Lattice-based, more general anti-leakage model and its application in decentralization

Fullversion : https://eprint.iacr.org/2023/699

Xiaokang Dai,[1,2] Jingwei Chen,[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 chenjingwei@cigit.ac.cn wuwenyuan@cigit.ac.cn yongfeng@cigit.ac.cn

Abstract. In the case of standard LWE samples $(\mathbf{A}, \mathbf{b} = \mathbf{sA} + \mathbf{e})$, $\mathbf{A}$ is typically uniformly over $\mathbb{Z}_q^{n\times m}$, and under the LWE assumption, the conditional distribution of $\mathbf{s}$ given $\mathbf{b}$ and $\mathbf{s}$ should be consistent. However, if an adversary chooses $\mathbf{A}$ adaptively, the gap between the two may be larger. In this work, we are mainly interested in quantifying $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$, while $\mathbf{A}$ an adversary chooses. Brakerski and Döttling answered the question in one case: they proved that when $\mathbf{s}$ is uniformly chosen from $\mathbb{Z}_q^n$, it holds that $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e}) \propto \rho_\sigma(\Lambda_q(\mathbf{A}))$. We prove that for any $d \leq q$, $\mathbf{s}$ is uniformly chosen from $\mathbb{Z}_d^n$ or is sampled from a discrete Gaussian, the above result still holds.
In addition, as an independent result, we have also proved the regularity of the hash function mapped to the prime-order group and its Cartesian product.
As an application of the above results, we improved the multi-key fully homomorphic encryption [16] and answered the question raised at the end of their work positively: we have GSW-type ciphertext rather than Dual-GSW, and the improved scheme has shorter keys and ciphertexts

Keywords: Leftover hash lemma · Leakage resilient cryptography · Multi-key FHE

1 Introduction

In the real world, hardware devices that host cryptographic algorithms expose additional information to the external environment during operation, such as noise, temperature, execution time, electromagnetic radiation, etc. If these features can be captured more accurately, then the intermediate state of the algorithm or private key may no longer be perfectly private.

In response to this attack model, the cryptographic community has re-evaluated the "black-box" adversary model and above adversary model with auxiliary inputs(noise, power, time, temperature, etc.) and proposed a series of corresponding solutions: such as [18] [24] [1] [29]. This line of work became known as "leakage-resilient cryptography" For more details, please refer to "Survey of Leakage-Resilient Cryptography [31]."

"Passive Leakage" Caused by Physical Devices : If we assume that our level of manufacturing technology can create such a set of cryptographic hardware: any algorithm running on it will not emit any sound, detect no radiation, and give output at a constant time, then the above leaks will not exist. Informally, we refer to such leaks in the real world but not in the ideal world as "passive leaks" (caused by the real physical world but unrelated to encryption, signing, computing tasks etc.). Next, we introduce another type of leakage different from "passive leakage", called "active leakage".

Active Leakage in Decentralization: In the era of massive data, it has become a trend for multiple companies and service providers to cooperate in providing data and training better parameters and models, such as Federated learning [32], privacy-preserving data mining [12].

Private information retrieval(PIR) [21], Secure multi-party computing(MPC) [42], Threshold fully homomorphic encryption(Th-FHE) and Multi-key fully homomorphic encryption(MKFHE) [33] provide technical support for the above applications. Depending on the assumptions, the above

techniques can be divided into two categories: the first with setup (trusted third party, common reference string(CRS)), and the second without setup (plain model).

Compared with the schemes or protocols under the plain model, those schemes that introduce a trusted third party or CRS are much simpler and more efficient, especially in the initialization phase. However, some people believe that introducing such assumptions seems like cheating (Since there is such a trusted third party, why not put everyone's data in his hands and then return the results to all parties?), so building cryptographic primitives under the plain model has also become a demand for some people.

The key issue here is that for the initialization of MPC, Th-FHE or MKFHE protocols, such as key generation, often rely on some common parameters. If these parameters come from a trusted third party, their regularity can be guaranteed, otherwise, the protocol initialization is often an interactive process that may involve data provided by other users (who may be adversaries), and the regularity of the data cannot be guaranteed, which may lead to the leakage of user privacy. We call this kind of leakage caused by the protocol itself "active leakage".

For example, In the MKFHE scheme [16], parties need to multiply their own private key $\mathbf{s}$ with $\mathbf{A}$ generated by other party and make $\mathbf{sA}$ public in order to support "ciphertext expansion". In the oblivious transfer protocol [13], the first round message $\mathbf{y} = \mathbf{tA} + \mathbf{e}$ of the sender is composed of its own secret $\mathbf{t}$ multiplied by $\mathbf{A}$ generated by the receiver plus a small disturbance. Similarly, the unbounded MPC protocol [5] also needs to make the class LWE sample $\mathbf{y} = \mathbf{sA} + \mathbf{e}$ public, where $\mathbf{A}$ is generated by the adversary.

Apart from the different reasons for "active leakage" and "passive leakage" mentioned above (one is caused by the physical world, and the other is caused by the protocol itself), there are also great differences in the way of leakage. There are many known side-channel attacks, including timing analysis attacks, power consumption attacks, electromagnetic analysis attacks, and optical analysis attacks. Therefore, designing cryptographic primitives resistant to a specific type of leakage may not be very meaningful. Thus, the formalization of leakage-resilient primitives does not care about specific attack methods but the private key(e.g., the conditional min-entropy of the key is sufficient).

However, the situation is different for "active leakage". As far as we know, the ways of "active leakage" are very limited, especially in the context of decentralized applications based on lattices. Therefore, it is necessary to study some "mainstream" or "common active leakage" and reasonably quantify them. Next, we will introduce specific examples and motivations.

Remark : We must admit that CRS has always been a dark cloud over secure multi-party computing, and how to weaken it has always been a research hotspot. Recently, the work [3] 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 randomness; otherwise, the challenging party can provide a publicly verifiable proof that certifies the authority's misbehaviour. We believe this could be an effective means of balancing authority.

1.1 Motivation

In MKFHE scheme [16], in order to support subsequent *ciphtertext expansion*, the "active leakage" was $\mathbf{b} = \mathbf{sA}_i$. Assuming there were k parties, each one needs to multiply their own private key $\mathbf{s}$ by the public keys $\{\mathbf{A}_i\}_{i\in[k-1]}$ of other $k-1$ parties and make $\{\mathbf{b}_i = \mathbf{sA}_i\}_{k-1}$ public. In order to quantify the effective bits of $\mathbf{s} \in \{0,1\}^m$ after disclosing $\{\mathbf{b}_i = \mathbf{sA}_i\}_{k-1}$, it estimated the leakage in the worst case : Assuming $\mathbf{b} \in \mathbb{Z}_q^n$, then $\{\mathbf{b}_i = \mathbf{sA}_i\}_{k-1}$ leaked $(k-1)n\log q$ bits of $\mathbf{s}$. According to the proof method in [16], based on the Leftover Hash Lemma(LHL), in order to make the statistical distance between ciphertext and uniform distribution less than $\frac{1}{2^\kappa}$, m should be at least $m - (k-1)n\log q \geq \log q + 2\kappa$.

In [13], it applied another "active leakage" model $\mathbf{s}|\mathbf{b} = \mathbf{sA} + \mathbf{e}$. To ensure that the entropy of $\mathbf{s}$ is still sufficient after $\mathbf{b} = \mathbf{sA} + \mathbf{e}$ is disclosed, it proved that $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e}) \geq -\log(\frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))} + 2^{-m})$. We believe that $\mathbf{s}|\mathbf{sA} + \mathbf{e}$ is a better "active leakage" model compared to $\mathbf{s}|\mathbf{sA}$, because $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$ establishes a relationship with $\Lambda_q(\mathbf{A})$, and its loss ratio is $O(\frac{1}{\log q})$, while the latter is $O(\frac{1}{n})$. Based on this, the work [13] constructed the first post-quantum secure oblivious transfer protocol under the plain model that can resist malicious receivers.

So far, we have seen two "active leakage" models, $\mathbf{s}|\mathbf{sA}$ and $\mathbf{s}|\mathbf{sA}+\mathbf{e}$. The former quantifies the conditional entropy of $\mathbf{s} \in \{0,1\}^*$ in a more rudimentary way, while the latter characterizes $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$ based on the properties of lattices, but is limited to $\mathbf{s} \leftarrow \mathbb{Z}_q^n$. We are interested in whether there is a similar result $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e}) \geq -\log(\frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))}+2^{-m})$, for any $d \leq q$, $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, or $\mathbf{s}$ is sampled from a discrete Gaussian.

Such a requirement is not groundless. In the LWE-like sample $\mathbf{sA}+\mathbf{e}$, it is sometimes convenient and necessary to bound the norm of $\mathbf{s}$. For example, in order to support bootstrapping in FHE, it is necessary to encrypt the private key $\mathbf{s}$. If $\mathbf{s}$ is uniform over $\mathbb{Z}_q$, how can it be filled into the plaintext space? Therefore, [6] reduced the LWE problem with secrets taken from discrete Gaussian to the standard LWE problem. MKFHE scheme [19] required that $\mathbf{s}$ must be sampled from the discrete Gaussian in order to alleviate the noise introduced by the *re-linearization* after multiplication of the ciphertext. Furthermore, [27] proved that Regev's encryption scheme was leakage-resilient when taking private key $\mathbf{s}$ from a small uniform range([27] only gave a reduction for $\mathbf{s} \in \{0,1\}^*$ in the original text, but the result holds for all sufficiently small $\mathbf{s}$). In addition, [5] uses the result of [13] to resist semi-malicious adversaries, but in their scheme, $\mathbf{s}$ is taken from a discrete Gaussian distribution.

Therefore, if we can characterize $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$ for any $d \leq q$, $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, or $\mathbf{s}$ is taken from a discrete Gaussian distribution. we believe that this result can be applied in many ways. Specifically, based on this result, we optimized the MKFHE [16], resulting in shorter keys and smaller ciphertexts. We introduce our results in the following section.

1.2 Our Results

For LWE samples whose secrets are sampled from a discrete Gaussian, we have the following result :

Theorem 1 *For a given matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ with $m = O(n\log q)$. Let $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \mathbf{s}\bar{\mathbf{A}}+\bar{\mathbf{e}})$, where $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\bar{\mathbf{e}} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $0 < \sigma < \frac{q}{2\sqrt{m+n}}$, be n LWE samples. Let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A})$, $\mathbf{b} = \mathbf{sA}+\mathbf{e}$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$. It holds that :*

$$\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}'+\mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}},\mathbf{e}|\bar{\mathbf{e}}\mathbf{A}'+\mathbf{e}) \geq \tilde{H}_\infty(\bar{\mathbf{e}},\mathbf{e}|\bar{\mathbf{b}},\mathbf{b}) \geq -\log\left(\frac{1}{\rho_\sigma(\Lambda_q(\tilde{\mathbf{A}})}+2^{-(m+n)}\right)$$

When the secret $\mathbf{s}$ is uniform, we proved a more general version of Lemma 3.2 in [13] (Lemma 3.2 is a special case of our theorem).

Theorem 2 *Let d, q, $0 < d \leq q$ be integers, $\mathbf{A} \in \frac{q}{d}\mathbb{Z}_d^{n\times m}$, $m = O(n\log d)$ and a parameter $0 < \sigma < \frac{d}{\sqrt{m}}$. Let $\mathbf{s} \leftarrow \mathbb{Z}_d^n$ and $\mathbf{e} \leftarrow \mathcal{D}_{\frac{q}{d}\mathbb{Z}^m,\sigma}$, then it holds that :*

$$\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e}) \geq -\log(\frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))}+2^{-m})$$

Clearly, when $d = q$, the above theorem degenerates to Lemma 3.2.

In addition, as an independent result, we also proved the regularity of the universal hash function mapped to a prime order group and its Cartesian product(Lemma6 and Corollary2) to prove the security of our improved scheme.

As an application of the above results, we optimized the MKFHE scheme in [16]. It must be pointed out that [16] seems to be becoming a cornerstone, which is increasingly used in constructing more complex protocols, especially in the MPC protocol with the optimal number of rounds. Such as [9] based on [16] constructed a three-round protocol in the simultaneous message exchange model with rushing adversaries that achieves sub-exponential concurrent super-polynomial simulation (SPS) security for secure multi-party computation for any efficiently computable function, in which all parties can receive output. Based on [16], [10] constructed a secure threshold multi-key FHE scheme for the class of access structures $\{0,1\}$-LSSSD. The work [28], based on [16], constructed an MPC while does not require the parties to be online simultaneously or interact with

each other. As the main building block [16] used in [8] to construct a maliciously circuit-private MKFHE scheme.

Therefore, the above applications should all benefit from our improved scheme. In particular, combined with the proof trick of [27] for the LWE variant of binary keys, we answer the question posed at the end of [16] in positive form: the ciphertext of our improved scheme is GSW-like constructed, instead of Dual GSW. In addition, compared with [16], our ciphertext and key are shorter, Table 1 lists the complexity comparison of the improved scheme:

Table 1: Complexity

Scheme	Key size	Ciphertext size	Hom-multiplication	Comunication in setup	Setup
[35]	$O(n^2 \log^2 q)$	$O(n^2 \log^2 q)$	$O(k^3 n^3 \log^2 q)$	-	CRS
[16]	$O(kn^2 \log^2 q)$	$O(k^2 n^2 \log^4 q)$	$O(k^6 n^3 \log^5 q)$	$O(kn^2 \log^2 q)$	-
our scheme	$O(n^2 \log^2 d)$	$O(n^2 \log(dq) \log d)$	$O(k^3 n^3 \log^2 qd)$	$O(n^2 \log qd \log d)$	-

k, n, q denotes number of parties, LWE dimension, modulus respectively. d is defined in our scheme with $d = q/\mathsf{poly}(\lambda)$. The key and ciphertext are counted in bits. The Hom-multipication column counts the number of multiplications on $\mathbb{Z}_q$ required for a homomorphic multiplication. The Communication in setup column counts the communication traffic required for the interactive key generation phase

Remark : It must be pointed out that we introduce stronger assumptions compared with [16]. Under the semi-malicious adversary, we require the lattice $\Lambda_q(\mathbf{A})$ to contain enough short vectors, and the former has no restriction on $\mathbf{A}$, so the complexity of their scheme is related to k.

1.3 Technic overview :

We note that for a given $\mathbf{y} = \mathbf{sA} + \mathbf{e} \mod q$, $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$, let $\mathbf{s}^*\mathbf{A}$ be the nearest lattice point to $\mathbf{y}$, $\mathbf{e}^*$ be the vector from $\mathbf{s}^*\mathbf{A}$ to $\mathbf{y}$, it holds that events $\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}$ and $\mathbf{e} = \mathbf{e}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}$ are equivalent, where $V \in \mathbb{Z}^m$ be the discrete *Voronoï cell* of $\Lambda_q(\mathbf{A})$. Thus, we have :

$$\Pr(\mathbf{s} = \mathbf{s}^* | \mathbf{y}) = \Pr(\mathbf{e} = \mathbf{e}^* | \mathbf{y}) = \Pr(\mathbf{e} \mod q \in V)$$

Therefore, as $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$, we can quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$ and $\tilde{H}_\infty(\mathbf{e}|\mathbf{sA} + \mathbf{e})$. Based on the above observation, [13] gave a low bound of $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$, which is also the low bound of $\tilde{H}_\infty(\mathbf{e}|\mathbf{sA} + \mathbf{e})$. We quantify it for $\mathbf{s} \leftarrow \chi^n$, $\mathbf{e} \leftarrow \chi^m$ or $\mathbf{s} \leftarrow \mathbb{Z}_d^n (d \leq q)$, $\mathbf{e} \leftarrow \chi^m$.

We first analyze the situation when $\mathbf{s} \leftarrow \chi^n$, $\mathbf{e} \leftarrow \chi^m$. Unlike above, for a given $\mathbf{y}$, we cannot determine the probability of $\mathbf{sA}$ taking $\mathbf{s}^*\mathbf{A}$(The nearest lattice point to $\mathbf{y}$). Therefore, we can not apply the above result directly. However, we observed the reduction process of LWE samples(with discrete Gaussian secrets) to the standard LWE samples(with uniform secrets) in [6]: the noise in the standard LWE samples turn into the secrets in the discrete Gaussian version LWE samples. From the above analysis, we can see that we can quantify the entropy of noise in standard LWE samples. Therefore, combining these two, we can quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$ for $\mathbf{s} \leftarrow \chi^n$, $\mathbf{e} \leftarrow \chi^m$. We point out that this result is not straightforward as it requires some properties of entropy.

Now, we consider the case of $\mathbf{s} \leftarrow \mathbb{Z}_d^n (d \leq q)$, $\mathbf{e} \leftarrow \chi^m$. According to the definition of average conditional Min-entropy:

$$\tilde{H}_\infty(X|E) = -\log(\mathbb{E}[\max_x \Pr[X|E = e]]$$

that is, for a given $\mathbf{y} = \mathbf{sA} + \mathbf{e}$, $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$ is determined by the $\mathbf{s}^*$ that maximizes the conditional probability $\Pr(\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e})$. According to the proof of Lemma 3.2 in [13], $\Pr(\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}) \propto \Pr(\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A})$, that is, $\Pr(\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e})$ gets the maximum, if and only if $\mathbf{s}^*\mathbf{A}$ is the lattice point closest to $\mathbf{y}$, that is, the error term $\mathbf{e}$ must fall in the *Voronoï cell* V. But when $\mathbf{s}$ is limited to a small range, the above conclusion does not necessarily hold. Let $d < q$ be an integer :

$$S = \{\mathbf{x} \in \mathbb{Z}^m, \mathbf{x} = \mathbf{sA} \mod q, \mathbf{s} \in \mathbb{Z}_d^n\}$$

obviously, S is a subset of q-ary lattice $\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m, \mathbf{x} = \mathbf{sA} \mod q, \mathbf{s} \in \mathbb{Z}_q^n\}$ (not necessarily a sub-lattice, it may not be closed). For any given $\mathbf{y} = \mathbf{sA} + \mathbf{e}$, where $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m, \sigma}$, by Bayes Rule, it holds that $\Pr(\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}) \propto \Pr(\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A})$. Now, we need to find a lattice point on S that is closest to $\mathbf{y}$. There are two possible cases :

– The nearest lattice point to $\mathbf{y}$ on S is the same as the nearest lattice point to $\mathbf{y}$ on the $\Lambda_q(\mathbf{A})$.
– These two points are different

As shown in Figure1, we interpret it in a two-dimensional lattice.

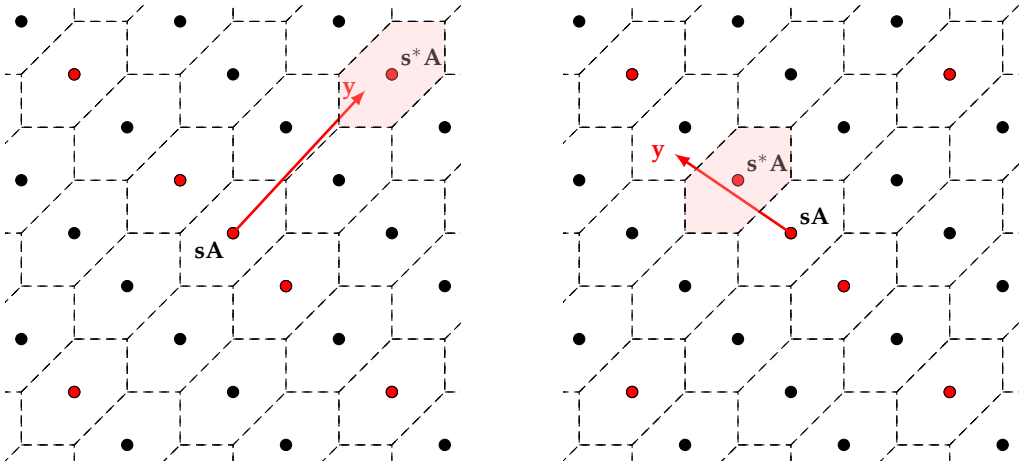

Fig. 1: Cases of the nearest point to $\mathbf{y}$: Red points are in S. The left panel shows that the closest point to $\mathbf{y}$ is on S, but the right panel shows that the closest point to $\mathbf{y}$ is clearly not on S

Obviously, in the second case, $\mathbf{y}$ falls outside the *Voronoï cell* of $\mathbf{s}^*\mathbf{A}$, $\mathbf{e} \notin V$. Therefore, we cannot use Lemma3.2 in [13] to get the $\tilde{H}_\infty(\mathbf{sA}+\mathbf{e} \mod q)$ low bound. The point is that $\mathbf{sA} \mod q$ doesn't necessarily traverse all the lattice points when limiting $\mathbf{s}$ to a small range. If $\forall \mathbf{s} \in \mathbb{Z}_d^n$, $S = \{\mathbf{x} \in \mathbb{Z}^m, \mathbf{x} = \mathbf{sA} \mod q, \mathbf{s} \in \mathbb{Z}_d^n\}$ be a lattice, then a similar conclusion can be obtained from Lemma3.2.

We found that as $\mathbf{A} \in \frac{q}{d}\mathbb{Z}^{n\times m}$, $\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \frac{q}{d}\mathbb{Z}^m, \mathbf{x} = \mathbf{sA} \mod q, \mathbf{s} \in \mathbb{Z}_d^n\}$ also be a lattice, similar to $\Lambda_q(\mathbf{A}')(\mathbf{A}' \in \mathbb{Z}^{n\times m})$ being a q-ary lattice defined over $\mathbb{Z}^m$, $\Lambda_q(\mathbf{A})$ being an d-ary lattice defined over $\frac{q}{d}\mathbb{Z}^m$. Therefore, for such lattice $\Lambda_q(\mathbf{A})$, when $\mathbf{s} \leftarrow \mathbb{Z}_d^n(d \le q)$, $\mathbf{e} \leftarrow \chi^m$, we can still quantify $\tilde{H}_\infty(\mathbf{sA}+\mathbf{e} \mod q)$.

The improvement on MKFHE scheme [16] requires us to show that $\mathbf{sA}+\mathbf{e}$ is still pseudorandom when $\mathbf{s}$ is lossy, where $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, $\mathbf{A} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times m}$, $\mathbf{e} \leftarrow \mathcal{D}_{\frac{q}{d}\mathbb{Z}^m,\sigma}$. Here, we borrow the proof techniques in [30] from binary LWE samples to low-dimensional standard LWE samples. Let $\mathbf{A} = \mathbf{BC}+\mathbf{E}$, where $\mathbf{B} \leftarrow \frac{q}{d}\mathbb{Z}^{n\times l}$, $\mathbf{C} \leftarrow \mathbb{Z}_d^{l\times m}$, $\mathbf{E} \leftarrow \mathcal{D}^{n\times m}_{\frac{q}{d}\mathbb{Z},\sigma'}$, it holds that :

$$\mathbf{sA}+\mathbf{e} = \mathbf{s}(\mathbf{BC}+\mathbf{E})+\mathbf{e} = \mathbf{sBC}+\mathbf{sE}+\mathbf{e}$$

By the Leftover hash lemma, as long as it is shown that the hash function determined by $\mathbf{B}$ is universal and $\mathbf{s}$ has sufficient conditional entropy, then it holds that $(\mathbf{B}, \mathbf{sB}) \approx (\mathbf{B}, \mathbf{u})$. In general, when $\mathbf{s} \in \{0,1\}^n$, for a uniformly selected $\mathbf{B}$ from $G^{n\times l}$(G is a general finite Abelian group), the hash function determined by it is usually *universal*. However, when $\mathbf{s} \in \mathbb{Z}_d^n$, the regularity of the hash function mapped to the general finite Abelian group cannot be guaranteed(there is a zero divisor). However, when G is isomorphic to the prime order group, the above hash functions are also *universal*.

Let $\mathbf{t} = \mathbf{sB}$, then $\mathbf{sA}+\mathbf{e} = \mathbf{tC}+\mathbf{sE}+\mathbf{e}$, where $\mathbf{tC}+\mathbf{e}$ are l dimension LWE sample. We can consider $\mathbf{tC}+\mathbf{sE}+\mathbf{e}$ as the ciphertext of the dual-Regev encryption scheme, where the public key, private key and plaintext are $(\mathbf{B}, \mathbf{t})$, $\mathbf{s}$, $\mathbf{sE}$ respectively, that is, the encrypted data is related to the private key. If it is assumed that the dual-Regev encryption scheme is *Circular Security*, then $\mathbf{tC}+\mathbf{sE}+\mathbf{e}$ should be computationally indistinguishable from the uniform distribution(The *Circular Security* should be a widely accepted assumption, which is used in FHE and key switch). Therefore, we can still use the GSW type to construct MKFHE, which is similar to [16], but the encoding of the plaintext is different. Note that our ciphertext $\mathbf{C} \in \frac{q}{d}\mathbb{Z}_d^{n\times m}$. We introduce the encoding and correctness of homomorphic evaluation in Section6.3.

1.4 Related works

The work of Brakerski and Döttling [14] on the hardness of LWE on general entropic distributions was dedicated to proving the hardness of entropy LWE: for a key distribution $\mathcal{S}$ with support over $\mathbb{Z}^n$, assuming that $\tilde{H}_\infty(\mathbf{s}|\mathbf{s}+\mathbf{e})$ is large enough, then the entropy LWE is hard (equivalent to the generalization of Goldwasser et al's work [27], which proved that when the key $\mathbf{s}$ is taken from $\{0,1\}$, and $\tilde{H}_\infty(\mathbf{s})$ is large enough, the binary LWE is anti-leakage). We must point out that our work is dedicated to characterizing the lower bound of $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$, where $\mathbf{A}$ may not be uniformly distributed. This kind of leakage model (we call it the "active leakage" model in our work) appears more in multi-party cooperation protocols, such as oblivious transfer, or MKFHE. The leakage model of $\tilde{H}_\infty(\mathbf{s}|\mathbf{s}+\mathbf{e})$ is more in line with the side channel attack (in our work, it becomes passive leakage).

Therefore, we believe that these two works should be complementary. Their research focuses on the hardness of entropy LWE, and consider how to quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{s}+\mathbf{e})$, which provides more confidence for anti-leakage cryptography. However, our work focuses on the characterization of the active leakage of $\mathbf{s}|\mathbf{sA}+\mathbf{e}$(there should be no side channel to obtain $\mathbf{s}$ by $\mathbf{sA}+\mathbf{e}$), which provides a tool for further weakening the setup (without CRS, trusted third party) in the MPC and MKFHE.

2 Preliminaries

2.1 Notation:

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 row vectors by default, and matrices are represented by uppercase bold letters such as $\mathbf{M}$. Let k be an integer, $[k]$ be the set of integers $\{1,\cdots,k\}$. If X is a distribution, then $a \leftarrow X$ denotes that value a is chosen according to the distribution X, or a finite set, then $a \leftarrow X$ denotes that the value of a is uniformly sampled from X. For two distribution X, Y, we use $X \approx_s Y$ to represent X and Y are statistically indistinguishable, where $X \approx_c Y$ are computationally indistinguishable.

Gadget decomposition over $\mathbb{Z}+\frac{1}{d}\mathbb{Z}$: In order to decompose elements in $\mathbb{Z}_q$ into binary, we review the Gadget matrix [34] [2] 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 $\mathbf{G}\mathbf{G}^{-1}(\mathbf{M}) = \mathbf{M}$.

Now, we consider decomposing the elements on $\mathbb{Z}_q+\frac{1}{d}\mathbb{Z}_d$ into binary. Let $\mathbf{g} = (2^{l_1-1}, 2^{l_1-2}, \cdots, 1, \frac{1}{d}, \frac{2}{d}, \cdots, \frac{2^{l_2-1}}{d})$ where $l_1 = \lceil \log q \rceil$, $l_2 = \lceil \log d \rceil$. For any $a \in \mathbb{Z}_q+\frac{1}{d}\mathbb{Z}_d$, let $a = a_0 + \frac{a_1}{d}(a_0 \in \mathbb{Z}_q, a_1 \in \mathbb{Z}_d)$, define $\mathbf{g}^{-1}(a) = \{0,1\}^{l_1+l_2}$ be the decomposition of a_0 and a_1. It holds that for any $a \in \mathbb{Z}_q+\frac{1}{d}\mathbb{Z}_d$, $\mathbf{g}\cdot\mathbf{g}^{-1}(a) = a$. Further, for $\mathbf{M} \in (\mathbb{Z}_q+\frac{1}{d}\mathbb{Z}_d)^{m\times n}$, let $\mathbf{G} = \mathbf{I}_m \otimes \mathbf{g}$, it holds that $\mathbf{G}^{-1}(\mathbf{M}) \in \{0,1\}^{m(l_1+l_2)\times n}$, $\mathbf{G}\mathbf{G}^{-1}(\mathbf{M}) = \mathbf{M}$.

2.2 Some background in probability

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

Average Conditional Min-Entropy(in [13]) 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 :

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

2.3 Universal hash function and Leftover hash lemma

The content of this subsection is mainly derived from [39] and [40]

Definition 2 *Let the seed U_d be uniformly distributed on $\{0,1\}^d$. We say that a function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k,ϵ)(strong) extractor if, for all random variables X on $\{0,1\}^n$ independent of U_d with $\tilde{H}_\infty(X) \geq k$,*

$$(\mathsf{Ext}(X, U_d), U_d) \approx)_\epsilon (U_m, U_d)$$

where U_m is uniformly distributed on $\{0,1\}^m$ independent of X and U_d.

Definition 3 *A keyed hash function or, equivalently, a family $\mathcal{H}$ of hash functions of size 2^d from $\{0,1\}^n$ to $\{0,1\}^m$ is called universal if, for every $x, y \in \{0,1\}^n$ with $x \neq y$,*

$$\Pr_{h\in\mathcal{H}}[h(x) = h(y)] \leq 2^{-m}$$

Theorem 3 ((Leftover Hash Lemma(LHL) [30])) *Let X be a random variable with universe U and $H_\infty(X) \geq k$. Fix $\epsilon > 0$. Let $\mathcal{H}$ be the universe hash family of size 2^d with output length $m = k - 2\log(\frac{1}{\epsilon})$. Define*

$$Ext(x, h) = h(x).$$

Then Ext is a strong $(k, \frac{\epsilon}{2})$ extractor with seed length d and output length m.

The leftover hash lemma simply states that a universal hash family gives an extractor. The seed is used to choose a hash function, and the output is simply the hash of the input. In the above theorem, $m = k - \log(\frac{1}{\epsilon})$ can be understood as the min-entropy in the output of this extractor decreasing from k to m. Xagawa [41] gives the following more easily applicable version

Lemma 2 (Lemma 4.2.3 in [41]) *Let $\mathcal{H}_k = \{h_k : k \in K\}$ be a universal hash function defined over finite set K, D, T :*

$$\begin{aligned} h_k \quad : \quad & D \to T \\ & x \mapsto h_k(x) \end{aligned}$$

where x is a random variable defined over D and independent from k. It holds that :

$$\Delta((U, h_k(x)), (U, V)) \leq 2^{-\frac{1}{2}(\tilde{H}_\infty(x) - \log|T| + 2)}$$

where U and V are uniform random variable defined over K and T.

The following lemma shows the regularity of the hash function mapping from $\{0,1\}^m$ to general finite Abelian group G:

Lemma 3 ([38], Claim 5.3) *Let G be a finite Abelian group, $Q = |G|$, m be integers. For any $g_1, \cdots, g_m \in G$, consider $\Delta(\sum_{i\in[m]} b_i g_i, u)$, where $b_i \leftarrow \{0,1\}$, $u \leftarrow G$. For uniformly chosen $g_1, \cdots, g_m \in G$, the statistical distance expectation is at most $(Q/2^m)^{\frac{1}{2}}$. In particular, the probability that the statistical distance exceeds $(Q/2^m)^{\frac{1}{4}}$ does not exceed $(Q/2^m)^{\frac{1}{4}}$.*

2.4 Some result on the lattice

Theorem 4 *Let Λ be a lattice, V be the Voronoï-cell of Λ, $\mathbf{t}, \mathbf{t}'$ are two vectors in $span(\Lambda)$, then the following three statements are equivalent:*

1. *$\mathbf{t}$ is the shortest vector in $\mathbf{t} + \Lambda$*
2. *$\mathbf{t} \in (\mathbf{t} + \Lambda) \bigcap V$*
3. *$\mathbf{v} = \mathbf{t} - \mathbf{t}' \in \Lambda$ is the nearest lattice point to $\mathbf{t}$.*

Definition 4 *Let $\rho_\sigma(\mathbf{x}) = \exp(-\pi||\mathbf{x}/\sigma||^2)$ be a Gaussian function scaled by a factor of $\sigma > 0$. Let $\Lambda \subset \mathbb{R}^m$ be a lattice, and $\mathbf{c} \in \mathbb{R}^m$. The discrete Gaussian distribution $D_{\Lambda+\mathbf{c},\sigma}$ with support $\Lambda + \mathbf{c}$ is defined as :*

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

Lemma 4 (in [13]) *Let $\Lambda \subseteq \Lambda_0 \subseteq \mathbb{R}^m$ be full rank lattices and let $T \subseteq \Lambda_0$ be a system of coset representatives of Λ_0/Λ, i,e. we can write every $\mathbf{x} \in \Lambda_0$ as $\mathbf{x} = \mathbf{t} + \mathbf{z}$ for unique $\mathbf{t} \in \Lambda$. Then it holds for any parameter $\sigma > 0$ that*

$$\frac{\rho_\sigma(T)}{\rho_\sigma(\Lambda_0)} \leq \frac{1}{\rho_\sigma(\Lambda)}.$$

Lemma 5 (in [11]) *Let $\Lambda \in \mathbb{R}^m$, $\sigma > 0$ and $\gamma > 0$ be such that $\Lambda \bigcap \gamma\mathcal{B}$ contains at least k linearly independent vectors. Then it holds that $\rho_\sigma(\Lambda) \geq (\sigma/\gamma)^k$.*

Theorem 5 (in [11]) *For any lattice $\Lambda \in \mathbb{R}^m$, parameter $\sigma > 0$ and $u \geq \frac{1}{\sqrt{2\pi}}$ it holds that*

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

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

Setting $\Lambda = \mathbb{Z}^m$ and $u = 1$ in Theorem 5, we obtain the following corollary.

Corollary 1 *Let $\sigma > 0$ and $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$. Then it holds that $||\mathbf{x}|| \leq \sigma \cdot \sqrt{m}$, except with probability 2^{-m}.*

2.5 Learning with Errors

The Learning With Errors(LWE) problem was introduced by Regev [38]. In general, we are primarily interested in its decision version.

Definition 5 (Decision-LWE) *For $n, m, q \in \mathbb{N}$ and for a distribution χ supported over $\mathbb{Z}$, the $DLWE_{n,m,q,\chi}$ is to distinguish the following distribution :*

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

It is often considered the hardness of solving $\mathsf{DLWE}_{n,m,q,\chi}$ for any $m = \mathsf{poly}(n \log q)$. The matrix version of this problem ask to distinguish $(\mathbf{A}, \mathbf{SA} + \mathbf{E})$ from $(\mathbf{A}, \mathbf{U})$ where $\mathbf{S} \leftarrow \mathbb{Z}_q^{k\times m}$, $\mathbf{E} \leftarrow \chi^{k\times m}$ and $\mathbf{U} \leftarrow \mathbb{Z}_q^{k\times m}$, whose hardness for any $k = \mathsf{poly}(n)$ can be established from $\mathsf{DLWE}_{n,m,q,\chi}$ via a routine hybrid-argument.

As shown in Regev [38], for certain module q and discrete Gaussian error distribution χ with parameter $\sigma = \alpha q \geq 2\sqrt{n}$, the $\mathsf{DLWE}_{n,m,q,\chi}$ is true as long as certain worst-case lattice problem is hard to solve using a quantum algorithm.

2.6 Road-map

In section3, we proved a more general result for $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$. In section4, we proved the regularity of the hash function defined on the prime order group and its Cartesian product. This result will be used in the security proof of our scheme. In section5, we proved the leakage-resilient property of LWE defined on $\frac{q}{d}\mathbb{Z}$. In section6, we gave our improved MKFHE scheme.

3 Lattice-based, more general anti-leakage model

In Section3.1, we first quantify the anti-leakage properties of LWE whose secrets are drawn from discrete Gaussian. However, when the secrets are uniform in a small range, the situation is different. In Section3.2, We describe a lattice contained on $\frac{q}{d}\mathbb{Z}^m$, then in Section3.3, we prove the anti-leakage property of the LWE samples on this lattice.

3.1 Anti-leakage properties of discrete Gaussian version of LWE samples

When $\mathbf{s}$ is taken from a discrete Gaussian distribution, we cannot directly apply the proof method in [13]. At this time, we need to use the reduction technique [6] from LWE (with discrete Gaussian secrets) to LWE (with uniform secrets).

Consider the following game :

- Alice picks a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and sends it to Bob.
- After receiving $\mathbf{A}$, Bob generates n standard LWE samples $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \mathbf{s}\bar{\mathbf{A}}, +\bar{\mathbf{e}})$, where $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\bar{\mathbf{e}} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$. Let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e}, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$, and send $(\mathbf{A}', \mathbf{b}, \bar{\mathbf{b}})$ to Alice.
- After receiving $(\mathbf{A}', \mathbf{b}, \bar{\mathbf{b}})$, Alice computes $(\mathbf{A}', \mathbf{b}' = \mathbf{b} + \bar{\mathbf{b}}\mathbf{A}')$.

The above game is essentially the reduction from discrete Gaussian LWE to standard LWE. Apparently $(\mathbf{A}', \mathbf{b}' = \bar{\mathbf{e}}\mathbf{A}' + \mathbf{e})$ are the LWE samples with discrete Gaussian secrets, but $\mathbf{A}'$ may not be uniform, because $\mathbf{A}$ is chosen by Alice. Now, we quantify $\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e})$.

Theorem 1. *For a given matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ with $m = O(n \log q)$, and $0 < \sigma < \frac{q}{2\sqrt{m+n}}$. Let $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \mathbf{s}\bar{\mathbf{A}} + \bar{\mathbf{e}})$, where $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\bar{\mathbf{e}} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$ be n LWE samples. Let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A})$, $\mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e}$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$. It holds that :*

$$\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \geq -\log\left(\frac{1}{\rho_\sigma(\Lambda_q(\tilde{\mathbf{A}})} + 2^{-(m+n)}\right)$$

Proof. Let $\tilde{\mathbf{e}} = (\bar{\mathbf{e}}, \mathbf{e})$, $\tilde{\mathbf{b}} = (\bar{\mathbf{b}}, \mathbf{b})$. According to the definition of average min-entropy, we have

$$\tilde{H}_\infty(\tilde{\mathbf{e}}|\tilde{\mathbf{b}}) = \tilde{H}_\infty(\tilde{\mathbf{e}}|\tilde{\mathbf{b}} = \mathbf{s}\tilde{\mathbf{A}} + \tilde{\mathbf{e}}) = -\log\left(\mathsf{E}_{\tilde{\mathbf{b}}}\left[\max_{\tilde{\mathbf{e}}^*} \Pr_{\mathbf{s},\tilde{\mathbf{e}}}[\tilde{\mathbf{e}} = \tilde{\mathbf{e}}^*|\tilde{\mathbf{b}} = \mathbf{s}\tilde{\mathbf{A}} + \tilde{\mathbf{e}}]\right]\right)$$

Obviously, $\tilde{\mathbf{e}}$ that maximizes the conditional probability $\Pr[\tilde{\mathbf{e}} = \tilde{\mathbf{e}}^*|\tilde{\mathbf{b}} = \mathbf{s}\tilde{\mathbf{A}} + \tilde{\mathbf{e}}]$ must fall in the *Voronoï cell* of the lattice point that nearest to $\tilde{\mathbf{b}}$, that is, $\tilde{\mathbf{e}}^* = \tilde{\mathbf{b}} - \mathbf{s}^*\tilde{\mathbf{A}}$($\mathbf{s}^*\tilde{\mathbf{A}}$ is the nearest lattice point to $\tilde{\mathbf{b}}$). By Theorem4, it holds that $\Pr[\tilde{\mathbf{e}} = \tilde{\mathbf{e}}^*|\tilde{\mathbf{b}} = \mathbf{s}\tilde{\mathbf{A}} + \tilde{\mathbf{e}}] = \Pr[\tilde{\mathbf{e}} \mod q \in V]$, where $V \in \mathbb{Z}^{m+n}$ is the discretized *Voronoï cell* of $\Lambda_q(\tilde{\mathbf{A}})$. By Theorem5, it holds that $||\tilde{\mathbf{e}}|| \leq \sigma \cdot \sqrt{m+n} < q/2$ except with probability $2^{-(m+n)}$, thus $\Pr[\tilde{\mathbf{e}} \mod q \in V] \leq \Pr[\tilde{\mathbf{e}} \in V] + 2^{-(m+n)}$. By Lemma4, it holds that $\Pr[\tilde{\mathbf{e}} \in V] \leq \frac{\rho_\sigma(V)}{\rho_\sigma(\mathbb{Z}^{(m+n)})} \leq \frac{1}{\rho_\sigma(\Lambda_q(\tilde{\mathbf{A}}))}$, therefore, $\Pr[\tilde{\mathbf{e}} \mod q \in V] \leq \frac{1}{\rho_\sigma(\Lambda_q(\tilde{\mathbf{A}}))} + 2^{-(m+n)}$. We have :

$$\begin{aligned}
\tilde{H}_\infty(\tilde{\mathbf{e}}|\tilde{\mathbf{b}}) &= -\log\left(\mathsf{E}_{\tilde{\mathbf{b}}}\left[\Pr[\tilde{\mathbf{e}} \mod q \in V]\right]\right) \\
&= -\log\left(\Pr[\tilde{\mathbf{e}} \mod q \in V]\right) \\
&\geq -\log\left(\frac{1}{\rho_\sigma(\Lambda_q(\tilde{\mathbf{A}}))} + 2^{-(m+n)}\right) \qquad (1)
\end{aligned}$$

According to the chain rule of entropy : $H(X, Y) = H(X) + H(Y|X)$, we have :

$$\tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}, \bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) - \tilde{H}_\infty(\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \qquad (2)$$

And because $\tilde{H}_\infty(\mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}, \bar{\mathbf{e}}) = 0$, then by the chain rule, we have :

$$\tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}, \bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}}, \bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \qquad (3)$$

Combining (2), (3) we have :

$$\tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}}, \bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) - \tilde{H}_\infty(\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \qquad (4)$$

Because $\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e} = \mathbf{b} + \bar{\mathbf{b}}\mathbf{A}'$, we have :

$$\tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \geq \tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}|\tilde{\mathbf{b}}) \qquad (5)$$

Combining (1), (4), (5) we have :

$$\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) = \tilde{H}_\infty(\bar{\mathbf{e}}, \mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \geq -\log\left(\frac{1}{\rho_\sigma(\Lambda_q(\tilde{\mathbf{A}})} + 2^{-(m+n)}\right)$$

■

3.2 Lattice over $\frac{q}{d}\mathbb{Z}^m$

Let $d, q \in \mathbb{Z}$ and $d \leq q$, $\mathbf{A} \in \frac{q}{d}\mathbb{Z}^{n\times m}$, $\mathbf{s} \in \mathbb{Z}_d^n$. Let [3]

$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \frac{q}{d}\mathbb{Z}^m : \mathbf{x} = \mathbf{sA} \mod q, \mathbf{s} \leftarrow \mathbb{Z}_d^n\}$$

It is easy to verify that $\Lambda_q(\mathbf{A})$ forms a lattice, for any $\mathbf{x}_1, \mathbf{x}_2 \in \Lambda_q(\mathbf{A})$, let $\mathbf{x}_1 = \mathbf{s}_1\mathbf{A} \mod q$, $\mathbf{x}_2 = \mathbf{s}_2\mathbf{A} \mod q$, there exist $\mathbf{x}_3 \in \Lambda_q(\mathbf{A})$ satisfying $\mathbf{x}_3 = \mathbf{x}_1 + \mathbf{x}_2 \mod q$, where $\mathbf{x}_3 = \mathbf{s}_3\mathbf{A} \mod q$, $\mathbf{s}_3 = \mathbf{s}_1 + \mathbf{s}_2 \mod d$. That is, $\Lambda_q(\mathbf{A})$ is closed under addition modulo q, and is a discrete additive subgroup of $\frac{q}{d}\mathbb{Z}^m$.

For those who are more familiar with lattice, it may be seen at a glance that $\Lambda_q(\mathbf{A})$ is isomorphic to the d-ary lattice (obtained by stretching d-ary lattice by a factor $\frac{q}{d}$). Such as for any $\mathbf{A} \in \frac{q}{d}\mathbb{Z}^{n\times m}$, let $\mathbf{A} = \frac{q}{d}\mathbf{A}'$, where $\mathbf{A}' \in \mathbb{Z}^{n\times m}$, there is a bijection ϕ between $\Lambda_d(\mathbf{A}') = \{\mathbf{x}' \in \mathbb{Z}^m : \mathbf{x}' = \mathbf{sA}' \mod d, \mathbf{s} \leftarrow \mathbb{Z}_d^n\}$ and $\Lambda_q(\mathbf{A})$: for any $\mathbf{x}' \in \Lambda_d(\mathbf{A}')$, let $\mathbf{x}' = \mathbf{v} + d \cdot \mathbf{c}$, where $\mathbf{v} \in \mathbb{Z}_d^m$, $\mathbf{c} \in \mathbb{Z}^m$, its image in $\Lambda_q(\mathbf{A})$ is $\mathbf{x} = \frac{q}{d}\mathbf{v} + q \cdot \mathbf{c}$.

$$\begin{aligned} \phi \quad : \quad & \Lambda_d(\mathbf{A}') \to \Lambda_q(\mathbf{A}) \\ & \mathbf{v} + d \cdot \mathbf{c} \mapsto \frac{q}{d} \cdot \mathbf{v} + q \cdot \mathbf{c}. \end{aligned}$$

3.3 Lossy model for d-ary lattices

Theorem 2. *Let d, q, $0 < d \leq q$ be integers. Fix a matrix $\mathbf{A} \in \frac{q}{d}\mathbb{Z}^{n\times m}$ with $m = O(n \log d)$, and a parameter $0 \leq \sigma \leq \frac{d}{2\sqrt{m}}$. Let $\mathbf{s} \leftarrow \mathbb{Z}_d^n$ and $\mathbf{e} \leftarrow \mathcal{D}_{\frac{q}{d}\mathbb{Z}^m,\sigma}$, Then it holds that :*

$$\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e} \mod q) \geq -\log(\frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))} + 2^{-m})$$

If $d = q$, the above theorem degenerates into Lemma 3.2 in [13]. Its proof is the same as [13]; for the sake of completeness, we list it here.

Proof. For a given $\mathbf{A} \in \frac{q}{d}\mathbb{Z}_d^{n\times m}$ and $\mathbf{y} \in \frac{q}{d}\mathbb{Z}_d^m$, let $\mathbf{s}^*$ be the point that maximizes the conditional probability $\Pr_{\mathbf{s}\leftarrow\mathbb{Z}_d^n}[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}]$. By Bayes Rule, it holds that :

$$\begin{aligned} &\Pr_{\mathbf{s}\leftarrow\mathbb{Z}_d^n}[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}] = \Pr[\mathbf{y} = \mathbf{sA} + \mathbf{e} \mid \mathbf{s}^*] \cdot \frac{\Pr[\mathbf{s} = \mathbf{s}^*]}{\Pr[\mathbf{y} = \mathbf{sA} + \mathbf{e}]} \\ &= \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A}] \cdot \frac{\Pr[\mathbf{s} = \mathbf{s}^*]}{\sum_{\mathbf{s}'} \Pr[\mathbf{y} = \mathbf{sA} + \mathbf{e} \mid \mathbf{s} = \mathbf{s}'] \Pr[\mathbf{s} = \mathbf{s}']} \\ &= \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A}] \frac{d^{-n}}{\sum_{\mathbf{s}'} \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A}] \cdot d^{-n}} \\ &= \frac{\Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A}]}{\sum_{\mathbf{s}'} \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}'\mathbf{A}]} \end{aligned}$$

For the given $\mathbf{A}$, $\mathbf{y}$, $\sum_{\mathbf{s}'} \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}'\mathbf{A}]$ is a constant, it holds that $\Pr[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}] \propto \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A}]$, thus the point maximizes $\Pr[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}]$ is the lattice point nearest to $\mathbf{y}$. Let $V \in \frac{q}{d}\mathbb{Z}^m$ be the *discretized Voronoï cell* of $\Lambda_q(\mathbf{A})$, that is V consists of all point in $\frac{q}{d}\mathbb{Z}^m$ that are closer to 0 than to any other point in Λ. By construction, V is a system of coset representatives of $\frac{q}{d}\mathbb{Z}^m \backslash \Lambda_q(\mathbf{A})$.

By Theorem4, it holds that $\Pr[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}] = \Pr[\mathbf{e} \mod q \in V]$. By Theorem5, it holds that $||\mathbf{e}|| \leq \frac{q}{d} \cdot \sigma \cdot \sqrt{m} < q/2$ except with probability 2^{-m}, thus $\Pr[\mathbf{e} \mod q \in V] \leq \Pr[\mathbf{e} \in$

[3] JC: Here the definition of mod has been extended to take the remainder of a rational number to an integer

$V] + 2^{-m}$. By Lemma4, it holds that $\Pr[\mathbf{e} \in V] \leq \frac{\rho_\sigma(V)}{\rho_\sigma(\frac{q}{d}\mathbb{Z}^m)} \leq \frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))}$, therefore, $\Pr[\mathbf{e} \mod q \in V] \leq \frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))} + 2^{-m}$, thus :

$$\begin{aligned}\tilde{H}_\infty(\mathbf{s} \mid \mathbf{sA}+\mathbf{e}) &= -\log\left(\mathrm{E}_{\mathbf{y}}\left[\max_{\mathbf{s}^*}\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s}=\mathbf{s}^* \mid \mathbf{y}=\mathbf{sA}+\mathbf{e}]\right]\right)\\ &= -\log\left(\mathrm{E}_{\mathbf{y}}[\Pr[\mathbf{e} \bmod q \in V]]\right)\\ &= -\log(\Pr[\mathbf{e} \bmod q \in V])\\ &\geq -\log\left(\frac{1}{\rho_\sigma\left(\Lambda_q(\mathbf{A})\right)} + 2^{-m}\right)\end{aligned}$$

■

4 Regularity of Hash Functions on Prime Order Groups and Their Cartesian Products

The work([38], Claim 5.3)proved that hash function family $\{\mathcal{H}_G = h_{\mathbf{g}} : \mathbf{g} \in G^m\}$ is universal, where :

$$\begin{aligned} h_{\mathbf{g}} \quad : \quad \{0,1\}^m \quad &\to \quad G \\ \mathbf{b} \quad &\mapsto \quad \sum_{i\in m} b_i g_i \end{aligned}$$

The above result requires that the preimage of $h_{\mathbf{g}}$ is taken from $\mathbb{Z}_2$, and G only needs to be a finite Abelian group. Here we relax the preimage of $h_{\mathbf{g}}$ and take it from $\mathbb{Z}_d$, where $d < q$ is an integer, but the order of the finite Abelian group G must be prime. We prove that the following hash function family is universal $\mathcal{H}_G = \{h_{\mathbf{g}} : \mathbf{g} \in G^m\}$

$$\begin{aligned} h_{\mathbf{g}} \quad : \quad \mathbb{Z}_d^m \quad &\to \quad G \\ \mathbf{b} \quad &\mapsto \quad \sum_{i\in[m]} b_i g_i \end{aligned}$$

Below we prove lemma6 and then extend to its Cartesian products.

Lemma 6 *Let G be a finite Abelian group with $|G| = q$ as a prime, m, d as integers, and $d \leq q$. For uniformly chosen $g_1, \cdots, g_m \in G$, $b_i \leftarrow \mathbb{Z}_d$, $u \leftarrow G$, the statistical distance $\Delta(\sum_{i\in[m]} b_i g_i, u)$ is expected to be at most $\frac{1}{2}\sqrt{\frac{q}{d^m}}$, in particular, the probability that the statistical distance exceeds $(\frac{q}{d^m})^{\frac{1}{4}}$ does not exceed $(\frac{q}{d^m})^{\frac{1}{4}}$*

Proof. As G is a finite Abelian group, it holds that for $\mathbf{b}, \mathbf{b}' \in \mathbb{Z}_d^m$, and $\mathbf{b} \neq \mathbf{b}'$, we have :

$$\Pr_{\mathbf{g}\leftarrow G^m}\left[\sum_i^m b_i g_i = \sum_{i=1}^m b'_i g_i \middle| \mathbf{b} \neq \mathbf{b}'\right] = \Pr_{\mathbf{g}\leftarrow G^m}\left[\sum_{i=1}^m (b_i - b'_i) g_i = 0 \middle| \mathbf{b} \neq \mathbf{b}'\right] \tag{6}$$

The above probability can be determined by counting the fixed $\mathbf{b}$ and $\mathbf{b}'$. When only the i-th element of $\mathbf{b} - \mathbf{b}'$ is non-zero, $b_i - b'_i \neq 0$, we have $\sum_{i=1}^m (b_i - b'_i) g_i = (b_i - b'_i) g_i = 0$. Because G is a finitely generated Abelian group and has prime order q, then G and $\mathbb{Z}_q$ are isomorphic. For any $b_i, b'_i \in \mathbb{Z}_d$, and $b_i - b'_i \neq 0$, there is $b_i - b'_i \in [-(d-1),\ d-1]/0$. Therefore, for $(b_i - b'_i) g_i = 0$, we have $g_i = 0$, and the remaining $m-1$ positions can be chosen randomly on G, thus $(6) = q^{m-1}/q^m = 1/q$.

When only the i-th and j-th elements of $\mathbf{b} - \mathbf{b}'$ are non-zero, we have $(b_i - b'_i) g_i + (b_j - b'_j) g_j = 0$, then $g_i = -(b_i - b'_i)^{-1}(b_j - b'_j) g_j$, where $(b_i - b'_i)^{-1}$ is the inverse of $b_i - b'_i$ on $b_i - b'_i$. For a given g_j, g_i is uniquely determined, and the remaining $m-2$ positions can be arbitrarily selected on G,

thus, (6) $= q^{m-2}q/q^m = 1/q$. Generally, when only k elements of $\mathbf{b} - \mathbf{b}'$ are non-zero, it can be derived from the linear relationship :

$$g_i = -(b_i - b_i')^{-1} \sum_{j \in [k]/i} (b_j - b_j')g_j$$

it holds that :

$$\Pr_{\mathbf{g} \leftarrow G^m}\left[\sum_i^m b_i g_i = \sum_{i=1} b_i' g_i \middle| \mathbf{b} \neq \mathbf{b}'\right] = \frac{q^{m-k}q^{k-1}}{q^m} = 1/q$$

Therefore, the family of hash functions $\mathcal{H}_G = \{h_{\mathbf{g}} : \mathbf{g} \in G^m\}$ defined above are universal. In particular, with $\mathbf{b} \leftarrow \mathbb{Z}_d^m$, the probability of collision is $1/d^m$, so the min-entropy is $m \log d$, the output of this hash function is $\log q$ bits, and $\epsilon = 2^{\frac{1}{2}(\log q - m \log d)}$. By the leftover hash lemma2, it holds that :

$$\Delta((\mathbf{g}, \sum_i b_i g_i), (\mathbf{g}, u)) \leq \frac{1}{2}\epsilon \leq \sqrt{\frac{q}{d^m}}$$

where $u \leftarrow G$.

The following estimate of the statistical distance expectation is similar to Lemma 4.3.3 in [41]. For any $\mathbf{g} = (g_1, \cdots, g_m) \in G^m$ define

$$P_{\mathbf{g}}(h) = \frac{1}{d^m}\left|\left\{\mathbf{b} \in \mathbb{Z}_d^m : \sum_{i=1}^m b_i g_i = h\right\}\right|$$

For a fixed $\mathbf{g} \in G^m$, define the collision boundary, that is, the l_2-norm of the function $P_{\mathbf{g}}$ on $\mathbb{R}^q$:

$$\begin{aligned}\sum_{h \in G} P_{\mathbf{g}}(h)^2 &= \Pr_{\mathbf{b}, \mathbf{b}' \leftarrow \mathbb{Z}_d^m}\left[\sum_{i=1}^m b_i g_i = \sum_{i=1}^m b_i' g_i\right] \\ &\leq \frac{1}{d^m} + \Pr_{\mathbf{b}, \mathbf{b}' \leftarrow \mathbb{Z}_d^m}\left[\sum_{i=1}^m b_i g_i = \sum_{i=1}^m b_i' g_i \middle| \mathbf{b} \neq \mathbf{b}'\right].\end{aligned}$$

Thus for random variable $\mathbf{g}$, it hold that :

$$\mathsf{Exp}_{\mathbf{g} \leftarrow G^m}\left[\sum_{h \in G} P_{\mathbf{g}}(h)^2\right] \in \frac{1}{d^m} \pm \frac{1}{q}$$

For any $\mathbf{x} \in \mathbb{R}^q$, it holds that $||\mathbf{x}||_\infty \leq \sqrt{q}||\mathbf{x}||_2$, we have :

$$\begin{aligned}\mathsf{Exp}_{\mathbf{g} \leftarrow G^m}\left[\sum_{h \in \mathbf{G}}\left|P_{\mathbf{g}}(h) - \frac{1}{q}\right|\right] &\leq \mathsf{Exp}_{\mathbf{g} \leftarrow G^m}\left[q^{1/2}\left(\sum_{h \in \mathbf{G}}\left(P_{\mathbf{g}}(h) - \frac{1}{q}\right)^2\right)^{1/2}\right] \\ &= q^{1/2}\mathsf{Exp}_{\mathbf{g} \leftarrow G^m}\left[\left(\sum_{h \in \mathbf{G}}\left(P_{\mathbf{g}}(h) - \frac{1}{q}\right)^2\right)^{1/2}\right] \\ &\leq q^{1/2}\left(\mathsf{Exp}_{g \leftarrow G^m}\left[\sum_{h \in \mathbf{G}} P_{\mathbf{g}}(h)^2\right] - \frac{1}{q}\right)^{1/2} \\ &\leq q^{1/2} \cdot d^{-m/2} = \sqrt{\frac{q}{d^m}}\end{aligned}$$

Thus :

$$\mathsf{Exp}_{\mathbf{g} \leftarrow G^m}\left[\Delta(\sum_i b_i g_i, u)\right] \leq \frac{1}{2}\sqrt{\frac{q}{d^m}}$$

By *averaging argument*(See Appendix A), we have :

$$\Pr_{\mathbf{g} \leftarrow G^m}\left[\Delta(\sum_i b_i g_i, u) \geq (\frac{q}{d^m})^{\frac{1}{4}}\right] \leq (\frac{q}{d^m})^{\frac{1}{4}}.$$

(Otherwise, it can be derived that $\mathsf{Exp}_{\mathbf{g}\leftarrow G^m}[\Delta(\sum_i b_i g_i, u)] \geq \frac{1}{2}\sqrt{\frac{q}{d^m}}$, contradictory) ■

Next, we extend the above lemma to the Cartesian product of prime order groups.

Corollary 2 *Let $G_1 \times G_2 \cdots \times G_k$ be the Cartesian product of finite Abelian groups $\{G_i\}_{i\in[k]}$, where $|G_i| = q_i$ be primes, $q_{\min} = \min\{q_i\}_{i\in[k]}$, m be an integer, $\{\mathbf{g}_t = (g_{i,1}, \cdots g_{t,k}) \in G_1 \times G_2 \cdots \times G_k\}_{t\in[m]}$. For uniformly chosen $\{\mathbf{g}_t\}_{t\in[m]}$, $b_i \leftarrow \mathbb{Z}_{q_{\min}}$, $\mathbf{u} \leftarrow (G_1 \times G_2 \cdots \times G_k)$, the statistical distance $\Delta((\sum_{t\in[m]} b_t g_{t,1}, \cdots, \sum_{t\in[m]} b_t g_{t,k}), \mathbf{u})$ is expected to be at most $(\prod_{i=1}^k q_i/q_{\min}^m)^{\frac{1}{2}}$, in particular, the probability that the statistical distance exceeds $(\prod_{i=1}^k q_i/q_{\min}^m)^{\frac{1}{4}}$ does not exceed $(\prod_{i=1}^k q_i/q_{\min}^m)^{\frac{1}{4}}$.*

Proof. Similar to the lemma 6, first prove the family of hash functions $\mathcal{H}_{G_1\times,\cdots,\times G_k} = \{h_{\mathbf{g}} : \mathbf{g} \in G_1\times,\cdots,\times G_k\}$ is universal :

$$\begin{aligned} h_{\mathbf{g}} : \mathbb{Z}_{q_{\min}}^m &\to G_1 \times \cdots \times G_k \\ \mathbf{b} &\mapsto (\sum_{i=1}^m b_i g_{i,1}, \sum_{i=1}^m b_i g_{i,2}, \cdots, \sum_{i=1}^m b_i g_{i,k}) \end{aligned}$$

when $\mathbf{b} \neq \mathbf{b}' \mod q_{\min}$, and only the α-th element is non-zero $\{(b_\alpha - b'_\alpha)g_{\alpha,j} = 0\}_{j\in[k]}$, it holds that $\{g_{\alpha,j} = 0\}_{j\in[k]}$, then the collision probability is $\frac{1}{\prod_{i=1}^k q_i}$. Similarly, only when the α-th and β-th elements are non-zero $\{(b_\alpha - b'_\alpha)g_{\alpha,j} + (b_\beta - b'_\beta)g_{\beta,j} = 0\}_{j\in[k]}$, the collision probability is $\frac{1}{\prod_{i=1}^k q_i}$. Generally, when t elements are non-zero, there are:

$$\left\{ \sum_{\substack{i\in S \\ S\subset[m]}}^{|S|=t} (b_i - b'_i)g_{i,j} = 0 \right\}_{j\in[k]}$$

the collision probability is $\frac{1}{\prod_{i=1}^k q_i}$. Thus $\mathcal{H}_{G_1\times,\cdots,\times G_k}$ is universal. The proof of the statistical distance is similar to the lemma6, which will not be repeated here. ■

Remark : We want to extend the above result to the general finite Abelian group, but the hash function mapping to it seems not to be universal(there is zero divisor). Such as, let $G \simeq \mathbb{Z}_q \times \mathbb{Z}_a$($q$ be prime, $a > q$ be an integer), $b \neq b' \mod q$. For any $g_1 \leftarrow \mathbb{Z}_q$, $g_2 \leftarrow \mathbb{Z}_a$, let $(b - b')g_1 = 0$, it holds that $g_1 = 0$, but $(b - b')g_2 = 0$ holds for any $b - b'$ satisfying $ord(g_2)|(b - b')$, where $order(g_2)$ is the order of g_2, which the probability of $(b - b')g_2 = 0$ is :

$$\Pr_{\substack{b,b'\leftarrow\mathbb{Z}_q \\ g_2\leftarrow G}}[(b - b')g_2 = 0 | b - b' \neq 0] = \sum_{i=1}^{q-1} \left(\Pr_{b,b'\leftarrow\mathbb{Z}_q}[(b - b') = i] \cdot \frac{gcd(i, a)}{a} \right)$$

The above probability is clearly greater than $\frac{1}{a}$.

5 Leakage-resistant properties of LWE over $\frac{q}{d}\mathbb{Z}^m$

In this section, we need to introduce the LWE problem on $\frac{q}{d}\mathbb{Z}^m$, and then prove its anti-leakage property. In fact, it will not be simpler than the standard LWE problem. Below, we introduce this non-standard LWE problem, then reduce it to the standard LWE problem (which is almost an observation), and finally prove its anti-leakage property.

5.1 The LWE problem over $\frac{q}{d}\mathbb{Z}^m$

In this work, we mainly use its decision version.

Definition 6 *For $n, m, d, q \in \mathbb{N}, d \leq q$, and a distribution χ supported over $\frac{q}{d}\mathbb{Z}$, the rational-DLWE$_{n,m,d,q,\chi}$ problem is to distinguish the following distribution :*

- *$\mathcal{D}_0$: the joint distribution $(\mathbf{A}, \mathbf{z}) \in (\frac{q}{d}\mathbb{Z}_d^{n\times m} \times \frac{q}{d}\mathbb{Z}_d^m)$ is sampled by $\mathbf{A} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times m}$, $\mathbf{z} \leftarrow \frac{q}{d}\mathbb{Z}_d^m$.*
- *$\mathcal{D}_1$: the joint distribution $(\mathbf{A}, \mathbf{b}) \in (\frac{q}{d}\mathbb{Z}_d^{n\times m} \times \frac{q}{d}\mathbb{Z}_d^m)$ is computed by $\mathbf{A} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times m}$, $\mathbf{b} = \mathbf{sA} + \mathbf{e} \mod q$, where $\mathbf{s} \leftarrow \mathbb{Z}_d^n, \mathbf{e} \leftarrow \chi^m$.*

As introduced in Preliminary, the standard DLWE$_{n,m,q,\bar{\chi}}$ is defined on $\mathbb{Z}$, when $\bar{\chi}$ is a discrete Gaussian distribution on $\mathbb{Z}$ with a standard deviation $\sigma > 2\sqrt{n}$, it will not be simpler than the hard problem on lattice. Now we build the reduction from rational-DLWE$_{n,m,d,q,\chi}$ to DLWE$_{n,m,d,\bar{\chi}}$.

Claim 1 *If an adversary can distinguish the rational-DLWE$_{n,m,d,q,\chi}$ problem with an advantage ϵ in time T, then he can also distinguish the standard DLWE$_{n,m,d,\bar{\chi}}$ problem with the same time and advantage.*

Proof. In above section, we have shown that there is a bijection between $\Lambda_d(\mathbf{A})$ and $\Lambda_q(\mathbf{A}')$, where $\mathbf{A}' = \frac{q}{d}\mathbf{A}, \mathbf{A} \in \mathbb{Z}_d^{n\times m}$. Similarly, there is a bijection between DLWE$_{n,m,d,\bar{\chi}}$ and rational-DLWE$_{n,m,d,q,\chi}$ samples. For any given standard LWE$_{n,m,d,\bar{\chi}}$ samples $(\mathbf{A}, \mathbf{b} = \mathbf{sA} + \mathbf{e} \mod d)$, let $\mathbf{b} = \mathbf{sA} + \mathbf{e} + d \cdot \mathbf{c}^m$ where $\mathbf{c} \in \mathbb{Z}^m$, it holds that :

$$\frac{q}{d}\mathbf{b} = \frac{q}{d} \cdot \mathbf{sA} + \frac{q}{d}\mathbf{e} + q \cdot \mathbf{c}$$

Let $\mathbf{A}' = \frac{q}{d}\mathbf{A}$, $\mathbf{b}' = \frac{q}{d}\mathbf{b}$, $\mathbf{e}' = \frac{q}{d}\mathbf{e}$, it holds that :

$$\mathbf{b}' = \mathbf{sA}' + \mathbf{e}' \mod q$$

where $\mathbf{A}' \in \frac{q}{d}\mathbb{Z}_d^{n\times m}$,$\mathbf{e}' \in \frac{q}{d}\mathbb{Z}$. Thus $(\mathbf{A}', \mathbf{b}')$ is sample of rational-DLWE$_{n,m,d,q,\chi}$.

Therefore, for rational-DLWE$_{n,m,d,q,\chi}$, when χ is a discrete Gaussian defined on $\frac{q}{d}\mathbb{Z}$ with standard deviation $\sigma > 2\sqrt{n}$, it will not be simpler than DLWE$_{n,m,d,\bar{\chi}}$.

■

5.2 Leakage resistance of rational LWE samples

Goldwasser [27] et al. proved the leakage-resilient property of such "weak" LWE samples $(\mathbf{A}, \mathbf{b} = \mathbf{sA} + \mathbf{e})$ where $\mathbf{s}$ is taken from $\{0,1\}^n$(as the entropy of $\mathbf{s}$ is sufficient, it is no simpler than the low-dimensional standard LWE problem). It essentially used the anti-leakage property of the leftover hash lemma and reduced it to low-dimensional LWE samples.

Next, we prove that the rational-DLWE$_{n,m,d,q,\chi}$ samples we defined also have anti-leakage properties. This proof needs to use the regularity result of the hash function family on the prime order group(Corollary2), and unlike [27], we need to use the *Circular Security* assumption.

Theorem 6 *Let n, q be integers and $d \leq q$ be prime, $\mathbf{s}$ be a random variable over $\mathbb{Z}_d^n$, having min-entropy at least k. For any $r \leq \frac{k-\omega(\log n)+2}{\log d}$, there is a ppt reduction from rational-DLWE$_{n,m,d,q,\chi}$ to distinguish dual Regev ciphertext(with public key $\mathsf{pk} = (\mathbf{B}, \mathbf{t})$, $\mathbf{B} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times r}, \mathbf{t} = \mathbf{sB} \mod q$, and plaintext is related to private key $\mathbf{s}$) defined over $\frac{q}{d}\mathbb{Z}$ with uniform distribution.*

Proof. For a given m rational LWE samples, $(\mathbf{A}, \mathbf{b} = \mathbf{sA} + \mathbf{e})$, where $\mathbf{A} \leftarrow \frac{q}{d}\mathbb{Z}^{n\times m}, \mathbf{e} \leftarrow \chi^m, \mathbf{s} \leftarrow \mathbb{Z}_d^n$ and $\tilde{H}_\infty(\mathbf{s}) \geq k$. By claim1, we can replace $\mathbf{A}$ with $\mathbf{BC} + \mathbf{E}$, where $\mathbf{B} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times r}, \mathbf{C} \leftarrow \mathbb{Z}_d^{r\times m}, \mathbf{E} \leftarrow \chi^{n\times m}$, it holds that $\mathbf{b} = \mathbf{sBC} + \mathbf{sE} + \mathbf{e}$. Let $\mathbf{t} = \mathbf{sB} \mod q$, as $\frac{q}{d}\mathbb{Z}_d$ is a finite Abelian group with d elements, for any randomly chosen $\mathbf{B} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times r}$, $h_\mathbf{B}$ defines a hash function mapping from $\mathbb{Z}_d^n$ to $\frac{q}{d}\mathbb{Z}_d^r$.

$$\begin{aligned} \mathcal{H}_{\frac{q}{d}\mathbb{Z}_d^r} &= \{h_\mathbf{B} : \mathbf{B} \in \frac{q}{d}\mathbb{Z}_d^{n\times r}\} \\ h_\mathbf{B} &: \mathbb{Z}_d^n \to \frac{q}{d}\mathbb{Z}_d^r \\ &\quad \mathbf{s} \mapsto \mathbf{sB} \mod q. \end{aligned}$$

By Corollary2, we have the family of hash functions $\mathcal{H}_{\frac{q}{d}\mathbb{Z}_d^r}$ is universal, further, by the leftover hash lemma2, we have :

$$\Delta((\mathbf{B},\mathbf{t}),(\mathbf{B},\mathbf{u})) \leq 2^{-\frac{1}{2}(\tilde{H}_\infty(\mathbf{s})-\log d^r+2)}$$

Further, for any $r \leq \frac{k-\omega(\log n)+2}{\log d}$, we have $\Delta((\mathbf{B},\mathbf{t}),(\mathbf{B},\mathbf{u})) \leq \mathsf{negl}(n)$, where $\mathbf{u} \leftarrow \frac{q}{d}\mathbb{Z}_d^r$. Thus $\mathbf{b} = \mathbf{tC} + \mathbf{sE} + \mathbf{e}$. We note that $\mathbf{tC} + \mathbf{e}$ are m rational LWE samples. In [27], they set the variance of $\mathbf{E}$ and $\mathbf{e}$ to satisfy $||\mathbf{sE}||/||\mathbf{e}|| = \mathsf{negl}(n)$, then get $\mathbf{e} \approx_s \mathbf{e} + \mathbf{sE}$ by smudging lemma1. Thus $\mathbf{b} \approx_{\mathbf{s}} \mathbf{tC} + \mathbf{e}$ and l dimension standard LWE samples are indistinguishable. However, this method is not suitable for us. Our χ is defined on $\frac{q}{d}\mathbb{Z}$, and $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, so $\mathbf{sE}$ will overturn q with a high probability, which leaves no room for us to set the variance of $\mathbf{E}$ and $\mathbf{e}$, to satisfy $||\mathbf{sE}||/||\mathbf{e}|| = \mathsf{negl}(n)$.

We noticed that $\mathbf{b} = \mathbf{tC} + \mathbf{e} + \mathbf{sE}$ could be regarded as the ciphertext of the dual Regev encryption, where $(\mathbf{B}, \mathbf{t} = \mathbf{sB})$ is the public key, $\mathbf{s}$ is the private key, and $\mathbf{sE}$ is the plaintext(related to the private key). Suppose we assume the dual-Regev encryption scheme is *Circular Security* (while the encrypted data is related to private key, the ciphertext is still computationally indistinguishable). In that case, we should have enough confidence in the leak resistance of $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$.

Considering that the *Circular Security* assumption exists in many places, such as the *key-switch* in the FHE scheme [15] and the bootstrapping in [25] [17] [26]. Therefore, if an adversary can distinguish the $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ with the private key $\mathbf{s}$ lossy, then he can distinguish the dual Regev ciphertext(with plaintext is related to the private key).

■

6 Optimized multi-key fully homomorphic encryption scheme

Multi-key fully homomorphic encryption(MKFHE) was proposed by López-Alt *et al.* [33], and constructed the first MKFHE based on the NTRU encryption scheme. It was an extension of the single-key fully homomorphic scheme (supports homomorphic operations between ciphertexts encrypted with different public keys)

After López-Alt *et al* proposed the concept of MKFHE, by introducing CRS, Clear and McGoldrick [22], Mukherjee and Wichs [35], Peikert and Shiehian [36] constructed the GSW type MKFHE. Chen [20] and Chen [19] constructed the MKFHE based on RLWE and applied it to privacy-preserving neural network training with multi parties. The work [16] was the first MKFHE scheme that does not introduce CRS, by the anti-leakage property of the dual-Regev encryption scheme, it proved the security of its scheme, as the entropy of the private key is sufficient(the tradeoff is that the length of the private key increases with the amount of leakage). Ananth et al. [4] removed CRS from a higher dimension; instead of using the leftover hash lemma or regularity lemma, they based on *Multiparty homomorphic encryption* and modified the initialization method of its root node to achieve this purpose.

It is worth noting that most of the GSW-type MKFHE follow the same paradigm :

- The total private key is the concatenation of multiple private keys
- All require a ciphertext expansion to convert ciphertext under different public keys into ciphertext under the total private key
- Distributed decryption needs to introduce large noise to guarantee security

In order to solve the above problems, Dai et al. [23] introduced the *keylifting* operation in the interactive key generation stage, which removed the expensive ciphertext expansion. Based on the Rényi divergence argument and the asymmetric properties of the GSW ciphertext, it removed the noise flooding technique used in encryption and distributed decryption phase making the parameters the same as that of the single-key FHE scheme.

MKFHE is a rapidly developing field that has dominated many applications and is becoming a building block for many primitives: a series of work [16] [35] [5] showed that MKFHE was an excellent base tool for building round-optimal MPC.

Judging from the above series of work, MKFHE is moving closer to single-key FHE in terms of protocol design, security assumptions, and parameter sizes (ideally, we hope that MKFHE can both supports multi-party participation and can be as concise and compact as FHE(no CRS, ciphertext expansion, and noise flooding). Intuitively speaking, the complexity lower bound of the MKFHE scheme should be FHE.

As an application of our result in the previous section, we give an optimized MKFHE scheme based on [16]. It must be pointed out that such optimization can also be applied to [22] [35] [36] [23] and other GSW-based MKFHE(constructed on $\mathbb{Z}$, can use the leftover hash lemma to remove CRS). We choose [16] as an example because it requires fewer changes, and the improved result is better. For completeness, we define MKFHE below and then describe our improved scheme.

6.1 The definition of MKFHE

Definition 7 *Let λ be the security parameter, L be the circuit depth, and k be the number of participants. A levelled multi-key fully homomorphic encryption scheme consists of a tuple of efficient probabilistic polynomial time algorithms* MKFHE=(Init, Gen, Enc, Expand, Eval, Dec) *which defines as follows.*

- $\mathsf{pp} \leftarrow \mathsf{setup}(1^\lambda, 1^L, \mathsf{crs})$ *: Input security parameter λ, circuit depth L, common reference string* crs *(generated by a third party or random oracle), output system parameter* pp *([22] [35] [36] [19])*
- $\mathsf{pp} \leftarrow \mathsf{Distributed\ setup}(1^\lambda, 1^L, 1^k)$ *: Input security parameter λ, circuit depth L, user number k output system parameter* pp*. ([16] [23])*
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{pp})$ *: Input* pp*, output a key pair for participant 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.*
- $c_i \leftarrow \mathsf{Expand}(\{\mathsf{pk}_i\}_{i\in[k]}, v_i, c_i)$*: Input the ciphertext c_i of participant i, the public key set $\{\mathsf{pk}_i\}_{i\in[k]}$ of all participants, 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 $\mathcal{C}$, the set of all ciphertext $\mathcal{S} = \{\bar{c}_i\}_{i\in[N]}$ while N is the input length of $\mathcal{C}$, 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 : In the initial definition of MKFHE given by López-Alt *et al* [33], there is no limitation on the initialization of parameters. According to a series of existing works, we divide the initialization of parameters into the above two types: setup and Distributed setup. The difference is that the former needs to introduce CRS and complete the initialization locally. In contrast, the latter does not need to introduce CRS, but the user completes the initialization interactively. In addition, although the initial MKFHE definition does not include auxiliary ciphertext and ciphertext expansion operations, in fact, the works [35] [37] [22] include this procedure to support homomorphic operations. The common private key depends on $\{\mathsf{sk}_i\}_{i\in[k]}$, 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.

6.2 An improved "GSW-style" MKFHE based on [16]

Our optimized scheme is similar to [16], except that their scheme was based on Dual-GSW(on $\mathbb{Z}$), while our is GSW type(on $\frac{q}{d}\mathbb{Z}$), which will lead to different plaintext encoding. Furthermore, their "active leakage" model is $\mathbf{s}|\mathbf{sA}$, while ours is $\mathbf{s}|\mathbf{sA}+\mathbf{e}$. The improved scheme is defined as follows:

- $\mathsf{pp} \leftarrow \mathsf{setup}(1^\lambda, 1^k, 1^L)$: On input security parameter λ, users number $k = \mathsf{poly}(\lambda)$, circuit depth L, let $n = \mathsf{poly}(\lambda)$ be an integer, $d = 2^{O(\lambda L)}$ be a prime, $m = n\log d$, $q = d \cdot \mathsf{poly}(\lambda)$ satisfying $q = 1 \mod d$. Let χ be a noise distribution defined over $\frac{q}{d}\mathbb{Z}$, where $e \leftarrow \chi$, $|e|$ is bounded by B_χ with overwhelming probability. Suitable choosing the above parameters to make $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ is infeasible, output $\mathsf{pp} = (k, n, m, d, q, \chi)$.
- $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{pp}, i)$: Input pp, i, output the key pair $(\mathsf{pk}_i, \mathsf{sk}_i)$ of party i, where $\mathsf{pk}_i = (\mathbf{A}_i, \mathbf{b}_{i,i})$, $\mathbf{A}_i \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times m}$, $\mathbf{s}_i \leftarrow \mathbb{Z}_d^n$, $\mathbf{e} \leftarrow \chi^m$, $\mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i + \mathbf{e} \mod q$, $\mathsf{sk}_i = (\mathbf{s}_i, -1)$.
- $\mathsf{Auxk}_i \leftarrow \mathsf{Auxiliary\ KeyGen}(\mathsf{sk_i}, \{\mathsf{pk_j}\}_{\mathsf{j}\in[\mathsf{k}]/\mathsf{i}})$: Input the private key sk_i of party i and other parties public keys $\{\mathsf{pk}_j\}_{j\in[k]/i}$, output the Auxiliary key(as needed for ciphertext expansion) $\mathsf{Auxk}_i = \{\mathbf{b}_{i,j}\}_{j\in[k]/i}$ of party i, where $\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j + \mathbf{e}_j$.
- $\mathbf{C}_i \leftarrow \mathsf{Enc}(\mathsf{pk}_i, u_i)$: Input public key pk_i, a plaintext $u_i \in \{0, q\}$, output ciphertext $\mathbf{C}_i = \begin{pmatrix}\mathbf{A}_i\\ \mathbf{b}_{i,i}\end{pmatrix} \cdot \mathbf{R} + \begin{pmatrix}\mathbf{0}\\ \mathbf{e}'\end{pmatrix} + u_i\mathbf{G}$, where $\mathbf{e}'$ is sampled from $\chi'^{(n+1)l}$ defined over $\frac{q}{d}\mathbb{Z}$ satisfying $||\mathbf{eR}/\mathbf{e}'||_\infty = \mathsf{negl}(\lambda)$, $\mathbf{R} \leftarrow \{0,1\}^{m\times(n+1)l}$, $l = \lceil \log qd \rceil$, $\mathbf{G}$ is a gadget matrix as defined in preliminary.

– $u \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathbf{C})$: Input ciphertext $\mathbf{C}$, private key sk, let $\mathbf{t} = \mathsf{sk}$, $\mathbf{w}^T = (0, \cdots, 0, \frac{\lfloor d/2 \rfloor}{d}) \in \frac{1}{d}\mathbb{Z}_d^{n+1}$, $\gamma = \mathbf{t} \cdot \mathbf{C}\mathbf{G}^{-1}(\mathbf{w}^T)$, output $u = \lfloor \frac{\gamma}{q/2} \rceil$.

6.3 The encoding check

Since our improved scheme is based on $\frac{q}{d}\mathbb{Z}$, this causes our plaintext encoding to be different from the GSW scheme on $\mathbb{Z}$ (theirs are $\{0,1\}$, while ours is $\{0,q\}$). Next, we point out that as long as the parameters are set reasonably, the plaintext evaluation over $\{0,q\}$ resulting in the homomorphic evaluation of the ciphertext is also closed. The decryption, homomorphic addition, and multiplication of the initial ciphertext are tested in the following. It must be pointed out that the initial ciphertext does not undergo homomorphic evaluation because different public keys encrypt it, and it is the "expanded" ciphertext that actually undergoes homomorphic evaluation. Because the "expanded" ciphertext and the initial ciphertext maintain the same decryption paradigm: $\mathbf{tC} \approx u\mathbf{tG}$, the two are consistent in decryption, homomorphic addition and multiplication. We choose the initial ciphertext for verification here because it is more concise to describe.

Correctness of decryption : For initial ciphertext $\mathbf{C} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R} + \begin{pmatrix} \mathbf{0} \\ \mathbf{e}' \end{pmatrix} + u\mathbf{G}$, if $u = 0$, we have

$$\gamma = \mathbf{t}\mathbf{C}\mathbf{G}^{-1}(\mathbf{w}^T) = \langle \mathbf{e}\mathbf{R} + \mathbf{e}', \mathbf{G}^{-1}(\mathbf{w}^T) \rangle.$$

thus, if $\langle \mathbf{e}\mathbf{R} + \mathbf{e}', \mathbf{G}^{-1}(\mathbf{w}^T) \rangle \leq q/4$, it holds that $u = \lfloor \frac{\gamma}{q/2} \rceil = 0$. if $u = q$, it holds that

$$\begin{aligned} \gamma = \mathbf{t}\mathbf{C}\mathbf{G}^{-1}(\mathbf{w}^T) &= \langle \mathbf{e}\mathbf{R} + \mathbf{e}', \mathbf{G}^{-1}(\mathbf{w}^T) \rangle + u\mathbf{t}\mathbf{G}\mathbf{G}^{-1}(\mathbf{w}^T) \\ &= \langle \mathbf{e}\mathbf{R} + \mathbf{e}', \mathbf{G}^{-1}(\mathbf{w}^T) \rangle + \frac{q}{2} + \frac{q}{d}\Delta. \end{aligned}$$

where $|\Delta| < 0.5$, thus if $\langle \mathbf{e}\mathbf{R} + \mathbf{e}', \mathbf{G}^{-1}(\mathbf{w}^T) \rangle + \frac{q}{d}\Delta < \frac{q}{4}$, it holds that $u = \lfloor \frac{\gamma}{q/2} \rceil = 1$

homomorphic addition : Let $\mathbf{C}_{\mathsf{add}} = \mathbf{C}_1 + \mathbf{C}_2$, where $\mathbf{C}_1$ are $\mathbf{C}_2$ the ciphertext under $(\mathbf{A}, \mathbf{b})$, it holds that

$$\gamma = \mathbf{t}\mathbf{C}_{\mathsf{add}}\mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}}) = \langle \mathbf{e}\mathbf{R}_1 + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_1' + \mathbf{e}_2',\ \mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}}) \rangle + (u_1 + u_2)\mathbf{t}\mathbf{G}\mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}})$$

– if $u_1 = u_2 = 0$ and $\langle \mathbf{e}\mathbf{R}_1 + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_1' + \mathbf{e}_2',\ \mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}}) \rangle \leq \frac{q}{4}$, it holds that : $u = \lfloor \frac{\gamma}{q/2} \rceil = 0$
– if $u_1 = 0, u_2 = q$(vice versa) , and $\langle \mathbf{e}\mathbf{R}_1 + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_1' + \mathbf{e}_2',\ \mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}}) \rangle + \frac{q}{d}\Delta \leq \frac{q}{4}$, it holds that : $u = \lfloor \frac{\gamma}{q/2} \rceil = 1$
– if $u_1 = u_2 = q$, it holds that :

$$\gamma = \langle \mathbf{e}\mathbf{R}_1 + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_1' + \mathbf{e}_2',\ \mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}}) \rangle + 2q(\frac{1}{2} + \frac{\Delta}{d}) \mod q$$

thus if $\langle \mathbf{e}\mathbf{R}_1 + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_1' + \mathbf{e}_2',\ \mathbf{G}^{-1}(\mathbf{w}^{\mathbf{T}}) \rangle + 2\frac{q}{d}\Delta < \frac{q}{4}$, we have $u = \lfloor \frac{\gamma}{q/2} \rceil = 0$

Homomorphic multiplication : In order for the ciphertext multiplication corresponding to the plaintext multiplication to be closed on $\{0,q\}$, we need $\frac{q^2}{d} = \frac{q}{d} \mod q$ (this is why we set $q = 1 \mod d$). Thus ,for any $a \in \frac{q}{d}\mathbb{Z}$, it holds that $qa = a \mod q$, $q^2 \cdot \mathbf{G} = q \cdot \mathbf{G} \mod q$. Let :

$$\begin{aligned} \mathbf{C}_{\mathsf{mult}} = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = &\begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R}_1\mathbf{G}^{-1}\left[\begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R}_2 + \begin{pmatrix} \mathbf{0} \\ \mathbf{e}_2' \end{pmatrix}\right] + u_2 \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R}_1 \\ &+ \begin{pmatrix} \mathbf{0} \\ \mathbf{e}_1'\mathbf{G}^{-1}\left[\begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R}_2 + \begin{pmatrix} \mathbf{0} \\ \mathbf{e}_2' \end{pmatrix}\right] \end{pmatrix} + u_2 \begin{pmatrix} \mathbf{0} \\ \mathbf{e}_1' \end{pmatrix} \\ &+ u_1 \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix} \mathbf{R}_2 + u_1 \begin{pmatrix} \mathbf{0} \\ \mathbf{e}_2' \end{pmatrix} + u_1u_2\mathbf{G}. \end{aligned}$$

Let $\mathbf{M} = \begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_1\mathbf{G}^{-1}\left[\begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_2 + \begin{pmatrix}\mathbf{0}\\ \mathbf{e}_2'\end{pmatrix}\right] + \begin{pmatrix}\mathbf{0}\\ \mathbf{e}_1'\mathbf{G}^{-1}\left[\begin{pmatrix}\mathbf{A}\\ \mathbf{b}\end{pmatrix}\mathbf{R}_2 + \begin{pmatrix}\mathbf{0}\\ \mathbf{e}_2'\end{pmatrix}\right]\end{pmatrix}$

we have

$$\gamma = \mathbf{t}\mathbf{C}_{\mathsf{mult}}\mathbf{G}^{-1}(\mathbf{w}^T) = \langle \mathbf{t}\mathbf{M} + u_2\mathbf{e}\mathbf{R}_1 + u_2\mathbf{e}_1' + u_1\mathbf{e}\mathbf{R}_2 + u_1\mathbf{e}_2', \quad \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + u_1u_2\mathbf{t}\mathbf{G}\mathbf{G}^{-1}(\mathbf{w}^T)$$

- if $u_1 = u_2 = 0$ and $\langle \mathbf{t}\mathbf{M}, \mathbf{G}^{-1}(\mathbf{w}^T)\rangle \leq \frac{q}{4}$, it holds that $\lfloor \frac{\gamma}{q/2} \rceil = 0$
- if $u_1 = q, u_2 = 0$(vice versa) and :

$$\langle \mathbf{t}\mathbf{M} + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_2', \quad \mathbf{G}^{-1}(\mathbf{w}^T)\rangle \leq \frac{q}{4}$$

  it holds that $\lfloor \frac{\gamma}{q/2} \rceil = 0$
- if $u_1 = u_2 = q$, we have :

$$\gamma = \underbrace{\langle \mathbf{t}\mathbf{M} + \mathbf{e}\mathbf{R}_1 + \mathbf{e}_1' + \mathbf{e}\mathbf{R}_2 + \mathbf{e}_2', \quad \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \frac{q}{d}\Delta}_{Error} + \frac{q}{2}$$

  and $Error \leq \frac{q}{4}$, it holds that $\lfloor \frac{\gamma}{q/2} \rceil = 1$

6.4 Security under Semi-malicious adversary

We note that the auxiliary key of i is $\mathsf{Auxk}_i = \{\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j + \mathbf{e}_j\}_{j\in[k]/i}$, where $\{\mathbf{A}_j\}_{j\in[k]/i}$ is generated by other $k-1$ parties, under the semi-honest adversary, $\{\mathbf{A}_j\}_{j\in[k]/i}$ is uniform over $\frac{q}{d}\mathbb{Z}_d^{n\times m}$. Under the rational-$\mathsf{DLWE}_{n,m,d,q,\chi}$ assumption, Auxk_i is indistinguishable from the uniform, and the scheme's security is obvious now.

However, under the semi-malicious adversary, $\{\mathbf{A}_j\}_{j\in[k]/i}$ may not be uniform, and the conditional distributions $\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i}$ and $\mathbf{s}_i$ may be quite different. In order to cover this "active leakage" model, we need to assume that the average min-entropy $\tilde{H}_\infty(\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i})$ of $\mathbf{s}_i$ is large enough, we have the following result :

Lemma 7 *Let $\mathbf{A}_i \in \frac{q}{d}\mathbb{Z}_d^{n\times m}$ be uniform, and $\{\mathbf{A}_j\}_{j\in[k]/i}$ be chosen by a rushing adversary after seeing $\mathbf{A}_i$. Let $\mathbf{s}_i \leftarrow \mathbb{Z}_d^n$, χ be a discrete Gaussian distribution over $\frac{q}{d}\mathbb{Z}$, $\mathbf{e}_j \leftarrow \chi^m$, and $\{\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j + \mathbf{e}_j\}_{j\in[k]/i}$. Assuming $\tilde{H}_\infty(\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i}) \geq n$, and dual-Regev encryption is circular security with public key $(\mathbf{B}, \mathbf{t})$, $\mathbf{B} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times r}$, $\mathbf{t} = \mathbf{s}_i\mathbf{B} \mod q$, $r = \frac{n-\omega(\log n)}{\log d}$, then it holds that $(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \mathbf{C})$ and $(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \mathbf{U})$, where $\mathbf{C}$ is the ciphertext of party i, $\mathbf{U} \leftarrow \frac{q}{d}\mathbb{Z}_d^{(n+1)\times(n+1)l}$, are (jointly) computational indistinguishable.*

Proof. Let $\mathbf{C} = \begin{pmatrix}\mathbf{C}_0\\ \mathbf{c}_1\end{pmatrix} = \begin{pmatrix}\mathbf{A}_i\\ \mathbf{b}_{i,i}\end{pmatrix}\mathbf{R} + \begin{pmatrix}\mathbf{0}\\ \mathbf{e}'\end{pmatrix}$, for $\mathbf{b}_{i,i} = \mathbf{s}_i\mathbf{A}_i + \mathbf{e}$, it holds that $\mathbf{c}_1 = \mathbf{s}_i\mathbf{A}_i\mathbf{R} + \mathbf{e}\mathbf{R} + \mathbf{e}' = \mathbf{s}_i\mathbf{C}_0 + \mathbf{e}\mathbf{R} + \mathbf{e}'$. By our parameter settings, we have $||\mathbf{e}\mathbf{R}/\mathbf{e}'|| = \mathsf{negl}(\lambda)$, thus :

$$\left(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \begin{pmatrix}\mathbf{C}_0\\ \mathbf{c}_1\end{pmatrix}\right) \approx_s \left(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \begin{pmatrix}\mathbf{C}_0\\ \mathbf{s}_i\mathbf{C}_0 + \mathbf{e}'\end{pmatrix}\right)$$

Using the leftover hash lemma with $\mathbf{A}_i$ as seed and $\mathbf{R}$ as source, we have $(\mathbf{A}_i, \mathbf{C}_0) \approx_s (\mathbf{A}_i, \mathbf{Z})$, where $\mathbf{Z} \leftarrow \frac{q}{d}\mathbb{Z}_d^{n\times(n+1)l}$, thus :

$$\left(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \begin{pmatrix}\mathbf{C}_0\\ \mathbf{s}_i\mathbf{C}_0 + \mathbf{e}'\end{pmatrix}\right) \approx_s \left(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \begin{pmatrix}\mathbf{Z}\\ \mathbf{s}_i\mathbf{Z} + \mathbf{e}'\end{pmatrix}\right)$$

We note that $\mathbf{Z}$ is independent of $\mathbf{s}_i$, as $\mathbf{C}_0$ is generated after $\mathbf{s}_i|\{\mathbf{b}_{i,j}\}$. Assuming $\tilde{H}_\infty(\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i}) \geq n$, let $r = \frac{n-\omega(\log n)}{\log d}$ and dual-Regev encryption is circular security. By Theorem6, it holds that :

$$\left(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \begin{pmatrix}\mathbf{Z}\\ \mathbf{s}_i\mathbf{Z} + \mathbf{e}'\end{pmatrix}\right) \approx_c \left(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \begin{pmatrix}\mathbf{Z}\\ \mathbf{z}\end{pmatrix}\right)$$

where $\mathbf{z} \leftarrow \mathbb{Z}_d^{(n+1)l}$, Thus$(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \mathbf{C})$ and $(\mathbf{A}_i, \{\mathbf{b}_{i,j}\}_{j\in[k]/i}, \mathbf{U})$, are (jointly) computational indistinguishable.

■

Remark: Note that the premise of the above result is that $\tilde{H}_\infty(\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i}) \geq n$, where $\mathbf{b}_{i,j} = \mathbf{s}_i\mathbf{A}_j + \mathbf{e}_j$. Assuming $i = 1$, we have

$$(\mathbf{b}_{1,2}, \mathbf{b}_{1,3}, \cdots, \mathbf{b}_{1,k}) = \mathbf{s}_1(\mathbf{A}_2|\mathbf{A}_3|\cdots|\mathbf{A}_k) + (\mathbf{e}_2|\mathbf{e}_3|\cdots|\mathbf{e}_k).$$

Let $\bar{\mathbf{A}} = (\mathbf{A}_2|\mathbf{A}_3|\cdots|\mathbf{A}_k)$, $\bar{\mathbf{e}} = (\mathbf{e}_2|\mathbf{e}_3|\cdots|\mathbf{e}_k)$, by Theorem2, if $0 < \sigma < \frac{d}{2\sqrt{m(k-1)}}$ we have

$$\tilde{H}_\infty(\mathbf{s}_i|\mathbf{s}_i\bar{\mathbf{A}} + \bar{\mathbf{e}}) \geq -\log(\frac{1}{\rho_\sigma(\Lambda_q(\bar{\mathbf{A}}))} + 2^{-m(k-1)}) \tag{7}$$

By lemma5, if $\mathsf{rank}(\Lambda_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$ and $\sigma > 4\gamma$, then it holds that $\rho_\sigma(\Lambda_q(\bar{\mathbf{A}}) > 2^{n+2}$(satisfying $\frac{1}{\rho_\sigma(\Lambda_q(\bar{\mathbf{A}}))} \leq 2^{-n} - 2^{m(k-1)}$, thus $\tilde{H}_\infty(\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i}) \geq n$).

We observe from [5] that one way to satisfy $\mathsf{rank}(\Lambda_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$ is to make $\bar{\mathbf{A}}$ have structure as

$$\bar{\mathbf{A}} = \left(\begin{array}{c|c|c|c} \mathbf{B}_2 & \mathbf{B}_3 & \cdots & \mathbf{B}_k \\ \mathbf{S}\mathbf{B}_2 + \mathbf{E}_2 & \mathbf{S}\mathbf{B}_3 + \mathbf{E}_3 & \cdots & \mathbf{S}\mathbf{B}_k + \mathbf{E}_k \end{array}\right)$$

(The work [5] constructed the Unbounded MPC protocol and used it against semi-malicious receivers). Thus it holds that :

$$\begin{pmatrix} \mathbf{I} & \\ \mathbf{S} & \mathbf{I} \end{pmatrix}^{-1} \cdot \bar{\mathbf{A}} = \left(\begin{array}{c|c|c|c} \mathbf{B}_2 & \mathbf{B}_3 & \cdots & \mathbf{B}_k \\ \mathbf{E}_2 & \mathbf{E}_3 & \cdots & \mathbf{E}_k \end{array}\right) \in \Lambda_q(\bar{\mathbf{A}})$$

Let $\mathbf{B}_i \leftarrow \frac{q}{d}\mathbb{Z}_d^{\frac{n}{2}\times m}$, $\mathbf{S} \leftarrow \mathbb{Z}_d^{\frac{n}{2}\times\frac{n}{2}}$, $\mathbf{E}_i \leftarrow \bar{\chi}^{\frac{n}{2}\times m}$, $\bar{\chi}$ be defined over $\frac{q}{d}\mathbb{Z}$ with standard deviation $\bar{\sigma}$ satisfying $\sqrt{m(k-1)} \cdot \bar{\sigma} \leq \gamma$, it holds that $\mathsf{rank}(\Lambda_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$, further on $\sigma > 4\gamma$, we have $\tilde{H}_\infty(\mathbf{s}_i|\mathbf{s}_i\bar{\mathbf{A}} + \bar{\mathbf{e}}) > n$. Let $\bar{\sigma} > 2\sqrt{n}$, by $\mathsf{rational\text{-}DLWE}_{\frac{n}{2},m,d,q,\bar{\chi}}$, $\bar{\mathbf{A}}$ looks random.

Put things together : In this subsection, we bring together the previous parameter requirements, in particular, the range of standard deviations for several discrete Gaussian distributions. By Theorem2, for (7) holds, we need $0 < \sigma < \frac{d}{2\sqrt{m(k-1)}}$. In order to make $\mathsf{rank}(\Lambda_q(\bar{\mathbf{A}}) \bigcap \gamma B) > \frac{n}{2}$, $\tilde{H}_\infty(\mathbf{s}|\mathbf{s}\bar{\mathbf{A}} + \bar{\mathbf{e}}) > n$, we need $\sqrt{m(k-1)}\bar{\sigma} < \gamma$, $\sigma > 4\gamma$; and $\bar{\sigma} > 2\sqrt{n}$ to make $\bar{\mathbf{A}}$ looks random. In Lemma7, we require $||\mathbf{e}\mathbf{R}/\mathbf{e}'||_\infty = \mathsf{negl}(\lambda)$.

To sum up, we get the parameters of $\bar{\chi}$ and χ respectively as follows :

$$\bar{\sigma} > 2\sqrt{n}, \quad 8\sqrt{mn(k-1)} < \sigma < \frac{d}{2\sqrt{m(k-1)}} \tag{8}$$

and χ' is a uniform distribution over $[-2^\lambda\sigma, 2^\lambda\sigma]$.

6.5 Ciphertext expansion

In order to convert the ciphertext under different keys into ciphertext under the same key, the GSW-type ciphertext needs to take a so-called "ciphertext expansion" operation. The private key corresponding to the expanded ciphertext is private key concatenation. A typical ciphertext expansion was the masking scheme defined in [35] [37] [22] : for any ciphertext $\mathbf{C} = \begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix}\mathbf{R} + u\mathbf{G}$ to be expanded(the corresponding private key was $\mathbf{t}$), input any $\mathbf{v} \in \mathbb{Z}_q^m$ and the ciphertext of the random matrix $\mathbf{R}$, the masking scheme applied the homomorphic property of the GSW scheme to output the ciphertext $\mathbf{X} \in \mathbb{Z}_q^{(n+1)\times(n+1)l}$ of $\mathbf{v}\mathbf{R}$ under $\mathbf{t}$(satisfying $\mathbf{t}\mathbf{X} \approx \mathbf{v}\mathbf{R}$), where the function of $\mathbf{X}$ is to eliminate the redundant items produced by decrypting $\mathbf{C}$ with other party's private key $\mathbf{t}'$.

We note that the above masking scheme works for our variant as well, simply because the encryption and decryption formulas are identical and all follow the GSW ciphertext structure(except with our scheme is defined over $\frac{q}{d}\mathbb{Z}$). Below, for completeness, we informally describe the process of ciphertext expansion.

A masking scheme for GSW ciphertext (defined in [35] [22] adapted to our scheme) : There exist a pair of algorithm (UniEnc, Extend)

- $\mathsf{UniEnc}(u, \mathsf{pk})$: On input a message $u \in \{0, q\}$ and a public key $\mathbf{t}$ of our scheme, it output a pair $(\mathcal{U}, \mathbf{C})$, where $\mathbf{C} \in \frac{q}{d}\mathbb{Z}_d^{(n+1)\times(n+1)l}$ and $\mathcal{U} \in \{0,1\}^*$
- $\mathsf{Extend}(\mathcal{U}, \mathbf{C}, \mathbf{v})$: On input $\mathcal{U}$, $\mathbf{C}$ and $\mathbf{v} \in \frac{q}{d}\mathbb{Z}_d^m$, it output $\mathbf{X} \in \frac{q}{d}\mathbb{Z}_d^{(n+1)\times(n+1)l}$.

Let $u_{i,j} \in \{0, q\}$ be the encoding of an item of $\mathbf{R}[i, j]$(row i, column j of $\mathbf{R}$), and $\mathcal{U} \in \{0,1\}^*$ be the ciphertext of $\mathbf{R}$ under $\mathbf{t}$, $\mathbf{v} \in \frac{q}{d}\mathbb{Z}_d^m$ be any vector, the correctness of above scheme guarantees that $\mathbf{tX} = \mathbf{vR} + \mathbf{e_X}$, which $||\mathbf{e_X}||_\infty$ is bounded by $(n+1)^4 l^4 B_\chi$

When $k = 2$, let $\bar{\mathbf{C}} = \begin{pmatrix} \mathbf{C} & \mathbf{X} \\ & \mathbf{C} \end{pmatrix} \in \frac{q}{d}\mathbb{Z}_d^{2(n+1)\times 2(n+1)l}$, be the expanded ciphertext of our scheme under public key $\mathbf{t}_1$, let $\mathbf{t}_2$ be another public key, it holds that :

$$\begin{aligned}(\mathbf{t}_1, \mathbf{t}_2)\bar{\mathbf{C}} &= (\mathbf{t}_1\mathbf{C} | \mathbf{t}_1\mathbf{X} + \mathbf{t}_2\mathbf{C}) \\ &\approx (u\mathbf{t}_1\mathbf{G} | \mathbf{t}_1\mathbf{X} + (\mathbf{b}_{2,1} - \mathbf{b}_{1,1})\mathbf{R} + u\mathbf{t}_2\mathbf{G})\end{aligned}$$

In above masking scheme, we can set $\mathbf{v} = \mathbf{b}_{1,1} - \mathbf{b}_{2,1}$, where $\mathbf{b}_{2,1}$ is the auxiliary key of party 2 and let $\mathcal{U}$ be the ciphertext of $\mathbf{R}$, then it holds that $\mathbf{t}_1\mathbf{X} \approx (\mathbf{b}_{1,1} - \mathbf{b}_{2,1})\mathbf{R}$, thus :

$$(\mathbf{t}_1, \mathbf{t}_2)\bar{\mathbf{C}} \approx u(\mathbf{t}_1, \mathbf{t}_2)\begin{pmatrix} \mathbf{G} & \\ & \mathbf{G} \end{pmatrix}$$

Thus $\bar{\mathbf{C}} = \begin{pmatrix} \mathbf{C} & \mathbf{X} \\ & \mathbf{C} \end{pmatrix}$ is the expanded ciphertext of $\mathbf{C}$ with only two parties. The above process can be extended to k parties. At this time, the expanded ciphertext of $\mathbf{C}$ is:

$$\bar{\mathbf{C}} = \begin{pmatrix} \mathbf{C} & \mathbf{X}_1 & \cdots & \mathbf{X}_{k-1} \\ & \mathbf{C} & & \\ & & \cdots & \\ & & & \mathbf{C} \end{pmatrix} \in \frac{q}{d}\mathbb{Z}_d^{k(n+1)\times k(n+1)l}$$

where the corresponding key is $(\mathbf{t}_1, \cdots, \mathbf{t}_k)$, and $\{\mathbf{X}_i\}_{i\in[k-1]}$ satisfying $\mathbf{t}_1\mathbf{X}_i \approx (\mathbf{b}_{1,1} - \mathbf{b}_{i+1,1})\mathbf{R}$.

Homomorphic addition and multiplication : Let $\bar{\mathbf{C}}_1, \bar{\mathbf{C}}_2$ be the ciphertext after ciphertext expansion, $\bar{\mathbf{t}} = (\mathbf{t}_1, \mathbf{t}_2, \cdots, \mathbf{t}_k)$ and $\bar{\mathbf{G}} = \begin{pmatrix} \mathbf{G} & & & \\ & \mathbf{G} & & \\ & & \cdots & \\ & & & \mathbf{G} \end{pmatrix} \in (\mathbb{Z}_q + \frac{1}{d}\mathbb{Z}_d)^{k(n+1)l\times k(n+1)l}$

- $\mathbf{C}_{\mathsf{add}} \leftarrow \mathsf{Add}(\bar{\mathbf{C}}_1, \bar{\mathbf{C}}_2)$: Input ciphertext $\bar{\mathbf{C}}_1$, $\bar{\mathbf{C}}_2$ output $\mathbf{C}_{\mathsf{add}} = \bar{\mathbf{C}}_1 + \bar{\mathbf{C}}_2$, it holds that : $\bar{\mathbf{t}} \cdot \mathbf{C}_{\mathsf{add}} \approx (u_1 + u_2)\bar{\mathbf{t}}\bar{\mathbf{G}}$
- $\mathbf{C}_{\mathsf{mult}} \leftarrow \mathsf{mult}(\bar{\mathbf{C}}_1, \bar{\mathbf{C}}_2)$: Input ciphertext $\bar{\mathbf{C}}_1$, $\bar{\mathbf{C}}_2$ output $\mathbf{C}_{\mathsf{mult}} = \bar{\mathbf{C}}_1 \cdot \mathbf{G}^{-1}(\bar{\mathbf{C}}_2)$, it holds that : $\bar{\mathbf{t}} \cdot \mathbf{C}_{\mathsf{mult}} \approx u_1 u_2 \bar{\mathbf{t}}\bar{\mathbf{G}}$

Accumulation of noise : Here, we estimate the noise accumulation by the evaluation of expanded ciphertext. Let $\bar{\mathbf{C}}_1$ be the expanded ciphertext of $\mathbf{C}_1$, we have :

$$\begin{aligned}\bar{\mathbf{t}}\bar{\mathbf{C}} &= (\mathbf{t}_1, \mathbf{t}_2, \cdots, \mathbf{t}_k)\begin{pmatrix} \mathbf{C}_1 & \mathbf{X}_1 & \cdots & \mathbf{X}_{k-1} \\ & \mathbf{C}_1 & & \\ & & \cdots & \\ & & & \mathbf{C}_1 \end{pmatrix} \\ &= (\mathbf{t}_1\mathbf{C}_1 | \mathbf{t}_1\mathbf{X}_1 + \mathbf{t}_2\mathbf{C}_1 | \cdots | \mathbf{t}_1\mathbf{X}_{k-1} + \mathbf{t}_k\mathbf{C}_1) \\ &= (\mathbf{eR} + \mathbf{e}' | \mathbf{eR} + \mathbf{e}' + \mathbf{e_X} | \cdots | \mathbf{eR} + \mathbf{e}' + \mathbf{e_X}) + u_1\bar{\mathbf{t}}\bar{\mathbf{G}} \\ &= \mathbf{e}_{\mathsf{init}} + u_1\bar{\mathbf{t}}\bar{\mathbf{G}}\end{aligned}$$

Therefore, the initial noise $||\mathbf{e}_{\mathsf{init}}||_\infty$ obtained by decrypting $\bar{\mathbf{C}}_1$ is bounded by $(m+(n+1)^4l^4)B_\chi + B_{\chi'}$. Suppose the multiplication depth of the circuit to be evaluated is L(The noise caused by multiplication grows much faster than addition, so generally only multiplication is counted), according to the noise analysis of GSW in [26], the noise $\mathbf{e}_L$ after L depth circuit evaluation in $\bar{\mathbf{C}}_L$, is bounded by $(k(n+1)l)^L\mathbf{e}_{\mathsf{init}}$. Let $\bar{\mathbf{w}}^T = (0,\cdots,0,\frac{\lfloor \frac{d}{2} \rfloor}{d}) \in \frac{1}{d}\mathbb{Z}_d^{k(n+1)}$, we have :

$$\bar{\mathbf{t}}\bar{\mathbf{C}}_L\mathbf{G}^{-1}(\bar{\mathbf{w}}^T) = \langle \mathbf{e}_L, \mathbf{G}^{-1}(\bar{\mathbf{w}}^T\rangle + \frac{u}{2} + \frac{u}{d}\Delta.$$

For correctness hold, it requires : $\langle \mathbf{e}_L, \mathbf{G}^{-1}(\bar{\mathbf{w}}^T\rangle + \frac{u}{d}\Delta \leq \frac{q}{4}$, by our parameter settings and equation(8), $k, n = \mathsf{poly}(\lambda)$, $l = \log qd$, $m = n\log d$, $B_\chi, B_{\chi'}$ are bounded by $\frac{q}{d}\sigma$ and $2^\lambda \cdot \frac{q}{d}\sigma$ respectively, we have :

$$\langle \mathbf{e}_L, \mathbf{G}^{-1}(\bar{\mathbf{w}}^T\rangle + \frac{u}{d}\Delta \leq (k(n+1)l)^L((m+(n+1)^4l^4)B_\chi + B_{\chi'})\log d + \frac{q}{d} \tag{9}$$

One can observe that decryption works correctly for some $d = 2^{O(\lambda L)}$, $q = \mathsf{poly}(\lambda)\cdot 2^{O(\lambda L)}$, it holds that $(9) \leq \frac{q}{4}$.

6.6 Comparison

The biggest difference between our optimized scheme and scheme [16] is similar to the difference between the GSW scheme and the Dual-GSW scheme, and the key and ciphertext sizes of their schemes are related to k. Compared with the MKFHE that introduces CRS, such as [35] our scheme is obviously not dominant, see the complexity comparison in the Table 2. The computation of our scheme is proportional to k^3, the communication in the setup phase is independent of k, and the total communication amount should be the ciphertext size multiplied by the input length of the circuit. In general, the complexity (computation and communication) of our scheme is better than [16], but worse than the scheme introducing CRS.

Table 2: Complexity

Scheme	Key size	Ciphertext size	Hom-multiplication	Comunication in setup	Setup
[35]	$O(n^2\log^2 q)$	$O(n^2\log^2 q)$	$O(k^3n^3\log^2 q)$	-	CRS
[16]	$O(kn^2\log^2 q)$	$O(k^2n^2\log^4 q)$	$O(k^6n^3\log^5 q)$	$O(kn^2\log^2 q)$	-
our scheme	$O(n^2\log^2 d)$	$O(n^2\log(dq)\log d)$	$O(k^3n^3\log^2 qd)$	$O(n^2\log qd\log d)$	-

k, n, q denotes number of parties, LWE dimension, modulus respectively. d is defined in our scheme with $d = q/\mathsf{poly}(\lambda)$. The key and ciphertext are counted in bits. The Hom-multipication column counts the number of multiplications on $\mathbb{Z}_q$ required for a homomorphic multiplication. The Communication in setup column counts the communication traffic required for the interactive key generation phase

References

1. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (Mar 2009)
2. 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)
3. 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)
4. 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)
5. 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)
6. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (Aug 2009)

7. 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)
8. Attrapadung, N., Hanaoka, G., Hiromasa, R., Matsuda, T., Schuldt, J.C.: Maliciously circuit-private multi-key fhe and mpc based on lwe. Designs, Codes and Cryptography pp. 1–40 (2022), https://doi.org/10.1007/s10623-022-01160-x
9. Badrinarayanan, S., Goyal, V., Jain, A., Khurana, D., Sahai, A.: Round optimal concurrent mpc via strong simulation. In: Kalai, Y., Reyzin, L. (eds.) Theory of Cryptography. pp. 743–775. Springer International Publishing, Cham (2017)
10. Badrinarayanan, S., Jain, A., Manohar, N., Sahai, A.: Secure mpc: Laziness leads to god. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 120–150. Springer International Publishing, Cham (2020)
11. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen 296, 625–635 (1993)
12. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A., Seth, K.: Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p. 1175–1191. CCS '17, Association for Computing Machinery, New York, NY, USA (2017), https://doi.org/10.1145/3133956.3133982
13. 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)
14. Brakerski, Z., Döttling, N.: Hardness of LWE on general entropic distributions. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 551–575. Springer, Heidelberg (May 2020)
15. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: Goldwasser, S. (ed.) ITCS 2012. pp. 309–325. ACM (Jan 2012)
16. 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)
17. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: Ostrovsky, R. (ed.) 52nd FOCS. pp. 97–106. IEEE Computer Society Press (Oct 2011)
18. Canetti, R., Dodis, Y., Halevi, S., Kushilevitz, E., Sahai, A.: Exposure-resilient functions and all-or-nothing transforms. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 453–469. Springer, Heidelberg (May 2000)
19. 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)
20. 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)
21. Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M.: Private information retrieval. J. ACM 45(6), 965–981 (nov 1998), https://doi.org/10.1145/293347.293350
22. 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)
23. Dai, X., Wu, W., Feng, Y.: Key lifting : Multi-key fully homomorphic encryption in plain model without noise flooding. Cryptology ePrint Archive, Paper 2022/055 (2022), https://eprint.iacr.org/2022/055, https://eprint.iacr.org/2022/055
24. Dziembowski, S.: Intrusion-resilience via the bounded-storage model. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 207–224. Springer, Heidelberg (Mar 2006)
25. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Mitzenmacher, M. (ed.) 41st ACM STOC. pp. 169–178. ACM Press (May / Jun 2009)
26. 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)
27. Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Robustness of the learning with errors assumption. In: Yao, A.C.C. (ed.) ICS 2010. pp. 230–240. Tsinghua University Press (Jan 2010)
28. Goyal, V., Masserova, E., Parno, B., Song, Y.: Blockchains enable non-interactive mpc. In: Nissim, K., Waters, B. (eds.) Theory of Cryptography. pp. 162–193. Springer International Publishing, Cham (2021)
29. Hazay, C., López-Alt, A., Wee, H., Wichs, D.: Leakage-resilient cryptography from minimal assumptions. Journal of Cryptology 29(3), 514–551 (Jul 2016)
30. 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)
31. Kalai, Y.T., Reyzin, L.: A survey of leakage-resilient cryptography. In: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, pp. 727–794 (2019)

32. Konečný, J., McMahan, H.B., Yu, F.X., Richtárik, P., Suresh, A.T., Bacon, D.: Federated learning: Strategies for improving communication efficiency (2017)
33. 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)
34. 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)
35. 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)
36. Peikert, C., Shiehian, S.: Multi-key FHE from LWE, revisited. In: Hirt, M., Smith, A.D. (eds.) TCC 2016-B, Part II. LNCS, vol. 9986, pp. 217–238. Springer, Heidelberg (Oct / Nov 2016)
37. Peikert, C., Shiehian, S.: Multi-key FHE from LWE, revisited. Cryptology ePrint Archive, Report 2016/196 (2016), https://eprint.iacr.org/2016/196
38. 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)
39. Reyzin, L.: Extractors and the leftover hash lemma. Lecture notes, available at https://www.cs.bu.edu/~reyzin/teaching/s11cs937/notes-leo-1.pdf
40. Vadhan, S.P.: Pseudorandomness. Foundations and Trends® in Theoretical Computer Science 7(1–3), 1–336 (2012), http://dx.doi.org/10.1561/0400000010
41. Xagawa, K.: Cryptography with lattices. Ph.D. thesis (2010), available at http://xagawa.net/pdf/2010Thesis.pdf
42. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982). pp. 160–164 (1982)

Appendix

A Averaging argument

In layman's terms, for any random variable X, if the expectation of X is at least ρ, then there must be a value of X that is at least ρ. Namely:

$$\mathsf{Exp}[X] \geq \rho \Longrightarrow \Pr[X \geq \rho] > 0.$$

see details : https://www.cs.princeton.edu/courses/archive/spr06/cos522/averaging.pdf

Claim 2 *If everyone likes at least $\frac{1}{3}$ of the books in the library, then there is a book in the library that at least $\frac{1}{3}$ of the people like.*

Proof. Suppose the number of people and books are N, B, respectively. Ask everyone to mark their favorite book with a red dot. Thus, the red dot mark in the book in the library has at least $\frac{NB}{3}$. Now assuming that there is no book that is liked by at least $\frac{1}{3}$ of the people, thus the amount of red dot marks in each book is less than $\frac{N}{3}$, which will cause the total number of red dot marks in books in the library to be less than $\frac{NB}{3}$, contradiction.

■