Fully Dynamic Multi-Key FHE Without Gaussian Noise

Yu Huang\(^1\), Kaigui Wu\(^1\), and Ming Chen\(^2\)

\(^1\)College of Computer Science, Chongqing University, Chongqing 400044, China
\(^2\)School of Mathematics and Computer Science, Yichun University, Yichun 336000, China

Corresponding author: Kaigui Wu (kaiguiwu@cqu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61662083.

ABSTRACT Fully dynamic multi-key fully homomorphic encryption (FHE) that allows an unlimited number of homomorphic operations for unconstrained parties. That is to say, it supports performing as many computational procedures on inputs (which are encrypted by an unrestricted number of parties) as needed. The existed fully dynamic multi-key FHE scheme is based on the learning with errors (LWE) problem. However, the LWE problem suffers from the intricate and laborious Gaussian sampling which extremely weakens the schemes' efficiencies. What's more, it has been lately revealed that Gaussian sampling creates lots of possible side-channel vulnerabilities that result in the disclosure of secret keys. The paper proposed a fully dynamic multi-key FHE that based on the learning with rounding (LWR) problem while sustaining almost the same security level.

INDEX TERMS Learning with errors, learning with rounding, multi-key FHE.

I. INTRODUCTION Fully homomorphic encryption (FHE), introduced by Rivest et al. [1] in 1978, is a very fascinating cryptography primitive which allows performing the unbounded number of computations on encrypted data while it remains encrypted. With this attractive attribute, FHE has many theoretical and functional applications. However, it takes over 30 years for the first scheme in Gentry’s break-through work [2], [3], since then it has developed rapidly and fast. Multi-key FHE is an extension of FHE which is proposed by López-Alt et al. [4]. MKFHE permitting us computation on ciphertexts encrypted by distinct and independent parties. Construct an on-the-fly multiparty computation (MPC) protocol are one of the most fascinating applications of it. In MKFHE, a trusted third party takes ciphertexts encrypted by different parties and performs computations on them. The result can then be decrypted via all of the keys involved in the computation procedure. Note that all keys need to be used for decryption due to security concerns. López-Alt et al. [4] construct an MKFHE scheme based on the NTRU scheme, but the scheme is controversial due to the fact that its security is based on a non-standard assumption on polynomial rings. Subsequently, Clear and McGoldrick [5] construct a scheme based on the learning with errors (LWE) problem whose security is supported by a worst-case hardness problem, using a variant of GSW-style FHE scheme [6]. Later, Mukherjee and Wichs [7] proposed a simpler but more efficient scheme of MKFHE and built a two-round MPC protocol upon it.

Peikert and Shiehian introduced the notion of single-hop and multi-hop MKFHE in [8]. Single-hop MKFHE means any new party is not allowed to participate except the parties determined ahead of the homomorphic computation step, while multi-hop MKFHE allows new participants to join in dynamically during the homomorphic evaluation procedure. Fully dynamic MKFHE which was proposed by Brakerski and Perlman in [9] is similar to multi-hop MKFHE, the difference between them is that fully dynamic MKFHE does not limit the number of users. We observe that both [5] and [7] are single-hop MKFHE while [4] is a multi-hop MKFHE scheme. In [9], Brakerski and Perlman proposed a fully dynamic MKFHE, and their ciphertexts grow just linearly with the number of parties involved in the encryption.

The above-mentioned FHEs and related schemes (e.g., [5]–[9]) are mostly based on the LWE problem which suffers an intricate and laborious Gaussian noise sampling problem. What’s more, it has been lately revealed in [10], [11] that Gaussian sampling creates lots of possible side-channel vulnerabilities that result in the disclosure of secret keys. Furthermore, it is currently very difficult to calculate Gaussian samples accurately.

The associate editor coordinating the review of this manuscript and approving it for publication was Noor Zaman.
exposures that cause the disclosure of secret keys. Though there are methods to prevent side-channel attacks, it is complicated and time-consuming.

Certainly, this triggered an idea that is there a method that can get rid of the Gaussian noise sampling process in constructing an FHE scheme without losing the security of the scheme (or almost the same level). The answer lies in the Learning with Rounding (LWR) problem.

A. RELATED WORK

The LWR problem was introduced by Banerjee, Peikert, and Rosen in [12], a variant of the LWE problem, which can be considered as a deterministic version of the LWE problem. Costache and Smart [13] constructed an FHE scheme without Gaussian noise based on the LWR problem, however, their scheme exists a “tangly modulus” problem according to [14]. In [14], Luo and Wang constructed a GSW-like FHE scheme based on the LWR problem. That is to say, their scheme eliminates the Gaussian noise sampling process needed in the previous FHE scheme. While they claim that their scheme exists a ''tangly modulus'' problem according to Gaussian noise based on the LWR problem, however, Costache and Smart [13] constructed an FHE scheme without Gaussian noise, they just construct a two-key FHE scheme indeed.

What’s more, there exist some obvious errors in their two-key FHE scheme. As to the hardness of the LWR problem, Alwen et al. [15] gave a reduction that allows for a polynomial modulus \( q \). However, only part of modulus \( q \) satisfies its result. Bogdanov et al. [16] eliminating the restriction on \( q \) but still requires samples less than \( O(q/Bp) \) which results in weaker security. Alperin-Sheriff and Apon [17] showed a dimension-preserving reduction from LWE to LWR which improves the security and efficiency of parameters. Liu and Wang [18] establish the hardness reduction by conducting a comprehensive study for Ring-LWR. In their work, they first present an algebraic framework of LWR based on [19], then generalizing a result in the plain LWR by a search Ring-LWR to decision Ring-LWR reduction and generalizing the plain LWE to LWR reduction by a reduction from Ring-LWE to Module Ring-LWR, their central techniques is a new ring leftover hash lemma.

Brakerski et al. [20] proved that bin-LWE ((0,1)-LWE), which means the key is selected uniformly and randomly from \([0,1]\), is not easier than the LWE problem. Hence, by combining Theorem 1 and the bin-LWE problem, we can uniformly and randomly choose the secret key of the LWR problem from \([0, 1]^n\). Then by combining the theorem in [16] and Lemma 1, we can get Theorem 2, where our scheme is based. Theorem 2 focuses on the search bin-LWE problem, which is harder than the decision bin-LWE problem.

B. OUR CONTRIBUTIONS

This paper focuses on designing a fully dynamic LWR-Based MKFHE scheme. Lots of LWE-Based FHE schemes have been proposed by utilizing the techniques of relinearization and modulus switching or approximate eigenvector. Considering that the LWR problem can be used to eliminate intricate and time-consuming Gaussian noise, we adapt it to design an LWR-Based fully dynamic MKFHE scheme. The efficiency of our scheme is almost equivalent to that of [9] without counting the cost of Gaussian noise sampling while sustaining almost the same security level. Our scheme can be seen as a substitute to the [9]. The contributions of this work are as follows:

1) A LWR-Based MKFHE scheme is proposed. Most MKFHE schemes are based on the LWE problem, thus suffering the intricate and laborious Gaussian sampling which extremely declines the schemes’ efficiencies. What’s more, it has been lately revealed that Gaussian sampling creates lots of possible side-channel exposures that cause the disclosure of secret keys. LWR problem allows us to dispense the costly Gaussian sampling required in the LWE problem while sustaining almost the same security level.

2) The proposed MKFHE is extended to the fully dynamic MKFHE that allows an unlimited number of homomorphic operations for unconstrained parties. That is to say, it supports performing as many computational procedures on inputs as needed.

C. PAPER ORGANIZATION

The rest of this paper is organized as follows: In Section II, we give the preliminaries such as the LWE problem, LWR problem. We describe a single key LWR-based FHE and extend it to a multi-key FHE scheme. In Section IV, the construction of the proposed Gaussian noise-free fully dynamic multi-key has been introduced. Summarizes the paper in Section V.

II. PRELIMINARIES

A. NOTATIONS

The paper uses \( \lambda \) to represent the security parameter and \( \text{negl}(\lambda) \) to represent a negligible function of \( \lambda \). Vectors are represented by bold lowercase symbols and matrices are represented by bold uppercase symbols. In general, vectors are considered as a row matrix. For any \( x \in \mathbb{Q}, |x|, [x], \) and \( [x] \) denote \( x \) round down, round up and round to the nearest integer respectively. All vectors are treated as rows. For an integer \( q \), we define the set \( \mathbb{Z}_q \triangleq \{-q/2, q/2\} \cap \mathbb{Z} \), and all logarithms on \( q \) are to base 2. We denote \( \ell_q = \lfloor \log q \rfloor \). All arithmetic are performed over \( \mathbb{Z} \) or \( \mathbb{Q} \) when division is used, and for a positive integer \( n \), let \( [n] \triangleq [1, \ldots, n] \). We let \( \mathbf{a}[i] \) denote the \( i \)-th component of vector \( \mathbf{a} \) and \( \mathbf{A}[i, j] \) denote the value of the element located in the \( i \)-th row and the \( j \)-th column of matrix \( \mathbf{A} \). Sequences of matrices \( \mathbf{M}_1, \ldots, \mathbf{M}_l \) are denoted by \( \mathbf{M} \). Let \( \mathbf{M}[k] \) be the \( k \)-th matrix. We let \( x \leftarrow \mathcal{D} \) denote that \( x \) is sampled uniformly and randomly from a distribution \( \mathcal{D} \) and \( s \leftarrow \mathcal{S} \) denote that \( s \) is uniform over a set \( \mathcal{S} \).

For \( x \in \mathbb{Z}_q \) we define \( |x| = \text{arg min}_{y=x \pmod{q}} |y| \) (this function satisfies the triangle inequality properties of standard absolute value). Further, we denote \( ||v||_\infty = \max_i |v[i]| \).

Given positive numbers \( n, m \) and two different modulus \( q, p \),...
for $n \times m$ matrix $A$, let $A \in \mathbb{Z}_{q}^{n \times m} \times \mathbb{Z}_{p}^{m}$ indicate that all row vectors of $A$ are over $\mathbb{Z}_{q}^{m}$ except the last one is over $\mathbb{Z}_{p}^{m}$, for examples, multiplying a matrix $A \in \mathbb{Z}_{q}^{n \times m} \times \mathbb{Z}_{p}^{m}$ by a matrix $R \in \{0, 1\}^{m \times m}$, we should multiply every row vector of $A$ by the matrix $R \in \{0, 1\}^{m \times m}$, and then take a modular operation. Note that the last row vector of $A$ is over $\mathbb{Z}_{p}^{m}$, and thus the multiplications between this row vector and the matrix $R \in \{0, 1\}^{m \times m}$ are evaluated over $\mathbb{Z}_{p}^{m}$, while all the other multiplications are evaluated over $\mathbb{Z}_{q}^{m}$. This rule also applies to the addition of two matrices over $\mathbb{Z}_{q}^{n \times m} \times \mathbb{Z}_{p}^{m}$.

Indeed, when performing computations on matrices, this is the significant modification between LWE and LWR.

B. LWE PROBLEM AND LWR PROBLEM

The LWE problem was initially proposed by Regev [21] as a variation of “learning parity with noise” [22], [23]. For positive integers $n$ and $q \geq 2$, a vectors $s \in \mathbb{Z}_{q}^{n}$, and a probability distribution $\chi$ over $\mathbb{Z}$, define the LWE distribution $A_{s, \chi}$ acquired by selecting a vector $a \leftarrow \mathbb{Z}_{q}^{n}$ uniformly and randomly, a noise $e \leftarrow \chi$, and outputting $(a, [a \cdot s] + e \cdot 1_{q}) \in \mathbb{Z}_{q}^{n} \times \mathbb{Z}_{q}$. The decisional LWE (DLWE) is defined as follows.

Definition 1 (DLWE): Let $\lambda$ be the security parameter, an integer dimension $n = n(\lambda)$, an integer modulus $q = q(\lambda) \geq 2$, and let $\chi = \chi(\lambda)$ be an error distribution over $\mathbb{Z}$. The DLWE$_{n, q, \chi}$ assumption is that the DLWE$_{n, q, \chi}$ problem is infeasible.

The learning with rounding (LWR) problem [12], was first proposed to improve the proficiency of pseudorandom generator (PRG) based on the LWE problem. The LWR problem can be regarded as a deterministic version of the LWE problem. The LWR problem remove the Gaussian noise by rounding, and the magnitude of it less than $1/2$ compared to LWE problem. The LWR problem remove the Gaussian noise problem can be regarded as a deterministic version of the LWE problem. We recall the definition of LWR [12] being $[\cdot]_{p} : \mathbb{Z}_{q}^{n} \rightarrow \mathbb{Z}_{p}$, where $p \geq q \geq 2$ will be apparent from the context as

$$\lfloor(x, s)_{q}\rfloor_{p} = \left[\frac{p}{q} \cdot (x, s)_{q}\right] \mod p \quad (1)$$

The definition of LWR problem is given as follows which is similar to LWE problem.

Definition 2 (DLWR): For integers $n$, $q > p$, $m$ and $s \leftarrow \mathbb{Z}_{q}^{n}$, let the LWR distribution LWR$_{n, p, q}$ be achieved by selecting a vector $a \leftarrow \mathbb{Z}_{q}^{n}$ uniformly and randomly, then outputting $(a, [a \cdot s]_{q}) \in \mathbb{Z}_{q}^{n} \times \mathbb{Z}_{q}$. The decisional LWR problem is to distinguish $m$ samples selected by the distribution LWR$_{n, p, q}$ from $m$ samples selected by the uniform distribution over $\mathbb{Z}_{q}^{n} \times \mathbb{Z}_{q}$ with non-negligible advantage. The DLWR$_{n, p, q}$ assumption is that the DLWR$_{n, p, q}$ problem is infeasible.

Theorem 1([16]): For every $\varepsilon > 0$, $n$, $m$, $q > 2pB$, and algorithm $\mathcal{D}$ such that

$$\Pr_{s}[\mathcal{D}(A, [As]_{p}) = 1] - \Pr_{a}[\mathcal{D}(A, [u]_{p}) = 1] \geq \varepsilon \quad (2)$$

where $A \in \mathbb{Z}_{q}^{n \times m}$, $s \leftarrow \{0, 1\}^{n}$ and $u \in \mathbb{Z}_{p}^{m}$ there exists an algorithm $\mathcal{L}$ that runs in time polynomial in $n$, $m$, the number of divisors of $q$, and the running time of $\mathcal{D}$ such that

$$\Pr_{s}[\mathcal{L}(A, As + e) = s] \geq \left(\frac{e}{4qm - \frac{n}{p^{m}}}\right)^{2} \cdot \frac{1}{1 + \frac{2Bp}{q}} \quad (3)$$

Lemma 1: If $p|q$, then the distribution $[u]_{p}$ is uniformly over $\mathbb{Z}_{q}^{n}$ for $u \leftarrow [u]_{q}$.

Theorem 2: For every $\varepsilon > 0$, $n$, $m$, $q > 2pB$, and algorithm $\mathcal{D}$ such that

$$\Pr_{s}[\mathcal{D}(A, [As]_{p}) = 1] - \Pr_{a}[\mathcal{D}(A, v) = 1] \geq \varepsilon \quad (4)$$

where $A \in \mathbb{Z}_{q}^{n \times m}$, $s \leftarrow \{0, 1\}^{n}$ and $v \in \mathbb{Z}_{p}$ there exists an algorithm $\mathcal{L}$ that runs in time polynomial in $n$, $m$, the number of divisors of $q$, and the running time of $\mathcal{D}$ such that

$$\Pr_{s}[\mathcal{L}(A, As + e) = s] \geq \left(\frac{e}{4qm - \frac{n}{p^{m}}}\right)^{2} \cdot \frac{1}{1 + \frac{2Bp}{q}} \quad (5)$$

C. VARIANT OF GADGET MATRIX

The gadget matrix first proposed by [24] can be used to construct an LWE-based FHE scheme [25]. There are two modulus $q, p$ in the LWR problem rather than one in the LWE problem, we introduce the variant of gadget matrix $G$ which is very suitable for constructing an LWR-based FHE scheme:

$$G := \begin{bmatrix} g & \cdots & g \end{bmatrix} \in \mathbb{Z}_{q}^{n \times N} \times \mathbb{Z}_{p}^{N}$$

where $g = (1, 2, \ldots, 2^{\ell-1}) \in \mathbb{Z}_{q}^{N}$, $g_{n+1} = (1, 2, \ldots, 2^{\ell-1}) \in \mathbb{Z}_{q}^{N}$, and $N = n\ell + \ell p$.

We also define the efficiently computable deterministic “short preimage” function $G^{-1}(\cdot) : \mathbb{Z}_{q}^{n \times m} \times \mathbb{Z}_{p}^{m} \rightarrow [0, 1]^{N \times N}$, which has the following property: for any matrix $A \in \mathbb{Z}_{q}^{n \times m} \times \mathbb{Z}_{p}^{m}$, it holds that $G \cdot G^{-1}(A) = A$.

Note that $G^{-1}(\cdot)$ is an efficiently computable function rather than a matrix. For those who familiar with GSW scheme, function $G^{-1}(\cdot)$ is equal to BitDecomp operation and multiplication by $G$ is the BitDecomp$^{-1}$ operation.

Definition 3 (Fully Dynamic Multi-Key FHE [9]): Let MKHE be a multi-key FHE scheme, $N = N_{t}$ be any polynomial in the security parameter, let $\mathcal{C} = \mathcal{C}_{t}$ be a sequence of circuits, set $\text{params} \leftarrow \text{Setup}(1^{\lambda})$ and $(pk_{t}, sk_{t}) \leftarrow \text{Keygen}(\text{params})$ for $t \in [N]$, and let $c_{t}$ be such that $\text{Dec}(sk_{j_{1}}, \ldots, sk_{j_{t}}) = \mu_{j_{t}}$, where $\{sk_{j_{1}}, \ldots, sk_{j_{t}}\} \subseteq \{sk_{1}, \ldots, sk_{N}\}$. MKHE if fully dynamic if

$$\Pr[\text{MKHE.Dec}(sk_{1}, \ldots, sk_{N}), \text{MKHE.Eval}(\mathcal{C}, (c_{1}, \ldots, c_{t}), (pk_{1}, \ldots, pk_{N})) \neq \ell(\mu_{1}, \ldots, \mu_{t})] = \text{negl}(\lambda)$$

Definition 4 (Bootstrapping [2], [3]): A scheme is bootstrapping if the following holds. It can homomorphically evaluate its own augmented decryption circuits and is also
weak circular secure (remain secure even the adversary who get the encryption of the secret key). This scheme can be transformed into a pure fully homomorphic encryption scheme.

Lemma 2([26]): Let $\lambda$, $n$, $q$, $p$ and $m \geq n\ell_q + \ell_p + 2\lambda$ be integers, and let $y \leftarrow Z_q^n \times Z_p$. For matrix $A \leftarrow Z_q^{n \times m} \times Z_p^m$, let $r \leftarrow \{0, 1\}^m$, one has

$$\Delta((A, A \cdot r), (A, y)) \leq \frac{1}{\sqrt{Z}} \leq 2^{-\lambda} \quad (6)$$

where $\Delta(X, Y)$ denotes the statistical distance between two distributions $X, Y$.

### III. LWR-BASED FULLY HOMOMORPHIC ENCRYPTION AND MULTI-KEY FHE SCHEME

#### A. LWR-BASED FULLY HOMOMORPHIC ENCRYPTION SCHEME

We present the LWR-based fully homomorphic encryption scheme, which is actually a restatement of the scheme of [14]. For easier comprehension, some changes have been made.

- **SKFHE.Setup($1^\lambda$):** choose parameters $n = n(\lambda)$, modulus $q = q(\lambda)$, $p = p(\lambda)$ satisfying $p, q, m(\lambda) = O(nq + \ell_p) \geq nq + \ell_p + 2\lambda$. Let $N = n \left[\ell_p\right] + \left[\ell_q\right]$ and params $= \{n, q, p, m\}$.

- **SKFHE.Keygen(params):** Sample $s \leftarrow \{0, 1\}^n$. Choose uniformly and randomly $m$ vectors $a_i \leftarrow Z_q^n$ and then compute

$$b_i = \left< a_i, s > q \right> \in Z_p$$

for $i \in [m]$. Set $A = (a_1^T, \ldots, a_m^T) \in Z_q^{n \times m}$ and $b = (b_1, \ldots, b_m)$. Set $sk = t = (-plq \cdot s, 1) \in Z_q^{n+1}$ and $pk = A \cdot b \in Z_q^{n \times m}$ and noise $e = (e_1, \ldots, e_m)$ where $e_i = b_i - (plq < a_i, s > q) \in [-1/2, 1/2]$ for $i \in [m]$. Thus we have $t \cdot A = e \mod p$, it holds because

$$t \cdot (a_i, b_i) = \frac{p}{q} \left< s, a_i > q \right> + b_i$$

$$= \frac{p}{q} \left< s, a_i > q \right> + kq + b_i$$

$$= \frac{p}{q} \left< s, a_i > q \right> \left< k \right> + b_i + e_i$$

$$\leq \frac{1}{2} m (N + 1) \quad (14)$$

where $G^1(C_2) \in [0, 1]^{N \times N}$ and $\left< e_i G^1(C_2) + \mu | e_2 \right>$ is the magnitude of noise after homomorphic multiplication, it holds that

$$\left< e_i G^1(C_2) + \mu | e_2 \right> \leq \frac{1}{2} m (N + 1) \quad (14)$$

Therefore, it is obvious that the magnitude of noise is equal to the size of noise after homomorphic multiplication.

In this scheme $q = (O(nq))^{L+O(1)}$, $p = (O(nq))^{L+O(1)}$ and satisfying $q \leq 2 mpB$ so as to achieve almost the same security level, thus the parameter $q$ is larger compared to $q$ in GSW13 and AP14 where $q = (O(nq))^{L+O(1)}$.

**Theorem 4:** The scheme described above is IND-CPA secure under the LWR$_{n,m,q,p}$ assumption.

We prove this Theorem 4 by the following series of hybrid experiments, our proof process mainly refers to [14] and [27].

**Game 0:** This is the real IND-CPA game.

**Game 1:** In this game m pairs $\{(a_i, b_i)\}_{i=1,...,m}$ are chosen uniformly from $Z_q^n \times Z_p$, rather than chosen from LWR samples compared to Game 0, to generate public key A. Then using the public key A to generate the ciphertext e by encrypting $\mu$ as the encryption procedure in Game 0.

**Game 2:** In this game, the ciphertext e is chosen uniformly from $Z_q^n \times Z_p$ and thus independently of the public key A compared to Game 1.

We claim that Game 0 and Game 1 are indistinguishable under the LWR$_{n,m,q,p}$ assumption. To prove this we assume there is an adversary A that can distinguish Game 0 and Game 1, then construct an algorithm B that collects input samples to generate the public key A and get the ciphertext e by encrypting a message $\mu$ by the public key A, then invokes A on (A, e), outputting the accept/reject decision. It is obvious that B is fully simulation game 0 and Game 1 depending on
its inputs, if the inputs are LWR samples, then algorithm $B$ simulates Game 0, otherwise, algorithm $B$ simulates Game 1. Therefore, $B$ and $A$ have equal distinguishing advantages. Because $B$’s advantage must be negligible by hypothesis, so is $A$’s.

Then we claim that Game 1 and Game 2 are statistically indistinguishable. This can be proved by Lemma 2 in Section II. Specifically, the term $A \cdot r$ in Game 1 and element $y \leftarrow Z^d_q \times \mathbb{Z}_q$ are statistically indistinguishable by Lemma 2. Hence, the ciphertext $c$ in Game 1 and Game 2 are statistically indistinguishable, adding any fixed vector to $A \cdot r$ does not change its uniform distribution.

In conclusion, we claim that Game 0 and Game 2 are indistinguishable under the LWR$_{n,m,q,p}$ assumption, and the ciphertext in Game 2 is independent of message $\mu$. This concludes the proof.

### C. LINEAR COMBINATION

We now describe the technique named Linear combination that plays an important role for construction of a multi-key FHE scheme.

Linear combination: Define a matrix $M \in \{0,1\}^{N \times N}$ and $C_{i,j} \in \mathbb{Z}_q^{n \times N}$, $Z_p^n$ be a SKFHE encryption of $M[i,j]$ for $i \in [N], j \in [N]$ under a secret key $t = (-p/q, 1) \in \mathbb{Z}_q^{n+1}$. Let $v \in \mathbb{Z}_q^n$ be a vector, then there is a polynomial-time deterministic algorithm

$$C_k = \text{LinComb} \left( \{C_{1,1}, \ldots, C_{m,n}\} \right)$$

which outputs $C_k \in \mathbb{Z}_q^{n \times N}$ such that $tC_k = vM + e$ where $\|e\|_\infty \leq (1/2)mN^3$.

The algorithm LinComb is implemented as follows:

1) For $i \in [N], j \in [N]$, define a matrix $Z_{i,j} \in \mathbb{Z}_q^{n \times N}$ as follows:

$$Z_{i,j}[a, b] = \begin{cases} v[i] & \text{when } a = n + 1, b = j, \\ 0 & \text{otherwise}. \end{cases}$$

2) Then output $C_k \in \mathbb{Z}_q^{n \times N}$ such that $C_k = \sum_{i=1}^{N} C_{i,j} G^{-1}(Z_{i,j})$.

Correctness follows because,

$$tC_k = t \sum_{i,j} C_{i,j} G^{-1}(Z_{i,j})$$

$$= \sum_{i,j} (M[i,j] tG \cdot e_{i,j}) G^{-1}(Z_{i,j})$$

$$= \sum_{i,j} (M[i,j] t \cdot Z_{i,j} + e_{i,j})$$

$$= \left[ \begin{array}{c} \sum_{i,j} M[i,j] Z_{i,j} + e' \\ \vdots \\ \vdots \\ \sum_{i,j} M[i,j] Z_{i,j} + e' \end{array} \right]$$

$$= (\frac{-p}{q} \cdot v \cdot M) + e'' = vM + e''$$

(17)

First recall that $\|e_{i,j}\|_\infty \leq (1/2)m(\|e\|_\infty)$ is the noise contained in $c_{i,j}$, then $\|e_{i,j}\|_\infty \leq (1/2)mN$, and finally $\|e\|_\infty \leq \frac{1}{2}(1/2)mN^3$.

### D. LWR-BASED MULTI-KEY FHE SCHEME

The reference [14] just considers s case of two keys and their scheme has errors. Now we introduce our LWR-Based MKFHE scheme.

- **MKFHE.Setup($\lambda$):** Run the Setup algorithm of SKFHE to generate the parameters:

$$\text{params} = (n, q, p, m) \leftarrow \text{SKFHE.Setup}(\lambda).$$

- **MKFHE.Keygen(params):** Run the Keygen algorithm of SKFHE to generate $pk$ and $sk$:

$$sk = t, pk = A \leftarrow \text{SKFHE.Keygen(params)}.$$

- **MKFHE.Enc($pk, \mu$):** Set $C = A \cdot R + \mu G \in \mathbb{Z}_q^{n \times N}$, where $R \in \mathbb{Z}_q^{m \times N}$ is the encryption randomness and use SKFHE encrypt $R[a, b]$ to get $mN$ ciphertexts for $a \in [m], b \in [N]$; $V_{a,b} \leftarrow \text{SKFHE.Enc}(pk, R[a, b])$. Set $\| = (V_{1,1}, \ldots, V_{m,N}) \in (\mathbb{Z}_q^{n \times N})^{mN}$ and output the pair $\| = (\|, C)$ as the ciphertext $\|$.

- **MKFHE.Expand$({pk}_1, \ldots, {pk}_K, i, \|):$** On input a series of public keys $pk_1, \ldots, pk_K$, a fresh ciphertext $\| = (\|, C)$ encrypted under the public key $pk_i$, run following algorithm for all $pk_i$ where $i \neq j$.

1. For $j \in \{\{pk_1, \ldots, pk_K\} \backslash \{i\}$, compute $X_j \leftarrow \text{LinComb}(\|, pk_j - pk_i).
2. Define a matrix $\hat{C}$ composed of $K^2$ sub-matrices, each sub-matrix $C_{a,b}$ is defined as:

$$C_{a,b} = \begin{cases} C & \text{when } a = b \\ X_j & \text{when } a \neq j \text{ and } b = j \\ 0 & \text{otherwise} \end{cases}$$

(18)

Below is the structure of the expanded ciphertext $\hat{C}$:

$$\begin{bmatrix} C & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \ddots \\ \vdots & \ddots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & C \end{bmatrix}$$

Row $i \rightarrow X_1 \cdots C \cdots X_K$

$\uparrow$

Column $i$
MKFHE.Dec((t₁,...,tₖ), Ĉ): On input a sequence of secret keys t₁,...,tₖ, construct the joint secret key 
\( \hat{t} = [t₁,...,tₖ] \in \mathbb{Z}_q^{(n+1)K} \). Then run the SKFHE.Dec algorithm.

**Theorem 5 ([14]):** The above multi-key FHE scheme is IND-CPA secure under the assumption of LWRₐₙₘ₉¬ₚ (the parameters in MKFHE is the same as we defined for SKFHE).

Now we analyze the noise in multi-key FHE scheme, suppose a sequences of \( K \) correctly generated key pairs such that \((pkᵢ, skᵢ)\) for \( i \in [K] \) and for message \( µ \) we have the corresponding expanded ciphertext Ĉ, let \( \hat{t} = [t₁,...,tₖ] \). Then
\[
\hat{t}Ĉ = [t₁X₁ + t₁C₁,...,tₖC₁, t₁Xₖ + tₖCₖ] = [\mu t₁G + e₁, ... , \mu tₖG + eₖ] \tag{19}
\]
where \( \|e\|₁ ≤ (1/2)²m \) and for \( j \neq i \), \( \|e\|₁ ≤ (1/2)²m(N³+1) \). Therefore \( \hat{t}Ĉ = \mu t hat G + e \) where \( \|e\|₁ ≤ (1/2)²m(N³+1) \). The correctness of MKFHE is guaranteed as long as the magnitude of noise \( e \) is less than \( 1/2, r \).

**IV. LWR-BASED FULLY DYNAMIC MULTI-KEY FHE SCHEME**

**A. CONSTRUCTION**

In this section, we proposed our LWR-Based fully dynamic multi-key FHE scheme FDMK. This scheme is a little different from the MKFHE scheme. The most important difference is that a ciphertext of this scheme is the last column of a matrix derived from MKFHE, due to the fact that only the last column is used in the decryption process, and the public key is extended with the encryption of the secret keys.

- **FDMK.Setup(\( 1^λ \)):** Choose a lattice dimension parameters \( n = n(λ) \) and modulus \( q = q(λ) \), \( p = p(λ) \) satisfying \( p|q \). Set \( m = (n - 1)α + β \) such that \( n|m \).

\[
\text{params} := (n, q, p, m)
\]

- **FDMK.Keygen(params):** Run the Keygen according to the scheme SKFHE to generate \( sk \)

\[
sk = t = (-p/q \cdot s, 1), \quad A = \left[ \begin{array}{c|c}
\hat{A} & b
\end{array} \right] \quad \text{SKFHE.Keygen (params)} \tag{20}
\]

Then use SKFHE to encrypt the secret key \( sk \) bit-by-bit for \( i \in [n\hat{q}] \). Let Bitᵢ(sk) represents the \( i \)-th position of \( sk \)

\[
\hat{s}[i] \leftarrow \text{SKFHE.Enc}(A, \text{Bitᵢ}(sk))
\]

The public key of this scheme is as follows:

\[
pk = (A, \hat{s})
\]

The \( \hat{s} \) part is not used for encryption but only for homomorphic evaluation.

- **FDMK Enc(pk, µ):** Sample uniformly and randomly \( r \in \mathbb{Z}_q^n \), and output the ciphertext:

\[
c = Ar + \mu q^{\hat{z}−1}u_i \in \mathbb{Z}_q^n \times \mathbb{Z}_p \tag{21}
\]

where \( u_i \) is the \( i \)-th standard basis vector.

**TABLE 1. The comparison between our scheme and others.**

| Scheme | Public key | Ciphertext | Gaussian Noise |
|--------|------------|------------|---------------|
| [7]    | 0(n²)      | 0(n²k²d³)  | Yes           |
| [8]    | 0(n(K + d)²) | 0(n²k(K + d)³) | Yes |
| [9]    | 0(π²)      | 0(πk)      | Yes           |
| Our scheme | 0(π²)      | 0(πk)      | No            |

- **FDMK.Dec((sk₁,...,skₖ), c):** Set \( \hat{t} = (sk₁,...,skₖ) \) and get decrypt message \( \mu' \)

\[
\mu' = \text{Threshold}(\hat{t}, c) \tag{22}
\]

where \( \text{Threshold}(\hat{t}, c) = \arg \min_{c \in [0, 1]} \text{noise}_{\hat{t}, c}(\hat{t}, c), \)

\[
\text{noise}_{\hat{t}, c}(\hat{t}, c) = \left\| \hat{t} \cdot c + 2\hat{z}−1\mu \right\|
\]

Then we state the security of FDMK scheme, which follows immediately from the security of MKFHE.

**Lemma 3:** If under the same DLWR parameter, MKFHE is weakly circular secure, we can conclude that FDMK is semantically secure.

Proof. Note that the ciphertext of FDMK is the last column of a matrix derived from MKFHE, and the public key in the FDMK is generated according to the MKFHE scheme, extended with the encryption of the secret keys, it is obvious that FDMK is semantically secure if MKFHE is weakly circular secure.

**B. COMPARISON WITH OTHERS**

Table 1 shows the comparison between our scheme and other schemes. Here \( n \) is the lattice dimension, \( K \) denotes the upper bounder of participants and \( k \) represents the actual number of parties who participated in encryption. As shown in Table 1, our scheme has better performance (the size of ciphertexts only grows linearly with the number of \( k \)) compared to [7] and [8], and leaves out the intricate and laborious Gaussian sampling process while maintaining similar performance compared to [9].

**V. CONCLUSION**

The paper proposes that the fully dynamic multi-key FHE can be based on the LWR problem. Therefore, our proposed scheme inherits the advantage of the fully dynamic multi-key FHE and LWR-based FHE scheme, for example, it dispenses the costly Gaussian sampling required in the LWE problem while sustaining almost the same security level and allows an unlimited number of homomorphic operations for unconstrained parties. However, our scheme is somehow ineffective due to the expensive bootstrapping process. Therefore, one can observe that our fully dynamic MKFHE as an alternative for the existing LWE-Based fully dynamic FHE scheme. Our future work includes the following:

1. The RLWR problem ([12]) is a ring version of the LWR problem. In general, FHE schemes based on the RLWR
problem have much better performance than schemes based on the LWR problem. Thus, we will construct a fully dynamic multi-key FHE scheme based on the RLWR problem.

2) Authenticated Key Exchange (AKE) [28] enables two parties to generate the session key securely over an insecure network. There are many AKE protocols (e.g., [29, 30]) over lattices, we can utilize the LWR problem to implements the authentication in AKE.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their detailed reviews and valuable feedback.

REFERENCES

[1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms,” Found. Secure Comput., vol. 4, no. 11, pp. 169–180, 1978.
[2] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in Proc. 41st Ann. ACM Symp. Theory Comput. (STOC), 2009, pp. 169–178.
[3] C. Gentry and D. Boneh, A Fully Homomorphic Encryption Scheme, no. 9, Stanford, CA, USA: Stanford Univ., 2009.
[4] A. López-Alt, E. Tromer, and V. Vaikuntanathan, “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption,” in Proc. 44th Symp. Theory Comput. (STOC), New York, NY, USA, 2012, pp. 1219–1234.
[5] M. Clear and C. McGoldrick, “Multi-identity and multi-key leveled FHE from learning with errors,” in Advances in Cryptology—CRYPTO, vol. 9216. Berlin, Germany: Springer, 2015, pp. 630–656.
[6] C. Gentry, A. Sahai, and B. Waters, “Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based,” in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer, 2013, pp. 75–92.
[7] P. Mukherjee and D. Wichs, “Two round multiparty computation via multi-key FHE,” in Advances in Cryptology—EUROCRYPT, vol. 9666. Berlin, Germany: Springer, 2016, pp. 735–763.
[8] C. Peikert and S. Shiehian, “Multi-key FHE from LWE, revisited,” in Theory of Cryptography—TCC, vol. 9986. Berlin, Germany: Springer, 2016, pp. 217–238.
[9] Z. Brakerski and R. Perlman, “Lattice-based fully dynamic multi-key FHE with short ciphertexts,” in Advances in Cryptology—CRYPTO, vol. 9814. Berlin, Germany: Springer, 2016, pp. 190–213.
[10] P. Pessl, “Analyzing the shuffling side-channel countermeasure for lattice-based signatures,” in Proc. Int. Conf. Cryptol. India, 2016, pp. 153–170.
[11] L. G. Bruinderink, A. Hülsing, T. Lange, and Y. Yarom, “Flush, gauss, and reload-a cache attack on the bliss lattice-based signature scheme,” in Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst., 2016, pp. 323–345.
[12] A. Banerjee, C. Peikert, and A. Rosen, “Pseudorandom functions and lattices,” in Advances in Cryptology—EUROCRYPT, vol. 7237. Berlin, Germany: Springer, 2012, pp. 719–737.
[13] A. Costache and N. P. Smart, “Homomorphic encryption without Gaussian noise,” IACR Cryptol. ePrint Arch., vol. 2017, p. 163, 2017.
[14] L. Luo, F. Wang, and K. Wang, “LWR-based fully homomorphic encryption, revisited,” Secur. Commun. Netw., vol. 2018, Apr. 2018, Art. no. 5967635.
[15] J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs, “Learning with rounding, revisited,” in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer, 2013, pp. 57–74.
[16] A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen, “On the hardness of learning with rounding over small modulus,” in Theory of Cryptography—TCC, vol. 9562. Berlin, Germany: Springer, 2016, pp. 209–224.
[17] J. Alperin-Sheriff and D. Apon, “Dimension-preserving reductions from LWE to LWR,” IACR Cryptol. ePrint Arch., vol. 2016, p. 589, 2016.
[18] F. Liu and Z. Wang, “Rounding in the rings,” in Proc. Annu. Int. Cryptol. Conf., 2020, pp. 296–326.
[19] C. Peikert and Z. Pepin, “Algebraically structured LWE, revisited,” in Proc. Theory Cryptogr. Conf., 2019, pp. 1–23.
[20] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, “Classical hardness of learning with errors,” in Proc. 45th Ann. ACM Symp. Theory Comput. (STOC), Palo Alto, CA, USA, 2013, pp. 575–584.
[21] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in Proc. 37th Ann. ACM Symp. Theory Comput. (STOC), Baltimore, MD, USA, 2005, pp. 84–93.
[22] A. Blum, M. Forst, M. Kearns, and R. J. Lipton, “Cryptographic primitives based on hard learning problems,” in Proc. Ann. Int. Cryptol. Conf., 1993, pp. 278–291.
[23] M. Alekhno, “More on average case vs approximation complexity,” in Proc. 44th Ann. IEEE Symp. Found. Comput. Sci., Oct. 2003, pp. 298–307.
[24] D. Micciancio and C. Peikert, “Trapdoors for lattices: Simpler, tighter, faster, smaller,” in Advances in Cryptology—EUROCRYPT, vol. 7237. Berlin, Germany: Springer, 2012, pp. 700–718.
[25] J. Alperin-Sheriff and C. Peikert, “Faster bootstrapping with polynomial error,” in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer, 2014, pp. 297–314.
[26] Z. Brakerski and V. Vaikuntanathan, “Efficient fully homomorphic encryption from (standard) LWE,” in Proc. IEEE 52nd Ann. Symp. Found. Comput. Sci., Oct. 2011, pp. 97–106.
[27] Z. Li and D. Wang, “Two-round PAKE protocol over lattices without NIZK,” in Int. Conf. Inf. Secur. Cryptol., 2018, pp. 138–159.
[28] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[29] 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, May 2015, pp. 553–570.
[30] Z. Li and D. Wang, “Achieving one-round password-based authenticated key exchange over lattices,” IEEE Trans. Services Comput., early access, Sep. 6, 2019, doi: 10.1109/TSC.2019.2939836.

YU HUANG received the B.S. degree from the College of Computer Science, Chongqing University, China, in 2018, where he is currently pursuing the M.S. degree. His main research interests include cryptography and information security.

KAIGUI WU received the bachelor’s degree from the Department of Mathematics, Sichuan Normal University, in 1989, the master’s degree from the College of Computer Science, Chongqing University, in 1993, and the Ph.D. degree in power system and automation from the School of Electrical Engineering, Chongqing University, in December 1999. He is currently a Professor and a Doctoral Tutor with Chongqing University. His main research interests include information security and big data analysis.

MING CHEN received the M.S. and Ph.D. degrees from the College of Computer Science, Chongqing University, in 2007 and 2011, respectively. He is currently an Associate Professor with Yichun University. His research interests include cryptography and information security.