Finite Field Elliptic Curve for Key Generation and Biometric Template Protection

Paul Knutson[†] Kiran Raja[§] Daniel Larsson[*] Raghavendra Ramachandra[§]
[†] Mobai AS, Norway
[§] Norwegian University of Science and Technology (NTNU), Norway
[*] University of South-Eastern Norway (USN), Norway

2021 IEEE International Workshop on Biometrics and Forensics (IWBF) | 978-1-7281-9556-8/20/$31.00 ©2021 IEEE | DOI: 10.1109/IWBF50991.2021.9465093

***Abstract*—The need to protect biometric data has been well advised according to various regulations and standards. The most popular Bloom Filter-based template protection schemes for iris recognition directly depend on the keys to avoid linkability challenges. This work presents a new approach for generating the keys directly from the iris biometric data using chaotic maps and elliptic curves over finite fields. Further, we present a new template protection scheme that can directly exploit the generated keys to provide better security using a Quarter-Rounded template encoding which employs the inter-relation of bits in the neighborhood of the iriscode. The proposed approach is validated on the publicly available IITD Iris database and the comparison to the state-of-art Bloom Filter template protection. The proposed approach achieves a comparable performance with the Bloom Filter template protection while eliminating key generation overhead. The proposed template creation approach achieves Genuine Match Rate (GMR) $= 99.15\%$ at $FMR = 0.01\%$ and $EER = 0.77\%$ on the IITD Iris database, with an unlinkability score of 0 and superior revocability.**

I. Introduction

Biometrics using face, iris, and fingerprint recognition have recently become standard for authentication in many applications. Different applications use the same biometric data and therefore require privacy-preserving data storage mechanism to avoid the negative impact if one of the databases is compromised [1], [2], [3], [4], [5]. Biometric data storage specifically need to respect three critical factors for privacy-preserving storage, aka, Biometric Template Protection (BTP): (1) irreversibility, (2) revokability and (3) unlinkability, in accordance to ISO/IEC standard for biometric data storage for template protection schemes [6].

The BTP schemes have been well investigated and have led to different strategies to achieve the same result. Popular BTP schemes such as Bloom filters [1] and variants like Cuckoo-filters [7], Morton-filters [8] or hash transformations has been proposed for iris recognition in recent years [2], [3], [4], [5]. Bloom filters provide a hash representation of the biometric data by merely dividing the entire iriscode into blocks of chosen length and width. To further address the linkability emerging from simple hashing of biometric data [9], the use of private key was proposed, where the key is used in simple linear relation to obtain a protected template (i.e., $B \oplus k$ where B is the biometric data of a chosen block and k is the key) [10].

Despite the good performance achieved by such Bloom filter based BTP schemes, the challenge of creating and choosing the keys remains. Typically such keys are chosen based on the applications, and when the biometric databases are compromised, the keys are changed to generate new templates. As it can be noted from the relationship of key and the biometric data, one can easily deduce the linkability challenge due to a linear relationship between the key and the biometric data. Given that the keys are typically a number directly related to the block size, the number of guesses needed is significantly lower, making the attacker succeed in a relatively low number of attempts. For instance, if the Bloom filter based scheme employs a block size of 5×20 bits, the largest key is usually limited to 20 if the hashed representation has a one-to-one relation to the protected template. Alternatively, a larger template size can be chosen to increase the size of the key, i.e., the key-space, and this leads to a larger size template leading to higher memory requirement for storage.

In this work, we address these two limitations of existing Bloom filter-based BTP schemes by providing a novel scheme that directly generates the keys from biometric data and provides a protected template. The key generation mechanism in our proposed approach relies on two key notions, namely chaotic maps and elliptic curves over finite fields. The generated keys are further used for creating the protected templates using a simple yet secure encoding. The proposed template protection is based on Quarter-Rounded encoding such that the key is iteratively used within a block to both reduce the linkability challenge and at the same time provide comparable performance to existing state-of-art Bloom filter BTP. We further refer to our proposed scheme as *Quarter-Round Biometric Templates*. The proposed approach is vetted for the robustness of biometric performance using publicly available IITD Iris database [11] consisting of 224 subjects and 2240 iris images. We complement the applicability of the proposed scheme further by analyzing the security aspects of the BTP schemes through a detailed unlinkability and revocability analysis.

The key contribution of this work can therefore be listed as:

- Presenting a new key generation mechanism from biometric data using chaotic maps and elliptic curves over finite fields, specifically for iris data protection.
- Presenting a novel way of template creation by exploiting inter-block and key relation that provides comparable performance to existing Bloom filter-based template protection scheme.

978-1-7281-9556-8/21/$31.00 ©2021 IEEE

- Providing an empirical evaluation of the proposed approach using a publicly available iris dataset together with a security analysis for both linkability and revocability.

In the rest of the paper, we present our proposed key generation mechanism in Section II. The key is further used for creating protected templates as presented in Section III. We further present a detailed empirical evaluation of the proposed approach in Section IV along with a brief overview of the database used. The security analysis is presented in Section V, and finally, we present some conclusions and potential future work to follow in Section VII.

II. Key Generation

As argued above, the key space is directly dependent on the size of the template. The real numbers used as the secret keys in existing BTP schemes are limited to the overall size of the template. To address such a challenge, we present a new scheme for key generation based on chaotic maps and elliptic curves over finite fields, which can directly employ biometric data using multiple strategies, for instance, selecting a user's biometric data from the enrollment set to generate the key or using a subset of enrolled subjects' biometric data to generate the key. We simply resort to the first strategy to validate the idea of key generation. We first provide a rationale of key generation in this section where the key generation is based on relaxed elliptic curve construction [12]. Our key generation mechanism involves estimating a random binary sequence B_N and then employ the same to derive the final key using the biometric data over an elliptic curve in a finite field. In the following section, we provide the idea behind chaotic maps and the relation to iriscodes for the final key generation.

A. Chaotic maps

Let A be the unit interval $[0,1] \subset \mathbb{R}$ and split A into two *disjoint* sets A_0 and A_1 of equal measure. In our situation we chose

$$A_0 := [0, 0.5] \qquad \text{and} \qquad A_1 := [0.5, 1].$$

Let Σ be a function $\Sigma : A \to A$.

Let $\sigma_0 = \sigma \in A$ and construct the set

$$S := \big\{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots\big\}, \quad \sigma_{i+1} = \Sigma(\sigma_i).$$

Through a suitable choice of Σ we can construct a sequence that is "random" in a weak sense. In this work, we employ the *logistic map*

$$\Sigma(x) = \lambda x(1-x), \qquad \lambda \in [1, 4]$$

to achieve the randomness. It is a classic fact that for $\lambda \approx 4$, this map is "chaotic" in the sense that the system is extremely sensitive to the choice of initial value σ_0. For $\lambda > 3.57$, an extremely slight change in initial value can (and typically will) change the sequence S completely. From the pair (A, Σ) above and the decomposition $A = A_0 \cup A_1$, we now construct a binary sequence

$$B_N := \big\{b_0, b_1, b_2, \dots, b_N\big\}, \qquad b_i \in \{0, 1\},$$

from

$$S_N := \big\{\sigma_0, \sigma_1, \sigma_2, \dots, \sigma_N\big\}$$

as follows:

$$b_i := \begin{cases} 0, & \text{if } \sigma_i \in A_0 \\ 1, & \text{if } \sigma_i \in A_1. \end{cases}$$

Therefore, B_N can be interpreted as the binary number $b_0 b_1 b_2 b_3 \cdots b_N$. For every $\epsilon_0, \epsilon_1 > 0$, the choice $\lambda + \epsilon_0$ and $\sigma_0 + \epsilon_1$ will dramatically change S and therefore B_N. The length N is obviously also variable.

Finally, let us remark that there are many other discrete chaotic systems, besides the logistic map, that can be used. However, for the sake of this note we restricted ourselves to the logistic map.

B. Elliptic curves over finite fields

We adopt a pedestrian view on elliptic curves with the following definition.

Definition 2.1: Let $q = p^n$, with $p \geq 5$ a prime. An *elliptic curve*, $\mathcal{E}$ over $\mathbb{F}_q$, is the plane curve in $\mathbb{F}_q^2$ defined by

$$y^2 = x^3 + bx + c, \quad \text{with } b, c \in \mathbb{F}_q, \tag{1}$$

and such that $-16(4b^3 + 27c^2) \neq 0$, together with a distinguished element $\mathtt{O} \notin \mathbb{F}_q^2$, the *point at infinity*. The set of solutions is denoted $\mathcal{E}(\mathbb{F}_q)$.

The set $\mathcal{E}(\mathbb{F}_q)$ is an abelian group under addition, which we denote $\underset{\mathcal{E}}{+}$. For the actual formulas defining the group structure we refer to [13].

C. Key generation using elliptic curves over finite fields and iriscodes

From now on we assume for simplicity that $n = 1$ so that $q = p$. Choose an element $\mathbf{z} \in \mathbb{F}_p$ and an elliptic curve $\mathcal{E}$ over $\mathbb{F}_p$. We will view $\mathbf{z}$ as the x-coordinate of a point on $\mathcal{E}$. However, this is not always possible. Indeed, for $\mathbf{z}$ to be the x-coordinate of a point on $\mathcal{E}$, we need to be able to solve the quadratic equation

$$y^2 = f(\mathbf{z}) = \mathbf{z}^3 + b\mathbf{z} + c. \tag{2}$$

in $\mathbb{F}_p$. This is not possible for all values of $\mathbf{z}$. If the equation fails to have a solution, we simply choose a new $\mathbf{z}$ until we get a $\mathbf{z}$ such that the Equation (2) is solvable.

Fix a point $\mathtt{p} \in \mathcal{E}(\mathbb{F}_p)$ and assume we have another point $\mathtt{q} \neq \mathtt{p}$ on $\mathcal{E}$ with $\mathbf{z}$ as x-coordinate. We now construct the following set of points on $\mathcal{E}$:

$$\boldsymbol{\zeta}_N := \Big\{\mathtt{q}, \zeta_1, \zeta_2, \zeta_3, \dots, \zeta_N\Big\} \subseteq \mathcal{E}(\mathbb{F}_p), \tag{3}$$

with ζ_j given by, for $b_j \in B_N$,

$$\zeta_j := j(1 + b_j)\mathtt{p} \underset{\mathcal{E}}{+} \mathtt{q}, \quad 0 \leq j \leq N, \quad \zeta_j := (x_j, y_j).$$

Viewing the coordinates $x_j, y_j \in \mathbb{F}_p$ as integers we write their binary expansion as $\bar{x}_j$ and $\bar{y}_j$.

We now define two functions L and R based on the binary iriscode. Let $b = b_0 b_1 \dots b_n$ be a binary iriscode. If n is odd

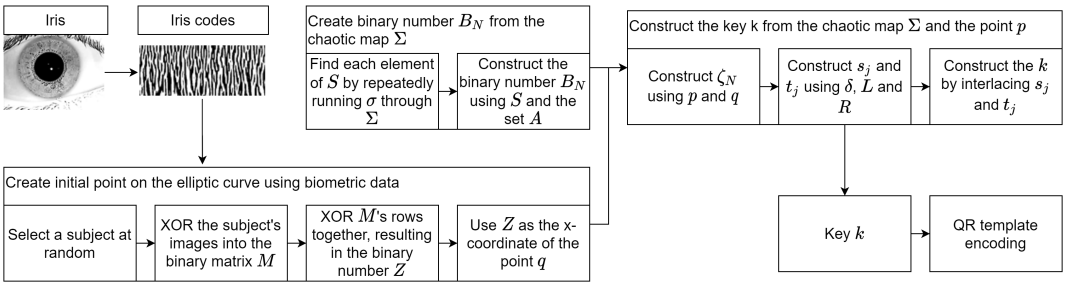

Fig. 1: Schematic of the proposed key generation and template protection scheme

we delete the middle digit, but we still denote the resulting number by b. Put

$$\mathsf{L}(b) := b_0 b_1 \cdots b_{\frac{n}{2}}, \quad \text{and} \quad \mathsf{R}(b) := b_{\frac{n}{2}+1} b_{\frac{n}{2}+2} \cdots b_n$$

We also introduce the function

$$\delta(j) = \begin{cases} 0, & \text{if } j \text{ even} \\ 1, & \text{if } j \text{ odd} \end{cases}$$

and, using this, the following two sequences $\{s_j\}$ and $\{t_j\}$ are created:

$$\begin{aligned} s_j &:= \delta(j)\mathsf{L}(\bar{x}_j) + \big(1-\delta(j)\big)\mathsf{R}(\bar{x}_j) \\ t_j &:= \big(1-\delta(j)\big)\mathsf{L}(\bar{y}_j) + \delta(j)\mathsf{R}(\bar{y}_j). \end{aligned} \tag{4}$$

Finally, the key is another binary number which is further used for template protection

$$\text{Key} := s_0 t_0 s_1 t_1 s_2 t_2 \cdots s_N t_N.$$

D. Usage of Key

As the key is directly proportional to iriscode, we assert that our proposed key generation mechanism can be used with any existing binary iriscode irrespective of feature extraction. In our specific case, we employ the 1D Log-Gabor iriscodes of the length 20×512 to validate the generation concept. However, we assert that other superior iriscode extraction schemes can provide stronger keys under the noisy setting of iris data.

III. Proposed Template Protection

We further present a new template protection scheme employing the generated key from the proposed key generation mechanism, as depicted in Figure 1. As noted from earlier works, iriscode also has a strong dependence on the inter-relation between the neighborhood pixels for providing higher verification performance [14]. Considering the linkability challenges and simultaneously exploiting the neighborhood relations of iriscodes in chosen blocks, we present a new Quarter-Round (QR) encoded template creation inspired by the Salsa20 stream cipher [15], [16]. We specifically employ such construction to create the templates based on the recently conducted security analysis where it was demonstrated as a secure encryption approach [16]. However, unlike the original construction where the problem of linkability does not exist in the data, the biometric databases have a strong unlinkability requirement. We, therefore, introduce the key for encoding the iriscode data to generate protected templates.

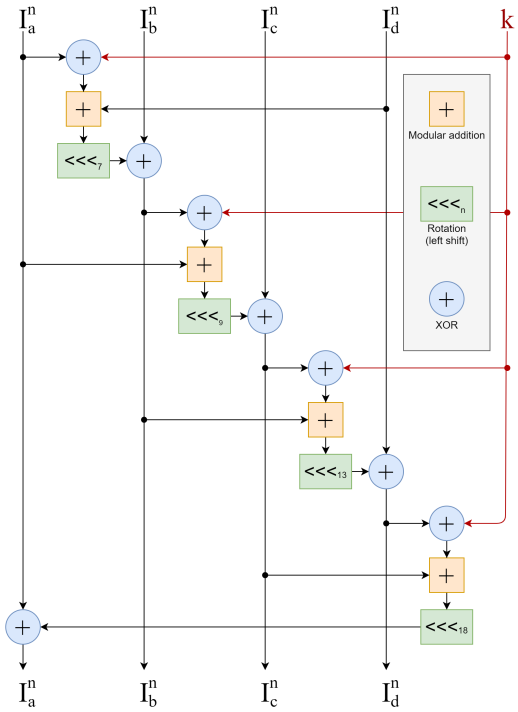

Fig. 2: Template creation using Quarter-Round (QR) encoding for each block of iriscode.

Further, to respect the backward compatibility of the proposed method to a Bloom filter-based template protection, we demonstrate the proposed approach with similar settings. Specifically, we divide the iriscode (I) into the number of blocks (n) of chosen length and width, i.e., $length = \{4, 8, 16, 32\}$ and $width = \{5, 10\}$. Each of the blocks is further reorganized into a 1-dimension array and further divided to result in 4 equal blocks $I_a^n, I_b^n, I_c^n, I_d^n$.

For each of the four blocks $I_a^n, I_b^n, I_c^n, I_d^n$, we use an ARX structure (Addition, Rotation and XOR) as presented below in

Equation 5:

$$\begin{aligned} I_b^n &= I_b^n \oplus (((I_a^n \oplus k) + I_d^n) \lll 7) \\ I_c^n &= I_c^n \oplus (((I_b^n \oplus k) + I_a^n) \lll 9) \\ I_d^n &= I_d^n \oplus (((I_c^n \oplus k) + I_b^n) \lll 13) \\ I_a^n &= I_a^n \oplus (((I_d^n \oplus k) + I_c^n) \lll 18) \end{aligned} \tag{5}$$

As it can be noted from Equation 5, the data from a chosen block of iriscode is not only encoding the data in a linear XOR format but also strictly enforces the usage of neighborhood relation before creating the protected templates. The summary of the QR template creation at a block level is presented in Figure 2.

Further, each of the resulting blocks from Equation 5 i.e., $I_a^n, I_b^n, I_c^n, I_d^n$ are combined to form a block of protected template. While different strategies can be employed, we simply concatenate them as one dimensional array for a given block of iriscode $I_p^n = [I_a^n || I_b^n || I_c^n || I_d^n]$. Such an operation is carried for all the blocks to obtain the final protected template.

IV. Experiments and Results

This section presents the experimental evaluation of our proposed approach on IITD Iris Database version 1.0 [11]. Although a wide variety of approaches can be used for comparing the proposed approach, we employ the Bloom filter template protection as our baseline due to similarity in the operational pipeline of the proposed approach to provide a fair comparison. Each of the iriscode comparisons, for both protected and unprotected template, are carried out using simple Hamming Distance measure [14], [17]. Further, the results are presented in Equal Error Rate (EER%) and an accompanying Genuine Match Rate (GMR=1-FNMR) at a False Match Rate of 0.01%.

A. IITD Iris Database version 1.0

The IITD Iris Database version 1.0 [11] provides the data captured from 224 subjects and 5 images per iris. We employ left iris images to provide a consistent comparison to earlier works [17], [18] which also employ only the left iris images totaling 1120 iris codes from 224 users with 5 iris codes per user. For each of the iris image, we extract the Log-Gabor encoding to obtain the iriscode [19] in the lines similar to earlier works on the Bloom-filter based template protection [1], [3], [18]. We further assert that our proposed key generation and template protection mechanism is independent of the feature extraction mechanism allowing the users to choose any binary representation. We follow the configurations recommended in earlier works on the same dataset, where the protected templates are created using iriscodes $\ell \in \{4, 8, 16, 32\}$ with 5 and 10 bits configuration [3], [18].

B. Results and Analysis

Table I provides the empirical results of the proposed template protection scheme based on the key generation mechanism. The results are further presented along with the results obtained from unprotected templates and protected templates using the Bloom Filter approach. As noted from Table I, the proposed approach provides comparable results against the Bloom filter-based template protection; however, without the overhead of creating the key manually.

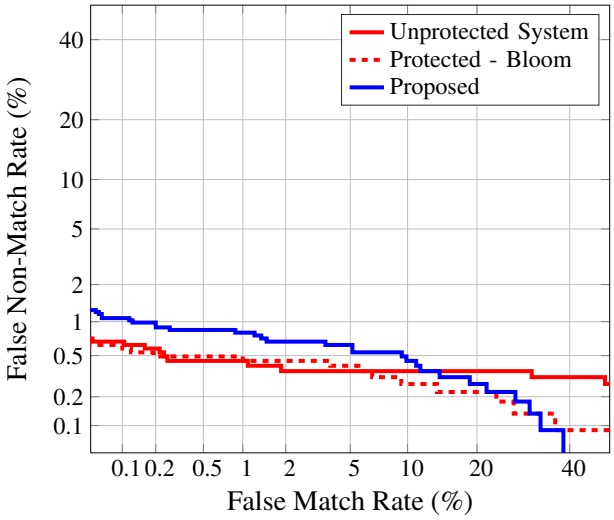

Fig. 3: Comparison of biometric performance using DET for IITD Iris Dataset with a configuration of $\ell = 4$ and 10 bits. While the proposed approach results in slightly higher EER as compared to Bloom filter based approach, it also results in lower FMR compensating the lower EER.

Further, the proposed approach using the key generation and template creation results in competitive performance (EER=0.75% and GMR=98.57%) with minimal loss in EER with respect to the Bloom filter-based approach (EER=0.38% and GMR=99.38%). While the EER is slightly lower than the Bloom filter approach, we note the gain in the FMR as depicted in the Detection Error Trade-off (DET) curves in Figure 3. However, we obtain an unlinkability score of 0, indicating the security of the proposed approach, as discussed in the next section. While we have used the configurations directly from the Bloom filter-based approach, we assert the scope for improvement of proposed template creation if other strategies for block creation can be employed. This factor needs further investigation and will be investigated in future works.

V. Security Analysis

To verify the strength of the proposed template protection using the key generation mechanism, we provide a security analysis using the Unlinkability Analysis Framework [20] and the revocability analysis framework. Specifically, unlinkability is achieved when the attacker is incapable of retrieving any information by comparing the protected templates generated from an identical iriscode by employing different keys generated. We also assume that if the templates from several databases or applications are compromised, the attacker can gain information on the template creation approach in an indirect manner. Thus the cancelability can be achieved by generating a new template simply by changing the keys generated

TABLE I: Results of proposed template protection scheme using proposed key generation mechanism compared to unprotected & Bloom filter based scheme on IITD Iris Dataset.

		5 Bits		10 Bits	
	Iriscode	EER	GMR @ 0.01% FMR	EER	GMR @ 0.01% FMR
Unprotected	Log-Gabor	0,36	99,11	0,36	99,11
Protected	Bloom - 4	**0,38**	**99,33**	**0,62**	**99,38**
	Bloom - 8	0,39	99,38	0,44	99,55
	Bloom - 16	0,40	99,15	0,26	98,84
	Bloom - 32	0,83	98,57	0,34	98,08
Proposed	Proposed - 4	**0.75**	**98.30**	**0.77**	**99.15**
	Proposed - 8	0.92	97.77	1.01	97.50
	Proposed - 16	1.65	96.38	1.53	95.31
	Proposed - 32	2.65	93.93	2.84	91.92

when the template in question is compromised, by selecting a different user from the enrollment set or by changing the p in Equation 2.1. In order to address the other two factors of the unlinkability [20] and the revocability, we simulate the verification experiments with different keys. Specifically, we generate (i) mated-imposter scores - the comparison score between two protected templates from the same iriscode computed by employing the same key generated from the proposed approach, and; (ii) non-mated-imposter scores - the comparison scores between two protected templates from two different iriscodes using two different keys generated from the proposed approach. Genuine scores correspond to comparison scores from the iriscode of the same person and the same key generated from the proposed approach, while imposter scores are the comparison scores are from the iriscodes of different persons with the same key.

A. Unlinkability Analysis

The framework measures the linkability $\mathrm{D}_{\leftrightarrow}^{sys}$ of the mated imposter distribution versus non mated imposter distribution to indicate how easily the scores can be used to link two subjects across two databases. A higher score indicates that the template protection results in a score distribution that can be easily linked across services. As seen from the Figure 4, a high degree of unlinkability is observed along with the unlinkability index given by $\mathrm{D}_{\leftrightarrow}^{sys}$ within the Figure 4 for IITD Iris dataset. A lower $\mathrm{D}_{\leftrightarrow}^{sys}$ indicates superior unlinkability. It can be clearly observed that the $\mathrm{D}_{\leftrightarrow}^{sys} = 0$ for all the configurations of the proposed approach with differing number of blocks and number of bits.

B. Revocability Analysis

To evaluate the revocability strength of the proposed key generation and template encoding approach, we analyse the score distribution of renewed protected templates through mated-imposter, genuine and non-mated-imposter score distribution. We conduct multiple rounds of verification using 24 different keys generated from the proposed approach to obtain all three distribution. Figure 5 presents the three distributions which indicate the revocability of the proposed approach.

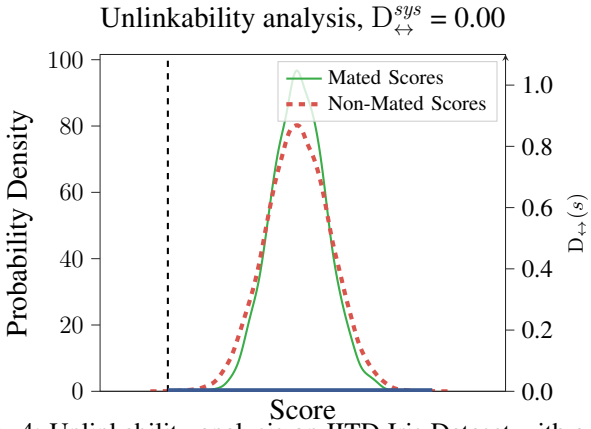

Fig. 4: Unlinkability analysis on IITD Iris Dataset with a configuration of $\ell = 4$ and 10 bits. *Note - Not all configurations lead to a $\mathrm{D}_{\leftrightarrow}^{sys} = 0$

Under a revocable situation, the score distribution shows no difference between the protected templates generated from the same individual iriscode or different individual iriscode by different keys generated from the proposed approach justifying the requirement of revocability. The revocability analysis resulted in a GMR of 99.15% and an EER of 0.77% with a clear overlap of mated-imposter and non-mated imposter score.

VI. Discussion on Future Work

The proposed approach has shown promising results for BTP. In this section, we list out a set of potential future works:

- Scope for key improvement: The proposed key generation in our work employs R and L in a very standard manner as given in Equation 4 [12]. The functions

$$s_j := \mathsf{R}(\bar{x}_j), \quad \text{and} \quad t_j := \mathsf{R}(\bar{y}_j).$$

  should further be investigated if the added layer of "mixing" left and right, adds to the randomness to make the key stronger and more random.
- Modality independence - In this work, to verify the concept, we have chosen iriscodes, but further investigations

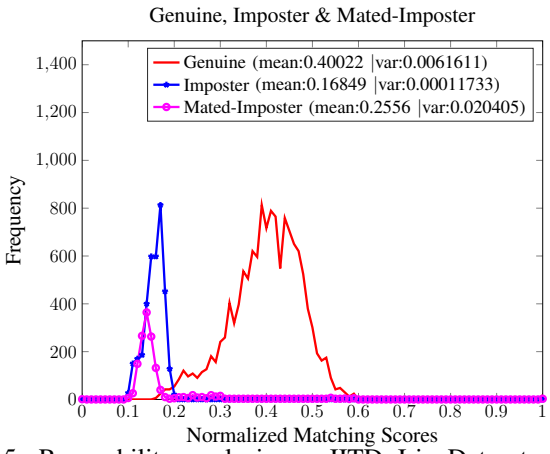

Fig. 5: Revocability analysis on IITD Iris Dataset with a configuration of $\ell = 4$ and 10 bits.

are needed to suitably modify the template protection scheme for other modalities such as face or fingerprint. We assert the proposed approach applicable to binary data such as iriscodes, and a similar argument can be extended to other modalities providing binary feature representations. However, the proposed approach is not studied for other biometric data, which may result in real-valued feature representation, and this needs to be conducted in future works.

- Key-generation and Key-binding: Given that the key can be generated directly from the biometric data, the approach can be used for key-generation and key-binding in biometrics for various modalities, which is not studied in this work.
- Selection of data for key generation: One of the subjects from the enrollment is randomly chosen to generate the key for all the subjects in the dataset. As an alternative strategy, it is also possible to employ pseudo-user biometric data to generate the keys or an averaged representation of enrollment data can be used. While the former will lead to enrollment independent and user-specific customization, the latter can help in devising optimized templates with known-apriori enrollment set. We leave the investigations of such strategies for future works in this direction.

VII. Conclusion

With the need for addressing key generation mechanism for biometric template protection, we presented a new key generation scheme based on chaotic maps and elliptic curves over finite fields. The proposed key generation approach is further complemented with the new template protection approach for iriscodes using the inter-relations between the iris bits in a Quarter-Round encoding scheme. The proposed approach was validated for the performance and compared against the popular Bloom filter based biometric template protection. While the proposed approach provides competitive performance compared to earlier method, this work eliminates the need for manual key generation procedure. The experiments conducted in IITD iris dataset has resulted in a Genuine Match Rate (GMR) $= 99.15\%$ at $FMR = 0.01\%$ and $EER = 0.77\%$ with ideal unlinkability and strong revocability. Modality independence of the proposed approach and extension to real valued feature vector will be further studied in the future works in this direction.

References

[1] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Biometrics (ICB), 2013 International Conference on*. IEEE, 2013, pp. 1–8.

[2] X. Dong, K. Wong, Z. Jin, and J.-l. Dugelay, "A cancellable face template scheme based on nonlinear multi-dimension spectral hashing," in *2019 7th International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 2019, pp. 1–6.

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

[4] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 393–407, 2017.

[5] D. Sadhya and B. Raman, "Generation of cancelable iris templates via randomized bit sampling," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2972–2986, 2019.

[6] ISO/IEC JTC1 SC27 Security Techniques, "ISO/IEC 24745:2011. information technology - security techniques - biometric information protection," International Organization for Standardization, 2011.

[7] K. Raja, R. Raghavendra, and C. Busch, "Towards reducing the error rates in template protection for iris recognition using custom cuckoo filters," in *2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, 2019, pp. 1–8.

[8] K. Raja, R. Raghavendra, and C. Busch, "Morton filters for iris template protection-an incremental and superior approach over bloom filters," in *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 2019, pp. 1–8.

[9] J. Hermans, B. Mennink, and R. Peeters, "When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system," in *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the*. IEEE, 2014, pp. 1–6.

[10] C. Rathgeb, F. Breitinger, H. Baier, and C. Busch, "Towards bloom filter-based indexing of iris biometric data," in *Biometrics (ICB), 2015 International Conference on*. IEEE, 2015, pp. 422–429.

[11] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.

[12] O. Reyad and Z. Kotulski, "Statistical analysis of the chaos-driven elliptic curve pseudo-random number generators," in *Intl. Conf. on Cryptography and Security Systems*. Springer, 2014, pp. 38–48.

[13] J. H. Silverman, *The arithmetic of elliptic curves*, ser. Graduate Texts in Mathematics. Springer-Verlag, New York, 1986, vol. 106. [Online]. Available: https://doi.org/10.1007/978-1-4757-1920-8

[14] J. Daugman, "Information theory and the iriscode," *IEEE transactions on information forensics and security*, vol. 11, no. 2, pp. 400–409, 2015.

[15] D. J. Bernstein *et al.*, "Chacha, a variant of salsa20," in *Workshop record of SASC*, vol. 8, 2008, pp. 3–5.

[16] G. Procter, "A security analysis of the composition of chacha20 and poly1305." *IACR Cryptol. ePrint Arch.*, vol. 2014, p. 613, 2014.

[17] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez, "Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris," in *International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 2015, pp. 1–6.

[18] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis and improvement of some biometric protected templates based on bloom filters," *Image and Vision Computing*, vol. 58, pp. 239–253, 2017.

[19] L. Masek *et al.*, "Recognition of human iris patterns for biometric identification," 2003.

[20] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420.