IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 6, 2018, accepted January 28, 2019, date of publication February 14, 2019, date of current version March 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2899359

High-Secure Fingerprint Authentication System Using Ring-LWE Cryptography

TUY NGUYEN TAN, (Student Member, IEEE), AND HANHO LEE, (Senior Member, IEEE)
Department of Information and Communication Engineering, Inha University, Incheon 22212, South Korea

Corresponding author: Hanho Lee (hhlee@inha.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Fund funded by the Ministry of Science, ICT, South Korea, under Grant 2016R1A2B4015421.

ABSTRACT This paper presents a high-secure fingerprint authentication system using ring learning with errors (ring-LWE) cryptography to protect users' fingerprint data more securely. A delay-optimized high-accuracy scheme for a fingerprint-features extraction approach is proposed to collect necessary features' information from fingerprint images. In addition, a ring-LWE cryptography scheme using low-latency number theoretic transform (NTT) polynomial multiplications is deployed to speed up the ring-LWE encryption and decryption times. As a result, the processing time of the fingerprint authentication system is significantly reduced, and the fingerprint data are effectively protected. The simulation results show that the proposed NTT multiplication-based ring-LWE cryptography scheme for fingerprint features outperforms the existing works up to 46% and 44% in terms of encryption time and decryption time, respectively. The latency of the whole fingerprint authentication system is less than 160 ms, which makes it suitable for practical applications. Furthermore, performance analysis on entropy and similarity of the encrypted fingerprint features proves the domination of the proposed system compared with the previous systems in terms of confidentiality.

INDEX TERMS Authentication, cryptography, encryption, fingerprint features, post-quantum, ring-LWE.

I. INTRODUCTION

Fingerprint authentication is one of the most reliable and mature biometric recognition techniques owing to the distinctiveness and stability that fingerprints can provide compared to other biometrics [1]. In cases of security checks, medical jurisprudence or disasters, fingerprint information stored in a database is often used to confirm individual identity. Two categories of fingerprint authentication methods exist, namely, texture-based methods and minutiae-based methods. The latter is more reliable and popular [2]. Minutiae-based algorithms represent a fingerprint image with a set of labeled minutiae referring to ridge ending and bifurcation. Fingerprint matching with the minutiae-based algorithm can be considered point pattern matching [3]. The detailed operations of fingerprint matching by minutiae can be found in [4].

Consider a typical fingerprint authentication system consisting of n local stations that connect to a remote server, as detailed in Figure 1. Users' fingerprints are initially collected by local sensing devices before being sent to a remote server database. The information sent from local stations to the remote server can be full fingerprint images or limited to fingerprint features. Generally, individual identification information (like fingerprint images or fingerprint features) sent over a network without any security solution is accessible to attackers and thus at risk. Therefore, Li and Kot [5] present a method to combine various fingerprints into a new identity before sending data to the server. The minutiae positions from one fingerprint, the orientation from another fingerprint, and the reference points from both fingerprints are extracted. However, there are concomitant risks associated with this method of storing and transmitting fingerprint data. If attackers distinguish a combined minutiae template from the original minutiae templates, they can recover the original fingerprint. Therefore, integrating a highly secure solution into the fingerprint authentication system to protect personal information during authentication, storage, and transmission is a necessity. Cryptosystems, in which only authorized users with a right key can access the hidden information, offer a potential solution that can be integrated into

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

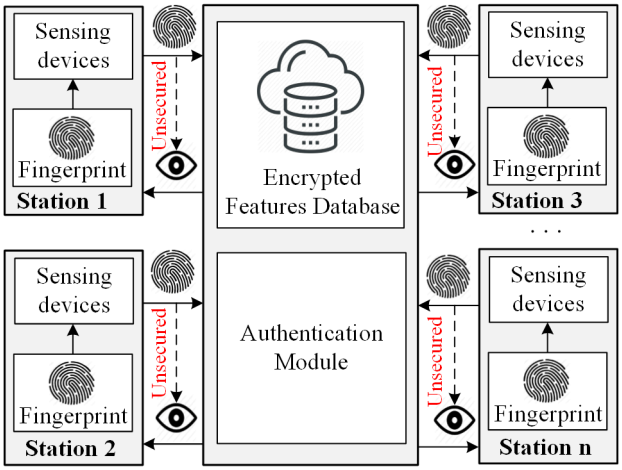

FIGURE 1. A typical fingerprint authentication system.

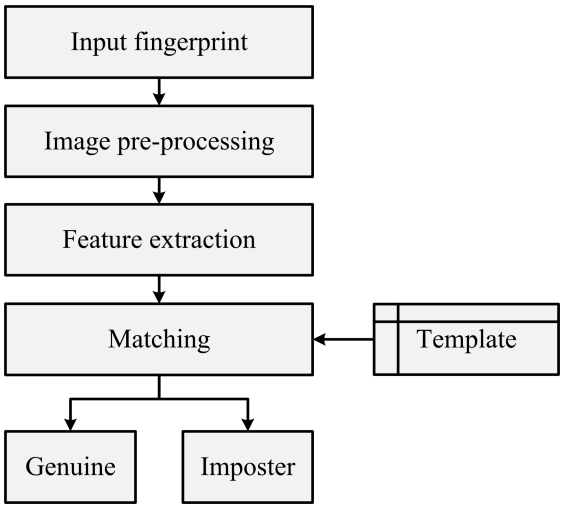

FIGURE 2. Flowchart of a fingerprint recognition system.

biometric authentication systems to provide a higher level of security.

Two types of cryptography are symmetric cryptography and asymmetric cryptography [6]–[8]. The former uses the same key for encryption and decryption operations, whereas the latter uses two separate keys called the public key and the private key for encryption and decryption. Popular asymmetric cryptography schemes include Rivest, Shamir, and Adleman (RSA) [9], and elliptic curve cryptography (ECC) [10], [11]. The encryption and decryption operations in ECC are based on an elliptic curve and arithmetic operations over Galois-field GF(p) or GF(2^m), where p and m are prime numbers. In the key generation operation, the receiver selects a random number for its private key k_S and a base point P_S to calculates the ECC point multiplication $Q_S = k_S \cdot P_S$ [12], [13]. The sender uses the public key of the receiver to encrypt input data before sending it to the receiver. At the receiver, the original data can be recovered using its secret key and ECC point multiplication operations. Although ECC uses a significantly smaller key length to offer a similar security level to traditional systems, such as RSA [12], it can be solved in polynomial time by a quantum computer. With the rapid improvements in cryptanalysis and the unpredictable development of the quantum computer, post-quantum security and practical alternatives for the future are needed [14]. Ring-learning with errors (ring-LWE) cryptography that based on the worst-case hardness of well-known lattice problems [15], [16], is considered as a great candidate for replacing these conventional cryptosystems because there is no known quantum computer that can efficiently solve the lattice problem.

In this work, a fingerprint authentication system using ring-LWE cryptography, the post-quantum cryptosystem, is introduced. To the best of our knowledge, this is the first work designing a fingerprint authentication system using the ring-LWE cryptography scheme. By applying novel fingerprint-feature extraction and NTT polynomial multiplication in the proposed ring-LWE cryptography-based fingerprint authentication system, the total processing time of the proposed system is much faster than other systems. Additionally, the encrypted data generated by the proposed system is more secure than the obtained results from existing schemes. Our main contributions are as follows:

1) We present a novel NTT polynomial multiplication scheme by removing bit-reverse operations in conventional NTT multiplication to speed up the polynomial multiplication time over ring operation;
2) We propose an optimal scheme for fingerprint-features extraction to reduce processing time and increase accuracy;
3) We propose and implement the ring-LWE cryptography system using the proposed NTT polynomial multiplication approach to enhance the encryption and decryption time;
4) We develop a fingerprint authentication system using our fingerprint-features extraction method and the proposed NTT multiplication-based ring-LWE cryptography scheme. The advantages of the proposed system in terms of processing time and security level can be proved by simulation results.

The rest of this paper is organized as follows: Section II provides background information about fingerprint features extraction, NTT polynomial multiplication, and ring-LWE cryptography. The proposed fingerprint authentication system using the NTT multiplication-based ring-LWE cryptography scheme is presented in Section III. Performance analysis and comparison are discussed in Section IV. Finally, conclusions are given in Section V.

II. BACKGROUND

A. FINGERPRINT RECOGNITION SYSTEM

The flowchart of a fingerprint recognition system is shown in Figure 2. Each input fingerprint sample is matched with those retrieved from the enrollment templates, to identify

whether the input fingerprint is from a person enrolled in the database (genuine) or not (imposter). As shown in Figure 2, the algorithm contains three main modules: image pre-processing, features extraction, and matching. Bozorth3 [17], an open source code, developed by the National Institute of Standards and Technology (NIST), is used to extract the minutiae features and perform matching. The module includes several processes such as segmentation, enhancement, singular point and minutiae extraction, and orientation field estimation. In this work, information on both minutiae points and singular points are requirements of the matching process. The matching module conducts nearest-neighbor-based matching, which uses the local structures formed by central minutia, and several of its nearest neighbor minutiae, to define the similarity.

B. RING-LWE CRYPTOGRAPHY

In ring-LWE problems, polynomials $a(x)$ and $s(x)$ are selected uniformly from a ring, $R_q = \mathbb{Z}_q[x]/f(x)$, where $f(x)$ is an irreducible polynomial of degree n [16]. Error polynomials $e_i(x)$ of degree n are sampled from error distribution χ, which is usually a discrete Gaussian distribution, χ_σ, with standard deviation σ. The ring-LWE distribution over $R_q \times R_q$ consists of tuples (a, t), where $t = a \times s + e$. It is very difficult to find s from a given polynomial number of sample pairs (a, t) from A_s, χ. Ring-LWE cryptography operations can be described as follows:

- *Key generation*: Generate the private key r_2 and the public key (a, p). The value of p is obtained from the computation:

$$p \leftarrow r_1 - a \times r_2 \tag{1}$$

- *Encryption*: Encrypt the input message m into the cipher-text (c_1, c_2).

$$(c_1, c_2) \leftarrow (a \times e_1 + e_2, p \times e_1 + e_3 + m_e) \tag{2}$$

  where e_1, e_2, and e_3 are error polynomials generated from Gaussian sampler, and m_e is the encoded value of the input message m.
- *Decryption*: Decrypt the cipher-text to get the original message m.

$$m_d \leftarrow c_1 \times r_2 + c_2 \tag{3}$$

The original message m is recovered from m_d by using a decoder presented by Roy *et al.* [18].

Among existing methods for sampling from a discrete Gaussian distribution, the Knuth-Yao algorithm [19], [20] is selected to generate error polynomials because this algorithm proves that the number of random bits required by the sampling algorithm is close to the entropy of the distribution and, thus, is near-optimal.

C. NUMBER THEORETIC TRANSFORM MULTIPLIER

Polynomial multiplication is the most computationally intensive operation in ring-LWE cryptography [15]. Given a_i in R_q, $i = 1, 2, \ldots, n-1$, a polynomials $a(x)$ over the ring R_q can be expressed as follows:

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \tag{4}$$

Let ω be a primitive n-th root of unity, the NTT of each coefficient of $a(x)$ is calculated as:

$$A_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \mod q \tag{5}$$

Then the inverse number theoretic transform (INTT) is defined as:

$$a_i = n^{-1} \sum_{j=0}^{n-1} A_j \omega^{-ij} \mod q \tag{6}$$

Let α and β are extended vectors of $a(x)$ and $b(x)$ by filling n zero elements. The multiplication of two polynomials $a(x)$ and $b(x)$ can be expressed in forms of NTT and INTT, where $\odot$ is the point-wise multiplication.

$$\begin{aligned} c(x) &= a(x) \cdot b(x) \\ &= INTT_\omega^{2n}(NTT_\omega^{2n}(\alpha) \odot NTT_\omega^{2n}(\alpha)) \end{aligned} \tag{7}$$

To avoid zero padding in NTT polynomial multiplication, we can use the negative wrapped convolution. Let $c = (c_0, c_1, \ldots, c_n)$ be the negative convolution of a and b, the negative wrapped convolution is computed as:

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} - \sum_{j=i+1}^{n-1} a_j b_{n+i-j} \tag{8}$$

Define $a' = (a_0, \psi a_1, \ldots, \psi a_{n-1})$, $b' = (b_0, \psi b_1, \ldots, \psi b_{n-1})$, and $c' = (c_0, \psi c_1, \ldots, \psi c_{n-1})$, where $\psi \equiv \omega \bmod q$, the NTT polynomial multiplication becomes:

$$c' = a' \cdot b' = INTT_\omega^n(NTT_\omega^n(a') \odot NTT_\omega^n(b')) \tag{9}$$

By using the negative wrapped convolution, the NTT multiplication can be calculated using only n-coefficient.

The general NTT-based polynomial multiplication and the data flow of the Cooley-Turkey algorithm [21] for NTT-based polynomial multiplication are shown in Figure 3.

III. PROPOSED FINGERPRINT AUTHENTICATION SYSTEM USING RING-LWE CRYPTOGRAPHY

A. PROPOSED FINGERPRINT AUTHENTICATION SYSTEM

The proposed fingerprint authentication system is described in Figure 4. This system consists of n local stations that equipped with fingerprint sensing devices, and integrated fingerprint-features extraction and ring-LWE encryption functions. The remote server consists of a database and installed ring-LWE decryption function to decrypt the messages received from stations. There are three main phases of operation in the proposed system. The first phase is called the registration phase. Users who want to authenticate with the system must initially register their fingerprint data at a corresponding local station. Data collected from station-deployed

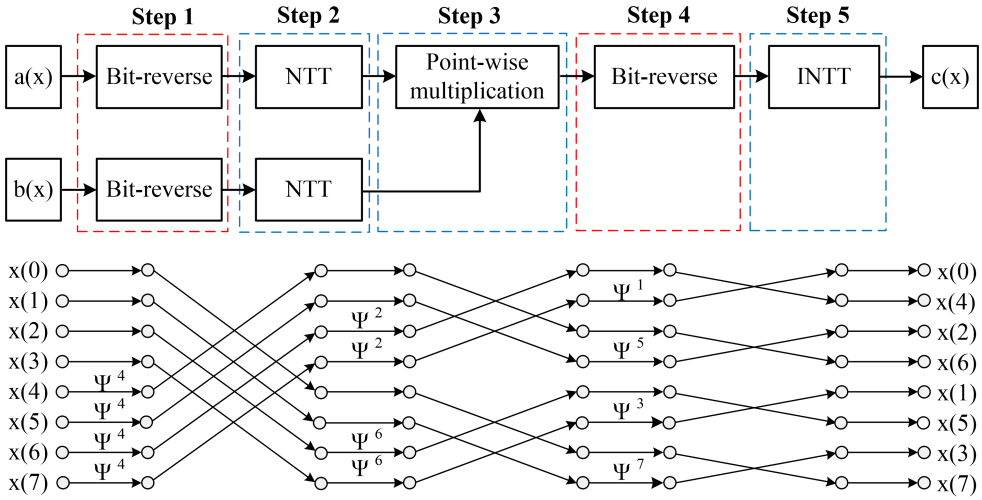

FIGURE 3. Block diagram of typical NTT polynomial multiplication and data flow of 8-point cooley-tukey algorithm.

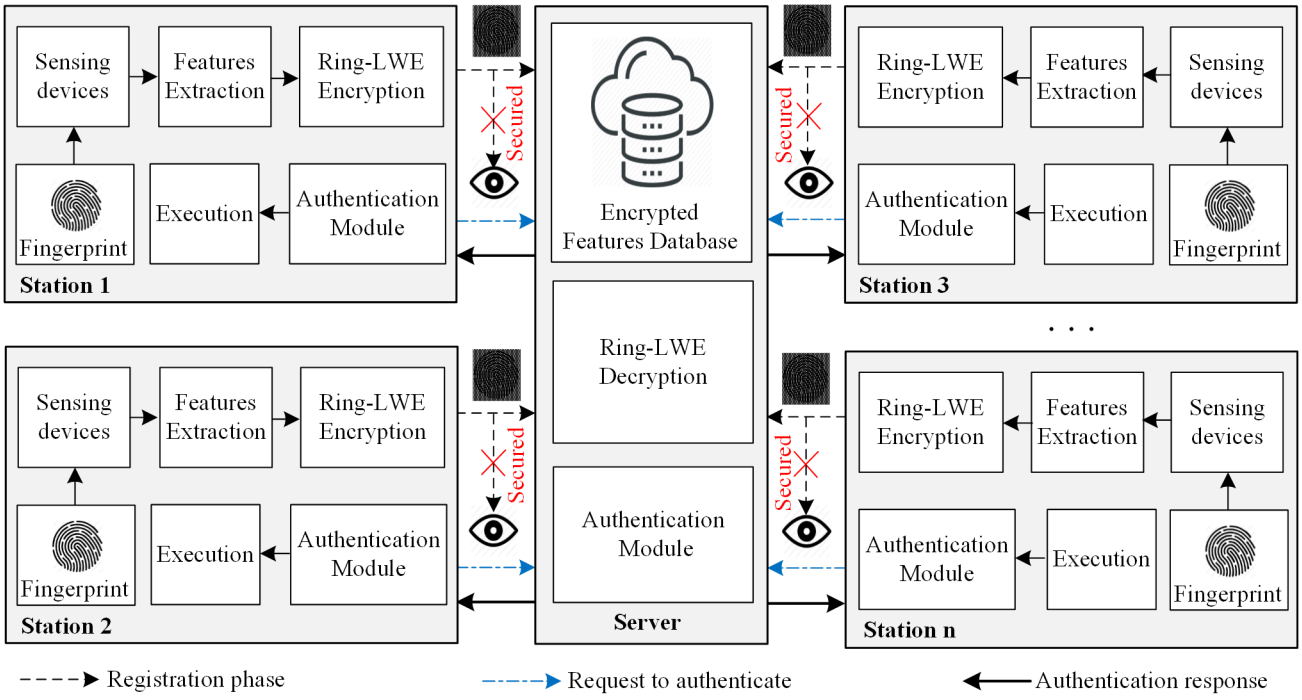

FIGURE 4. Block diagram of the proposed fingerprint authentication system using NTT multiplication-based ring-LWE cryptography.

sensing devices are then extracted to get the necessary features using the proposed fingerprint extraction scheme installed at local stations. These features are encrypted using the proposed NTT multiplication-based ring-LWE encryption scheme to get the encrypted data. The authentication module at each station sends users encrypted features to the server where each users' data are stored in the encrypted features database.

In the second phase, once a user needs to perform a fingerprint authentication with the system, a station collects the users' encrypted data and sends it to the server with a Request-To-Authenticate (RTA) message. Upon receiving an RTA message from a user, the server performs decryption of the message using the proposed ring-LWE decryption scheme and compares results with the registered data to decide whether the user has the right to access the system or not. If the RTA sent from a local station is accepted, the server sends an Accept-To-Authenticate (ATA) message in the response to the corresponding station, and allows the user to access the system; otherwise,

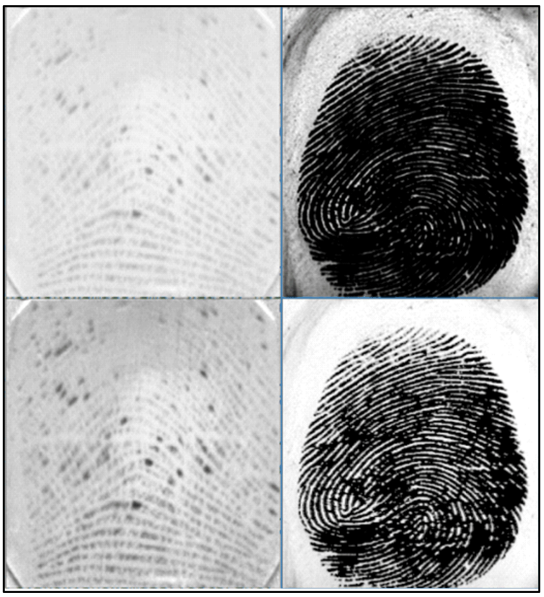

FIGURE 5. Image contrast enhancement by Gamma correction. Top row: input image; bottom row: enhanced images, column-wise, respectively.

the server sends a Reject message to deny the user access.

B. FINGERPRINT FEATURES EXTRACTION

To safeguard the performance of the system against bad quality samples, a preprocessing module is developed before applying the Bozorth3 module for feature extraction and matching. Owing to the quality of the sensor or the pressure of the users' finger on the sensor, as well as the dryness of the finger, the captured image can be very bright or dark. In these conditions, the minutiae list extracted from Bozorth3 is very noisy as it contains many spurious minutiae. In addition, many minutiae cannot be detected, resulting in bad matching. In this work, we propose the use of Gamma correction method [22] to adjust the brightness of the input image based on the state estimated adaptively from the input image. Gamma correction is defined as:

$$s = c \times r^{\gamma} \tag{10}$$

where each pixel r of the input image is transformed to the output level s by powering r to a γ (constant $c = 1$ in our work). The parameter γ is adaptively estimated from the grey-scale level of the input image by:

$$\gamma = \frac{\sum_{x=1,y=1}^{x=N,y=M} I(x,y)}{M \times N \times L/2} \tag{11}$$

where I indicates the input image of size $M \times N$; L is the grey level of I ($L = 255$ for 8-bit images). For the image of a dry finger, the intensity of the input is high so that γ is greater than 1, leading to the contrast of output image being expended in the direction of reducing the total brightness of the image. The converse is true for a fingerprint image, as illustrated in Figure 5. For normal cases, the value of γ is around 1, and therefore the input image is slightly modified.

C. PROPOSED NUMBER THEORETIC TRANSFORM MULTIPLIER

The polynomial multiplication is an arithmetic operation that requires the most computation time. To speed up the processing time and reduce the complexity of ring-LWE cryptography, a novel NTT-based polynomial multiplication is proposed. Theoretically, an NTT-based polynomial multiplication described in Figure 3 consists of five steps including the first bit-reverse process, NTT process, point-wise multiplication, the second bit-reverse process, and INTT processes. Noticeably, conventional NTT-based multiplication requires two bit-reverse operations, in step 1 and step 4, respectively, to compute polynomial multiplication. By using the Cooley-Tukey algorithm in the NTT-based polynomial multiplication operation, we can reduce two bit-reverse operations; therefore, the system computation time and complexity are remarkably decreased.

D. PROPOSED HIGH-SECURE FINGERPRINT AUTHENTICATION SYSTEM USING RING-LWE CRYPTOGRAPHY

The proposed fingerprint authentication system using ring-LWE cryptography is shown in Figure 6. In the registration phase, fingerprint collected from local sensing devices is extracted to get necessary features using the proposed fingerprint-features extraction scheme. In our scheme, we use four main features of the fingerprint, including x-coordinate, y-coordinate, ridge direction θ, and minutiae type t. These features are then encrypted by the ring-LWE encryption function. At the beginning of the encryption process, input information for each feature is encoded to get the encoded polynomial over the ring R_q. Depending on the value of i-th bit of the input features, the corresponding i-th value of the encoded polynomials can be 0 or $(q-1)/2$. In addition, a discrete Gaussian sampler generates three error polynomials $e_1(x)$, $e_2(x)$, and $e_3(x)$ in R_q that participate in the encryption and decryption processes. The next operation of the encryption process is calculating two polynomial multiplications $a(x) \times e_1(x)$ and $p(x) \times e_1(x)$ using two proposed NTT polynomial multipliers *Multiplier* 1 and *Multiplier* 2, respectively. The *Adder* 1 adds the multiplication result $a(x) \times e_1(x)$ and the error polynomial $e_2(x)$ to generate the cipher-text $c_1(x)$. Cipher-text $c_2(x)$ is calculated by the *Adder* 2 using the output from the *Multiplier* 2, the error polynomial $e_3(x)$, and the encoded message m_e. To minimize the latency of the multipliers and adders in the encryption operation, we use the parallel operations to multiply and add all array elements of two corresponding inputs of multipliers or adders. Finally, the encrypted message (c_1, c_2) is generated. This encrypted message is initially registered with the remote server and this information is stored in the server database. The registration phase is thereby completed.

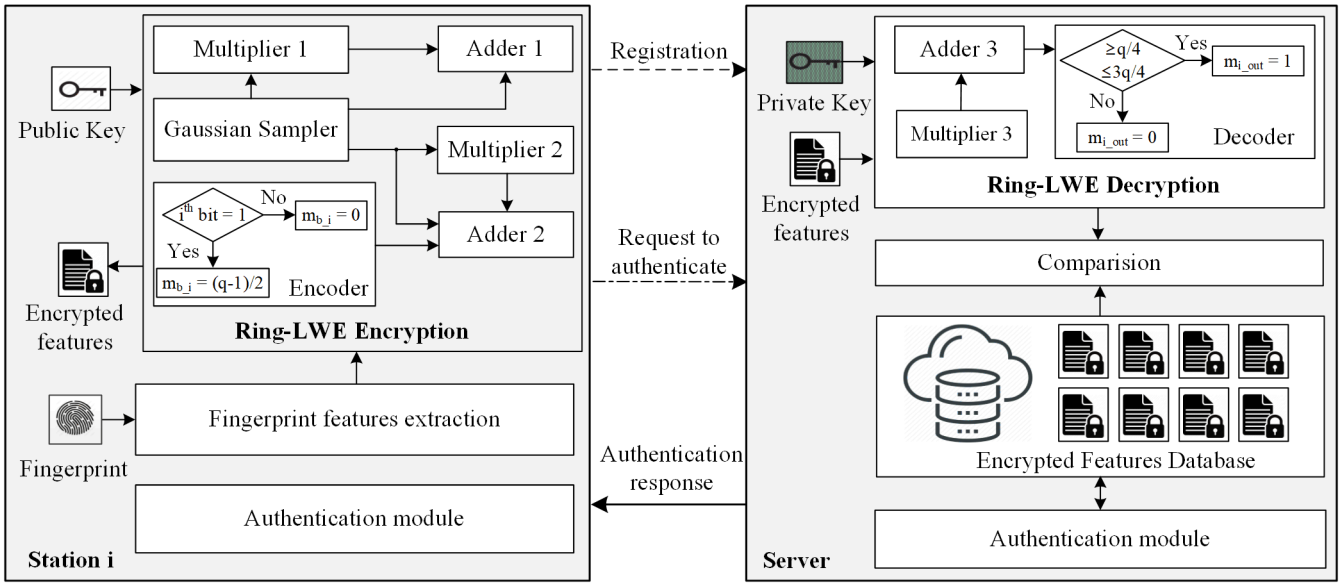

FIGURE 6. Proposed high-secure fingerprint authentication system using ring-LWE cryptography.

When a user who has already registered with the system requests to access, the users' fingerprint is encrypted using the same ring-LWE encryption scheme described in the registration phase. The encrypted fingerprint features are sent to the remote server with an RTA message. Upon receipt of the RTA message from the local station, the server runs the ring-LWE decryption function to decrypt the received message and registered message for comparison. The decoded message m_d is calculated from the private key $r_2(x)$ and encrypted information (c_1, c_2) of fingerprint features using the *Multiplier* 3 and the *Adder* 3. These values are then decoded to return the binary values of the initial image pixels. Matching and comparison are shown in Figure 7. The matching function installed at the server performs the comparison to decide if the user may access the system or not. Depending on the result from matching function, the server determines whether to send an Accept-To-Access message (ATA), or a Reject message to the correlative station.

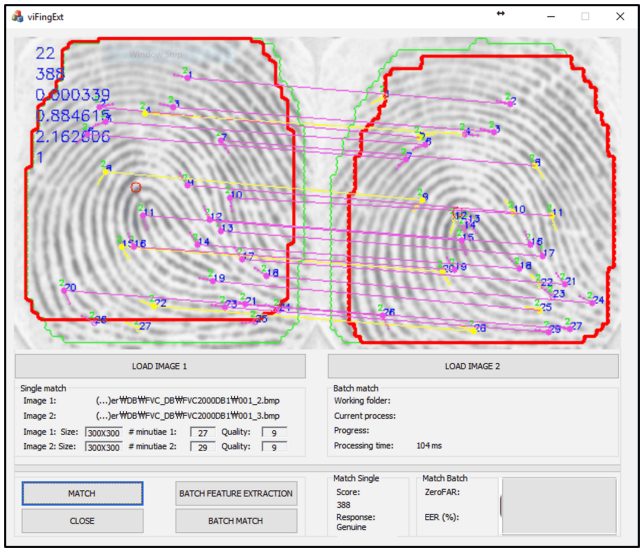

FIGURE 7. Matching and comparison at the server.

IV. PERFORMANCE ANALYSIS AND COMPARISON

A. SIMULATION ENVIRONMENT

The proposed system is evaluated using Microsoft Visual Studio 2015 and OpenCV 3.1 installed on a Dell machine (including an Intel Core i7-6700 3.40 GHz processor, 16 GB RAM, and running with Windows 10 64-bit operating system). The proposed fingerprint authentication system is tested on public databases in Fingerprint Verification Competition (FVC) including FVC2000, FVC2002, and FVC2004. There are four sub-databases in each database named DB1, DB2, DB3, and DB4. Each sub-database consists of 100 fingerprints with eight impressions of each fingerprint. The detailed database information can be referred in [23]–[25]. In this work, the experiment is carried out on DB1 and DB2 of each dataset. In addition, we implement fingerprint images encryption and decryption in software using ECC algorithm in [12] for comparison.

B. SECURITY LEVEL ANALYSIS AND COMPARISON

In the first step of evaluation, a simulation to prove that ring-LWE cryptography can achieve a higher security level than existing cryptography systems is conducted. Some important parameters are analyzed to ensure that it is difficult for strangers to recover the original image from the achieved encrypted data. To ensure confidentiality, the encrypted data should be highly uncorrelated to the original. To measure the degree of similarity between the input image and the

TABLE 1. Comparison in normalized correlation factor and entropy.

Algorithm	Correlation Factor	Entropy of original image (bits/pixel)	Entropy of encrypted image (bits/pixel)	Improvement in entropy (bits/pixel)
Kobayashi [27]	0.0242	–	7.4764	–
Algorithm I [26]	0.0081	5.8739	7.8909	2.0170
Algorithm II [26]	0.0081	5.8739	7.9969	2.1230
Proposed	0.0056	5.7274	7.9843	2.2569

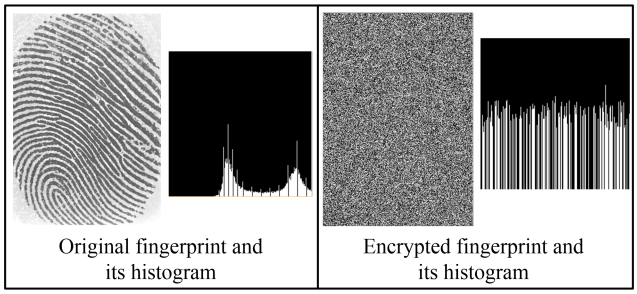

FIGURE 8. Histogram of fingerprint and its encrypted image.

encrypted image, a normalized correlation metric is used. This metric will be very close to zero if the input image and encrypted image are completely different. The comparison in correlation factors between our proposed scheme and the algorithms of Al-Haj *et al.* [26] and Kobayashi *et al.* [27] can be seen in Table 1. The proposed scheme clearly obtains approximately 30.9% lower correlation factor than Al-Haj's. Remarkably, the obtained correlation factor is about 23% of that in Kobayashi's. This proves a complete difference between the encrypted image generated by the proposed scheme and the input image.

Image histogram analysis aids in visualizing the correlation between the plain-text and cipher-text images by giving the probability of appearance for each grey level [26]. This histogram is significantly different indicates that the original image and the encrypted image have a very low correlation. As can be seen from Figure 8, the histogram of the encrypted fingerprint is much different from the original one. Furthermore, since the distribution of the appearance probabilities of the grey levels is equitable, it is extremely difficult to predict information from the encrypted image.

Entropy is a parameter to measure the uncertainty present in the encrypted image. The degree of randomness and confidentiality in the encrypted image is high when its entropy is high. Given that the maximum theoretical entropy value for a grey-scale image is eight bits per pixel [26], the entropy values of an encrypted image obtained from the proposed scheme and previous works are presented in Table 1. The entropy value of an encrypted image using the proposed scheme is close to eight bits per pixel, demonstrating the effectiveness of the proposed algorithms in hiding the details of the original biometric images. Compared to Kobayashi algorithm, the proposed scheme achieves better values for entropy. Additionally, the improvement in entropy between the encrypted image and the original image from the proposed scheme is 39.41%, which is higher than the values achieved from Algorithm I (34.34%) and Algorithm II (36.14%) in [26].

TABLE 2. EER of the proposed system over FVC databases.

Dataset	FVC2000	FVC2002	FVC2004
DB1	2.28	2.34	7.17
DB2	1.38	1.96	5.65

TABLE 3. Comparison in fingerprint encryption and decryption latency.

Algorithm	Encryption time (ms)	Decryption time (ms)
ECC[12]	220	73
Algorithm I [26]	557×10^3	591×10^3
Algorithm II [26]	331×10^3	379×10^3
Kobayashi [27]	601×10^3	620×10^3
Ring-LWE [28]	64	33
Proposed (full image)	56	29
Proposed (features only)	30	16

C. SYSTEM ACCURACY ANALYSIS AND COMPARISON

The experimental process follows the scenario designed in FVC, which includes genuine and imposter matching. Genuine matching: each impression of a finger is chosen as a template fingerprint and matched with the rest of impressions. The total number of genuine matching impression is $N \times C_m^2$, where N denotes the total number of unique fingers, and m denotes the impressions of each finger. In FVC, each sub-database includes the fingerprint of $N = 100$ individuals in $m = 8$ compression; thus, the total genuine matching number is 2,800.

Imposter matching: the first impression sample of each finger is matched with the first impression of the rest of all the other fingers. The imposter matching number is C_N^2; here, the total imposter matching number is $100 \times 99/2 = 4,950$.

Equal Error Rate (EER) is used to evaluate the matching rate, which is defined from the false acceptance rate and false rejection rate. When the rates are equal, the common

TABLE 4. Comparison in average processing time of different databases.

Dataset	Subset	Image size	Average minutiae	Average enc. time (ms)	Average dec. time (ms)	Average FX runtime (ms)
FVC2000	DB1	300×300	31.4	29	14	24
FVC2000	DB2	256×364	36.4	30	17	25
FVC2002	DB1	388×374	33.2	31	19	66
FVC2002	DB2	296×560	41.6	38	22	67
FVC2004	DB1	640×480	37.3	32	17	110
FVC2004	DB2	328×364	37.6	33	16	50

value is referred to as the EER. The EER values of the proposed system are presented in Table 2. These EER values are compared with the results of the International Competition for Fingerprint Verification Algorithms for industry products [23]–[25], including FVC2000, FVC2002, and FVC2004. Generally, the achieved EER is ranked in the top fifteen algorithms with the lowest EER in all FVCs. This allows our proposal to be turned into real industry products. Specifically, EER results of the proposed scheme on DB1 and DB2 are 54.9% and 49.8% lower than that of the CETP and CSPN algorithms, which rank third in the FVC2000 [23], respectively. For challenging images due to fingerprint conditions (too wet or too dry) in FVC2004 [25], our EER on DB1 is about 2.4% smaller than that of the algorithm ranked seventh, P071, and EER on DB2 is similar to that of ranked tenth algorithm, P016.

D. SYSTEM LATENCY EVALUATION

The encryption and decryption processing times for an eight-bit depth fingerprint image with the size of 300 × 300 pixels using different algorithms and schemes are shown in Table 3. In our work, encryption and decryption operations for both fingerprint images and fingerprint features, using NTT multiplication-based ring-LWE cryptography, are implemented for comparison. As can be seen, for the completed fingerprint encryption and decryption operation, the total processing time of the proposed ring-LWE cryptographic scheme for a full image outperforms the ECC [12] scheme by about 19%. The processing time is speeded up about 14% compared with our previous work in [28]. Encryption and decryption times are extremely short compared to the normalized values of Algorithm I, Algorithm II [26], and Kobayashi's [27]. Moreover, the encryption and decryption times for only fingerprint features are improved by about 46% compared to the correlative values of the full fingerprint images. This result can be explained that the number of fingerprint features is much smaller than the number of pixels in a full image. The proposed algorithm performs four encryption and decryption operations corresponding to four features which are mentioned in Section III-D.

The implementations of the proposed high-security fingerprint authentication system for three open datasets FVC2000, FVC2002, and FVC2004, including DB1 and DB2, are conducted to get the processing time. The simulation results are shown in Table 4. The presented data indicate the average values. Depending on the fingerprint size and its characteristics, the number of extracted features are different. The largest average number of extracted features is 41.6, obtained from the FVC2002 DB2, followed by the result obtained from the FVC2004 DB2. FVC2000 DB1 has the lowest number of average features. In addition, from Table 4, the largest value of the total processing time for the each dataset, including encryption time, decryption time, and features extraction and matching time, is smaller than 160 ms. Notably, for the subset DB1 of the dataset FVC2000, the total processing time is only 69 ms. With this low processing time, the proposed system can be applied in realistically authentication systems.

V. CONCLUSION

A novel high-security fingerprint authentication system using ring-LWE cryptography is presented in this paper. By using the novel NTT multiplication and feature extraction approach, the processing time of the proposed system is improved remarkably. Simulation results show that the proposed system achieves low processing times, and can be used in real-time authentication systems. In addition, with the high level of security offered by ring-LWE cryptography, users' personal fingerprints are completely protected. Therefore, the proposed fingerprint authentication system can be applied in systems that require a high-security level, such as biometric authentication, medical image transmission, and IoT security.

REFERENCES

[1] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1179–1192, Jul. 2017.
[2] E. Liu *et al.*, "A key binding system based on N-nearest minutiae structure of fingerprint," *Pattern Recognit. Lett.*, vol. 32, no. 5, pp. 666–675, Apr. 2011.
[3] H. Ogawa, "Labeled point pattern matching by Delaunay triangulation and maximal cliques," *Pattern Recognit.*, vol. 19, no. 1, pp. 35–40, May 1986.
[4] R. Gil *et al.*, "Fingerprint verification system in tests in moodle," *IEEE Rev. Iberoamer. Tecnol. Aprendizaje*, vol. 8, no. 1, pp. 23–30, Feb. 2013.
[5] S. Li and A. C. Kot, "Fingerprint Combination for Privacy Protection," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 350–360, Feb. 2013.
[6] M. Abdalla, F. Benhamouda, and D. Pointcheval, "Public-key encryption indistinguishable under plaintext-checkable attacks," *IET Inf. Secur.*, vol. 10, no. 6, pp. 288–303, Oct. 2016.

[7] F. Heuer, T. Jager, S. Schäge, and E. Kiltz, "Selective opening security of practical public-key encryption schemes," *IET Inf. Secur.*, vol. 10, no. 6, pp. 304–318, Oct. 2016.
[8] K. Wang, M. Wu, P. Xia, S. Xie, W. Lu, and S. Shen, "A secure authentication scheme for integration of cellular networks and MANETs," in *Proc. IEEE Int. Conf. Neural Netw. Signal Process.*, Zhenjiang, China, Jun. 2008, pp. 315–319.
[9] X. Huang and W. Wang, "A novel and efficient design for an RSA cryptosystem with a very large key size," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 62, no. 10, pp. 972–976, Oct. 2015.
[10] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Des., Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000.
[11] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2004.
[12] T. T. Nguyen and H. Lee, "Efficient algorithm and architecture for elliptic curve cryptographic processor," *J. Semicond. Technol. Sci.*, vol. 16, no. 1, pp. 118–125, 2016.
[13] G. D. Sutter, J. Deschamps, and J. L. Imaña, "Efficient elliptic curve point multiplication using digit-serial binary field operations," *IEEE Trans. Ind. Electron.*, vol. 60, no. 1, pp. 217–225, Jan. 2013.
[14] D. D. Chen *et al.*, "High-speed polynomial multiplication architecture for ring-LWE and SHE cryptosystems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 157–166, Jan. 2015.
[15] W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, "Exploring the feasibility of fully homomorphic encryption," *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 698–706, Mar. 2015.
[16] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *Proc. IEEE Symp. Secur. Privacy*, San Jose, CA, USA, May 2015, pp. 553–570.
[17] C. I. Watson *et al.*, "User's guide to NIST biometric image software," NIST, Gaithersburg, MD, USA, Tech. Rep. 7392, 2007.
[18] S. S. Roy, F. Vercauteren, and I. Verbauwhede, "High precision discrete Gaussian sampling on FPGAs," in *Selected Areas in Cryptography*. Berlin, Germany: Springer, 2014, pp. 383–401.
[19] C. Du and G. Bai, "Towards efficient discrete Gaussian sampling for lattice-based cryptography," in *Proc. 25th Int. Conf. Field Program. Logic Apps.*, London, U.K., Sep. 2015, pp. 1–6.
[20] S. S. Roy, F. Vercauteren, N. Mentens, D. D. Chen, and I. Verbauwhede, "Compact ring-LWE cryptoprocessor," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2014, pp. 371–391.
[21] J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series," *Math. Comput.*, vol. 19, no. 90, pp. 297–301, 1965.
[22] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002, pp. 80–84.
[23] D. Maio, D. Maltoni, and R. Cappelli. (2000). *Fingerprint Verification Competition*. [Online]. Available: bias.csr.unibo.it/fvc2000
[24] D. Maio, D. Maltoni, and R. Cappelli. (2002). *Fingerprint Verification Competition* [Online]. Available: bias.csr.unibo.it/fvc2002
[25] D. Maio, D. Maltoni, and R. Cappelli. (2004). *Fingerprint Verification Competition*. [Online]. Available: bias.csr.unibo.it/fvc2004
[26] A. Al-Haj, G. Abandah, and N. Hussein, "Crypto-based algorithms for secured medical image transmission," *IET Inf. Secur.*, vol. 9, no. 6, pp. 365–373, Nov. 2015.
[27] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto, "Providing integrity and authenticity in DICOM images: A novel approach," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 4, pp. 582–589, Jul. 2009.
[28] T. N. Tan and H. Lee, "A delay-efficient ring-LWE cryptography architecture for biometric security," in *Proc. IEEE Int. Symp. Circuits Syst.*, Baltimore, MD, USA, May 2017, pp. 2210–2213.

TUY NGUYEN TAN received the B.S. degree in electronic and telecommunication engineering from the Danang University of Technology, Vietnam, in 2009, and the M.S. degree in information and communication engineering, Inha University, South Korea, in 2016, where he is currently pursuing the Ph.D. degree in information and communication engineering. His research interest includes algorithm and architecture design for cryptosystems.

HANHO LEE received the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Minnesota, Minneapolis, in 1996 and 2000, respectively. In 1999, he was a Member of Technical Staff-1 with Lucent Technologies, Bell Labs, Holmdel, NJ, USA. From 2000 to 2002, he was a Member of the Technical Staff with Lucent Technologies (Bell Labs Innovations), Allentown. From 2002 to 2004, he was an Assistant Professor with the Department of Electrical and Computer Engineering, University of Connecticut, USA. Since 2004, he has been with the Department of Information and Communication Engineering, Inha University, where he is currently a Professor. From 2010 to 2011, he was a Visiting Scholar with Bell Labs, Alcatel-Lucent, Murray Hill, NJ, USA. His research interests include algorithm and architecture design for cryptographic, forward error correction coding, and digital signal processing.