MT-PRO: Multibiometric Template Protection Based On Homomorphic Transciphering

Pia Bauspieß*†, Chiara-Marie Zok*, Anamaria Costache†,
Christian Rathgeb*, Jascha Kolberg*, and Christoph Busch*†
* Hochschule Darmstadt, da/sec - Biometrics and Security Research Group,
{christian.rathgeb, jascha.kolberg, christoph.busch}@h-da.de
† NTNU – Norwegian University of Science and Technology,
{pia.bauspiess, anamaria.costache}@ntnu.no

***Abstract*—Reliable authentication of individuals is the foundation of trusted digital interaction. Biometrics lend themselves ideally to this goal. However, biometric data must be protected under computation according to European laws and international standards. Over the past ten years, fully homomorphic encryption has become a popular tool for biometric template protection. However, it comes with the security risk of cryptographic key material, which requires careful management and could be leaked, leaving the stored templates vulnerable to attacks. To meet this challenge, we present the novel MT-PRO protocol utilising homomorphic transciphering to improve the security of such systems against offline decryption attacks. Our protocol does not impair the biometric performance and allows for multi-biometric comparisons of fixed-length feature representations. Furthermore, we evaluated our protocol on public data sets with open-source implementation available at https://github.com/dasec/MT-PRO and discuss its real-world application potential.**

***Index Terms*—template protection, fully homomorphic encryption, multibiometrics, homomorphic transciphering**

I. Introduction

Trustworthy digital communication requires reliable authentication mechanisms, i.e., the ability to tie a human user to their digital identity. The need for reliable authentication is present in many applications, ranging from online banking and legal transactions to telemedicine. Biometric characteristics are uniquely suited to provide such authentication mechanisms, as they allow for a persistent identification of individuals [1].

However, there exist a number of concerns regarding biometric authentication, which can be classified into two main categories: concerns about the reliability (or security) of biometric authentication, and concerns about the protection of biometric feature vectors stored and used in the system (i.e., privacy). For the privacy protection of biometric reference templates, the ISO/IEC 24745 standard on biometric information protection [2] defines clear requirements: *i) unlinkability*, two protected templates stored in different applications cannot be linked to the same subject, *ii) renewability*, new templates can be created from the same source if the previously stored reference was leaked without the need to re-enrol a subject, and *iii) irreversibility*, it is impossible to reconstruct original samples given only protected templates. Furthermore, both the computational and biometric performance (i.e., accuracy) of the unprotected system should be preserved.

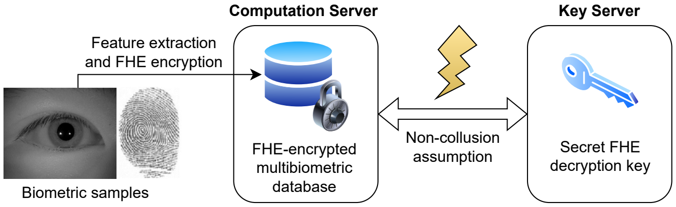
Computation Server
Key Server
Feature extraction and FHE encryption
Biometric samples
FHE-encrypted multibiometric database
Non-collusion assumption
Secret FHE decryption key

Fig. 1. Security risk in FHE-based biometric template protection: if the non-collusion assumption is violated, the encrypted reference database can be decrypted by an attacker, leaving the enrolled templates vulnerable to attacks.

Recent solutions to biometric template protection apply *Fully Homomorphic Encryption* (FHE) for encrypted storage and comparison of biometric feature vectors [3]–[6]. The established architecture for these works includes a two-server setup, where a trusted key server manages the cryptographic key material, while a computation server has access to the encrypted reference database (Fig. 1). This scenario is typically considered in a semi-honest adversary model (aside from [7]), where the two servers must not collaborate. If they do, or an attacker gains access to the cryptographic key material in another way, the database could be decrypted and the enrolled subjects would be vulnerable to impersonation attacks.

This non-collusion assumption can be considered the weakest point in FHE-based template protection systems, as it does not reflect real-world adversary capabilities. This has lead to a decreased trust in outsourced biometric authentication compared to on-device biometric authentication, e.g., FaceID [8]. Security against attackers who have obtained secret components of a biometric system has previously only been achieved using cancelable biometrics [9], which can decrease the accuracy of the system. The accuracy of biometric comparisons however determines the reliability of biometric authentication, and thereby, its security. As biometric feature representations are noisy due to intra-class variance, they introduce the risk of false-accepts, which can lower the security of the biometric system. In response, *multibiometric* systems have received increased interest in recent years [4], [10]–[12]. Through the combination of multiple biometric modalities (e.g., iris and fingerprint), the false-accept rate can be lowered significantly [12], increasing the overall security level.

A secure and reliable biometric authentication system would therefore address both of the aforementioned research challenges: security and privacy. In this work, we present such a system with our novel MT-PRO protocol that utilises the cryptographic concept of *Homomorphic Transciphering* (HT) [13]. Using HT, the protected database receives an additional layer of encryption, such that the leakage of the FHE secret does not enable a viable attack on the database. We describe our contribution as follows.

- We present the novel MT-PRO protocol for secure and privacy-preserving multibiometric verification with HT. To the best of our knowledge, this is the first application of HT to biometric template protection.
- Our MT-PRO protocol is secure against an attacker who has obtained both the protected multibiometric database and the corresponding FHE secret key. Compared to related work considering this attack model, our protocol does not impair the biometric performance of the system. We give a vulnerability analysis of established FHE-based BTP approaches with regard to these *offline attacks* and compare our work to the state-of-the-art in the field.
- We present a reproducible experimental evaluation of MT-PRO and give a comprehensive security analysis, showing how the shortcomings of current FHE-based BTP approaches have been addressed.

The remainder of this article is structured as follows: Section II discusses related work and gives context to our contribution, before we define the cryptographic backbones of our work in Section III. As our main contribution, Section IV presents our proposed MT-PRO protocol for HT-based multibiometric template protection secure against offline attacks, including a vulnerability analysis of previous work. The experimental evaluation of MT-PRO is presented in Section V with a security analysis, before we offer conclusions in Section VI.

II. Related Work

The concept of HT has previously received interest from various research fields, including cloud computing [14] and privacy-preserving genomic comparisons [15]. However, these previous works have only used FHE schemes based on integer plaintexts, which in the context of real-valued biometric feature representations lead to accuracy loss through quantization. In comparison, our MT-PRO protocol utilises an encryption scheme that operates directly on floating point data [16], such that no accuracy is lost in the encrypted domain.

More recently, the problem of FHE-based template protection schemes secure against offline decryption attacks has been investigated in biometric research, with [9] proposing a combination of *Cancelable Biometrics* (CB) and FHE to mitigate the leakage of secret key material. However, the application of CB yields an accuracy loss [17] in addition to requiring quantisation to accommodate for integer-based FHE.

Regarding the aspect of an additional layer of encryption in MT-PRO, a notable recent work is [12], who utilise the concept of password-hardening for fuzzy vaults. While [12] also add a password-derived symmetric key to their scheme, the symmetric decryption is performed on the client side. Thereby, the client gains access to the original protected database entry, i.e., the locked fuzzy vault, and can potentially perform offline attacks. In MT-PRO on the other hand, the symmetric decryption is performed inside the FHE circuit on the server side, such that the client does not learn the protected reference template, while the server does not learn the symmetric key. Table I gives an overview of related works.

TABLE I
Qualitative comparison of related work.

Reference	BTP approach	Preserve accuracy	Prevent offline attacks	Post-Quantum Security
Canteaut et al. 2017 [14]	FHE + HT*	✗	✓	✓
Singh et al. 2018 [15]	FHE + HT*	✗	✓	✓
Boddeti 2018 [18]	FHE	(✓)	✗	✓
Otroshi et al. 2022 [9]	CB + FHE	✗	✓	✓
Sperling et al. 2022 [11]	FHE	✓	✗	✓
Ours	FHE + HT	✓	✓	✓

*not applied to biometric data

III. Background

A. Homomorphic Encryption (HE)

HE is a cryptographic technique that allows for computation on encrypted data that translate directly to computation on the underlying plaintext. HE schemes are classified by the arithmetic operations they allow for, where FHE allows for the evaluation of arbitrary arithmetic circuits [19]. For the scope of our work, we give a simplified definition of the following FHE functionalities [16]:

- $(sk, pk) \leftarrow \mathit{HomKeyGen}(1^\lambda)$: on input of the security parameter λ, generates a secret key sk and public key pk, where pk includes the homomorphic evaluation keys.
- $c_m \leftarrow \mathit{HomEnc}(pk, m)$: on input of the public key pk and a message m, outputs a ciphertext c_m.
- $c_{f(m_1,m_2)} \leftarrow \mathit{HomEval}(pk, c_{m_1}, c_{m_2})$: on input of the public key pk and two ciphertexts c_{m_1} and c_{m_2}, outputs an encryption $c_{f(m_1,m_2)}$ of the evaluation of a function f on the underlying plaintext messages m_1 and m_2.
- $m' \leftarrow \mathit{HomDec}(sk, c_m)$: on input of the secret key sk and ciphertext c_m, outputs a message m'. It holds that $m = m'$ with overwhelming probability.

B. Homomorphic Transciphering (HT)

HT [13] combines FHE and symmetric encryption. We first define a symmetric cipher with the following functions:

- $k \leftarrow \mathit{SymKeyGen}(1^\lambda)$: on input of the security parameter λ, this function generates a key k .
- $c_m \leftarrow \mathit{SymEnc}(k, m)$: on input of the key k and a message m, this function outputs a ciphertext c_m.
- $m \leftarrow \mathit{SymDec}(k, c_m)$: on input of key k and ciphertext c_m, this function outputs the message m.

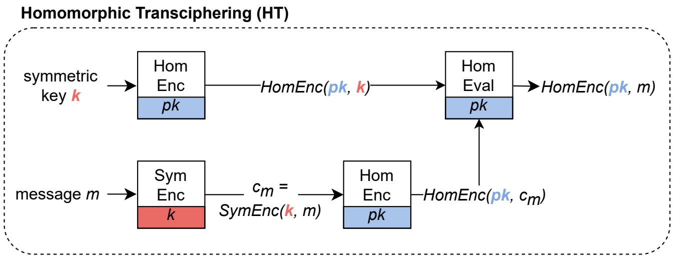

Fig. 2. FHE encryption using Homomorphic Transciphering (HT) [13].

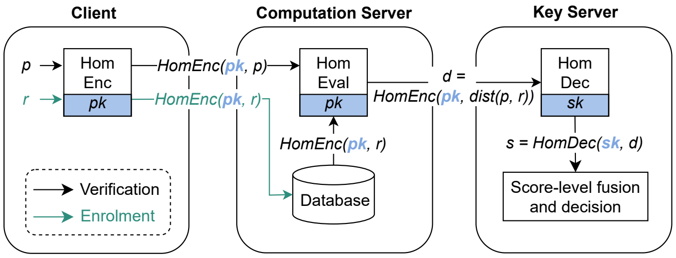

Fig. 3. FHE-protected verification baseline system as used in [3]–[6].

Let (sk, pk) be a FHE key pair as defined above. Then, HT allows for the transformation of a symmetric encryption $\mathit{SymEnc}(k, m)$ of a message m to a homomorphic encryption of the same message m, i.e., $\mathit{HomEnc}(pk, m)$, using a homomorphic encryption of the symmetric key, i.e., $\mathit{HomEnc}(pk, k)$. An illustration of the HT functionality can be seen in Fig. 2.

The transciphering functionality performs a homomorphic evaluation of the decryption circuit of the symmetric cipher. Thereby, the party computing the transciphering does not gain access to the symmetric key k or the message m. Typically, a client device will compute the symmetric encryption of m which requires less computational workload and bandwidth, while a server will compute the transciphering operation and retrieve the homomorphic encryption of m. It is important to note that not all symmetric ciphers are considered *FHE-friendly*, i.e., only symmetric ciphers specifically developed for an application to transciphering can be used [13].

IV. Protocol

We will now describe our MT-PRO protocol in detail. We begin with a description of the unprotected and protected baseline system using FHE, including a vulnerability analysis under offline attacks. Then, we will describe the integration of HT and discuss its benefits and drawbacks.

A. Pre-processing

Biometric characteristics can be captured by various sensors depending on the biometric modality. In our protocol, we consider combinations of multiple biometric modalities, known as *multibiometrics*. We consider only feature vectors that can be expressed as fixed-length, ordered vectors. However, our protocol is unconstrained in terms of the length of single vectors, number of vectors, and data type (i.e., binary, integer, or floating point values). In particular, a combination of different feature representations and comparison functions can be used in MT-PRO. After capturing and feature extraction, we consider the reference template or probe feature vector as a concatenation of individually extracted vectors. The cryptographic solution for deriving the combined comparison score will be explained in further detail later in this Section.

B. Two-Server Architecture

Our MT-PRO protocol builds on the established architecture [3]–[6] consisting of a computation server and key server as described above. A client capturing and extracting the reference and probe feature vectors interacts with the computation server in order to initiate an enrolment or verification transaction. In prior works, both servers are considered to act as semi-honest adversaries, i.e., such that they do not deviate from the given protocol, and do not collude in sharing any data they receive or store. We will continue our description of the baseline system under this model before considering the risk of offline attacks and its impact on this security assumption.

C. Unprotected Baseline System

The unprotected baseline system performs enrolment and verification transactions on plaintext data. During enrolment, the unencrypted reference template is stored in the database. Then, for a verification transaction, a fresh probe feature set is sent to the computation server, who computes the comparison score and determines the verification outcome.

D. Protected Baseline System

The protected baseline system shown in Fig. 3 performs the same transactions as the unprotected system, however, while operating on encrypted instead of plaintext data. During enrolment, the client encrypts the reference template to a ciphertext $\mathit{HomEnc}(pk, r)$, which is stored in the database. During verification, the client encrypts the probe feature vector to $\mathit{HomEnc}(pk, p)$, which is sent to the computation server. Through the properties of FHE, the distance score can be computed based on the encrypted reference and probe templates, yielding an encrypted comparison score $d = \mathit{HomEnc}(pk, \mathit{dist}(p, r))$. The key server, using the FHE secret key sk, can decrypt the score to $\mathit{HomDec}(sk, d)$ and determine the verification outcome after threshold comparison.

E. Vulnerability Analysis

Considering real-world adversaries, the FHE-protected baseline system described in Section IV-D established over the past ten years [3]–[6] can be vulnerable to the following attack. Having gained access to the protected reference database consisting of ciphertexts $\mathit{HomEnc}(pk, r)$, and the FHE secret key sk, an attacker can easily decrypt and obtain the reference templates, from which samples can be reconstructed with high confidence [20], [21]. If a template is compromised, its biometric instance (e.g., a finger or eye) can no longer be used for trustworthy authentication due to the risk of impersonations attacks, which could be viable for several decades [1]. We call this attack scenario an *offline decryption attack* or *offline*

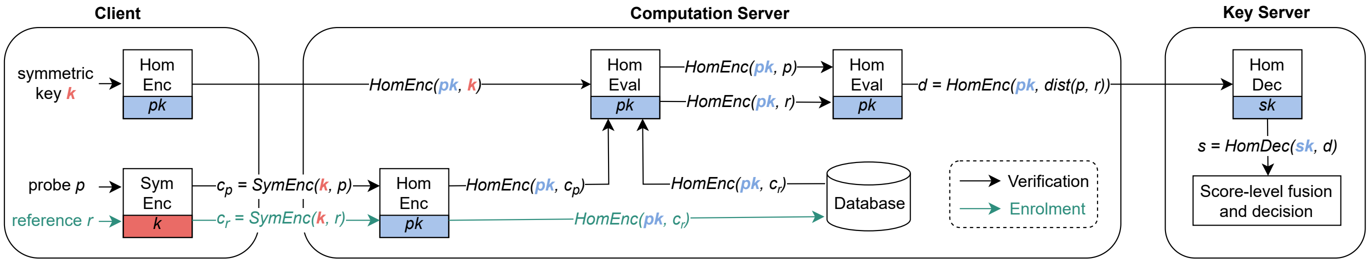

Fig. 4. Proposed MT-PRO protocol based on HT [13] and FHE [16] ensuring protection of the encrypted database under offline decryption attacks. If an attacker gains access to the database and the FHE secret key, it cannot decrypt the encrypted references due to the additional layer of symmetric encryption.

attack, as the attack can be executed without active access to the system and thereby in an unobtrusive manner.

It is important to note that the addition of zero-knowledge proofs in previous works such as [7] does not withstand such offline attacks, and can therefore not be considered a complete solution to the security challenge. While zero-knowledge proofs guarantee that the computations have been calculated correctly, and can therefore aid in the detection of an attacker deviating from the protocol, they do not protect the encrypted database from decryption once an attacker has gained access to the FHE secret key. We will therefore now present our MT-PRO protocol secure against offline attacks.

F. Enrolment in MT-PRO

In the MT-PRO enrolment phase (Fig. 4), the client computes a symmetric encryption of the reference template $c_r = SymEnc(k, r)$ instead of a homomorphic encryption as in the baseline system, using the symmetric key k. Then, the client sends c_r to the computation server, who computes an additional layer of encryption around the symmetric ciphertext through encrypting it homomorphically to $HomEnc(pk, c_r)$. This ciphertext is then stored in the reference database.

G. Verification in MT-PRO

During MT-PRO verification, also shown in Fig. 4, the client repeats the symmetric encryption for the freshly extracted probe features and computes $SymEnc(k, p)$. In addition, it computes a homomorphic encryption of its symmetric secret key k, yielding $HomEnc(pk, k)$. Then, both ciphertexts are sent to the computation server, who executes the HT. Upon receiving $SymEnc(k, p)$, the computation server computes a homomorphic encryption $HomEnc(pk, c_p)$. Then, $HomEnc(pk, c_p)$, $HomEnc(pk, c_r)$ and $HomEnc(pk, k)$ are inputs to the HT circuit as described in [13]. Using $HomEnc(pk, k)$, the homomorphic evaluation of the symmetric decryption function is computed. As outputs, the computation server obtains FHE ciphertexts $HomEnc(pk, p)$ and $HomEnc(pk, r)$, and the comparison score is computed, which will be described in the following. The key server decrypts the comparison score and determines the verification outcome.

H. Multibiometric Comparisons in MT-PRO

In the MT-PRO protocol, combinations of multiple biometric modalities can be used. For this, we extend the concept of coefficient packing presented by [5], where multiple templates are concatenated and encrypted into the same ciphertext. Two challenges arise with regard to multibiometrics: different template lengths and different comparison functions. Through sharing the template order and length (but no information about the underlying data), the computation server can execute the respective comparison functions for each subcomponent of the multibiometric template. To ensure that no information is overwritten, the masking technique from [22] is applied, where only the final comparison score at the start position within the multibiometric plaintext vector is revealed. The individual scores are then combined though an average score level fusion.

I. Key Management in MT-PRO

Regarding the management of the additional symmetric secret key k within MT-PRO, several options arise:

1) Device key: The symmetric key k can be embedded into the client device, as is typical in IoT applications. This approach has the advantage that the data subject does not need to manage any key material. As the key is static, the reference database can be encrypted as described above, and the transciphering will be correct upon verification. However, the risk of key leakage is larger as one key is used for potentially many subjects, and all reference database entries corresponding to the device key must be re-encrypted when the key is updated. Additionally, a subject can only be verified from the same device that was used during enrolment.

2) Static User Key: Alternatively, the secret key can be made user-specific. To ease key management on the user side, a password-derived key can be used. As long as this key is static, i.e., derived from the password in a deterministic manner, the protocol can be executed as in the case of a device key. Upon a key update, only the corresponding entry for one subject needs to be re-encrypted in the database. Note that contrary to classical password authentication, no hashed password is stored at the computation server, further improving the protection against offline attacks.

3) Ephemeral User Key: The symmetric key can also be derived from password-authenticated key exchange, corresponding to session keys that are different for each authentication attempt. This approach yields a higher security level for the symmetric key as it is no longer feasible to brute-force. As a significant drawback however, the reference database cannot

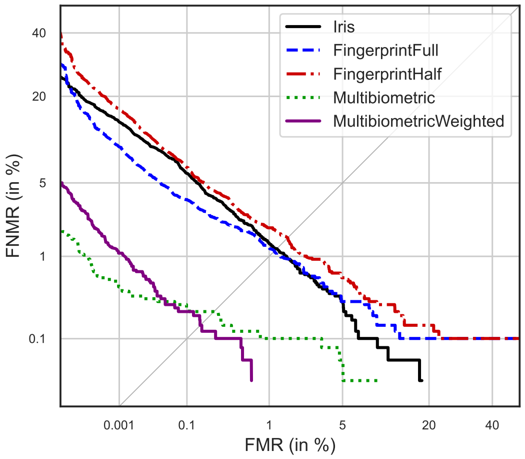

Fig. 5. DET curve showing the multibiometric system performance, where FMR is the false-match rate and FNMR is the false non-match rate [23].

be encrypted with a symmetric cipher, as the keys used during enrolment and verification will be different. This is useful in classical HT scenarios where large amounts of data are encrypted and HT is mainly used for workload reduction on the client side, but not applicable to prevent offline attacks.

V. Experimental Evaluation

We implemented our MT-PRO protocol using the framework by [13], which is based on the Lattigo [24] FHE library. The cryptographic components are the stream cipher HERA [13] and the CKKS [16] FHE scheme. All parameters are chosen at a security level of 128bits. For reproducibility of our results, our implementation is available at https://github.com/dasec/MT-PRO. Due to the high RAM requirements of the HT framework, a Debian GNU 11 server with an AMD EPYC processor at 32x2.8GHz CPU and 128GB RAM was used.

To illustrate the multibiometric verification, we used the newly available deep fingerprint embeddings by [25] of the MCYT [26] database, and deep iris embeddings by [27] of the CASIA Iris Thousand database [28]. For both modalities, 512-dimensional real vectors are extracted, where the fingerprint feature vectors can be split into two 256-dimensional vectors representing the textural and minutiae-derived information, respectively. Cosine distance is used as the comparison function. We evaluated the individual performance (shown as *Iris* and *FingerprintFull* in Fig. 5), the performance using the first 256 dimensions of the fingerprint features (*FingerprintHalf* in Fig. 5), the combined performance of both 512-dimensional feature sets (*Multibiometric* in Fig. 5) as well as the multibiometric performance where only the first 256 dimensions of the fingerprint features are used. For the latter, the individual modalities' scores were scaled according to their dimension (*MultibiometricWeighted* in Fig. 5). By using different-length feature representations, we show the functionality of MT-PRO described in Section IV-H compared to previous approaches considering only feature representations of the same length [5]. MT-PRO can also be instantiated with binary feature representations using the Hamming distance for comparison.

TABLE II
MT-PRO Execution times for verification and enrolment.

MT-PRO Component	Time (s)
Symmetric template encryption	0.42
Homomorphic template encryption	0.21
User key encryption	3.40
Template transciphering	107.64
FHE comparisons	66.40
Comparison score decryption	0.17
Enrolment	0.63
Verification	330.22
Protected Baseline Verification (without HT)	66.78

A. Results

The biometric performance of our MT-PRO protocol can be observed in Fig. 5, where the weighted multibiometric system is the preferred approach. We note however that our protocol is independent of the multibiometric combinations, and that the individual system performance will depend on the modalities and feature representations used. Due to the use of floating-point based FHE [16], the biometric performance of the unprotected baseline system is maintained.

The computational performance can be viewed in Table II. It can be seen that the transciphering operation, i.e., transferring the symmetrically encrypted probe and reference to their homomorphically encrypted representation, is the most expensive operation at 107.64 seconds, followed by the FHE operations at 66.40 seconds. This shows that while the concept of HT is meaningful on a theoretical basis, it is not yet applicable in real-world systems. Further improvements on the cryptographic components are required to improve these transactions times, as further dimensionality reduction of the biometric templates would not yield a significant improvement. Due to larger parameter choices required for HT, the baseline cost of FHE comparisons is also higher than in previous works [5].

B. Security Analysis

MT-PRO fulfils the ISO/IEC 24745 [2] requirements of unlinkability and renewability due to security of the FHE scheme against chosen-plaintext attacks [16]. Post-quantum secure irreversibility is provided by the Ring-Learning With Errors [29] hardness assumption of the FHE and HT schemes [13].

1) Security Against Offline Decryption Attacks: We reconsider the adversary from Section IV-E that has gained access to the encrypted database and the FHE secret key. In MT-PRO, the adversary only has access to a database with entries $\mathit{HomEnc}(pk, c_r) = \mathit{HomEnc}(pk, \mathit{SymEnc}(k, r))$. Therefore, FHE decryption only yields $\mathit{SymEnc}(k, r)$, which cannot be decrypt without the key k. This security guarantee assumes that the database can be attacked in storage, while the computation server is not corrupted during verification. If the adversary gains access to *HomEnc(pk,k)* during verification, the database could be decrypted. However, an attack on the database is the more realistic attack scenario from a forensic standpoint, as databases are static and outsourced targets.

2) Security Under Full Disclosure Model: The ISO/IEC 30136 [30] standard on performance testing of biometric template protection schemes defines the *full disclosure* attack model for biometric systems, where an adversary has access to all algorithms and all secrets used in the system. The standard adds that this security assumption can be restricted to the adversary knowing a subset of the secret information handled throughout the system. Thereby, the security of MT-PRO against offline decryption attack can be considered as a partial fulfilment of the full disclosure model, as MT-PRO remains secure if the FHE secret key is leaked to an attacker. Notably, MT-PRO achieves this security without accuracy loss of the biometric comparisons, which is an advantage compared to previous work [9]. However, the symmetric key k as well as its homomorphic encryption $HomEnc(pk, k)$ must be kept secret. As k can be freshly derived from a user-password for each authentication attempt as described in Section IV-I, it is not easily accessible to an attacker. Additional protection of k could be achieved through the use of multi-party computation, however, at the cost of an additional computational overhead.

VI. Conclusion

In this work, we presented the MT-PRO protocol for fully homomorphic encryption-based biometric template protection secure against offline decryption attacks even if an attacker gains access to the secret key of the homomorphic encryption scheme. To achieve this, we applied homomorphic transciphering to template protection for the first time, yielding a system with post-quantum security and unimpaired biometric performance. Our experimental evaluation showed that homomorphic transciphering is not yet feasible. Therefore, further improvement of the cryptographic components is required.

Acknowledgment

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] R. Kessler, O. Henninger, and C. Busch, "Fingerprints, forever young?" in *Intl. Conf. on Pattern Recognition (ICPR)*, 2021, pp. 8647–8654.

[2] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2022. Information Technology - Security Techniques - Biometric Information Protection*, International Organization for Standardization, 2022.

[3] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, "Packed homomorphic encryption based on ideal lattices and its application to biometrics," in *Intl. Conf. on Availability, Reliability, and Security*. Springer, 2013, pp. 55–74.

[4] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognition*, vol. 67, pp. 149–163, July 2017.

[5] P. Bauspieß, J. Olafsson, J. Kolberg, P. Drozdowski, C. Rathgeb, and C. Busch, "Improved homomorphically encrypted biometric identification using coefficient packing," in *Proc. IEEE Intl. Workshop on Biometrics and Forensics (IWBF)*, 2022.

[6] J. J. Engelsma, A. K. Jain, and V. N. Boddeti, "HERS: Homomorphically encrypted representation search," *IEEE Trans. on Biometrics, Behavior, and Identity Science (T-BIOM)*, 2022.

[7] A. Bassit, F. Hahn, J. Peeters, T. Kevenaar, R. Veldhuis, and A. Peter, "Fast and accurate likelihood ratio-based biometric verification secure against malicious adversaries," *IEEE Trans. on Information Forensics and Security (TIFS)*, vol. 16, pp. 5045–5060, 2021.

[8] Apple Inc., "About Face ID advanced technology," 2022. [Online]. Available: https://support.apple.com/en-us/HT208108

[9] H. Otroshi-Shahreza, C. Rathgeb, D. Osorio-Roig, V. Krivokuća, S. Marcel, and C. Busch, "Hybrid protection of biometric templates by combining homomorphic encryption and cancelable biometrics," in *Proc. Intl. Joint Conf. on Biometrics (IJCB)*. IEEE, October 2022.

[10] P. Drozdowski, C. Rathgeb, B.-A. Mokroß, and C. Busch, "Multi-biometric identification with cascading database filtering," *IEEE Trans.on Biometrics, Behavior, and Identity Science*, vol. 2, no. 3, pp. 210–222, July 2020.

[11] L. Sperling, N. Ratha, A. Ross, and V. N. Boddeti, "HEFT: Homomorphically encrypted fusion of biometric templates," in *Proc. Intl. Joint Conference on Biometrics (IJCB)*. IEEE, 2022.

[12] C. Rathgeb, B. Tams, J. Merkle, V. Nesterowicz, U. Korte, and M. Neu, "Multi-biometric fuzzy vault based on face and fingerprints," in *Proc. Intl. Joint Conference on Biometrics (IJCB)*. IEEE, 2023.

[13] J. Cho, J. Ha, S. Kim, B. Lee, J. Lee, J. Lee, D. Moon, and H. Yoon, "Transciphering framework for approximate homomorphic encryption," in *Intl. Conf. on the Theory and Application of Cryptology and Information Security*. Springer, 2021, pp. 640–669.

[14] A. Canteaut, S. Carpov, C. Fontaine, J. Fournier, B. Lac, M. Naya-Plasencia, R. Sirdey, and A. Tria, "End-to-end data security for IoT: from a cloud of encryptions to encryption in the cloud," in *Cesar Conf.*, 2017.

[15] K. Singh, R. Sirdey, and S. Carpov, "Practical personalized genomics in the encrypted domain," in *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 2018, pp. 139–146.

[16] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Intl. Conf. on the Theory and Appl. of Crypt. and Information Security*. Springer, 2016, pp. 409–437.

[17] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 3, March 2011.

[18] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in *Proc. Intl. Conf. on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 2018, pp. 1–10.

[19] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *ACM Symposium on Theory of Computing*, 2009, pp. 169–178.

[20] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, September 2007.

[21] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[22] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, and C. Busch, "On the application of homomorphic encryption to face identification," in *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*. Gesellschaft für Informatik e.V., September 2019, pp. 173–180.

[23] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 19795-1:2021. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, Intl. Org. for Standardization, June 2021.

[24] C. V. Mouchet, J.-P. Bossuat, J. R. Troncoso-Pastoriza, and J.-P. Hubaux, "Lattigo: A multiparty homomorphic encryption library in Go," in *Proc. of the 8th Workshop on Encrypted Computing and Applied Homomorphic Cryptography*, 2020, pp. 64–70.

[25] T. Rohwedder, D. Osorio-Roig, C. Rathgeb, and C. Busch, "Benchmarking fixed-length fingerprint representations across different embedding sizes and sensor types," in *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*. Gesellschaft für Informatik e.V., September 2023.

[26] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy *et al.*, "MCYT baseline corpus: a bimodal biometric database," *Proc. Intl. Conf. Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, December 2003.

[27] H. Otroshi-Shahreza, P. Melzi, D. Osorio-Roig, C. Rathgeb, C. Busch, S. Marcel, R. Tolosana, and R. Vera-Rodriguez, "Benchmarking of cancelable biometrics for deep templates," *arXiv:2302.13286*, 2023.

[28] Chinese Academy of Sciences Institute of Automation, "CASIA Iris Thousand database," available at http://biometrics.idealtest.org/.

[29] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Annual Intl. Conf. on the Theory and Appl. of Cryptographic Techniques*. Springer, 2010, pp. 1–23.

[30] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 30136:2018. Information technology – Security techniques – Performance testing of biometric template protection schemes*, Intl. Org. for Standardization, 2018.