Research Article

An Effective NTRU-Based Fully Homomorphic Encryption Scheme

Xiaoyue Qin , Ruwei Huang , and Huifeng Fan

School of Computer and Electronic Information, Guangxi University, Nanning, Guangxi 530004, China

Correspondence should be addressed to Ruwei Huang; ruweih@gxu.edu.cn

Received 12 March 2021; Revised 23 July 2021; Accepted 27 July 2021; Published 9 August 2021

Academic Editor: Chien Ming Chen

Copyright © 2021 Xiaoyue Qin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Fully homomorphic encryption (FHE) supports arbitrary computations on ciphertexts without decryption to protect users' privacy. However, currently, there are still some shortcomings in research studies on FHE. For example, the NTRU-based FHE scheme constructed using the approximate eigenvector method requires complex matrix multiplications, and the power-of-two cyclotomic ring cannot prevent subfield attacks. To address these problems, this paper proposed a NTRU-based FHE scheme constructed based on the power-of-prime cyclotomic ring and made the following improvements: (1) the power-of-prime cyclotomic ring is immune to subfield attacks; (2) complex matrix multiplications are replaced with matrix-vector multiplications to modify the ciphertext forms and decryption structures, so as to gain advantages in storage, transportation, and computations; (3) the single instruction multiple data (SIMD) technology is introduced, and homomorphic operations are executed through the Chinese remainder theorem, further improving the scheme computation and storage efficiency. The ciphertext of the scheme is in a form of a vector, and no key exchange is required for homomorphic operations. In addition, this scheme can eliminate the decisional small polynomial ratio (DSPR) assumption under certain conditions and only relies on the ring learning with errors (RLWE) assumption. The standard security model can prove that this scheme is secure against chosen-plaintext (IND-CPA) attacks. Compared with similar schemes, the proposed scheme improves the efficiency at least by a factor of $l\varphi(x)/d + 1$ and quadratically decreases the noise growth rate.

1. Introduction

Fully homomorphic encryption supports arbitrary computations on the ciphertext without the requirement of decryption, and the result obtained is same as direct computations on plaintext after decryption. This can well solve the contradiction between the security of user privacy and the outsourcing of data storage and computation in an outsourced computing environment. Therefore, fully homomorphic encryption is widely applied in cloud computing, healthcare, blockchain, and other industries [1]. The existing FHE schemes can be divided into three types: integer-type [2], Regev-type [3], and NTRU-type [4]. The first two types of schemes have low efficiency of homomorphic computations and large cost of key generation, while in the NTRU-based FHE scheme, algorithms can only use modular multiplication and modular inverse, which results in a faster decryption speed [5, 6] and plays a promising role in the resource-constrained IoT environment. It can provide mutual authentication for devices and servers as well as

resistance to known attacks. IoT devices based on the NTRU-based scheme can be connected to authentication schemes such as those described in the literature [7, 8], improving the overall authentication efficiency of schemes as well as preventing quantum attacks. Therefore, the study of the NTRU-based FHE scheme is of great significance.

In 2013, Gentry et al. proposed a FHE scheme, which was constructed based on the technique of approximate eigenvectors [9]. The homomorphic addition and homomorphic multiplication of this scheme are achieved by doing simple addition and multiplication on the matrix. The scheme is relatively simple, fast, and easy to understand, and the implementation of homomorphic computations can be achieved without computing the public key and only with the help of the user's public key [10]. In addition, the authors pointed out that the technique can be applied to construct an FHE scheme based on NTRU. However, no specific implementation was provided. The F-NTRU scheme proposed by Dor and Sunar [11] and the improved scheme proposed by Li et al. [12] are all constructed by adopting the

flattening technique and the BitDecomp technique to derive an NTRU-based scheme based on approximate eigenvectors. However, the ciphertext of the FHE scheme constructed using approximate eigenvectors is in the form of a matrix. The ciphertext size is relatively large, and complex matrix multiplications are required, which greatly affects the computational efficiency. In 2018, Khedr and Gulak [13] used NTT (FastNumber-TheoreticTransform) to perform matrix multiplication instead of circular convolution in the F-NTRU scheme to make the computation simple, but none of these improvements can essentially avoid matrix multiplication.

Meanwhile, the security of the above schemes is based on the power-of-two cyclotomic ring. The schemes based on this cyclotomic ring have a simple structure, but they cannot prevent subfield attacks [14, 15] and use SIMD techniques [16]. Migliore et al. [17] also verified that the F-NTRU scheme suffers from the possibility of subfield attacks, so finding a more secure ring to guarantee the security of the scheme is especially important. In 2016, Doroz et al. [18] proposed for the first time a DHS16 scheme based on the power-of-prime cyclotomic ring to improve the LTV12 scheme [19], which improves the efficiency of the scheme in practical applications but does not give a theoretical proof of security. In 2018, Yu et al. [20] changed the ring structure of the SS11 scheme [21] to a power-of-prime cyclotomic ring and improved the key generation algorithm using a Gaussian distribution with regular embedding to make its security proven.

To address the abovementioned problems that occurred in the process of constructing FHE schemes using approximate eigenvectors, this paper firstly applies the existing power-of-two cyclotomic polynomial to the power-of-prime cyclotomic polynomial in terms of security enhancement and gives an NTRU-type FHE scheme based on the power-of-prime cyclotomic ring. The scheme eliminates the DSPR assumption under certain conditions, and its security only depends on the RLWE assumption. The standard security model can prove that this scheme is secure against chosen-plaintext (IND-CPA) attacks. In terms of improving efficiency, the scheme introduces SIMD techniques and uses matrix-vector multiplication instead of complex matrix multiplication, which greatly enhances the efficiency. The ciphertext of the scheme is in a form of a vector, which is more advantageous in storage, transportation, and computation. In addition, the calculation order of multiplication can further optimize the noise management.

2. Basic Knowledge

The power-of-prime cyclotomic ring [22] on which this scheme is based is a special case of cyclotomic polynomial. The construction of the key generation algorithm involves Gaussian distribution under regular embedding [23]. The security of this scheme depends on RLWE assumption as well as DSPR assumption [24], and the security model proves that this scheme is secure against IND-CPA attacks [25]. This section focuses on the cyclotomic polynomial, RLWE assumption, DSPR assumption, Gaussian

distribution with regular embedding, and definition of the security model.

2.1. Symbolic Representation. If A indicates an algorithm, $x \leftarrow A$ indicates that x is obtained based on that algorithm. If A indicates a collection, $x \leftarrow A$ indicates that x is randomly chosen from Collection A . For any integer q , if $Z_q = [-q/2, q/2) \cap \mathbb{Z}$, integer x , $[x]_q$ indicates $(x \bmod q) \in Z_q$. Use lowercase letters to represent a multi-dimensional vector. For example, for vector y , y_i indicates its i th component. The polynomial of an indeterminate of x is represented using lowercase letters, for example, $f(x)$.

2.2. Cyclotomic Polynomial

Definition 1 (cyclotomic polynomial, see [22]). Assume Field K is the field of characteristic P , n is a positive integer that cannot be divided by P with no remainder, ξ_n is a primitive n th root of unity in Field K , and the polynomial $\Phi_n(x) = \prod_{i=1, \gcd(i,n)=1}^n (x - \xi_n^i)$ is called the n th cyclotomic polynomial in Field K . Adjoin a primitive n th root of unity to Field Q of rational numbers to get an extension field $K = Q(\xi_n)$, which is called the n th cyclotomic field.

- (i) When $n = 2^d, d \in \mathbb{Z}^*$, $\Phi_n(x) = x^n + 1$
- (ii) When n is a prime number, $\Phi_n(x) = x^{n-1} + x^{n-2} + \dots + x + 1$
- (iii) When d is a prime number, $n = d^v, v \in \mathbb{Z}^*$, $\Phi_n(x) = \Phi_d(x^{d^{v-1}})$, $R = \mathbb{Z}[x]/\Phi_n(x)$, and $R_q = R/q$ R is the power-of-prime cyclotomic polynomial ring.

Theorem 1 (see [22]). If F_q is a finite field and n is a positive integer, the sufficient and necessary condition for cyclotomic polynomial of order n Q_n to be reducible over $F_q[x]$ is that the exponent of $q \bmod n$ is $\Phi_n(x)$ (that is, q is the primitive root of $\bmod n$). It can be seen from Theorem 1 that if $n \equiv \pm 1 \bmod 8$ is a prime or the square exponent of a prime, Q_n is reducible over $F_2[x]$ [26].

Theorem 2 (see [22]). If F_q is a finite field, n is a positive integer, and $\gcd(n, d) = 1$, cyclotomic polynomial $\Phi_n(x)$ can be decomposed into the product of $\varphi(x)/d$ different monic irreducible polynomials $f_i(x)$ of degree 2 in $F_q[x]$, that is, $\Phi_n(x) = \prod_{i=0}^{l-1} f_i(x)$, where d is the exponent of $q \bmod n$, meeting the requirement of being the minimum integer of $q^d \equiv 1 \pmod{n}$, and $l = \varphi(x)/d$.

Theorem 3 (see [27]). If $n \in \mathbb{N}$, $\Phi_n(x) = x^n + 1$, and Ring $R = \mathbb{Z}[x]/\Phi_n(x)$, for any a and $b \in R$, the function is

$$\begin{aligned} \|ab\| &\leq \|a\| \|b\|, \\ \|ab\|_{\infty} &\leq n \|a\|_{\infty} \|b\|_{\infty}. \end{aligned} \quad (1)$$

Theorem 4 (see [20]). If $n = d^v$, d is a prime number, and $\Phi_n(x) = \Phi_d(x^{d^{v-1}})$, then $R = \mathbb{Z}[x]/\Phi_n(x)$. For any a and $b \in R$, in the worst case, the function

$$\|ab\|_{\infty} \leq 2\sqrt{\varphi(n)}\|a\|_{\infty}\|b\|_{\infty}. \quad (2)$$

2.3. Gaussian Distribution with Regular Embedding

Definition 2 (Gaussian distribution with regular embedding, see [26]). Assume that $P(X) \in \mathbb{Z}[x]$ is a monic reducible polynomial of degree n , $R = \mathbb{Z}[x]/P(x)$, the roots of $P(X)$ in the field of complex numbers are $w_1, w_2, \dots, w_n$, respectively, $V = (w_j^{n-i})_{ij}, 0 \leq i \leq n-1$, and $1 \leq j \leq n$ is called a regular transformation matrix. Let $t = t_{n-1}x^{n-1} + t_{n-2}x^{n-2} + \dots + t_0 \in R$, the embedding of coefficients is represented by $t_{n-1}, t_{n-2}, \dots, t_0$, and the transformation of regular embedding is represented by $\sigma(t) = (t_{n-1}, t_{n-2}, \dots, t_0)V\sigma$, and Gaussian distribution with regular embedding is represented as follows:

$$D_{\sigma^{-1}(t)} = \sigma(t) \cdot V^{-1}, \quad (3)$$

$$D_{\sigma^{-1}, \sigma}(x) = \frac{\rho_{\sigma}(x)}{\rho_{\sigma}(\mathbb{Z}^n)}.$$

2.4. RLWE $(\Phi, \mathbf{n}, \mathbf{q}, \chi)$ Assumption

Definition 3 (RLWE $(\Phi, \mathbf{n}, \mathbf{q}, \chi)$ assumption, see [27]). Assume $n = d^v$, d is a prime number, and $\Phi_n(x) = \Phi_d(x^{d^{v-1}})$. Define polynomial ring $R = \mathbb{Z}[x]/\Phi_n(x)$, $R_q = R/qR$, and a discrete Gaussian distribution χ on ring R with regular embedding. The RLWE $(\Phi, \mathbf{n}, \mathbf{q}, \chi)$ assumption states that, for a random ring element $s \leftarrow R_q$, given a polynomial $(a_i, b_i = a_i \cdot s + e_i) \in (R_q)^2$ where a_i is uniformly random in R_q and e_i is drawn from an error distribution χ , it is very hard to distinguish whether b_i is drawn from computations or directly from the uniform distribution of R_q .

2.5. DSPR $(\Phi, \mathbf{n}, \mathbf{q}, \chi)$ Assumption

Definition 4 (DSPR $(\Phi, \mathbf{n}, \mathbf{q}, \chi)$ assumption, see [24]). Let $n = d^v$, d is a prime number, and $\Phi_n(x) = \Phi_d(x^{d^{v-1}})$. Define polynomial ring $R = \mathbb{Z}[x]/\Phi_n(x)$, $R_q = R/qR$, and a discrete Gaussian distribution χ on ring R with regular embedding. The DSPR $(\Phi, \mathbf{n}, \mathbf{q}, \chi)$ assumption is that it is hard to distinguish whether the element f of the polynomial $h = g/f$, where f and g are sampled from distribution χ , is drawn from a uniformly random element of R_q or is reversible in $R_q = R/qR$.

2.6. Security Model

Definition 5 (security model, see [25]). Define a game between the attacker and challenger. This game is divided into four phases.

Setup phase: the challenger runs the key generation algorithm of the encryption scheme to generate a public key and makes the attacker get the public key.

Oracle machine access phase: the attacker chooses the plaintext and initiates queries to the oracle machine for encryption. After the attacker gets the ciphertext in a response, the attacker can submit the chosen plaintext multiple times in different stages and get the ciphertexts corresponding different plaintexts.

Challenge phase: the attacker chooses two plaintext messages m_0 and m_1 and sends them to the challenger. The challenger chooses $b \in \{0, 1\}$ and sends the ciphertext $c = \text{Enc}_{pk}(m_b)$ to the attacker.

Guess phase: the attacker gives his guess b' corresponding to the ciphertext. When $b' = b$, the attacker wins.

Assume that there is an encryption scheme ε for the public key within the bounded polynomial time, and a tiny function $\text{negl}(\lambda)$ that gets the advantage of the attacker A is

$$\text{Adv}_{\text{IND-CPA}}(A) = \left| \frac{\Pr[A(pk, \text{Enc}_{pk}(m_0 = 1))]}{-\Pr[A(pk, \text{Enc}_{pk}(m_1 = 1))]} \right| = \text{negl}(\lambda), \quad (4)$$

where $\text{negl}(\lambda)$ can be ignored and λ is the security parameter of the scheme. The game includes an attacker of polynomial time attacker A . Let $\text{Adv}_{\text{IND-CPA}}(A)$ be the probability that attacker A wins in the game. This scheme is secure against IND-CPA attacks.

3. Efficient NTRU-Based Fully Homomorphic Encryption

This section first introduces the SIMD technique for plaintext batch processing, then describes the algorithm construction of the scheme in this paper, and finally proves the correctness of the encryption and decryption process and homomorphic operations of the scheme and provides an analysis of the noise growth during the process.

3.1. SIMD Technique. It can be derived from Theorems 1 and 2 that the power-of-prime cyclotomic ring can be decomposed into multiple irreducible polynomials in $F_q[x]$. Therefore, in this paper, we use the Chinese remainder theorem [28] to batch process the data of plaintext slots and perform homomorphic computations in parallel to improve the execution efficiency of the scheme. The specific procedure is given below.

Decompose the entire plaintext space $R_p = R/pR$ into l subrings with the same size. The corresponding plaintext slots are $\mathbb{Z}_2[x]/f_1(x), \dots, \mathbb{Z}_2[x]/f_l(x)$, inside which $m_i(x)$ plaintexts are waiting to be encrypted. Then, combine l plaintexts in the slots into a plaintext space. $c(x)$ and $c'(x)$ indicate the ciphertexts obtained after encryption using a same plaintext space, respectively, and their corresponding plaintexts are $m_1(x), m_2(x), \dots, m_l(x)$ and $m'_1(x), m'_2(x), \dots, m'_l(x)$, respectively.

The homomorphic operations that are performed in parallel on l plaintexts are as follows:

$$\begin{aligned} l_{\text{add}}((m_1(x), m_2(x), \dots, m_l(x)), (m'_1(x), m'_2(x), \dots, m'_l(x))) &= m_1(x) + m'_1(x), \dots, m_l(x) + m'_l(x), \\ l_{\text{mult}}((m_1(x), m_2(x), \dots, m_l(x)), (m'_1(x), m'_2(x), \dots, m'_l(x))) &= m_1(x) \cdot m'_1(x), \dots, m_l(x) \cdot m'_l(x), \end{aligned} \quad (5)$$

where l_{add} and l_{mult} indicate the batch homomorphic addition and homomorphic multiplication operations on plaintexts, respectively. Therefore, homomorphic operations can be regarded as being executed in parallel on the plaintext slots by using the SIMD technique. Because data at different indexes within the arrays can never interact, l_{add} and l_{mult} operations are not sufficient to perform arbitrary computations on encrypted arrays. To obtain a complete operation set of data arrays, this paper introduces the l_{permute} operation described in the literature [29] to impose an arbitrary ordering on data in arrays and supports plaintext slots of $m(x) \rightarrow m(x^{2^i})$ to move cyclically by i plaintext slots. When $i = 1$, the plaintext slot of $m(x)$ moves by one slot. Accordingly, the plaintext of each plaintext slot is changed to $m_2(x), m_l(x), \dots, m_1(x)$, so as to perform the whole operations on the data. When the ciphertext requires decryption, the Chinese remainder theorem is used for reversible processing to decrypt to l plaintexts.

3.2. Scheme Construction. Assume that λ is a security parameter, L is the number of circuit layers, and n is a dimension and a power of a prime number. Let $R = \mathbb{Z}[x]/\Phi_n(x)$, where $\Phi_n(x) = \prod_{i=1, \gcd(i,n)=1}^n x - \xi^i$ is cyclotomic polynomial, the number of times for each $f_i(x)$ is d , $\varphi(n) = \text{dl} = n(L, L)$, $F_{q^d}^l$ is the vector space of plaintexts, and mapping CRT_q is the isomorphic mapping from $F_{q^d}^l$ to R_q .

3.2.1. Key Generation Algorithm. Select a relatively large standard error σ , and make f represent $f = p \cdot f' + 1$ where f' is a polynomial sampled from a discrete Gaussian distribution $D_{\mathbb{Z}^n, \sigma}(x)$ with regular embedding. Input n and $q \in \mathbb{Z}$, $p \in R_q^*$, and $\sigma \in R$, where R_q^* is a collection of reversible elements in R_q . $R_q = R/qR = \mathbb{Z}_q[x]/\Phi$. Output $(sk, pk) \in R \times R_q^*$. The detailed procedure is as follows:

First sample f' from a discrete Gaussian distribution $D_{\mathbb{Z}^n, \sigma}(x)$ with regular embedding; let $f = p \cdot f' + 1$. If $f \bmod q \notin R_q^*$, sample again.

Then, sample g from a discrete Gaussian distribution $D_{\mathbb{Z}^n, \sigma}(x)$ with regular embedding. If $g \bmod q \notin R_q^*$, sample again.

Finally, return $sk = f$ and $pk = h = pgf^{-1} \in R_q^*$.

3.2.2. Encryption Algorithm. Use the Chinese remainder theorem to calculate the plaintext $m \leftarrow \text{CRT}_q(m_1(x), m_2(x), \dots, m_l(x)) \in R_q$. Let m' represent $(m, 2^1m, \dots, 2^{l-1}m)$. c is the length corresponding to message m and is the ciphertext of $l = \log q$. Column vector $c = (c_0, c_1, \dots, c_{l-1})^T$, where $c_i = 2^i m + hs_i + pe_i$.

3.2.3. Additive Homomorphism. c^+ represents the result obtained by performing the homomorphic addition operation

on two plaintexts. c' and c'' represent the fresh ciphertexts in a form of a column vector. Because the ciphertexts are in the same form, only a simple addition operation is needed to achieve the homomorphic addition operation:

$$c^+ = c' + c''. \quad (6)$$

3.2.4. Multiplicative Homomorphism. c^* indicates the result obtained by performing the homomorphic multiplication operation on two ciphertexts. The ciphertext c^* obtained through calculation is a column vector, which is in a same form as the original ciphertext. Therefore, no key exchange is required:

$$c^* = \text{BitDecomp}(c') \cdot c''. \quad (7)$$

3.2.5. Decryption Algorithm. c' indicates the fresh ciphertext in a form of a column vector. When performing decryption operations, the first element c'_0 of this ciphertext is selected for calculation:

$$m = c'_0 f \bmod p. \quad (8)$$

According to $(m_1(x), m_2(x), \dots, m_l(x))m \leftarrow \text{CRT}_q^{-1}(x) \in F_{q^d}^l$, l plaintexts can be decrypted.

3.3. Correctness Analysis. In this section, the encryption and decryption process of the scheme and the corresponding noise growth are analyzed.

It can be known from the encryption and decryption algorithms that

$$\begin{aligned} \text{Dec}(\text{Enc}(m)) &= c'_0 f \bmod p = (mf + pgs_0 + pe_0 f) \bmod p, \\ &= (mf + p(gs_0 + e_0 f)) \bmod p = mf \bmod p. \end{aligned} \quad (9)$$

Because $f \equiv 1 \pmod{p}$, $c'_0 f \bmod p = m$ can be obtained from formula (9). Combine the Chinese remainder theorem $(m_1(x), m_2(x), \dots, m_l(x))m \leftarrow \text{CRT}_q^{-1}(x) \in F_{q^d}^l$ to decrypt to l plaintexts.

Theorem 1 (encryption noise). q, n, R_q , and χ are parameters of the preceding encryption scheme. The upper bound of χ is B . For any $\leftarrow \chi$, calculate $f = p \cdot f' + 1$ and make $f \equiv 1 \pmod{p}$. If $f \bmod q \notin R_q^*$, sample again. Let $h = \text{Keygen}(f)$ and $c' \leftarrow \text{Enc}(h, m)$; then, v exists and $v_\infty \leq 2p\sqrt{\varphi(n)}((1+p)B^2 + B)$, which establishes the following equation:

$$c'_0 f = mf + p(gs_0 + e_0 f) \in R_q, \quad (10)$$

where $v = p(gs_0 + e_0 f)$ is the noise of the ciphertext. $mf = m(p \cdot f' + 1)$ contains part of noise of mf' to correct

messages that have few packaging [30]. Therefore, this part of noise is ignored in this paper.

Proof. According to the basic encryption scheme $c'_0 f = mf + pgs_0 + pe_0 f$, let $v = pgs_0 + pe_0 f$ be the noise of the fresh ciphertext. As the upper bound of χ is B , we can know that the upper bound of coefficient g , s , and e is B , and the upper bound of coefficient f is $pB + 1$. Combining Theorem 4, we can obtain that the upper bound of coefficient gs_0 is $2\sqrt{\varphi(n)}B^2$ and the upper bound of coefficient of $e_0 f$ is $2\sqrt{\varphi(n)}B(pB + 1)$. Above all, the upper bound of coefficient

v is $2p\sqrt{\varphi(n)}((1 + p)B^2 + B)$, which is $v_\alpha \leq 2p\sqrt{\varphi(n)}((1 + p)B^2 + B)$. $\square$

Theorem 2 (decryption noise). For any f and $c' \in R_q$, $f \equiv 1 \pmod{p}$. If $c'_0 f = mf + v \in R_q$ is met and $v_\alpha \leq q/2p$, then

$$\text{Dec}(f, c'_0) = m. \quad (11)$$

Proof. If $v_\alpha \leq q/2p$, then

$$\text{Dec}(f, c'_0) = c'_0 f \pmod{p} = mf + p(gs_0 + e_0 f) \pmod{p} = mf \pmod{p} = m. \quad (12)$$

Combining Theorem 1, we can reach the conclusion that when the noise is less than $q/2p$, the decryption is successful. $\square$

3.4. Homomorphism Analysis. Let c' and c'' be the ciphertexts that are encrypted using the proposed scheme. The corresponding private key is f . It can be found from the decryption definition that $cf = (c_0, c_1, \dots, c_{l-1})^T f = (2^0 mf + hs_0 f + pe_0 f, 2^1 mf + hs_1 f + pe_1 f, \dots, 2^{l-1} mf$

$+ hs_{l-1} f + pe_{l-1} f)^T = (2^0 m, 2^1 m, \dots, 2^{l-1} m)^T f + hsg + pef$. $f = m$ Power of 2 (f) + $2v$, where $v = hsg + pef$.

3.4.1. Additive Homomorphism. Let c^+ be a ciphertext that is equivalent to the encryption of the sum of the two plaintexts. The ciphertext form is not changed, and the following can prove the additive homomorphism:

$$\begin{aligned} c^+ f &= (c' + c'')f = c' f + c'' f = (m_1 \text{Powerof} 2(f) + 2v_1) + (m_2 \text{Powerof} 2(f) + 2v_2), \\ &= (m_1 + m_2) \text{Powerof} 2(f) + 2(v_1 + v_2). \end{aligned} \quad (13)$$

From formula (13), ciphertext c^+ can be seen as a result of the sum of two plaintexts. Therefore, this scheme has the additive homomorphism.

3.4.2. Addition Noise. Let c_0^+ represent the first row of the fresh ciphertext on which the homomorphic addition operation is performed. $E = 2p\sqrt{\varphi(n)}((1 + p)B^2 + B)$. According to the addition definition, $c_0^+ f = (m_1 + m_2)$

$\text{Powerof} 2(f) + v_1 + v_2$, where $v_1 = ps'_0 g + pe'_0 f$ and $v_2 = ps''_0 g + pe''_0 f$. Because $v_\alpha \leq E$, we can get $v_1 + v_2 \leq 2E \leq 4\sqrt{\varphi(n)}((1 + p)B^2 + B)$.

3.4.3. Multiplicative Homomorphism. Let c^* be a ciphertext that is equivalent to the encryption of the multiplication result of two plaintexts. The following can prove the multiplicative homomorphism:

$$\begin{aligned} c^* f &= \text{BitDecomp}(c') \cdot c'' f = \text{BitDecomp}(c') \cdot (m_2 \text{Powerof} 2(f) + 2v_2), \\ &= c' f m_2 + 2 \text{BitDecomp}(c') v_2 = m_2 (m_1 \text{Powerof} 2(f) + 2v_1) + 2 \text{BitDecomp}(c') v_2 \\ &= m_2 m_1 \text{Powerof} 2(f) + 2v_1 m_2 + 2 \text{BitDecomp}(c') v_2, \end{aligned} \quad (14)$$

where the value ranges of v_1 , v_2 , and $\text{BitDecomp}(c')$ are small. It can be seen from formula (14) that c^* can be decrypted to the multiplication result of two plaintexts; therefore, this scheme has multiplicative homomorphism.

3.4.4. Multiplication Noise. After the homomorphic addition operation is performed on two ciphertexts, the noise is the sum of the noises of two ciphertexts. After the

homomorphic multiplication operation is performed, the noise is the multiplication result of the noises of two ciphertexts. Therefore, the factor that affects the correctness of decryption is multiplicative homomorphism. Therefore, this paper presents the noise obtained by performing the homomorphic multiplication and the calculated noise of the ciphertext circuit layer L .

Let c_0^* represent the first row of the fresh ciphertext after the homomorphic multiplication operation was performed

on it. Let v^* represent the noise after a homomorphic multiplication operation. According to the multiplication definition, we have a formula $c^*f = m_2m_1\text{Powerof2}(f) + 2v_1m_2 + 2\text{BitDecomp}(c')v_2$, where $v_1 = ps'_0g + pe'_0f$, $v_2 = ps''_0g + pe''_0f$, $v_\alpha \leq E$, and c'_0 is the first row of matrix $\text{BitDecomp}(c')$, a polynomial containing $l-1$ coefficients whose value is 0 or 1. Through the formula, we can get $\text{BitDecomp}(c')v_{2\alpha} \leq nlE$. Because m indicates $\varphi(x)/d$ plaintexts of $m(x)$, we can get $2v_1m_{2\alpha} \leq 2\varphi(x)/dE$. Therefore, $v_\alpha^* \leq 2nlE + 2\varphi(x)/dE$.

Assume that the noise of the i th layer is c^i ; according to the homomorphic operation, we can get $c^i = c^{i-1} * c^{i-1}$. The calculated noise of this scheme after the second multiplication circuit is as follows:

$$c^3 = c^2 * c^2 = (2nlE + 2E) * (2nlE + 2E) = (2nlE + 2E)^2. \quad (15)$$

A homomorphic multiplication operation is performed on $2\varphi(x)/d$ plaintexts. Therefore, the maximum noise deduced from the calculation of a circuit with a depth of L is

$$c^L = (2nlE + 2E)^{dL/\varphi(X)}. \quad (16)$$

As long as $(2nlE + 2E)^{dL/\varphi(X)}$ does not exceed $q/2p$, the encryption of ciphertexts is correct. To compare with the F-NTRU scheme in terms of the noise, this paper analyzes the noise growth of the F-NTRU scheme.

Let c' and c'' be the ciphertexts encrypted by using the F-NTRU scheme. The corresponding private key is f , c'_0 represents the first row of the ciphertext after a homomorphic multiplication operation is performed, and v^* represents the noise after a homomorphic multiplication operation is performed. According to the F-NTRU scheme, the multiplication definition is

$$c'_0f = (m_1 \cdot m_2 + c'_0 \cdot c_{(0,0)}' + c''_0 \cdot m_1 + c'_0 \cdot m_2 + \dots + c'_{(0,l-1)} \cdot c_{l-1}'')f. \quad (17)$$

$c'_i = ps'_ig + pe'_if = v$ and $c''_i = ps''_ig + pe''_if = v$. Because $v_\alpha \leq E$, we can get that $c''_0 \cdot m_{1\alpha} = c'_0 \cdot m_{2\alpha} \leq E$, $c''_0 \cdot c'_{(0,0)} + \dots + c'_{(0,l-1)} \cdot c_{(l-1)\alpha}'' = c'_0 \cdot c''_0 \leq nE^2$. Therefore, in the F-NTRU scheme, the noise after a homomorphic multiplication operation is performed is $v_\alpha^* \leq 2E + nE^2$. Assume that the noise of the i th layer is c^i , $c^i = c^{i-1} * c^{i-1}$ according to the homomorphic operation, and the noise calculated after the second multiplication circuit in the F-NTRU scheme is as follows:

$$c^3 = c^2 * c^2 = (2E + nE^2) * (2E + nE^2) = (2E + nE^2)^2. \quad (18)$$

A homomorphic multiplication operation is performed on two plaintexts. Therefore, the maximum noise deduced from the calculation of a circuit with a depth of L is

$$c^L = (2E + nE^2)^L. \quad (19)$$

As long as $(2E + nE^2)^L$ does not exceed the encryption condition of the F-NTRU scheme, the ciphertext can be decrypted correctly. Combining the noise analysis of this scheme, we can get that compared with the F-NTRU scheme, the noise growth of this scheme after a

homomorphic multiplication operation is performed decreases quadratically. In addition, the noise growth frequency of the F-NTRU scheme is $\varphi(x)/d$ times of this scheme. Therefore, this scheme has a better performance in the noise management.

3.4.5. Multiplication Computation Optimization. As the noise depends mainly on the noise of the first ciphertext, changing the order of multiplication can optimize the homomorphic computation of the scheme. For example, there are 4 initial ciphertexts denoted as c_1, c_2, c_3 , and c_4 . The original order of computation is first calculate $c_5 = c_1 \cdot c_2$, then calculate $c_6 = c_3 \cdot c_4$, and then get the final ciphertext c_7 obtained by calculating $c_7 = c_5 \cdot c_6$. However, when the order of computation changes to first calculate $c_5 = c_1 \cdot c_2$, then calculate $c_6 = c_3 \cdot c_5$, and then get the final ciphertext c_7 obtained by calculating $c_7 = c_4 \cdot c_6$, the dependence on the noise of the multiplied ciphertext can be reduced because the noise growth of such schemes is asymmetric. For example, in the literature [31] when using the first computation order, the noise obtained after the calculation of the circuit with a depth of L is $(N+1)L \cdot E$. However, when the second computation order is used, the noise obtained after the same calculation is $(L \cdot N + 1) \cdot E$. The noise of the former grows exponentially, while the noise of the latter grows linearly; therefore, changing the multiplication order can optimize the homomorphic computation of the scheme and reduce the noise growth rate of the homomorphic multiplication, which means that the latter computation order can meet the calculation of a circuit with a depth more than L for the same noise threshold. For details, see the literature [32].

3.5. Security Analysis

Theorem 3. Assume that $n = d^v, d$, and $q \geq 8n$ are prime numbers, and $q \equiv 1 \pmod{n}$ is met. When $r \geq \varphi(n) \sqrt{(2\ln(6)/\pi) \cdot q^{1/\varphi(n)}}$, there exists a probability of $1 - n^{-\omega(1)}$ that f and g meet the following formulas:

$$\|f\| \leq \omega(\sqrt{nlm}) \cdot \|p\|r, \quad (20)$$

$$\|g\| \leq \omega(\sqrt{lnm}) \cdot r. \quad (21)$$

The security of this scheme at this time only relies on the RLWE (Φ, n, q, χ) assumption.

Proof. When f and g meet the above situation, there exists a probability of $1 - n^{-\omega(1)}$ that formulas (20) and (21) can be established [21]. For polynomial f' , same parameters also apply to the formula $f = p \cdot f' + 1$, that is, there exists a probability of $1 - n^{-\omega(1)}$ that $f \leq p \cdot f' + 1 \leq \omega(\sqrt{n \ln n}) \cdot p$. Combining Theorem 4, we can get that there exists a probability of $1 - n^{-\omega(1)}$ that $f \leq 1 + 2\sqrt{\varphi(n)}pf' \leq \omega(\sqrt{n \ln n}) \cdot pr$. For a power-of-two cyclotomic ring and a power-of-prime cyclotomic ring, we already prove that, in normal cases, polynomial f, g, h have a relatively smaller value. Therefore, sample f and g with a certain width of r ,

and make the public key h distribute uniformly when its norm growth does not affect a single homomorphic multiplication operation. Combining the inverse property, we can get that the inverses of f, g, f^{-1} , and g^{-1} that belong to R_q . Therefore, we get the following formula:

$$\frac{g}{f} = g \cdot f^{-1}. \quad (22)$$

In the DSPR assumption, $h = 2g/f$ can be changed to $2h'$. In the RLWE (Φ, n, q, χ) assumption, $c^* = hs + 2e + m$ can be changed to $c^* = u + m$. In $c^* = hs + 2e + m$, the value range of e is very small and can be ignored. Combining formula (22), we can convert the form of fraction in the DSPR assumption to the form of multiplication in the RLWE (Φ, n, q, χ) assumption. Therefore, the security of this scheme can be reducible over the RLWE (Φ, n, q, χ) assumption. $\square$

Theorem 4. Assume that λ is a security parameter, L is the number of layers of a circuit, and n is a dimension and a power of a prime number. Let $R = \mathbb{Z}[x]/\Phi_n(x)$. Under the prerequisite of RLWE (Φ, n, q, χ) assumption, this scheme is secure against IND-CPA attacks.

Proof. The following adopts the game hopping method to prove. In the formulas, $\text{Adv}_{\text{IND-CPA}}(A)$ indicates the advantage of attacker A in the Game.

Game 0: standard IND-CPA game, that is, the challenger invokes the KeyGen algorithm of the scheme and makes attacker A get the generated public key pk . A has the capability of accessing the oracle machine for encryption. The challenger outputs the ciphertext $c = \text{Enc}_{pk}(m_b)$, and attacker A tries to distinguish the plaintexts corresponding to c . In $m_b, b \in (0, 1)$, Game 0 the advantage of attacker A is

$$\text{Adv}_{\text{IND-CPA}}(A) = \left| \frac{\Pr[A(pk, \text{Enc}_{pk}(m_0 = 1))]}{-\Pr[A(pk, \text{Enc}_{pk}(m_1 = 1))]} \right|. \quad (23)$$

Game 1: the difference between Game 1 and Game 0 is the method to generate a public key. In Game 1, public key pk is not sampled from the Gaussian distribution with regular embedding and a private key sk . But it is directly selected at random in a uniform way from R_q^* . It can be obtained from Definition 3 that the result generated from the discrete Gaussian distribution cannot be distinguished from the distribution probability of R_q^* . It can be seen from the literature [33] that the error between the result generated from the discrete Gaussian distribution and the distributed result of R_q^* is within $2^{-\Omega(n)}$. Therefore, we get the following formula:

$$|\text{Adv}_{\text{Game1}}(A) - \text{Adv}_{\text{IND-CPA}}(A)| \leq 2^{-\Omega(n)}. \quad (24)$$

Game 2: the difference between Game 2 and Game 1 is that the encryption algorithm of Game 2 is not performed according to the scheme, but is randomly selected in a uniform way from $\{0, 1\}$. From Theorem 3, we can get that the DSPR (Φ, n, q, χ) assumption in this scheme has been reducible over RLWE (Φ, n, q, χ) . Therefore, in Game 2 and Game 1, the advantage difference of attacker A lies in the solution to the RLWE (Φ, n, q, χ) problem:

$$|\text{Adv}_{\text{Game2}}(A) - \text{Adv}_{\text{Game1}}(A)| \leq \text{RLWE}(\Phi, n, q, \chi) \text{Adv}(A). \quad (25)$$

Game 3: in Game 3, the ciphertext c given by the challenger is no longer generated by the encryption algorithm. It is selected randomly in a uniform way from $\{0, 1\}$. The security analysis of Game 3 is the same as Game 2. We get the following formula:

$$|\text{Adv}_{\text{Game3}}(A) - \text{Adv}_{\text{Game2}}(A)| \leq \text{RLWE}(\Phi, n, q, \chi) \text{Adv}(A). \quad (26)$$

In Game 3, the public key pk and ciphertext c given by the challenger are all random, which are not related to plain text $m_b, b \in (0, 1)$. Therefore, attacker A has no advantage in Game 3 that means

$$\text{Adv}_{\text{Game3}}(A) = 0. \quad (27)$$

From formulas (23)–(27), we can get

$$\begin{aligned} \text{Adv}_{\text{IND-CPA}}(A) &\leq 2^{-\Omega(n)} + \text{RLWE}(\Phi, n, q, \chi) \text{Adv}(A) \\ &\quad + \text{RLWE}(\Phi, n, q, \chi) \text{Adv}(A). \end{aligned} \quad (28)$$

Above all, in the RLWE (Φ, n, q, χ) assumption, $\text{RLWE}(\Phi, n, q, \chi) \text{Adv}(A)$ can be ignored, which meets the requirement of Definition 5. Therefore, this scheme is secure against IND-CPA attacks. $\square$

4. Performance Analysis

In this section, the proposed scheme and the F-NTRU scheme are analyzed to show the advantages of the proposed scheme in terms of ciphertext size and homomorphic computational complexity.

4.1. Ciphertext Size Analysis. The ciphertext of the F-NTRU scheme consists of two polynomials whose number of times is less than 2^n , and the ciphertext extension is in a matrix form of $\lceil \log q \rceil \cdot \lceil \log q \rceil$. From Theorem 3, we can get that the upper bound of the size is $\lceil \log q \rceil^2 \cdot n \cdot \log q^2$. The public key used by the F-NTRU scheme consists of two polynomials, and the size is $n \cdot \log q^2$. During decryption, a polynomial private key has the number of times less than 2^n and coefficient less than $(2B + 1)$, and the size is $\log(2B + 1)$. In this scheme, the ciphertext is a polynomial in a form of a dimension vector $\log q$. It can be deduced from Theorem 4 that the ciphertext size of this scheme is $2\lceil \log q \rceil \cdot \sqrt{\varphi(n)} \cdot \log q^2$. The cyclotomic polynomial of the public key and private key of the scheme in this paper is different from that of the F-NTRU scheme. Therefore, the sizes of the public key and private key in this scheme are changed and are $2\varphi(n) \cdot \log q^2$ and $\log(2B + 1)$, respectively, compared with the F-NTRU scheme. The details are shown in Table 1.

As can be seen from Table 1, compared with the F-NTRU scheme, this scheme optimizes the public key size while keeping the private key size unchanged. The ciphertext size of this scheme is reduced from quadratic to

TABLE 1: Comparison of the size of ciphertext.

Scheme	Ciphertext size	Public key size	Private key size	Polynomial
F-NTRU	$\lceil \log q \rceil^2 \cdot n \cdot \log q^2$	$n \cdot \log q^2$	$\log(2B + 1)$	$\Phi_n(x) = x^n + 1$
Scheme in this paper	$2\lceil \log q \rceil \cdot \sqrt{\varphi(n)} \cdot \log q^2$	$2\varphi(n) \cdot \log q^2$	$\log(2B + 1)$	$\Phi_n(x) = \Phi_d(x^{d^{n-1}})$

TABLE 2: Comparison of computational complexity.

Scheme	Ciphertext	Communication volume (pieces)	Computational volume for addition operations	Computational volume for multiplication operations
F-NTRU	$2\varphi(x)/d$	$2\varphi(x)/d$	$\varphi(x)/d \cdot l \cdot T_{\text{add}}$	$\varphi(x)/d \cdot l \cdot l \cdot T_{\text{mult}}$
Scheme in this paper	$2\varphi(x)/d$	2	T_{add}	$l \cdot T_{\text{mult}}$

cubic, which gains more advantages in storage and transmission.

4.2. Computational Complexity Analysis. Assume that the time for performing a vector addition operation is T_{add} and for performing a vector multiplication operation is T_{mult} . In the F-NTRU scheme, performing a homomorphic addition operation $(C' + C'')$ is equivalent to performing l times of vector addition operations and performing a homomorphic multiplication operation $C' \cdot C''$ is equivalent to performing $l \times l$ times of vector multiplication operations. However, in this scheme, performing a homomorphic addition operation $(C' + C'')$ is equivalent to performing one single vector addition operation and performing a homomorphic multiplication operation $\text{BitDecomp}(c') \cdot c''$ is equivalent to performing l times of vector multiplication operations. Because in the $\text{BitDecomp}(c')$ matrix form of $\text{BitDecomp}(c') \cdot c''$, c'' is in a form of a vector. The computational volume of the matrix calculation and a column vector operation actually equal l times of vector multiplication operations. In addition, in this scheme, multiple plaintexts are packed into one ciphertext using the Chinese remainder theorem for parallel processing, which effectively improves the computational efficiency. For details, see Table 2:

From Table 2, it can be seen that this scheme improves the efficiency by a factor of $l + 1$ by changing the ciphertext to a form of a vector. The adoption of the batch processing technique also helps enhance the computational efficiency by a factor of $\varphi(x)/d + 1$. Therefore, in terms of efficiency, this scheme overall improves by a factor of $l\varphi(x)/d + 1$ compared with the F-NTRU scheme. In terms of communication cost, the plaintext space in this scheme is divided into $\varphi(x)/d$ plaintext slots, which has lower communication cost and computational cost. Normally, matrix-vector multiplication is $O(l^2)$ order of magnitude faster than matrix multiplication, but since this scheme does not use the flattening technique to binarize the ciphertexts, the multiplication operation of values is slower than that of binarized values. Fortunately, the actual time spent in computing a large number of products of matrix vectors (value 0) is greatly reduced. This is a major breakthrough in terms of efficiency after the matrix multiplication is replaced with the matrix-vector multiplication in this scheme.

5. Conclusion

To solve the problems of constructing fully homomorphic encryption schemes using approximate eigenvectors, this paper proposes an NTRU-based fully homomorphic encryption scheme based on a power-of-prime cyclotomic ring. This scheme can eliminate the DSPR assumption under certain conditions so that the scheme only relies on the RLWE assumption and can also be secure against IND-CPA attacks. The ciphertext of this scheme is in a form of a vector, and the use of matrix-vector multiplication operations instead of complex matrix multiplication operations effectively improves the efficiency of the scheme. Meanwhile, the noise growth decreases quadratically. Combining the multiplication execution order optimization method, the scheme performs better in noise management. Compared with the F-NTRU scheme, the ciphertext of this scheme has obvious advantages in storage, transportation, and computation, but the reduction in the number of times to decompose polynomial mods using the Chinese remainder theorem in this scheme affects the security of the RLWE (Φ, n, q, χ) assumption. Therefore, security parameters need to be selected more stringently in order to ensure the data security.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was one of the phased achievements of the project supported by the National Natural Science Foundation of China (Grant no. 62062009).

References

- [1] L. Ruiqi and J. Chunfu, "A multi key homomorphic encryption scheme based on NTRU," *Acta Cryptologica Sinica*, vol. 7, no. 05, pp. 683–697, 2020.
- [2] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Annual International Conference on the Theory and Applications of*

- Cryptographic Techniques*, pp. 24–43, Springer, French Riviera, May 2010.
- [3] G. C. Brakerski and V. Vaikuntanathan, “(Leveled) fully homomorphic encryption without bootstrapping,” in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pp. 309–325, New York, NY, USA, January 2012.
 - [4] J. W. Bos, K. Lauter, J. Loftus et al., “Improved security for a ring-based fully homomorphic encryption scheme,” in *Proceedings of the IMA International Conference on Cryptography and Coding*, p. 4564, Springer, Oxford, UK, December 2013.
 - [5] F. Hu, K. Wilhelm, M. Schab, M. Lukowiak, S. Radziszowski, and Y. Xiao, “NTRU-based sensor network security: a low-power hardware implementation perspective,” *Security and Communication Networks*, vol. 2, no. 1, pp. 71–81, 2009.
 - [6] Q. Xiaoyue and H. Ruwei, “Research on the homomorphic encryption of NTRU system,” *Computer Application Research*, vol. 2021, Article ID 0, 8 pages, 2021.
 - [7] D. Wang and P. Wang, “Two birds with one stone: two-factor authentication with security beyond conventional bound,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.
 - [8] S. Qiu, D. Wang, G. Xu, and S. Kumari, “Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices,” *IEEE Transactions on Dependable and Secure Computing*, vol. 30, 2020.
 - [9] C. Gentry, A. Sahai, and B. Waters, “Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based,” *Advances in Cryptology-Crypto 2013*, vol. 41, pp. 75–92, 2013.
 - [10] L. Xengpeng, M. Chunguang, and Z. Hongsheng, “Research on holomorphic encryption,” *Acta Cryptologica*, vol. 4, no. 6, pp. 561–578, 2017.
 - [11] Y. Dorz and B. Sunar, “Flattening NTRU for evaluation key free homomorphic encryption,” *Journal of Mathematical Cryptology*, vol. 14, no. 1, 2016.
 - [12] Z. C. Li, J. M. Zhang, Y. T. Yang et al., “A fully homomorphic encryption scheme based on NTRU,” *ACTA Electronica Sinica*, vol. 46, no. 4, pp. 938–944, 2018.
 - [13] A. Khedr and G. Gulak, “SecureMed: secure medical computation using GPU-accelerated homomorphic encryption scheme,” *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 2, pp. 597–606, 2018.
 - [14] M. Albrecht, S. Bai, and L. Ducas, “A subfield lattice attack on overstretched NTRU assumptions,” in *Proceedings of Annual Cryptology Conference*, pp. 153–178, Springer, Santa Barbara, CA, USA, August 2016, Cham.
 - [15] J. H. Cheon, J. Jeong, and C. Lee, “An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero,” *LMS Journal of Computation and Mathematics*, vol. 19, pp. 255–266, 2016.
 - [16] N. P. Smart and F. Vercauteren, “Fully homomorphic SIMD operations,” *Designs, Codes & Cryptography*, vol. 71, no. 1, pp. 57–81, 2014.
 - [17] V. Migliore, G. Bonnoron, and C. Fontaine, “Practical parameters for somewhat homomorphic encryption (she) schemes on binary circuits,” *IEEE Transactions on Computers*, vol. 2018, Article ID 2808962, 1 page, 2018.
 - [18] Y. Doröz, Y. Hu, and B. Sunar, “Homomorphic AES evaluation using the modified LTV scheme,” *Designs, Codes and Cryptography*, vol. 80, no. 2, 2016.
 - [19] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, “On-the fly multiparty computation on the cloud via multikey fully homomorphic encryption,” in *Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, pp. 1219–1234, New York, NY, USA, May 2012.
 - [20] Y. Yu, G. Xu, and X. Wang, “Provably secure NTRU instances over prime cyclotomic rings,” in *Proceedings of the IACR International Workshop on Public Key Cryptography*, Amsterdam, Netherlands, March 2017.
 - [21] D. Stehlé and R. Steinfeld, *Making NTRU as Secure as Worst-Case Problems over Ideal Lattices*, Springer-Verlag, Berlin, Germany, 2011.
 - [22] H. N. Rudolf Lidl and F. M. Cohn, *Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.
 - [23] Z. Haonan, L. Ningbo, C. Xiaoliang, and Y. Xiaoyuan, “Multi key holomorphic scheme based on prime power order cyclotomic polynomial ring,” *Information Network Security*, vol. 20, no. 5, pp. 83–87, 2020.
 - [24] C. Xiaoliang, Z. Haonan, Z. Tanping, L. Ningbo, and Y. Xiaoyuan, “Decryption structure of multi key homomorphic encryption scheme based on public key cryptosystem,” *Computer Application*, vol. 41, pp. 1–7, 2021.
 - [25] D. D. Stebila, “An introduction to provable security,” 2021.
 - [26] C. Yinlan, “Cyclotomic polynomials over finite fields,” *Journal of Hubei Normal University*, vol. 32, no. 2, pp. 1–5, 2012.
 - [27] V. Lyubashevsky, C. Peikert, and O. Regev, “On ideal lattices and learning with errors over rings,” in *Proceedings of the 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, French Riviera, May 2010.
 - [28] J. H. Cheon, J. Kim, M. S. Lee et al., “CRT-based fully homomorphic encryption over the integers,” *Information Sciences*, vol. 310, pp. 149–162, 2015.
 - [29] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption,” in *Proceedings of the 44th symposium on Theory of Computing*, pp. 1219–1234, New York, NY, USA, May 2012.
 - [30] J. Hoffstein and J. Silverman, “Optimizations for NTRU,” in *Proceedings of the Public Key Cryptography & Computational Number Theory*, Warsaw, Poland, September 2000.
 - [31] C. Gentry, C. Peikert, and V. Vaikuntanathan, “How to use a short basis: trapdoors for hard lattices and new cryptographic constructions,” in *Proceedings of the STOC*, pp. 197–206, Springer-Verlag, Victoria, TX, USA, May 2008.
 - [32] C. Zhigang and Z. Guomin, “NTRU type fully homomorphic encryption scheme without key exchange L,” *Journal of Network and Information Security*, vol. 3, no. 1, pp. 39–45, 2017.
 - [33] V. Lyubashevsky, C. Peikert, and O. Regev, “A toolkit for ring-LWE cryptography,” in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Athens, Greece, May 2013.