IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 16, 2020, accepted September 28, 2020, date of publication October 5, 2020, date of current version October 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3028703

A Post-Quantum Biometric Template Protection Scheme Based on Learning Parity With Noise (LPN) Commitments

ROSARIO ARJONA AND ILUMINADA BATURONE
Instituto de Microelectrónica de Sevilla (IMSE-CNM), Universidad de Sevilla-CSIC, 41092 Seville, Spain

Corresponding author: Rosario Arjona (arjona@imse-cnm.csic.es)

This work was supported in part by the Spanish Agencia Estatal de Investigación and Fondo Europeo de Desarrollo Regional (FEDER) under Project TEC2017-83557-R and Project RTC-2017-6595-7, and in part by the Consejería de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía, under Project AT17_5926_USE and Project US-1265146. The work of Rosario Arjona was supported by a Postdoctoral Fellowship from the Spanish National Cybersecurity Institute (INCIBE).

ABSTRACT Biometric recognition has the potential to authenticate individuals by an intrinsic link between the individual and their physical, physiological and/or behavioral characteristics. This leads a higher security level than the authentication solely based on knowledge or possession. One of the reasons why biometrics is not completely accepted is the lack of trust in the storage of biometric templates in external servers. Biometric data are sensitive data which should be protected as is contemplated in the data protection regulation of many countries. In this work, we propose the use of biometric Learning Parity With Noise (LPN) commitments as template protection scheme. To the best of our knowledge, this is the first proposal for biometric template protection based on the LPN problem (that is, the difficulty of decoding random linear codes), which offers post-quantum security. Biometric features are compared in the protected domain. Irreversibility, revocability, and unlinkability properties are satisfied as well as resistance to False Acceptance Rate (FAR), cross-matching, Stolen Token, and similarity-based attacks. A recognition accuracy with a 0% FAR is achieved, because user-specific secret keys are employed, and the False Rejection Ratio (FRR) can be adjusted depending on a threshold to preserve the accuracy of the unprotected scheme in the Stolen Token scenario. A good performance in terms of execution time, template storage and operation complexity is obtained for security levels at least of 80 bits. The proposed scheme is employed in a dual-factor authentication protocol from the literature to illustrate how it provides security using authentication and database (cloud) servers that can be malicious. The proposed LPN-based protected scheme can be applied to any biometric trait represented by binary features and any matching score based on Hamming or Jaccard distances. In particular, experimental results are included of a practical finger vein-based recognition system implemented in Matlab.

INDEX TERMS Biometric template protection, post-quantum security, LPN commitments, dual-factor authentication, authentication protocol, finger veins.

I. INTRODUCTION

Nowadays, our society has accepted extensively the use of biometric systems as a way of user authentication. The problem is that biometric data, which are stored as template at the registration phase or enrollment, are sensitive and, hence, should be protected, as contemplated in the data protection regulation of many countries [1]. Another problem is that biometric data that are revealed cannot be employed any more to avoid impersonation and privacy attacks. This also motivates to protect templates since people cannot provide many biometric traits.

The ISO/IEC 24745 standard on biometric information protection establishes the requirements of irreversibility, unlinkability, and revocability for biometric template protection schemes [1]. Irreversibility means that no information related to the biometric data can be recovered even if protected templates are compromised. Hence, biometric data remain private. Unlinkability means that no adversary can know which individual is the owner of the protected template,

The associate editor coordinating the review of this manuscript and approving it for publication was Marina Gavrilova.

thus allowing user identity privacy. In case a protected template is compromised, it should be revocable or renewable to obtain a new protected template from the same biometric sample.

Traditionally, biometric template protection schemes have been classified into 1) biometric cryptosystems and 2) feature transformations or cancelable biometrics [2].

Biometric cryptosystems bind a secret cryptographic key to the biometric data. Among them, fuzzy extractor, fuzzy vault and fuzzy commitment schemes were proposed, the latter being widely employed [3]–[5]. In Fuzzy Commitments [6], the commitments are Auxiliary or Helper Data generated as a combination of biometric data with an error correction codeword indexed by a cryptographic key. A cryptographic hash of the secret key (or of the error correction codeword) is stored together with the Helper Data. Biometric data should be represented as binary strings and the Hamming distance is used as the distance metric. Matching is performed by attempting to recover the cryptographic key from the Helper Data and the input biometric data, applying error correction decoding. Irreversibility is based on the computational difficulty to retrieve either the key or the biometric data from the stored Helper Data. Unlinkability and revocability are based on employing different keys.

The recognition accuracy of biometric cryptosystems is worse than the systems without protection, also known as the baseline systems. Hence, their security is very much lower than a cryptographic system because their False Acceptance Rate (FAR) is not sufficiently small. Considering a brute-force attack (also known as FAR attack), FAR should be smaller than 2^{-N} to achieve at least N-bit security. However, the FAR of biometric systems usually ranges from 10^{-5} (17 bits) to 10^{-7} (24 bits) [4]. Therefore, multibiometric fusion should be employed to improve security. Another limitation of biometric cryptosystems that forces the use of multibiometric fusion is the low entropy of biometric traits [4].

In the feature transformation approach, the biometric template is protected by a transformation function, which is applied at the registration and the verification phases. Therefore, biometric data are compared in the protected domain. Transformations can be non-invertible or invertible (salting). Transformation functions proposed in the literature are BioHashing [7], Alignment-Robust Hashing (ARH) [8], re-mapping and warping [9], and Bloom filters [10]. Unlinkability and revocability are based on the variation of the parameters of the transformation functions. Irreversibility depends on the difficulty to obtain the original biometric data from the transformed data.

Transformed templates often contain less information than the original templates. Hence, the usual consequence is a recognition performance degradation compared to the baseline version (without transformation) [7]–[11]. As in biometric cryptosystems, multibiometric fusion should be employed to improve security [12].

The accuracy obtained with the transformation can be improved due to the entropy added by a user-specific secret key as in salting schemes. In fact, the advantage of salting schemes, such as BioHashing [7], is that, theoretically, there is the possibility of achieving a 0% error rate due to the use of a dual recognition based on the biometric information and the user-specific secret key. However, this is risky and not advisable because an attacker can use the device with the user-specific secret key to improve the chances of successful authentication. This is known as the Stolen Token scenario [7]. Besides, as happens to biometric cryptosystems, a limitation of many salting schemes is that their security is very much lower than a cryptographic system because they are not robust to FAR attacks [13].

In the other side, most of cancelable biometric schemes apply similarity-preserving transformations, also called Locality Sensitive Hashing, in order to preserve in the protected domain the accuracy performance obtained in the unprotected domain [14], [15]. The problem is that this similarity or distance-preserving property (distances between unprotected samples are nearly the same as the distances between protected samples) can be exploited by similarity-based attacks that break these schemes. If an attacker can access the protected template, he/she can apply a search algorithm to generate first guesses randomly, transform them to the protected domain, compute the distances with the protected template, use the information to improve the probability of success with new guesses, and repeat the process until reaching a successful guess. The work in [15] confirms the vulnerability of BioHashing and Bloom-filter schemes to a Genetic Algorithm enabled similarity-based attack. The work in [14] introduces non-linearity in the transformation with the aid of a deep neural network, but this requires retraining whenever a new user is enrolled.

An alternative approach recently proposed to preserve the accuracy of baseline systems is homomorphic encryption [16]. When it is employed in a biometric application, the template and the input biometric data are encrypted by using a public key. The comparison is performed in the encrypted domain by means of an encrypted score computation operation. Thus, the resulting score after comparison is encrypted. In order to obtain the final score, a decryption operation by using a private key should be applied.

The practical implementation of Fully Homomorphic Encryption schemes is still a challenge because not all the operations needed to obtain an encrypted score are feasible due to their high cost in computational and memory requirements [2]. The practical proposals of biometric Homomorphic Encryption schemes only allow a limited subset of operations (additions or multiplications) in the encrypted domain. The most used approach is the additively homomorphic scheme and, specifically, the Paillier homomorphic encryption scheme [17]. In the schemes based on Paillier homomorphic encryption, the security of the operations employed are based on hard problems that cannot be solved nowadays in polynomial time, such as the Discrete Logarithm

Problem and the Integer Factorization Problem. However, these problems are not so complex for quantum computers, which is a relevant threat to consider, because protected schemes that nowadays are considered secure will not be so in the future.

Among the systems believed to resist the attacks of quantum computers, lattice-based cryptography has attracted most interest. Lattice cryptography uses high-dimensional geometric structures to hide information creating problems that are considered impossible to solve if the private key is unknown, even for quantum computers. Homomorphic encryption can be also constructed on the lattice problem fundamentals. In [18], two variants of Homomorphic Encryption are employed based on ideal-lattice and, particularly, ring-LWE (ring Learning With Errors) schemes, which are an example of ideal lattice cryptography.

The drawback of homomorphic encryption-based approaches is not only their high computational cost but also their memory requirements since the size of the protected template is around two order of magnitude greater than the unprotected template [18]. In addition, a simple attack algorithm has been reported to the authentication server that computes the final decrypted score. The biometric data can be revealed in at most 2N−T queries, where N is the bit-length of the biometric template and T is the authentication threshold [19].

In this work, we propose a post-quantum lightweight solution based on lattice cryptography. Specifically, Learning Parity with Noise (LPN) commitments are employed to protect biometric data. Our proposal of biometric LPN commitments uses a public generator matrix to convert biometric data to linear codewords that then are randomized with a user-specific secret. LPN commitments are not opened (the secrets are not revealed) but compared in the protected domain. The commitments using impostor secrets are detected and directly rejected without proceeding to calculate a biometric similarity score. Hence, False Acceptance Rate is 0%.

In comparison, conventional Fuzzy Commitments also uses a public generator matrix but to convert a secret to a linear codeword that is then combined with the biometric data. Biometric cryptosystems using Fuzzy Commitments accept an individual if the commitment can be opened (the secret can be reconstructed) because the biometric data provided at verification is enough similar to the data provided at enrollment. Hence, FAR is not 0% and FAR attacks can be successful.

LPN-based schemes have been applied to pseudorandom generators, symmetric key encryption, secret-key authentication protocols, public-key identification, and zero-knowledge proofs [20], [21]. However, to the best of our knowledge, this is the first proposal of LPN-based cryptography for biometric template protection. The main contributions of this paper are the following:

- The first biometric template protection scheme based on LPN commitments, whose hardness is a NP complete problem to classical and quantum computers.
- A low cost solution in terms of computational and memory requirements for protected template generation and storage (lower than approaches based on homomorphic encryption).
- High security against attacks to recover the biometric data, because comparison is done in the protected domain, using efficient cryptographic protocols.
- Resistance to similarity-based attacks because LPN commitments are random (computationally hiding) and, hence, do not preserve the distance values obtained between unprotected samples with respect to the distance values obtained between protected samples.
- A recognition accuracy with a FAR of 0% because user-specific secret keys are employed in the biometric LPN commitments. In case of the Stolen Token scenario, where an attacker uses a client device with a user-specific secret key, the accuracy of the unprotected approach is preserved.
- A security level comparable to a cryptographic system, even with unibiometric systems.
- Experimental results are included from a practical implementation in Matlab.
- The proposed solution was applied to a finger vein-based biometric system, compared to other systems, and evaluated in terms of irreversibility, revocability and unlinkability, as established in the standard ISO/IEC 24745.

This work is structured as follows. Section II describes our proposal of application of LPN commitments to biometric template protection. The operations required are defined, and a security analysis is carried out, considering a distributed scenario with cloud-based services where our scheme is included in an authentication protocol proposed in the literature. The implementation of biometric LPN commitments by using Matlab functions is explained in Section III. Parameters are selected to achieve several security levels and performance is evaluated in terms of execution time, template storage and operation complexity. In addition, a comparison to homomorphic encryption-based proposals is included. A practical realization is presented in Section IV by using finger veins. Accuracy, irreversibility, revocability, unlinkability, and resistance to attacks are proven and compared to other proposals of biometric template protection schemes applied to finger veins. Finally, Section V concludes the work.

II. PROPOSAL OF BIOMETRIC TEMPLATE PROTECTION BASED ON LPN COMMITMENTS

A. DEFINITION OF BIOMETRIC LPN COMMITMENTS

Commitment schemes are fundamental cryptographic primitives for cryptographic protocols. A commitment scheme allows a party to commit to a message by using a secret key to maintain it hidden to others. The security properties required by a commitment are the hiding and binding properties. Hiding means that one cannot learn anything about the committed message from the commitment. Binding means that the commitment created for a message is different to the commitment created for a different message.

An LPN commitment is based on encoding a message (in our proposal, biometric data) by using a random linear code with some noise added to the codeword. Formally, the LPN commitment to an m-bit message $B \in \{0,1\}^m$ is as follows [21]:

$$Com\,(B) = A \cdot (r||B) \oplus e \tag{1}$$

where $\cdot$ applies the bitwise AND and XOR operations; $||$ is the concatenation of two vectors; $\oplus$ is the bitwise XOR operation; r is a uniformly random vector $\in \{0,1\}^l$ included to add randomness; e is a low-weight uniformly random vector $\in \{0,1\}^n$ following a Bernoulli distribution with parameter τ $(0 < \tau < 1/2)$, i.e., every bit in e has a probability τ of being 1 and probability $(1-\tau)$ of being 0 ($e\,[i]$ has $\Pr\,[e\,[i] = 1] = \tau$ and $\Pr\,[e\,[i] = 0] = 1 - \tau$); and A is a uniformly random matrix $A = A'||A'' \in \{0,1\}^{n\times k}$ with $k = l + m$ and $n \geq k$.

The resulting $Com\,(B)$ is a vector $\in \{0,1\}^n$. The weight w of e is determined by the Hamming Weight (HW) of e (that is, $w = \sum_{i=1}^{n} e[i]$). When the weight of e is exactly $n\tau$, instead of expected, the LPN problem is named as exact LPN (xLPN for short) [21].

Using the same notation as above, the search version of the LPN problem with parameters $k \in \mathbb{N}$ (the length of a secret s), $\tau \in \mathbb{R}$ (the noise rate in the $e\,[i]$), and $n \in \mathbb{N}$ (the number of samples), asks to find a k-bit secret s from the n noisy linear equations resulting from $b = A \cdot s \oplus e$, where A is public. In our case, r and B (the biometric data) concatenated form the secret. The computationally hard problem underlying the security (i.e., the computational hiding property) of the LPN commitment scheme is the search LPN problem, which can be stated as the NP complete problem of decoding random linear codes [22]. Since the decoding problem in random linear codes is known to be robust for quantum as well as for classical computers, the search LPN problem is suitable for the construction of quantum-resistant commitments of secret biometric data B.

Setting $n = \theta(k) = \theta(l+m)$ large enough, the commitment scheme becomes computationally hiding and perfectly binding (with overwhelming probability over the choice of A). On the one hand, the binding property is satisfied by the large distance of the code generated by the random matrix A. On the other hand, the hiding property is satisfied by the LPN assumption which implies that $A \cdot s \oplus e$ is pseudorandom.

Let us define a linear code $\mathtt{C}$ as a k-dimensional subspace of $\{0,1\}^n$. In the decoding problem, the input is a noisy version of a codeword $c \in \mathtt{C}, c \oplus e$, with error vector $e \in \{0,1\}^n$ of Hamming weight w. In a typical setting, the weight w is upper bounded by the code distance d, which is the minimum Hamming distance between two codewords (full distance decoding). The target of decoding is to recover the codeword c (which is equivalent to find e).

Every instance of the LPN problem is an instance of a syndrome decoding problem where n is the length of the codeword, k is the linear code rank, A is the generator matrix, and w is the linear code distance (d) obtained from an error parameter τ as $w = n\tau$. Let n be the number of samples, we can write an LPN instance as the following matrix-vector tuple:

$$A \cdot s \in \{0,1\}^{n\times k} \times \{0,1\}^k \text{ satisfying } A \cdot s = b \oplus e \tag{2}$$

where $e = (e_1, \ldots, e_n)$ and the i^{th} row of A and b represent the i^{th} LPN sample.

Nowadays, the best algorithms for decoding random binary linear codes formulated as a syndrome decoding problem are based on Information Set Decoding (ISD) [23], a probabilistic decoding strategy that essentially tries to guess k correct positions in the noisy received word, b. The running time, T, of decoding algorithms is typically a function of the parameters n, k and w. If the Gilbert-Varshamow bound is used, w is a function of n and k, and therefore the running time can be expressed as a function of n and k only. For all Information Set Decoding algorithms, the highest running time is achieved when the code rate k/n is slightly below $1/2$. In that case, the ISD algorithms offer exponential running times of the form $T\,(n) = 2^{an}$ where α is a constant which can be used as a metric to compare the different algorithms.

B. COMPARISON OF BIOMETRIC LPN COMMITMENTS IN THE PROTECTED DOMAIN

In general, the algorithms of a commitment scheme are: key generation ($KGen$), which results a public commitment key; commitment generation (Com), which outputs a commitment for a message; and verification Ver, which verifies the commitment. In the LPN commitment scheme proposed in [21], $KGen$ generates the public key A; Com outputs the randomness r and the commitment from the public key A and a message m: $Com\,(m) = A \cdot (r||m) \oplus e$; and Ver takes the key A, the randomness r, the commitment $Com\,(m)$, and the message m, and outputs 1 (successful verification) if $Com(m) \oplus A \cdot (r||m)$ has weight w, and 0 (failed verification) otherwise.

In our proposal of biometric LPN commitments, the message is the biometric data, B_t at enrollment, and B_v at matching, which should be always protected. Therefore, in our proposal, $KGen$ generates the public matrix A, Com outputs r_t and $Com\,(B_t) = A \cdot (r_t||B_t) \oplus e_t$ at enrollment, and r_v and $Com\,(B_v) = A \cdot (r_v||B_v) \oplus e_v$ at matching, and Ver is modified to work only with protected data, that is, with commitments. Our verifier combines the biometric LPN commitments by a XOR operation as follows:

$$Com\,(B_t) \oplus Com\,(B_v) = A \cdot [(r_t||B_t) \oplus (r_v||B_v)] \oplus e_t \oplus e_v \tag{3}$$

This result can be considered as a system of linear equations with A as coefficient matrix and $A|[Com\,(B_t) \oplus Com\,(B_v)]$ as augmented matrix. If $Com\,(B_t)$ and $Com\,(B_v)$ are generated from the genuine prover, $e_t = e_v$. Hence, the XOR operation applied to genuine commitments results

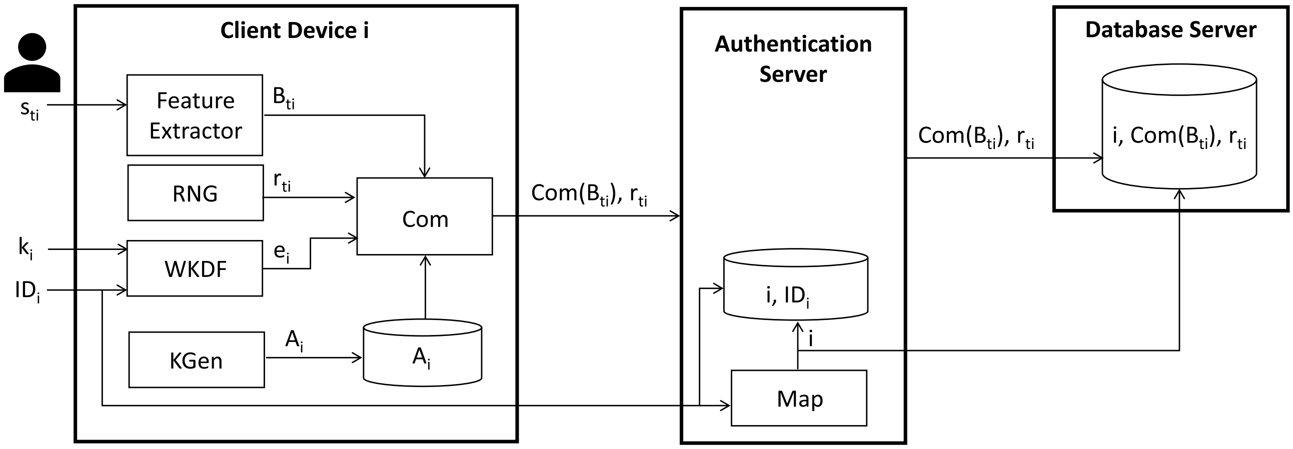

FIGURE 1. Enrollment phase of the authentication protocol based on biometric LPN commitments.

$[Com\,(B_t) \oplus Com\,(B_v)] = A \cdot [(r_t||B_t) \oplus (r_v||B_v)]$. Solving the system of linear equations (by means of Gaussian elimination, for instance), $[(r_t||B_t) \oplus (r_v||B_v)] = (r_t \oplus r_v||B_t \oplus B_v)$ is obtained.

Since r_t and r_v can be known by the verifier, it can be checked if $(r_t \oplus r_v)$ is correct. Then, the verifier employs $(B_t \oplus B_v)$ to compute the score measurement of the template and the input features. Typically, the score is based on the Fractional Hamming Distance (FHD), which can be computed as follows:

$$FHD\,(B_t, B_v) = \frac{HD(B_t, B_v)}{m} = \frac{\sum_{i=1}^{m} (B_t\,[i] \oplus B_v\,[i])}{m} \tag{4}$$

where HD is the Hamming Distance and m is the total number of bits in the biometric data.

In addition, the score can be based on the Jaccard Distance (JD), which can be computed as follows:

$$JD(B_t, B_v) = \frac{2 \cdot FHD(B_t, B_v)}{FHD\,(B_t, B_v) + FHW(B_t) + FHW(B_v)} \tag{5}$$

where FHW is the Fractional Hamming Weight (that is $FHW(B) = (\sum_{i=1}^{m} B\,[i])/m$).

In the case of Jaccard distance, the Hamming weights of the biometric data are needed, but this is not a problem since they do not reveal any sensitive information about biometric data. If the score calculated (based on $FHD\,(B_t, B_v)$ or $JD(B_t, B_v)$) is below an authentication threshold, the verification outputs 1 (success), and outputs 0 (failure), otherwise.

If $Com\,(B_t)$ and $Com\,(B_v)$ are generated from genuine and impostor provers, $e_t \neq e_v$. In this case, the system of linear equations with A as coefficient matrix and A$|[Com\,(B_t) \oplus Com\,(B_v)]$ as augmented matrix cannot be solved, because the rank of the augmented matrix is higher than the rank of the coefficient matrix. As stated by the Rouché–Frobenius theorem, the system has solution if and only if the ranks of the coefficient matrix and the augmented matrix are equal. Therefore, the impostor is directly rejected without proceeding to a score measurement.

C. USE OF BIOMETRIC LPN COMMITMENTS IN AN AUTHENTICATION PROTOCOL

In this work, we apply biometric LPN commitments in the typical scenario where cloud-based services and distributed architectures are employed, as proposed in [13]. The entities involved are: 1) N users ($i = 1, \ldots, N$), each one with a client device; 2) a client device which obtains user biometrics, identities and keys; 3) an authentication server in charge of the verification of biometric LPN commitments; and 4) a database server for (cloud) storage. In this protocol, there are two authentication factors: 1) the biometrics, and 2) the knowledge of a user key or the possession of a token with the user key stored in a secure memory or reconstructed with a Physical Unclonable Function (PUF) [24]. In the following, the knowledge of a user key is considered, as being more general [13].

The enrollment and verification phases are illustrated in Fig. 1 and Fig. 2. During the enrollment phase, the client device acquires the biometric samples s_{ti}, the user key k_i and the user identity ID_i. From the biometric samples s_{ti}, the client device extracts the biometric features B_{ti}. e_i is derived by using what we call a Weighted Key Derivation Function (WKDF) from the user key k_i and the user identity ID_i. This function starts from an all-zero vector of n elements. Since the resulting vector e_i must have a constant weight w, as commented in Subsection II.A, it means that $w = n\tau$ ones are inserted in the sequence of zeros. The positions in which the w ones are introduced follow a uniform distribution of random values in the range $[1, n]$ provided by a deterministic random generator. The deterministic random generator provides the same positions if the user introduces the same k_i and ID_i. If a random position is repeated, it is discarded, and a new position is generated until w ones are inserted. More details about this function are given in the following Section. A practical implementation can be seen in [25].

The random vector r_{ti} is generated by using a Random Number Generator (RNG). The public matrix A_i, which is obtained by the $KGen$ algorithm, can be stored locally in

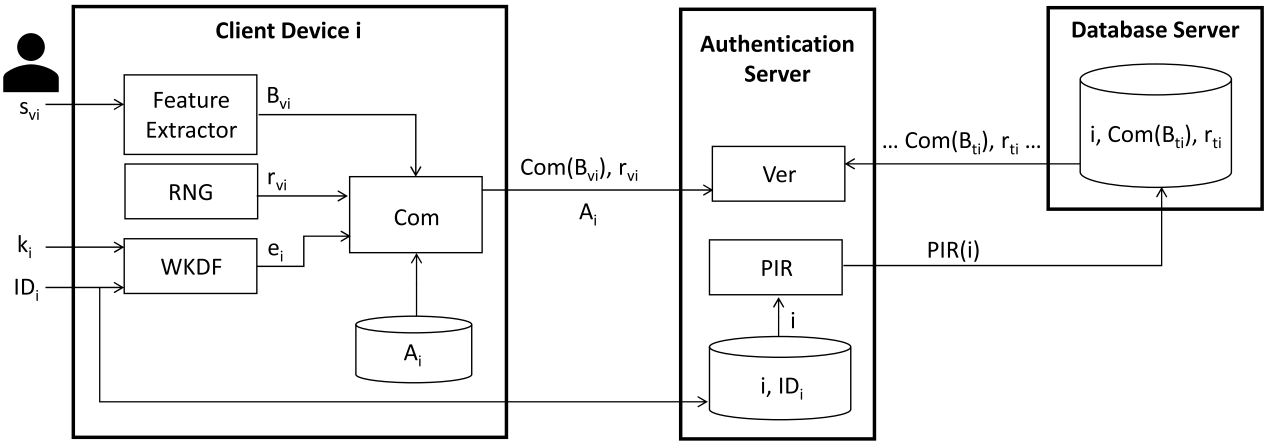

FIGURE 2. Verification phase of the authentication protocol based on biometric LPN commitments.

the client device. Then, the associated biometric LPN commitment $Com\,(B_{ti}) = A_i \cdot (r_{ti}||B_{ti}) \oplus e_i$ is created. The client device sends $(ID_i, Com\,(B_{ti})\,, r_{ti})$ to the authentication server. The authentication server maps ID_i to a unique index i, stores (i, ID_i) in its local database and sends $(i, Com\,(B_{ti})\,, r_{ti})$ to the database server for storage.

During the verification phase, the client device acquires the biometric samples s_{vi}, the user key k_i and the user identity ID_i. The input biometric features B_{vi} are extracted from the biometric samples s_{vi}, e_i is derived by using the WKDF from the input user key k_i and the user identity ID_i, and r_{vi} is generated by using the RNG. Then, the associated biometric LPN commitment $Com\,(B_{vi}) = A_i \cdot (r_{vi}||B_{vi}) \oplus e_i$ is created using the retrieved A_i. The client device sends $(ID_i, Com\,(B_{vi})\,, r_{vi})$ to the authentication server, and also A_i (although this is a public matrix that could be obtained in another way). The authentication server recovers i from its local database associated to the received ID_i and $(Com\,(B_{ti})\,, r_{ti})$ from the database server by using a private information retrieval (PIR) scheme. Then, the authentication server carries out the verification algorithm as described in Subsection II.B. A Private Information Retrieval (PIR) is a protocol that allows the authentication server to retrieve an element of the database server without the owner of the database being able to determine which element was queried. A secure PIR is employed together with the database anonymization, as proposed in [13], to satisfy the user identity privacy.

The communication channels among the protocol entities are assumed to be secure, which is a usual scenario. This means that an external adversary cannot intercept or modify a message which is communicated through the channels. Besides, the client device is assumed to be trusted, that is, we do not consider it stores user IDs, keys or biometric samples, or executes a malicious software. Finally, at the enrollment phases, all the entities are assumed to behave honestly.

However, an external adversary can use the client device to carry out impersonation attacks, which is the Stolen Token scenario commented in Introduction, and can attack also the information stored in the database server. Biometric LPN commitments are robust to these attacks as described in the following section.

In addition, since external adversaries cannot obtain more information than the internal ones, the protocol considers malicious authentication and database servers at the verification phase. If the authentication server is malicious, the target is to learn the user biometrics or keys. However, this is not possible because the authentication server does not have access to this information. If the database is malicious, the target is to obtain the link between the commitment and the user identity. However, since the database is anonymized and a PIR protocol is employed, the user identity privacy is satisfied.

D. SECURITY ANALYSIS OF THE BIOMETRIC LPN COMMITMENT AS TEMPLATE PROTECTION SCHEME

According to the ISO/IEC 24745:2011 standard on biometric information protection [1], the biometric template protection schemes should fully meet the security requirements of irreversibility, revocability (or renewability) and unlinkability.

Irreversibility is related to the difficulty to recover the original biometric features from the protected template. Irreversibility in an LPN commitment is based on the security of the LPN problem, which is the hardness of decoding random linear codes (a NP complete problem resistant to quantum algorithms) [20]. Since A and e are both random, the resulting LPN commitment is random. Hence, in terms of Shannon entropy, the entropy in bits of the biometric LPN commitments is practically 100%, independently of the biometric feature. The entropy provided by Fuzzy Commitments is lower, as depicted in Table 1, with data taken from [5].

Revocability (or renewability) is related to the ability to create a new and different protected template from the same biometric features of the same individual i by using different keys. This security requirement is associated to the binding property of an LPN commitment [21]. If $Com\,(B_{ti}) = A_i \cdot (r_{ti}||B_{ti}) \oplus e_i$ is created from the biometric features B_{ti} and another random $Com'\,(B_{ti}) = A'_i \cdot (r'_{ti}||B_{ti}) \oplus e'_i$ can be created

TABLE 1. Entropy in bits of fuzzy commitments [5] and LPN commitments.

Binarized Feature	Commitment	Entropy in bits
FingerVein	Fuzzy	21.80 %
Fingerprint	Fuzzy	22.38 %
Finger knuckle	Fuzzy	10.17 %
Finger shape	Fuzzy	22.40 %
Any	LPN	~100 %

from the same biometric features B_{ti}, $Com\,(B_{ti}) \neq Com'\,(B_{ti})$ with $Com\,(B_{ti})$ and $Com'\,(B_{ti})$ random (computationally hiding). This is also true if $A_i = A'_i$.

Unlinkability avoids possible cross-comparisons with other databases, thus ensuring the individual privacy. This property is related to the difficulty to determine if two protected templates created from different biometric samples of the same individual i and different keys belong to the same individual. Similarly to revocability, $Com\,(B_{ti}) \neq Com(B'_{ti})$ with $Com\,(B_{ti})$ and $Com(B'_{ti})$ random (computationally hiding) if $Com\,(B_{ti}) = A_i \cdot (r_{ti}||B_{ti}) \oplus e_i$ and $Com\left(B'_{ti}\right) = A'_i \cdot ({r'}_{ti}||{B'}_{ti}) \oplus e'_i$. This is also true if $A_i = A'_i$.

The decodability based cross-matching attack presented in [26] for Fuzzy Commitments is based on XOR-ing two Fuzzy Commitments created with the same linear Error Correction Code. The attack checks whether the result is decodable and, hence, detects that the biometric features are similar. In biometric LPN Commitments this attack is not possible since e_i and e'_i should be equal to decode the system of linear equations.

FAR attack occurs due to interclass correlation between biometric samples from different individuals that are very similar. It reduces considerably the security of Fuzzy Commitments and salting schemes, as commented in Introduction. For LPN biometric commitments, if the value of e is unknown, the $A|[Com\,(B_t) \oplus Com\,(B_v)]$-based equation system cannot be resolved although the biometric features B_t and B_v were similar. Therefore, FAR attacks are avoided by a biometric LPN commitment-based template protection scheme.

In addition to these security requirements, a template protection scheme should maintain the security under the named Stolen Token scenario. Originally, the Stolen Token scenario comes from the Biohashing technique [27], where a physical device or token stores the user key. In our context application, this scenario is possible since an attacker can access the client device and employ it for recognition during the verification phase. The commitment is created with $e_v = e_t$ and the verifier obtains a matching score from $[B_t \oplus B_v]$. However, B_t belongs to the genuine individual and B_v belongs to the impostor individual. Therefore, the recognition results are the same as in the unprotected system.

Concerning similarity-based attacks, if an attacker knows the protected template $Com\,(B_{ti}) = A_i \cdot (r_{ti}||B_{ti}) \oplus e_i$, generates first guesses randomnly, and transforms them to the protected domain, $Com\left(B'\right) = A_i \cdot (r'||B') \oplus e'$, the distance between $Com\,(B_{ti})$ and $Com\left(B'\right)$ does not reveal information about the distance between B_{ti} and B', because $Com\,(B_{ti})$ and $Com\left(B'\right)$ are random (computationally hiding). To carry out a similarity-based attack in the authentication protocol described above, the attacker should be successful to discover the association between a commitment and a user identity, that is, the attacker should break the database anonymization and, in addition, should employ the client device of that user, that is, should be in the Stolen Token scenario. Only then, the attacker is able to generate $Com\left(B'\right) = A_i \cdot (r'||B') \oplus e_i$, and from the distance between $Com\,(B_{ti})$ and $Com\left(B'\right)$ is able to extract information about the distance between B_{ti} and B'.

III. IMPLEMENTATION AND PERFORMANCE EVALUATION

A. SOFTWARE IMPLEMENTATION OF THE BIOMETRIC LPN COMMITMENT-BASED PROTECTION SCHEME

Our proposal has been developed in Matlab and thus the implementation of operations is based on Matlab functions. The first step to create a biometric LPN commitment is to generate the keys. The generation of the $n \cdot (l+m)$-bit matrix A requires a uniformly distributed random generator. This is possible by employing the Matlab function *rand* if the result is rounded. The generation of the n-bit vector e requires a weighted uniform random bit generator with Hamming weight equals to $n\tau$. The Matlab function *randperm* determines randomly the positions of the $n\tau$ elements of e with value 1. The rest of the elements are established to 0. A seed is employed by *randperm* which is associated to the user identity and key. In this way, the Matlab function *randperm* acts as a Weighted Key Derivation Function (WKDF).

The LPN commitment $Com\,(B) = A \cdot (r||B) \oplus e$ is composed of binary (AND) multiplications and binary (XOR) additions. The LPN commitment operation is translated to Matlab code as a 2-modulo operation applied to the addition of $A \cdot (r||B)$ and e. Previously, the biometric features B are extracted and concatenated to r. The generation of l-bit vectors r is performed with a uniformly distributed random generator based on the Matlab function *rand*.

At the verification phase, the authentication server has to solve the system of linear equations composed of A as coefficient matrix, $[Com\,(B_t) \oplus Com\,(B_v)]$ as matrix of independent terms and $A|[Com\,(B_t) \oplus Com\,(B_v)]$ as augmented matrix. In order to employ Gaussian elimination, superior matrix triangularization is applied to A. The *gflineq* Matlab function used for this operation finds a particular solution over prime Galois field of two elements. Two types of operations are required: 1) swap a current row with a row containing a major element, and 2) clear all non-zero elements in the column except the major element and set the major element to one by adding to one row a scalar multiple of another and applying a 2-module operation. Given the independent terms composed of $[Com\,(B_t) \oplus Com\,(B_v)]$, the authentication server checks firstly if the rank of the augmented matrix $A|[Com\,(B_t) \oplus Com\,(B_v)]$ is k (like the coefficient matrix A). If the ranks are different, the authentication server finishes the verification with a failure.

TABLE 2. Performance of biometric LPN commitment-based protection schemes.

Security Level (bits)	k ($r\|\|B$ Length)	$n \times k$ (A Matrix Size)	A and e Generation Time (ms)	A Superior Matrix Triangularization Time (s)	Commitment Time (ms)	Comparison Time (ms)
80	416	904 · 416	6.19	1.04	0.31	12.73
128	666	1,447 · 666	14.20	4.44	0.78	26.99
256	1,331	2,893 · 1,331	57.65	50.13	2.18	87.43
512	2,662	5,786 · 2,662	246.60	849.49	19.80	516.80

TABLE 3. Comparison of template storage and operation requirements.

Proposal	Protected Vector Length / Unprotected Vector Length	Decryption Required	Operations
Paillier Homomorphic Encryption [17]	x 128	Yes	Discrete logarithm with large exponents
Ideal-Lattice Homomorphic Encryption [18]	x 80	Yes	Polynomial multiplication based on Number-TheoreticTransform (NTT)
Ring-LWE Homomorphic Encryption [18]	x 120		
Biometric LPN commitments	x 2.17	No	Matrix operations based on AND and XOR

B. BIOMETRIC LPN COMMITMENT PARAMETERS AND PERFORMANCE

The LPN commitment parameters can be selected according to the latest results on Information Set Decoding (ISD) algorithms presented in [23]. In that work, the worst-case running time obtained for decoding random binary linear codes (considering full distance decoding) is $2^{0.0885 \cdot n}$, which means a security level of $0.0885 \cdot n$ bits. It is achieved for $k/n = 0.46$ with relative distance $\mathrm{w}/n = \mathrm{d}/n = 0.1237$, by using an improved proposal of the BJMM decoding algorithm of Becker *et al.* [28]. The value of n is selected to achieve the security level and then k and w are obtained. For different security levels, Table 2 shows execution times of the main operations in the LPN commitment-based template protection schemes. Execution times correspond to average of ten runs, executing the software implementation described above in an Intel Core 3.3 GHz i5-7400 CPU. The most timing consuming operation is the triangularization of the matrix A. However, the operations and the values required for the superior matrix triangularization can be pre-calculated at the enrollment phase and can be known by the authentication server to speed up the comparison of biometric LPN commitments at the verification phase.

Table 3 shows a comparison of our proposal to others proposals from the literature based on homomorphic encryption. The proposal in [18] offers a security level as high as ours (more than 80-bit security against exhaustive-search and birthday attacks). The results of our proposal consider the parameters selected in Table 2. The n values determine the protected vector length while the k values determine the unprotected vector length. The storage requirements of our proposal are the lowest. Regarding the cost of the operations at the verification phase, encryptions and decryptions are the most costly operations for homomorphic encryption approaches [29]. In contrast, our proposal does not require decryption and the operations involved are the simplest.

IV. PRACTICAL REALIZATION WITH FINGER VEINS

A. BIOMETRIC RECOGNITION BASED ON FINGER VEINS

Although our proposal can be applied to any biometric trait represented by binary features, this Section proposes an example of realization to protect finger vein features. The extractor of finger veins employed is based on the Wide Line Detector, which is a state-of-art finger vein extractor [30] initially proposed in [31].

The input to the Wide Line Detector is the brightness of a finger-vein image F and the output is a binary feature image V whose background pixels have the logic value '0' and the vein pixels have the logic value '1'. A circular neighborhood region N with radius r is defined for each center pixel (x_0, y_0) from F as follows:

$$N(x_0, y_0) = \left\{(x, y) \mid (x - x_0)^2 + (y - y_0)^2 \leq r^2\right\} \quad (6)$$

and the brightness similarity between two pixels is measured by:

$$b\,(x, y, x_0, y_0, u) = \left\{\begin{matrix} 0 & F\,(x, y) - F\,(x_0, y_0) > u \\ 1 & \mathit{otherwise} \end{matrix}\right\} \quad (7)$$

where u is a brightness contrast threshold.

Then, each pixel (x_0, y_0) in V is defined as follows:

$$V(x_0, y_0) = \begin{cases} 0, & \mathit{if}\ m\ (x_0, y_0) > g \\ 1, & \mathit{otherwise} \end{cases} \quad (8)$$

where m is the summation of the similarities within the circular neighborhood region:

$$m(x_0, y_0) = \sum\nolimits_{(x,y) \in N(x_0,y_0)} b\,(x, y, x_0, y_0, u) \quad (9)$$

and g is a geometric threshold defined as half the maximum value that m can take.

Since the feature vectors extracted are unbalanced (with a great difference for the number of 1's and 0's), we propose to measure the matching score with the Jaccard distance, which is the score already commented in Subsection II.B as Equation (5). With the knowledge of $FHW(B_t)$ and $FHW(B_v)$, the authentication server can compute this score from the biometric LPN commitments, and compare it with a threshold to output a success or a failure. We point out that our matching score is normalized, while that proposed in [32] is not.

B. ACCURACY ANALYSIS OF THE UNPROTECTED APPROACH

In order to obtain biometric recognition results, we applied the Wide Line Detector to extract features from the finger vein images from the Tsinghua University Finger Vein database [33], in particular from THU-FVFDT3 FV3_Test (which contains 4 samples of finger vein images for each 610 individuals). We use the Wide Line Detector implementation from [34] with the parameters $r = 5$, $u = 1$ and $g = 41$.

Matching experiments were performed following the FVC (Fingerprint Verification Competition) protocol [35]: Genuine comparisons were made between every pair of samples corresponding to the same individual (in total, $(4\cdot 3/2)\cdot 610 = 3{,}660$ comparisons). Impostor comparisons were made between the first sample of an individual and the first sample of the rest of the individuals (in total, $(610\cdot 609/2) = 185{,}745$ comparisons).

The finger vein image has $370 \cdot 576$ pixels, but the area centered on the middle of the image, which corresponds roughly to the middle phalanx, is usually described as the most stable and the most discriminant area for finger vein recognition, as indicated in [3]. Hence, we have evaluated feature vectors of finger veins formed by $32 \cdot 64$ bits (that is, 2,048 bits), and no displacements were applied to the feature vectors, as in [3]. The EER (Equal Error Rate) obtained (when the False Rejection Rate equals to the False Acceptance Rate) was 0.34 %.

C. RECOGNITION ACCURACY ANALYSIS OF THE PROTECTED APPROACH

The analysis is performed by considering the parameters selected in Table 2 for an 80-bit security with $k = 416$, which determines the number of divisions of the unprotected feature vector, and $n = 904$, which determines the protected feature vector length according to the number of divisions of the unprotected feature vector. For a 2,048-bit unprotected feature vector, eight 256-bit divisions are considered (with $l = 160, m = 256$ and $k = l + m = 416$). The time to compare two commitments is 101,84 ms using the above described Matlab implementation. Although this time is competitive, it can be reduced considerably if the code is optimized.

Table 4 shows a comparison of the recognition accuracy of our proposal and other template protection schemes based on finger veins. Our proposal is the only one that does not reduce the recognition accuracy in the protected domain. The False Acceptance Rate of the protected approach is 0% because an impostor, who does not know the user-specific secret key (the user key in the authentication protocol in Subsection II.C), is directly rejected. The False Rejection Rate (FRR) can be adjusted depending on the authentication threshold selected for the biometric data. If the authentication threshold of the EER of the unprotected domain is also used in the protected approach, the FRR = 0.34%, as shown in Table 4. In that case, in the Stolen Token scenario, the EER = 0.34% is preserved. In all the other proposals, the recognition accuracy when using the protected approach is always reduced.

TABLE 4. Comparison of recognition accuracy of the unprotected and protected approaches applied to finger veins wide line detector.

Proposal	Database	Unprotected Approach EER (%)	Protected Approach EER (%)
Re-mapping [8]	UTFVP	0.46	3.72
	PLUS LED	0.53	4.42
	PLUS Laser	1.38	5.52
Warping [8]	UTFVP	0.46	1.16
	PLUS LED	0.53	1.00
	PLUS Laser	1.38	2.02
Alignment-Robust Hashing [8]	UTFVP	0.46	3.90
	PLUS LED	0.53	5.27
	PLUS Laser	1.38	5.67
Bloom filters [10]	SDMULA-HMT11	1.5	2.1

Fuzzy Commitment [3]	UTFVP	0.56	FAR=0.01 or 0.03
			FRR=4.31 or 3.05

Fuzzy Commitment [5]	HKPUFI	0.36	0.76

Biometric LPN Commitment (This work)	THU-FVFDT3	0.34	FAR=0
			FRR=0.34

D. SECURITY ANALYSIS OF THE PROTECTED APPROACH

In order to evaluate unlinkability, we applied the framework proposed in [36] by considering the distributions of mated and non-mated instances. The Jaccard distances of mated instances are computed with the commitments of templates extracted from different samples of the same instance by using different e values. The Jaccard distances of non-mated instances are computed with the commitments of templates extracted from samples of different instances by using different e values. If both distributions coincide, the unlinkability of a scenario is proven. Fig. 3 proves the unlinkability of our proposal.

The revocability property is satisfied if different protected templates can be generated from the same sample by using different e values. The results are shown in Fig. 3. This distribution overlaps extensively with the two above, and, therefore, the revocability of our proposal is also proven.

Regarding unlinkability, our proposal outperforms the results obtained by using re-mapping, warping and Alignment-Robust Hashing proposals included in [8]. The rest of the proposals do not provide unlinkability results. Revocability results are not provided by the proposals considered.

The evaluation of the resistance to similarity-based attacks of the biometric LPN commitments was performed according to [14], which considers that protected templates are secure only if the mutual information between the normalized

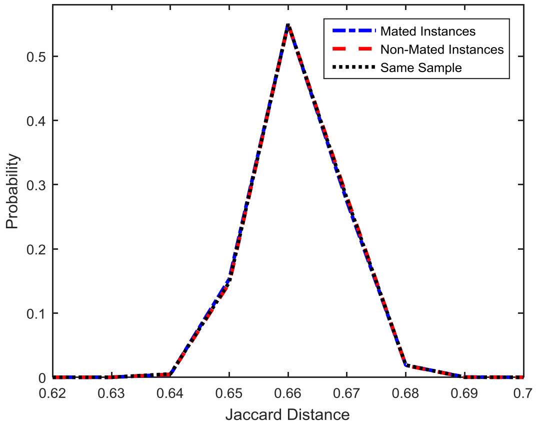

FIGURE 3. Score distributions for the evaluation of revocability and unlinkability.

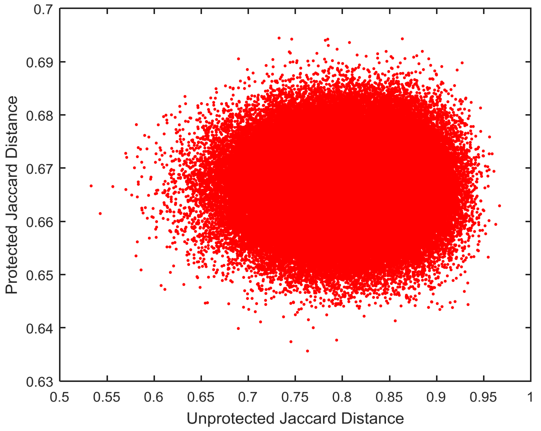

FIGURE 4. Correlation between the impostor unprotected distances and the impostor protected distances.

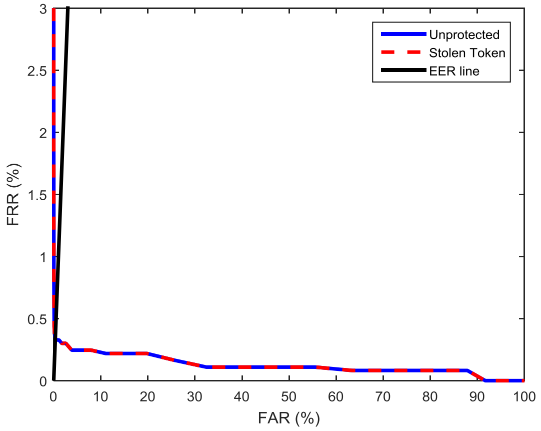

FIGURE 5. DET Curve for the unprotected and the Stolen Token approaches.

distances of the impostor data in the protected and unprotected domains is very small. In [14], mutual information is assumed to be upper bounded by the variance of the distribution of the impostor protected distances. The results obtained are shown in Fig. 4. It illustrates that the impostor protected distances (y-axis) do not change with respect to their impostor unprotected distances (x-axis), that is, their correlation is quite small. In fact, the variance of the impostor protected distances was $4.104 \cdot 10^{-5}$, much lower than the variance obtained for the solution proposed in [14] whose value is 0.31425. Therefore, it is very difficult for an attacker to infer the unprotected distances.

Regarding the Stolen Token scenario, let us consider a scenario where an attacker is able to generate the biometric LPN commitment at the verification phase using the same values for A and e. As expected, Fig. 5 illustrates through the DET curve that the recognition results from the unprotected and the Stolen Token approaches are the same. In [7], the recognition performance in the Stolen Token scenario is significantly worse because the recognition results are affected by the dimensionality reduction of the BioHashing transformation.

V. CONCLUSION

In this work, we have proposed the use of LPN commitments to construct a biometric template protection scheme. To the best of our knowledge, this is the first proposal of such schemes based on the LPN problem. Its use is described with a dual factor authentication in a distributed scenario where authentication and database servers can be malicious.

Irreversibility is based on the LPN problem, which is the difficulty of decoding random linear codes. Parameters are selected to obtain security of 80, 128, 256 and 512 bits. The analysis of execution times (of the order of milliseconds using a non-optimized code for the verification of biometric LPN commitments), template storage (with a length of the protected vector of, approximately, 2 times the length of the unprotected vector), and operation complexity (based on ANDs and XORs) shows that a practical realization has low cost. Hence, this scheme is feasible for hardware with constrained resources and verification at real time. Accuracy performance is achieved with a FAR of 0% and a FRR that can be adjusted depending on the authentication threshold selected for the biometric data and can be set to preserve the accuracy of the unprotected scheme in the Stolen Token scenario. Revocability, unlinkability, and resistance to FAR, cross-matching, and similarity-based attacks are also achieved. Experimental results are compared to other proposals from the literature based on homomorphic encryption, transformation, and biometric cryptosystems.

The application of biometric LPN commitments is possible for any biometric trait represented by binary features. In this work, the biometric LPN commitments are applied to finger veins extracted by the Wide Line Detector. For this realization, we have proposed a comparison of finger veins based on the Jaccard distance (more suitable for binary feature vectors with an unbalanced number of ones and zeros).

REFERENCES

[1] *Information Technology–Security Techniques–Biometric Information Protection*, document ISO/IEC 24745:2011, 2011.

[2] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[3] M. Favre, S. Picard, J. Bringer, and H. Chabanne, "Balancing is the key: Performing finger vein template protection using fuzzy commitment," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, Angers, France, Feb. 2015, pp. 1–8.

[4] T. Murakami, T. Ohki, and K. Takahashi, "Optimal sequential fusion for multibiometric cryptosystems," *Inf. Fusion*, vol. 32, pp. 93–108, Nov. 2016.

[5] J. Peng, Q. Li, A. A. Abd El-Lalif, and X. Niu, "Finger multibiometric cryptosystem based on score-level fusion," *Int. J. Comput. Appl. Technol.*, vol. 51, no. 2, pp. 120–130, Jan. 2015.

[6] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur. (CCS)*, 1999, pp. 1–21.

[7] V. Krivokuća and S. Marcel, "On the recognition performance of BioHash-protected finger vein templates," in *Handbook Vascular Biometrics* Cham, Switzerland: Springer, 2019, ch. 15, pp. 465–480.

[8] S. Kirchgasser, C. Kauba, Y.-L. Lai, J. Zhe, and A. Uhl, "Finger vein template protection based on alignment-robust feature description and index-of-maximum hashing," *IEEE T-BIOM*, vol. 2, no. 4, pp. 337–349, Oct. 2020.

[9] E. Piciucco, E. Maiorana, C. Kauba, A. Uhl, and P. Campisi, "Cancelable biometrics for finger vein recognition," in *Proc. 1st Int. Workshop Sens., Process. Learn. for Intell. Mach. (SPLINE)*, Jul. 2016, pp. 1–5.

[10] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on Bloom filters," *Inf. Fusion*, vol. 42, pp. 37–50, Jul. 2018.

[11] R. Dwivedi and S. Dey, "Securing fingerprint template using noninvertible ridge feature transformation" *Proc. SPIE*, vol. 27, no. 5, Oct. 2018, Art. no. 053031.

[12] R. Dwivedi and S. Dey, "Score-level fusion for cancelable multi-biometric verification," *Pattern Recognit. Lett.*, vol. 126, pp. 58–67, Sep. 2019.

[13] A. Abidin, E. Argones-Rúa, and B. Preneel, "An efficient entity authentication protocol with enhanced security and privacy properties," in *Proc. Int. Conf. Cryptol. Netw. Secur. (CANS)* (Lecture Notes in Computer Science), vol. 10052. Cham, Switzerland: Springer, Oct. 2016, pp. 1–16.

[14] Y. Chen, Y. Wo, R. Xie, C. Wu, and G. Han, "Deep secure quantization: On secure biometric hashing against similarity-based attacks," *Signal Process.*, vol. 154, pp. 314–323, Jan. 2019.

[15] X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," in *Proc. IEEE 10th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Tampa, FL, USA, Sep. 2019, pp. 23–26.

[16] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 42–52, Mar. 2013.

[17] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017.

[18] M. Yasuda, "Secure Hamming distance computation for biometrics using ideal-lattice and ring-LWE homomorphic encryption," *Inf. Secur. J., Global Perspective*, vol. 26, no. 2, pp. 85–103, Mar. 2017.

[19] A. Abidin and A. Mitrokotsa, "Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-LWE," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Atlanta, GA, USA, Dec. 2014, pp. 1–6.

[20] K. Pietrzak, "Cryptography from learning parity with noise," in *Proc. SOFSEM* (Lecture Notes in Computer Science), vol. 7147. Cham, Switzerland: Springer, 2012, pp. 99–114.

[21] A. Jain, S. Krenn, K. Pietrzak, and A. Tentes, "Commitments and efficient zero-knowledge proofs from learning parity with noise," in *Proc. Adv. Cryptol. (ASIACRYPT)* (Lecture Notes in Computer Science), vol. 7658. Cham, Switzerland: Springer, 2012, pp. 663–680.

[22] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Trans. Inf. Theory*, vol. 4, no. 3, pp. 384–386, May 1978.

[23] L. Both and A. May, "Decoding linear codes with high error rate and its impact for LPN security," in *Proc. Post-Quantum Cryptography (PQCrypto)* (Lecture Notes in Computer Science), vol. 10786. Cham, Switzerland: Springer, 2018, pp. 25–46.

[24] R. Maes, "PUF-based entity identification and authentication," in *Physically Unclonable Functions*. Berlin, Germany: Springer, 2013, pp. 117–141.

[25] M. A. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "PUF-derived IoT identities in a zero-knowledge protocol for blockchain," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100057.

[26] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 107–121, Mar. 2011.

[27] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Nov. 2004.

[28] A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1+1=0$ improves information set decoding," in *Proc. Adv. Cryptol. (EUROCRYPT)* (Lecture Notes in Computer Science), vol. 7237. Cham, Switzerland: Springer, pp. 520–536, 2012.

[29] C. Jost, H. Lam, A. Maximov, and B. J. M. Smeets. *Encryption Performance Improvements of the Paillier Cryptosystem*. Accessed: Sep. 15, 2020. [Online]. Available: https://eprint.iacr.org/2015/864

[30] L. Yang, G. Yang, X. Xi, K. Su, Q. Chen, and Y. Yin, "Finger vein code: From indexing to matching," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1210–1223, May 2019.

[31] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, "Finger-vein authentication based on wide line detector and pattern normalization," in *Proc. 20th Int. Conf. Pattern Recognit.*, Aug. 2010, pp. 1–4.

[32] N. Miura, A. Nagasaka, and T. Miyatake, "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Mach. Vis. Appl.*, vol. 15, no. 4, pp. 194–203, Oct. 2004.

[33] *Tsinghua University Finger Vein and Finger Dorsal Texture Database (THU-FVFDT)*. Accessed: Sep. 15, 2020. [Online]. Available: http://www.sigs.tsinghua.edu.cn/labs/vipl/thu-fvfdt.html

[34] B. Ton. *Wide Line Detector*. MATLAB Central. Accessed: Sep. 15, 2020. [Online]. Available: https://es.mathworks.com/matlabcentral/fileexchange/35754-wide-line-detector?s_tid=FX_rc2_behav

[35] *Fingerprint Verification Competition (FVC)*. Accessed: Sep. 15, 2020. [Online]. Available: https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx

[36] 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, Feb. 2017.

ROSARIO ARJONA received the degree in computer science engineering and the Ph.D. degree (Hons.) in microelectronics from the University of Seville, Seville, Spain, in 2009 and 2014, respectively. Since September 2009, she has been with the Instituto de Microelectrónica de Sevilla, University of Seville-CSIC. She is currently with the Department of Electronics and Electromagnetism, University of Seville, where she is an Assistant Professor. She has collaborated with 14 national and international research and industrial projects. She is the author of 24 scientific articles. She holds one patent. She is one of the developers of Xfuzzy environment. Her main research interests include crypto-biometric systems, multibiometric systems, physical unclonable functions (PUFs), image processing, pattern recognition, neuro-fuzzy systems, hardware security, design of digital systems on ASICs and FPGAs, and microcontrollers.

ILUMINADA BATURONE received the degree (Hons.) and Ph.D. degree (Hons.) in physics from the University of Seville, Seville, Spain, in 1991 and 1996, respectively. She has been with the Instituto de Microelectrónica de Sevilla, University of Seville-CSIC, since 1990. She is currently with the Department of Electronics and Electromagnetism, University of Seville, where she is a Full Professor. She has coauthored the books *Microelectronic Design of Fuzzy Logic-Based Systems* (CRC Press, 2000) and *Fuzzy Logic-Based Algorithms for Video De-Interlacing* (Springer, 2010). She has more than 150 scientific articles. She has participated in more than 40 Spanish and European research and industrial projects and leading 12 of them. She holds three patents. She is one of the developers of Xfuzzy environment. Her current research interests include hardware security, microelectronic design of crypto-biometric systems, hardware design for embedded control, and neuro-fuzzy systems.