way to Read Data from Memory”, Proc. First International IEEE Security in Storage Workshop (SISW), 2002, pp. 65–69.

[11] P. A. Grassi et al., Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B, 2017: https://doi.org/10.6028/NIST.SP.800-63b

[12] R. Maes, PUF-Based Entity Identification and Authentication. Physically Unclonable Functions, Chapter 5, pp. 117–141. Springer, 2013.

[13] I. Baturone, M. A. Prada-Delgado, and S. Eiroa, “Improved Generation of Identifiers, Secret Keys, and Random Numbers from SRAMs”, IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2653–2668, 2015.

[14] R. Arjona, and I. Baturone, “A Dual-Factor Access Control System based on Device and User Intrinsic Identifiers”, Proc. 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp. 4731–4736, 2016.

[15] R. Cappelli, M. Ferrara, and D. Maltoni, “Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 12, pp. 2128–2141, 2010.

[16] R. Cappelli, M. Ferrara, and D. Maltoni, “Fingerprint Indexing based on Minutia Cylinder Code”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 5, pp. 1051–1057, 2011.

[17] M. Ferrara, D. Maltoni, and R. Cappelli, “Noninvertible Minutia Cylinder-Code Representation”, IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1727–1737, 2012.

[18] L. Mirmohamadsadeghi, and A. Drygajlo, “A Template Privacy Protection Scheme for Fingerprint Minutiae Descriptors”, Proc. IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2013.

[19] M. Ferrara, D. Maltoni, and R. Cappelli, “A Two-Factor Protection Scheme for MCC Fingerprint Templates”, Proc. IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2014.

[20] R. Cappelli, M. Ferrara, D. Maltoni, and M. Tistarelli, “MCC: A Baseline Algorithm for Fingerprint Verification in FVC-onGoing”, Proc. 11th International Conference on Control Automation Robotics & Vision (ICARCV), 2010.

[21] M. A. Prada-Delgado, A. Vázquez-Reyes, and I. Baturone, “Physical Unclonable Keys for Smart Lock Systems using Bluetooth Low Energy”, Proc. 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp. 4808–4813, 2016.

[22] A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics. Springer, 2006.

[23] C. Watson, G. Fiumara, E. Tabassi, S. L. Cheng, P. Flanagan, and W. Salamon, “NIST Fingerprint Vendor Technology Evaluation”, 2014.

[24] Minutia Cylinder-Code SDK: http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=82&pathSubj=111%7C%7C8%7C%7C82&Req=&

[25] M. Gomez-Barrero, J. Galbally, A. Morales, and J. Fierrez, “Privacy-Preserving Comparison of Variable-Length Data With Application to Biometric Template Protection”, IEEE Access, vol. 5, pp. 8606–8619, 2017.