


Article

Efficient SMC Protocol Based on Multi-Bit Fully Homomorphic Encryption

Zong-Wu Zhu  and Ru-Wei Huang *

School of Computer and Electronic Information, Guangxi University, Nanning 530004, China;
zongwuzhu@st.gxu.edu.cn

* Correspondence: ruweih@gxu.edu.cn

Abstract: Aiming at the problems of large ciphertext size and low efficiency in the current secure multi-party computation (SMC) protocol based on fully homomorphic encryption (FHE), the paper proves that the fully homomorphic encryption scheme that supports multi-bit encryption proposed by Chen Li et al. satisfies the key homomorphism. Based on this scheme and threshold decryption, a three-round, interactive, leveled, secure multi-party computation protocol under the Common Random String (CRS) model is designed. The protocol is proved to be safe under the semi-honest model and the semi-malicious model. From the non-interactive zero-knowledge proof, it can be concluded that the protocol is also safe under the malicious model. Its security can be attributed to the Decisional Learning With Errors (DLWE) and a variant of this problem (some-are-errorless LWE). Compared with the existing secure multi-party computation protocol based on fully homomorphic encryption under the CRS model, the ciphertext size of this protocol is smaller, the efficiency is higher, the storage overhead is smaller, and the overall performance is better than the existing protocol.

Keywords: fully homomorphic encryption; secure multi-party computation; multi-bit encryption; threshold decryption; decisional learning with errors



Citation: Zhu, Z.-W.; Huang, R.-W. Efficient SMC Protocol Based on Multi-Bit Fully Homomorphic Encryption. *Appl. Sci.* **2021**, *11*, 10332. <https://doi.org/10.3390/app112110332>

Academic Editor: Arcangelo Castiglione

Received: 7 September 2021

Accepted: 31 October 2021

Published: 3 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

As cloud computing develops rapidly, the problem of user privacy data security has become increasingly prominent. Fully Homomorphic Encryption (FHE) has just solved the problem of data privacy computing. Fully homomorphic encryption was first proposed by Rivest et al. [1] in 1978, which could perform various meaningful calculations on ciphertext without knowing the key. In other words, for any plain-text m and function f , there is $f(Enc(m)) = Enc(f(m))$. Since Gentry et al. [2] proposed the first fully homomorphic encryption scheme in 2009, many fully homomorphic encryption schemes such as BV11 [3], BGV12 [4], Bra12 [5], GSW13 [6], and CKKS17 [7] have appeared in recent years. Fully homomorphic encryption can be used as a building block of a secure multi-party computation (SMC) protocol and shows good potential in the design of a secure multi-party computation protocol. In addition, the concept of secure multi-party computation originated from the millionaire problem proposed by Yao [8], which is characterized by allowing multiple parties to jointly calculate a certain function to obtain the result without private data being leaked out.

Nowadays, domestic and international scholars have carried out much research on the secure multi-party computation protocol based on the fully homomorphic encryption scheme. In 2012, López-Alt et al. [9] proposed the concept of Multi-Key Fully Homomorphic Encryption (MFHE). Based on the improved NTRU scheme [10], an MFHE scheme was constructed, which can operate the input encrypted under multiple unrelated keys, but the complexity is too high. In 2016, based on the Learning With Errors (LWE) assumption, Mukherjee et al. (MW16 scheme) [11] implemented a multi-key secure multi-party computation protocol with only two rounds of interaction under the CRS model, achieving the best interaction rounds, but the ciphertext matrix was too large. In 2017, Wang et al. [12]

constructed a simple three-round, leveled, multi-key, secure multi-party computation protocol under the CRS model based on the GSW13 scheme. Compared with the MW16 scheme, although an additional round of interaction was added, the complexity of encryption and decryption was low, and the ciphertext expansion rate was small, which did not require a running key. In 2018, due to the problem that the secure multi-party computation protocol under the CRS model weakened the user's ability to independently generate their own keys, Kim et al. (KLP18 scheme) [13] constructed a three-round, secure, multi-party computation protocol without CRS. The protocol was safe against semi-malicious opponents, but it could not fight against completely malicious opponents. In 2020, Tang et al. [14] improved the ciphertext extension method of the KLP18 scheme with the help of the coding operation in Li's scheme [15] and designed a three-round, secure, multi-party computation protocol based on MFHE without the CRS model, improving the efficiency and reducing decryption noise, but it still could not prove that it was safe in a fully malicious environment. In 2021, Tang et al. [16] proved the key homomorphism of the multi-bit fully homomorphic encryption scheme proposed by Li [17]. Moreover, based on this scheme, a three-round, secure, multi-party computation protocol that could support multi-bit encryption under the CRS model was designed, which further reduced the complexity of the NAND gate.

It can be seen from the above related work that although the secure multi-party computation protocol under the CRS-free model allows MFHE users to independently generate their own keys, the secure multi-party computation protocol under this model is not secure enough to resist completely malicious adversaries. What is more, nowadays, the fully homomorphic encryption-based secure multi-party computation protocol under the CRS model has problems such as large ciphertext size and insufficient efficiency. Therefore, to solve the problems mentioned above, a three-round secure multi-party computation protocol that can resist malicious opponents under the CRS model is designed in this paper with the help of the New Fully Homomorphic Encryption (NFHE) scheme [18] and threshold decryption. This protocol supports multi-bit encryption. In addition, compared with the existing secure multi-party computation protocol under the CRS model, the ciphertext size of the protocol is smaller, and the overall performance is better than the existing protocol.

2. Preliminaries

2.1. Symbolic Representation

In this paper, \mathbb{Z} , \mathbb{R} , and \mathbb{Z}_q respectively represent the integer set, real number set, and integer modulo q residual ring. Bold italic lowercase letters represent vectors, and bold italic uppercase letters refer to matrices. Moreover, the length of the n -dimensional

vector a is defined as its Euclidean norm $\|a\| = \sqrt{\sum_{i=0}^{n-1} a_i^2}$, and the length of the vector set S is defined as $\|S\| = \max_{a \in S} \|a\|$. $a \leftarrow D$ means randomly selecting variable a from probability distribution D , and $a \xleftarrow{R} U$ means randomly and uniformly selecting variable a from set U . Vector $a \in \mathbb{Z}_q^n$ can be expressed as $a = (a_0, \dots, a_{n-1})$. The polynomial $b \in R_q$ can be expressed as $b = (b_0, \dots, b_{n-1}) \cdot c_i$ represents the i -th row of the matrix C , I_n is the n -dimensional identity matrix, and $\varphi(y)$ refers to the probability $Pr[y \leq x | y \sim N(0, 1)]$. In addition, for the polynomial $b, c \in R$, $b \times c = bc \bmod (x^n + 1)$ can be defined.

In this paper, the logarithmic function \log is based on 2, except that the basis is specified. O and o represent the complexity of the calculation. At the same time, for variable σ and any constant c , if $f(\sigma) = O(\sigma^c)$, then $f(\sigma)$ can be expressed as $\text{poly}(\sigma)$. If there is $f(\sigma) = o(\sigma^{-c})$, then $f(\sigma)$ can be expressed as $\text{negl}(\sigma)$, which is called a negligible function of σ .

2.2. Definitions and Theorems

Definition 1. ([19]) (Learning With Errors, LWE) For the vector $s \in \mathbb{Z}_q^n$, the LWE distribution $A_{s,\chi}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ refers to uniformly selecting $a \in \mathbb{Z}_q^n$ at random, selecting the error $e \leftarrow \chi$, and outputting $(a, b = a \cdot s + e \bmod q)$.

Definition 2. (Search.LWE $_{m,n,q,\chi}$) For vectors $s \in \mathbb{Z}_q^n$, s is recovered from the given m independent samples $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ selected from the distribution of $A_{s,\chi}$.

Definition 3. (Decision.LWE $_{m,n,q,\chi}$) For vector $s \in \mathbb{Z}_q^n$, the attacker is required to distinguish two sets of random variables containing m independent samples with non-negligible advantage. The two sets of variables are taken from the uniform distributions on distributions $A_{s,\chi}$ and $\mathbb{Z}_q^n \times \mathbb{Z}_q$, respectively.

Definition 4. (Some-are-errorless LWE) for $q \geq 1$, $n > 0$, the error distribution on R is χ' , $T_q = \{0, \frac{1}{q}, \dots, \frac{q-1}{q}\}$, where $q \in \mathbb{Z}$. The distribution $A'_{s,\chi}$ on $T_q^n \times T_q$ refers to uniformly selecting $a \in T_q^n$, selecting the error $e \leftarrow \chi'$, and outputting $(a, b = a \cdot s + e)$. Some-are-errorless LWE distinguishes the following two situations.

- (1) Select all samples uniformly from $T_q^n \times T_q$.
- (2) For the vector $s \in T_q^n$, the previous sample is selected from $A'_{s,0}$. All the remaining samples are selected from $A'_{s,\chi}$. In other words, the previous sample is $(a_i, b = a_i \cdot s)$, and no error e is introduced. The remaining samples are $(a_i, b = a_i \cdot s + e_i)$, $i > 1$, and each sample introduces a small error e_i .

Definition 5. Secure multi-party computation. The general formal definition of an SMC agreement [9] can be described as follows. It is assumed that there are N participants $\{P_1, P_2, \dots, P_N\}$, and $x_i (i \in [N])$ is the private data owned by each participant P . In addition, all participants jointly calculate a certain effective function $y = f(x_1, x_2, \dots, x_N)$. After the calculation, each P_i can obtain y but cannot obtain the private data of other participants.

Theorem 1. If $\alpha_i (i \in [N])$ is a series of independent random variables that obey a bounded distribution of B_χ , then the random variable $\alpha = \frac{1}{N} \sum_{i=1}^N \alpha_i$ also obeys the bounded distribution of B_χ .

Proof. Suppose $E(\alpha_i) = \frac{B_\chi}{\text{poly}(\sigma)}$, according to Markov inequality,

$$\begin{aligned} \Pr\{|\alpha| > B_\chi\} &\leq \frac{E(|\alpha|)}{B_\chi} = \frac{1}{N \cdot B_\chi} E\left(\sum_{i=1}^N \alpha_i\right) \\ &= \frac{1}{\text{poly}(\sigma)}. \text{ So, the conclusion holds.} \\ \text{End. } \square \end{aligned}$$

2.3. Secure Multi-Party Computation Model

(a) Semi-honest model: All participants will strictly abide by the agreement and will not actively change the agreement or data. However, intermediate calculation results may be retained and used to calculate the private data of other participants.

(b) Semi-malicious model: The adversary can decide whether to faithfully execute the original agreement based on the input and a certain degree of randomness.

(c) Malicious model: All computing participants can tamper with or leak the agreement and data at will, and even prevent the normal execution of the agreement.

3. Efficient Fully Homomorphic Encryption Scheme

This scheme is an improved NFHE scheme based on GSW13 in reference [18], and the structure of the scheme is as follows. The modulus q and the dimension N are settled, and the ciphertext C is an $N \times N$ -dimensional matrix defined on \mathbb{Z}_p . In addition, each component

of the matrix is much smaller than q . The private key sk of C is an N -dimensional vector defined on \mathbb{Z}_p . Let the plain-text μ be a small integer. When $C \cdot sk = \mu \cdot sk + e$, C is called the ciphertext of μ , where e is the small error vector. In the decryption process, first extract the i -th row C_i of C , then calculate $x \leftarrow \langle C_i, sk \rangle = \mu \cdot sk_i + e_i$, and finally output $\mu = \lfloor x / sk_i \rfloor$, where sk_i is the i -th element of sk , e_i is the i -th element of e , and $i \in [0, N - 1]$. The message μ can be regarded as an eigenvalue of the ciphertext matrix C , and the private key sk is the approximate eigenvector of C corresponding to the eigenvalue μ .

The structure of the scheme is as follows. First of all, defining functions such as $mbDpt(a)$, $mbDpt^{(-1)}(a')$, $mbFlatten(a')$, and $pofmb(b)$, the expansion method of the NFHE scheme is given. Then, based on the above functions, the five polynomial time algorithms included in the NFHE program are designed, namely the key generation algorithm $NFHE.Keygen(n, q)$, the encryption algorithm $NFHE.Encrypt(pk, \mu)$, the decryption algorithm $NFHE.Decrypt(sk, C)$, the homomorphic addition algorithm $NFHE.Add(C_1, C_2)$, and the homomorphic multiplication algorithm $NFHE.Mult(C_1, C_2)$.

Let a and b be vectors on \mathbb{Z}_q^k . k is a positive integer, q is a modulus, and p is a power of 2. $t = \lceil \log_p q \rceil$, and $N = kt$. The definition of each function is shown in the following formula.

$$mbDpt(a) = a' = (a_{1,1}, \dots, a_{1,t}, \dots, a_{k,1}, \dots, a_{k,t}) \in \mathbb{Z}_p^N$$

where a' is an N -dimensional vector, $a_i = \sum_{j=1}^t a_{i,j} p^{j-1}$, $a_{i,j} \in \mathbb{Z}_p$.

$$mbDpt^{(-1)}(a') = \left(\sum p^j \cdot a_{1,j}, \dots, \sum p^j \cdot a_{k,j} \right)$$

$$mbFlatten(a') = mbDpt(mbDpt^{(-1)}(a'))$$

$$pofmb(b) = (b_1, pb_1, \dots, p^{t-1}b_1, \dots, b_k, pb_k, \dots, p^{t-1}b_k)$$

- Key generation algorithm $NFHE.Keygen(n, q)$. For a positive integer n , the depth of the homomorphic operation is l . Randomly and uniformly select $A \xleftarrow{R} \mathbb{Z}_q^{n \times n}$ from $\mathbb{Z}_q^{n \times n}$, and sample s from the discrete Gaussian distribution $\chi^{n \times 1}$ on $\mathbb{Z}^{n \times 1}$. In addition, $e \leftarrow \chi^n$. The public key is $pk = (A, b = A \cdot s + e) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n$, and the private key is $sk = \begin{pmatrix} -s \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$.
- Encryption algorithm $NFHE.Encrypt(pk, \mu)$. For the plain-text $\mu \in \{0, 1\}$ to be encrypted, randomly selecting r_i , $e_{i,1} \leftarrow \chi^n$ and $e_{i,2} \leftarrow \chi$, $i = 1, \dots, (n+1) \cdot t$, calculate $C_{i,1} = A^T \cdot r_i + e_{i,1} \in \mathbb{Z}_q^n$ and $C_{i,2} = b^T \cdot r_i + e_{i,2} \in \mathbb{Z}_q$. Among them, e_{ij} is the j -th element of e_i , and C_{ij} is the j -th element of C_i . Let C' be a matrix formed by arraying $m = (n+1) \cdot t$ ciphertexts as column vectors, whose dimension is $(n+1) \times m$. Output ciphertext $C = mbFlatten(\mu \cdot I_N + mbDpt(C')) \in \mathbb{Z}_p^{m \times m}$.
- Decryption algorithm $NFHE.Decrypt(sk, C)$. For ciphertext $C \in \mathbb{Z}_p^{m \times m}$ and private key $sk = \begin{pmatrix} -s \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$, let $s' = pofmb(sk)$, and calculate and output plain-text $\mu = \lfloor \langle s', C_{m-1} \rangle / (q/2p) + \frac{1}{2} \rfloor \bmod 2$.
- Homomorphic addition algorithm $NFHE.Add(C_1, C_2)$. Input the ciphertext C_1 and C_2 , and output the new ciphertext $C = mbFlatten(C_1 + C_2)$ obtained after homomorphic addition.

Homomorphic multiplication algorithm $NFHE.Mult(C_1, C_2)$. Input the cipher-text C_1 and C_2 , and output the new ciphertext $C = mbFlatten(C_1 \cdot C_2)$ obtained after homomorphic multiplication.

3.1. The Correctness of the Scheme

First, correctly analyze the homomorphic addition and multiplication of the scheme. For the homomorphic addition, there will be $C = \text{mbFlatten}((\mu_1 + \mu_2) \cdot I_N + \text{mbDmp}(C_1 + C_2))$ and $\text{NFHE.Dec}(sk, C) = (\mu_1 + \mu_2) \bmod 2$. After homomorphic addition is performed on each scheme, the noise will not exceed twice the original ciphertext. For homomorphic multiplication, there will be $C \cdot sk = \mu_1 \cdot \mu_2 \cdot sk + \mu_2 \cdot e_1 + C_1 \cdot e_2$ and $\text{NFHE.Dec}(sk, C) = \mu_1 \cdot \mu_2$ (e_1 and e_2 refers to the noise in ciphertext C_1 and C_2). Since the coefficient of μ_2 is $\{0, 1\}$, and the coefficient of C_1 is limited to \mathbb{Z}_p , the noise will not exceed $pN + 1$ times the original ciphertext after each homomorphic multiplication.

Theorem 2. For the NFHE scheme, L represents the maximum depth of the homomorphic operation circuit. In the case of no homomorphic operation, if C is the ciphertext obtained by encrypting 0, when $|\langle C_{m-1}, s' \rangle| < q / \left[4p(pN + 1)^L \right]$, the scheme will be correct.

Proof. According to the analysis of the correctness of homomorphic addition and multiplication, after each homomorphic operation, the noise does not exceed $pN+1$ times of the original ciphertext. Therefore, when $|\langle C_{m-1}, s' \rangle| < q / \left[4p(pN + 1)^L \right]$, after performing no more than L homomorphic operations, $|\langle C_{m-1}, s' \rangle| < q / (4p)$. According to the decryption algorithm, when $|\langle C_{m-1}, s' \rangle| < q / (4p)$, there is $\langle s', C_{m-1} \rangle / (q/2p) < 1/2$. Therefore, if the encrypted message is 0, then $\langle C_{m-1}, s' \rangle$ is closer to 0 than $q / (2p)$, $\mu = \lfloor \langle s', C_{m-1} \rangle / (q/2p) + 1/2 \rfloor \bmod 2 < \lfloor 1/2 + 1/2 \rfloor \bmod 2 = 0$. Otherwise, the situation is reversed, and the correctness of the scheme can be guaranteed.

For the ciphertext obtained by encrypting 0, there are

$$\langle C_{m-1}, s' \rangle = \langle r, s \rangle + e_{m-1,2} - \langle e_{m-1,1}, e \rangle$$

Therefore, as long as the appropriate parameter q is selected, the correctness can be satisfied by making it large enough. \square

3.2. Security of the Scheme

Theorem 3. Supposing that parameters $n = \text{poly}(\lambda)$ and $q = \text{poly}(\lambda)$ are the polynomials of the security parameter λ , if the attacker can distinguish the ciphertext of the NFHE scheme from the uniform distribution on $\mathbb{Z}_p^{m \times m}$ with a non-negligible advantage, the $\text{DLWE}_{q,n,2n+1,\chi}$ problem can also be solved. Therefore, if the problem is assumed to be difficult, then the NFHE scheme can achieve IND-CPA security.

The detailed proof can be found in reference [18].

3.3. Optimization Based on Multi-Bit Encryption

In the GSW13 scheme and the NFHE scheme, although the plaintext messages are all $\mu \in \{0, 1\}$, the GSW13 scheme cannot support multi-bit encryption under the condition that the system parameters remain unchanged [17]. In addition, the NFHE scheme adopts the following modifications to realize multi-bit encryption without changing system parameters.

Encryption Algorithm $\text{NFHE.Encrypt}(pk, \mu)$. For plain-text $\mu \in \mathbb{Z}_p$, uniformly select r_i , $e_{i,1} \leftarrow \chi^n$, $e_{i,2} \leftarrow \chi$, and $i = 1, \dots, (n+1) \cdot t$ at random. Calculate $C_{i,1} = A^T \cdot r_i + e_{i,1} \in \mathbb{Z}_q^n$ and $C_{i,2} = b^T \cdot r_i + e_{i,2} \in \mathbb{Z}_q$. Let C' be a matrix formed by arranging $m = (n+1) \cdot t$ ciphertexts as column vectors, the dimension of which is $(n+1) \times m$. Then output the ciphertext $C = \text{mbFlatten}(\mu \cdot I_N + \text{mbDpt}(C')) \in \mathbb{Z}_p^{m \times m}$.

Decryption algorithm $\text{NFHE.Decrypt}(sk, C)$. For ciphertext $C \in \mathbb{Z}_p^{m \times m}$ and private key $sk = \begin{pmatrix} -s \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$, let $s' = \text{pofmb}(sk)$, and calculate and output plain-text $\mu = \lfloor \langle s', C_{m-1} \rangle / (q/2p) + \frac{1}{2} \rfloor \bmod p$.

When not performing homomorphic operation, if the plain-text message is μ' , according to the encryption/decryption process, there will be $\mu = \left\lfloor \langle s', C_{m-1} \rangle / (q/2p) + \frac{1}{2} \right\rfloor \bmod p = \left\lfloor \mu' + e/(q/2p) + \frac{1}{2} \right\rfloor \bmod p$ after decryption. When $|e/(q/2p)| < 1/2$, there will be $\mu = \mu'$, which can be decrypted correctly. For homomorphic addition, there will be $C = \text{mbFlatten}((\mu_1 + \mu_2) \cdot I_N + \text{mbDpt}(C_1 + C_2))$ and $\text{NFHE.Dec}(sk, C) = (\mu_1 + \mu_2) \bmod p$. For homomorphic multiplication, there will be $C \cdot sk = \mu_1 \cdot \mu_2 \cdot sk + \mu_2 \cdot e_1 + C_1 \cdot e_2$ and $\text{NFHE.Dec}(sk, C) = \mu_1 \cdot \mu_2$. Therefore, it can be decrypted correctly.

After homomorphic multiplication, since the coefficients of μ_2 and C_1 are both limited to \mathbb{Z}_p , the noise does not exceed $pN + p$ times of the original ciphertext. Therefore, when performing multi-bit encryption, the noise limit of Theorem 2 becomes $|\langle C_{m-1}, s' \rangle| < q/\left[4p(pN + p)^L\right]$. In addition, due to $pN = pkt \gg p$, the effect of this change on modulus q can be ignored.

4. Key Homomorphism of NFHE Scheme

4.1. Definition of Key Homomorphism

It is assumed that $F : K \times X \rightarrow Y$ is a pseudo-random function (PRF) [20], and K is the key space, which has a group structure and satisfies a certain \oplus operation on the group. Besides, X is the plain-text space, and Y is the ciphertext space. If for any $k_1, k_2 \in K$ and $\xi \in X$, an effective algorithm can be found to calculate $F(k_1 \oplus k_2, \xi)$ from $F(k_1, \xi)$ and $F(k_2, \xi)$.

Now its definition is extended to multiple keys, assuming that the number of keys is N . For a public key encryption scheme E , if (pk_i, sk_i) is the effective public key or private key pair of the scheme, and for $pk = g(pk_1, pk_2, \dots, pk_N)$, $sk = g'(sk_1, sk_2, \dots, sk_N)$ can be found. (pk, sk) can also be the effective public key or private key pair of E and E is called the key pair homomorphic nature. Among them, g and g' are both effective computable functions. In particular, if both g and g' are sum (product/linear) functions, then E is said to have the property of key addition (multiplication/linear) homomorphism.

4.2. Proof of Key Homomorphism

In the NFHE scheme, $s \in \mathbb{Z}^{n \times 1}$, $sk = \bar{t} = \begin{pmatrix} -s \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$ is the private key, and $pk = \bar{K} = (A, b = A \cdot s + e) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n$ is the public key. Denote it as $pk = \bar{K} = \frac{1}{N} \sum_{i=1}^N \bar{K}_i$. If pk is used to encrypt the plain-text μ , $C = \text{mbFlatten}(\mu \cdot I_N + \text{mbDpt}(C')) = \text{mbFlatten}(\mu \cdot I_N + \text{mbDpt}(r \cdot K))$ is obtained.

$sk = \bar{t} = \frac{1}{N} \sum_{i=1}^N \bar{t}_i$ can be used to decrypt the ciphertext. In other words, if A remains unchanged, the scheme will satisfy the linear homomorphism of the key.

$$\begin{aligned} \text{Proof. } \bar{t}\bar{K} &= \frac{1}{N} \sum_{i=1}^N \bar{t}_i \cdot \frac{1}{N} \sum_{i=1}^N \bar{K}_i \\ &= \begin{pmatrix} -\frac{1}{N} \sum_{i=1}^N s_i \\ 1 \end{pmatrix} \begin{pmatrix} A, \frac{1}{N} \sum_{i=1}^N b_i \end{pmatrix} \\ &= \frac{1}{N} \sum_{i=1}^N e_i \approx 0 \end{aligned}$$

is right. Therefore, there is still $\bar{t}C = \text{mbFlatten}(\mu \cdot I_N + \text{mbDpt}(r \cdot \bar{K}))\bar{t} = \mu \cdot \bar{t} + r \cdot \bar{K} \cdot \bar{t} = \mu \cdot \bar{t} + r \cdot e = \mu \cdot \bar{t} + \bar{e}$. and $\bar{e} = r \cdot e$

Therefore, plain-text μ can be obtained by decryption according to the original scheme. Therefore, when A is unchanged, the scheme will satisfy the linear homomorphism of the key. \square

5. Secure Multi-Party Computation Protocol Based on NFHE Scheme

5.1. SMC Protocol Based on Leveled NFHE Scheme

The basic NFHE scheme in this paper is leveled, which can only carry out a limited number of homomorphic operations. Although this limitation can be removed by bootstrapping to achieve any number of homomorphic operations, most of the advantages of the scheme will also be destroyed. Therefore, an SMC protocol based on the leveled NFHE scheme can be constructed.

π_f : Under the CRS model, a protocol for safely computing a single-valued function f is constructed, which is always safe under the semi-honest model and the semi-malicious model. The details are as follows.

Preprocessing: Set parameter, ensuring that all participants share parameter settings. Choose a lattice dimension parameter n , where λ is the security parameter. Pick an error distribution χ and a modulus q , such that for $l = \lfloor \log q \rfloor + 1$, the some-are-errorless $LWE_{n,q,l,\chi}$ holds. Let $\bar{m} = n \cdot l$. A common random string matrix $A \xleftarrow{R} \mathbb{Z}_q^{n \times n}$ is selected.

Input: For $i \in [N]$, each participant P_i inputs private data $x_i \in \{0, 1\}$, then calculate the function $f(\{0, 1\}^N \rightarrow \{0, 1\})$. d is the circuit depth of f .

Round 1. For P_i , the following is operated.

- Generate $(pk_i, sk_i) \leftarrow \text{NFHE.Keygen}(n, q)$.
- Release the public key $\{pk_i\}_{i \in [N]}$.

Round 2. Each P_i receives the public key $\{pk_i\}_{i \in [N] \setminus \{i\}}$ of others and performs the following operations.

- Calculate the joint public key $pk = \bar{K} = \frac{1}{N} \sum_{i=1}^N \bar{K}_i$.
- pk is used to calculate ciphertext $C = \text{mbFlatten}(\mu \cdot I_N + \text{mbDpt}(C'))$ and publish ciphertext $\{C_i\}_{i \in [N]}$.

Round 3. Each party P_i receives the ciphertext $\{C_i\}_{i \in [N] \setminus \{i\}}$ of others and performs the following operations.

- Perform homomorphic operations.
- Perform threshold decryption. P_i selects a random vector $\gamma'_i \leftarrow \chi^{\bar{m}-l}$. Let $\gamma_i = (\gamma'_i, 0, \dots, 0) \in \chi^{\bar{m}}$, then calculate the partial decryption result $\eta_i = \bar{t}_i \cdot C + \gamma_i \in \mathbb{Z}_q^{\bar{m}}$. Finally, release η_i .

Output: Each participant P_i accepts others to decrypt $\{\eta_i\}_{i \in [N] \setminus \{i\}}$. Calculate

$\eta = \frac{1}{N} \sum_{i=1}^N \eta_i = \bar{t}C + \frac{1}{N} \sum_{i=1}^N \gamma_i = \bar{t}C + \gamma$, then calculate $v = \eta G^{-1}(w^T)$, where $G^{-1}(w^T)$ is a bit decomposition of w^T and $w = (0, 0, \dots, \lfloor \frac{q}{2} \rfloor)$. If the value of v is close to 0, then $\mu = 0$. If the value of v is close to $\lfloor \frac{q}{2} \rfloor$, then $\mu = 1$.

5.2. Correctness

The correctness of the agreement mainly depends on two aspects:

- a. It has been proven that it is right to use the NFHE scheme in the protocol, so it is only necessary to verify whether the parameters used are correct. Besides, it can be seen from this scheme that through setting the parameter mentioned above, the noise does not exceed $pN + p$ times of the original ciphertext after each homomorphic operation. Therefore, when $|\langle C_{m-1}, s' \rangle| < q / \left\lceil 4p(pN + p) \right\rceil^L$, if it does not exceed L homomorphic operations, $|\langle C_{m-1}, s' \rangle| < q / (4p)$, and the scheme can be decrypted correctly.
- b. The correctness of the encryption and decryption of the protocol mainly involves three issues. Upon analyzing the key homomorphism in the previous scheme, it can be seen that the key pair used in protocol π_f is effective. Besides, from Theorem 1, it can be seen that the joint error in protocol π_f also obeys B_χ bounded distribution. Then, prove the correctness of the protocol joint decryption.

Proof. According to $\eta = \frac{1}{N} \sum_{i=1}^N \eta_i = \bar{t}C + \frac{1}{N} \sum_{i=1}^N \gamma_i = \bar{t}C + \gamma$

$$\text{There is } \eta G^{-1}(w^T) = (\bar{t}C + \gamma)G^{-1}(w^T) \\ = \bar{t}CG^{-1}(w^T) + \gamma G^{-1}(w^T)$$

$$= \mu \left\lceil \frac{q}{2} \right\rceil + \left(\gamma'_1, \dots, \gamma'_{(\bar{m}-l)}, 0, \dots, 0 \right) G^{-1} \begin{pmatrix} 0 \\ \vdots \\ \left\lceil \frac{q}{2} \right\rceil \end{pmatrix} = \mu \left\lceil \frac{q}{2} \right\rceil$$

Since $G^{-1} \left\lceil \frac{q}{2} \right\rceil$ is a bit decomposition of $\left\lceil \frac{q}{2} \right\rceil$, the maximum decomposition length of $\left\lceil \frac{q}{2} \right\rceil$ is $\lfloor \log q \rfloor + 1$. Moreover, from $l = \lfloor \log q \rfloor + 1$, the maximum length of $G^{-1} \begin{pmatrix} \left\lceil \frac{q}{2} \right\rceil \\ \vdots \\ \left\lceil \frac{q}{2} \right\rceil \end{pmatrix}$ is l . Then, as the last l bits in γ are all 0, and the protocol can correctly perform joint decryption. \square

5.3. Security

5.3.1. In Semi-Honest Model

In the CRS model, the security of the protocol is based on the following issues.

- Under the above settings, the security of the NFHE solution can be attributed to the DLWE problem.
- In $\eta_i = \bar{t}_i \cdot C + \gamma_i$ and $\eta = \bar{t}C + \gamma$, the first l components in γ_i and γ obey the bounded distribution of B_χ , which implies that these two equations constitute two some-are-errorless LWE instances discussed in Section 2. Therefore, after each party announces its own η_i in Round 3, its private key and joint key will not be disclosed, and the protocol is safe under the semi-honest model.

5.3.2. In Semi-Malicious Model

To be easily expressed, $\rho_i = \eta_i G^{-1}(w^T) + \varepsilon_i = v_i + \varepsilon_i$ and $\varepsilon_i \leftarrow \chi$ are used to replace η_i as part of the decryption of P_i . If the ρ_i obtained by simulation is indistinguishable from the real ρ_i obtained by decrypting η_i , the η_i obtained by the simulation will be also indistinguishable from the real η_i .

Theorem 4. *If f is a computable function with N inputs and one output of a deterministic polynomial time (PPT), then the above protocol π_f can realize that f is safe when facing a semi-malicious adversary who happens to capture $N - 1$ participants.*

Proof. A PPT simulator S is constructed to target a semi-malicious adversary who has captured $N - 1$ users, and this static semi-malicious adversary is denoted as \mathbf{A} . P_h is assumed as the only honest party left. Simulator S performs the following operations on behalf of P_h .

In the second round, the simulator S uses 0 to replace the real input of the honest party P_h for encryption. Then the simulator S obtains the input and private keys of $N - 1$ captured parties from the “evidence tape”. These inputs are sent by S to an ideal machine to obtain the output y . Meanwhile, the ciphertext C that performed the homomorphic calculation can be obtained. Moreover, S calculates the simulated part to decrypt $\rho'_h \leftarrow S(y, C, h, \{sk_i\}_{i \in [N] \setminus \{h\}})$ for P_h , and the decryption results of the simulated part are published in the third round, instead of the real decryption.

A series of mixed attack games are used to prove that the real result and the simulated result cannot be distinguished, namely $IDEAL_{F,S,Z} \stackrel{\text{comp}}{\approx} REAL_{\pi,A,Z}$. Z represents a specific environment.

Game $REAL_{\pi,A,Z}$: In the real environment Z , there is a semi-malicious adversary who executes protocol π_f .

Game $HYB_{\pi,A,Z}$: Similar to game $REAL_{\pi,A,Z}$, the difference is that it is assumed that P_h obtains all the private keys $\{sk_i\}_{i \in [N] \setminus \{h\}}$ after the second round, and in the third round, the simulated part is used to decrypt $\rho'_h \leftarrow S(y, C, h, \{sk_i\}_{i \in [N] \setminus \{h\}})$ instead of the real decryption being released.

Game $IDEAL_{F,S,Z}$: Similar to game $HYB_{\pi,A,Z}$, except that in the second round, P_h uses 0 to replace the real input encryption and is released. \square

Lemma 1. $REAL_{\pi,A,Z} \stackrel{\text{stat}}{\approx} HYB_{\pi,A,Z}$

Proof. The difference between the two games is that the decryption ρ'_h of the real part of P_h is replaced by analog decryption ρ'_h . So, if $v = \mu \left\lceil \frac{q}{2} \right\rceil + e'$, its simulated decryption algorithm can be

$$\rho'_h = N\mu \left\lceil \frac{q}{2} \right\rceil + Ne' - \sum_{i \neq h} \bar{t}_i CG^{-1}(w^T) + \epsilon'_h = N\mu \left\lceil \frac{q}{2} \right\rceil + Ne' + \epsilon'_h - \sum_{i \neq h} v_i$$

where $e' \leftarrow \chi$, $\epsilon'_h \leftarrow \chi$.

The real decryption result of P_h is: if $v = \frac{1}{N} \sum_{i \in [N]} v_i = \mu \left\lceil \frac{q}{2} \right\rceil + e' \Rightarrow Ne' = \sum_{i \in [N]} v_i - N\mu \left\lceil \frac{q}{2} \right\rceil$, then:

$$\begin{aligned} \rho_h &= \eta_h G^{-1}(w^T) + \epsilon_h = v_h + \epsilon_h \\ &= \sum_{i \in [N]} v_i - \sum_{i \neq h} v_i + \epsilon_h \\ &= \sum_{i \in [N]} v_i - N\mu \left\lceil \frac{q}{2} \right\rceil + N\mu \left\lceil \frac{q}{2} \right\rceil - \sum_{i \neq h} v_i + \epsilon_h \\ &= Ne' + N\mu \left\lceil \frac{q}{2} \right\rceil - \sum_{i \neq h} v_i + \epsilon_h \end{aligned}$$

where $\epsilon_h \leftarrow \chi$.

It is easy to determine that ϵ_h and ϵ'_h are statistically indistinguishable, which proves that ρ_h and ρ'_h cannot be distinguished, so the conclusion is proven. \square

Lemma 2. $HYB_{\pi,A,Z} \stackrel{\text{comp}}{\approx} IDEAL_{F,S,Z}$

Proof. The ciphertext generated by P_h is the only difference between the two games. From the semantic security of the encryption method of the NFHE scheme, it can be seen that the ciphertext is computationally indistinguishable, so the two games are also computationally indistinguishable.

From Lemma 1 and Lemma 2, $IDEAL_{F,S,Z} \stackrel{\text{comp}}{\approx} REAL_{\pi,A,Z}$ can be obtained.
End. \square

5.3.3. In Malicious Model

Due to the SMC protocol under the CRS model, if the protocol is proven to be safe under the semi-malicious model, the protocol can be converted into a protocol under the malicious model by non-interactive zero-knowledge proofs (NIZKs) [21]. Therefore, the SMC protocol designed in this paper is also safe under the malicious model.

5.4. Performance and Comparison

References [11,12] are both single-bit SMC protocols. If B is the number of input bits, then the two schemes need to be repeated B times. Reference [16] and the SMC protocol in this paper both support multi-bit encryption, which only needs to be executed once.

Compared with the protocol in reference [16], the protocol constructed in this paper has the following two improvements.

(a) From the perspective of efficiency, the protocol constructed in this paper improves the ciphertext size $(n+1)^2 \lceil \log q \rceil^2$ by modifying the expansion method of the GSW13 scheme, and the obtained cipher-text size is $\frac{(n+1)^2 \lceil \log q \rceil^2}{\lceil \log p \rceil}$. In addition, under the multi-bit encryption, the ciphertext size is $\frac{(n+B)^2 \lceil \log q \rceil^2}{\lceil \log p \rceil}$, as shown in Table 1. Therefore, the performance of the protocol under the existing CRS model is the best.

(b) Moreover, in terms of storage overhead, the ciphertext of the NFHE scheme based on the SMC protocol in this paper is a matrix, so the ciphertext expansion rate is also $O(1)$. At the same time, since the size of the ciphertext is much larger than the size of the key, the protocol in this paper effectively reduces the storage overhead of the system by greatly compressing the size of the ciphertext.

The main performance comparison of the existing secure multi-party computation protocols based on fully homomorphic encryption under the CRS model is shown in Table 1, where “Basic” represents the basic fully homomorphic encryption scheme used in the protocol; “Rd” represents the protocol Interactive rounds; “CTE Ratio” represents the ciphertext expansion ratio; “Depth” represents the complexity of the NAND gate; and the last column “Ciphertext Size” represents the size of the ciphertext. B is the number of input bits; N is the number of users; n is the lattice dimension; d is the NAND depth of the circuit to be evaluated; $\omega < 2.3727$ is a constant; $q \in \mathbb{Z}$ is a modulus; and p is a power of 2.

Table 1. Performance comparison of SMC protocol based on FHE.

Protocol	Basic	Rd	CTE Ratio	Depth	Ciphertext Size
Mukherjee et al. [11]	GSW13	2	$O(1)$	$\tilde{O}(BN(nd)^\omega)$	$(n+1)^2 \lceil \log q \rceil^2$
Wang et al. [12]	GSW13	3	$O(1)$	$\tilde{O}(B(nd)^\omega)$	$(n+1)^2 \lceil \log q \rceil^2$
Tang et al. [16]	GSW13	3	$O(1)$	$\tilde{O}((nd)^\omega)$	$(n+B)^2 \lceil \log q \rceil^2$
Ours	GSW13	3	$O(1)$	$\tilde{O}((nd)^\omega)$	$\frac{(n+B)^2 \lceil \log q \rceil^2}{\lceil \log p \rceil}$

6. Conclusions

Based on the efficient FHE scheme, a leveled, multi-bit, multi-key, secure multi-party computation protocol under the CRS model is constructed in this paper. This protocol has a total of three rounds of communication, which is proven to be safe in a semi-honest and semi-malicious environment, and the security is based on DLWE and the some-are-errorless LWE. Moreover, compared with the existing protocol, the ciphertext expansion rate of this protocol is small, and the multi-bit encryption greatly reduces the number of homomorphic calculations. Meanwhile, the complexity of the NAND gate is low, and the ciphertext size is small. The overall performance is optimal among the existing FHE-based secure multi-party computation protocols. Therefore, for the next study steps, attention will be paid to how to conduct the appropriate methods to ensure the safe transmission of data and meet the coordination requirements of the session when implementing the protocol. Meanwhile, the protocol will be further improved to achieve practical standards.

Author Contributions: Both authors took part in the discussion of the work described in this paper. Z.-W.Z. wrote the paper; R.-W.H. revised and finalized the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the National Natural Science Foundation Project under Grant No. 62062009 and the Guangxi Innovation-Driven Development Project under Grant Nos. AA17204058-17 and AA18118047-7.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No data were used to support this study.

Acknowledgments: The authors would also like to thank the anonymous referees for their constructive comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rivest, R.L.; Adleman, L.; Dertouzos, M.L. On data banks and privacy homomorphisms. *Found. Secur. Comput.* **1978**, *4*, 169–180.
2. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 169–178.
3. Brakerski, Z.; Vaikuntanathan, V. Efficient Fully Homomorphic Encryption from (Standard) LWE. In Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, Palm Springs, CA, USA, 22–25 October 2011; pp. 97–106.
4. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. (Leveled) fully homomorphic encryption without bootstrapping. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, Cambridge, MA, USA, 8–10 January 2012; pp. 309–325.
5. Brakerski, Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2012; pp. 868–886.
6. Gentry, C.; Sahai, A.; Waters, B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; pp. 75–92.
7. Cheon, J.H.; Kim, A.; Kim, M.; Song, Y. Homomorphic encryption for arithmetic of approximate numbers. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017; pp. 409–437.
8. Yao, A.C. Protocols for secure computations. In Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 3–5 November 1982; pp. 160–164.
9. López-Alt, A.; Tromer, E.; Vaikuntanathan, V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In Proceedings of the forty-fourth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 19–22 May 2012; pp. 1219–1234.
10. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A ring-based public key cryptosystem. In Proceedings of the International Algorithmic Number Theory Symposium, Portland, OR, USA, 21–25 June 1998; pp. 267–288.
11. Mukherjee, P.; Wichs, D. Two round multiparty computation via multi-key FHE. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 8–12 May 2016; pp. 735–763.
12. Wang, H.; Feng, Y.; Ding, Y.; Tang, S. A multi-key SMC protocol and multi-key FHE based on some-are-errorless LWE. *Soft Comput.* **2019**, *23*, 1735–1744. [\[CrossRef\]](#)
13. Kim, E.; Lee, H.S.; Park, J. Towards round-optimal secure multiparty computations: Multikey FHE without a CRS. In Proceedings of the Australasian Conference on Information Security and Privacy, Wollongong, Australia, 11–13 July 2018; pp. 101–113.
14. Tang, C.; Hu, Y.; Li, X. Three Round Secure Multiparty Computation Based on Multi-key Full-Homomorphic Encryption without CRS. *J. Cryptogr.* **2021**, *8*, 273–281.
15. Li, Z. *Lattice-Based Fully Homomorphic Encryption and Its Applications*; Harbin Engineering University: Harbin, China, 2018.
16. Tang, C.; Hu, Y. Secure multi-party computing based on multi-bit fully homomorphic encryption. *Chin. J. Comput.* **2021**, *44*, 836–845.
17. Li, Z.; Ma, C.; Morais, E.; Du, G. Multi-bit Leveled Homomorphic Encryption via Dual. LWE-Based. In Proceedings of the Information Security and Cryptology: 12th International Conference, Inscrypt 2016, Beijing, China, 4–6 November 2016.
18. Chen, L.; Zhou, Y.; Duan, R. Design of fully homomorphic encryption scheme supporting multi-bit encryption. *Appl. Res. Comput.* **2021**, *38*, 579–583.
19. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *JACM* **2009**, *56*, 1–40. [\[CrossRef\]](#)
20. Boneh, D.; Lewi, K.; Montgomery, H.; Raghunathan, A. Key homomorphic PRFs and their applications. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; pp. 410–428.
21. Asharov, G.; Jain, A.; López-Alt, A.; Tromer, E.; Vaikuntanathan, V.; Wichs, D. Multiparty computation with low communication, computation and interaction via threshold FHE. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012; pp. 483–501.