1. INTRODUCTION

There has been a decent rise of the usage fingerprint authentication in recent years with the feature introduced in mobile phones and personal computers. Fingerprint authentication is used in many areas as stated, to unlock the phones, to purchase an app from the store on the phone, to enter a vault secured by fingerprint, and the list continues. Fingerprint authentication being one of the most reliable and secure methods for authentication has been the reason for this high rise. Fingerprints are often regarded as a personal property so protecting them from unauthorized access is a high priority to prevent misuse.

In a general Minutiae-based fingerprint authentication algorithm as depicted in Figure 1, there exist some local stations that connect to the server with the database of fingerprints. The fingerprint details sent by these stations to the server need to be protected from attackers. Li and Kot [2] presented a method which includes combining the minutiae details, orientation details and reference points from multiple fingerprints for security. But an attacker can obtain the original fingerprint by using multiple templates. Therefore, a need for a cryptography algorithm is needed for better security and protection of the fingerprint data. This paper focuses on Ring-LWE algorithm for this purpose.

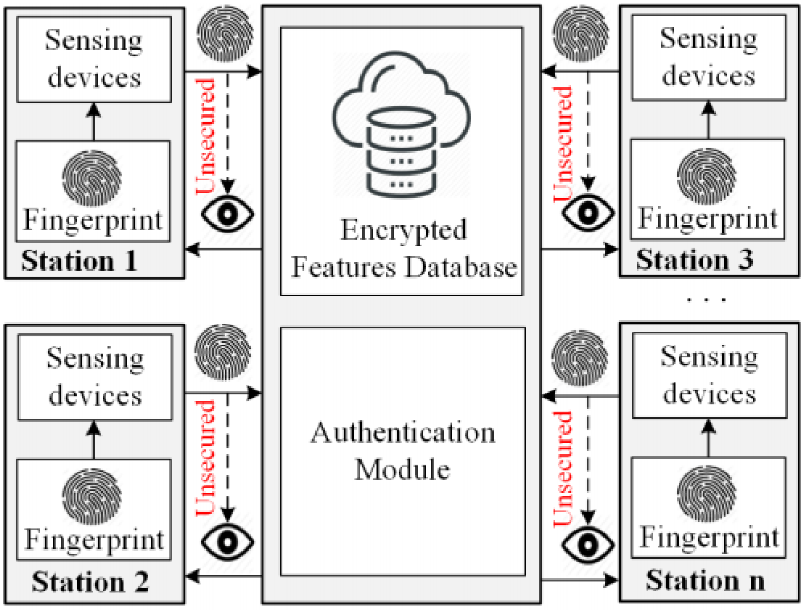

Figure 1: A typical fingerprint authentication system [1]

There are various methods used in cryptography which include Rivest, Shamir, and Adleman (RSA) [3] and Elliptic Curve Cryptography (ECC) [4] algorithms which use public and private keys for encryption and decryption. The disadvantage of these algorithms is that they can be solved in polynomial time by a quantum computer. This paper focuses on Ring-LWE algorithm. Ring-learning with errors (Ring-LWE) cryptography is based on the worst-case hardness of well-known lattice problems [5], [6], and 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.

1.1 Homomorphic Cryptography

In homomorphic Encryption, [5] we assume that a data x needs to sent to cloud to carry out a function f(x). A system must carry out the encryption and return a function F such that:

$$\mathrm{Dec}(F(\mathrm{Enc}(x))) = f(x)$$

Where Dec(y) mean Decrypted y and Enc(y) means Encrypted y.

This method computes encrypted data directly, while looking like as if the operation is performed on the decrypted data.

1.2 Ring Learning with Errors Cryptography

Learning with errors was first introduced by O. Regev [7]. Its main claim to fame is being as hard as worst-case lattice problems, hence rendering all cryptographic constructions based on it secure under the assumption that worst-case lattice problems are hard. Ring-LWE is an efficient implementation of original LWE. Ring-LWE asks to recover secret s from a noisy system such as:

$$a_0(x)s(x) + e_0(x) = b_0(x) \bmod q\ R$$

$$a_1(x)s(x) + e_1(x) = b_1(x) \bmod q\ R$$

$$a_2(x)s(x) + e_2(x) = b_2(x) \bmod q\ R$$

…

…

Here q is a prime, R is $Z[x]/(x^n + 1)$, n is a power of 2.

$a_i(x)$ are uniformly random polynomials, and $e_i(x)$ are unknown small random polynomials which contribute to hardness.

1.3 Number Theoretic Transform Multiplier

Using NTT and Inverse NTT in calculations makes the algorithm much faster than using polynomial multiplications as they are very intensive operations [5]. Given a_i in R_q, i = 1, 2, . . . , n − 1, a polynomials a(x) over the ring R_q can be expressed as follows:

$$a(x) = a_0 + a_1x + a_2x^{2} + \cdot\cdot\cdot + a_{n-1}x^{n-1}$$

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

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

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

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

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 ⊙ is the point-wise multiplication.

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

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

$$c_i = \sum_{j=0}^{i} a_jb_{i-j} - \sum_{j=i+1}^{n-1} a_jb_{n+i-j}$$

The general NTT-based polynomial multiplication is shown in Figure 2.

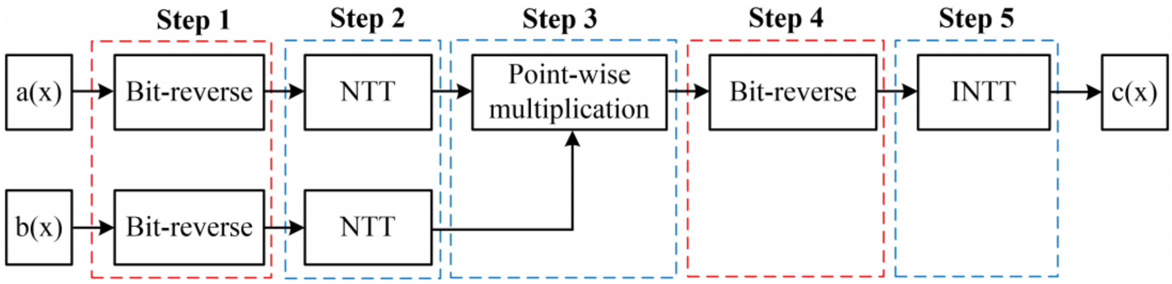

Figure 2: Block diagram of typical NTT polynomial multiplication [1]

2. PROBLEM IDENTIFICATION

With the increased usage of fingerprint authentication is various areas, the need to protect the fingerprint data is crucial. Therefore, Li and Kot [2] presented 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 biometric authentication systems to provide a higher level of security. For this, the original base paper introduced Ring-LWE cryptography algorithm for fingerprint authentication because of its hardness. NTT and Inverse NTT are used to carry out polynomial multiplication much efficiently.

3. OBJECTIVES

In the original base paper by Tuy Nguyen Tan and Hanho Lee [1] a fingerprint authentication system using ring-LWE cryptography, the post-quantum cryptosystem, is introduced. Ring-LWE along with NTT polynomial make this process secure and fast. The main contributions of the paper include:

- Tuy and Hanho presented 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.
- An optimal scheme for fingerprint-features extraction to reduce processing time and increase accuracy.
- Implementation of the ring-LWE cryptography system using the proposed NTT polynomial multiplication approach to enhance the encryption and decryption time.
- A fingerprint authentication system using fingerprint-features extraction method and the NTT multiplication-based ring-LWE cryptography scheme is thus proposed.
- Future work includes making the algorithm more efficient and faster by reducing latency. Possibly, by using parallel operations which may increase load on the hardware.

4. RESEARCH METHODOLOGY

Tuy and Hanho [1] proposed a fingerprint authentication system is described in Figure 3. 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. The features are then extracted and encrypted using NTT multiplication-based ring-LWE encryption. 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. Then, the server performs decryption of the message and compares results with the registered data. If the RTA sent from a local station is accepted, the server sends an Accept-To-Authenticate (ATA) message, otherwise sends a Reject message.

In feature extraction phase, Gamma correction method [8] is used to adjust the brightness of the input image for better quality image. Gamma correction is defined as:

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

Where each pixel r of the input image is transformed to the output level s by powering r to a γ. The parameter γ is adaptively estimated from the grey-scale level of the input image by:

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

Where I indicates the input image of size M × N; L is the grey level of I (L = 255 for 8-bit images)

An NTT-based polynomial multiplication described in Figure 2 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 [9] in the NTT-based polynomial multiplication operation, two bit-reverse operations can be reduced; therefore, the system computation time and complexity are remarkably decreased.

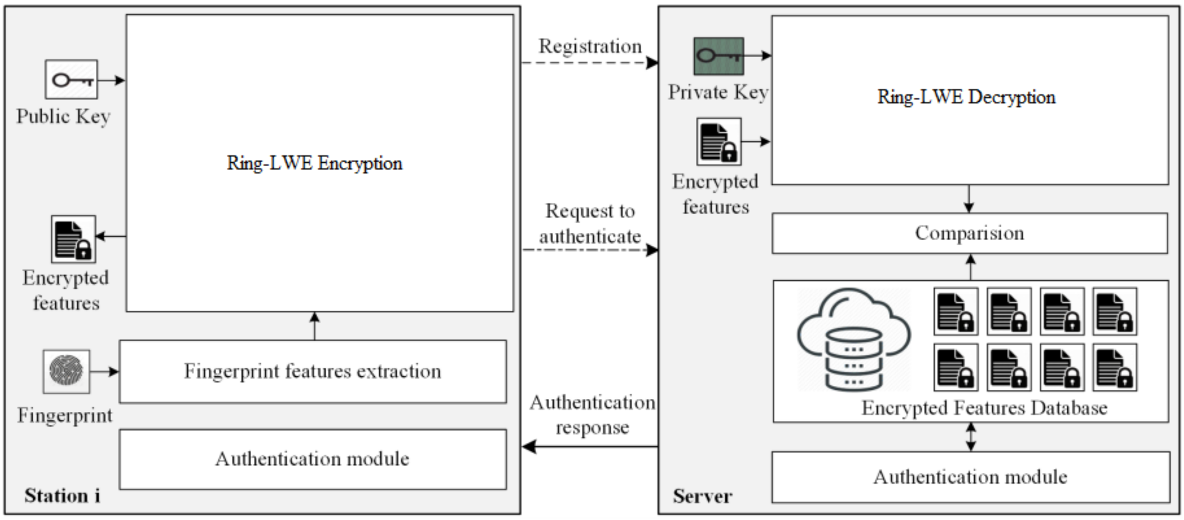

Figure 3: Secure fingerprint authentication system using ring-LWE cryptography [1]

In the system as depicted in Figure 3, 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. 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. Then $a(x) \times e_1(x)$ and $p(x) \times e_1(x)$ are calculated using two 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 (c1, c2) is generated. This encrypted message is initially registered with the remote server and this information is stored in the server database.

When a user who has already registered with the system requests to access, the users' fingerprint is encrypted again then 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 (c1, c2) of fingerprint features. The matching function installed at the server performs the comparison to decide if the user may access the system or not.

5. LITERATURE REVIEW

Tuy Nguyen Tan and Hanho Lee (2019) proposed the original High-Secure Fingerprint Authentication System Using Ring-LWE Cryptography [1]. In the paper, a high-secure fingerprint authentication system using ring learning with errors (ring-LWE) cryptography to protect users' fingerprint data more securely is proposed. 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. 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.

Mulagala Sandhya and Munaga V.N.K. Prasad (2016) proposed a system for securing fingerprint templates using fused structures [10]. The study presented a protection method for fingerprint templates by using fused structures at the feature level. The authors computed two transformed features from minutiae points: namely, local structure and distant structure. These structures are represented as bit-strings. A fusion on bit-strings is done at the feature level to produce a cancellable template. An equal error rate (EER) of 2.19, 1.6 and 6.14% on Fingerprint Verification Competition (FVC) 2002 Database (DB)1 through DB3 databases and an EER of 11.89, 12.71, 17.6% on FVC 2004 DB1 through DB3 proves the tenability of the proposed method. Thus, the authors developed a method for generating cancellable fingerprint templates using fused structures at the feature level. The fused structure is built by using LS and DS computed from the fingerprint minutiae points. The fused structures computed resulted in maintaining a good balance between security and performance.

Luiz Octavio Massato Kobayashi et al. (2009) proposed a paper titled "Providing Integrity and Authenticity in DICOM Images: A Novel Approach "[11]. In the paper, authors showed the increasing adoption of information systems in healthcare has led to a scenario where patient information security is more and more being regarded as a critical issue. Allowing patient information to be in jeopardy may lead to irreparable damage, physically, morally, and socially to the patient, potentially shaking the credibility of the healthcare institution. Thus, the paper presented a method using cryptographic means to improve trustworthiness of medical images, providing a stronger link between the image and the information on its integrity and authenticity, without compromising image quality to the end user.

Ali Al-Haj et al. (2005) proposed Crypto-based algorithms for secured medical image transmission [12]. In this study, the authors proposed two crypto-based algorithms capable of providing confidentiality, authenticity and integrity services to medical images exchanged in telemedicine applications. Strong cryptographic functions with internally generated symmetric keys and hash codes are used. The advanced encryption standard-Galois counter mode is used with the whirlpool hash function to provide confidentiality and authenticity, and the elliptic curve digital signature algorithm is used to provide authenticity and integrity. The proposed algorithms are based on the digital imaging and communication in medicine (DICOM) standard; however, unlike the standard, the algorithms provide confidentiality, authenticity and integrity for the header data, as well as for the pixel data of the DICOM images. Effectiveness of the proposed algorithms is evaluated and demonstrated through extensive experimentation using a benchmark set of DICOM images.

Li et al. (2015) [13] built a new framework for security analysis that uses information theoretic details and computational security. A multibiometric cryptosystem for fingerprints using decision level fusion was built that provides stronger security and better accuracy. The author constructed a fingerprint-based multibiometric cryptosystem (MBC) using decision level fusion. Hash functions are employed in our construction to further protect each single biometric trait. The experimental results and security analysis demonstrate that the proposed MBC provides stronger security and better authentication accuracy compared with a cryptosystem based on single biometric.

Sandhya et al. (2016) [14] developed a method for a cancellable template design for fingerprints using a feature set construction from the Delaunay triangles. The authors propose two methods namely FS_INCIR and FS_AVGLO to construct a feature set from the Delaunay triangles. The feature set computed is quantised and mapped to a 3D array to produce fixed length 1D bit string. This bit string is applied with a DFT to generate a complex vector. Finally, the complex vector is multiplied by user's key to generate a cancellable template. The proposed computation of feature set maintained a good balance between security and performance. These methods are tested on FVC 2002 and FVC 2004 databases and the experimental results show satisfactory performance. Further, the authors analysed the four requirements namely diversity, revocability, irreversibility and accuracy for protecting biometric templates. Thus, the feasibility of proposed scheme is depicted.

Wong et al. (2017) [15] built a binary cancellable template using minutia descriptor called multi-line code (MLC). The MLC template is transformed to a fixed-length bit-string using kernel principal components analysis. The author developed a fixed-length binary cancellable fingerprint template generation scheme based on a minutia descriptor known as the multi-line code (MLC). While retaining the core of MLC algorithm, we transform the unordered and variable-size MLC template into an ordered and fixed-length bit-string using kernel principal components analysis (KPCA) and state-of the-art binarization techniques. The construction of a proper kernel suited for the scenario was validated using Mercer's Theorem.

Sandhya and Prasad (2017) [16] designed a fingerprint cryptosystem using multiple spiral curves of minutiae points and fuzzy commitment scheme. The author proposed a cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme. The method is built by combining cancelable biometrics and biometric cryptosystems. First, we compute transformed minutiae features using multiple spiral curves. Further, these transformed features are encrypted using fuzzy commitment scheme. Hence, a secure template is obtained. Experimental results and analysis prove the credibility of proposed method with recently presented methods of fingerprint template protection

Jin et al. (2016) [17] proposed an Error Correcting Code (ECC)-free key binding scheme along with cancellable transforms for minutiae-based fingerprint biometrics. In this paper, author proposed an ECC-free key binding scheme along with cancellable transforms for minutiae-based fingerprint biometrics. Apart from that, the minutiae information is favourably protected by a strong non-invertible cancellable transform, which is crucial to prevent a number of security and privacy attacks. Experiments conducted on FVC2002 and FVC2004 show that the accuracy performance is comparable to state-of-the-arts. Author further demonstrated that the proposed scheme is robust against several major security and privacy attacks.

6. REFERENCES

[1] T. N. Tan and H. Lee, "High-Secure Fingerprint Authentication System Using Ring-LWE Cryptography," in IEEE Access, vol. 7, pp. 23379-23387, 2019.

[2] 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

[3] 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.

[4] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York, NY, USA: Springer, 2004.

[5] 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.

[6] 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.

[7] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6):34, 2009. Preliminary version in STOC’05.

[8] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002, pp. 80–84.

[9] 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

[10] M. Sandhya and M. V. N. K. Prasad, "Securing fingerprint templates using fused structures," in IET Biometrics, vol. 6, no. 3, pp. 173-182, 5 2017.

[11] L. O. M. Kobayashi, S. S. Furuie and P. S. L. M. Barreto, "Providing Integrity and Authenticity in DICOM Images: A Novel Approach," in IEEE Transactions on Information Technology in Biomedicine, vol. 13.

[12] Al-Haj, Ali & Abandah, Gheith & Hussein, Noor. (2015). Crypto-based algorithms for secured medical image transmission. IET Information Security. 9. 10.1049/iet-ifs.2014.0245.

[13] Li, C., Hu, J., Pieprzyk, J., et al.: ‘A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion’, IEEE Trans. Inf. Forensics Sec., 2015, 10, pp. 1193–1206

[14] Sandhya, M., Prasad, Munaga V.N.K., Chillarige, R.R.: ‘Generating cancellable fingerprint templates based on Delaunay triangle feature set construction’, IET Biometrics, 2016, 5, pp. 131–139

[15] Wong, W.J., Teoh, A.B., Kho, Y.H., et al.: ‘Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template’, Pattern Recognit., 2016, 51, pp. 197–208

[16] Sandhya, M., Prasad, Munaga V.N.K.: ‘Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme’, Int. J. Pattern Recognit. Artif. Intell., 2016, doi: 10.1142/S0218001417560043

[17] Jin, Z., Teoh, A.B.J., Goi, B.-M., et al.: ‘Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation’, Pattern Recognit., 2016, 56, pp. 50–62