A. Brömme, C. Busch, N. Damer, A. Dantcheva, M. Gomez-Barrero, K. Raja,
C. Rathgeb, A. Sequeira, and A. Uhl (Eds.): BIOSIG 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021

Bloom Filter vs Homomorphic Encryption: Which approach protects the biometric data and satisfies ISO/IEC 24745?

Amina Bassit[1], Florian Hahn[2], Chris Zeinstra[3], Raymond Veldhuis[4], Andreas Peter[5]

Abstract: Bloom filter (BF) and homomorphic encryption (HE) are popular modern techniques used to design biometric template protection (BTP) schemes that aim to protect the sensitive biometric information during storage and the comparison process. However, in practice, many BTP schemes based on BF or HE violate at least one of the privacy requirements of the international standard ISO/IEC 24745: irreversibility, unlinkability and confidentiality. In this paper, we investigate the state-of-the-art BTP schemes based on these two approaches and assess their relative strengths and weaknesses with respect to the three requirements of ISO/IEC 24745. The results of our investigation showed that the choice between BF and HE depends on the setting where the BTP scheme will be deployed and the level of trustworthiness of the parties involved in processing the protected template. As a result, HE enhanced by verifiable computation techniques can satisfy the privacy requirements of ISO/IEC 24745 in a trustless setting.

Keywords: Bloom filter, homomorphic encryption, biometric template protection, ISO/IEC 24745.

1 Introduction

A biometric template is a compact representation of a physiological or a behavioral biometric characteristic such as face, iris, voice, etc. The biometric characteristic itself is not a secret as, in a human-to-human interaction, humans recognize each other from their actual characteristics. However, in a human-to-machine interaction, a biometric template becomes a numerical equivalent of the human characteristic understandable by a machine. Thus, a biometric template reflects the identity of an individual that allows him to be recognized by the system. Given the fact that systems are subject to various types of security threats, a biometric template must be well-protected.

The literature [JNN08, SP17] defines *biometric template protection* (BTP) schemes as the branch of biometrics that tackles the problem of persevering biometric templates while maintaining the recognition performance. There exist different approaches to design BTP schemes that try to satisfy the privacy requirements of the international standard ISO/IEC 24745 [Se11]: irreversibility, unlinkability and confidentiality. Among those approaches, *Bloom filter* (BF) based BTPs, process the template in the transformed domain, while *homomorphic encryption* (HE) based BTPs, process the template in the encrypted domain. Both approaches have common and exclusive interesting properties that deal with the BTP challenges and the tradeoffs.

[1] University of Twente, DMB Group and SCS Group, Enschede, The Netherlands, a.bassit@utwente.nl
[2] University of Twente, SCS Group, Enschede, The Netherlands, f.w.hahn@utwente.nl
[3] University of Twente, DMB Group, Enschede, The Netherlands, c.g.zeinstra@utwente.nl
[4] University of Twente, DMB Group, Enschede, The Netherlands, r.n.j.veldhuis@utwente.nl
[5] University of Twente, SCS Group, Enschede, The Netherlands, a.peter@utwente.nl

There are several surveys that investigate either Bloom filter [BM04, GA13] or homomorphic encryption [MSM17, Ac18, WNK20] and their applications in general. However, none of them focuses on examining these two approaches from a biometrics point of view.

In this paper, we investigate the differences between BF-based BTP schemes and HE-based BTP schemes. We analyze the state-of-the-art in both approaches by studying their core functionalities and how they are exploited in the design of BTP schemes. As both approaches seem promising, we compare their advantages and disadvantages with respect to different levels: fulfillment of the privacy requirements of ISO/IEC 24745, application usability, protected template flexibility, template size and runtime efficiency. We conclude by reflecting on which of BF or HE has the potential to satisfy the three requirements of ISO/IEC 24745 in a trustless setting.

2 Background

In this section, we discuss Bloom filter and homomorphic encryption as technologies we are about to investigate in the context of biometric recognition. We also provide the privacy requirements recommended by ISO/IEC 24745 [Se11].

2.1 Bloom Filter

A standard Bloom filter (BF) is an efficient data structure that is used to verify whether an element belongs to a set or not. Let us denote $S = \{x_1, \cdots, x_n\}$ where $x_i \in \{0,1\}^*$ [3] a set of n elements to-be-represented. A BF consists of an m bits array initially set to zero. The filter uses k independent hash functions $h_1, \cdots, h_k$, where $h_i : \{0,1\}^* \rightarrow \{0,1,\cdots,m-1\}$, that are assumed to be uniformly random. To insert an element $x \in S$ in the BF, the bit at index $h_i(x)$ is set to one for all $1 \leq i \leq k$. To verify whether an element y belongs to S, for all $i \in [1,k]$ the bit at index $h_i(y)$ must be activated [4]. Hence, if at least one index is not activated then with certainty y does not belong to S otherwise y probably belongs to S since the indexes could have been activated by some elements of S distinct from y. [KM08] provides an extensive study on the selection of optimal parameters (k,n and m) of a BF and [Hu09] provides a tool to estimate them and observe parameters variation.

BF is used in biometrics not only for being a space-efficient data structure but also for its invariant property with respect to element insertion since the BF of a set of elements S is identical to the BF of any permutation of S. This property is important for disposing of the inconvenient features alignment, and thus to allow an alignment-free technique. The BFs used in biometrics differ from the standard ones in the number of hash functions, they use a single hash function that is binary-to-integer, and the verification of element membership, instead they calculate the weighed Hamming distance between the BFs of two sets. BFs are close if the distance is small and thus their corresponding sets are likely to overlap.

[3] The set $\{0,1\}^*$ refers to the binary set of arbitrary length

[4] BF is activated at index j means it is set to one at index j.

2.2 Homomorphic Encryption

Homomorphic encryption (HE) allows computation over encrypted data without decryption; $E(x)*E(y)=E(x\circ y)$ where $E(x)$ (resp. $E(y)$) is an encryption of x (resp. y), $*$ operation in the encrypted domain and $\circ$ operation in the plaintext domain. The operations $*$ and $\circ$ can be either an addition, a multiplication or both; depending on HE scheme type. There are three types of HE schemes: partially HE (PHE), somewhat HE (SWHE) and fully HE (FHE). PHE schemes (e.g. Paillier [Pa99], ElGamal [El85]) support only one operation unlimited number of times with a plaintext space either binary or integer. SWHE schemes (e.g. BGN [BGN05]) support a limited [5] number of operations, usually a limited number of multiplications and an arbitrary number of additions, and operate also on a binary or integer plaintext space. FHE schemes (e.g. BFV [Br12,FV12], BGV [BGV14], CKKS [Ch17]) support an unlimited number of both operations and are fundamentally based on Gentry's construction [Ge09] that enables refreshing ciphertexts to prevent them from reaching the allowed limit in each operation, and thus they remain decryptable. Unlike the classical PHEs and SWHEs, that have a limited choice of the plaintext, the state-of-the-art FHEs support binary (e.g. BFV), integers (e.g. BGV), real numbers and complex numbers (e.g. CKKS). Moreover, they offer a new style of operations, called *single-instruction multiple-data* (SIMD), that significantly contributes to speeding up FHEs. For instance, they allow encryption of a vector of plaintexts, packing of a vector of ciphertexts into a single ciphertext, permutations within the same ciphertext and automorphisms of a ciphertext. Although, the practical improvements on accelerating FHE schemes are considerable, it is still an active area of research.

HE offers flexibility in processing encrypted data, however it comes with a significant cost that impacts the storage as well as the runtime. The HE ciphertexts have a large size which implies that the biometric encrypted templates have a large size as well. The biometric recognition performed in the plaintext domain is significantly faster than the biometric recognition performed in the encrypted domain since they require several multiplications which are resource demanding operations under HE. The impact that HE has on the memory space and the runtime is undesirable in biometric recognition systems that try to minimize both of them to meet the usability requirement. However, this optimization should not be at the expense of their security.

2.3 Privacy Requirements of ISO/IEC 24745

The international standard ISO/IEC 24745 [Se11] establishes requirements and guidelines on how the biometric information should be protected throughout its entire lifecycle: storage, transfer and processing. The standard highlights the importance of binding a biometric reference with the corresponding subject identity as well as the privacy protection of subjects' biometric information during the processing. In this work, we focus on the ISO/IEC 24745 privacy requirements that are: *Irreversibility:* for a fixed pre-defined usage (such as recognition), the raw biometric data must be transformed into an irreversible representation that precisely fits the task of the pre-defined usage. *Unlinkability:* there must be no relationship between the stored biometric templates neither across applications nor databases. *Confidentiality:* the biometric template must be preserved and not exposed to unauthorized parties trying to gain unauthorized accesses.

[5] SWHE schemes produce noisy ciphertexts where the noise grows along with each homomorphic operation until it reaches its limit. Subsequently, the resulted ciphertext can no longer be decryptable.

3 Bloom Filter based BTP Schemes

Cancelable biometric systems [TKL08, SS18, Ku20], that apply non-invertible transformations to preserve the biometric template, suffer from significant degradation in their recognition performance due to the use of non-invertible transformations (such as cryptographic hash functions) that hurt the biometric accuracy. BF-based BTP schemes overcome this drawback by taking advantage from the invariant property of BFs to conceal a distorted version of the raw biometric sample in a BF-based template and thus achieve diffusion of the statistical properties of biometric features while maintaining their distinctiveness.

First Category BF-based BTPs: [RBB13] introduced the first BF-based BTP scheme (which we call *first category BF-based BTP scheme* and illustrate in Figure 1), as a form of cancelable biometric system that preserves the recognition performance by circumventing the feature alignment problem during the comparison process. This is achieved since BFs are invariant with respect to the insertion of elements as the BF of a set of elements S is identical to the BF of any permutation of S. This first category of BF-based BTPs was tested on irises [RBB13, Ra14, RB14, Ra15], faces [Go14] and fingerprints [Li15] to demonstrate the diversity of this approach with respect to the biometric modalities as long as they can be expressed as binary feature vectors.

The early security assessment of the first category of BF-based BTPs was studied by [HMP14] who confirmed the irreversibility of their templates but questioned their unlinkability. In particular, the authors showed that for $T_1 = \{\mathrm{BF}^{M}_{B_i}(K_1)\}_1^k$ and $T_2 = \{\mathrm{BF}^{M}_{B_i}(K_2)\}_1^k$ two BF-based templates generated from the same iriscode M using different keys $K_1 \neq K_2$ are determined to conceal the same iriscode with a probability of 96% assuming that the biometric samples are uniformly random. Later, [BMR17] extended the unlinkability analysis and considered the non-uniformity of biometric samples inherited from the acquisition noise to determine whether $\tilde{T}_1 = \{\mathrm{BF}^{M_1}_{B_i}(K_1^i)\}_1^k$ and $\tilde{T}_2 = \{\mathrm{BF}^{M_2}_{B_i}(K_2^i)\}_1^k$, with different iriscodes and different keys, are from the same iris. Their attack is a brute force over the possible keys K per block that saves the key with the lowest dissimilarity score. In other terms, for each block B_i it searches for

$$K = \underset{\hat{K}\in[0,2^n-1]}{\operatorname{argmin}} \; DS\big(\mathrm{BF}^{M_1}_{B_i}(K_1^i), \mathrm{BF}^{M_2}_{B_i}(K_2^i \oplus \hat{K})\big)$$

where $\mathrm{BF}^{M_2}_{B_i}(K_2^i \oplus \hat{K})$ is computed only from $\mathrm{BF}^{M_2}_{B_i}(K_2^i)$ and $\hat{K}$ by activating the BF at index $j \oplus \hat{K}$ if and only if BF at index j is activated. Hence, the distribution of the dissimilarity scores of the original BF-based templates $DS\big(\mathrm{BF}^{M_1}_{B_i}(K_1^i), \mathrm{BF}^{M_2}_{B_i}(K_2^i)\big)$ and the distribution of the attacked templates $DS\big(\mathrm{BF}^{M_1}_{B_i}(K_1^i), \mathrm{BF}^{M_2}_{B_i}(K_2^i \oplus K)\big)$, where the key K has been chosen from the lowest dissimilarity score, overlap and have a slightly similar error rate. Then, [BMR17] analyzed the irreversibility of a 1st category BF-based template without key $K=0$ and proposed two attacks that try to reconstruct an approximation of the unprotected template only by extracting some partial information from the protected template. The first attack consists of reconstructing a block by replacing all its columns with the same column computed from averaging the activated indexes of the BF of the protected template. The second attack requires a training set of the form (M_{ID}, T_{ID}) where T_{ID} is the protected template concealing the iriscode M_{ID}. The attack consists of reconstructing the iriscode of a protected template from the test set by replacing each block with the block corresponding to the nearest BF belonging to the protected templates of the training set. This attack assumes that $K = 0$ which implies that it does not take into account neither the variability of the key among different subjects nor the effect of the key for the same subject. As reported by the authors, the experimental results of both attacks are ineffective.

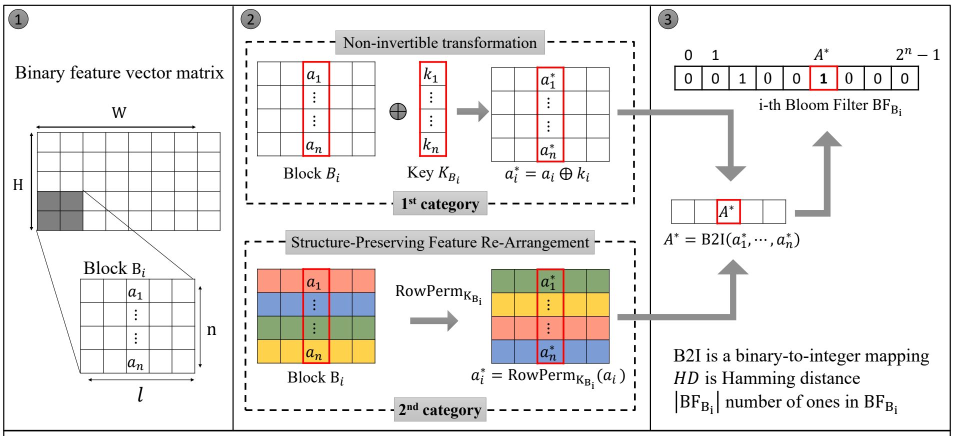
Second Category BF-based BTPs: In order to address the linkability vulnerability of 1st category BF-based BTPs, [Go16b] proposed a technique called *structure-preserving feature re-arrangement* to replace the XOR with the key before computing the BF, and thus the *second category BF-based BTP scheme* that we illustrate in Figure 1. This technique permutes the rows of a feature block according to a keyed random permutation to diffuse the statistical properties of a biometric feature vector and at the same time to preserve the biometric performance. Later, [Ma17] uses the same technique with a minor addition, that is, after a row-wise permutation there is a circular shift within each column. However, this circular shifting does not contribute to the dissipation of the biometric information but rather might lead to some accuracy loss since different columns after shifting might result in the same column.

[Go17a] studied the unlinkability of any BTP scheme from an information theory perspective and proposed a linkability evaluation procedure (Section 5 in [Go17a]). This procedure helps to assess whether two protected templates of a given BTP scheme are concealing the same or different biometric instances. This is determined only by observing the score resulted from the BTP's comparison measure and comparing it with the prior mated score distribution and the prior unmated score distribution. The same work defined three degrees of unlinkability that are: *fully unlinkable*, *semi unlinkable*, and *fully linkable* templates. [Go17a] tested their framework analysis on a HE-based BTP that uses Euclidean distance and reported that it is fully unlinkable while the BF-based BTP in [Go16b] lies between fully unlinkable and semi unlinkable. Note that this procedure works only if the comparison score is known, however for an HE-base BTPs this score can be hidden [PPV17] and only the comparison outcome is revealed. Hence, this procedure studied the unlinkability of the underlying unprotected template instead of the one protected by HE.

4 Homomorphic Encryption based BTP Schemes

Homomorphic Encryption (HE) has been the centerpiece of many privacy-preserving schemes, in particular biometric recognition in the encrypted domain [AM14, Ka15, IJL20] as it allows processing of encrypted templates without decryption. The use of an IND-CPA[6] secure HE scheme guarantees unlinkability, irreversibility and confidentiality under the constraint of the hardness of the underlying mathematical problem. Unlike classical BTP schemes, HE-based BTPs provide template protection even for a remote biometric recognition since an encrypted template can be sent over an unprotected public channel as only the party holding the private key is able to decrypt, and thus the importance of key management in the design of HE-based BTPs. Hence, HE allows a distributed comparison between the client and the server where only the party with the disclosure right is entitled to learn the recognition outcome. Therefore, in this survey,

[6] Indistinguishability under Chosen Plaintext Attack ensures that the encryption of the same plaintext twice yields two different ciphertexts. This property contributes to the dynamism of the protected template.


1
Binary feature vector matrix
W
H
Block B_i
a_1
a_n
n
l
2
Non-invertible transformation
a_1
a_n
k_1
k_n
a_1^*
a_n^*
Block B_i
Key K_{B_i}
$a_i^* = a_i \oplus k_i$
1st category
Structure-Preserving Feature Re-Arrangement
a_1
a_n
$\mathrm{RowPerm}_{K_{B_i}}$
a_1^*
a_n^*
Block B_i
$a_i^* = \mathrm{RowPerm}_{K_{B_i}}(a_i)$
2nd category
3
0 1 A^* $2^n - 1$
0 0 1 0 0 1 0 0 0
i-th Bloom Filter BF_{B_i}
A^*
$A^* = \mathrm{B2I}(a_1^*, \cdots, a_n^*)$
B2I is a binary-to-integer mapping
HD is Hamming distance
$|\mathrm{BF}_{B_i}|$ number of ones in BF_{B_i}

1 Extract binary feature vectors and partition them into k feature blocks of dimension $n \times l$

2 Each block B_i is transformed using one of the transformations below:
- **1st category** uses the non-invertible transformation based on a XOR with a key
- **2nd category** uses the Structure-Preserving Feature Re-Arrangement based on a row-wise random permutation

3 Compute a Bloom filter BF_{B_i} for each transformed block B_i.
The BF-based template T is of the set of those BFs $T = \{\mathrm{BF}_{B_i}\}_1^k$
The dissimilarity between two templates T_1 and T_2 is given by

$$DS(T_1, T_2) = \sum_{i=1}^{k} DS\left(\mathrm{BF}_{B_i}^1, \mathrm{BF}_{B_i}^2\right) \text{ where } DS\left(\mathrm{BF}_{B_i}^1, \mathrm{BF}_{B_i}^2\right) = \frac{HD\left(\mathrm{BF}_{B_i}^1, \mathrm{BF}_{B_i}^2\right)}{\left|\mathrm{BF}_{B_i}^1\right| + \left|\mathrm{BF}_{B_i}^2\right|}$$

Fig. 1: Overview of the 1st category and the 2nd category BF-based BTP schemes. Step 1 and Step 3 are common to both categories. In Step 2, the 1st category (resp. 2nd category) each block is transformed via a XOR with user's key (resp. row-wise random permutation). Note that the key is user-specific and should be different from an application to another to avoid cross-matching over databases. The original scheme [RBB13] uses the same key for all blocks while [BMR17], who assessed its security, proposed to use a different key per block, as depicted in this figure.

we classify HE-based BTPs according to their key management approach: either a single key HE[7], where the template is encrypted with the public key of one of the parties and is decryptable with its private key, or threshold HE where the template is encrypted using a joint public key between the client and the server and is decryptable using their both partial private keys.

Single key HE-based BTPs: The choice of a suitable HE scheme for designing a HE-based BTP scheme depends on the comparison measure that produces either a similarity score or a dissimilarity score. Some comparison measures (such as Hamming distance) can be efficiently implemented under encryption using only a PHE scheme while others that consume more multiplications (such as Cosine similarity) can benefit from SIMD operations of a SWHE scheme or a FHE scheme to improve their efficiency under encryption. The design of a HE-based BTP

[7] Here, single key means that there is one single private key (decryption key) that is retained by one single party unlike in threshold HE where the private key is divided between more than one single party or in multi-key HE where each party holds its own private key.

scheme also depends on the recognition protocol architecture, the parties involved (such as client, authentication server and database server, where the two later are sometimes combined as a single server), which party has the right to learn the recognition outcome based on which the key management is handled.

For applications such as access control, the client is entitled to learn the recognition outcome. For instance, schemes such as [Ba10, SSNS15, Ch16] encrypt the template with the client's public key and stores the encrypted template on the server's database who computes the comparison measure under encryption and sends the final score encrypted to the client. While in other applications such as remote authentication to a service, the authentication server is entitled to learn the recognition outcome. For example, schemes such as [Še14, Go16a, GBFG16, Go17b, Ko20] differentiate between an authentication server and a database server with the assumption that both do not collude. In these schemes, the template is encrypted with the authentication server's public key and stored on the database server. This time the database server performs the comparison under encryption and sends the encrypted final score to the authentication server. In both cases, the party, entitled to learn the recognition outcome, decrypts the encrypted final score and then compares it with the system's threshold, if the score exceeds the threshold then the party counts it as a match otherwise a no match. Hence, the comparison is not fully in the encrypted domain as the comparison with the threshold is performed after the decryption and the entitled party learns more than what it needs to learn, the final score and the recognition outcome.

In some schemes, such as [Up10, IJL20], the template is encrypted with the client's public key although the authentication server is the entitled party. For the comparison measure, [Up10] uses the support vector machine (SVM) classifier while [IJL20] uses the squared Euclidean distance (SED). During the enrollment of a given individual, in [Up10] the classifier is trained on several biometric samples of that individual and the encrypted template is formed by encrypting the classifier's parameters using the client's public key while in [IJL20] the encrypted template is simply the encrypted feature vector.

During the comparison, in [Up10] the client sends an encrypted freshly extracted feature vector to the authentication server who multiples them feature-wise with the encrypted template and a random value in order to blind the individual products. Subsequently, the server sends these blinded products to the client who decrypts and adds them and then sends back the result to the server so that it cancels out the blinding to learn the final score based on which it makes its decision. Similarly, in [IJL20] the server computes a blinded SED under encryption, sends the encrypted blinded final score to the client who decrypts it and sends it back. Then, the server removes the blinding from the blinded final score and performs the comparison with the threshold. Again in these cases the final score is revealed to the server and thus the comparison with the threshold is performed outside the encrypted domain.

Threshold HE-based BTPs: The encryption of the template with the authentication server's public key, even if the encrypted template is stored on the database server, is unsafe since in case the authentication server intercepts the communication between the client and the database server or illegally obtains the encrypted template, the authentication server is able to decrypt the encrypted template and learns the clear template that is supposed to be protected. HE-based BTP schemes such as [Ka15, PPV17] use a threshold variant of HE to encrypt the template in order to address the above mentioned limitation introduced by the use of a single key HE scheme. Hence, a threshold HE encrypted template cannot be decrypted by neither the client nor the server on his own but instead both of them need to participate in the decryption process, and thus a better control of the biometric data flow from both parties.

In general, the exposure of the final score, whether to the client or to the server, leaks the closeness between a freshly processed biometric data (probe) and the static previously processed biometric data (template) as well as the quality of a user's biometric modality. Taking advantage from HE that allows processing under encryption, [PPV17] shows that the final score can be hidden. Moreover, [PPV17] performs the comparison with the threshold under encryption and then reveals only the recognition outcome, *match* or *no match*, at moment of decryption.

Tab. 1: Comparison Table Showing the Advantages and Disadvantages of Each Approach

BTP approaches	**BF-based BTP**		**HE-based BTP**	
Categories	**1st Category**	**2nd Category**	**Single Key HE**	**Threshold HE**
Schemes	[RBB13, Ra14, RB14] [Go14, Ra15, Li15]	[Go16b, Ma17]	[Up10, Ch16, SSNS15] [Ba10, Še14, IJL20, Ko20]	[Ka15, PPV17]
Irreversibility	✓	✓	✓	✓
Unlinkability	✗[1]	✓[2]	✓	✓
Confidentiality	✓	✓	✓	✓
Supported modalities	All	All	All	All
Supported features	Binary and integer	Binary and integer	Binary, integer and float	Binary, integer and float
Feature alignment	Not needed [3]	Needed [3,4]	Needed	Needed
Comparison	Centralized	Centralized	Centralized and distributed	Centralized and distributed
Malleability	Malleable	Malleable	Malleable	Malleable
Final score exposure	Exposed	Exposed	Can be hidden	Can be hidden
Template dynamism	Static [5]	Static [5]	Refreshable and Randomizable	Refreshable and Randomizable
Template size	Linear in #feature blocks and BF size	Linear in #feature blocks and BF size	Linear in #features and ciphertext size	Linear in #features and ciphertext size
Runtime Efficiency	Fast	Fast	Practical to slow [6]	Practical to slow [6]
Recognition Accuracy	No accuracy loss	No accuracy loss	No accuracy loss	No accuracy loss

[1] Shown by [HMP14] and [BMR17]. [2] [Go17a] reports that it is slightly linkable. [3] However, it compares BFs generated from the same block of features. [4] For faces, it assumes pre-aligned images. [5] Once it is generated, it cannot be refreshed. [6] Depends on HE scheme security level.

5 BF-based BTP Schemes vs HE-based BTP Schemes

Both approaches present pros and cons and differently satisfy the tradeoff efficiency-security which makes a binary decision between these approaches difficult to make. Table 1 summarizes and compares BF-based BTP schemes and HE-based BTP schemes with respect to the privacy requirements of ISO/IEC 24745 (rows 4, 5 and 6), supported modalities and their nature (rows 7, 8 and 9), biometric recognition protocol (rows 10, 11 and 12), template's characteristics (rows 13 and 14) and performance of the overall BTP (rows 15 and 16). Note that *malleability* means whether the protected template can be inconspicuously altered. A BF-based template can be modified by flipping activated/deactivated bits while HE-based template can be modified by injecting ciphertexts to the encrypted template since HE is malleable by nature. Therefore, a verification mechanism needs to be applied along with BTP schemes to check the validity of the protected template and monitor the correctness of comparison operations.

6 Conclusion

In this paper, we investigated existing BF-based BTPs and HE-based BTPs with regard to the fulfillment of the privacy requirements of ISO/IEC 24745. While both approaches preserve the biometric accuracy, however they present advantages and disadvantages that vary according to the tradeoff efficiency-security. The choice of using one approach over the other depends on the setting where the BTP scheme is intended to be deployed and the level of trustworthiness of the parties involved in processing the protected template. In both approaches, the protected template needs to be treated with cautiousness since according to [Si12] and [AM14] if the parties do not follow the recognition protocol as prescribed, then serious biometric leakage can happen. Unlike BF-based BTPs, HE-based BTPs are more able to deal with this kind of misbehavior since they can be combined with secure and verifiable computation techniques to monitor the flow of the computation and thus satisfy the privacy requirements of ISO/IEC 24745 in a trustless setting.

Acknowledgment

This work was supported by the PriMa project that has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860315.

We would like to thank Christoph Busch and Marcel Grimmer for their inspiring lecture that motivated the research done in this paper.

References

[Ac18] Acar, Abbas; Aksu, Hidayet; Uluagac, A Selcuk; Conti, Mauro: A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (CSUR), 51, 2018.

[AM14] Abidin, Aysajan; Mitrokotsa, Aikaterini: Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-lwe. In: 2014 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2014.

[Ba10] Barni, Mauro; Bianchi, Tiziano; Catalano, Dario; Di Raimondo, Mario; Labati, Ruggero Donida; Failla, Pierluigi; Fiore, Dario; Lazzeretti, Riccardo; Piuri, Vincenzo; Piva, Alessandro et al.: A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE, 2010.

[BGN05] Boneh, Dan; Goh, Eu-Jin; Nissim, Kobbi: Evaluating 2-DNF formulas on ciphertexts. In: Theory of cryptography conference. Springer, 2005.

[BGV14] Brakerski, Zvika; Gentry, Craig; Vaikuntanathan, Vinod: (Leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT), 6, 2014.

[BM04] Broder, Andrei; Mitzenmacher, Michael: Network applications of Bloom filters: A survey. Internet mathematics, 1, 2004.

[BMR17] Bringer, Julien; Morel, Constance; Rathgeb, Christian: Security analysis and improvement of some biometric protected templates based on Bloom filters. Image and Vision Computing, 58, 2017.

[Br12] Brakerski, Zvika: Fully homomorphic encryption without modulus switching from classical GapSVP. In: Annual Cryptology Conference. Springer, 2012.

[Ch16] Cheon, Jung Hee; Chung, HeeWon; Kim, Myungsun; Lee, Kang-Won: Ghostshell: Secure Biometric Authentication using Integrity-based Homomorphic Evaluations. IACR Cryptology ePrint Archive, 2016.

[Ch17] Cheon, Jung Hee; Kim, Andrey; Kim, Miran; Song, Yongsoo: Homomorphic encryption for arithmetic of approximate numbers. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2017.

[El85] ElGamal, Taher: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31, 1985.

[FV12] Fan, Junfeng; Vercauteren, Frederik: Somewhat practical fully homomorphic encryption. IACR Cryptol. ePrint Arch., 2012.

[GA13] Geravand, Shahabeddin; Ahmadi, Mahmood: Bloom filter applications in network security: A state-of-the-art survey. Computer Networks, 57, 2013.

[GBFG16] Gomez-Barrero, Marta; Fierrez, Julian; Galbally, Javier: Variable-length template protection based on homomorphic encryption with application to signature biometrics. In: 2016 4th International Conference on Biometrics and Forensics (IWBF). IEEE, 2016.

[Ge09] Gentry, Craig et al.: A fully homomorphic encryption scheme, volume 20. Stanford university Stanford, 2009.

[Go14] Gomez-Barrero, Marta; Rathgeb, Christian; Galbally, Javier; Fierrez, Julian; Busch, Christoph: Protected facial biometric templates based on local gabor patterns and adaptive Bloom filters. In: 2014 22nd International Conference on Pattern Recognition. IEEE, 2014.

[Go16a] Gomez-Barrero, Marta; Fierrez, Julian; Galbally, Javier; Maiorana, Emanuele; Campisi, Patrizio: Implementation of fixed-length template protection based on homomorphic encryption with application to signature biometrics. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2016.

[Go16b] Gomez-Barrero, Marta; Rathgeb, Christian; Galbally, Javier; Busch, Christoph; Fierrez, Julian: Unlinkable and irreversible biometric template protection based on Bloom filters. Information Sciences, 370, 2016.

[Go17a] Gomez-Barrero, Marta; Galbally, Javier; Rathgeb, Christian; Busch, Christoph: General framework to evaluate unlinkability in biometric template protection systems. IEEE Transactions on Information Forensics and Security, 13, 2017.

[Go17b] Gomez-Barrero, Marta; Maiorana, Emanuele; Galbally, Javier; Campisi, Patrizio; Fierrez, Julian: Multi-biometric template protection based on homomorphic encryption. Pattern Recognition, 67, 2017.

[HMP14] Hermans, Jens; Mennink, Bart; Peeters, Roel: When a Bloom filter is a doom filter: security assessment of a novel iris biometric template protection system. In: 2014 international conference of the biometrics special interest group (BIOSIG). IEEE, 2014.

[Hu09] Hurst, Thomas: , Bloom Filter Calculator, 2009.

[IJL20] Im, Jong-Hyuk; Jeon, Seong-Yun; Lee, Mun-Kyu: Practical Privacy-Preserving Face Authentication for Smartphones Secure Against Malicious Clients. IEEE Transactions on Information Forensics and Security, 15, 2020.

[JNN08] Jain, Anil K; Nandakumar, Karthik; Nagar, Abhishek: Biometric template security. EURASIP Journal on advances in signal processing, 2008, 2008.

[Ka15] Karabat, Cagatay; Kiraz, Mehmet Sabir; Erdogan, Hakan; Savas, Erkay: THRIVE: threshold homomorphic encryption based secure and privacy preserving biometric verification system. EURASIP Journal on Advances in Signal Processing, 2015.

[KM08] Kirsch, Adam; Mitzenmacher, Michael: Less hashing, same performance: Building a better Bloom filter. Random Structures & Algorithms, 33, 2008.

[Ko20] Kolberg, Jascha; Drozdowski, Pawel; Gomez-Barrero, Marta; Rathgeb, Christian; Busch, Christoph: Efficiency Analysis of Post-quantum-secure Face Template Protection Schemes based on Homomorphic Encryption. In: 2020 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, 2020.

[Ku20] Kumar, Nitin et al.: Cancelable biometrics: A comprehensive survey. Artificial Intelligence Review, 53, 2020.

[Li15] Li, Guoqiang; Yang, Bian; Rathgeb, Christian; Busch, Christoph: Towards generating protected fingerprint templates based on Bloom filters. In: 3rd International workshop on biometrics and forensics (IWBF 2015). IEEE, 2015.

[Ma17] Martiri, Edlira; Gomez-Barrero, Marta; Yang, Bian; Busch, Christoph: Biometric template protection based on Bloom filters and honey templates. IET Biometrics, 6, 2017.

[MSM17] Martins, Paulo; Sousa, Leonel; Mariano, Artur: A survey on fully homomorphic encryption: An engineering perspective. ACM Computing Surveys (CSUR), 50, 2017.

[Pa99] Paillier, Pascal: Public-key cryptosystems based on composite degree residuosity classes. In: International conference on the theory and applications of cryptographic techniques. Springer, 1999.

[PPV17] Peeters, Joep; Peter, Andreas; Veldhuis, Raymond NJ: Fast and Accurate Likelihood Ratio Based Biometric Comparison in the Encrypted Domain. arXiv preprint arXiv:1705.09936, 2017.

[Ra14] Rathgeb, Christian; Breitinger, Frank; Busch, Christoph; Baier, Harald: On application of Bloom filters to iris biometrics. IET Biometrics, 3, 2014.

[Ra15] Rathgeb, Christian; Breitinger, Frank; Baier, Harald; Busch, Christer: Towards Bloom filter-based indexing of iris biometric data. In: 2015 international conference on biometrics (ICB). IEEE, 2015.

[RB14] Rathgeb, Christian; Busch, Christoph: Cancelable multi-biometrics: Mixing iris-codes based on adaptive Bloom filters. Computers & Security, 42, 2014.

[RBB13] Rathgeb, Christian; Breitinger, Frank; Busch, Christoph: Alignment-free cancelable iris biometric templates based on adaptive Bloom filters. In: 2013 international conference on biometrics (ICB). IEEE, 2013.

[Se11] Secretary, ISO Central: Information technology – Security techniques – Biometric information protection. Standard ISO/IEC 24745:2011, International Organization for Standardization, 2011.

[Še14] Šeděnka, Jaroslav; Govindarajan, Sathya; Gasti, Paolo; Balagani, Kiran S: Secure outsourced biometric authentication with performance evaluation on smartphones. IEEE Transactions on Information Forensics and Security, 10, 2014.

[Si12] Simoens, Koen; Bringer, Julien; Chabanne, Hervé; Seys, Stefaan: A framework for analyzing template security and privacy in biometric authentication systems. IEEE Transactions on Information forensics and security, 7, 2012.

[SP17] Sandhya, Mulagala; Prasad, Munaga VNK: Biometric template protection: A systematic literature review of approaches and modalities. Biometric Security and Privacy, 2017.

[SS18] Sadhya, Debanjan; Singh, Sanjay Kumar: Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions. Multimedia Tools and Applications, 77, 2018.

[SSNS15] Shahandashti, Siamak F; Safavi-Naini, Reihaneh; Safa, Nashad Ahmed: Reconciling user privacy and implicit authentication for mobile devices. Computers & Security, 53, 2015.

[TKL08] Teoh, Andrew BJ; Kuan, Yip Wai; Lee, Sangyoun: Cancellable biometrics and annotations on biohash. Pattern recognition, 41, 2008.

[Up10] Upmanyu, Maneesh; Namboodiri, Anoop M; Srinathan, Kannan; Jawahar, CV: Blind authentication: a secure crypto-biometric verification protocol. IEEE transactions on information forensics and security, 5, 2010.

[WNK20] Wood, Alexander; Najarian, Kayvan; Kahrobaei, Delaram: Homomorphic encryption for machine learning in medicine and bioinformatics. ACM Computing Surveys (CSUR), 53, 2020.