On the Feasibility of Fully Homomorphic Encryption of Minutiae-Based Fingerprint Representations

Pia Bauspieß[1 2][a], Lasse Vad[1], Håvard Myrekrok[1], Anamaria Costache[1][b], Jascha Kolberg[2][c], Christian Rathgeb[2][d] and Christoph Busch[1 2][e]

[1] *NTNU – Norwegian University of Science and Technology, Norway*

[2]*da/sec - Biometrics and Security Research Group, Hochschule Darmstadt, Germany*

{*pia.bauspiess, anamaria.costache*}*@ntnu.no*

{*jascha.kolberg, christian.rathgeb, christoph.busch*}*@h-da.de*

Keywords: Fingerprint Template Protection, Minutia-Based Fingerprint Representations, Fully Homomorphic Encryption, Post-Quantum Security

Abstract: Protecting minutiae-based fingerprint templates with fully homomorphic encryption has recently been recognised as a hard problem. In this work, we evaluate state-of-the-art fingerprint recognition based on minutiae templates using post-quantum secure fully homomorphic encryption that operates directly on floating point numbers, such that no simplification or quantisation of the comparison algorithm is necessary. In a practical evaluation on a publicly available dataset, we run a benchmark and provide directions for future work.

1 INTRODUCTION

Fingerprint patterns allow for an irrevocable and accurate identification of individuals over several decades (Kessler et al., 2021). Images and templates representing such patterns have therefore, along with other biometric data, been recognised as sensitive personal data by the European Union's General Data Protection Regulation and the ISO/IEC 24745 (ISO/IEC JTC1 SC27 Security Techniques, 2022) standard.

In its most recent version from 2022, the standard places particular emphasis on Biometric Information Protection (BIP) in the presence of quantum computers. In their Quantum Manifesto (EU Parliament, 2016), the European Union expects quantum computers to pose a realistic threat within the next 15 years. Comparing this time frame to the the retention period for biometric systems ranging from 5 (European Data Protection Supervisor, 2018) up to 12 years (Kessler et al., 2021), it becomes evident that long-term protection of biometric data needs to be addressed today.

More concretely, access to a quantum computer would allow an attacker to break the unlinkability, irreversibility, and renewability assurances of classically protected BIP systems, leaving the enrolment data vulnerable for malicious exploitation. These three requirements are defined in ISO/IEC 24745 (ISO/IEC JTC1 SC27 Security Techniques, 2022) as *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 biometric instance without the need to re-enrol, and *iii) irreversibility*, it is impossible to retrieve original templates given only protected templates. Considering the quantum challenge, this work proposes a BIP system that achieves long-term protection according to the standard's requirements through the use of post-quantum cryptography.

However, the lift to post-quantum security does not come without challenges. In particular, the combination of accurate minutiae-based fingerprint recognition and BIP through Fully Homomorphic Encryption (FHE) has recently been recognised as a notorious hard problem by leading researchers in biometrics (Engelsma et al., 2019). So far, solutions have only been proposed for fixed-length fingerprint representations (Kim et al., 2020), or using classically secure cryptography (Gomez-Barrero et al., 2017a). The novelty and objective of this work is therefore to evaluate minutiae-based fingerprint comparison with FHE on floating point numbers, an encryption scheme

[a] https://orcid.org/0000-0003-0225-1674

[b] https://orcid.org/0000-0001-8793-6116

[c] https://orcid.org/0000-0002-3128-8049

[d] https://orcid.org/0000-0003-1901-9468

[e] https://orcid.org/0000-0002-9159-2923

which enjoys increasing interest since its proposal in 2017 (Cheon et al., 2017). As a lattice-based FHE scheme, its post-quantum security is provided by the Ring-Learning with Errors (R-LWE) (Lyubashevsky et al., 2010) hardness assumption.

This work presents post-quantum secure minutiae-based fingerprint comparison algorithm (Cappelli et al., 2010) using FHE, where the comparison algorithm has not been simplified or quantised in order to be compatible with the encryption scheme. Furthermore, we highlight challenges inherent to the application of FHE to minutiae-based fingerprint comparison and provide an experimental benchmark from which we draw conclusions for future work.

The rest of this paper is structured as follows: Section 2 contextualises our contribution, before we present our proposed system in Section 3. We give an experimental evaluation in Section 4 and draw our conclusions in Section 5.

2 RELATED WORK

Fingerprint recognition has historically been based on minutiae, which are defined as ridge endings and bifurcations of fingerprint ridges. While comparison algorithms with high accuracy have been developed (Cappelli et al., 2010; Važan, 2021), they reflect the complexity inherent to comparing two sets of minutiae such as rotation, non-linear transformation, and absence of an inherent ordering. In their development, they have not necessarily considered the application of encryption schemes, which offer only a limited number of operations that can be computed with feasible computational effort (Iliashenko and Zucca, 2021). Therefore, two research directions have emerged that approach the challenge of combining fingerprint recognition with encryption: one is to develop fingerprint representations with simple distance functions as comparison metrics that maintain high recognition accuracy, while the other is to apply and adapt compatible encryption schemes to complex minutiae-based comparators.

Indeed, FHE for fixed-length representations has been proposed for different biometric modalities such as face (Boddeti, 2018; Kolberg et al., 2020; Bauspieß et al., 2022) and iris (Kolberg et al., 2019) with high accuracy and real-time efficiency. For fingerprint specifically, the most prominent representation is Jain et al.'s *FingerCode* (Jain et al., 2000). Notable works on encrypting this representation include (Barni et al., 2010; Gomez-Barrero et al., 2017b; Yang et al., 2020). However, the encryption schemes used are based on classical assumptions and do not hold in the quantum age. A recent work using FHE with post-quantum security on FingerCode templates is (Kim et al., 2020). The FHE scheme (Chillotti et al., 2020) applied here only tolerates binary values, which is compatible with FingerCodes, but not with minutiae templates.

Minutiae-based comparators share the difficulty of finding close pairs within the sets of k reference minutiae and l probe minutiae, the mapping between which can be neither injective nor surjective due to potential missing or spurious minutiae. In addition, samples might be rotated, translated or distorted, requiring either prealignment or a rotation-invariant approach. In theory, FHE allows for the evaluation of arbitrary circuits on encrypted input data (Gentry, 2009). In practice however, both alignment and set comparison are functions that can only be described using conditional statements, the number of which in prevalent approaches is high (Važan, 2021; Zhang and Koushanfar, 2016). Their combination with FHE is therefore not straightforward, and more importantly too costly for practical applications (Iliashenko and Zucca, 2021). In contrast to that, the comparison of alignment-free fixed-length representations can be performed by computing a simple distance function on the encrypted templates, the result of which is typically decrypted to evaluate the comparison against the decision threshold.

Classically secure homomorphic encryption, which is only partially or somewhat homomorphic (Gentry, 2009), has been applied to minutiae-based comparison (Gomez-Barrero et al., 2017a). However, these schemes lack post-quantum security. This is also true for a approaches based on cancelable biometric templates constructed based on randomized feature transformation, most recently represented by an approach by (Rahman et al., 2022), which do not adhere to formal secuirty proofs and are vulnerable to unlinkability attacks. In particular, the indistinguishability under chosen plaintext attacks provided by (F)HE schemes, which gives formal security in terms of ISO/IEC 24745 (ISO/IEC JTC1 SC27 Security Techniques, 2022) is not given in the latter. Other works (Liu and Zhao, 2017; Zhang and Koushanfar, 2016; Gilkalaye and Derakhshani, 2021) have utilised secure multi-party computation (MPC), which is generally speaking more flexible than FHE. As a drawback, it introduces a communication overhead, and practical post-quantum secure MPC has only been explored recently (Büscher et al., 2020).

Table 1 gives a qualitative overview of the most relevant related works discussed in this Section and provides a comparison against our proposed approach.

Table 1: Qualitative comparison of related work on cryptographic fingerprint template protection.

Reference	**Template protection category**	**Cryptographic scheme**	**Variable-length feature representation**	**Post-quantum security**
(Barni et al., 2010)	HE	ElGamal (Elgamal, 1985) Pailler (Paillier, 1999)	✗	✗
(Gomez-Barrero et al., 2017b) (Yang et al., 2020)	HE	Pailler (Paillier, 1999)	✗	✗
(Zhang and Koushanfar, 2016) (Gilkalaye and Derakhshani, 2021)	MPC	Garbled Circuits (Yao, 1986)	✓	✗
(Gomez-Barrero et al., 2017a)	HE	Pailler (Paillier, 1999)	✓	✗
(Kim et al., 2020)	FHE	TFHE (Chillotti et al., 2020)	✗	✓
Ours	FHE	CKKS (Cheon et al., 2017)	✓	✓

3 PROPOSED SYSTEM

We study a combination of the minutiae-based fingerprint comparison algorithm Minutia Cylinder-Code (MCC) (Cappelli et al., 2010) and the state-of-the-art FHE encryption scheme Cheon-Kim-Kim-Song (CKKS) (Cheon et al., 2017) to illustrate the challenges that arise in the process.

3.1 Background

Before we describe our proposed system, we introduce the necessary background in this Section. Subsequently, we introduce the baseline verification scheme without encryption, and finally, our proposed protected system.

Throughout this work, we consider a biometric system operating in verification mode. In a setup phase, subjects are enrolled to the system with their fingerprint features. During a verification transaction, a fresh probe sample is captured a biometric claim, i.e., the claimed identity of the data subject, is transferred to the database along with the probe feature set. Then, a comparison between the probe features and the reference template corresponding to the claim is computed, resulting in a comparison score in the range $[0,1]$, where 1 indicates highest similarity. Finally, this score is compared against a predetermined decision threshold and the comparison trial is accepted or rejected accordingly. In the following section, we describe this comparison algorithm in more detail.

3.1.1 Minutia Cylinder Code

Minutia Cylinder-Code (MCC) (Cappelli et al., 2010) is a fingerprint comparison algorithm that takes as input two minutiae-based fingerprint templates as standardized in ISO/IEC 19794-2 (ISO/IEC JTC1 SC37 Biometrics, 2011) and outputs a similarity score that can further be used for an automated comparison. Minutiae are significant points in the pattern of fingerprint ridges: ridge endings and bifurcations, where one ridge line splits into two. We remind the reader of the following definition of an ISO/IEC 19794-2 (ISO/IEC JTC1 SC37 Biometrics, 2011) fingerprint template in the notation of (Cappelli et al., 2010), Section 3.

Definition 1 (Fingerprint Template)**.** A fingerprint template is an unordered set $T = \{m_i\}_{i=1}^{N}$ of minutiae m_i, where N is the number of minutiae found in a given fingerprint image. Each minutia is given as a tuple $m = (x_m, y_m, \theta_m)$ of its location in terms of x- and y-coordinate (x_m, y_m) given in pixels from the left upper corner of the sample together with its tangential angle with respect to the x-axis θ_m.

Note that the number of minutiae N varies between captures, not only between different subjects, but also within repeated captures of the same instance. This is due to noise during the capture process: depending on the image quality and capture conditions, minutiae can either be missed during feature extraction, or spurious minutiae can be added, resulting in different length representations of the same fingerprint. In addition, the location of the minutiae are subject to fuzzyness, as their location and angle can be distorted through rotation, translation and non-linear transformations. Therefore, minutiae-based fingerprint comparison comprises of the complex problem of accurately comparing two unordered, variable-sized sets of noisy points, a number of which can be spurious.

To address the aforementioned challenges, MCC introduces a local structure associated with each minutiae referred to as a *minutia cylinder*. This structure incorporates information about the neighbourhood of each minutiae, i.e., further minutiae found in close proximity and their spatial and directional relationship with the center minutiae (Cappelli et al., 2010). This approach ensures system interoperability as the cylinder representation is still based on ISO/IEC 19794-2 (ISO/IEC JTC1 SC37 Biometrics, 2011) fingerprint templates. In particular, the variable-length representation is maintained, as the number of minutia cylinders corresponds to the number of minutiae in a fingerprint template. We restate the following definitions from (Cappelli et al., 2010), Section 3.

Definition 2 (Minutia Cylinder)**.** A minutia cylinder is given by a fixed radius R and height 2π centered around the location (x_m, y_m) of a minutia m. It is discretized into small cuboids, called *cells*, which are orientated in the direction of the tangential angle θ_m of the center minutiae. It can be represented as a vector $\mathbf{c}_m \in [0,1]^n$, where n denotes the total number of cells in a cylinder.

As a minutia cylinder only contains relative information concerning the relationship between the minutiae, such as distance and directonal difference, but no global information, it can be considered translation and rotation invariant (Cappelli et al., 2010). The same properties also make it robust against minor non-linear transforms during capture such as different levels of pressure applied on the fingerprint sensor. Most importantly, the fixed-radius neighbourhood is a key component in the handling of missing and spurious minutiae (Cappelli et al., 2010).

Definition 3 (Contribution Score)**.** Each cell inside a minutia cylinder is assigned a numerical value C_m, called *contribution score*, which details the likelihood of finding another minutia in a small neighbourhood with a compatible directional difference.

For a more technical definition along with insightful figures, the reader is referred to (Cappelli et al., 2010), Section 3.

Definition 4 (Cylinder Set)**.** Given a fingerprint template T, its corresponding cylinder set is defined as the set of valid cylinders $\mathbf{c}_m$ for $m \in T$. A cylinder is considered valid if it contains a sufficient number of contribution scores, i.e., exeeding a pre-defined threshold of a minimal number of contribution scores and a minimal number of contributing neighbour minutiae.

Finally, a reference fingerprint template can be compared against a probe feature set based on their cylinder set representations. Therefore, we restate the comparison process given in (Cappelli et al., 2010).

Definition 5 (Conditional Contribution)**.** Let $\mathbf{c}_a$ and $\mathbf{c}_b$ be cylinders corresponding to minutia a in a reference template and minutia b in a probe template. Then, $\mathbf{c}_{a|b} = \mathbf{c}_a$ where $\mathbf{c}_b \neq 0$. In other words, $\mathbf{c}_{a|b}$ contains all contributions from $\mathbf{c}_a$ where $\mathbf{c}_b$ has contribution from corresponding cells.

Definition 6 (Candidate Pair)**.** Two cylinders represented by $\mathbf{c}_a$ and $\mathbf{c}_b$ are considered a *candidate pair* if and only if they satisfy the following requirements:

1. The directional difference between the two minutiae a and b is not greater than $\frac{\pi}{2}$.
2. At least 60% of corresponding elements in the two vectors $\mathbf{c}_a$ and $\mathbf{c}_b$ are non-zero.
3. $\|\mathbf{c}_{a|b}\| + \|\mathbf{c}_{b|a}\| \neq 0$.

Intuitively, it can be seen that these conditions enable to filter out the most relevant pairings of cylinders. Firstly, the orientation of the minutiae should be reasonably close in order to be considered as a mated comparison trial. Secondly, there is a significant overlap in the contribution scores associated with each minutia cylinder, and thirdly, the contributions in said overlap should occur at similar indices, indicating that the spacial relationships to neighbour minutiae are similar. Based on valid pairings of cylinders according to these criteria, the overall similarity between two cylinders is given by the following definition.

Definition 7 (Cylinder similarity)**.** The cylinder similarity between two cylinders represented by their vectors $\mathbf{c}_a$ and $\mathbf{c}_b$ is given as

$$\gamma(a,b) = \begin{cases} 1 - \frac{\|\mathbf{c}_{a|b} - \mathbf{c}_{b|a}\|}{\|\mathbf{c}_{a|b}\| + \|\mathbf{c}_{b|a}\|}, & \text{if } \mathbf{c}_a \text{ and } \mathbf{c}_b \text{ are } \textit{candidate pairs}. \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

The cylinder similarity allows to calculate local similarity scores for each minutia pair. From those local scores, a global similarity score indicating the similarity between two fingerprints can be calculated. The authors of (Cappelli et al., 2010) propose four different strategies for global score consolidation. In our work, *Local Similarity Sort* (LSS) is applied, where the top k cylinder similarity scores are averaged to produce the global similarity score.

3.1.2 Fully Homomorphic Encryption

Fully Homomorphic Encryption (FHE) schemes allow for additions and multiplications of ciphertexts that correspond directly to operations on the corresponding plaintexts (Rivest et al., 1978). More formally, a cryptographic scheme is *homomorphic* if

$$Enc_{pk}(a * b) = Enc_{pk}(a) * Enc_{pk}(b) \tag{2}$$

for an operation $*$. In partially homomorphic encryption schemes, this property is limited to either addition or multiplication. In comparison, FHE schemes allow for a combination of additions and multiplications, making them applicable to a wider variety of use cases.

The public-key encryption scheme used in this work is the Cheon-Kim-Kim-Song (CKKS) (Cheon et al., 2017). Historically, FHE schemes have first been proposed for integer or binary input data. Only more recently, (Cheon et al., 2017) have proposed a scheme that operated on floating point numbers directly, eliminating the need for input quantisation or significant rounding. While the scheme does come with an approximation error, its order of mangnitude is not significant to the application in our work.

Similarly to other FHE schemes, the security of CKKS based on the hardness of the Ring-Learning with Errors (R-LWE) problem (Lyubashevsky et al., 2010). Encryption within such schemes is a probabilistic operation, meaning that every encryption uses fresh randomness. In addition, encryption in CKKS is indistinguishable under chosen-plaintext attacks (IND-CPA), such that an attacker cannot distiguish between an encryption of 0 and an encryption of 1. In particular, an attacker cannot distinguish between two encryptions of the same input, e.g., the biometric template of a specific data subject, and an encryption of a different input, e.g. the biometric template of a different subject. For more details, we refer the reader to the original scheme (Cheon et al., 2017).

3.2 Baseline System

The baseline system operates in verification mode on unprotected data without encryption. During enrolment, the reference subjects' fingerprint samples are captured and features are extracted as ISO/IEC 19794-2 (ISO/IEC JTC1 SC37 Biometrics, 2011) fingerprint templates. From the templates, the MCC cylinder sets are constructed as described above, and stored in the reference database. For a verification transaction, a probe subject's features are extracted in the same manner and represented as a cylinder set. Then, the probe cylinder set is compared against the reference cylinder set corresponding to the claimed identitiy of the probe subject. The comparison outcome is the global similarity score of the two cylinder sets, which is compared against the pre-defined decision threshold to yield the comparison trial outcome.

3.3 Protected System

The protected system builds on the baseline system, but with the addition of FHE. The reference templates are stored in ciphertext form, and the probe features are encrypted before comparison. Through the homomorphic properties of the FHE scheme, the comparison algorithm can be computed on the encrypted data, ensuring privacy protection of the underlying data.

We work in an established client-server architecture with a computation server (CS) controlling the database of encrypted reference templates and an authentication server (AS) controlling the secret key for decryption in a semi-honest adversary model (Yasuda et al., 2013). Figure 1 shows the workflow of the protected system.

In the first step, the client captures a fingerprint sample and generates a cylinder set from it. For each minutia point m, it constructs the encrypted cylinder as a tuple of three CKKS ciphertexts $[Enc_{pk}(\theta_m), Enc_{pk}(\mathbf{c}_m), Enc_{pk}(\mathbf{c}_m^{\text{val}})]$ using coefficient packing. The first ciphertext is the encrypted cylinder angle θ_m, which inherits the minutia angle. The second ciphertext is an encryption of the contribution vector $\mathbf{c}_m$, while the third ciphertext stores the vector $\mathbf{c}_m^{\text{val}}$, which represents the validity of each cell related to minutia m. Even though cylinders are encrypted individually, they cannot be utilised for hill-climbing attacks due to the chosen plaintext security of the encryption scheme. In other words, the separate encryption of multiple cylinders does not lower the privacy protection compared to an encryption of the entire set of cylinders.

For CS to execute the comparison between all probe and reference cylinders, it first determines pairs of cylinders that can be considered *candidate pairs*. Following Definition 6, the first condition requires the directional difference between two cylinders to be lower than $\frac{\pi}{2}$. This is evaluated in the encrypted domain by subtracting the two encrypted minutia angles $Enc_{pk}(\theta_a) - Enc_{pk}(\theta_b) = Enc_{pk}(\theta_a - \theta_b)$. The resulting difference is decrypted at AS and compared against $\frac{\pi}{2}$ by CS. The comparison is computed in plaintext, as evaluating encrypted conditional statements is complex (Iliashenko and Zucca, 2021). However, the difference between two angles does not reveal the orientation of the original minutiae, and therefore, does not leak critical information.

For the second condition, CS verifies that over 60% of the corresponding elements in $\mathbf{c}_a$ and $\mathbf{c}_b$ are non-zero by calculating a common validity vector as the a homomorphic multiplication of two encrypted validity vectors $Enc_{pk}(\mathbf{c}_a^{\text{val}})$ and $Enc_{pk}(\mathbf{c}_b^{\text{val}})$. The number of elements in the resulting packed vector can be obtained by applying the rotation technique first introduced in (Boddeti, 2018). The resulting value is decrypted in order to evaluate the condition. If the amount of non-zero elements in the two vectors is below 60% of the total amount of elements, the cylinders are not *candidate pairs* and are not considered

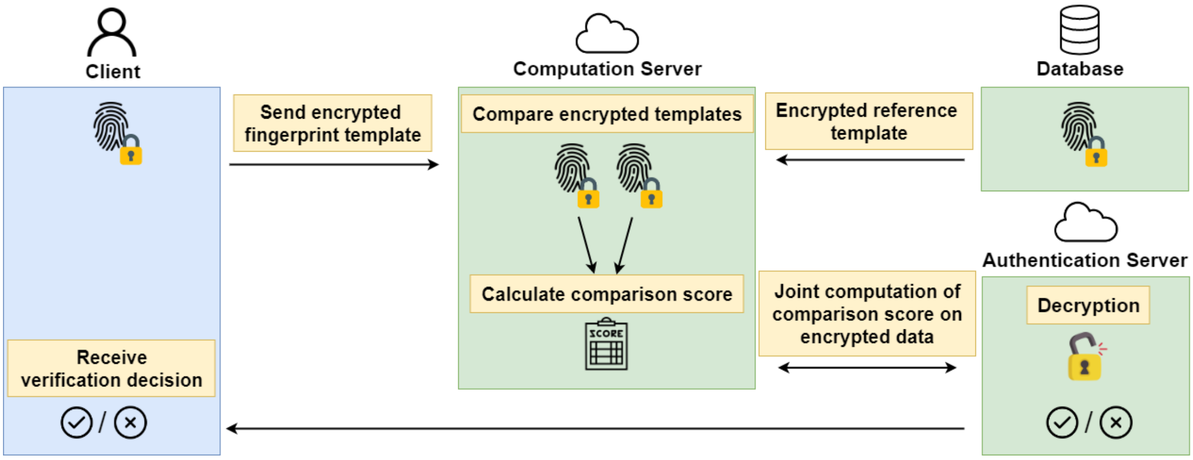
Client
Send encrypted fingerprint template
Computation Server
Compare encrypted templates
Encrypted reference template
Database
Authentication Server
Calculate comparison score
SCORE
Joint computation of comparison score on encrypted data
Decryption
Receive verification decision
✓ / ⊗
✓ / ⊗

Figure 1: Simplified flowchart of the proposed solution.

Table 2: Homomorphic operations for the encrypted comparison of two minutia cylinders.

MCC operation	Enc	EvalAdd	EvalSub	EvalMult	EvalAtIndex(· , 1)	Dec
Cylinder encryption	3	—	—	—	—	—
Directional difference	—	—	1	—	—	1
Common validity	—	$n-1$	1	2	$n-1$	1
Denominator	—	$2(n-1)$	2	2	$2(n-1)$	2
Numerator	—	$n-1$	2	1	$n-1$	1
Total	3	$4(n-1)$	6	5	$4(n-1)$	5

further.

The third step is calculating the vectors $Enc_{pk}(\mathbf{c}_{a|b})$ and $Enc_{pk}(\mathbf{c}_{b|a})$ and their norms. For this step, CS multiplies $Enc_{pk}(\mathbf{c}_a)$ and $Enc_{pk}(\mathbf{c}_b)$ with the common validity vector homomorphically, which filters out contributions of cells that should not be taken into account for the cylinder similarity score. The Euclidean norm of the resulting vectors $Enc_{pk}(\mathbf{c}_{a|b})$ and $Enc_{pk}(\mathbf{c}_{b|a})$ can then again be evaluated as above. Then, AS decrypts $Enc_{pk}(||\mathbf{c}_{a|b}||)$ and $Enc_{pk}(||\mathbf{c}_{b|a}||)$ and CS checks that $||\mathbf{c}_{a|b}|| + ||\mathbf{c}_{b|a}|| \neq 0$.

For the cylinder pairings that can be considered *candidate pairs*, the final cylinder similarity score is given in Definition 7. The denominator has already been calculated in the previous step, while the numerator is calculated by performing one homomorphic subtraction of $Enc_{pk}(\mathbf{c}_{a|b}) - Enc_{pk}(\mathbf{c}_{b|a}) = Enc_{pk}(\mathbf{c}_{a|b} - \mathbf{c}_{b|a})$, and evaluating the Euclidean norm $||Enc_{pk}(\mathbf{c}_{a|b} - \mathbf{c}_{b|a})||$ of the result as before. The remaining parts of the cylinder similarity $\gamma(a,b)$ are calculated in plaintext, and the method is repeated $m_1 \cdot m_2$ times for m_1 cylinders in the probe and m_2 cylinders in the reference template. The global comparison score is consolidated using local similarity sort (Cappelli et al., 2010) and is compared against a threshold that determines whether to accept or reject the verification attempt.

An overview of the workload of homomorphic operations is summarized in Table 2. Note that the computation of one Euclidean norm requires one homomorphic subtraction and multiplication as well as $n-1$ additions and rotations by one position (Boddeti, 2018), where $n = 1536$ is the fixed number of cells in each cylinder. We account for the encryption of the reference template during enrolment, such that only the encryption of the probe template remains. To complement Table 2, Table 3 gives the relative cost of the FHE operations.

4 EXPERIMENTAL EVALUATION

In this Section, we give an experimental evaluation of our proposed system as well as a security analysis according to ISO/IEC 24745 (ISO/IEC JTC1 SC27 Security Techniques, 2022). Further, we compare the performance of our system against the state of the art.

Table 3: Relative cost of CKKS (Cheon et al., 2017) operations implemented in PALISADE (Rohloff et al., 2017).

Operation on encrypted data	**Add**	**Subtract**	**Rotate**	**Decrypt**	**Multiply**	**Encrypt**
Relative cost	1	5	24	33	46	52

4.1 Performance

The experiments have been conducted on an Ubuntu server version 1.13.0-1ubuntu1.1 with 4GHz CPU and 128GB RAM. The proposed system has been evaluated on the publicly available MCYT database (Ortega-Garcia et al., 2003) containing fingerprint images of 330 subjects with 12 samples of each finger per subject. For feature extraction of the ISO/IEC 19794-2 (ISO/IEC JTC1 SC37 Biometrics, 2011) minutiae templates, the SourceAFIS (Važan, 2021) implementation was used. The MCC (Cappelli et al., 2010) algorithm was implemented in C++ based on the original paper without any further optimisations or simplifications. For the implementation of the FHE scheme, the PALISADE library (Rohloff et al., 2017) providing the CKKS (Cheon et al., 2017) encryption scheme was used.

The recognition accuracy of our implementation for the baseline system and the protected system is shown in Figure 2. The biometric performance of the protected system is not impacted through the application of FHE, as all computations are carried out in the same manner as in the baseline system, with the difference being the computation of ciphertexts on contrast to the unencrypted datain the baseline system. As the FHE scheme is able to operate on floating point numbers, no simplification or quantisation was need for our approach. This stands in contrast to other schemes (Kim et al., 2020; Gomez-Barrero et al., 2017a), where accuracy loss has to be accepted in order to accommodate the chosen encryption scheme.

Note that the contribution of our work is independent of the biometric performance of the baseline system, which could vary depending on the database used. Instead, the contribution of our proposed system lies in the unimpaired accuracy after the application of BIP, as CKKS is currently the only FHE scheme known to operate on floating point numbers directly (Cheon et al., 2017).

Transaction times for the proposed system are presented in Table 4. Note that transaction times for the baseline system can be considered negligent in comparison, as they are lower than 50ms throughout all system components on comparable hardware (Cappelli et al., 2010). For the computational performance of the protected system, the relevant metric is the number of cylinders that need to be compared, which corresponds to the number of minutiae in the probe and reference template. In the evaluated database, the median number of minutiae per template was 35, with the lowest number of 6 and highest of 100 minutiae, both of which can be traced back to poor sample quality. The average number of cylinder comparisons for one verification can therefore be extrapolated as $35 \cdot 35 = 1225$.

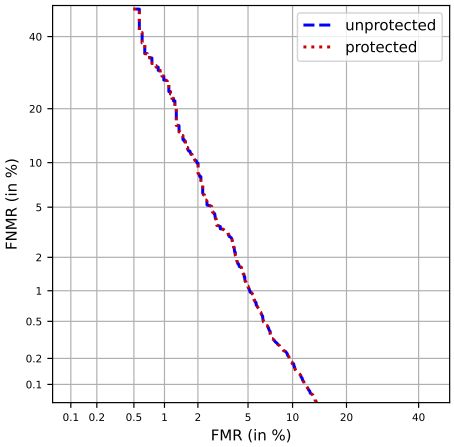

Figure 2: Detection error trade-off curve for the evaluated MCYT (Ortega-Garcia et al., 2003) database.

Table 4: Transaction times for the proposed system in seconds.

Step	**Cylinder**	**Template**
Key generation	—	0.08
Enrolment	—	0.53
Verification		
Probe encryption	—	0.53
Direct. diff.	0.004	4.13
Common validity	0.017	25.12
Nom. + Denom.	3.80	11410.38
Total	—	11525.03

Evidently, the obtained execution times show that the system is not practical in real-life applications, with a verification transaction taking approximately 192 minutes. The main bottleneck is the computation of the Euclidean norms. This has already been recognised as a challenge in biometric systems (Bauspieß et al., 2022). Within the calculation of the norms, the most costly operation is the rotation of ciphertexts, as can be derived from Table 3.

4.2 Security Analysis

We evaluate the protected system with respect to the requirements defined in ISO/IEC 24745 (ISO/IEC JTC1 SC27 Security Techniques, 2022). Firstly, unlinkability in the protected system is given through the chosen-plaintext security of the applied CKKS scheme. By the fresh random component generated for every encryption operation, even two ciphertexts computed from the exact same template look indistinguishable from a random input to an attacker. Therefore, it is not possible for an attacker to link ciphertexts corresponding to a certain data subjects to any other ciphertext within our proposed system, or any other BIP system the subject is enrolled in.

Similarly, the CKKS scheme yields renewability, as a template from the same instance can be re-encrypted and still be used securely in the system. In case the template is no longer available in plaintext form, or decryption is not possible for security reasons, an encryption of 0 can be homomorphically added to the previously stored reference to ensure a newly randomized representation of the ciphertext (Bassit et al., 2021).

Finally, irreversibility of the protected templates is guaranteed through the hardness of the Ring-LWE problem, which the security of the CKKS scheme builds upon. Notably, this assumption only holds true for correct parameter choices (Albrecht et al., 2018), which are enforced within the PALISADE library (Rohloff et al., 2017).

5 CONCLUSION

Recent standards have placed emphasis on the long-term protection of biometric data. Therefore, this work has evaluated the application of post-quantum secure FHE on minutiae-based fingerprint comparison. The challenge of minutiae-based comparison lies in the variable length of the templates, absence of an inherent order, and thereby more complex comparison which requires conditional statements before a global comparison score can be obtained. In a case study and experimental evaluation, it has been shown that it is not yet practical to evaluate such algorithms using FHE. The computational overhead of FHE is expected to decrease with further research in cryptography, while at the same time more efficient representations of biometric data need to be found that do not impair the recognition accuracy. In this regard, recent works based on deep neural networks have reported significant improvements for fixed-length fingerprint representation (Engelsma et al., 2019). Until efficient post-quantum protection for high-accuracy fingerprint representations has been developed, classically secure HE or post-quantum secure MPC should be considered.

Acknowledgements

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

Albrecht, M. R., Chase, M., Chen, H., Ding, J., Goldwasser, S., et al. (2018). Homomorphic encryption standard. Technical report, HomomorphicEncryption.org, Toronto, Canada.

Barni, M., Bianchi, T., Catalano, D., Di Raimondo, M., Labati, R., et al. (2010). A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In *IEEE Intl. Conf. on Biometrics: Theory Applications and Systems (BTAS)*, pages 1–7. IEEE.

Bassit, A., Hahn, F., Peeters, J., Kevenaar, T., Veldhuis, R., and Peter, A. (2021). Fast and accurate likelihood ratio-based biometric verification secure against malicious adversaries. *IEEE transactions on information forensics and security*, 16:5045–5060.

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

Boddeti, V. N. (2018). Secure face matching using fully homomorphic encryption. In *Intl. Conf. on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–10. IEEE.

Büscher, N., Demmler, D., Karvelas, N. P., Katzenbeisser, S., Krämer, J., et al. (2020). Secure two-party computation in a quantum world. In *Intl. Conf. on Applied Cryptography and Network Security*, pages 461–480. Springer.

Cappelli, R., Ferrara, M., and Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Trans. on Pattern Analysis and Machine Intelligence*.

Cheon, J. H., Kim, A., Kim, M., and Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In *Intl. Conf. on the Theory and Application of Cryptology and Information Security*, pages 409–437. Springer.

Chillotti, I., Gama, N., Georgieva, M., and Izabachène, M. (2020). TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34–91.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. on Information Theory*, 31(4):469–472.

Engelsma, J. J., Cao, K., and Jain, A. K. (2019). Learning a fixed-length fingerprint representation. *IEEE Trans. on Pattern Analysis and Machine Intelligence (TPAMI)*, 43(6):1981–1997.

EU Parliament (2016). *EU Quantum Manifesto: A New Era of Technology*.

European Data Protection Supervisor (2018). *Report on logging to the SIS II at national level*.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178.

Gilkalaye, B. P. and Derakhshani, R. (2021). Secure authentication using a garbled circuit variant for arithmetic circuits. In *IEEE Intl. Symposium on Technologies for Homeland Security (HST)*, pages 1–7. IEEE.

Gomez-Barrero, M., Galbally, J., Morales, A., and Fierrez, J. (2017a). Privacy-preserving comparison of variable-length data with application to biometric template protection. *IEEE Access*, 5(1):8606–8619.

Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., and Fierrez, J. (2017b). Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 67:149–163.

Iliashenko, I. and Zucca, V. (2021). Faster homomorphic comparison operations for BGV and BFV. *Proc. on Privacy Enhancing Technologies*, 2021(3):246–264.

ISO/IEC JTC1 SC27 Security Techniques (2022). *ISO/IEC 24745:2022. Information Technology - Security Techniques - Biometric Information Protection*. International Organization for Standardization.

ISO/IEC JTC1 SC37 Biometrics (2011). *ISO/IEC 19794-2:2011 Information Technology - Biometric Data Interchange Formats - Part 2: Finger Minutiae Data*. International Organization for Standardization.

Jain, A., Prabhakar, S., Hong, L., and Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE Trans. on Image Processing*, 9(5):846–859.

Kessler, R., Henninger, O., and Busch, C. (2021). Fingerprints, forever young? In *Proc. Intl. Conf. on Pattern Recognition (ICPR)*, pages 8647–8654.

Kim, T., Oh, Y., and Kim, H. (2020). Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption. *Security and Communication Networks*, 2020.

Kolberg, J., Bauspieß, P., Gomez-Barrero, M., Rathgeb, C., Dürmuth, M., and Busch, C. (2019). Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification. In *IEEE Workshop on Information Forensics and Security (WIFS)*, pages 1–6.

Kolberg, J., Drozdowski, P., Gomez-Barrero, M., Rathgeb, C., and Busch, C. (2020). Efficiency analysis of post-quantum-secure face template protection schemes based on homomorphic encryption. In *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*, pages 175–182. Gesellschaft für Informatik e.V.

Liu, E. and Zhao, Q. (2017). Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with l1 minimization. *Neurocomputing*, 259:3–13.

Lyubashevsky, V., Peikert, C., and Regev, O. (2010). On ideal lattices and learning with errors over rings. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 1–23. Springer.

Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J.-J., Vivaracho, C., et al. (2003). MCYT baseline corpus: a bimodal biometric database. *IEE Proceedings-Vision, Image and Signal Processing*, 150(6):395–401.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Intl. Conf. on the Theory and Applications of Cryptographic Techniques*, pages 223–238. Springer.

Rahman, M. M., Mishu, T. I., and Bhuiyan, M. A. A. (2022). Performance analysis of a parameterized minutiae-based approach for securing fingerprint templates in biometric authentication systems. *Journal of Information Security and Applications*, 67:103209.

Rivest, R. L., Adleman, L., Dertouzos, M. L., et al. (1978). On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180.

Rohloff, K., Cousins, D., and Polyakov, Y. (2017). *The PALISADE Lattice Cryptography Library*. `https://git.njit.edu/palisade/PALISADE`.

Važan, R. (2021). Sourceafis fingerprint matcher v3.13.0. `https://sourceafis.machinezoo.com/`, accessed 2022-01-18.

Yang, W., Wang, S., Yu, K., Kang, J. J., and Johnstone, M. N. (2020). Secure fingerprint authentication with homomorphic encryption. In *Digital Image Computing: Techniques and Applications (DICTA)*, pages 1–6. IEEE.

Yao, A. (1986). How to generate and exchange secrets. In *Annual Symposium on Foundations of Computer Science (SFCS)*, pages 162–167. IEEE.

Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., and Koshiba, T. (2013). Packed homomorphic encryption based on ideal lattices and its application to biometrics. In *Intl. Conf. on Availability, Reliability, and Security*, pages 55–74. Springer.

Zhang, Y. and Koushanfar, F. (2016). Robust privacy-preserving fingerprint authentication. In *IEEE Intl. Symposium on Hardware Oriented Security and Trust (HOST)*, pages 1–6. IEEE.