# Key lifting : a more efficient weak MKFHE scheme in the plain model against rational adversary

Xiaokang Dai[1] Wenyuan Wu[✉,2] and Yong Feng[2]

[1] University of Chinese Academy of Sciences, Beijing, 100049 China
[2] Chongqing Key Laboratory of Automated Reasoning and Cognition,Chongqing Institute of Green and Intelligent Technology, Chongqing, 400714, China
daixiaokang@cigit.ac.cn wuwenyuan@cigit.ac.cn yongfeng@cigit.ac.cn

**Abstract.** Ciphertext expansion is an essential component for Multi-key Fully Homomorphic Encryption(MKFHE) scheme based on the Learning With Error(LWE) problem to enable multi-key function. In order to achieve ciphertext expansion, the random matrix used in encryption must be encrypted. For an boolean circuit with input length $N$, multiplication depth $L$, security parameter $\lambda$ , the number of additional encryptions introduced to achieve ciphertext expansion is $O(N\lambda^6L^4)$, which is a lot of overhead for computationally sensitive local users. On the other hand, current MKFHE schemes tend to be based on strong assumptions, either based on Common Reference String model(CRS), or only against to semi-malicious adversaries, or the both. For stronger adversary models, such as covert adversaries or rational adversaries, expensive zero-knowledge proofs need to be introduced to ensure security. From the perspective of improving efficiency and security, we propose the notion of weak-MKFHE and construct the first weak-MKFHE scheme based on LWE. By introducing a key lifting procedure, the local encryption $O(N\lambda^6L^4)$ is reduced to $O(N)$. Furthermore, our scheme does not rely on CRS and is robust against rational adversaries. For a stronger adversary (between rational adversaries and malicious adversaries), we show that we can catch him with non-negligible probability. We believe our results are interesting for some specific scenarios, especially for computationally-sensitive and trust-sensitive scenarios.
Unfortunately, due to the structural properties of polynomial rings, we cannot trivially transplant LWE-based construction methods to RLWE-based MKFHE. We can only construct RLWE-based MKFHE under Random Oracle Model(ROM).

**Keywords:** Multi-key homomorphic encryption · LWE · RLWE · Leakage resilient cryptography · Rational adversaries.

## 1 Introduction

**Fully Homomorphic Encryption(FHE).** The concept of FHE was proposed by Rivest et al. [RAD+78], within a year of publishing of the RSA scheme [RSA78]. The first truly fully homomorphic scheme was proposed by Gentry in his doctoral dissertation [Gen09a]in 2009. Based on Gentry's ideas, a series of FHE schemes have been proposed [Gen09b] [vGHV10] [BGV12] [FV12] [GSW13] [CGGI16] [CKKS17], and their security and efficiency have been continuously improved. FHE is suitable to the problem of unilateral outsourcing computations. However in the case of multiple data providers, in order to support homomorphic evaluation, data must be encrypted by a common public key. Due to privacy of data, it is unreasonable to require participants to use other people's public keys to encrypt their own data.

**Multiparty Computation (MPC).**This problem was initialized by Yao in [Yao82] [Yao86], who considered two-party scenarios and gave a solution. Later, Goldreich, Micali and Wigderson extended the model to $k$ participants with malicious adversaries in [MGW87]. Compared to FHE, MPC is more mature, as [Orl11] mentioned, "generic MPC is a fast moving field: In 2009 the first implementation of MPC for 2 parties with active security [PSSW09], was able to evaluate a circuit of $3 \times 10^4$ gates in $10^3$ seconds. Only two years after, the same circuit is evaluated in less than 5 seconds [NNOB12]". Subsequently, for active attacks, the literature [LP07] [Lin13] made a series of improvements.The first large-scale and practical application of multi-party computation (demonstrated on an actual auction problem) took place in Denmark in January 2008. However, MPC also has disadvantages: it suffers from high communication overhead and is vulnerable to attacks by corrupt participants, as [CD+15] mentioned, "All the general protocols we have seen require a number of rounds that is linear in the depth of circuit. We do not know if this is inherent, in fact, we do not even know which functions can be computed with unconditional security and a constant number of rounds".

**Multi-key Fully Homomorphic Encryption(MKFHE).**To deal with this dilemma, López-Alt et al. proposed the concept of MKFHE in [LTV12] and construct the first MKFHE scheme based on modified-NTRU [SS11]. Conceptually, it is an enhancement of the FHE on function that allows data provider to encrypt data independent from other participants, its key generation and data encryption are done locally. To get the evaluated result, all participants are required to execute a round of threshold decryption protocol.

After López-Alt et al. proposed the concept of MKFHE, many schemes were proposed. In 2015, Clear and McGoldrick [CM15] constructed a GSW [GSW13] LWE-based MKFHE. This scheme defined the total key as the concatenation of all keys, and constructed a masking scheme to converts the ciphertext under single key to total key by introducing CRS and circular LWE assumptions, which only supports single-hop computation. In 2016, Mukherjee and Wich [MW16], Perkert and shiehian [PS16], Brakerski and Perlman [BP16] constructed MKFHE scheme based on GSW respectively. [MW16] simplified the mask scheme of [CM15], and focused on constructing a two-round MPC protocol. The work of [PS16] and [BP16] was dedicated to constructing a multi-hop MKFHE, but their used different methods. [BP16] introduced bootstrapping to realize ciphertext expansion, thereby realizing the multi-hop function. [PS16] realized multi-hop function through ingenious construction. It is worth mentioning that all MKFHE schemes constructed based on the LWE scheme require a ciphertext expansion procedure.

### 1.1 Motivation

**Structure is a double-edged sword :** due to the more compact structure on polynomial ring and various efficient ring algorithms, it is generally believed that FHE scheme based on RLWE is more efficient than the homomorphic scheme based on LWE. This is the reason why most current homomorphic schemes, such as [CDKS19] [MTBH21] are constructed based on RLWE. However LHL lemma over integer ring $\mathbb{Z}$ enjoys the leakage resilient property : It can transform an average quality random sources into higher quality [ILL89], which is incomparable to cyclotomic ring $R : \mathbb{Z}[x]/f(x), f(x) = x^d + 1$, as [DSGKS21]mentioned if the $j$-th Number theoretical Transfer(NTT) coordinate of each ring element in $\mathbf{x} = (x_1, \dots, x_l)$. is leaked, then the $j$-th NTT coordinate of $a_{l+1} = \sum a_i x_i$ is defined, so $a_{l+1}$ is very far from uniform, yet this is only a 1/n leakage rate. Thus, LWE-based multi-key homomorphic scheme can remove CRS, but infeasible for RLWE-based MKFHE scheme.

Therefore, no matter how efficient the RLWE-based MKFHE is, it has not been possible to get rid of CRS so far. In some specific scenarios, for example, the data provider challenges the randomness of the common reference string, or challenges the fairness of a trusted third party. To deal with this dilemma, we can only choose the MKFHE based on LWE assumption. However, the efficiency of current LWE-based MKFHE is hardly satisfactory.

**Ciphertext expansion is expensive :** for MKFHE based on LWE, in order to support homomorphic evaluation, it is necessary to encrypt the random matrix $\mathbf{R} \in \mathbb{Z}_q^{m \times m}$ of each ciphertext to prepare for ciphertext expansion. For a boolean circuit with input length $N$, multiplication depth $L$, security parameter $\lambda$, $m = n \log q + \omega(\log \lambda)$, the additional encryption operation introduced is $O(N\lambda^6 L^4)$, which is $O(N)$ for single-key FHE. For computing-sensitive participants, this is a lot of overhead.

**More powerful adversary :** The semi-malicious adversary model assumes that the adversary follows the step specified by protocol, but can arbitrarily choose values from a random distribution, while a rational adversary can adaptively choose any value from any distribution(more detail please refer to Section 3.2). An MKFHE scheme against semi-malicious adversaries may not be secure in the presence of rational adversaries. For example, [BHP17] introduced Adaptively-secure Commitment [PPV08] and Zero-knowledge proof in order to fight stronger adversaries. [AJL$^+$12] assumed that the input of the adversary would not exceed the specified bound, otherwise the security of the scheme cannot be guaranteed.

### 1.2 Our Results

For trust-sensitive and computationally-sensitive data providers, facing the dilemma mentioned above, it is difficult to find a suitable solution. In order to formalize this situation, we appropriately *tighten* *and loosened* the original definition of MKFHE, the modified definition handles the dilemma better. Following this definition, we construct the first weak-MKFHE scheme based on LWE in the plain model against rational adversaries.

Since regularity lemma [LPR13] on rings has no corresponding leakage resilient properties, we cannot apply the LWE construction routine trivially to RLWE-based MKFHE, as a compromise, we introduce a round of bit commitment protocol to guarantee the independence of each participants, construct the corresponding weak-MKFHE based on ROM. We give a review of our definition and two scheme below.

**The definition of weak-MKFHE :**
Different from previous definition [MW16], we abandon ciphertext expansion procedure, instead, introducing a key lifting procedure which has the same function with ciphertext expansion, but at a lower cost. In addition to the properties that required by MKFHE, such as *Correctness, Compactness, semantic security, Simulatability of decryption*, weak-MKFHE should satisfy the following two additional properties :

- **Locally Computationally Compactness :** A leveled weak-MKFHE is locally computationally compact if the participants do the same number of encryptions as the single-key FHE scheme.
- **Low round complexity :** Only constant round interaction is allow in Key lifting procedure.

**Scheme#1: LWE-based weak-MKFHE under plain model against rational adversaries :**
The security of Scheme#1 is based on the LWE assumption. The total private key is the sum of the private keys of all participants. We note that previous MKFHE schemes adopt this key structure are all based on the CRS model. Not only is the CRS removed, our solution is simpler and more efficient in construction : For a circuit with an input length $N$, our scheme requires local users to perform $O(N)$ encryption operations, while is $O(N\lambda^6 L^4)$ for those schemes that require ciphertext expansion. We simulate the security of Scheme#1 in the presence of rational adversaries, for a more aggressive adversary we will catch him with a non-negligible probability.

However, in order to ensure the semantic security of encryption and make the threshold decryption procedure simulatable, we have to choose a larger smuging error to conceal the local decryption result. We bound the participants $k$ by poly$(\lambda)$, because a larger $k$ will lead to a larger smuging error, which further leads to a larger $q$. Here, we choose $q = 2^{\lambda L} B_\chi$, the approximate factor of the GapSVP problem on lattice is $\tilde{O}(2^{\lambda L})$ for such $q$. For detailed security and parameters, please refer to Section4.

We give the efficiency comparison with the scheme [PS16] in Table1. Since we have no ciphertext expansion, our scheme has a much lower computational overhead.

| Scheme | Space | | Time | Adversary model | CRS |
|---|---|---|---|---|---|
| | PubKey + EvalKey | CT | EvalkeyGen | | |
| [PS16] | $\tilde{O}(\lambda^6 L^4(k + N\lambda^3 L^2))$ | $\tilde{O}(Nk^2\lambda^6 L^4)$ | $\tilde{O}(N\lambda^{14} L^9)$ | Semi-malicious | Yes |
| [BHP17] | $\tilde{O}(k^4\lambda^{15} L^{11})$ | $\tilde{O}(Nk^4\lambda^8 L^6)$ | $\tilde{O}(Nk^3\lambda^{15} L^{10})$ | Semi-malicious | Yes |
| Scheme#1 | $\tilde{O}(k^2\lambda^6 L^4)$ | $\tilde{O}(Nk^2\lambda^8 L^6)$ | - | rational | NO |

**Table 1.** The notation $\tilde{O}$ hides logarithmic factors. The public key, evaluation key and ciphertext size are bits; the EvalkeyGen column denotes the number of multiplication operations over $\mathbb{Z}_q$; $k$ denotes participants number; $L$ denotes the circuit depth; $\lambda$ is the security parameter.
**Remark :** We replaced $n$ with $\lambda$. To achieve $2^\lambda$ security against known lattice attacks, one must have $n = \Omega(\lambda \log q/B_\chi)$, for our parameter settings $q = O(2^{\lambda L} B_\chi)$, thus we would like to be $n = \Omega(\lambda^2 L)$.

**Scheme#2: RLWE-based weak-MKFHE under ROM :**
Scheme#2 is based on circular RLWE. We introduce a bit commitment protocol to guarantee the randomness of each participant's public key. Due to the sum key structure, the dimension of $\mathbf{t} \otimes \mathbf{t}$ is independent of $k$, so the ciphertext relinearization algorithm pull the ciphertext after tensor product back to initial dimension by one shot, in addition, the "one shot algorithm" introduces less noise. We

compared with [CDKS19] in terms of memory and computational overhead, the results are shown in Table2.

| Scheme | Space | | Time | | Adversary model | CRS |
|---|---|---|---|---|---|---|
| | Evalkey | CT | Relinear | Mult | | |
| [CDKS19] | $\tilde{O}(kd)$ | $\tilde{O}(kd)$ | $\tilde{O}(k^2d)$ | $\tilde{O}(k^2d)$ | Semi-malicious | Yes |
| Scheme#2 | $\tilde{O}(kd)$ | $\tilde{O}(d)$ | $O(1)$ | $\tilde{O}(d)$ | Semi-malicious | ROM |

**Table 2.** The Evalkey and CT size are in bits, the Relinear and Mult columns denotes the number of scalar operations over $\mathbb{Z}_q$. The notation $\tilde{O}$ hides logarithmic factors, $k$ denotes the number of participants; $d$ denotes the dimension of the RLWE problem.

### 1.3 Related works

Unlike our scheme, [CM15] [PS16] [MW16] [BP16] [CDKS19] used the concatenation of all private key as the total key structure, and CRS are introduced. [AJJM20] removes CRS from a higher dimension, instead of using LHL or regularity lemma, they base on Multiparty Homomorphic Encryption(MHE) and modify the initialization method of its root node to achieve this purpose, more details please refer to [AJJM20]. [AJL$^+$12] is the first scheme that introduce the summation of all private key as the total key, which is also under CRS and only against semi-malicious adversaries. [BHP17] is the first scheme using the leakage resilient property of LHL to get rid of the CRS, which against semi-malicious adversaries and has the concatenation total key structure, and ciphertext expansion is essential. For their scheme, to against more powerful adversary, extra tools such as Adaptively-secure Commitment and Zero-knowledge proof are needed.

### 1.4 Overview of our construciton

Scheme#1 is based on DGSW scheme. we briefly review it first : let $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{(m\times n)})$, $\mathbf{s} \leftarrow \{0,1\}^m$, $\mathsf{pk} = (\mathbf{A}, \mathbf{b} = \mathbf{sA})$, $\mathsf{sk} = \mathbf{t} = (-\mathbf{s}, 1)$, plaintext $u \in \{0,1\}$, the DGSW ciphertext $\mathbf{C}$:

$$\mathbf{C} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \mathbf{E} + u\mathbf{G},\ \mathbf{R} \leftarrow U(\mathbb{Z}_q^{(n\times m)}),\ \mathbf{E} \text{ is an noise matrix, } \mathbf{G} \text{ is a gadget matrix.}$$

Obviously, $\mathbf{tC} \approx u\mathbf{tG}$ (omit small noise)

**Key Lifting procedure :** Following the definition of weak-MKFHE, it requires the ciphertext encrypted by hybrid key hk which are outputted by wMKLift$(\cdot)$ and are different among participants, to support homomorphic evaluation without extra modification. We achieve this property by allowing two round interaction between participants.

For the convenience of explanation, we assume that there are only two participants $\mathsf{p}_1, \mathsf{p}_2$, naturally, the whole process can be extended to $N$ participants.

- $\{\mathsf{hk}_1\} \leftarrow \mathsf{wMKLift}(\{\mathsf{pk}_1, \mathsf{sk}_1\})$: input the DGSW key pair of $\mathsf{p}_1$, where $\mathsf{pk}_1 = (\mathbf{A}_1, \mathbf{b}_{1,1})$, $\mathbf{b}_{1,1} = \mathbf{s}_1\mathbf{A}_1$, $\mathbf{A}_1 \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{s}_1 \leftarrow U\{0,1\}^{m-1}$. $\mathsf{p}_1$, $\mathsf{p}_2$ are engaged in the following two interaction
  - First round : $\mathsf{p}_1$ broadcasts $(\mathbf{A}_1, \mathbf{b}_{1,1})$ and receives $\{\mathbf{A}_2, \mathbf{b}_{2,2}\}$ (from $\mathsf{p}_2$).
  - Second round : $\mathsf{p}_1$ generates and disclose $\mathbf{b}_{1,2}$, where $\mathbf{b}_{1,2} = \mathbf{s}_1\mathbf{A}_2$

After above two round interaction, $\mathsf{p}_1$ receives $\mathbf{b}_{2,1}$(from $\mathsf{p}_2$). Let $\mathbf{b}_1 = \mathbf{b}_{1,1} + \mathbf{b}_{2,1}$, $\mathsf{p}_1$ output hybrid key $\mathsf{hk}_1 = (\mathbf{A}_1, \mathbf{b}_1)$, similarly, $\mathsf{p}_2$ outputs hybrid key $\mathsf{hk}_2 = (\mathbf{A}_2, \mathbf{b}_2)$.

After the **Key Lifting procedure** is completed, $\mathsf{p}_1$ and $\mathsf{p}_2$ get the corresponding hybrid keys $\mathsf{hk}_1$, $\mathsf{hk}_2$. In short, what the key lifting procedure does is convert the DGSW key pair of $\mathsf{p}_1$ and $\mathsf{p}_2$ into the hybrid keys $\mathsf{hk}_1$, $\mathsf{hk}_2$, which are used to encrypt their data. Let $\bar{\mathbf{t}} = (-\mathbf{s}, 1)$, $\mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2$, for ciphertext $\mathbf{C}_1$, $\mathbf{C}_2$ encrypted by hybrid key $\mathsf{hk}_1$, $\mathsf{hk}_2$ respectively :

$$\mathbf{C}_1 = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{b}_1 \end{pmatrix} \mathbf{R}_1 + \mathbf{E}_1 + u_1\mathbf{G}, \qquad \mathbf{C}_2 = \begin{pmatrix} \mathbf{A}_2 \\ \mathbf{b}_2 \end{pmatrix} \mathbf{R}_2 + \mathbf{E}_2 + u_2\mathbf{G},$$

obviously we have $\bar{\mathbf{t}}\mathbf{C}_1 \approx u_1\bar{\mathbf{t}}\mathbf{G}$, $\bar{\mathbf{t}}\mathbf{C}_2 \approx u_2\bar{\mathbf{t}}\mathbf{G}$ (omit small error). Therefore, although $\mathbf{C}_1$ and $\mathbf{C}_2$ are encrypted by different hybrid keys, they correspond to the same decryption key $\bar{\mathbf{t}}$. As we'll point out later, however, this structure will drew some security concern. We remedy this problem by increasing the noise bounds in the last row of the noise matrix $\mathbf{E}$. we discuss the security of Scheme#1 in Section 4.5

**Scheme#2:** Compared with [CDKS19], Scheme#2 has one more round of bit commitment protocol and adopts the sum key structure. Due to the sum key structure, the Relinear algorithm can pull the ciphertext after the tensor product back to initial dimension by one shot. For a more details, please refer to section 5.

## 2 Preliminaries

### 2.1 Notation:

In this work, $\lambda$ denotes security parameter, $\mathsf{negl}(\lambda)$ denotes the negligible function parameterized by $\lambda$, vectors are represented by lowercase bold letters such as $\mathbf{v}$, unless otherwise specified, vectors are row vectors by default, and matrices are represented by uppercase bold letters such as $\mathbf{M}$, $[k]$ denotes the set of integers $\{1, \ldots, k\}$. If $X$ is a distribution, then $a \leftarrow X$ denotes that value $a$ according to the distribution $X$. If $X$ is a finite set, then $a \leftarrow U(X)$ denotes that the value of $a$ is uniformly sampled from $X$. For two distribution $X, Y$ parameterized by $\lambda$, we use $X \overset{\mathsf{stat}}{\approx} Y$ to represent $X$ and $Y$ are statistically indistinguishable. Similarly, $X \overset{\mathsf{comp}}{\approx} Y$ means that there are computationally indistinguishable.

In order to decompose elements in $\mathbb{Z}_q$ into binary, we review the Gadget matrix [MP12] [AP14] here, let $\mathbf{G}^{-1}(\cdot)$ be the computable function that for any

$$\mathbf{M} \in \mathbb{Z}_q^{m\times n}, \text{ We have } \mathbf{G}^{-1}(\mathbf{M}) \in \{0,1\}^{ml\times n}, \text{ where } l = \lceil \log q \rceil$$

Let $\mathbf{g} = (1, 2, \ldots, 2^{l-1}) \in \mathbb{Z}_q^l$, $\mathbf{G} = \mathbf{I}_m \otimes \mathbf{g} \in \mathbb{Z}_q^{m\times ml}$, it satisfies $\mathbf{G}\mathbf{G}^{-1}(\mathbf{M}) = \mathbf{M}$.

**Definition 1.** *A distribution ensemble $\{\mathcal{D}_n\}_{n\in[N]}$ supported over integer, is called B-bounded if :*

$$\Pr_{e\leftarrow\mathcal{D}_n}\left[\, |e| > B \,\right] = \mathsf{negl}(n).$$

In order to prove the security of our scheme under plain model and enable the simulatability of threshold decryption, we need the following lemma which is introduced by [AJL+12]:

**Lemma 2 (in [AJL+12]).** *Let $B_1 = B_1(\lambda)$, and $B_2 = B_2(\lambda)$ be positive integers and let $e_1 \in [-B_1, B_1]$ be a fixed integer, let $e_2 \in [-B_2, B_2]$ be chosen uniformly at random, Then the distribution of $e_2$ is statistically indistinguisable from that of $e_2 + e_1$ as long as $B_1/B_2 = \mathsf{negl}(\lambda)$.*

### 2.2 The Small Integer Solution(SIS) Problem

The Small Integer Solution(SIS) problem was introduced by Ajtai in the seminal work [Ajt96] which presented a family of one-way function based on SIS problem. Subsequent series of works [Mic04] [MR04] [GPV08] [MP13] have made efforts to reduce the size of $q$, the definition below comes from [MR04]:

**Definition 3 (in [MR04]).** *The small integer solution problem $\mathsf{SIS}_{m,n,q,\beta}$(in the $\ell_\infty$ norm) is : given an integer $q$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a real $\beta$, find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m/\{\mathbf{0}\}$ such that $\mathbf{A}\mathbf{z} = \mathbf{0} \mod q$ and $||\mathbf{z}||_\infty < \beta$*

[MP13] proved that solving the $\mathsf{SIS}_{m,n,q,\beta}$ problem is at least as hard as approximating lattice problems in the worst case on lattices :

**Theorem 4 (in [MP13]).** *Let $n$ and $m = \mathsf{poly}(n)$ be integers, let $\beta$ be reals, let $Z = \{\mathbf{z} \in \mathbb{Z}^m : ||\mathbf{z}||_\infty < \beta\}$, and let $q > \beta \cdot n^\delta$ for some constant $\delta > 0$. Then solving (on the average, with non-negligible probability) $\mathsf{SIS}_{m,n,q,\beta}$ with parameters $m, n, q\beta$ and solution set $Z/\{\mathbf{0}\}$ is at least as hard as approximating lattice problems in the worst case on $n$ dimensional lattices to within $\gamma = \tilde{O}(\beta\sqrt{n})$.*

### 2.3 The Learning With Error(LWE) Problem

The Learning With Error problem was introduced by Regev [Reg05].

**Definition 5** (LWE). *Let $\lambda$ be security parameter, for parameters $n = n(\lambda)$ be an integer dimension, $q = q(\lambda) > 2$ be an integer, and a distribution $\chi = \chi(\lambda)$ over $\mathbb{Z}$, the $\mathsf{LWE}_{n,q,\chi}$ problem is to distinguish the following distribution:*

- *$\mathcal{D}_0$ : the jointly distribution $(\mathbf{A}, \mathbf{z}) \in (\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^n)$ is sampled by $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n}) \quad \mathbf{z} \leftarrow U(\mathbb{Z}_q^n)$*
- *$\mathcal{D}_1$: the jointly distribution $(\mathbf{A}, \mathbf{b}) \in (\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^n)$ is computed by $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n}) \quad \mathbf{b} = \mathbf{sA} + \mathbf{e}$, where $\quad \mathbf{s} \leftarrow U(\mathbb{Z}_q^n) \quad \mathbf{e} \leftarrow \chi^m$*

The $\mathsf{LWE}_{n,q,\chi}$ assumption assuming that $\mathcal{D}_0 \overset{\mathsf{comp}}{\approx} \mathcal{D}_1$. Regev [Reg05] proved that for certain moduli $q$ and Gaussian error distributions $\chi$ the $\mathsf{LWE}_{n,q,\chi}$ problem is true as long as certain worst case lattice problems are hard to solve using a quantum algorithm.

### 2.4 The Ring Learning With Error(RLWE) Problem

Lyubaskevsky, Peikert and Regev defines The RLWE problem in [LPR10] as follows:

**Definition 6** (RLWE). *Let $\lambda$ be a security parameter. For parameters $d = d(\lambda)$, where $d$ is a power of 2, $q = q(\lambda) > 2$ ,and a distribution $\chi = \chi(\lambda)$ over $R = \mathbb{Z}[x]/x^d + 1$, let $R_q = R/qR$, the $\mathsf{RLWE}_{d,q,\chi}$ problem is to distinguish the following distribution:*

- *$\mathcal{D}_0$: the jointly distribution $(a, z) \in R_q^2$ is sampled by $(a, z) \leftarrow U(R_q^2)$.*
- *$\mathcal{D}_1$: the jointly distribution $(a, b) \in R_q^2$ is computed by $a \leftarrow U(R_q)$, $b = as + e$, where $s \leftarrow U(R_q)$, $e \leftarrow \chi$.*

[LPR10] gave a reduction from the $\mathsf{RLWE}_{d,q,\chi}$ problem to the $\mathsf{Gap\text{-}SVP}$ problem on an ideal lattice, which is now generally considered to be intractable. Specially, [LPR10] indicated that The $\mathsf{RLWE}_{n,q,\chi}$ problem is also infeasible when $s$ is sampled from nosie distribution $\chi$. In homomorphic encryption, this property is especially popular, because the low-norm $s$ introduces less noise during homomorphic computation.

### 2.5 Dual-GSW(DGSW) Encryption scheme

The DGSW scheme [BHP17] and GSW scheme is similar to Dual-Regev scheme and Regev scheme resp. which is defined as follows:

- $\mathsf{pp} \leftarrow \mathsf{Gen}(1^\lambda, 1^L)$ : For a given security parameter $\lambda$, circuit depth $L$, choose a appropriate lattice dimension $n = n(\lambda, L)$, $\quad m = n\log q + \omega(\lambda)$, a discrete Gaussian distribution $\chi = \chi(\lambda, L)$ over $\mathbb{Z}$, which is bouned by $B_\chi$, module $q = \mathsf{poly}(n) \cdot B_\chi$ satisfying the $\mathsf{LWE}_{n,q,\chi,B_\chi}$ problem, Output $\mathsf{pp} = (n, m, q, \chi, B_\chi)$ as the initial parameters.
- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$: Let $\mathsf{sk} = \mathbf{t} = (-\mathbf{s}, 1)$, $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$, where $\mathbf{s} \leftarrow U\{0,1\}^{m-1}$, $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m-1\times n})$, $\mathbf{b} = \mathbf{sA} \mod q$
- $\mathbf{C} \leftarrow \mathsf{Enc}(\mathsf{pk}, u)$: Input public key $\mathsf{pk}$ and plaintext $u$, choose a random matrix $\mathbf{R} \leftarrow U(\mathbb{Z}_q^{n\times w})$, $w = ml$, $l = \lceil \log q \rceil$ and an error matrix $\mathbf{E} \leftarrow \chi^{n\times w}$, Output the ciphertext :

$$\mathbf{C} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \mathbf{E} + u\mathbf{G}, \text{ where } \mathbf{G} \text{ is a gadget Matrix.}$$

- $u \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathbf{C})$: Input private key $\mathsf{sk}$, ciphertext $\mathbf{C}$, let $\mathbf{w} = (0, \ldots, \lceil q/2 \rceil) \in \mathbb{Z}_q^m$, $v = \langle \mathbf{tC}, \mathbf{G}^{-1}(\mathbf{w}^T) \rangle$, output $u' = \lceil \frac{v}{q/2} \rfloor$.

**Homomorphic addition and multiplication:**
For ciphertext $\mathbf{C}_1,\ \mathbf{C}_2 \in \mathbb{Z}_q^{m \times w}$, let $\mathbf{C}_{\mathsf{add}} = \mathbf{C}_1 + \mathbf{C}_2,\ \mathbf{C}_{\mathsf{mult}} = \mathbf{C}_1 \mathbf{G}^{-1}(\mathbf{C}_2)$. It is easy to verify that $\mathbf{C}_{\mathsf{add}}$ and $\mathbf{C}_{\mathsf{mult}}$ are ciphertext of $u_1 + u_2$ and $u_1 u_2$, respectively.

For the security and correctness of the DGSW scheme, please refer to [BHP17]. Compared with the GSW scheme, DGSW scheme has bigger ciphertext, which is $O(n^2 \log^3 q)$, while $O(n^2 \log q)$ for GSW scheme. As [BHP17] mentioned, DGSW scheme makes it more convenient to use the leakage resilient property of LHL to remove CRS.

### 2.6 Multi-Key Fully Homomorphic Encryption(MKFHE)

We review the definition of MKFHE in detail here, the main purpose of which is to compare with the definition of weak-MKFHE we proposed later.

**Definition 7.** *Let $\lambda$ be the security parameter, $L$ be the circuit depth, and $k$ be the number of participants. A Leveled multi-key fully homomorphic encryption scheme consists of a tuple of efficient probabilistic polynomial time algorithms* MKFHE=(Init, MKGen, MKEnc, MKExpand, MKEval, MKDec) *which defines as follows.*

- $\mathsf{pp} \leftarrow \mathsf{Init}(1^\lambda, 1^L)$ *: Input security parameter $\lambda$, circuit depth $L$, output system paremeter* $\mathsf{pp}$. *We assume that all algorithm take* $\mathsf{pp}$ *as input.*
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{MKGen}(\mathsf{pp}, \mathsf{id})$ *: Input* $\mathsf{pp}$*, identity* $\mathsf{id}$*, output a key pair for participant* $\mathsf{p}_i$*.*
- $c_i \leftarrow \mathsf{MKEnc}(\mathsf{pk}_i, u_i)$ *: Input* $\mathsf{pk}_i$ *and $u_i$, output ciphertext $c_i$.*
- $\bar{c}_i \leftarrow \mathsf{MKExpand}(\mathsf{pk}, c_i)$*:Input the ciphertext $c_i$ of participant* $\mathsf{p}_i$*, the public key set* $\mathsf{pk} = \{\mathsf{pk}_i\}_{i \in [k]}$ *of all participants, output expanded ciphertext $\bar{c}_i$ which is under* $f(\mathsf{sk}_i, \ldots \mathsf{sk}_k)$ *whose structure is undefined.*
- $\bar{c}_{eval} \leftarrow \mathsf{MKEval}(\bar{c}, \mathcal{C})$*:Input circuit $\mathcal{C}$, the set of all ciphertext $\bar{c} = \{\bar{c}_1 \ldots \bar{c}_N\}$ while $N$ is the input length of circuit $\mathcal{C}$, output evaluated ciphertext $\bar{c}_{eval}$*
- $u \leftarrow \mathsf{MKDec}(\bar{c}_{eval}, f(\mathsf{sk}_1 \ldots \mathsf{sk}_k))$ *: Input evaluated ciphertext $\bar{c}_{eval}$, total private key function* $f(\mathsf{sk}_1 \ldots \mathsf{sk}_k)$*, output $u$*

**Remark :**

1. The $\mathsf{MKExpand}(\cdot)$ algorithm is not necessary. For example, in the RLWE-based MKFHE scheme, the ciphertext expansion procedure is trivial, but in the LWE-based MKFHE scheme, the ciphertext expansion is a complicated and time-consuming process.
2. The ciphertext structure function $f(\mathsf{sk}_1, \ldots, \mathsf{sk}_k)$ represents an organization form, or a certain function, which is not unique, for example, it can be the concatenation of all keys or the sum of all keys.

**Properties implicited in the definition of MKFHE :** For the above definition, each participant is required in key generation and encryption phase independently to generates their own keys and completes the encryption operation without interaction between participants. These two phases are similar to single-key homomorphic encryption, the computational overhead is independent of $k$ and only related to $\lambda$ and $L$, only in the decryption phase, interaction is involved when participants perform a round of decryption protocol.

## 3 The weak version of Multi-key Fully homomorphic encryption(weak-MKFHE) scheme

### 3.1 The definition of weak-MKFHE

In order to cope with computationally-sensitive and trust-sensitive scenarios, we appropriately *tighten and loosen* the definition of MKFHE, we abandon ciphertext expansion procedure and introduce a **Key lifting** procedure. In addition, a tighter bound is required on the amount of local computation, as a compromise, we allow a small amount of interaction during **Key lifting**.

**Definition 8.** *A leveled* weak-MKFHE *scheme is a tuple of probabilistic polynomial time algorithm* (Init, wMKGen, wMKLift, wMKEnc, wMKEval, wMKDec)*, which can be divided into two phases, online phase:* wMKLift *and* wMKDec*, where interaction is allowed between participants, but the rounds should be constant, local phase :* wMKInit, wMKGen, wMKEnc*, and* wMKEval*, whose operations do not involve interaction. These five algorithms are described as follows:*

- $\mathsf{pp} \leftarrow \mathsf{wMKInit}(1^{\lambda}, 1^{L})$*:Input security parameter* $\lambda$*, circuit depth* $L$*, output public parameters* pp.
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{wMKGen}(\mathsf{pp}, \mathsf{id})$*:Input public parameter* pp*, identity* id*, output the key pair of participant* $\mathsf{p}_i$
- $\mathsf{hk}_i \leftarrow \mathsf{wMKLift}(\mathsf{pk}_i, \mathsf{sk}_i, \mathsf{id})$*: Input key pair of participants* $\mathsf{p}_i$*, output the hybrid key* $\mathsf{hk}_i$ *of* $\mathsf{p}_i$*..*
- $c_i \leftarrow \mathsf{wMKEnc}(\mathsf{hk}_i, u_i)$*: Input* $u_i$ *and* $\mathsf{hk}_i$*, output ciphertext* $c_i$
- $\hat{c} \leftarrow \mathsf{wMKEval}(\mathcal{C}, S)$*: Input circuit* $\mathcal{C}$*, ciphertext set* $S = \{c_i\}_{i\in[N]}$ *, output ciphertext* $\hat{c}$
- $u \leftarrow \mathsf{wMKDec}(\hat{c}, f(\mathsf{sk}_1 \dots \mathsf{sk}_k))$*: Input evaluated ciphertext* $\hat{c}$*,* $f(\mathsf{sk}_1 \dots \mathsf{sk}_k)$*, output* $u$*.*

**Remark :** weak-MKFHE does not have ciphertext expansion procedure, indeed, the inputed ciphertext set $S$ in $\mathsf{wMKEval}(\cdot)$ is encrypted by participants under their own hybrid key $\mathsf{hk}_i$ which are different among participants, however, the resulting ciphertext $c_i$ supports homomorphic evaluation without extra modification.

we require weak-MKFHE to satisfy the following properties:

**Locally Computationally Compactness :** *A leveled* weak-MKFHE *is locally computationally compact if the participants do the same number of encryptions as the single-key FHE scheme.*

**Low round complexity :** *Only constant round interaction is allow in* $\mathsf{wMKLift}(\cdot)$ *procedure.*

**IND-CPA security of encryption :** *Let* $\lambda$ *be the security parameter,* $L = \mathsf{poly}(\lambda)$ *is the circuit depth, for any probabilistic polynomial time adversary* $\mathcal{A}$*, he can distinguish the following two distributions with negligible advantage.*

$$\Pr\left[\,\mathcal{A}(\mathsf{pp}, \mathsf{pk}, \mathsf{wMKEnc}(\mathsf{pk}, 1)) - \mathcal{A}(\mathsf{pp}, \mathsf{pk}, \mathsf{wMKEnc}(\mathsf{pk}, 0)) \neq 0\,\right] = \mathsf{negl}(\lambda).$$

**Correctness and Compactness :** *A leveled* weak-MKFHE *scheme is correct if for a given security parameter* $\lambda$*, circuit depth* $L$*, participants* $k$*, we have the following*

$$\Pr\left[\,\mathsf{wMKDec}(f(\mathsf{sk}_1 \dots \mathsf{sk}_k), \hat{c}) \neq \mathcal{C}(u_1 \dots u_N)\,\right] = \mathsf{negl}(\lambda).$$

*probability is negligible, where* $\mathcal{C}$ *is a circuit with input length* $N$ *and depth length less than* $L$*. A leveled* weak-MKFHE *scheme is compact, if the size* $\hat{c}$ *of evaluated ciphertext is bounded by* $\mathsf{poly}(\lambda, L, k)$*, but independent of circuit size.*

### 3.2 Adversary model

**Rational adversary VS. Semi-malicious adversary**

the notion of semi-malicious adversary was introduce in [AJL+12], somewhat similar with the semi-honest model, semi-malicious adversary follows the steps specified in the protocol, but differently that the semi-honest model, it can choose the randomness that this protocol expect arbitrary and adaptively(as opposed to just choosing it at random).

The notion of rational adversary was introduced in [IML05]. Their work consider the problem which $N$ players were engaged in a competitive game to maximize their payoffs while maintaining their reputation. They give a definition of rational adversary and related security in the language of Game Theory, involving **mediated games** and **Nash equilibria**, more details please refer to [cited]. We give the definition of it in cryptography language.

**Rational Adversary(In Cryptography)**

**Definition 9.** *An adversary is rational if he runs the protocol as prescribed, but can adaptively choose arbitrarily value for any distribution(as opposed to just random uniform distribution) in the protocol to compromise other's privacy, while maintaining that the probability of being caught is* $\mathsf{negl}(\lambda)$*.*

It worth noting that the rational adversary is the midpoint between semi-malicious adversary and malicious adversary. Indeed, he can choosing arbitrary value for any distribution not just random distribution.

**Simulatability under rational adversary(In Cryptography)**

**Simulatable :** *The security definition can also be cast in ideal/real paradigm. Let $\Gamma$ be the game sequence played by honest players, $\Delta$ be the game sequence played by rational players, and $\phi$ be the advantage of learning other player's privacy, if $\phi(\Delta) - \phi(\Gamma) = \mathsf{negl}(\lambda)$, we say that game $\Gamma$ rational simulates $\Delta$.*

## 4 Scheme#1 : a weak-MKFHE scheme based on DGSW in plain model against rational adversary

### 4.1 Key lifting procedure

Following the definition of weak-MKFHE, it requires the ciphertext encrypted by hybrid key hk which is outputted by $\mathsf{wMKLift}(\cdot)$ algorithm is different among participants, to support homomorphic evaluation without extra modification. We achieve this property by allowing two round interaction between participants.

**Key Lifting**

- $\{\mathsf{hk}_i\}_{i\in[k]} \leftarrow \mathsf{wMKLift}(\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]})$: Input the DGSW key pair $\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]}$ of all participants, where $\mathsf{pk}_i = (\mathbf{A}_i, \mathbf{b}_{i,i})$, $\mathbf{A}_i \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{s}_i \leftarrow U\{0,1\}^{m-1}$, $\mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i \mod q$. All participants are engaged in the following two interaction :
  - First round : $\mathsf{p}_i$ broadcasts $(\mathbf{A}_i, \mathbf{b}_{i,i})$ and receives all $\{\mathbf{A}_j, \mathbf{b}_{j,j}\}_{j\in[k]}$.
  - Second round : $\mathsf{p}_i$ generates and disclose $\{\mathbf{b}_{i,j}\}_{j\in[k]}$, where $\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j \mod q$

After above two round interaction, $\mathsf{p}_i$ receives $\{\mathbf{b}_{j,i}\}_{j\in[k]}$

$$\text{let } \mathbf{b}_i = \sum_{j=1}^{k} \mathbf{b}_{j,i},\ \mathsf{p}_i \text{ output hybrid key } \mathsf{hk}_i = (\mathbf{A}_i, \mathbf{b}_i)$$

Let $\bar{\mathbf{t}} = (-\mathbf{s}, 1)$, $\mathbf{s} = \sum_{i=1}^{k} \mathbf{s}_i$, for ciphertext $\mathbf{C}_i$, $\mathbf{C}_j$ encrypted by hybrid key $\mathsf{hk}_i$, $\mathsf{hk}_j$ respectively :

$$\mathbf{C}_i = \begin{pmatrix} \mathbf{A}_i \\ \mathbf{b}_i \end{pmatrix} \mathbf{R}_1 + \mathbf{E}_1 + u_i\mathbf{G}, \qquad \mathbf{C}_j = \begin{pmatrix} \mathbf{A}_j \\ \mathbf{b}_j \end{pmatrix} \mathbf{R}_2 + \mathbf{E}_2 + u_j\mathbf{G},$$

obviously we have $\bar{\mathbf{t}}\mathbf{C}_i \approx u_i\bar{\mathbf{t}}\mathbf{G}$, $\bar{\mathbf{t}}\mathbf{C}_j \approx u_j\bar{\mathbf{t}}\mathbf{G}$(omit small error). Therefore, although $\mathbf{C}_i$ and $\mathbf{C}_j$ are encrypted by different hybrid keys, they correspond to the same decryption key $\bar{\mathbf{t}}$. As we'll point out later, however, this structure will drew some security concern. We remedy this problem by increasing the noise bounds in the last row of the noise matrix $\mathbf{E}$. we discuss the security of the scheme in Section 4.5

### 4.2 The entire scheme

Scheme#1 is based on the DGSW scheme, containing the following five algorithm (Init, wMKGen, wMKLift, wMKEnc, wMKEval, wMKDec)

- $\mathsf{pp} \leftarrow \mathsf{wMKInit}(1^\lambda, 1^L)$ : Let $\lambda$ be security parameter, $L$ be circuit depth, lattice dimension $n = n(\lambda, L)$, noise distribution $\chi$ over $\mathbb{Z}$, and $e \leftarrow \chi$, where $|e|$ is bounded by $B_\chi$, modulus $q = 2^{\lambda L}B_\chi$, $k = \mathsf{poly}(\lambda)$, $m = kn\log q + \lambda$, suitable choosing above parameters to make $\mathsf{LWE}_{n,m,q,B_\chi}$ is infeasible. Output $\mathsf{pp} = (k, n, m, q, \chi, B_\chi)$
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{wMKGen}(\mathsf{pp})$ : Input pp, output the DGSW key pair $(\mathsf{pk}_i, \mathsf{sk}_i)$ of participants $\mathsf{p}_i$, where $\mathsf{pk}_i = (\mathbf{A}_i, \mathbf{b}_{i,i})$, $\mathbf{A}_i \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{s}_i \leftarrow U\{0,1\}^{m-1}$, $\mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i \mod q$.
- $\mathsf{hk}_i \leftarrow$ **Key Lifting** : All participants are engaged in the **Key lifting procedure 4.1**, output the hybrid key $\mathsf{hk}_i$.

- $\mathbf{C}_i \leftarrow \mathsf{wMKEnc}(\mathsf{hk}_i, u_i)$: Input hybrid key $\mathsf{hk}_i$, plaintext $u_i$, output ciphertext $\mathbf{C}_i = \begin{pmatrix}\mathbf{A}_i\\ \mathbf{b}_i\end{pmatrix}\mathbf{R} + \mathbf{E} + u_i\mathbf{G}$, where $\mathbf{R} \leftarrow \chi^{n\times ml}$, $l = \lceil \log q \rceil$, $\mathbf{E} = \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1\end{pmatrix}$, $\mathbf{E}_0 \leftarrow \chi^{(m-1)\times ml}$, $\mathbf{e}_1 \leftarrow \chi'^{\,ml}$, $\chi'$ is a distribution over $\mathbb{Z}$, satisfying $|\mathbf{e}_1|$ is bounded by $2^{\lambda^{\epsilon_1}} B_\chi$, $\epsilon_1 \in (0, \frac{1}{2})$, $\mathbf{G} = \mathbf{I}_m \otimes \mathbf{g}$ is a gadget matrix.
- $\hat{\mathbf{C}} \leftarrow \mathsf{wMKEval}(S, \mathcal{C})$ : Input the ciphertext $S = \{\mathbf{C}_i\}_{i\in[N]}$ which are encrypted by hybrid key $\{\mathsf{hk}_i\}_{i\in[k]}$, circuit $\mathcal{C}$ with input length $N$, output $\hat{\mathbf{C}}$.

**Homomorphic addition and multiplication**

- $\mathbf{C}_{\mathsf{add}} \leftarrow \mathsf{wMKAdd}(\mathbf{C}_1, \mathbf{C}_2)$: Input ciphertext $\mathbf{C}_1$, $\mathbf{C}_2$, output $\mathbf{C}_{\mathsf{add}} = \mathbf{C}_1 + \mathbf{C}_2$, Obviously $\bar{\mathbf{t}}\mathbf{C}_{\mathsf{add}} \approx (u_1 + u_2)\bar{\mathbf{t}}\mathbf{G}$
- $\mathbf{C}_{\mathsf{mult}} \leftarrow \mathsf{wMKMult}(\mathbf{C}_1, \mathbf{C}_2)$: Input ciphertext $\mathbf{C}_1$, $\mathbf{C}_2$, output $\mathbf{C}_{\mathsf{mult}} = \mathbf{C}_1\mathbf{G}^{-1}(\mathbf{C}_2)$, Obviously $\bar{\mathbf{t}}\mathbf{C}_{\mathsf{mult}} \approx u_1u_2\bar{\mathbf{t}}\mathbf{G}$

**Distributed decryption** Similar to [MW16], the decryption procedure is a distributed procedure :

- $\mathsf{LocalDec}$: Input $\hat{\mathbf{C}}$, let $\hat{\mathbf{C}} = \begin{pmatrix}\mathbf{C}_0\\ \mathbf{c}_1\end{pmatrix}$, where $\mathbf{C}_0 \in \mathbb{Z}_q^{(m-1)\times ml}$, $\mathbf{c}_1 \in \mathbb{Z}_q^{ml}$, $\mathsf{p}_i$ computes $\beta_i = \langle \mathbf{s}_i,\ \mathbf{C}_0\mathbf{G}^{-1}(\mathbf{w}^T)\rangle$, and set $\gamma_i = \beta_i + e_i''$, where $\mathbf{w} = (0, \ldots, 0, \lceil q/2 \rceil) \in \mathbb{Z}_q^m$, $e_i'' \leftarrow \chi''$ is a distribution over $\mathbb{Z}$, satisfying $|e_i''| < 2^{L\lambda^{\epsilon_2}} B_\chi$, $\epsilon_2 \in (\frac{1}{2}, 1)$, then $\mathsf{p}_i$ broadcast $\gamma_i$
- $\mathsf{FinalDec}$: After received $\{\gamma_i\}_{i\in[k]}$, let $\gamma = \sum_{i=1}^k \gamma_i + \langle \mathbf{c}_1,\ \mathbf{G}^{-1}(\mathbf{w}^T)\rangle$, output $u = \lceil \frac{\gamma}{q/2} \rfloor$

### 4.3 Bootstrapping

In order to eliminate the dependence on the circuit depth to achieve fully homomorphism, we need to use Gentry's bootstrapping technology. It is worth noting that the bootstrapping procedure of $\mathsf{Scheme\#1}$ is the same as single-key homomorphic scheme: After **Key lifting** procedure, participant $\mathsf{p}_i$ uses hybrid key $\mathsf{hk}_i$ to encrypt $s_i$ to obtain evaluation key $\mathsf{evk}_i$. Because $\mathsf{evk}_i$ and $\hat{\mathbf{C}}$ are both ciphertexts under $\bar{\mathbf{t}} = (-\sum_{i=1}^k \mathbf{s}_i, 1)$, homomorphic evaluation of the decryption circuit could be executed directly as $\hat{\mathbf{C}}$ are need to be refresh. Therefore, in order to evaluate any depth circuit, we only need to set the initial parameters to satisfy the homomorphic evaluation of the decryption circuit.

However, for those $\mathsf{MKFHE}$ schemes that requires ciphertext expansion, additional ciphertext expansion is required, for the reason that $\hat{\mathbf{C}}$ is the ciphertext under $\bar{\mathbf{t}}$, but $\{\mathsf{evk}_i\}_{i\in[k]}$ are the ciphertext under $\{\mathbf{t}_i\}_{i\in[k]}$. This is another large amount of computational overhead, because in order to expand $\{\mathsf{evk}_i\}_{i\in[k]}$, participant $\mathsf{p}_i$ needs to encrypt the random matrix of the ciphertext corresponding to $\mathsf{evk}_i$.

### 4.4 Correctness analysis

To illustrate the correctness of $\mathsf{Scheme\#1}$, we first study the accumulation of noise:

$$\text{Let } \mathbf{s} = \sum_{i=1}^k \mathbf{s}_i,\ \ \mathbf{t} = (-\mathbf{s}, 1),\ \text{ for fresh ciphertext } \mathbf{C} = \begin{pmatrix}\mathbf{A}_i\\ \mathbf{b}_i\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1\end{pmatrix} + u\mathbf{G}$$

we have $\mathbf{tC} = \mathbf{e}_1 + \mathbf{sE}_0 + u\mathbf{tG}$, let $\mathsf{e}_{\mathsf{init}} = \mathbf{e}_1 + \mathbf{sE}_0$, Obviously $|\mathsf{e}_{\mathsf{init}}| < (2^{\lambda^{\epsilon_1}} + km)B_\chi$.

After $L$ depth circuit evaluation, let $\mathbf{e}_L = (ml)^L \mathsf{e}_{\mathsf{init}}$. According to the **distributed encryption** of $\mathsf{Scheme\#1}$ we have :

$$\gamma = \sum_{i=i}^k \beta_i + \mathbf{C}_1\mathbf{G}^{-1}(\mathbf{w}^T) = \langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \sum_{i=1}^k e_i'' + u\lfloor \frac{q}{2} \rceil \tag{1}$$

Let $e_{\mathsf{final}} = \langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \sum_{i=1}^k e_i''$. In order to decrypt correctly, it requires $e_{\mathsf{final}} < \frac{q}{4}$. For our parameter settings, obviously $|e_i''| > \langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle$, for taking the logarithm of both sides:

$$\log e_i'' = \lambda^{\epsilon_2} L$$
$$\log\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle = \log(knL(\lambda)^{(2L+1)}(2^{\lambda^{\epsilon_2}} + k^2 n\lambda L))B_\chi = O(L + \lambda^{\epsilon_2})$$

thus $e_{\mathsf{final}} < \frac{q}{4}$.

### 4.5 Simulatability under rational adversary

In $\mathsf{Scheme\#1}$, the value $\phi(\varGamma) - \phi(\varDelta)$ between the game sequence $\varGamma$ and $\varDelta$ depends on the choose of $\{\mathbf{A}_i, \mathbf{s}_i\}_{i\in[k]}$. For a honest player $\mathsf{p}_i$, he generates $\mathbf{A}_i \leftarrow U(\mathbb{Z}_q^{(m\times n)})$, $\mathbf{s}_i \leftarrow \{0,1\}^m$ as the protocol specification, but an adversary(rational or irrational) may generates it arbitrarily. Brakerski et al. [BHP17] proved that the $\mathsf{DGSW}$ scheme is leakage resilient, thus for arbitrary $\mathbf{A}_i$ the value $\phi(\varGamma) - \phi(\varDelta) = \mathsf{negl}(\lambda)$. We deal with what happens when $\mathbf{s}_i$ changes. Let $B_{\mathsf{sis}}$ be the bound keeping the $\mathsf{SIS}_{m,n,q,B_{\mathsf{sis}}}$ problem hard, according to Theorem 4, if $B_{\mathsf{sis}} \ll q^{n/m}$, the problem is vacuously hard, most likely, such solutions do not exists, if $B_{\mathsf{sis}} \gg \gamma^m \cdot q^{n/m}$, this is an instance of $\mathsf{approx\text{-}SVP}$ with exponential approximation factor $\gamma$, which can be solved by LLL [LLL82]. Somewhere in between these bounds is where cryptography takes place, typically for $B_{\mathsf{sis}} = q^{n/m} \cdot \mathsf{poly}(\lambda)$. For our parameter Settings $B_{\mathsf{sis}} = q^{n/m} \cdot \mathsf{poly}(\lambda) = \mathsf{poly}(\lambda)$.

Depending on the choice of $\mathbf{s}_i$, it can be divided into two cases : (1) $|\mathbf{s}_i|_\infty < B_{\mathsf{sis}}$, (2) $|\mathbf{s}_i|_\infty > B_{\mathsf{sis}}$. In addition, there is a special case where the player $\mathsf{p}_i$ dose not generate $\mathbf{s}_i$ at all, but adaptively choose $\{\mathbf{b}_i\}_{i\in[k]}$.

For a rational adversary, he is better off generating $|\mathbf{s}_i|_\infty < B_{\mathsf{sis}}$, otherwise, in the latter two case he will be caught with non-negligible probability. First we prove **Case 1**.

**Case 1 :** $|\mathbf{s}_i|_\infty < B_{\mathsf{sis}}$.

We complete the simulation by constructing a reduction from $\mathsf{Scheme\#1}$ to the $\mathsf{DGSW}$ scheme. Consider the following $\mathsf{Game}$:

1. Challenger generates $\mathsf{pk}_{\mathsf{DGSW}} = (\mathbf{A}, \mathbf{b}_1)$ where $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{b}_1 = \mathbf{s}_1\mathbf{A}$, $\mathbf{s}_1 \leftarrow U\{0,1\}^m$ and send $\mathsf{pk}_{\mathsf{DGSW}}$ to rational adversary $\mathcal{A}$
2. $\mathcal{A}$ adaptively chooses $\{\mathbf{s}_i\}_{i\in[k]/1}$ where $|\mathbf{s}_i| < B_{\mathsf{sis}}$ and generates $\{\mathbf{b}_i\}_{i\in[k]/1}$, $\mathbf{b}_i = \mathbf{s}_i\mathbf{A}$, choose a bit $u \in \{0,1\}$ and set $\mathsf{hk}_{\mathsf{Scheme\#1}} = (\mathbf{A}, \mathbf{b})$, where $\mathbf{b} = \sum_{i=1}^{k} \mathbf{b}_i$, then send $\mathsf{hk}_{\mathsf{Scheme\#1}}$ and $u$ to Challenger.
3. Challenger choose a bit $\alpha \in \{0,1\}$, if $\alpha = 0$ , set $\mathbf{C}_{\mathsf{Scheme\#1}} \leftarrow \mathsf{wMKEnc}(\mathsf{hk}_{\mathsf{Scheme\#1}}, u)$, otherwise $\mathbf{C}_{\mathsf{Scheme\#1}} \leftarrow U(\mathbb{Z}_q^{m\times ml})$, and send $\mathbf{C}_{\mathsf{Scheme\#1}}$ to $\mathcal{A}$
4. After receiving $\mathbf{C}_{\mathsf{Scheme\#1}}$, $\mathcal{A}$ output bit $\bar{\alpha}$, if $\bar{\alpha} = \alpha$, then $\mathcal{A}$ wins.

**Lemma 10.** *Let* $\mathsf{Adv} = |Pr[\bar{\alpha} = \alpha] - \frac{1}{2}|$ *denote $\mathcal{A}$'s advantage in winning the game, If $\mathcal{A}$ can win the game with advantage* $\mathsf{Adv}$*, then $\mathcal{A}$ can distinguish between the ciphertext distribution of* $\mathsf{DGSW}$ *and the uniform random distribution with the same advantage.*

*Proof.* We construct $\mathbf{C}_{\mathsf{Scheme\#1}}$ by $\mathsf{DGSW.Enc}(\mathsf{pk}_{\mathsf{DGSW}}, u)$:

1. First, Challenger generates $\mathsf{pk}_{\mathsf{DGSW}}$ like the step 1 of above $\mathsf{Game}$, set $\mathbf{C}_{\mathsf{DGSW}} = \mathsf{DGSW.Enc}(\mathsf{pk}_{\mathsf{DGSW}}, u)$ send the both to $\mathcal{A}$.
2. $\mathcal{A}$ generates $\{\mathbf{s}_i\}_{i\in[k]/1}$, let $\mathbf{s}' = \sum_{i=2}^{k} \mathbf{s}_i$, $\mathbf{C}_{\mathsf{DGSW}} = \begin{pmatrix} \mathbf{C}_0 \\ \mathbf{c}_1 \end{pmatrix}$, $\mathbf{C}' = \begin{pmatrix} \mathbf{C}_0 \\ \mathbf{c}_1 + \mathbf{c}'_1 \end{pmatrix}$, where $\mathbf{c}'_1 = \mathbf{s}'\mathbf{C}_0$, obviously $\mathbf{C}' = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \begin{pmatrix} \mathbf{E}_0 \\ \mathbf{e}_1 + \mathbf{s}'\mathbf{E}_0 \end{pmatrix}$.

For our parameter settings $|\mathbf{e}_1| < 2^{\lambda^{\epsilon_1}} B_\chi$, $|\mathbf{s}'\mathbf{E}_0| < kmB_\chi B_{\mathsf{sis}}$, thus $\mathbf{e}_1/\mathbf{s}'\mathbf{E}_0 = \mathsf{negl}(\lambda)$, we have $\mathbf{C}' \overset{\mathsf{stat}}{\approx} \mathbf{C}_{\mathsf{Scheme\#1}}$, if $\mathcal{A}$ can distinguish between $\mathbf{C}_{\mathsf{Scheme\#1}}$ and uniform random distribution by advantage $\mathsf{Adv}$, then he can distinguish between $\mathsf{DGSW.Enc}(\mathsf{pk}_{\mathsf{DGSW}}, u)$ and the uniform random distribution with the same advantage.

**Remark:** we require $k$ to be bounded by $\mathsf{poly}(\lambda)$, because if a larger $k$ is introduced, it will lead to a larger smudging error, which further leads to a larger $q$. For our choice of $q = 2^{\lambda L} B_\chi$, the corresponding approximation factor of the $\mathsf{SVP}$ problem is $\tilde{O}(2^{\lambda L})$

**Case 2 :** $|\mathbf{s}_i|_\infty > B_{\mathsf{sis}}$.

In the second round of **Key lifting procedure**, after $\mathsf{p}_i$ generates and discloses $\{\mathbf{b}_{i,j}\}_{j\in[k]}$, where $\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j \mod q$, $|\mathbf{s}_i|_\infty > B_{\mathsf{sis}}$, any participant $\mathsf{p}_{j,j\neq i}$ can solve $\mathbf{s}_i \in \mathbb{Z}_q^m$ with non-negligible probability. Note that being able to solve for $\mathbf{s}_i$ doesn't imply anything. Because $m = kn\log q + \lambda >$

$n \log q$, for a given $\mathbf{b}_{i,j} \in \mathbb{Z}_q^m$, there are many trivial solution $\mathbf{s}_i \in \mathbb{Z}_q^m$ satisfy $\mathbf{b}_{i,j} = \mathbf{s}_i \mathbf{A}_j$. However, $\mathsf{p}_j$ can check the set $\{\mathbf{b}_{i,t}\}_{t\in[k]/j}$ against the value of $\mathbf{s}_i$, as long as there is a $\mathbf{b}_{i,t} \in \{\mathbf{b}_{i,t}\}_{t\in[k]/j}$ that satisfies $\mathbf{b}_{i,t} = \mathbf{s}_i \mathbf{A}_t$, then $\mathsf{p}_i$ is cheating. Note that there is a negligible false positive rate here : let $\mathbf{s}_1 \in \{0,1\}^m$, $\mathbf{s}_2 \in \mathbb{Z}_q^m$, $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{(m\times n)})$, satisfy $\mathbf{s}_1\mathbf{A} = \mathbf{s}_2\mathbf{A}$, for another $\mathbf{A}' \leftarrow U(\mathbb{Z}_q^{(m\times n)})$, the probability that $\mathbf{s}_1\mathbf{A}' = \mathbf{s}_2\mathbf{A}'$ happens exactly is $2^{-n\log q}$.

thus if an adversary set $|\mathbf{s}_i|_\infty > B_{\mathsf{sis}}$, he will be caught with non-negligible probability.

**Case 3 :** $\mathsf{p}_i$ dose not generate $\mathbf{s}_i$ at all, but adaptively choose $\{\mathbf{b}_{i,j}\}_{j\in[k]}$.

Indeed, in this case, $\mathsf{p}_i$ can not be found cheating until the decryption procedure. By default, the decryption result is readable. Due to the mismatch between the public key and the private key, the decryption result is unreadable. When the private key is required to prove innocence, $\mathsf{p}_i$ will be found to be a cheater.

### 4.6 Simulatability of distributed decryption procedure

Similar to [MW16], we get a weak simulation of the distributed decryption procedure: input all private keys $\{\mathsf{sk}_j\}_{j\in[k]/i}$ except $\mathsf{sk}_i$, evaluated result $u_{\mathsf{eval}}$, ciphertext $\hat{\mathbf{C}}$, we can simulate the local decryption result $\gamma_i$. For stronger security requirements : input any private key set $\{\mathsf{sk}_j\}_{j\in S}$, $S$ is any subset of $[k]$, evaluated result $u_{\mathsf{eval}}$ and ciphertext $\hat{\mathbf{C}}$, to simulate $\{\gamma_i\}_{i\in U,\ U=[k]-S}$, we don't know how to achieve it.

According to equantion 1 we have $\gamma = \sum_{i=1}^k \gamma_i + \mathbf{C}_1\mathbf{G}^{-1}(\mathbf{w}^T)$

$$\text{thus } \gamma_i = u_{\mathsf{eval}} \lfloor \frac{q}{2} \rceil + e_{\mathsf{final}} + \sum_{i=1}^k e_i'' + \mathbf{C}_1\mathbf{G}^{-1}(\mathbf{w}^T) - \sum_{j\neq i}^k \gamma_j$$

For a simulator $\mathcal{S}$, input $\{\mathsf{sk}_j\}_{j\in[k]/i}$, evaluated result $u_{\mathsf{eval}}$, ciphertext $\hat{\mathbf{C}}$, output simulated $\gamma_i'$

$$\gamma_i' = u_{\mathsf{eval}} \lfloor \frac{q}{2} \rceil + \sum_{i=1}^k e_i'' + \mathbf{C}_1\mathbf{G}^{-1}(\mathbf{w}^T) - \sum_{j\neq i}^k \gamma_j.$$

For our parameter settings, we have :

$$|\sum_{i=1}^k e_i''| < k \cdot 2^{L\lambda^{\epsilon_2}} B_\chi$$
$$e_{\mathsf{final}} < kn(L\lambda)^{(2L+1)}(2^{\lambda^{\epsilon_2}} + k^2 nL\lambda)B_\chi = 2^{O(L\lambda^{\epsilon_1})}B_\chi$$
$$\text{thus } |e_{\mathsf{final}} / \sum_{i=1}^k e_i''| = k \cdot 2^{-\omega(L\lambda^{\epsilon_2} - L\lambda^{\epsilon_1})} = \mathsf{negl}(\lambda)$$

we have $\gamma_i \overset{\mathsf{stat}}{\approx} \gamma_i'$.

## 5 Scheme#2 : weak-MKFHE based on RLWE in ROM

It is regrettable that general polynomial ring $R : \mathbb{Z}[x]/f(x)$ cannot enjoy the leak resilient property of the leftover hash lemma on the integer ring $\mathbb{Z}$. This means that we cannot transplant the above construction process trivially to RLWE-based FHE. Indeed, [DSGKS21] pointed out that for $\mathbf{x} = (x_1, \ldots, x_l) \in R^l$, if the *j-th* NTT coordinate of each $x_{i,i\in[l]}$ is leaked, then the *j-th* NTT coordinate of $a_{l+1} = \sum_{i=1}^l a_i x_i$ is defined, thus $a_{l+1}$ is far from random, although the leakage ratio is only 1/n. We also noticed a trivial solution : for $\mathbf{a}, \mathbf{s} \in R_q^l$, $b = \langle \mathbf{a}, \mathbf{s} \rangle \in R_q$, $b$ leaks information about $\mathbf{s}$ at most $n \log q$ bits, therefore, as long as we set $l$ long enough, for example, $l = l + n\log q$, then obviously $b$ is close to uniformly random, but this will result in a extremely large key, thus it is not practical.

To ensure the independence of the $\{a_i\}_{i\in[k]}$ generated by each participant, we simply added a round of bit commitment protocol. Under the Random Oracle Model, the cryptographic hash function is used to ensure the independence of $\{a_i\}_{i\in[k]}$. Let $H : \{0,1\}^\star \to \{0,1\}^\lambda$ be a cryptography hash function, $a_i \in R_q,\ H(a_i) = \delta_i$. For a given $\delta \in \{0,1\}^\lambda$, an adversary $\mathcal{A}$ sends a query $x \in \{0,1\}^\star$ to $H$, which happens to have probability $\Pr[H(x) = \delta] = \frac{1}{2^\lambda}$. Let $\mathsf{Adv}$ denotes the probability that $\mathcal{A}$ finds a collision after making $q_{\mathsf{ro}} = \mathsf{poly}(\lambda)$ queries, Obviously $\mathsf{Adv} = \mathsf{negl}(\lambda)$, we have the following result.

**Lemma 11.** *For a given $\delta \in \underline{\{0,1\}}^\lambda$, k probabilistic polynomial time(ppt) adversary $\mathcal{A}$, Each $\mathcal{A}$ makes $q_{ro} = \mathsf{poly}(\lambda)$ queries to $H$, let $\overline{\mathsf{Adv}}$ denotes the probability of finding a collision, then:* $\overline{\mathsf{Adv}} = \mathsf{negl}(\lambda)$

For $\mathsf{Scheme\#2}$, we only describe its key generation and re-linearization procedure in detail, the encryption, evaluation and decryption algorithm is similar to other $\mathsf{RLWE\text{-}based}$ $\mathsf{MKFHE}$ schemes.

### Key generation with bit commitment.

$k$ participants perform the following steps to get their own public key and evaluation key

1. $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$:Input security parameter $\lambda$, circuit depth $L$, output $\mathsf{pp} = (d, q, \chi, B_\chi)$, which $\chi$ is an noise distribution over $R : \mathbb{Z}[x]/x^d + 1$, satisfying $e \leftarrow \chi$, $||e||_\infty^{can}$ is bounded by $B_\chi$, and $\mathsf{RLWE}_{d,q,\chi,B_\chi}$ is infeasible.
2. $\mathsf{p}_i$ generates $\varPhi_i = \{a_i, \mathbf{d}_i, \mathbf{f}_i\}$ where $a_i \leftarrow U(R_q)$ is used for public key, $\mathbf{d}_i$, $\mathbf{f}_i \leftarrow U(R_q^l)$ for evaluation key, and commitment $\varPsi_i = \{\delta_i,\ \epsilon_i,\ \zeta_i\}$, $\delta_i = H(a_i)$, $\epsilon_i = H(\mathbf{d}_i)$, $\zeta_i = H(\mathbf{f}_i)$, broadcast $\varPsi_i$.
3. After all $\{\varPsi_i\}_{i\in[k]}$ are public, $\mathsf{p}_i$ discloses $\varPhi_i$.
4. After receiving $\{\varPhi_j\}_{j\in[k]/i}$, $\mathsf{p}_i$ broadcast $\{b_i,\ \mathbf{h}_i\}$, where $b_i = as_i + e_1$, $\mathbf{h}_i = \mathbf{d}s_i + \mathbf{e}_2$, $a = \sum_{i=1}^k a_i$, $\mathbf{d} = \sum_{i=1}^k \mathbf{d}_i$, $(s_i,\ e_1,\ \mathbf{e}_2) \leftarrow \chi^{l+2}$.
5. After receiving $\{b_j,\ \mathbf{h}_j\}_{j\in[k]/i}$, $\mathsf{p}_i$ output $\mathsf{pk}_i = (a, b)$ and evaluation key $\mathsf{evk}_i = (\mathbf{h}_i, \boldsymbol{\eta}_i, \boldsymbol{\theta}_i)$

$$b = \sum_{i=1}^k b_i \qquad \boldsymbol{\eta}_i = \mathbf{d}r_i + \mathbf{e}_3 + s_i\mathbf{g}$$

$$\boldsymbol{\theta}_i = \mathbf{f}s_i + \mathbf{e}_4 + r_i\mathbf{g} \qquad (r_i,\ \mathbf{e}_3,\ \mathbf{e}_4) \leftarrow \chi^{2l+1}$$

### Re-linearization ciphertext

Multiplying two ciphertext $\mathbf{c}_1$, $\mathbf{c}_2 \in R_q^2$, which under the same private key $\mathbf{t} = (1, s)$, $s = \sum_{i=1}^k s_i$, resulting $\mathbf{c}_{\mathsf{mult}} = \mathbf{c}_1 \otimes \mathbf{c}_2 \in R_q^4$, where its corresponding private key is $\mathbf{t} \otimes \mathbf{t} = (1, s, s, s^2)$. In order to re-linearize $\mathbf{c}_{\mathsf{mult}}$ , we need to construct the ciphertext of $s^2$ under $\mathbf{t}$. Let total evaluation key $\boldsymbol{\varPi} = (\boldsymbol{\eta}, \boldsymbol{\theta}, \mathbf{h})$.

$$\text{where } \boldsymbol{\eta} = \sum_{i=1}^k \boldsymbol{\eta}_i \quad \boldsymbol{\theta} = \sum_{i=1}^k \boldsymbol{\theta}_i \quad \mathbf{h} = \sum_{i=1}^k \mathbf{h}_i$$

Let $\mathbf{k} = (\mathbf{k}_0, \mathbf{k}_1)$, $\mathbf{k}_0 = -\boldsymbol{\theta}\mathbf{g}^{-1}(\mathbf{h}) \in R_q^l$, $\mathbf{k}_1 = (\boldsymbol{\eta} + \mathbf{f}\mathbf{g}^{-1}(\mathbf{h})) \in R_q^l$, obviously $\mathbf{k}_0 + \mathbf{k}_1 s \approx s^2\mathbf{g}$ (omit small error). Let $\mathbf{c}_{\mathsf{mult}} = (c_0, c_1, c_2, c_3)$.

$$\begin{aligned}\langle \mathbf{c}_{mult}, \mathbf{t} \otimes \mathbf{t}\rangle &= c_0 + (c_1 + c_2)s + s^2 c_3 \\ &= c_0 + (c_1 + c_2)s + s^2\mathbf{g}\mathbf{g}^{-1}(c_3) \\ &= c_0 + \mathbf{k}_0\mathbf{g}^{-1}(c_3) + (c_1 + c_2 + \mathbf{k}_1\mathbf{g}^{-1}(c_3))s.\end{aligned}$$

Let $\mathbf{c}_{\mathsf{linear}} = (c_0', c_1')$, $c_0' = c_0 + \mathbf{k}_0\mathbf{g}^{-1}(c_3)$, $c_1' = c_1 + c_2 + \mathbf{k}_1\mathbf{g}^{-1}(c_3)$, output $\mathbf{c}_{\mathsf{linear}}$ as re-linearized ciphertext. The algorithm defines as follows:

- $\mathbf{c}_{\mathsf{linear}} \leftarrow \mathsf{Relinear}(\mathbf{c}_{\mathsf{mult}},\ \{\mathsf{evk}_i\}_{i\in[k]})$: Input $\mathbf{c}_{\mathsf{mult}} \in R_q^4$, evaluation key $\{\mathsf{evk}_i\}_{i\in[k]}$, perform the following algorithem, output $\mathbf{c}_{\mathsf{linear}} = (c_0', c_1')$.

Due to the sum structure of keys, the dimension of $\mathbf{t} \otimes \mathbf{t}$ is independent of participants $k$, thus above algorithm pulls the tensor product ciphertext back to initial dimension by one shot, and introduces less noise than those keys with concatenation structure.

```
Ciphertext Relinearization
Input: $\mathbf{c}_{\mathsf{mult}} = (c_0, c_1, c_2, c_3) \in R_q^4,\ \{\mathsf{evk}_i\}_{i\in[k]} = \{\mathbf{h}_i,\ \boldsymbol{\eta}_i,\ \boldsymbol{\theta}_i\}_{i\in[k]}$
Output: $\mathbf{c}_{\mathsf{linear}} = (c_0', c_1') \in R_q^2$
1: $\boldsymbol{\eta} \leftarrow \sum_{i=1}^{k} \boldsymbol{\eta}_i,\ \boldsymbol{\theta} \leftarrow \sum_{i=1}^{k} \boldsymbol{\theta}_i,\ \mathbf{h} \leftarrow \sum_{i=1}^{k} \mathbf{h}_i$
2: $\mathbf{k}_0 \leftarrow -\boldsymbol{\theta}\mathbf{g}^{-1}(\mathbf{h}),\ \mathbf{k}_1 \leftarrow \boldsymbol{\eta} + \mathbf{f}\mathbf{g}^{-1}(\mathbf{h})$
3: $c_0' \leftarrow c_0 + \mathbf{k}_0\mathbf{g}^{-1}(c_3),\ c_1' \leftarrow c_1 + c_2 + \mathbf{k}_1\mathbf{g}^{-1}(c_3)$
4: Output: $(c_0', c_1')$
5: End.
```

## 6 Conclusions

For the LWE-based MKFHE in order to alleviate the overhead of the local participants, we proposed the concept of weak-MKFHE which introduced a **Key lifting** procedure, getting rid of expensive ciphertext expansion operation and construct a DGSW style weak-MKFHE under plain model. Our Scheme#1 is more friendly to local participants than previous scheme, since there is no need to encrypt random matrix preparing for ciphertext expansion. However, to support semantic security and threshold decryption, module $q$ is required to be $O(2^{\lambda L})$ , such a large $q$ results in high overhead of ciphertext evaluation. Reducing $q$ while ensuring security is the future direction.

For the multi-key homomorphic scheme based on RLWE, although the computation overhead of the local participants is not large: to perform re-linearization, only one ring element needs to be encrypted, but the common random string is always an insurmountable hurdle. Constructing RLWE-type MKFHE under plain model is the future direction.

## References

AJJM20. P. Ananth, A. Jain, Z. Jin, and G. Malavolta. Multi-key fully-homomorphic encryption in the plain model. In *TCC 2020, Part I*, *LNCS* 12550, pages 28–57. Springer, Heidelberg, November 2020.

AJL+12. G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs. Multiparty computation with low communication, computation and interaction via threshold FHE. In *EUROCRYPT 2012*, *LNCS* 7237, pages 483–501. Springer, Heidelberg, April 2012.

Ajt96. M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

AP14. J. Alperin-Sheriff and C. Peikert. Faster bootstrapping with polynomial error. In *CRYPTO 2014, Part I*, *LNCS* 8616, pages 297–314. Springer, Heidelberg, August 2014.

BGV12. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In *ITCS 2012*, pages 309–325. ACM, January 2012.

BHP17. Z. Brakerski, S. Halevi, and A. Polychroniadou. Four round secure computation without setup. In *TCC 2017, Part I*, *LNCS* 10677, pages 645–677. Springer, Heidelberg, November 2017.

BP16. Z. Brakerski and R. Perlman. Lattice-based fully dynamic multi-key FHE with short ciphertexts. In *CRYPTO 2016, Part I*, *LNCS* 9814, pages 190–213. Springer, Heidelberg, August 2016.

CD+15. R. Cramer, I. B. Damgård, et al. *Secure multiparty computation.* Cambridge University Press, 2015.

CDKS19. H. Chen, W. Dai, M. Kim, and Y. Song. Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In *ACM CCS 2019*, pages 395–412. ACM Press, November 2019.

CGGI16. I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *ASIACRYPT 2016, Part I*, *LNCS* 10031, pages 3–33. Springer, Heidelberg, December 2016.

CKKS17. J. H. Cheon, A. Kim, M. Kim, and Y. S. Song. Homomorphic encryption for arithmetic of approximate numbers. In *ASIACRYPT 2017, Part I*, *LNCS* 10624, pages 409–437. Springer, Heidelberg, December 2017.

CM15. M. Clear and C. McGoldrick. Multi-identity and multi-key leveled FHE from learning with errors. In *CRYPTO 2015, Part II*, *LNCS* 9216, pages 630–656. Springer, Heidelberg, August 2015.

DSGKS21. D. Dachman-Soled, H. Gong, M. Kulkarni, and A. Shahverdi. Towards a ring analogue of the leftover hash lemma. *Journal of Mathematical Cryptology*, 15(1):87–110, 2021.

FV12. J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012. https://eprint.iacr.org/2012/144.

Gen09a. C. Gentry. *A fully homomorphic encryption scheme.* Stanford university, 2009.

Gen09b. C. Gentry. Fully homomorphic encryption using ideal lattices. In *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009.

GPV08. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

GSW13. C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *CRYPTO 2013, Part I*, *LNCS* 8042, pages 75–92. Springer, Heidelberg, August 2013.

ILL89. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions (extended abstracts). In *21st ACM STOC*, pages 12–24. ACM Press, May 1989.

IML05. S. Izmalkov, S. Micali, and M. Lepinski. Rational secure computation and ideal mechanism design. In *46th FOCS*, pages 585–595. IEEE Computer Society Press, October 2005.

Lin13. Y. Lindell. Fast cut-and-choose based protocols for malicious and covert adversaries. In *CRYPTO 2013, Part II*, *LNCS* 8043, pages 1–17. Springer, Heidelberg, August 2013.

LLL82. A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.

LP07. Y. Lindell and B. Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In *EUROCRYPT 2007*, *LNCS* 4515, pages 52–78. Springer, Heidelberg, May 2007.

LPR10. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *EUROCRYPT 2010*, *LNCS* 6110, pages 1–23. Springer, Heidelberg, May / June 2010.

LPR13. V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-lwe cryptography. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 35–54. Springer, 2013.

LTV12. A. López-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *44th ACM STOC*, pages 1219–1234. ACM Press, May 2012.

MGW87. S. Micali, O. Goldreich, and A. Wigderson. How to play any mental game. In *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC*, pages 218–229. ACM, 1987.

Mic04. D. Micciancio. Almost perfect lattices, the covering radius problem, and applications to ajtai's connection factor. *SIAM Journal on Computing*, 34(1):118–169, 2004.

MP12. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *EUROCRYPT 2012*, *LNCS* 7237, pages 700–718. Springer, Heidelberg, April 2012.

MP13. D. Micciancio and C. Peikert. Hardness of sis and lwe with small parameters. In *Annual Cryptology Conference*, pages 21–39. Springer, 2013.

MR04. D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. In *45th FOCS*, pages 372–381. IEEE Computer Society Press, October 2004.

MTBH21. C. Mouchet, J. R. Troncoso-Pastoriza, J.-P. Bossuat, and J.-P. Hubaux. Multiparty homomorphic encryption from ring-learning-with-errors. *PoPETs*, 2021(4):291–311, October 2021.

MW16. P. Mukherjee and D. Wichs. Two round multiparty computation via multi-key FHE. In *EUROCRYPT 2016, Part II*, *LNCS* 9666, pages 735–763. Springer, Heidelberg, May 2016.

NNOB12. J. B. Nielsen, P. S. Nordholt, C. Orlandi, and S. S. Burra. A new approach to practical active-secure two-party computation. In *CRYPTO 2012*, *LNCS* 7417, pages 681–700. Springer, Heidelberg, August 2012.

Orl11. C. Orlandi. Is multiparty computation any good in practice? In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5848–5851. IEEE, 2011.

PPV08. O. Pandey, R. Pass, and V. Vaikuntanathan. Adaptive one-way functions and applications. In *CRYPTO 2008*, *LNCS* 5157, pages 57–74. Springer, Heidelberg, August 2008.

PS16. C. Peikert and S. Shiehian. Multi-key fhe from lwe, revisited. In *Theory of Cryptography Conference*, pages 217–238. Springer, 2016.

PSSW09. B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams. Secure two-party computation is practical. In *ASIACRYPT 2009*, *LNCS* 5912, pages 250–267. Springer, Heidelberg, December 2009.

RAD$^+$78. R. L. Rivest, L. Adleman, M. L. Dertouzos, et al. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

Reg05. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

RSA78. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

SS11. D. Stehlé and R. Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 27–47. Springer, 2011.

vGHV10. M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In *EUROCRYPT 2010*, *LNCS* 6110, pages 24–43. Springer, Heidelberg, May / June 2010.

Yao82. A. C.-C. Yao. Protocols for secure computations (extended abstract). In *23rd FOCS*, pages 160–164. IEEE Computer Society Press, November 1982.

Yao86. A. C.-C. Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society Press, October 1986.