Key lifting: Multi-key Fully Homomorphic Encryption in plain model without noise flooding

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

[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. Multi-key Fully Homomorphic Encryption (MKFHE), based on the Learning With Error assumption (LWE), usually lifts ciphertexts of different users into new ciphertexts under a common public key, allowing for homomorphic evaluation. The efficiency of the current Multi-key Fully Homomorphic Encryption (MKFHE) scheme is mainly restricted by two aspects:

1. **Expensive ciphertext expansion** : In a boolean circuit with an input length N, multiplication depth L, and security parameter λ, the number of additional encryptions introduced to achieve ciphertext expansion is $O(N\lambda^6 L^4)$.
2. **Noise flooding technology leading to a large modulus** q: To ensure the security of the scheme, the introduction of noise flooding technology during the encryption and distributed decryption stages results in a significant modulus $q = 2^{O(\lambda L)} B_\chi$. This compromises the whole scheme and leads to sub-exponential approximation factors $\gamma = \tilde{O}(n \cdot 2^{\sqrt{nL}})$.

This paper solves the first problem by presenting a framework called Key-Lifting Multi-key Fully Homomorphic Encryption (KL-MKFHE). With this *key lifting* procedure, the number of encryptions for a local user is reduced to $O(N)$, similar to single-key fully homomorphic encryption (FHE). For the second problem, we prove the discrete Gaussian version of the Smudging lemma. Combined with the encryption's anti-leakage properties, we remove the noise flooding technique that was previously used in the distributed decryption. Secondly, we propose an analysis method based on Rényi divergence, which removes the noise flooding technique during encryption. These approaches significantly reduce the size of the modulus q (where $\log q = O(L)$) and the computational overhead of the entire scheme.

Keywords: Multi-key homomorphic encryption · Rènyi divergence · Noise flooding · Leakage resilient cryptography.

1 Introduction

Multi-key Fully Homomorphic Encryption (MKFHE**).** To address the privacy concerns of multiple data providers, López-Alt et al. [17] introduced the concept of MKFHE and developed the first MKFHE scheme based on the modified-NTRU [27]. Conceptually, it enhances the functionality of Fully Homomorphic Encryption(FHE) by allowing data providers to encrypt data independently from other parties. Key generation and data encryption are done locally. To obtain the evaluated result, all parties are required to execute a round of threshold decryption protocol.

After López-Alt et al. proposed the concept of MKFHE, many schemes were developed. In 2015, Clear and McGoldrick [13] constructed a LWE-based MKFHE scheme. This scheme defined the common private key as the concatenation of all private keys. It constructed a masking scheme to convert ciphertext under individual public keys to the common public key by introducing a Common Reference String (CRS) and the circular-LWE assumptions. In 2016, Mukherjee and Wichs [22], Peikert and Shiehian [24], and Brakerski and Perlman [10] constructed MKFHE schemes based on GSW, respectively. Mukherjee and Wichs [22] simplified the masking scheme of [13] and focused on constructing a two-round MPC protocol. Different methods in [24] and [10] were proposed delicately to construct a multi-hop MKFHE. It is worth mentioning that all MKFHE schemes constructed based on LWE require a ciphertext expansion procedure.

1.1 Motivation

A series of works [4, 9, 22] have shown that MKFHE is an excellent base tool for building round-optimal MPC. However, despite its attractive appearance, the construction of MKFHE involves some

cumbersome operations and unavoidable assumptions. Below, we will provide a description of the MKFHE scheme and state our goal in the final paragraph of this subsection.

Ciphertext expansion is expensive. Although the MKFHE based on LWE can utilize the Leftover Hash Lemma (LHL) to remove CRS, to convert the ciphertext under different keys to the ciphertext under the same key (known as the ciphertext expansion procedure), parties and the computing server need to do much preparatory work. For ciphertext expansion, it is necessary to encrypt the random matrix $\mathbf{R} \in \mathbb{Z}_q^{m \times m}$ for each ciphertext. For a boolean circuit with an input length of N, multiplication depth of L, security parameter of λ, and $m = n \log q + \omega(\log \lambda)$, the additional encryption operation introduced is $O(N\lambda^6 L^4)$, in contrast to $O(N)$ for single-key FHE.

CRS looks inevitable. Due to the compact structure of the polynomial ring and some fascinating parallel algorithms such as SIMD, it is generally believed that FHE scheme based on RLWE is more efficient than FHE based on LWE. This is why most current MKFHE schemes, such as [11, 12, 21], are constructed based on RLWE. The Leftover Hash Lemma (LHL) over the integer ring $\mathbb{Z}$ possesses the leakage-resilient property. It can transform average-quality random sources into higher-quality ones [16], which can be utilized to get rid of CRS as [9] does. However, the regularity lemma [18] over polynomial rings does not have corresponding properties, as mentioned in [14]. If the j-th Number Theoretical Transfer (NTT) coordinate of each ring element in $\mathbf{x} = (x_1, \ldots, x_l)$ is leaked, then the j-th NTT coordinate of $a_{l+1} = \sum a_i x_i$ is defined. As a result, a_{l+1} is far from being uniform, even though this is only a 1/n leakage rate. Therefore, it seems to be more difficult to remove CRS for RLWE-based MKFHE.

Noise flooding technology results in a large modulus q. As far as we know, whether it is MKFHE or Threshold Fully Homomorphic Encryption (Th-FHE), such as [5, 9, 10, 13, 22], a great noise needs to be introduced during the encryption or the distributed decryption to ensure security. Otherwise, the private key may be compromised. To simulate partial decryption, assuming that the noise accumulated after the evaluation is $\mathbf{e}_{eval}$ and the private key is $\mathbf{s}$, the flooding noise e_{sm} must satisfy $\langle \mathbf{e}_{eval}, \mathbf{s} \rangle / e_{sm} = \mathsf{negl}(\lambda)$. To ensure the correctness of the decryption result, the modulus q needs to satisfy $q \geq 4e_{sm}$. Thus, noise flooding results in a q that is exponentially larger than the q in a single-key FHE. Typically, in [22], the flooding noise $e_{sm} = 2^{O(L\lambda \log \lambda)} B_\chi$, the modulus $q = 2^{\omega(L\lambda \log \lambda)} B_\chi$, and the corresponding approximation factor of GapSVP_γ is $\gamma = \tilde{O}(n \cdot 2^{\lambda L})$ (which is sub-exponential in n by replacing $\lambda = O(\sqrt{n/L})$[3].

Our goal : We strive to make MKFHE "closer" to FHE in terms of security assumptions and efficiency.

- Without CRS : we **do not assume** the existence of a dealer or a common reference string
- Data providers do **as many encryptions as the single-key FHE**($O(N)$ for the circuit with input length N).
- $q = 2^{O(L)} B_\chi$ of **the same size as the single-key FHE**, while $q = 2^{O(\lambda L)} B_\chi$ for those schemes introduced noise flooding.

1.2 Related works

Except sum type of key structures [5], concatenation structures were studied in [10, 11, 13, 22, 24] together with CRS. Ananth et al. [3] removed CRS from a higher dimension; instead of using LHL or regularity lemma, they based on *Multiparty Homomorphic Encryption* and modified the initialization method of its root node to achieve this purpose. Brakerski et al. [9] was the first scheme using the leakage resilient property of LHL to get rid of CRS, which had the concatenation common private key structure, and ciphertext expansion was essential. All of the above schemes introduced noise flooding technology in distributed decryption phase.

Recently, the work [2] has proposed an alternative approach: instead of removing it, they proposed the concept of accountability of CRS, that is, the generator of CRS should be responsible for its

[3] To achieve 2^λ security against known lattice attacks, one must have $n = \Omega(\lambda \log q / B_\chi)$

randomness; otherwise, the challenging party can provide a publicly verifiable proof that certifies the authority's misbehaviour. This could be an effective way to balance authority. We compare some properties in related work in Table 1.

Table 1. Scheme property comparison

Scheme	Key structure	CRS	Noise flooding	Interaction(setup phase)
THFHE [5]	S	✓	✓	✓
MKFHE [11]	C	✓	✓	×
MKFHE [22]	C	✓	✓	×
MKFHE [9]	C	✓	✓	✓
Our scheme	S	×	×	✓

S" and "C" in the column of Key structure represent the sum or concatenated key structure, respectively. ✓ indicates that the corresponding operation or assumption needs to be introduced, or × indicates that it is not required.

1.3 Our Contributions

We propose the concept of KL-MKFHE. Compared with MKFHE, it imposes more stringent requirements on assumptions, parameters, and computational complexity, making it closer to single-key FHE. (As a compromise, we allow a limited amount of interaction during the key generation)

KL-MKFHE. Different from the previous definition [22], we abandon the ciphertext expansion procedure, instead, introduces a *key lifting* procedure at a lower cost. Informally, the *key lifting* is an interactive protocol. The input is the key pair of all parties. After the protocol, the "lifted" key pair outputs, called the hybrid key, which has such properties :

- *Everyone's hybrid key is different.*
- *The ciphertext encrypted by different hybrid keys supports homomorphic evaluation.*

In addition to the properties that are required by MKFHE, such as *Correctness, Compactness, and Semantic security*, KL-MKFHE should satisfy the following three additional properties:

- **Plain model :** *No trusted setup or Common Reference String*
- **Locally Computationally Compactness :** *For a computational task corresponds to a Boolean circuit with an input length of N, a KL-MKFHE scheme is locally computationally compact if the parties do $O(N)$ encryptions as the single-key* FHE *scheme.*
- **Low round complexity :** *Only two round interaction is allowed in the key lifting procedure.*

Smudging lemma over discrete Gaussian. We prove the discrete Gaussian version of the smudging lemma. Since we are considering the distribution of masked terms, Theorem 1 has smaller noise terms compared to the general lemma, reducing from superpolynomial to polynomial. This result should be widely used. As long as the noise you want to drown out is discrete Gaussian, our results can be utilized instead of the general smudging lemma, which significantly reduces the parameter size. As an additional contribution, we apply Theorem 1 to remove the noise flooding technique in DGSW encryption.

Furthermore, by combining the Corollary 1 of this theorem with the properties of leakage-resistant encryption, we remove the noise flooding technique in the distributed decryption stage.

Theorem 1 *Let $\mathcal{D}_{\mathbb{Z},\sigma}$ be the discrete gaussian distribution over $\mathbb{Z}$ with variance σ^2. Let $n > 0$ be an integer. Let $\mathbf{e}_1 \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $\mathbf{e}_2 \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $\mathbf{M} \leftarrow \{0,1\}^{n\times n}$. Let $\delta \in \mathbb{R}$ and*

$$\frac{\rho_{\Sigma'}(\mathbb{Z}^n)}{\rho_{\Sigma}(\mathbb{Z}^n)} = \delta\sqrt{\frac{\det(\Sigma')}{\det(\Sigma)}}$$

if $\delta > e^{-2+\frac{6\pi}{n+1}}$, we have :

$$\Delta(\mathbf{e}_1\mathbf{M},\ \mathbf{e}_1\mathbf{M}+\mathbf{e}_2) < 2^{-n}$$

where Σ and Σ' are the covariance matrix of $\mathbf{e}_1\mathbf{M}$ and $\mathbf{e}_1\mathbf{M}+\mathbf{e}_2$ respectively.

Remark: You can think of $\mathbf{e}_2$ as a term that needs to be hidden. If the smudging lemma is used, we need $||\mathbf{e}_1\mathbf{M}/\mathbf{e}_2||_\infty = \mathsf{suppoly(n)}$, but in our Theorem 1 we obviously have $||\mathbf{e}_1\mathbf{M}/\mathbf{e}_2||_\infty = O(n)$.

Corollary 1 *Let $\mathcal{D}_{\mathbb{Z},\sigma}$ be the discrete gaussian distribution over $\mathbb{Z}$ with variance σ^2. Let $m > 0$, $n > 0$ be two integers. Let $\mathbf{E}_1 \leftarrow \mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$, $\mathbf{E}_2 \leftarrow \mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$, $\mathbf{M} \leftarrow \{0,1\}^{n\times n}$. Let $\delta \in \mathbb{R}$ and*

$$\frac{\rho_{\Sigma'}(\mathbb{Z}^{mn})}{\rho_{\Sigma}(\mathbb{Z}^{mn})} = \delta\sqrt{\frac{\det(\Sigma')}{\det(\Sigma)}}$$

if $\delta > e^{-2+\frac{2\pi(m+1)}{n+1}+\frac{2}{mn}}$, we have

$$\Delta(\mathbf{E}_1\mathbf{M},\ \mathbf{E}_1\mathbf{M}+\mathbf{E}_2) < 2^{-n}$$

where Σ and Σ' are the covariance matrix of $\mathbf{E}_1\mathbf{M}$ and $\mathbf{E}_1\mathbf{M}+\mathbf{E}_2$ respectively.

LWE-based KL-MKFHE under the plain model. Our scheme is based on the LWE assumption. The common private key is the sum of the private keys of all parties. The MKFHE or Th-FHE schemes [20] [5] that use this key are based on the CRS model. For a circuit with an input length N, our scheme has local users to perform $O(N)$ encryption, which is $O(N\lambda^6L^4)$ for schemes that require ciphertext expansion. In addition, since we remove the noise flooding technique, our scheme has $q = 2^{O(L)}$, while $q = 2^{O(\lambda L)}$ for other schemes. We give a comparison with schemes [9], [24], and [5] in Table 2.

Table 2. Scheme complexity comparison

Scheme	Module q	Extra encryption	Interaction(setup phase)	CRS
MKFHE [24]	$2^{O(\lambda L)}B_\chi$	$\tilde{O}(N\lambda^{14}L^9)$	×	✓
MKFHE [9]	$2^{O(\lambda L)}B_\chi$	$\tilde{O}(Nk^3\lambda^{15}L^{10})$	2 rounds	×
Th-FHE [5]	$2^{O(\lambda L)}B_\chi$	×	1 rounds	✓
Our scheme	$2^{O(L)}B_\chi$	×	2 rounds	×

The notation $\tilde{O}$ hides logarithmic factors. The "Module q" column denotes the module base; the "Extra encryption" column denotes the number of multiplications over $\mathbb{Z}_q$; λ denotes the security parameter, k denotes the number of parties, B_χ denotes the initial LWE noise, and N, L, W denote the input length, depth, and output length of the circuit, respectively. In [24], [9], and [5], n represents the dimension of the LWE problem. In order to compare under the same security level, we replace n with the expression in terms of λ and L. To achieve 2^λ security against known lattice attacks, one must have $n = \Omega(\lambda \log q/B_\chi)$. For our parameter settings $q = 2^{O(L)}B_\chi$, thus we would have $n = \Omega(\lambda L)$, while $n = \Omega(\lambda^2 L)$ for the previous scheme with noise flooding.

2 Technical Overview

Before going into a detailed technical description, we first give a general idea so that we can have an intuitive understanding. The discrete Gaussian version of the smudging lemma is obtained from the observation of the continuous Gaussian distribution: when n is large enough, the sum of n independent and identically distributed (iid) Gaussian distributions is almost the same as the sum of $n+1$ idd Gaussian distributions. Let X, Y be Gaussian distributions with variance $n\sigma^2$ and $(n+1)\sigma^2$ in $\mathbb{R}$ respectively, with probability density function

$$f(x) = \frac{1}{\sqrt{n}\sigma}e^{-\frac{\pi x^2}{n\sigma^2}}, \qquad g(x) = \frac{1}{\sqrt{n+1}\sigma}e^{-\frac{\pi x^2}{(n+1)\sigma^2}}$$

As shown in Figure 1, the intersection point of $f(x)$ and $g(x)$ falls outside $\sqrt{\frac{n+1}{2\pi}}\sigma$(when $x > \sqrt{\frac{n+1}{2\pi}}\sigma$, it holds that $g(x) > f(x)$). The statistical distance between X and Y is

$$\Delta(X,Y) = \int_{||x||_\infty > \sqrt{\frac{n+1}{2\pi}}\sigma} g(x) - f(x)\,dx < \int_{||x||_\infty > \sqrt{\frac{n+1}{2\pi}}\sigma} g(x)\,dx = \mathsf{negl}(n).$$

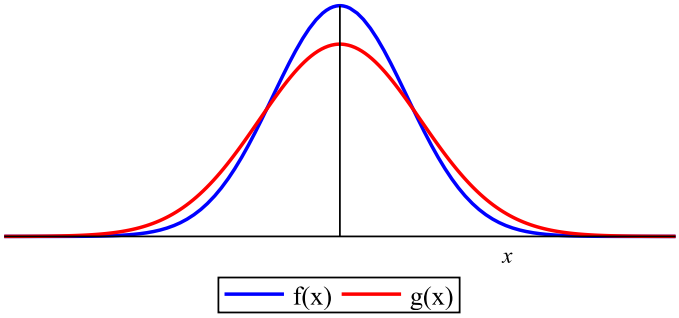

Fig. 1. Probability density function of one-dimensional Gaussian distribution

That is to say, if the masked item e is Gaussian with variance σ^2, we only need to sample e' from a Gaussian distribution with variance $n\sigma^2$. Then, $e + e' \overset{\text{stat}}{\approx} e'$, and $||e/e'|| = O(n^{-1})$ (while for the general smudging lemma $||e/e'|| = \mathsf{negl}(n)$).

The one-dimensional case is relatively simple. Now consider the two-dimensional case. Let Σ_1, Σ_2 be symmetric positive definite matrices on $\mathbb{R}^{2\times 2}$. Let the probability density functions $f(\mathbf{x})$ and $g(\mathbf{x})$ be

$$f(\mathbf{x}) = \frac{1}{\sqrt{\det(\Sigma_1)}} e^{-\pi \mathbf{x} \Sigma_1^{-1} \mathbf{x}^T}, \qquad g(\mathbf{x}) = \frac{1}{\sqrt{\det(\Sigma_2)}} e^{-\pi \mathbf{x} \Sigma_2^{-1} \mathbf{x}^T}$$

as shown in Figure 2.

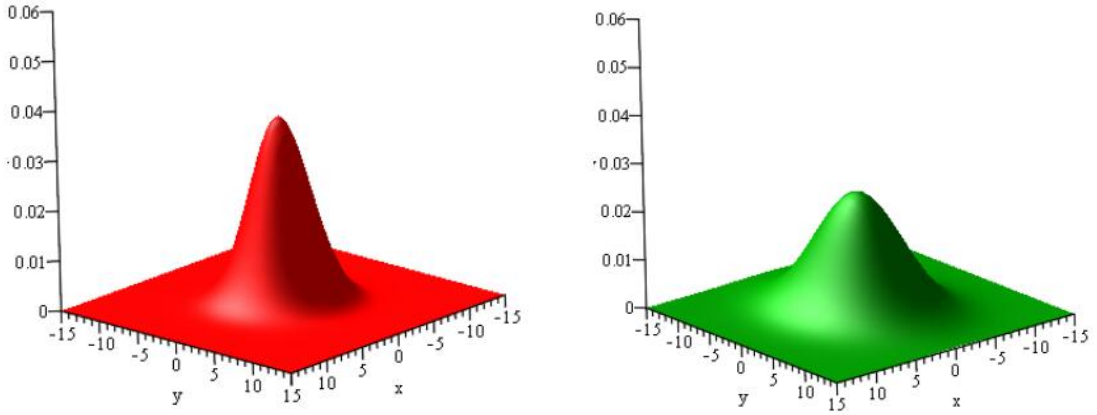

Fig. 2. Probability density function of two-dimensional Gaussian distribution

At this time, the intersection of $f(\mathbf{x})$ and $g(\mathbf{x})$ is a space curve, as shown in the left panel of Figure 3.

Projected onto the xy plane, it is an ellipse, as shown in the right panel of Figure 3. Let the ellipse be $\mathcal{E}_{ints}$

$$\mathcal{E}_{ints} : \frac{1}{\pi} \ln\left(\frac{\det(\Sigma_1)}{\det(\Sigma_2)}\right) = \mathbf{x}(\Sigma_2^{-1} - \Sigma_1^{-1})\mathbf{x}^T$$

Then the statistical distance between $f(\mathbf{x})$ and $g(\mathbf{x}$ is

$$\Delta(f(\mathbf{x}), g(\mathbf{x})) = \int_{\mathbb{R}^2 \setminus \mathcal{E}_{ints}} g(\mathbf{x}) - f(\mathbf{x}) \leq \int_{\mathbb{R}^2 \setminus \mathcal{E}_{ints}} g(\mathbf{x}) \tag{1}$$

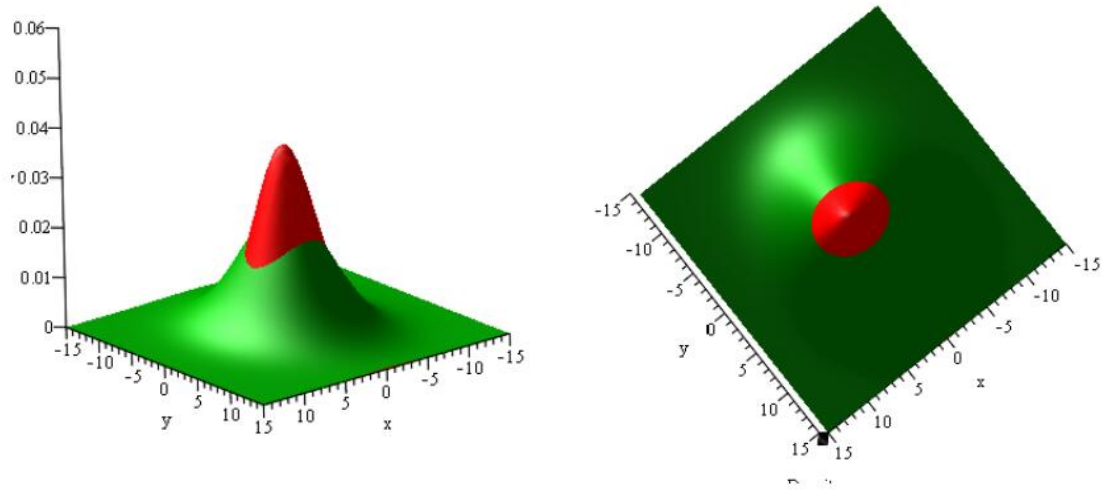

Fig. 3. The intersection of $f(\mathbf{x})$ and $g(\mathbf{x})$

The upper bound on the right side of Equation 1 is not easy to find, because the integral region and the integral function are inconsistent. The integral region is determined by the ellipse $\Sigma_2^{-1} - \Sigma_1^{-1}$, while the integral function $g(\mathbf{x})$ is determined by the ellipse Σ_2. The isoprobability line of $g(\mathbf{x})$ is shown in Figure 4 which is determined by the ellipse Σ_2. For the integral of the area enclosed by

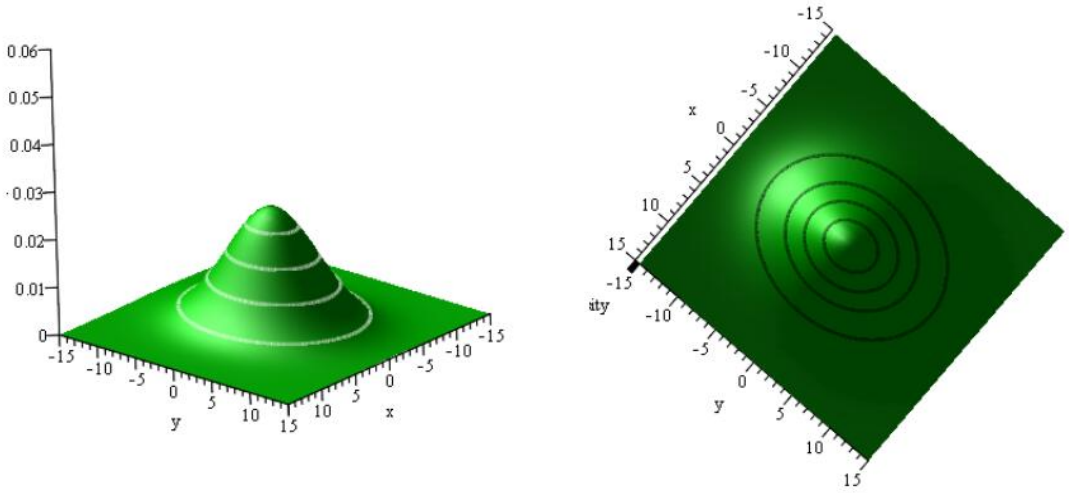

Fig. 4. Equal probability lines of two-dimensional Gaussian distribution

the isoprobability line, there is a closed analytical expression that can be applied, which is generally called the tail probability of the Gaussian distribution [**?**]

$$\Pr[\mathbf{x}\Sigma_2^{-1}\mathbf{x} \geq \chi_2^2(\alpha)] = \int_{\mathbf{x}\Sigma_2^{-1}\mathbf{x}^T \geq \chi_2^2(\alpha)} g(x) < 1 - \alpha \tag{2}$$

where $\chi_2^2(\alpha)$ is the quantile function of the chi-square distribution with 2 degrees of freedom and α as the probability [**?**]. Note that the upper bound of the statistical distance between $f(\mathbf{x})$ and $g(\mathbf{x})$ requires integrating $g(\mathbf{x})$ outside the ellipse $\mathcal{E}_{ints}$, but the existing results support integrating $g(\mathbf{x})$ outside a region of the ellipse Σ_2. Put the isoprobability lines and intersection line in one picture, as shown in Figure 5. Projecting Figure 5 onto the xy plane, we get the left panel of Figure 6. Since we only need to find the upper bound of the statistical distance, we can find an ellipse $\mathcal{E}_{insc}$ in the shape

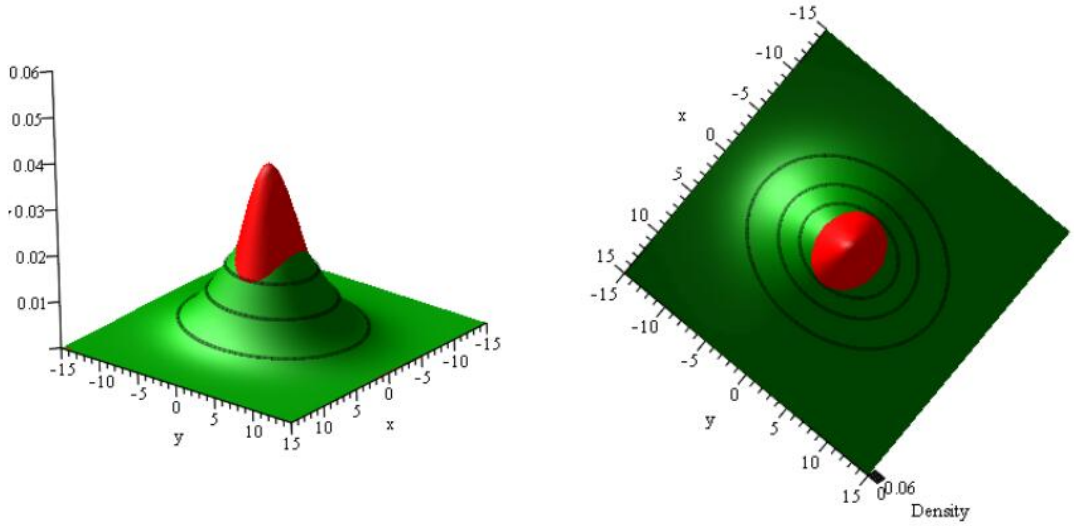

Fig. 5. Lines of intersection and lines of isoprobability

of Σ_2 and inscribe the ellipse $\mathcal{E}_{ints}$. At this time, we have the statistical distance

$$\Delta(f(\mathbf{x}), g(\mathbf{x})) = \int_{\mathbb{R}^2 \setminus \mathcal{E}_{ints}} g(\mathbf{x}) - f(\mathbf{x}) \leq \int_{\mathbb{R}^2 \setminus \mathcal{E}_{ints}} g(\mathbf{x}) \leq \int_{\mathbb{R}^2 \setminus \mathcal{E}_{insc}} g(\mathbf{x})$$

Let the ellipse $\mathcal{E}_{insc}$ be

$$\mathcal{E}_{insc} : \mathbf{x}\Sigma_2^{-1}\mathbf{x}^T = k$$

where $k \in \mathbb{R}$ is the radius to be determined. Then $\mathcal{E}_{insc}$ is exactly the smaller blue ellipse in the right

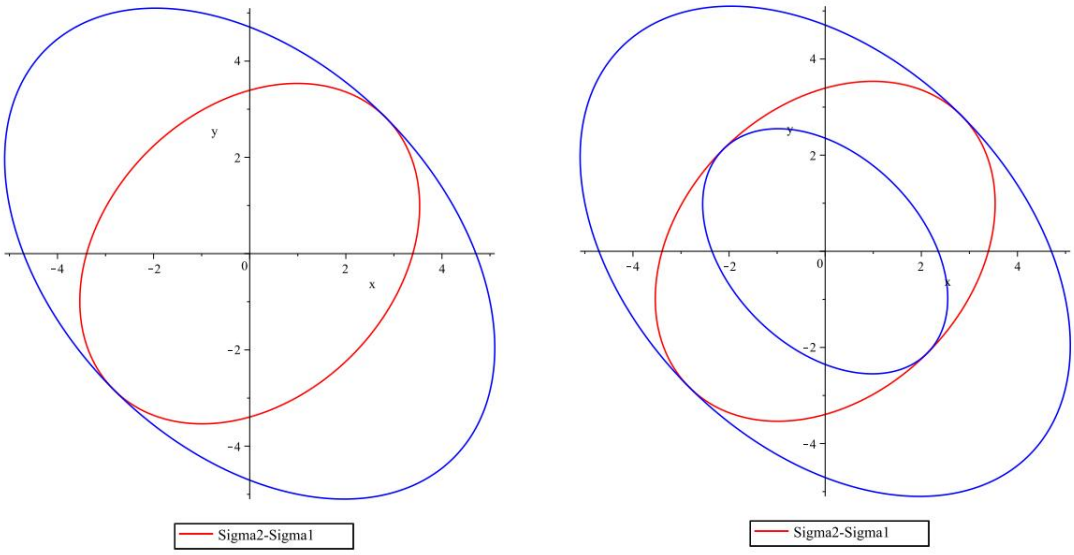

Fig. 6. Project to xy plane

panel of Figure 6. At this time, the radius k to be determined satisfies $k\lambda_1 = \lambda_2$, where λ_1 is the maximum eigenvalue of Σ_2, and λ_2 is the minimum eigenvalue of $\Sigma_2 - \Sigma_1$. Further, according to the result of Equation (2), the upper bound of the statistical distance can be determined.

Extending the above result to a multi-dimensional discrete Gaussian distribution requires solving the intersection equation, which forms an ellipsoid in this case. Additionally, it involves extending Banaszczyk's spherical theorem to the ellipsoid. The discrete Gaussian summation on $\mathbb{Z}^n$ is not simple. As a compromise, we use continuous Gaussian integrals instead. Generally speaking, the idea is the same as that of one dimension: first, find the intersection point, and then the statistical distance.

Asymmetry of ciphertext multiplication. The distributed decryption of the MKFHE will leak the noise accumulated after the homomorphic evaluation and the decryptor's private key. In order to ensure security, previous MKFHE, such as [5,9,11,22], will use a large noise term to "drown out" this part of the private term. Because we are only concerned with the security of the initial ciphertext (note that the noise after the homomorphic evaluation may compromise the privacy of the circuit), it is sufficient to prove that the noise of distributed decryption is independent of the noise in the initial ciphertext, provided that the scheme is anti-leakage. Then even without the drown term, the semantic security of the initial ciphertext can still be guaranteed.

For the Dual GSW-like scheme, we observed that the noise after homomorphic multiplication is highly regular. Let $\mathbf{C}_{\mathsf{mult}} = \mathbf{C}_1\mathbf{G}^{-1}(\mathbf{C}_2)$, the noise in $\mathbf{C}_{\mathsf{mult}}$ hardly contains the noise of $\mathbf{C}_2$. In fact, let $\mathbf{E}_1$ and $\mathbf{E}_2$ be the noise of $\mathbf{C}_1$ and $\mathbf{C}_2$, respectively. The noise in $\mathbf{C}_{\mathsf{mult}}$ is $\mathbf{E}_1\mathbf{G}^{-1}(\mathbf{C}_2) + \mathbf{E}_2$. By our Corollary 1, we have

$$\mathbf{E}_1\mathbf{G}^{-1}(\mathbf{C}_2) + \mathbf{E}_2 \overset{\mathsf{stat}}{\approx} \mathbf{E}_1\mathbf{G}^{-1}(\mathbf{C}_2)$$

In other words, if we left-multiply the initial ciphertext by a "dummy" ciphertext(plaintext is 1), then the noise in the resulting ciphertext hardly contains the noise in the initial ciphertext. Thus, the resulting noise by decrypting the ciphertext after homomorphic evaluation hardly contains any noise in the initial ciphertext, except for the decryptor's private key.

Suppose our scheme is leakage-resilient and can predict the extent of private key leakage in the distributed decryption process beforehand. In that case, we only need to cover this portion of the leakage amount during parameter initialization. Even without the "drown" term in the distributed decryption, it can guarantee the semantic security of the initial ciphertext. The disadvantage is that the complexity of our scheme could be more circuit-dependent. However, there is no noise flooding in encryption and distributed decryption, so we can set $q = 2^{O(L)}B_\chi$ to be the same size as the single-key FHE, where $q = 2^{O(\lambda L)}B_\chi$ in [5] [22] with noise flooding technology. Correspondingly, the approximation factor of Gapsvp_γ is reduced to $\gamma = \tilde{O}(n \cdot 2^L)$.

Optimized security proof method based on Rényi divergence : In order to prove the security of a scheme, a routine is to construct an instance of the scheme from a well-known hard problem instance. Unfortunately, sometimes this process does not go so smoothly. To make the constructed distribution statistically indistinguishable from the target distribution, you need to add noise distribution to bridge the gap between the two. This is where noise flooding comes into play. For example, [5] and [9] adopted this method to prove security. Unfortunately, the additional noise tends to be significant, which reduces the efficiency of the scheme.

Shi et al. [6] pointed out that Rényi divergence can also be used to distinguish between problems. They proved that, under certain conditions, if there is an algorithm that can distinguish problem P, then there is also an algorithm that can distinguish problem P'. Note that it does not require that the P problem is indistinguishable from P'. This is where the Rényi divergence comes into play. Based on the result of [6, Theorem 4.2], our proof method is as follows:

1. Define the P problem as distinguishing our scheme's ciphertext from a uniform distribution.
2. Prove that for a given hard problem instance I, there exists a distribution $\mathcal{D}$ from which a sample x can be constructed from this instance I.
3. Define the P' problem as distinguishing $\mathcal{D}$ from a uniform distribution.

Thus, if there is an adversary who can distinguish the P problem, then they can also distinguish the P' problem and can also distinguish the hard problem instance I from the uniform distribution.

We believe that this Rényi divergence-based proof method provides an alternative approach for those proofs that do not wish to introduce significant noise to ensure security.

2.1 Roadmap:

In Section 3, we define some symbols and list some commonly used definitions and our extended results on lattice. In Section 4, we define the KL-MKFHE. In Section 5, we proved the discrete Gaussian version of smudging lemma. In Section 6, we constructed the KL-MKFHE scheme based on LWE. In Section 7 we prove the security of our scheme. In Section 8, we used the asymmetric properties and anti-leakage properties of DGSW ciphertext to remove the noise flooding technology in the distributed decryption.

3 Preliminaries

3.1 Notation:

Let λ, n, and q be the security parameter, LWE dimension, and modulus base respectively. Let $\mathsf{negl}(\lambda)$ be a negligible function parameterized by λ. Lowercase bold letters such as $\mathbf{v}$, unless otherwise specified, represent vectors. Vectors are typically represented as row vectors, while matrices are denoted 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 the value a is chosen 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. Let $\Delta(X, Y)$ denote the statistical distance between X and Y. For two distributions X and Y, we use $X \overset{\mathsf{stat}}{\approx} Y$ to represent that X and Y are statistically indistinguishable, while $X \overset{\mathsf{comp}}{\approx} Y$ represents that they are computationally indistinguishable.

To decompose elements in $\mathbb{Z}_q$ into binary, we review the Gadget matrix [1, 19] here. Let $\mathbf{G}^{-1}(\cdot)$ be the computable function that for any $\mathbf{M} \in \mathbb{Z}_q^{m \times n}$, it holds that $\mathbf{G}^{-1}(\mathbf{M}) \in \{0,1\}^{ml \times n}$, 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 $\mathbf{G}\mathbf{G}^{-1}(\mathbf{M}) = \mathbf{M}$.

3.2 Some background in probability theory

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

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

Lemma 1 (Smudging lemma [5]) *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, Then the distribution of e_2 is statistically indistinguishable from that of $e_2 + e_1$ as long as $B_1/B_2 = \mathsf{negl}(\lambda)$.*

Average Conditional Min-Entropy(in [8]) Let X be a random-variable supported on a finite set $\mathcal{X}$, and let Z be a random variable supported on a finite set $\mathcal{Z}$. The average-conditional min-entropy $\tilde{H}_\infty(X|Z)$ of X given Z is defined as :

$$\tilde{H}_\infty(X|Z) = -\log(E_z\left[\max_{x \in \mathcal{X}} \Pr[X = x | Z = z]\right]).$$

The Rènyi divergence (in [6]) : For any two discrete probability distributions P and Q such that $\mathsf{Supp}(P) \subseteq \mathsf{Supp}(Q)$ where $\mathsf{Supp}(P) = \{x : P(x) \neq 0\}$ and $a \in (1, +\infty)$, The Rènyi divergence of order a is defined by :

$$R_a(P||Q) = \left(\sum_{x \in \mathsf{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}}\right)^{\frac{1}{a-1}}$$

Omitting the a subscript when $a = 2$, defining the The Rènyi divergence of order 1 and $+\infty$ by :

$$R_1(P||Q) = \exp\left(\sum_{x \in \mathsf{Supp}(P)} P(x) \log \frac{P(x)}{Q(x)}\right)$$

$$R_\infty(P||Q) = \max_{x \in \mathsf{Supp}(P)} \frac{P(x)}{Q(x)}.$$

The definitions are extended naturally to continuous distributions. The divergence R_1 is the (exponential of) the Kullback-Leibler divergence.

Theorem 2 ([6, Theorem 4.2]) *Let Φ, Φ' denote two distribution with $\mathsf{Supp}(\Phi) \subseteq \mathsf{Supp}(\Phi')$, and $D_0(r)$ and $D_1(r)$ denote two distributions determined by some parameter $r \in \mathsf{Supp}(\Phi')$. Let P, P' be two decision problems defined as follows :*

- *Problem P: distinguish whether input x is sampled from distribution X_0 or X_1, where*

$$X_0 = \{x : r \hookleftarrow \Phi, x \hookleftarrow D_0(r)\}, \qquad X_1 = \{x : r \hookleftarrow \Phi, x \hookleftarrow D_1(r)\}.$$

- *Problem P': distinguish whether input x is sampled from distribution X'_0 or X'_1, where*

$$X'_0 = \{x : r \hookleftarrow \Phi', x \hookleftarrow D_0(r)\}, \qquad X'_1 = \{x : r \hookleftarrow \Phi', x \hookleftarrow D_1(r)\}.$$

Assume that $D_0(\cdot)$ and $D_1(\cdot)$ satisfy the following public sampleability property: there exists a sampling algorithm S with run-time T_S such that for all (r, b), given any sample x from $D_b(r)$:

- *$S(0, x)$ outputs a fresh sample distributed as $D_0(r)$ over the randomness of S,*
- *$S(1, x)$ outputs a fresh sample distributed as $D_1(r)$ over the randomness of S.*

Then, given a T-time distinguisher $\mathcal{A}$ for problem P with advantage ϵ, we can construct a distinguisher $\mathcal{A}'$ for problem P' with run-time and distinguishing advantage, respectively, bounded from above and below by (for any $a \in (1, +\infty]$):

$$\frac{64}{\epsilon^2} \log\left(\frac{8R_a(\Phi||\Phi')}{\epsilon^{a/(a-1)+1}}\right) \cdot (T_S + T) \qquad \text{and} \qquad \frac{\epsilon}{4 \cdot R_a(\Phi||\Phi')} \cdot \left(\frac{\epsilon}{2}\right)^{\frac{a}{a-1}}.$$

3.3 Gaussian distribution on Lattice

Definition 2 *Let $\rho_\sigma(\mathbf{x}) = \exp(-\pi||\mathbf{x}/\sigma||^2)$ be a Gaussian function scaled by a factor of $\sigma > 0$. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and $\mathbf{c} \in \mathbb{R}^n$. The discrete Gaussian distribution $D_{\Lambda+\mathbf{c},\sigma}$ with support $\Lambda + \mathbf{c}$ is defined as :*

$$D_{\Lambda+\mathbf{c},\sigma}(\mathbf{x}) = \frac{\rho_\sigma(\mathbf{x})}{\rho_\sigma(\Lambda + \mathbf{c})}$$

We note that $\rho_\sigma(\mathbf{x})$ is just a special case of $\rho_\Sigma(\mathbf{x})$, where $\Sigma = \sigma^2\mathbf{I}$. Therefore, some results on $\sigma^2\mathbf{I}$ should be naturally extended to Σ(symmetric positive definite)

Definition 3 *Let $\rho_\Sigma(\mathbf{x}) = e^{-\pi\mathbf{x}\Sigma^{-1}\mathbf{x}^T}$ be a Gaussian function with covariance matrix Σ(symmetric positive definite). Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and $\mathbf{c} \in \mathbb{R}^n$. The discrete Gaussian distribution $D_{\Lambda+\mathbf{c},\Sigma}$ with support $\Lambda + \mathbf{c}$ is defined as :*

$$D_{\Lambda+\mathbf{c},\Sigma}(\mathbf{x}) = \frac{\rho_\Sigma(\mathbf{x})}{\rho_\Sigma(\Lambda + \mathbf{c})}$$

Obviously, the above definition does satisfy the definition of a probability distribution. For a positive definite matrix Σ, when $||\mathbf{x}|| \to \infty$, $\rho_\Sigma(\mathbf{x})$ converges.

Poisson's summation formula : We recall that the Fourier transform of $\rho_\Sigma(\mathbf{x})$ is $\hat{\rho}_\Sigma(\mathbf{k}) = \det(\Sigma)\rho_{\Sigma^{-1}}(\mathbf{k})$. The Poisson's summation formula of $\rho_\Sigma(\mathbf{x})$ on a full-rank lattice Λ is :

$$\rho_\Sigma(\Lambda) = \det(\Sigma)\det(\Lambda^*)\rho_{\Sigma^{-1}}(\Lambda^*)$$

Lemma 2 *For positive definite matrix Σ_1 and Σ_2, if $\Sigma_1\Sigma_2 - \Sigma_2$ is positive definite, then it holds that :*

$$\rho_{\Sigma_1\Sigma_2}(\Lambda) \leq \det(\Sigma_1)\rho_{\Sigma_2}(\Lambda)$$

Banaszczyk's spherical theorem

Theorem 3 ([7]) *Let $\mathcal{B} = \{\mathbf{x} \in \mathbb{R}^m : ||\mathbf{x}|| \leq 1\}$ be the closed ball of radius 1 in $\mathbb{R}^n$, for any lattice $\Lambda \in \mathbb{R}^m$, parameter $\sigma > 0$ and $u \geq 1/\sqrt{2\pi}$ it holds that*

$$\rho_\sigma(\Lambda \backslash u\sigma\sqrt{m}\mathcal{B}) \leq 2^{-c_u \cdot m} \cdot \rho_\sigma(\Lambda),$$

where $c_u = -\log(\sqrt{2\pi e}u \cdot e^{-\pi u^2})$

The ellipsoid version of the Banaszczyk's spherical Theorem.

Theorem 4 *For any lattice $\Lambda \in \mathbb{R}^m$, let $\Sigma \in \mathbb{R}^{m\times m}$ be a positive definite matrix, $\mathcal{E}(k) = \{\mathbf{x} \in \mathbb{R}^m : \mathbf{x}\Sigma^{-1}\mathbf{x}^T \leq k\}$ be a ellipsoid in $\mathbb{R}^n$ with radius $k > 0$, then it holds that :*

$$\rho_\Sigma(\Lambda \backslash \mathcal{E}(k)) \leq 2^{-2k+m} \cdot \rho_\Sigma(\Lambda)$$

We give the proofs of the above theorem and lemma in Appendix B.1B.2

3.4 The Learning With Error(LWE) Problem

The Learning With Error problem was introduced by Regev [26].

Definition 4 (Decision-LWE) *Let λ 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 $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n})$ $\mathbf{z} \leftarrow U(\mathbb{Z}_q^n)$*
- *$\mathcal{D}_1$: the jointly distribution $(\mathbf{A}, \mathbf{b}) \in (\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^n)$ is computed by $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n})$ $\mathbf{b} = \mathbf{sA} + \mathbf{e}$, where $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ $\mathbf{e} \leftarrow \chi^m$*

As shown in Regev [26] [23], the $\mathsf{LWE}_{n,q,\chi}$ problem with χ being discrete Gaussian distribution with parameter $\sigma = \alpha q \geq 2\sqrt{n}$ is at least as hard as approximating the shortest independent vector problem(SIVP) to within a factor of $\gamma = \tilde{O}(n/\alpha)$ in *worst case* dimension n lattices. It leads to the Decision-$\mathsf{LWE}_{n,q,\chi}$ assumption $\mathcal{D}_0 \overset{\mathsf{comp}}{\approx} \mathcal{D}_1$.

3.5 Dual-GSW(DGSW) Encryption scheme

The DGSW scheme [9] and GSW scheme are similar to the Dual-Regev scheme and Regev scheme, respectively. The DGSW scheme is defined as follows:

- $\mathsf{pp} \leftarrow \mathsf{Gen}(1^\lambda, 1^L)$: For a given security parameter λ, circuit depth L, choose an appropriate lattice dimension $n = n(\lambda, L)$, $m = n\log q + \omega(\lambda)$, a discrete Gaussian distribution $\chi = \chi(\lambda, L)$ over $\mathbb{Z}$, which is bounded by B_χ, module $q = \mathsf{poly}(n) \cdot B_\chi$, 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 pk and plaintext $u \in \{0,1\}$, 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 $\mathbf{E} \leftarrow \chi^{m\times w}$, Output the ciphertext :

$$\mathbf{C} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \mathbf{E} + u\mathbf{G}$$

  where $\mathbf{G}$ is a gadget Matrix.
- $u \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathbf{C})$: Input private key 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 $u' = \lceil \frac{v}{q/2} \rceil$.

Leak resistance: Brakerski et al. proved in [9] that DGSW is leak-resistant. Informally, even if a part of the private key of the DGSW scheme is leaked, the DGSW ciphertext remains semantically secure. As Lemma 3 states:

Lemma 3 (In [9]) *Let χ be LWE noise distribution bounded by B_χ, χ' a distribution over $\mathbb{Z}$ bounded by $B_{\chi'}$, satisfying $B_\chi / B_{\chi'} = \mathsf{negl}(\lambda)$. Let $\mathbf{A}_i \in \mathbb{Z}_q^{(m-1)\times n}$ be uniform, and let $\mathbf{A}_j$ for all $j \neq i$ be chosen by a rushing adversary after seeing $\mathbf{A}_i$. Let $\mathbf{s}_i \leftarrow \{0,1\}^{m-1}$ and $\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j$. Let $\mathbf{r} \in \mathbb{Z}_q^n$ be uniform, $\mathbf{e} \leftarrow \chi^{m-1}$, $e' \leftarrow \chi'$. Then under the LWE assumption, the vector $\mathbf{c} = \mathbf{A}_i\mathbf{r} + \mathbf{e}$ and number $c' = \langle \mathbf{b}_{i,i}, \mathbf{r} \rangle + e'$ are (jointly) pseudorandom, even given the $\mathbf{b}_{i,j}$'s for all $j \in [k]$ and the view of the adversary that generated the $\mathbf{A}_j$'s.*

3.6 Multi-Key Fully Homomorphic Encryption

We review the definition of MKFHE in detail here, with the main purpose of comparing it to the definition of KL-MKFHE proposed later.

Definition 5 *Let λ be the security parameter, L be the circuit depth, and k be the number of parties. A leveled multi-key fully homomorphic encryption scheme consists of a tuple of efficient probabilistic polynomial-time algorithms* MKFHE=(Init, Gen, Enc, Expand, Eval, Dec)*, which are defined as follows.*

- $\mathsf{pp} \leftarrow \mathsf{Init}(1^\lambda, 1^L)$ *: Input security parameter λ, circuit depth L, output system parameter* pp*. We assume that all algorithms take* pp *as input.*
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{pp}, \mathsf{crs})$ *: Input* pp*, common reference string* crs *(generated by a third party or random oracle), output a key pair for party i.*
- $c_i \leftarrow \mathsf{Enc}(\mathsf{pk}_i, u_i)$ *: Input* pk_i *and plaintext u_i, output ciphertext c_i.*
- $v_i \leftarrow \mathsf{Enc}(\mathsf{pk}_i, r_i)$*: Input* pk_i *and the random r_i used in ciphertext c_i, output auxiliary ciphertext v_i.*
- $\bar{c}_i \leftarrow \mathsf{Expand}(\{\mathsf{pk}_i\}_{i\in[k]}, v_i, c_i)$*:Input the ciphertext c_i of party i, the public key set $\{\mathsf{pk}_i\}_{i\in[k]}$ of all parties, auxiliary ciphertext v_i, output expanded ciphertext $\bar{c}_i$ which is under $f(\mathsf{sk}_i, \dots \mathsf{sk}_k)$ whose structure is undefined.*
- $\bar{c}_{eval} \leftarrow \mathsf{Eval}(\mathcal{S}, \mathcal{C})$*:Input circuit $\mathcal{C}$, the set of all ciphertext $\mathcal{S} = \{\bar{c}_i\}_{i\in[N]}$ while N is the input length of circuit $\mathcal{C}$, output evaluated ciphertext $\bar{c}_{eval}$*
- $u \leftarrow \mathsf{Dec}(\bar{c}_{eval}, f(\mathsf{sk}_1 \dots \mathsf{sk}_k))$ *: Input evaluated ciphertext $\bar{c}_{eval}$, private key function $f(\mathsf{sk}_1 \dots \mathsf{sk}_k)$, output u (This is usually a distributed process).*

Remark : Although the definition of MKFHE in [17] does not include auxiliary ciphertext v_i and a ciphertext expansion procedure, the works [13, 22, 25] actually incorporate this procedure to facilitate homomorphic evaluation. This procedure seems essential. We list it here for comparison with KL-MKFHE. The common private key depends on $\{\mathsf{sk}_i\}_{i\in[k]}$. The function f is a certain function, which is not unique; for example, it can be the concatenation of all keys or the sum of all keys.

Properties implicated in the definition of MKFHE: In the above definition, each party is required to independently generate their keys and complete the encryption operation without any interaction between them during the key generation and encryption phases. These two phases are similar to single-key homomorphic encryption. The computational overhead is independent of k and only related to λ and L. Only during the decryption phase, interaction occurs when parties engage in a round of decryption protocol.

4 Key Lifting Multi-key Fully Homomorphic Encryption

We avoid expensive ciphertext expansion procedures and introduce a relatively simple *Key lifting* procedure to replace it. In addition, a tighter bound is required on the amount of local computation and parameter size. As a compromise, we allow a small amount of interaction during *Key lifting*.

Definition 6 *A KL-MKFHE scheme is a tuple of probabilistic polynomial-time algorithms* (Init, Gen, KeyLifting, Enc, Eval, Dec)*, which can be divided into two phases: the online phase (*KeyLifting *and* Dec*) where interaction is allowed between parties, and the local phase (*Init, Gen, Enc, *and* Eval*) where operations do not involve interaction. These five algorithms are described as follows:*

- $\mathsf{pp} \leftarrow \mathsf{Init}(1^\lambda, 1^L)$*:Input security parameter λ, circuit depth L, output public parameters* pp*.*
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{pp})$*:Input public parameter* pp*, output the key pair of party i*
- $\{\mathsf{hk}_i\}_{i\in[k]} \leftarrow \mathsf{KeyLifting}(\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]})$*: Input key pair $\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]}$ of all parties, output the hybrid key $\{\mathsf{hk}_i\}_{i\in[k]}$ of all parties. (online phase: two-round interaction)*
- $c_i \leftarrow \mathsf{Enc}(\mathsf{hk}_i, u_i)$*: Input plaintext u_i and* hk_i*, output ciphertext c_i*
- $\hat{c} \leftarrow \mathsf{Eval}(\mathcal{C}, S)$*: Input circuit $\mathcal{C}$, ciphertext set $S = \{c_i\}_{i\in[N]}$, output ciphertext $\hat{c}$*
- $u \leftarrow \mathsf{Dec}(\hat{c}, f(\mathsf{sk}_1 \dots \mathsf{sk}_k))$*: Input evaluated ciphertext $\hat{c}$, $f(\mathsf{sk}_1 \dots \mathsf{sk}_k)$, output $\mathcal{C}(u_i)_{i\in[N]}$.(online phase: one round interaction)*

Remark : KL-MKFHE does not require a ciphertext expansion procedure. In fact, the input ciphertext set S in $\mathsf{Eval}(\cdot)$ is encrypted by parties using their respective hybrid keys hk_i, which are different for each party. However, the resulting ciphertext c_i supports homomorphic evaluation without any additional modifications.

we require KL-MKFHE to satisfy the following properties :

Plain model : *No trusted setup or Common Reference String*

Locally Computationally Compactness : *For a computational task corresponds to a Boolean circuit with an input length of N, a KL-MKFHE scheme is locally computationally compact if the parties do $O(N)$ encryptions as the single-key* FHE *scheme.*

Two round interaction : *Only two round interaction is allow in* $\mathsf{KeyLifting}(\cdot)$ *procedure.*

The indistinguishable of initial ciphertext : *Let N and W be the input and output length of a circuit, respectively. Let $\{c_i\}_{i\in[N]}$, $\{\gamma_i\}_{i\in[W]}$ be the initial ciphertext and partial decryption result, respectively. The following two distributions are computationally indistinguishable for any probabilistic polynomial-time adversary $\mathcal{A}$.*

$$(\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[k]}, \{\mathsf{hk}_i\}_{i\in[k]}, \{c_i\}_{i\in[N]}, \{\gamma_i\}_{i\in[W]}) \overset{\mathsf{comp}}{\approx} (\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[k]}, \{\mathsf{hk}_i\}_{i\in[k]}, \mathbf{U}, \{\gamma_i\}_{i\in[W]})$$

where $\mathbf{U}$ *is uniform*

Correctness and Compactness : *A KL-MKFHE scheme is correct if for a given security parameter λ, circuit depth L, parties k, we have the following*

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

probability is negligible, where $\mathcal{C}$ is a circuit with input length N and depth length less than or equal to L. A KL-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.*

5 Smudging lemma over discrete Gaussian

Next, we will prove two results regarding discrete Gaussians on the integer lattice $\mathbb{Z}^n$. Simply put, when n is large enough, the distribution of the sum of n iid discrete Gaussians is statistically indistinguishable from the distribution of the sum of $n+1$ iid discrete Gaussians. This is similar to the continuous Gaussian distribution.

Theorem 5 *Let $\mathcal{D}_{\mathbb{Z},\sigma}$ be the discrete gaussian distribution over $\mathbb{Z}$ with variance σ^2. Let $n > 0$ be an integer. Let $\mathbf{e}_1 \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $\mathbf{e}_2 \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $\mathbf{M} \leftarrow \{0,1\}^{n\times n}$. Let $\delta \in \mathbb{R}$ and*

$$\frac{\rho_{\Sigma'}(\mathbb{Z}^n)}{\rho_{\Sigma}(\mathbb{Z}^n)} = \delta\sqrt{\frac{\det(\Sigma')}{\det(\Sigma)}}$$

if $\delta > e^{-2+\frac{6\pi}{n+1}}$, we have :

$$\Delta(\mathbf{e}_1\mathbf{M}, \mathbf{e}_1\mathbf{M} + \mathbf{e}_2) < 2^{-n}$$

where Σ and Σ' are the covariance matrix of $\mathbf{e}_1\mathbf{M}$ and $\mathbf{e}_1\mathbf{M} + \mathbf{e}_2$ respectively.

Note that $\int_{\mathbb{R}^n} \rho_\Sigma(\mathbf{x})\, d\mathbf{x} = \sqrt{\det(\Sigma)}$. In other words, when the ratio of the discrete Gaussian sum and the ratio of the continuous Gaussian integral are not significantly different (up to δ), Theorem 5 applies.

Proof. We can think of $\mathbf{e}_1\mathbf{M}$ as an n-dimensional random variable $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ over $\mathbb{Z}^n$, where $\{x_i = \sum_{j=1}^{n} e_j z_{j,i}\}_{i\in[n]}$, e_j is the j-th element of $\mathbf{e}_1$, $z_{j,i}$ is the element in row j and column i of $\mathbf{M}$. According to the properties of covariance, we have the covariance matrix Σ of $\mathbf{x}$

$$\Sigma = \begin{pmatrix} \frac{1}{2}n\sigma^2 & \frac{1}{4}n\sigma^2 & \cdots & \frac{1}{4}n\sigma^2 \\ \frac{1}{4}n\sigma^2 & \frac{1}{2}n\sigma^2 & \cdots & \frac{1}{4}n\sigma^2 \\ & & \cdots & \\ \frac{1}{4}n\sigma^2 & \frac{1}{4}n\sigma^2 & \cdots & \frac{1}{2}n\sigma^2 \end{pmatrix}, \qquad Cov(x_i, x_j) \begin{cases} \frac{1}{2}n\sigma^2, & if\ i = j \\ \frac{1}{4}n\sigma^2, & if\ i \neq j \end{cases} \tag{3}$$

In the same way, we can also regard $\mathbf{e}_1\mathbf{M}+\mathbf{e}_2$ as a n-dimensional random variable $\mathbf{x}' = (x_1+e'_1, x_2+e'_2, \cdots, x_n+e'_n)$, where e'_i is the i-th element of $\mathbf{e}_2$. Let Σ' be the covariance matrix of $\mathbf{x}'$, by the properties of covariance, we have $\Sigma' = \Sigma + \sigma^2\mathbf{I}$. Thus, we have $\mathbf{x} \sim \mathcal{D}_{\mathbb{Z}^n,\Sigma}(\mathbf{x})$, and $\mathbf{x}' \sim \mathcal{D}_{\mathbb{Z}^n,\Sigma'}(\mathbf{x})$. The probability density function of $\mathbf{x}$ and $\mathbf{x}'$ are $f(x)$ and $g(x)$ respectively

$$f(\mathbf{x}) = \frac{\rho_\Sigma(\mathbf{x})}{\rho_\Sigma(\mathbb{Z}^n)} = \frac{e^{-\pi\mathbf{x}\Sigma^{-1}\mathbf{x}^T}}{\rho_\Sigma(\mathbb{Z}^n)} \qquad g(\mathbf{x}) = \frac{\rho_{\Sigma'}(\mathbf{x})}{\rho_{\Sigma'}(\mathbb{Z}^n)} = \frac{e^{-\pi\mathbf{x}\Sigma'^{-1}\mathbf{x}^T}}{\rho_{\Sigma'}(\mathbb{Z}^n)}$$

Let $f(x) = g(x)$, we have

$$e^{\pi\mathbf{x}(\Sigma^{-1}-\Sigma'^{-1})\mathbf{x}^T} = \frac{\rho_{\Sigma'}(\mathbb{Z}^n)}{\rho_\Sigma(\mathbb{Z}^n)}.$$

Because $\Sigma' = \Sigma + \sigma^2\mathbf{I}$, we have $\Sigma'^{-1} = \Sigma^{-1} - (\Sigma + \frac{1}{\sigma^2}\Sigma^2)^{-1}$ by the Woodbury matrix identity or the Hua's identity. Thus, we have

$$e^{\pi\mathbf{x}(\Sigma+\frac{1}{\sigma^2}\Sigma^2)^{-1}\mathbf{x}^T} = \frac{\rho_{\Sigma'}(\mathbb{Z}^n)}{\rho_\Sigma(\mathbb{Z}^n)}$$

take the logarithm, we have

$$\mathbf{x}(\Sigma + \frac{1}{\sigma^2}\Sigma^2)^{-1}\mathbf{x}^T = \frac{1}{\pi}\ln\frac{\rho_{\Sigma'}(\mathbb{Z}^n)}{\rho_\Sigma(\mathbb{Z}^n)}$$

Let $\mathbf{B} = \Sigma + \frac{1}{\sigma^2}\Sigma^2$, $a = \frac{1}{\pi}\ln\frac{\rho_{\Sigma'}(\mathbb{Z}^n)}{\rho_\Sigma(\mathbb{Z}^n)}$, we have the ellipsoid equation $\mathcal{E}_{ints}$ of the intersection of $f(\mathbf{x})$ and $g(\mathbf{x})$ is

$$\mathcal{E}_{ints}: \quad \mathbf{x}\frac{1}{a}\mathbf{B}^{-1}\mathbf{x}^T = 1$$

When $\mathbf{x}$ is on the ellipsoid $\mathcal{E}_{ints}$, we have $\mathbf{x}\frac{1}{a}\mathbf{B}^{-1}\mathbf{x}^T = 1$, $f(x) = g(x)$, when $\mathbf{x}$ is outside $\mathcal{E}_{ints}$, we have $\mathbf{x}\frac{1}{a}\mathbf{B}^{-1}\mathbf{x}^T > 1$, $f(x) < g(x)$, when $\mathbf{x}$ is inside the $\mathcal{E}_{ints}$, we have $\mathbf{x}\frac{1}{a}\mathbf{B}^{-1}\mathbf{x}^T < 1$, $f(x) > g(x)$. By the definition of Statistical distance and the above result, we have

$$\Delta(\mathbf{x},\mathbf{x}') = \frac{1}{2}\sum_{\mathbf{x}\in\mathbb{Z}^n}|g(x)-f(x)| = \frac{1}{2}\left(\sum_{\mathbf{x}\in\mathcal{E}_{ints}}(f(x)-g(x)) + \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}}(g(x)-f(x))\right) \tag{4}$$

also because

$$\sum_{\mathbf{x}\in\mathbb{Z}^n} f(x) = \sum_{\mathbf{x}\in\mathcal{E}_{ints}} f(x) + \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}} f(x) = 1 \tag{5}$$

$$\sum_{\mathbf{x}\in\mathbb{Z}^n} g(x) = \sum_{\mathbf{x}\in\mathcal{E}_{ints}} g(x) + \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}} g(x) = 1 \tag{6}$$

Let (5) - (6), we have

$$\sum_{\mathbf{x}\in\mathcal{E}_{ints}}(f(x)-g(x)) = \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}}(g(x)-f(x)) \tag{7}$$

Substituting Equation (7) into Equation (4), we have

$$\Delta(\mathbf{x},\mathbf{x}') = \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}} g(\mathbf{x}) - f(\mathbf{x}) < \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}} g(\mathbf{x})$$

Because the "shapes" of $\mathcal{E}_{ints}$ and $g(\mathbf{x})$ are inconsistent (The "shape" of $\mathcal{E}_{ints}$ is $\frac{1}{a}\mathbf{B}^{-1}$, and the "shape" of $g(\mathbf{x})$ is Σ'), we need to find an ellipsoid with the "shape" of Σ' inscribed in $\mathcal{E}_{ints}$. Let $k > 0$ and

$$k\mathbf{x}^T = \frac{1}{a}\Sigma'\mathbf{B}^{-1}\mathbf{x}^T.$$

When k takes the minimum eigenvalue of $\frac{1}{a}\Sigma'\mathbf{B}^{-1}$, we have $k\mathbf{x}\Sigma'^{-1}\mathbf{x}^T = 1$ is inscribed in $\mathcal{E}_{ints}$. The minimum eigenvalue of $\Sigma'\mathbf{B}^{-1}$ and the maximum eigenvalue of $\mathbf{B}\Sigma'^{-1} = \frac{1}{\sigma^2}\Sigma$ are exactly reciprocals of each other, which is $\frac{n(n+1)}{4}$. Therefore, the ellipsoid $\mathcal{E}_{insc}$ that is inscribed in $\mathcal{E}_{ints}$ is

$$\mathcal{E}_{insc}: \quad \mathbf{x}\Sigma'^{-1}\mathbf{x}^T = \frac{an(n+1)}{4}$$

Thus, we have

$$\Delta(\mathbf{x},\mathbf{x}') = \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}} g(\mathbf{x}) - f(\mathbf{x}) < \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{ints}} g(\mathbf{x}) < \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{insc}} g(\mathbf{x})$$

By Theorem 4 and the assumption $\delta > e^{-2+\frac{6\pi}{n+1}}$, we have

$$\sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\mathcal{E}_{insc}} g(\mathbf{x}) < 2^{-\frac{an(n+1)}{4}+n} < 2^{-n}$$

■

Remark : We cannot accurately obtain the value of the discrete Gaussian sum $\rho_\Sigma(\mathbb{Z}^n)$, so we can only use the integral of the Gaussian function $\int_{\mathbb{R}^n}\rho_\Sigma(\mathbf{x})\,d\mathbf{x} = \sqrt{\det(\Sigma)}$ instead. This is our motivation for introducing δ. Numerical experiments show that the difference between the two is not significant, and the ratio is close to 1. Therefore, $\delta > e^{-2+\frac{6\pi}{n+1}}$ should be considered a conservative estimate.

The above results can be easily extended to discrete Gaussian matrices $\mathbf{E}_1$.

Corollary 2 *Let $\mathcal{D}_{\mathbb{Z},\sigma}$ be the discrete gaussian distribution over $\mathbb{Z}$ with variance σ^2. Let $m > 0$, $n > 0$ be two integers. Let $\mathbf{E}_1 \leftarrow \mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$, $\mathbf{E}_2 \leftarrow \mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$, $\mathbf{M} \leftarrow \{0,1\}^{n\times n}$. Let $\delta \in \mathbb{R}$ and*

$$\frac{\rho_{\Sigma'}(\mathbb{Z}^{mn})}{\rho_\Sigma(\mathbb{Z}^{mn})} = \delta\sqrt{\frac{\det(\Sigma')}{\det(\Sigma)}}$$

if $\delta > e^{-2+\frac{2\pi(m+1)}{n+1}+\frac{2}{mn}}$, we have

$$\Delta(\mathbf{E}_1\mathbf{M}, \mathbf{E}_1\mathbf{M}+\mathbf{E}_2) < 2^{-n}$$

where Σ and Σ' are the covariance matrix of $\mathbf{E}_1\mathbf{M}$ and $\mathbf{E}_1\mathbf{M}+\mathbf{E}_2$ respectively.

Proof. The proof of Corollary 2 is exactly the same as the proof of Theorem 5, except that the covariance matrices of $\mathbf{E}_1\mathbf{M}$ and $\mathbf{e}_1\mathbf{M}$ are different. Also, we can think of $\mathbf{E}_1\mathbf{M}$ as an mn-dimensional random variable $\mathbf{x} = (x_1, x_2, \cdots, x_{mn})$ over $\mathbb{Z}^{mn}$, where $\{x_i = \sum_{j=1}^n e_{c,j}z_{j,d}\}_{i\in[mn]}$, $c = \lceil\frac{i}{n}\rceil$, $d = i \mod n$, $e_{c,j}$ is the element in row c and column j of $\mathbf{E}_1$, $z_{j,d}$ is the element in row j and column d of $\mathbf{M}$. Let $\mathbf{T} \in \mathbb{R}^{n\times n}$ be the symmetric matrix

$$\mathbf{T} = \begin{pmatrix} \frac{1}{2}n\sigma^2 & \frac{1}{4}n\sigma^2 & \cdots & \frac{1}{4}n\sigma^2 \\ \frac{1}{4}n\sigma^2 & \frac{1}{2}n\sigma^2 & \cdots & \frac{1}{4}n\sigma^2 \\ & & \cdots & \\ \frac{1}{4}n\sigma^2 & \frac{1}{4}n\sigma^2 & \cdots & \frac{1}{2}n\sigma^2 \end{pmatrix} \tag{8}$$

The covariance matrix $\Sigma \in \mathbb{R}^{mn\times mn}$ of the random variable $\mathbf{x}$ is

$$\Sigma = \begin{pmatrix} \mathbf{T} & & & \\ & \mathbf{T} & & \\ & & \cdots & \\ & & & \mathbf{T} \end{pmatrix} \qquad Cov(x_i, x_j)\begin{cases} \frac{1}{2}n\sigma^2, & if\ i = j \\ \frac{1}{4}n\sigma^2, & if\ |i-j| < n,\ i \neq j \\ 0, & if\ |i-j| \geq n,\ i \neq j \end{cases}$$

The following proof is the same as Theorem 5, we omit it here.

■

5.1 DGSW ciphertext leakage-resilient proof based on Theorem 5

As an application of our Theorem 5, we give the anti-leakage proof of DGSW ciphertext to compare with the general smudging lemma. For a given DGSW ciphertext :

$$\mathbf{C} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \begin{pmatrix} \mathbf{E} \\ \mathbf{e} \end{pmatrix}$$

where $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{b} = \mathbf{sA}$, $\mathbf{s} \leftarrow \{0,1\}^{m-1}$, $\mathbf{R} \leftarrow U(\mathbb{Z}_q^{n\times ml})$, $\mathbf{E} \leftarrow \chi^{(m-1)\times ml}$, $\mathbf{e} \leftarrow \chi'^{ml}$, $l = \lceil \log q \rceil$. Let $\mathbf{C}_0 = \mathbf{AR} + \mathbf{E}$, thus $\mathbf{C}$ can be rewritten as :

$$\mathbf{C} = \begin{pmatrix} \mathbf{C}_0 \\ \mathbf{sC}_0 + \mathbf{e} - \mathbf{sE} \end{pmatrix} \tag{9}$$

The proof in [9] required $||\mathbf{sE}/\mathbf{e}||_\infty = \mathsf{negl}(\lambda)$, thus $\mathbf{C} \overset{\mathsf{stat}}{\approx} \begin{pmatrix} \mathbf{C}_0 \\ \mathbf{sC}_0 + \mathbf{e} \end{pmatrix}$. Assuming $\tilde{H}_\infty(\mathbf{s}|f(\mathbf{s}))$ is sufficient, using the leftover hash lemma with $\mathbf{C}_0$ as a seed and $\mathbf{s}$ as a source, they had that $(\mathbf{C}_0, \mathbf{sC}_0)$ were jointly statistically indistinguishable from uniform, which Lemma 3 followed.

Smudging lemma over discrete gaussian : Below we show that $||\mathbf{sE}/\mathbf{e}||_\infty = \mathsf{negl}(\lambda)$ is not necessary to prove that DGSW is leakage-resilient. Let r be an integer, assuming $\tilde{H}_\infty(\mathbf{s}|f(\mathbf{s})) = r$. Because $\mathbf{s} \leftarrow \{0,1\}^{m-1}$, χ is discrete gaussian over $\mathbb{Z}$ with variance σ^2, we have $\mathbf{e}_2 = \mathbf{sE}$ distributed like discrete Gaussian on $\mathbb{Z}^{ml}$ with variance at most $(m - \frac{1}{2}r - 1)\sigma^2$. When the bits lost in $\mathbf{s}$ are all 1, the maximum variance is obtained. Note that even if the components of $\mathbf{e}_2$ are generated by the same $\mathbf{s}$ and the different columns of $\mathbf{E}$, they are independent(this can be checked by calculating their covariance).

By Theorem 5, in order to "drown out" $\mathbf{e}_2$, we can set $\mathbf{e} = \mathbf{e}_1\mathbf{M}$, where $\mathbf{e}_1 \leftarrow \mathcal{D}_{\mathbb{Z}^{ml},(m-\frac{1}{2}r-1)\sigma^2}$, $\mathbf{M} \leftarrow \{0,1\}^{ml\times ml}$. If $\delta > e^{-2+\frac{6\pi}{ml+1}}$, we have $\Delta(\mathbf{e}, \mathbf{e}+\mathbf{e}_2) < 2^{-n}$, thus $\mathbf{C} \overset{\mathsf{stat}}{\approx} \begin{pmatrix} \mathbf{C}_0 \\ \mathbf{sC}_0 + \mathbf{e} \end{pmatrix}$. The subsequent proof is the same as above. Note that at this time, we have $||\mathbf{e}_2/\mathbf{e}||_\infty = \frac{1}{\mathsf{poly}(\lambda)}$.

6 A KL-MKFHE scheme based on DGSW in the plain model without noise flooding

Our scheme is based on DGSW. In this section, we first introduce the *key lifting* process, describe the entire scheme, and finally give the correctness analysis.

We intentionally place the security proof and the proof of the asymmetric properties of the Dual-GSW ciphertext in the next two section. This is to emphasize the difference between our approach and traditional methods which using noise flooding technology. At the same time, in order to clearly describe these two parts, we really need two separate sections to elaborate on them. We believe this combination is reasonable.

6.1 Key lifting procedure

Following the definition of KL-MKFHE, the hybrid keys $\{\mathsf{hk}_i\}_{i\in[k]}$ obtained by the $\mathsf{KeyLifting}(\cdot)$ algorithm are distinct from each other. Each party encrypts their plaintext u_i using hk_i and obtains $\mathbf{C}_i$. The ciphertexts $\{\mathbf{C}_{i\in[N]}\}$ can be evaluated without extra computation, as stated in Claim 1. We achieve this property by allowing two-round interaction between parties.

$\{\mathsf{hk}_i\}_{i\in[k]} \leftarrow \mathsf{KeyLifting}(\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]})$: Input the DGSW key pair $\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]}$ of all parties, where $\mathsf{pk}_i = (\mathbf{A}_i, \mathbf{b}_{i,i})$, $\mathbf{A}_i \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{s}_i \leftarrow U\{0,1\}^{m-1}$, $\mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i \mod q$. Assuming there is a broadcast channel, all parties engage in the following two interactions:

- First round : i broadcasts pk_i and receives $\{\mathsf{pk}_j\}_{j\in[k]\setminus i}$ from the channel.
- Second round : i generates and broadcasts $\{\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j\}_{j\in[k]\setminus i}$, and receives $\{\mathbf{b}_{j,i} = \mathbf{s}_j\mathbf{A}_i\}_{j\in[k]\setminus i}$ from the channel.

After above two round interaction, i receives $\{\mathbf{b}_{j,i} = \mathbf{s}_j\mathbf{A}_i\}_{j\in[k]/i}$. Let $\mathbf{b}_i = \sum_{j=1}^{k}\mathbf{b}_{j,i}$, i obtains hybrid key $\mathsf{hk}_i = (\mathbf{A}_i, \mathbf{b}_i)$.

Claim 1 *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* hk_i, hk_j *respectively :*

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

it holds that(omit small error) :

$$\bar{\mathbf{t}}\mathbf{C}_i \approx u_i\bar{\mathbf{t}}\mathbf{G}, \quad \bar{\mathbf{t}}\mathbf{C}_j \approx u_j\bar{\mathbf{t}}\mathbf{G}$$
$$\bar{\mathbf{t}}(\mathbf{C}_i + \mathbf{C}_j) \approx (u_i + u_j)\bar{\mathbf{t}}\mathbf{G}, \quad \bar{\mathbf{t}}\mathbf{C}_i\mathbf{G}^{-1}(\mathbf{C}_j) \approx (u_iu_j)\bar{\mathbf{t}}\mathbf{G}$$

Proof. According to the construction of $\mathsf{KeyLifting}(\cdot)$, it holds that :

$$\bar{\mathbf{t}}\mathbf{C}_i = \left(\sum_{i=1}^{k} -\mathbf{s}_i, 1\right)\left[\begin{pmatrix}\mathbf{A}_i\\ \sum_{j=1}^{k}\mathbf{b}_{j,i}\end{pmatrix} + \mathbf{E}_i + u_i\mathbf{G}\right] = \bar{\mathbf{t}}\mathbf{E}_i + u_i\bar{\mathbf{t}}\mathbf{G} \approx u_i\bar{\mathbf{t}}\mathbf{G}.$$

Similarly, $\bar{\mathbf{t}}\mathbf{C}_j \approx u_j\bar{\mathbf{t}}\mathbf{G}$, and $\bar{\mathbf{t}}(\mathbf{C}_i + \mathbf{C}_j) \approx (u_i + u_j)\bar{\mathbf{t}}\mathbf{G}$

$$\bar{\mathbf{t}}\mathbf{C}_i\mathbf{G}^{-1}(\mathbf{C}_j) \approx u_i\bar{\mathbf{t}}\mathbf{G}\mathbf{G}^{-1}(\mathbf{C}_j) \approx u_i\bar{\mathbf{t}}\mathbf{C}_j \approx (u_iu_j)\bar{\mathbf{t}}\mathbf{G}$$

■

Therefore, although $\mathbf{C}_i$ and $\mathbf{C}_j$ are encrypted by different hybrid keys, they correspond to the same decryption key $\bar{\mathbf{t}}$ and support homomorphic evaluation without any additional modifications.

6.2 The entire scheme

Our scheme is based on the DGSW scheme, which includes the following five algorithms (Init, Gen, $\mathsf{KeyLifting}$, Enc, Eval, Dec)

- $\mathsf{pp} \leftarrow \mathsf{Init}(1^\lambda, 1^L, 1^W)$: Let λ be security parameter, L circuit depth, W circuit output length, lattice dimension $n = n(\lambda, L)$, noise distribution χ over $\mathbb{Z}$, $e \leftarrow \chi$, where $|e|$ is bounded by B_χ with overwhelming probability, modulus $q = 2^{O(L)}B_\chi$, $k = \mathsf{poly}(\lambda)$, $m = (kn + W)\log q + \lambda$, suitable choosing above parameters to make $\mathsf{LWE}_{n,m,q,B_\chi}$ is infeasible. Output $\mathsf{pp} = (k, n, m, q, \chi, B_\chi)$
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{pp})$: Input pp, output the DGSW key pair $(\mathsf{pk}_i, \mathsf{sk}_i)$ of parties i, where $\mathsf{pk}_i = (\mathbf{A}_i, \mathbf{b}_{i,i})$, $\mathbf{A}_i \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{s}_i \leftarrow U\{0,1\}^{m-1}$, $\mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i \mod q$.
- $\mathsf{hk}_i \leftarrow \mathsf{KeyLifting}(\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i\in[k]})$: All parties are engaged in the *Key lifting* procedure 6.1, output the hybrid key hk_i.
- $\mathbf{C}_i \leftarrow \mathsf{Enc}(\mathsf{hk}_i, u_i)$: Input hybrid key hk_i, plaintext $u_i \in \{0,1\}$, output ciphertext $\mathbf{C}_i = \begin{pmatrix}\mathbf{A}_i\\ \mathbf{b}_i\end{pmatrix}\mathbf{R} + \mathbf{E} + u_i\mathbf{G}$, where $\mathbf{R} \leftarrow U(\mathbb{Z}_q^{n\times ml})$, $l = \lceil\log q\rceil$, $\mathbf{E} \leftarrow \chi^{m\times ml}$, $\mathbf{G} = \mathbf{I}_m \otimes \mathbf{g}$ is a gadget matrix.
- $\mathbf{C}^{(L)} \leftarrow \mathsf{Eval}(S, \mathcal{C})$: Input the ciphertext set $S = \{\mathbf{C}_i\}_{i\in[N]}$ which are encrypted by hybrid key $\{\mathsf{hk}_i\}_{i\in[k]}$, circuit $\mathcal{C}$ with input length N, depth L, output $\mathbf{C}^{(L)}$.

Homomorphic addition and multiplication : Let $\mathbf{C}_i$ and $\mathbf{C}_j$ be ciphertexts under hybrid keys hk_i and hk_j respectively. By Claim 1, we have the following results.

- $\mathbf{C}_{\mathsf{add}} \leftarrow \mathsf{Add}(\mathbf{C}_i, \mathbf{C}_j)$: Input ciphertext $\mathbf{C}_i$, $\mathbf{C}_j$, output $\mathbf{C}_{\mathsf{add}} = \mathbf{C}_i + \mathbf{C}_j$, which $\bar{\mathbf{t}}\mathbf{C}_{\mathsf{add}} \approx (u_i + u_j)\bar{\mathbf{t}}\mathbf{G}$
- $\mathbf{C}_{\mathsf{mult}} \leftarrow \mathsf{Mult}(\mathbf{C}_i, \mathbf{C}_j)$: Input ciphertext $\mathbf{C}_i$, $\mathbf{C}_j$, output $\mathbf{C}_{\mathsf{mult}} = \mathbf{C}_i\mathbf{G}^{-1}(\mathbf{C}_j)$, which $\bar{\mathbf{t}}\mathbf{C}_{\mathsf{mult}} \approx u_iu_j\bar{\mathbf{t}}\mathbf{G}$

Distributed decryption Similar to [22], the decryption procedure is a distributed procedure :

- $\gamma_i \leftarrow \mathsf{LocalDec}(\mathbf{C}^{(L)}, \mathbf{s}_i)$: Input $\mathbf{C}^{(L)}$, let $\mathbf{C}^{(L)} = \begin{pmatrix}\mathbf{C}_{up}\\ \mathbf{c}_{low}\end{pmatrix}$, where $\mathbf{C}_{up}$ is the first $m-1$ rows of $\mathbf{C}^{(L)}$, and $\mathbf{c}_{low}$ is last row of $\mathbf{C}^{(L)}$. i computes $\gamma_i = \langle -\mathbf{s}_i, \mathbf{C}_{up}\mathbf{G}^{-1}(\mathbf{w}^T)\rangle$, where $\mathbf{w} = (0, \ldots, 0, \lceil q/2\rceil) \in \mathbb{Z}_q^m$, then i broadcast γ_i
- $u_L \leftarrow \mathsf{FinalDec}(\{\gamma_i\}_{i\in[k]})$: After receiving $\{\gamma_i\}_{i\in[k]}$, let $\gamma = \sum_{i=1}^{k}\gamma_i + \langle\mathbf{c}_{low}, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle$, output $u_L = \lceil\frac{\gamma}{q/2}\rceil$

6.3 Correctness analysis

To illustrate the correctness of our scheme, we first study the accumulation of noise. For fresh ciphertext $\mathbf{C} = \begin{pmatrix} \mathbf{A}_i \\ \mathbf{b}_i \end{pmatrix} \mathbf{R} + \begin{pmatrix} \mathbf{E}_0 \\ \mathbf{e}_1 \end{pmatrix} + u\mathbf{G}$ under $\bar{\mathbf{t}}$, it holds that $\bar{\mathbf{t}}\mathbf{C} = \mathbf{e}_1 - \mathbf{s}\mathbf{E}_0 + u\bar{\mathbf{t}}\mathbf{G}$. Let $\mathbf{e}_{init} = \mathbf{e}_1 - \mathbf{s}\mathbf{E}_0$, after L depth circuit evaluation :

$$\bar{\mathbf{t}}\mathbf{C}^{(L)} = \mathbf{e}_L + u_L\bar{\mathbf{t}}\mathbf{G} \tag{10}$$

According to the noise analysis of GSW in [15], the noise $\mathbf{e}_L$ in $\mathbf{C}^{(L)}$ is bounded by $(ml)^L\mathbf{e}_{\text{init}}$. By the distributed decryption in our scheme, it is proven that:

$$\begin{aligned}\gamma &= \sum_{i=1}^{k}\gamma_i + \langle \mathbf{c}_{low}, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle = \langle \sum_{i=1}^{k} -\mathbf{s}_i, \mathbf{C}_{up}\mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \langle \mathbf{c}_{low}, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle \\ &= \bar{\mathbf{t}}\mathbf{C}^{(L)}\mathbf{G}^{-1}(\mathbf{w}^T) = \langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + u_L\lceil\frac{q}{2}\rceil\end{aligned}$$

In order to decrypt correctly, it requires $\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle < \frac{q}{4}$. For our parameter settings :

$$\begin{aligned}\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle &\le l \cdot ||\mathbf{e}_L||_\infty \\ &\le l \cdot (ml)^L \cdot ||\mathbf{e}_{init}||_\infty \\ &\le l \cdot (ml)^L \cdot (km+1)B_\chi\end{aligned}$$

Thus, $\log(\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle) = \tilde{O}(L)$. For those $q = 2^{O(L)}B_\chi \ge 4\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T\rangle$, requirements are fulfilled.

7 Security Proof against Semi-Malicious Adversary

There are two main security concerns about $\mathsf{KeyLifting}(\cdot)$. First, a semi-malicious adversary may generate a matrix $\mathbf{A}$ with a trapdoor, and then $\mathbf{s}_i$ is leaked. More specifically, in the $\mathsf{KeyLifting}(\cdot)$ phase, $\{\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j\}_{j\in[k]}$ will lose $\mathbf{s}_i$ at most $kn\log q$ bits. Second, a semi-malicious adversary $\mathcal{A}$ may generate $\mathbf{b}_{j,i}$ adaptively after observing $\mathbf{b}_{i,i}$. As a result, the hybrid key $\mathbf{b}_i$ of party i may not be distributed as required.

This place is very subtle. In the first round of $\mathsf{KeyLifting}(\cdot)$, the semi-malicious adversary has already generated $\{\mathsf{pk}_j\}_{j\in[k]\setminus i}$. However, we have noticed that because $\{\mathbf{A}_j\}_{j\in[k]\setminus i}$ may not be uniform, the adversary can find multiple groups of $\{\mathbf{s}'_j \in \{0,1\}^{m-1}, \mathbf{s}'_j \neq \mathbf{s}_j\}$ that satisfy $\mathbf{s}'_j\mathbf{A}_j = \mathbf{s}_j\mathbf{A}_j$. So in the second round (we always assume that the adversary makes the last move, that is, the adversary has already obtained the leakage of $\mathbf{s}_i$ and seen $\mathbf{b}_{i,i}$), the adversary $\mathcal{A}$ can choose any $\mathbf{s}'_j$ from $\{\mathbf{s}'_j \in \{0,1\}^{m-1}, \mathbf{s}'_j \neq \mathbf{s}_j, \mathbf{s}'_j\mathbf{A}_j = \mathbf{s}_j\mathbf{A}_j\}$ to construct $\mathbf{b}_{j,i}$ and control $\mathbf{b}_i$ as much as possible. So, for semi-malicious adversaries, we assume that $\mathbf{s}_j$ in $\{\mathsf{pk}_j\}_{j\in[k]/i}$ and $\mathbf{s}'_j$ in $\{\mathbf{b}_{j,i}\}_{j\in[k]/i}$ can be different.

The general solution is to introduce a flooding noise in encryption to ensure security. Large encryption noise leads to a large modulus q, which, in turn, results in significant computational and communication overhead. To address this problem, we proposed an analysis method based on Rényi divergence and get rid of the flooding noise in the encryption. In the following, we first introduce the general method and then give an optimization proof method based on Rényi divergence.

7.1 A common approach(By noise flooding)

We complete the simulation by constructing a reduction from our scheme to the DGSW scheme. We assume that the first party is the Challenger and the other $k-1$ parties are controlled by the adversary $\mathcal{A}$. Consider the following Game:

1. Challenger generates $\mathsf{pk}_1 = (\mathbf{A}_1, \mathbf{b}_{1,1} = \mathbf{s}_1\mathbf{A}_1)$ where $\mathbf{A}_1 \leftarrow U(\mathbb{Z}_q^{(m-1)\times n})$, $\mathbf{s}_1 \leftarrow U\{0,1\}^{m-1}$ sends pk_1 to adversary $\mathcal{A}$

2. After receiving pk_1, $\mathcal{A}$ generates $\{\mathsf{pk}_i\}_{i\in[k]/1}$, where $\mathsf{pk}_i = (\mathbf{A}_i, \mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i)$, sends it to Challenger.
3. After receiving $\{\mathsf{pk}_i\}_{i\in[k]/1}$, Challenger sets $\{\mathbf{b}_{1,i} = \mathbf{s}_1\mathbf{A}_i\}_{i\in[k]/1}$(the leakage of $\mathbf{s}_1$), sends it to $\mathcal{A}$
4. After receiving $\{\mathbf{b}_{1,i}\}_{i\in[k]/1}$, $\mathcal{A}$ adaptively chooses $\{\mathbf{s}'_i\}_{i\in[k]/1}$, where $\mathbf{s}'_i \in \{0,1\}^{m-1}$, sets $\{\mathbf{b}_{i,1} = \mathbf{s}'_i\mathbf{A}_1\}_{i\in[k]/1}$, sends it to Challenger.
5. After receiving $\{\mathbf{b}_{i,1}\}_{i\in[k]/1}$, Challenger sets $\mathsf{hk}_1 = (\mathbf{A}_1, \sum_{i=1}^{k}\mathbf{b}_{i,1})$.
6. $\mathcal{A}$ chooses a bit $u \leftarrow \{0,1\}$, sends it to Challenger.
7. Challenger chooses a bit $\alpha \leftarrow \{0,1\}$, if $\alpha = 0$ sets $\mathbf{C} \leftarrow \mathsf{Enc}(\mathsf{hk}_1, u)$, otherwise $\mathbf{C} \leftarrow U(\mathbb{Z}_q^{m\times ml})$, sends $\mathbf{C}$ to $\mathcal{A}$.
8. After receiving $\mathbf{C}$, $\mathcal{A}$ outputs bit $\bar{\alpha}$, if $\bar{\alpha} = \alpha$, then $\mathcal{A}$ wins.

Obviously the above Game simulates the $\mathsf{KeyLifting}(\cdot)$ and $\mathsf{Enc}(\cdot)$ of our scheme. The first four steps outline the detailed process of $\mathsf{KeyLifting}(\cdot)$, assuming a rushing adversary.

Claim 2 *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* Adv*, then* $\mathcal{A}$ *can distinguish between the ciphertext of* DGSW *and the uniform distribution with the same(up to negligible) advantage.*

Proof. After the third step of the above game, $\mathcal{A}$ obtained pk_1 and $\{\mathbf{b}_{1,i}\}_{i\in[k]/1}$(the leakage of $\mathbf{s}_1$). Next, we use the ciphertext of DGSW to construct $\mathbf{C}$. Let :

$$\mathbf{C}_{\mathsf{DGSW}} = \begin{pmatrix}\mathbf{A}_1\\ \mathbf{b}_{1,1}\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1\end{pmatrix} = \begin{pmatrix}\mathbf{C}_0\\ \mathbf{c}_1\end{pmatrix}$$

be the Dual-GSW ciphertext generated by pk_1, which is semantically secure by Lemma 3, even if $\mathbf{s}_1$ is lossy. Let $\mathbf{s}' = \sum_{i=2}^{k}\mathbf{s}'_i$ are adaptively chosen by $\mathcal{A}$ after seeing pk_1 and $\{\mathbf{b}_{1,i}\}_{i\in[k]/1}$(the leakage of $\mathbf{s}_1$). Let

$$\mathbf{C}' = \mathbf{C}_{\mathsf{DGSW}} + \begin{pmatrix}\mathbf{0}\\ \mathbf{s}'\mathbf{C}_0\end{pmatrix}$$

it holds that :

$$\mathbf{s}'\mathbf{C}_0 = \mathbf{s}'(\mathbf{A}_1\mathbf{R} + \mathbf{E}_0) = \sum_{i=2}^{k}\mathbf{b}_{i,1}\mathbf{R} + \mathbf{s}'\mathbf{E}_0$$

$$\begin{aligned}\mathbf{C}' &= \mathbf{C}_{\mathsf{DGSW}} + \begin{pmatrix}\mathbf{0}\\ \mathbf{s}'\mathbf{C}_0\end{pmatrix}\\ &= \begin{pmatrix}\mathbf{A}_1\\ \mathbf{b}_{1,1}\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1\end{pmatrix} + \begin{pmatrix}\mathbf{0}\\ \mathbf{s}'\mathbf{C}_0\end{pmatrix}\\ &= \begin{pmatrix}\mathbf{A}_1\\ \mathbf{b}_1\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1 + \mathbf{s}'\mathbf{E}_0\end{pmatrix}\end{aligned}$$

If $||\mathbf{e}_1||_\infty$ is bounded by $2^\lambda B_\chi$, and $||\mathbf{s}'\mathbf{E}_0||_\infty < kmB_\chi$, then $\mathbf{s}'\mathbf{E}_0/\mathbf{e}_1 = \mathsf{negl}(\lambda)$. By Lemma 1, it holds that $\mathbf{C}' \overset{\mathsf{stat}}{\approx} \mathbf{C}$. If $\mathcal{A}$ can distinguish between $\mathbf{C}$ and the uniform distribution by advantage Adv, then he can also distinguish between $\mathbf{C}_{\mathsf{DGSW}}$ and the uniform distribution with the same (up to negligible) advantage. ■

Remark: When $||\mathbf{e}_1||_\infty$ is bounded by $2^\lambda B_\chi$, according to the correctness analysis in Section 6.3, the initial noise $\mathbf{e}_{init} = \mathbf{e}_1 - \mathbf{s}\mathbf{E}_0$ is bounded by $(2^\lambda + km)B_\chi$. After L-level evaluation, $\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle$ is bounded by $l\cdot(ml)^L\cdot(2^\lambda + km)B_\chi$, $\log(\langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle) = \tilde{O}(\lambda + L)$. Thus, this results in a $q = 2^{O(\lambda+L)}B_\chi$.

7.2 Distinguishing DGSW ciphertext with a linear relationship between noise and random numbers

In this section, we introduce a new problem: distinguishing DGSW ciphertext with a linear relationship between noise and random numbers. From Lemma 3, we already know that DGSW ciphertext is

leakage-resistant. This means that even if the key $\mathbf{s}$ is lossy, DGSW ciphertext remains semantically secure. Here, we take it one step further: not only is $\mathbf{s}$ lossy, but we also leak the linear relationship between random numbers and noise in the ciphertext.

This new problem is introduced because we will use it in the optimization proof method based on Rènyi divergence. We believe it will be useful in other places as well. Below, we will formally define it.

Definition 7 (DGSWLRL) *Let λ be security parameter, $n = n(\lambda)$, $w = w(\lambda)$, $q = q(\lambda)$, $m = O(n \log q)$ be integers satisfying $n|w$. Let $\chi = \chi(\lambda)$ and $\chi' = \chi'(\lambda)$ be two distribution defined over $\mathbb{Z}$, bounded by B_χ and $2^\lambda B_\chi$ respectively. Let $\mathsf{pk}_{DGSW} = (\mathbf{A}, \mathbf{b} = \mathbf{sA})$, where $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n})$, $\mathbf{s} \leftarrow \{0,1\}^m$. Let $f(\cdot)$ be any computable functions. Assuming $\tilde{H}_\infty(\mathbf{s}|f(\mathbf{s})) \geq \log q + 2\lambda$, consider the following* Game.

1. *Challenger generates the DGSW ciphertext:*

$$\mathbf{C}_{DGSW} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \begin{pmatrix} \mathbf{E} \\ \mathbf{e} \end{pmatrix}$$

   where $\mathbf{R} \leftarrow U(\mathbb{Z}_q^{n\times w})$, $\mathbf{E} \leftarrow \chi^{m\times w}$, $\mathbf{e} \leftarrow \chi'^{w}$. Then computes $\{\mathbf{v}_i\}_{i\in[g]}$ by $\{\mathbf{v}_i\mathbf{R}_i = \mathbf{e}_i\}$, where $\mathbf{R}_i \in \mathbb{Z}_q^{n\times n}$ and $\mathbf{e}_i \in \mathbf{Z}_q^n$ are the i-th block of $\mathbf{R} = (\mathbf{R}_1, \mathbf{R}_2, \cdots, \mathbf{R}_g)$ and $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_g)$, respectively. Send $\{\mathbf{v}_i\}_{i\in[g]}$ and $\mathbf{C}_{DGSW}$ to adversary $\mathcal{A}$.
2. *After receiving $\{\mathbf{v}_i\}_{i\in[g]}$ and $\mathbf{C}_{DGSW}$, $\mathcal{A}$ try to distinguish :*

$$\left(\mathsf{pk}_{DGSW}, \{\mathbf{v}_i\}_{i\in[g]}, f(\mathbf{s}), \mathbf{C}_{DGSW}\right) \qquad \text{and} \qquad \left(\mathsf{pk}_{DGSW}, \{\mathbf{v}_i\}_{i\in[g]}, f(\mathbf{s}), \mathbf{U}\right)$$

If A can distinguish the two by a non-negligible advantage, then A wins, otherwise the challenger wins.

Obviously, if there are no $\{\mathbf{v}_i\}_{i\in[g]}$, then this problem can be directly proved by Lemma 3. Before starting the proof, let's take a look at $\{\mathbf{v}_i\}_{i\in[g]}$. For a uniform matrix $\mathbf{R}_i$, it is highly likely to be reversible, and furthermore, $\mathbf{v}_i = \mathbf{e}_i\mathbf{R}_i^{-1}$. Thus it defines a bijection from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^n$, so giving $\mathbf{v}_i$ will expose the linear relationship between $\mathbf{e}_i$ and $\mathbf{R}_i$. How much does this linear relationship contribute to distinguishing DGSW ciphertext? Next, we prove that, to some extent, this linear relationship is equivalent to reducing the dimension of the LWE problem under the DGSW ciphertext by 1.

For convenience, we abbreviate this problem as DGSWLRL[4] problem.

Lemma 4 *If there is an adversary who can distinguish the DGSWLRL problem, then he can also distinguish the DGSW ciphertext ($n-1$ dimensional* LWE*) from a uniform distribution.*

Proof. For a given DGSW ciphertext $\mathbf{C}_{\mathsf{DGSW}}$ and $\{\mathbf{v}_i\}_{i\in[g]}$, let $\mathbf{c}$ be the last row first n items of $\mathbf{C}_{\mathsf{DGSW}}$. It holds that :

$$\left.\begin{aligned} \mathbf{bR}_1 + \mathbf{e}_1 &= \mathbf{c} \\ \mathbf{v}_1\mathbf{R}_1 &= \mathbf{e}_1 \end{aligned}\right\} \tag{11}$$

Next, we will prove that (11) can be constructed from low-dimensional DGSW ciphertext (note that $\mathbf{R}_1 \in \mathbb{Z}_q^{n\times n}$). Let $\mathbf{c}'$ be the last row fisrt n items of a $n-1$ dimensional DGSW ciphertext(without linear relationship leakage). It holds that :

$$\mathbf{b}'\mathbf{R}_1' + \mathbf{e}_1' = \mathbf{c}'$$

where $\mathbf{b}' = \mathbf{sA}'$, $\mathbf{A}' \leftarrow U(\mathbb{Z}_q^{m\times(n-1)})$, $\mathbf{R}_1' \leftarrow U(\mathbb{Z}_q^{(n-1)\times n})$, $\mathbf{e}_1' \leftarrow \chi'^{n}$. Let

$$\mathbf{b}' = (b_1', b_2', \cdots, b_{n-1}'), \quad \mathbf{R}_1' = \begin{pmatrix} \mathbf{r}_1' \\ \mathbf{r}_2' \\ \cdots \\ \mathbf{r}_{n-1}' \end{pmatrix}, \quad b_n = \mathbf{sa}_n^T, \quad \mathbf{a}_n \leftarrow U(\mathbb{Z}_q^m),$$

$$\{\mathbf{r}_i = \mathbf{r}_i'(\mathbf{I} - b_i'^{-1}b_n\mathbf{W})^{-1}\}_{i\in[n-1]}, \quad \mathbf{W} \leftarrow U(\mathbb{Z}_q^{n\times n}), \quad \mathbf{r}_n = \mathbf{W}_0 - \sum_{i=1}^{n-1}\mathbf{r}_i\mathbf{W},$$

$$\mathbf{W}_0 = \mathbf{e}_1'\mathbf{T}, \quad \mathbf{T} \leftarrow U(\mathbb{Z}_q^{n\times n})$$

[4] DGSW ciphertext with linear relationship leakage

Let $\bar{\mathbf{b}} = (\mathbf{b}', b_n)$, $\bar{\mathbf{R}}_1 = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \cdots \\ \mathbf{r}_n \end{pmatrix}$, $\bar{\mathbf{e}}_1 = \mathbf{e}'_1$, $\bar{\mathbf{c}} = \mathbf{c}' + b_n \mathbf{W}_0$. It holds that :

$$\bar{\mathbf{b}}\bar{\mathbf{R}}_1 + \bar{\mathbf{e}}_1 = \bar{\mathbf{c}}$$

Because $\mathbf{W}_0 = \mathbf{r}_n + \sum_{i=1}^{n-1} \mathbf{r}_i \mathbf{W} = \bar{\mathbf{e}}_1 \mathbf{T}$, we have

$$\mathbf{r}_1 \mathbf{W}\mathbf{T}^{-1} + \mathbf{r}_2 \mathbf{W}\mathbf{T}^{-1} + \cdots + \mathbf{r}_{n-1}\mathbf{W}\mathbf{T}^{-1} + \mathbf{r}_n \mathbf{T}^{-1} = \bar{\mathbf{e}}_1$$

Let v_i be the eigenvalue of the $\mathbf{WT^{-1}}$ corresponding eigenvector $\mathbf{r}_i$, we have $\{v_i \mathbf{r}_i = \mathbf{r}_i \mathbf{W}\mathbf{T}^{-1}\}_{i\in[n-1]}$, $v_n \mathbf{r}_n = \mathbf{r}_n \mathbf{T}^{-1}$ thus

$$v_1 \mathbf{r}_1 + v_2 \mathbf{r}_2 + \cdots + v_{n-1}\mathbf{r}_{n-1} + v_n \mathbf{r}_n = \bar{\mathbf{e}}_1$$

Thus, we have (12) corresponding to (11) :

$$\left.\begin{aligned} \bar{\mathbf{b}}\bar{\mathbf{R}}_1 + \bar{\mathbf{e}}_1 = \bar{\mathbf{c}} \\ v_1 \mathbf{r}_1 + v_2 \mathbf{r}_2 + \cdots + v_{n-1}\mathbf{r}_{n-1} + v_n \mathbf{r}_n = \bar{\mathbf{e}}_1 \end{aligned}\right\} \tag{12}$$

Obviously, the distributions of $\mathbf{b}$ and $\bar{\mathbf{b}}$ are consistent. For $\{\mathbf{r}_i\}_{i\in[n-1]}$, we have

$$\{\mathbf{r}_i = \mathbf{r}'_i (\mathbf{I} - {b'_i}^{-1} b_n \mathbf{W})^{-1}\}$$

Because $\mathbf{W}$ is uniform over $\mathbb{Z}_q^{n\times n}$, $(\mathbf{I} - {b'_i}^{-1} b_n \mathbf{W})^{-1}$ defines a bijection from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^n$, so the distributions of $\{\mathbf{r}'_i\}_{i\in[n-1]}$ and $\{\mathbf{r}_i\}_{i\in[n-1]}$ are consistent. Furthermore, because $\mathbf{T}$ and $\mathbf{W}$ are both uniform and independent on $\mathbb{Z}_q^{n\times n}$, $\mathbf{r}_n = \bar{\mathbf{e}}_1 \mathbf{T} - \sum_{i=1}^{n-1} \mathbf{r}_i \mathbf{W}$ is uniform over $\mathbb{Z}_q^{n\times n}$. Therefore $\mathbf{R}_1$ and $\bar{\mathbf{R}}_1$ are consistent.

Therefore, we completed the construction from $n-1$ dimensional DGSW ciphertext (without linear relationship leakage) to n-dimensional DGSW ciphertext (with linear relationship leakage), and the former can be directly proved by Lemma 3. Notice that this only completes the construction of the first block. The remaining $g-1$ blocks can be completed using a hybrid argument routine.

■

7.3 Rényi divergence-based optimization :

The work of Shi et al. [6] pointed out that Rényi divergence can also be applied in distinguishing problems, and in some cases, it can lead to better parameters than statistical distance. Based on these results, they obtained improved parameters for the Regev encryption scheme. Theorem 2 states that if there exists an algorithm that can distinguish the P problem, then there also exists an algorithm that can distinguish the P' problem. Our proof method is as follows:

- Define the P problem as distinguishing our ciphertext from a uniform distribution.
- Prove that for a given DGSW ciphertext, there exists a distribution X'_0, and a sample x of X'_0 can be constructed from this DGSW ciphertext.
- Define the P' problem as distinguishing X'_0 from a uniform distribution.

Thus, if there is an adversary who can distinguish the P problem, then they can also distinguish the P' problem and the DGSW ciphertext from the uniform distribution.

Claim 3 *Let a be a constant in $\mathbb{R}^+$. Let the encryption run-time of our scheme be T_S. If there is an adversary who can distinguish the ciphertext of our scheme from a uniform distribution with a run-time of T and an advantage of ϵ, then the adversary can distinguish the DGSWLRL problem with a run-time and advantage that are bounded from above and below, respectively:*

$$\frac{64}{\epsilon^2} \log\left(\frac{\mathsf{poly}(\lambda)}{\epsilon^{a/(a-1)+1}}\right) \cdot (T_S + T) \quad \textit{and} \qquad \frac{\epsilon}{4 \cdot \mathsf{poly}(\lambda)} \cdot \left(\frac{\epsilon}{2}\right)^{\frac{a}{a-1}}.$$

Proof. We first define several distributions. Let $\mathbf{0}^{ml}$ be the zero vector of length ml, Φ be the distribution of the hybrid key $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H})$ followed by $\mathbf{0}^{ml}$, and $f(\mathbf{s})$ be the leakage of the private key $\mathbf{s}$, which is determined by the $\mathsf{KeyLifting}(\cdot)$ procedure.

$$(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s})) \hookleftarrow \Phi$$

Obviously, Φ simulates the $\mathsf{KeyLifting}(\cdot)$[5] process of our scheme. Let $\mathcal{D}_0(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}))$ be the joint distribution of $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}))$ and the ciphertext $\begin{pmatrix}\mathbf{A}_\mathsf{H}\\ \mathbf{b}_\mathsf{H}\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1\end{pmatrix}$ encrypted by $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H})$ over the randomness $\mathbf{R} \leftarrow U(\mathbb{Z}_q^{n\times ml})$, $\mathbf{E}_0 \leftarrow \chi^{(m-1)\times ml}$, $\mathbf{e}_1 \leftarrow \chi^{ml}$:

$$(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}), \begin{pmatrix}\mathbf{A}_\mathsf{H}\\ \mathbf{b}_\mathsf{H}\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{E}_0\\ \mathbf{e}_1\end{pmatrix}) \hookleftarrow \mathcal{D}_0(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}))$$

Obviously, $\mathcal{D}_0(\cdot)$ simulates the encryption of our scheme. Let $\mathcal{D}_1(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}))$ be the joint distribution of $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}))$ and $\mathbf{U} \leftarrow U(\mathbb{Z}_q^{m\times ml})$:

$$(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}), \mathbf{U}) \hookleftarrow \mathcal{D}_1(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{0}^{ml}, f(\mathbf{s}))$$

Define P problem as follows :

- Problem P : distinguish whether input x is sampled from distribution X_0 or X_1, where

$$X_0 = \{x : r \hookleftarrow \Phi, x \hookleftarrow \mathcal{D}_0(r)\}, \qquad X_1 = \{x : r \hookleftarrow \Phi, x \hookleftarrow \mathcal{D}_1(r)\}.$$

Obviously, the P problem is to distinguish the ciphertext of our scheme from uniform.

Construct auxiliary distribution : Before defining the P' problem, we need to construct an auxiliary distribution. For the random $\bar{\mathbf{R}} \leftarrow U(\mathbb{Z}_q^{n\times ml})$ and $\bar{\mathbf{e}}_1 \leftarrow \chi'^{ml}$[6], without loss of generality, assuming $\frac{ml}{n} = g$, we can divide $\bar{\mathbf{R}}$ into g square matrices

$$\bar{\mathbf{R}} = (\bar{\mathbf{R}}_1, \bar{\mathbf{R}}_2, \cdots, \bar{\mathbf{R}}_g)$$

where $\bar{\mathbf{R}}_i \in \mathbb{Z}_q^{n\times n}$. Similarly

$$\bar{\mathbf{e}}_1 = (\bar{\mathbf{e}}_{1,1}, \bar{\mathbf{e}}_{1,2}, \cdots, \bar{\mathbf{e}}_{1,g})$$

where $\bar{\mathbf{e}}_{1,i} \in \mathbb{Z}_q^n$. Let $\{\mathbf{v}_i \in \mathbb{Z}_q^n\}_{i\in[g]}$ be the solution of equation $\{\mathbf{v}_i\bar{\mathbf{R}}_i = \bar{\mathbf{e}}_{1,i}\}_{i\in[g]}$. Obviously, if $\mathbf{R}_i$ is random over $\mathbb{Z}_q^{n\times n}$, then $\mathbf{v}_i$ has a unique solution with an overwhelming probability(See Appendix A). Let $\mathcal{D}$ be the distribution over the randomness of $\bar{\mathbf{R}}$ and $\bar{\mathbf{e}}_1$.

$$\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_g) \hookleftarrow \mathcal{D}$$

Let Φ' be the joint distribution of hybrid key, $\mathcal{D}$ and the leakage of $\mathbf{s}$:

$$(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s})) \hookleftarrow \Phi'$$

Let $\mathcal{D}_0(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}))$ be the joint distribution of $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}))$ and the ciphertext

$$\mathbf{C} = \begin{pmatrix}\mathbf{A}_\mathsf{H}\mathbf{R} + \mathbf{E}_0\\ (\mathbf{b}_\mathsf{H} + \mathbf{v}_1)\mathbf{R}_1 + \mathbf{e}_{1,1}, (\mathbf{b}_\mathsf{H} + \mathbf{v}_2)\mathbf{R}_2 + \mathbf{e}_{1,2}, \cdots, (\mathbf{b}_\mathsf{H} + \mathbf{v}_g)\mathbf{R}_g + \mathbf{e}_{1,g}\end{pmatrix}$$

encrypted by $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v})$ over the randomness $\mathbf{R} = (\mathbf{R}_1, \cdots, \mathbf{R}_g) \leftarrow U(\mathbb{Z}_q^{n\times ml})$, $\mathbf{E}_0 \leftarrow \chi^{(m-1)\times ml}$, $\mathbf{e}_1 = (\mathbf{e}_{1,1}, \cdots, \mathbf{e}_{1,g}) \leftarrow \chi^{ml}$:

$$(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}), \mathbf{C}) \hookleftarrow \mathcal{D}_0(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}))$$

Similarly, Let $\mathcal{D}_1(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}))$ be the joint distribution of $(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}))$ and the uniform $\mathbf{U}$

$$(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}), \mathbf{U}) \hookleftarrow \mathcal{D}_1(\mathbf{A}_\mathsf{H}, \mathbf{b}_\mathsf{H}, \mathbf{v}, f(\mathbf{s}))$$

Let P' be the decision problems defined as follows :

[5] Here we ignore the input of Φ, which should be $\mathbf{s}$, $\mathbf{A}_\mathsf{H}$ and other party's DGSW key pair, but it is irrelevant here.

[6] Note that $||\mathbf{e}_1||/||\bar{\mathbf{e}}_1|| = \mathsf{negl}(\lambda)$.

– Problem P' : distinguish whether input x is sampled from distribution X'_0 or X'_1, where

$$X'_0 = \{x : r \hookleftarrow \Phi', x \hookleftarrow \mathcal{D}_0(r)\}, \qquad X'_1 = \{x : r \hookleftarrow \Phi', x \hookleftarrow \mathcal{D}_1(r)\}.$$

So far, we have completed the construction of the P and P' problems. Next, we show that some samples of X'_0 can be constructed from samples of DGSWLRL. Let $\left(\mathsf{pk}_{\mathsf{DGSW}}, \{\mathbf{v}_i\}_{i\in[g]}, f(\mathbf{s}), \mathbf{C}_{\mathsf{DGSW}}\right)$ be a DGSWLRL sample generated by Challenger. After receiving $\mathbf{s}'$ from the adversary $\mathcal{A}$, he can construct a tuple $(\mathbf{A}_{\mathsf{H}}, \mathbf{b}_{\mathsf{H}}, \mathbf{v}, f(\mathbf{s}), \mathbf{C}')$, by setting $\mathbf{A}_{\mathsf{H}} = \mathbf{A}_{\mathsf{DGSW}}$, $\mathbf{b}_{\mathsf{H}} = \mathbf{b}_{\mathsf{DGSW}} + \mathbf{s}'\mathbf{A}_{\mathsf{H}}$, and $\mathbf{C}' = \mathbf{C}_{\mathsf{DGSW}} + \begin{pmatrix} \mathbf{0} \\ \mathbf{s}'\mathbf{C}_0 \end{pmatrix}$, where $\mathbf{C}_0$ is the first $m-1$ rows $\mathbf{C}_{\mathsf{DGSW}}$. We note that this tuple is exactly a sample of X'_0, when $r = (\mathbf{A}_{\mathsf{H}}, \mathbf{b}_{\mathsf{H}}, \mathbf{v}, f(\mathbf{s}))$, and the $\bar{\mathbf{R}}$ used in $\mathbf{v}$ and the $\mathbf{R}$ used in $\mathcal{D}_0$ are consistent.

Next, we verify the conditions for the establishment of Theorem 2. Firstly, we have $\mathsf{Supp}(\Phi) \subseteq \mathsf{Supp}(\Phi')$, and $\mathcal{D}_0(\cdot)$, $\mathcal{D}_1(\cdot)$ are determined by pre-image sample $r \in \mathsf{Supp}(\Phi')$. Since the outputs of $\mathcal{D}_0(\cdot)$ and $\mathcal{D}_1(\cdot)$ contain the r of the prior distributions Φ and Φ', thus $\mathcal{D}_0(\cdot)$ and $\mathcal{D}_1(\cdot)$ satisfy the publicly sampleable property required by Theorem 2. The sampling algorithm S is just the encryption of our scheme with hybrid key $(\mathbf{A}_{\mathsf{H}}, \mathbf{b}_{\mathsf{H}}, \mathbf{0}^{ml})$ or $(\mathbf{A}_{\mathsf{H}}, \mathbf{b}_{\mathsf{H}}, \mathbf{v})$, over the randomness of $\{\mathbf{R}, \mathbf{E}_0, \mathbf{e}_1\}$

By Theorem 2, if given a T- time distinguisher $\mathcal{A}$ for problem P with advantage ϵ, we can construct a distinguisher $\mathcal{A}'$ for problem P'(also for distinguishing DGSWLRL) with run-time and distinguishing advantage, respectively, bounded from above and below by(for any $a \in (1, +\infty]$) :

$$\frac{64}{\epsilon^2}\log\left(\frac{8R_a(\Phi||\Phi')}{\epsilon^{a/(a-1)+1}}\right)\cdot(T_S+T) \quad and \quad \frac{\epsilon}{4\cdot R_a(\Phi||\Phi')}\cdot\left(\frac{\epsilon}{2}\right)^{\frac{a}{a-1}}.$$

Assume that $R_a(\Phi||\Phi')$ is *well-behaved*[7], that is, there is a in $\mathbb{R}^+$ such that $R_a(\Phi||\Phi') = \mathsf{poly}(\lambda)$, then we have :

$$\frac{64}{\epsilon^2}\log\left(\frac{\mathsf{poly}(\lambda)}{\epsilon^{a/(a-1)+1}}\right)\cdot(T_S+T) \quad and \quad \frac{\epsilon}{4\cdot \mathsf{poly}(\lambda)}\cdot\left(\frac{\epsilon}{2}\right)^{\frac{a}{a-1}}.$$

■

Remark : Under the semi-honest adversary model, $\{\mathbf{A}_i\}_{i\in[k]}$ and $\{\mathbf{s}_i\}_{i\in[k]}$ are sampled as specified by the protocol, and the security is guaranteed. Under the semi-malicious adversary model, the common approach assumes that $\mathbf{b}_{j,i} = \mathbf{s}_j\mathbf{A}_i$ and $\{\mathbf{s}_{j\in[k]/1}\} \in \{0,1\}^{m-1}$ are chosen adaptively, and introduces large noise in the encryption to ensure security. However, in our proof method based on the Rényi divergence, in order to better quantify $R_a(\Phi||\Phi')$, we introduce heuristic assumptions.

8 Decryption without noise flooding

We note that introducing noise flooding in the partial decryption phase is essential to guarantee the semantic security of fresh ciphertext, and noise flooding achieves this by masking the private key in the partial decryption noise. For partial decryption to be simulatable, the magnitude of the noise introduced needs to be exponentially larger than the noise after the homomorphic evaluation.

By noise flooding : To illustrate how our approach works, let us first review the noise flooding technique. Let $\mathbf{C}^{(L)} = \begin{pmatrix} \mathbf{C}_{up} \\ \mathbf{c}_{low} \end{pmatrix}$ be the ciphertext after L-layer homomorphic multiplication. With a flooding noise $e''_i \leftarrow U[-B_{smdg}, B_{smdg}]$, introduced in $\mathsf{LocalDec}(\cdot)$, we have

$$\gamma_i = \langle -\mathbf{s}_i, \mathbf{C}_{up}\mathbf{G}^{-1}(\mathbf{w}^T)\rangle + e''_i$$

By Equation (10) and $\mathsf{FinalDec}(\cdot)$

$$\gamma_i = u_L\lceil\frac{q}{2}\rceil + \langle \mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + e''_i - \langle \mathbf{c}_{low}, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \langle \sum_{j\neq i}^{k}\mathbf{s}_j, \mathbf{C}_{up}\mathbf{G}^{-1}(\mathbf{w}^T)\rangle$$

[7] We have not yet found a suitable a. Here we can only introduce this heuristic assumption

For a simulator $\mathcal{S}$, input $\{\mathsf{sk}_j\}_{j\in[k]/i}$, evaluated result u_L, ciphertext $\mathbf{C}^{(L)}$, output simulated γ_i'

$$\gamma_i' = u_L\lceil\frac{q}{2}\rceil + e_i'' - \langle\mathbf{c}_{low}, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \langle\sum_{j\neq i}^{k}\mathbf{s}_j, \mathbf{C}_{up}\mathbf{G}^{-1}(\mathbf{w}^T)\rangle$$

In order to make the partial decryption process simulatable, it requires

$$\langle\mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + e_i'' \overset{\mathsf{stat}}{\approx} e_i''$$

For the parameter settings in [22] : $B_{smdg} = 2^{L\lambda\log\lambda}B_\chi$, $q = 2^{\omega(L\lambda\log\lambda)}B_\chi$, it holds that

$$|\langle\mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle/e_i''| = \mathsf{negl}(\lambda)$$

thus $\gamma_i \overset{\mathsf{stat}}{\approx} \gamma_i'$. In short, the noise e_i'' is introduced to "drown out" the private key $\mathbf{s}_i$ and the noise $\mathbf{E}_i$ in initial ciphertext of party i contained in $\mathbf{e}_L$(The noise obtained by decrypting the ciphertext of level L, $\bar{\mathbf{t}}\mathbf{C}^{(L)} = \mathbf{e}_L + u_L\bar{\mathbf{t}}\mathbf{G}$). Thus the partial decryption result of party i can be simulated.

Without noise flooding : Through the above analysis, we point out that as long as our encryption scheme is leakage-resilient and $\mathbf{e}_L$ is independent of the noise $\{\mathbf{E}_i\}_{i\in[N]}$ in the initial ciphertext, there is no need to introduce noise flood in the partial decryption. Before the homomorphic evaluation begins, we can left-multiply each initial ciphertext by a "dummy" ciphertext whose plaintext is 1 to drown out the noise in the initial ciphertext. For example, let the "dummy" and initial ciphertext be $\mathbf{C}_{\mathsf{dummy}}$, $\mathbf{C}$, respectively.

$$\mathbf{C}_{\mathsf{dummy}} = \begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_1 + \mathbf{E}_1 + \mathbf{G}, \qquad \mathbf{C} = \begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_2 + \mathbf{E}_2 + u\mathbf{G}.$$

After the homomorphic multiplication , we obtain

$$\mathbf{C}_{\mathsf{mult}} = \mathbf{C}_{\mathsf{dummy}}\mathbf{G}^{-1}(\mathbf{C}) = \mathit{\Pi} + \mathit{\Psi} + u\mathbf{G}$$

where

$$\mathit{\Pi} = \begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_1\mathbf{G}^{-1}(\mathbf{C}) + \begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_2$$
$$\mathit{\Psi} = \mathbf{E}_1\mathbf{G}^{-1}(\mathbf{C}) + \mathbf{E}_2.$$

We have $\bar{\mathbf{t}}\mathit{\Pi} = 0$, $\mathit{\Psi}$ is the noise after the the homomorphic multiplication. By Corollary 2, we have

$$\mathit{\Psi} \overset{\mathsf{stat}}{\approx} \mathbf{E}_1\mathbf{G}^{-1}(\mathbf{C}).$$

Therefore, the ciphertext after homomorphic evaluation hardly contains the noise in the initial ciphertext $\{\mathbf{C}_i\}_{i\in[N]}$. Let $\mathbf{e}_L = \bar{\mathbf{t}}\mathit{\Psi}$, therefore, $\langle\mathbf{e}_L, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle \in \mathbb{Z}_q$ leaks party i's private key $\mathbf{s}_i$ with at most $\log q$ bits. For a circuit with output length W, the partial decryption leaks $W\log q$ bits of $\mathbf{s}_i$. Because our scheme is leakage-resilient, as long as we set the key length reasonably as $m = (kn+W)\log q + \lambda$, the initial ciphertext $\{\mathbf{C}_i\}_{i\in[N]}$ are semantically secure.

The key length of our scheme is related to the output length of the circuit. When the circuit output length $W < kn(\lambda-1)$, our scheme has a shorter key than the previous scheme (using noise flooding technology with key length $m' = kn\log q' + \lambda$, modules $q' = 2^{O(\lambda L)}B_\chi$). For our scheme, $m = (kn+W)\log q + \lambda$, and $q = 2^{O(L)}B_\chi$, in order to make $m < m'$, it is only required that $W < kn(\lambda-1)$. Therefore, for circuits with small output fields, our scheme does not result in longer keys.

8.1 Bootstrapping

In order to eliminate the dependence on circuit depth and achieve full homomorphism, we need to utilize Gentry's bootstrapping technology. It is worth noting that the bootstrapping procedure of our scheme is the same as the single-key homomorphic scheme: After *Key lifting* procedure, party i uses

hybrid key hk_i to encrypt $\mathbf{s}_i$ to obtain evaluation key evk_i. Because evk_i and $\mathbf{C}^{(L)}$ 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 $\mathbf{C}^{(L)}$ needs to be refreshed. Therefore, to evaluate any depth circuit, we only need to set the initial parameters in order to satisfy the homomorphic evaluation of the decryption circuit.

However, for those MKFHE schemes that require ciphertext expansion, additional ciphertext expansion is necessary. This is because $\mathbf{C}^{(L)}$ is the ciphertext under $\bar{\mathbf{t}}$, while $\{\mathsf{evk}_i\}_{i\in[k]}$ are the ciphertext under $\{\mathbf{t}_i\}_{i\in[k]}$. In order to expand $\{\mathsf{evk}_i\}_{i\in[k]} \to \{\widehat{\mathsf{evk}_i}\}_{i\in[k]}$, party i needs to encrypt the random matrix of the ciphertext corresponding to evk_i. The extra encryption of i needs to be done locally is $O(\lambda^9 L^6)$.

9 Conclusions

For the LWE-based MKFHE, we proposed the concept of KL-MKFHE to reduce the overhead of the local parties. This concept introduces a *Key lifting* procedure, getting rid of expensive ciphertext expansion operations and allowing the construction of a DGSW style KL-MKFHE under the plain model. Our scheme is more friendly to local parties than the previous scheme, for which the local encryption $O(N\lambda^6 L^4)$ are reduced to $O(N)$. By abandoning noise flooding, it compresses q from $2^{O(\lambda L)}B_\chi$ to $2^{O(L)}B_\chi$, reducing the computational scale of the entire scheme. However, the key length depends on the number of parties and the amount of leakage, which limits the scheme's application to some extent. Further work will focus on compressing the key length.

References

1. Alperin-Sheriff, J., Peikert, C.: Faster bootstrapping with polynomial error. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 297–314. Springer, Heidelberg (Aug 2014)
2. Ananth, P., Asharov, G., Dahari, H., Goyal, V.: Towards accountability in crs generation. In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021. pp. 278–308. Springer International Publishing, Cham (2021)
3. Ananth, P., Jain, A., Jin, Z., Malavolta, G.: Multi-key fully-homomorphic encryption in the plain model. In: Pass, R., Pietrzak, K. (eds.) TCC 2020, Part I. LNCS, vol. 12550, pp. 28–57. Springer, Heidelberg (Nov 2020)
4. Ananth, P., Jain, A., Jin, Z., Malavolta, G.: Unbounded multi-party computation from learning with errors. In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021. pp. 754–781. Springer International Publishing, Cham (2021)
5. Asharov, G., Jain, A., López-Alt, A., Tromer, E., Vaikuntanathan, V., Wichs, D.: Multiparty computation with low communication, computation and interaction via threshold FHE. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 483–501. Springer, Heidelberg (Apr 2012)
6. Bai, S., Lepoint, T., Roux-Langlois, A., Sakzad, A., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. Journal of Cryptology 31(2), 610–640 (Apr 2018)
7. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen 296, 625–635 (1993)
8. Brakerski, Z., Döttling, N.: Two-message statistically sender-private OT from LWE. In: Beimel, A., Dziembowski, S. (eds.) TCC 2018, Part II. LNCS, vol. 11240, pp. 370–390. Springer, Heidelberg (Nov 2018)
9. Brakerski, Z., Halevi, S., Polychroniadou, A.: Four round secure computation without setup. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017, Part I. LNCS, vol. 10677, pp. 645–677. Springer, Heidelberg (Nov 2017)
10. Brakerski, Z., Perlman, R.: Lattice-based fully dynamic multi-key FHE with short ciphertexts. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 190–213. Springer, Heidelberg (Aug 2016)
11. Chen, H., Dai, W., Kim, M., Song, Y.: Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In: Cavallaro, L., Kinder, J., Wang, X., Katz, J. (eds.) ACM CCS 2019. pp. 395–412. ACM Press (Nov 2019)
12. Chen, L., Zhang, Z., Wang, X.: Batched multi-hop multi-key FHE from ring-LWE with compact ciphertext extension. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017, Part II. LNCS, vol. 10678, pp. 597–627. Springer, Heidelberg (Nov 2017)
13. Clear, M., McGoldrick, C.: Multi-identity and multi-key leveled FHE from learning with errors. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 630–656. Springer, Heidelberg (Aug 2015)

14. Dachman-Soled, D., Gong, H., Kulkarni, M., Shahverdi, A.: Towards a ring analogue of the leftover hash lemma. Journal of Mathematical Cryptology 15(1), 87–110 (2021)
15. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (Aug 2013)
16. Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-random generation from one-way functions (extended abstracts). In: 21st ACM STOC. pp. 12–24. ACM Press (May 1989)
17. López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Karloff, H.J., Pitassi, T. (eds.) 44th ACM STOC. pp. 1219–1234. ACM Press (May 2012)
18. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 35–54. Springer, Heidelberg (May 2013)
19. Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (Apr 2012)
20. Mouchet, C., Troncoso-Pastoriza, J., Hubaux, J.P.: Computing across trust boundaries using distributed homomorphic cryptography. Cryptology ePrint Archive, Paper 2019/961 (2019), https://eprint.iacr.org/2019/961, https://eprint.iacr.org/2019/961
21. Mouchet, C., Troncoso-Pastoriza, J.R., Bossuat, J.P., Hubaux, J.P.: Multiparty homomorphic encryption from ring-learning-with-errors. PoPETs 2021(4), 291–311 (Oct 2021)
22. Mukherjee, P., Wichs, D.: Two round multiparty computation via multi-key FHE. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 735–763. Springer, Heidelberg (May 2016)
23. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Mitzenmacher, M. (ed.) 41st ACM STOC. pp. 333–342. ACM Press (May / Jun 2009)
24. Peikert, C., Shiehian, S.: Multi-key fhe from lwe, revisited. In: Theory of Cryptography Conference. pp. 217–238. Springer (2016)
25. Peikert, C., Shiehian, S.: Multi-key FHE from LWE, revisited. Cryptology ePrint Archive, Report 2016/196 (2016), https://eprint.iacr.org/2016/196
26. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC. pp. 84–93. ACM Press (May 2005)
27. Stehlé, D., Steinfeld, R.: Making ntru as secure as worst-case problems over ideal lattices. In: Annual international conference on the theory and applications of cryptographic techniques. pp. 27–47. Springer (2011)

Appendix

A Probability that $\{v_i\}_{i\in[g]}$ has a solution

Random Matrices : For a prime q, the probability that a uniformly random matrix $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$(with $m \geq n$) has full rank is :

$$\Pr[\mathsf{rank}(\mathbf{A}) < n] = 1 - \prod_{i=0}^{n-1}(1 - q^{i-m}).$$

For equations :

$$\{\mathbf{v}_i\mathbf{R}_i = \mathbf{e}_{1,i}\}_{i\in[g]}$$

if $\{\mathbf{R}_i\}_{i\in[g]}$ are all invertible, obviously $\{\mathbf{v}_i\}_{i\in[g]}$ has a solution. For a random matrix $\mathbf{R}$ over $\mathbb{Z}_q^{n\times n}$, the probability that it is invertible is $\prod_{i=0}^{n-1}(1 - q^{i-n})$. For the parameter settings in our scheme, $q = 2^{O(L)}B_\chi$, $m = (kn + W)\log q + 2\lambda$, $g = mL/n$, the probability that $\{\mathbf{R}_i\}_{i\in[g]}$ are all invertible is :

$$\Pr = (\prod_{i=0}^{n-1}(1 - (2^L)^{i-n})^{\frac{(kn+W)L^2+2\lambda L}{n}} \geq (1 - 2^{-L})^{(kn+W)L^2+2\lambda L}$$

This probability is close to 1, for 2^{-L} decreases faster than L^2. We tested the probability on **Maple18** by set $q = 2^{100}$, $k = 50$, $n = 500$, $W = 1000$, $\lambda = 128$(which should be able to cover the actual application) obtained $\Pr > 1 - 10^{21}$.

B The proof of Lemma 2 and Theorem 4

Recall that the integral of $\rho_\Sigma(\mathbf{x})$ is $\det(\Sigma)$, thus the Fourier transform of $\rho_\Sigma(\mathbf{x})$ is $\hat{\rho}_\Sigma(\mathbf{k}) = \det(\Sigma)\rho_{\Sigma^{-1}}(\mathbf{k})$, and the Poisson summation formula of $\rho_\Sigma(\mathbf{x})$ is $\rho_\Sigma(\Lambda) = \det(\Sigma)\det(\Lambda^*)\rho_{\Sigma^{-1}}(\Lambda^*)$

B.1 The proof of Lemma 2

By the Poisson summation formula, we have :

$$\begin{aligned}\rho_{\Sigma_1\Sigma_2} &= \det(\Sigma_1)\det(\Sigma_2)\det(\Lambda^*)\rho_{(\Sigma_1\Sigma_2)^{-1}}(\Lambda^*)\\ \det(\Sigma_1)\rho_{\Sigma_2} &= \det(\Sigma_1)\det(\Sigma_2)\det(\Lambda^*)\rho_{\Sigma_2^{-1}}(\Lambda^*)\end{aligned}$$

If $\rho_{\Sigma_2^{-1}}(\Lambda^*) > \rho_{(\Sigma_1\Sigma_2)^{-1}}(\Lambda^*)$, then we done. For $\rho_{\Sigma_2^{-1}}(\mathbf{x}) = e^{-\pi\mathbf{x}\Sigma_2\mathbf{x}^T}$, $\rho_{(\Sigma_1\Sigma_2)^{-1}}(\mathbf{x}) = e^{-\pi\mathbf{x}\Sigma_1\Sigma_2\mathbf{x}^T}$, if $\Sigma_1\Sigma_2 - \Sigma_2$ is positive semi-definite, then we have $\rho_{\Sigma_2^{-1}}(\mathbf{x}) > \rho_{(\Sigma_1\Sigma_2)^{-1}}(\mathbf{x})$, thus $\rho_{\Sigma_2^{-1}}(\Lambda^*) > \rho_{(\Sigma_1\Sigma_2)^{-1}}(\Lambda^*)$.

B.2 The proof of Theorem 4

Let $\mathcal{E}(k) = \{\mathbf{x} \in \mathbb{R}^m : \mathbf{x}\Sigma_2^{-1}\mathbf{x}^T < k\}$ be the ellipsoid with "shape" Σ_2 and radius k, and positive definite matrix Σ_1, Σ_2, we have :

$$\begin{aligned}\rho_{\Sigma_1\Sigma_2}(\Lambda) &\geq \rho_{\Sigma_1\Sigma_2}(\Lambda\backslash\mathcal{E}(k))\\ &= \sum_{\mathbf{x}\in(\Lambda\backslash\mathcal{E}(k))} e^{-\pi\mathbf{x}(\Sigma_1\Sigma_2)^{-1}\mathbf{x}^T+\pi\mathbf{x}\Sigma_2^{-1}\mathbf{x}^T}\cdot e^{-\pi\mathbf{x}\Sigma_2^{-1}\mathbf{x}^T}\\ &= \sum_{\mathbf{x}\in(\Lambda\backslash\mathcal{E}(k))} e^{\frac{1}{2}\pi\mathbf{x}\Sigma_2^{-1}\mathbf{x}^T}\cdot e^{-\pi\mathbf{x}\Sigma_2^{-1}\mathbf{x}^T} \qquad (\text{let } \Sigma_1 = 2\mathbf{I})\\ &\geq \sum_{\mathbf{x}\in(\Lambda\backslash\mathcal{E}(k))} e^{\frac{1}{2}\pi k}\cdot e^{-\pi\mathbf{x}\Sigma_2^{-1}\mathbf{x}^T}\\ &= e^{\frac{\pi}{2}k}\cdot\rho_{\Sigma_2}(\Lambda\backslash\mathcal{E}(k))\end{aligned}$$

By Lemma 2 we have $2^m\cdot\rho_{\Sigma_2}(\Lambda) \geq \rho_{2\Sigma_2}(\Lambda)$ and $e^{\frac{\pi}{2}} > 4$, thus $\rho_{\Sigma_2}(\Lambda\backslash\mathcal{E}(k)) < 2^{m-2k}\cdot\rho_{\Sigma_2}(\Lambda)$.