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

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 $\mathbb{Z}_q^{n\times m}$. Under the DLWE assumption, the conditional distribution of $\mathbf{s}|(\mathbf{A}, \mathbf{b})$ and $\mathbf{s}$ is expected to be consistent. However, in the case where an adversary chooses $\mathbf{A}$ adaptively, the disparity between the two entities may be larger. In this work, our primary focus is on the quantification of the Average Conditional Min-Entropy $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$ of $\mathbf{s}$, 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 $d \leq q$, when $\mathbf{s}$ is uniformly chosen from $\mathbb{Z}_d^n$ or is sampled from a discrete Gaussian distribution, there are also similar results.

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 [12] 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

Secure multi-party computation(MPC) [31], Threshold fully homomorphic encryption(Th-FHE) and Multi-key fully homomorphic encryption(MKFHE) [23] provide technical support for computing tasks involving multiple users. Depending on the assumptions, the techniques mentioned above can be divided into two categories: the first with setup (trusted third party, common reference string(CRS)), while the second without setup (plain model).

Compared to schemes or protocols under the plain model, those schemes that involve a trusted third party or CRS are much simpler and more efficient, particularly during 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.) Therefore, building cryptographic primitives under the plain model has also become a demand for some people.

The key issue here is that the initialization of MPC, Th-FHE, or MKFHE protocols, such as key generation, often relies on some common parameters. If these parameters come from a trusted third party, their integrity can be guaranteed.

If there is no trusted third party or CRS, then the initialization of the protocol is usually an interactive process involving users. At this time, the reliability of the data cannot be guaranteed, which may result in the compromise of user privacy.

For example, in the MKFHE scheme [12], parties need to multiply their own private key $\mathbf{s}$ with a matrix $\mathbf{A}$ generated by another party and make $\mathbf{sA}$ public in order to support "ciphertext expansion". In the oblivious transfer protocol [9], 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 error. Similarly, the unbounded MPC protocol [2] also requires the LWE samples $\mathbf{y} = \mathbf{sA} + \mathbf{e}$ to be made public, where $\mathbf{A}$ is generated by the adversary.

1.1 Motivation

In the MKFHE scheme [12], assuming there are k parties, in order to support subsequent *ciphtertext expansion*, each party needs to multiply their own private key $\mathbf{s}$ by the public keys $\{\mathbf{A}_i\}_{i\in[k-1]}$ of the other $k-1$ parties and make $\{\mathbf{b}_i = \mathbf{s}\mathbf{A}_i\}_{i\in[k-1]}$ public. In order to quantify the average conditional min-entropy $\tilde{H}_\infty(\mathbf{s}|\{\mathbf{b}_i\}_{i\in[k-1]})$ of $\mathbf{s} \in \{0,1\}^m$ after disclosing $\{\mathbf{b}_i = \mathbf{s}\mathbf{A}_i\}_{k-1}$, the leakage in the worst case was estimated. For $\mathbf{b}_i \in \mathbb{Z}_q^n$, $\{\mathbf{b}_i = \mathbf{s}\mathbf{A}_i\}_{i\in[k-1]}$ leaks $\mathbf{s}$ with a maximum of $(k-1)n\log q$ bits. According to the proof in [12], based on the Leftover Hash Lemma (LHL), in order to ensure that the statistical distance between the ciphertext and the uniform distribution is less than $\frac{1}{2^\lambda}$, m should be at least $m-(k-1)n\log q \geq \log q + 2\lambda$.

In [9], another "active leakage" model was applied as $\mathbf{s}|\mathbf{b} = \mathbf{sA}+\mathbf{e}$. To ensure that the entropy of $\mathbf{s}$ remains 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 the model $\mathbf{s}|\mathbf{sA}+\mathbf{e}$ 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 $\Lambda_q(\mathbf{A})$. Additionally, the loss ratio is $O(\frac{1}{\log q})$ provided that $\Lambda_q(\mathbf{A})$ has enough short vectors, whereas the latter is $O(\frac{1}{n})$. Based on this, the work [9] 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 $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA})$ 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 for any $d \leq q$, where $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, or $\mathbf{s}$ is sampled from a discrete Gaussian distribution.

Such a requirement is not baseless. In the LWE-like sample $\mathbf{sA}+\mathbf{e}$, it is sometimes convenient and necessary to bound the norm of $\mathbf{s}$. In order to support bootstrapping in FHE, it is necessary to encrypt the private key $\mathbf{s}$. If $\mathbf{s}$ is uniformly distributed over $\mathbb{Z}_q$, how can it be filled into the plaintext space? Therefore, [3] reduced the LWE samples with discrete Gaussian secrets to the LWE samples with uniform secrets. MKFHE scheme [14] requires that $\mathbf{s}$ be sampled from the discrete Gaussian distribution in order to mitigate the noise introduced by the *re-linearization* after multiplication of the ciphertext. Furthermore, [20] proved that Regev's encryption scheme is leakage-resilient when the private key $\mathbf{s}$ is taken from a small uniform range. The work [20] only provided a reduction for $\mathbf{s} \in \{0,1\}^*$, but the result holds for all sufficiently small $\mathbf{s}$. In addition, the paper [2] utilizes the result of [9] to defend against semi-malicious adversaries. However, in their proposed scheme, $\mathbf{s}$ is drawn from a discrete Gaussian distribution.

Therefore, if we can characterize $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$ for any $d \leq q$, where $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, 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 [12], resulting in shorter keys and smaller ciphertexts. We will present our results in the following section.

1.2 Our Results

For LWE samples whose secrets are sampled from a discrete Gaussian distribution $\mathcal{D}_{\mathbb{Z}^n,\sigma}$, 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:*

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

Let d be an integer and χ be the noise distribution in the standard LWE distribution, which is bounded by B_χ. For LWE samples whose secrets are sampled uniformly from $\mathbb{Z}_d^n$, we have the following result.

Theorem 2 *Let λ, n, q, d, $m = O(n\log q)$ be integers, χ be the discrete Gaussian distribution over $\mathbb{Z}$ bounded by B_χ. Let χ' be the uniform distribution over $\mathbb{Z}_d$ satisfying $\frac{B_\chi}{d} = \mathsf{negl}(\lambda)$. For a given matrix*

$\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, *let* $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \mathbf{s}\bar{\mathbf{A}} + \bar{\mathbf{e}})$, *where* $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\bar{\mathbf{e}} \leftarrow \chi'^n$. *Let* $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\mathbf{e} \leftarrow \chi'^m$, $\mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e}$. *It holds that:*

$$\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \geq \log(|\Lambda_q(\tilde{\mathbf{A}}) \bigcap V_{\tilde{\mathbf{b}}}(d)|)$$

where $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A})$, $\tilde{\mathbf{b}} = (\bar{\mathbf{b}}, \mathbf{b})$, $V_{\tilde{\mathbf{b}}}(d)$ *is the hypercube with* $\tilde{\mathbf{b}}$ *as the center point and* d *as the side length.*

For the LWE samples whose secrets are uniformly sampled from $\mathbb{Z}_d^n$ for any $d \in \mathbb{Z}$, where $d \leq q$, we present a more general results of Lemma 3.2 in [9] (Lemma 3.2 is a special case of our Theorem).

Theorem 3 *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 :*

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

Clearly, when $d = q$, the above Theorem degenerates to Lemma 3.2 in [9]. 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 (Lemma 6 and Corollary 2). This result will be used in the security proof of our improved scheme.

As an application of the above results, we optimized the MKFHE scheme in [12]. It must be pointed out that [12] is becoming a cornerstone, increasingly used in constructing more complex protocols, particularly in the MPC protocol with the optimal number of rounds. Such as [6], based on [12], constructed a three-round protocol in the simultaneous message exchange model with rushing adversaries. This protocol achieves sub-exponential concurrent super-polynomial simulation (SPS) security for secure multi-party computation for any efficiently computable function, allowing all parties to receive output. Based on [12], the work [7] constructed a secure threshold multi-key FHE scheme for the class of access structures $\{0,1\}$-LSSSD. The work [21], based on [12], constructed an MPC that does not require the parties to be online simultaneously or interact with each other. As the main building block [12] used in [5] to construct a maliciously circuit-private MKFHE scheme.

Therefore, the aforementioned applications should all benefit from our improved scheme. In particular, combined with the proof trick of [20] for the LWE variant of binary keys, we provide a positive answer to the question raised at the end of [12]: the ciphertext of our improved scheme is constructed in a GSW-like manner, rather than Dual GSW. In addition, compared with [12] and [24], our ciphertext and key are shorter, as shown in Table 1.

Table 1: Complexity

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

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.

1.3 Related works

The work of Brakerski and Döttling [10] 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 [20], 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 $\tilde{H}_\infty(\mathbf{s}|\mathbf{s}\mathbf{A} + \mathbf{e})$, where $\mathbf{A}$ may not be uniformly distributed. This type of leakage model is more prevalent 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 complement each other. Their research focuses on the hardness of entropy LWE, and considers 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 characterizing the active leakage of $\mathbf{s}|\mathbf{sA}+\mathbf{e}$(there should be no side channel to obtain $\mathbf{s}$ from $\mathbf{sA}+\mathbf{e}$), 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 typically represented as row vectors, while matrices are denoted by uppercase bold letters such as $\mathbf{M}$. Let k be an integer and $[k]$ be the set of integers $\{1,\cdots,k\}$. If X is a distribution, then $a \leftarrow X$ denotes that the value a is chosen according to the distribution X. If X is a finite set, then $a \leftarrow X$ denotes that the value of a is uniformly sampled from X. For two distributions X and Y, we use $X \approx_s Y$ to represent that X and Y are statistically indistinguishable, while $X \approx_c Y$ represents that they are computationally indistinguishable.

For positive integers n and $q > 2$, a vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a probability distribution χ on $\mathbb{Z}_q$, we define $A_{\mathbf{s},\chi}$ as the distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, an error term $e \leftarrow \chi$, and outputting $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$. In general, unless otherwise specified, all operations are performed modulo q.

Gadget decomposition over $\frac{q}{d}\mathbb{Z}_d$: Let $d \leq q$ be two integers. We will consider decomposing the elements of $\frac{q}{d}\mathbb{Z}_d$ into binary. Let $\mathbf{g} = \frac{q}{d}(1, 2, \ldots, 2^{l-1})$ where $l = \lceil \log d \rceil$. For any $a \in \frac{q}{d}\mathbb{Z}_d$, let $a = \frac{q}{d} \cdot t$, where $t \in \mathbb{Z}_d$. We define $\mathbf{g}^{-1}(a) = \{0,1\}^l$ as the decomposition of t. For any $a \in \frac{q}{d}\mathbb{Z}_d$, it holds that $\mathbf{g} \cdot \mathbf{g}^{-1}(a) = a$. Furthermore, for $\mathbf{M} \in \frac{q}{d}\mathbb{Z}_d^{m \times n}$, let $\mathbf{G} = \mathbf{I}_m \otimes \mathbf{g}$, it holds that $\mathbf{G}^{-1}(\mathbf{M}) \in \{0,1\}^{ml \times n}$ and $\mathbf{G}\mathbf{G}^{-1}(\mathbf{M}) = \mathbf{M}$.

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 :*

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

Lemma 1 (Smudging Lemma [4]) *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 [9]) 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 [28] and [29]

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 4 ((Leftover Hash Lemma(LHL) [22])) *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 provides 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 [30] presents a more easily applicable version.

Lemma 2 (Lemma 4.2.3 in [30]) *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 ([27], 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 5 *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 $\mathcal{D}_{\Lambda+\mathbf{c},\sigma}$ with support $\Lambda + \mathbf{c}$ is defined as :*

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

Lemma 4 (in [9]) *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 $\mathbf{t} \in \Lambda$ and $\mathbf{z} \in \Lambda$. 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 [9]) *Let $\mathcal{B}$ be the unit ball. 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 6 (in [8]) *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 6, 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}.*

Theorem 7 (The Gaussian Heuristic) *Let $\mathcal{L}$ be a random lattice, for all sufficiently large $S \subset \mathbb{R}^n$, it holds that*

$$\left| S \bigcap \mathcal{L} \right| \approx vol(S) / \det(\mathcal{L})$$

2.5 Learning with Errors

The Learning With Errors(LWE) problem was introduced by Regev [27]. 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 $(\mathbf{A}, \mathbf{b} = \mathbf{sA} + \mathbf{e}) \in (\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m)$ by m samples of $A_{\mathbf{s},\chi}$*

It is often considered the hardness of solving DLWE$_{n,m,q,\chi}$ for any $m = \text{poly}(n \log q)$. 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 $k = \text{poly}(n)$ can be established from DLWE$_{n,m,q,\chi}$ via a routine hybrid-argument.

As shown in Regev [27], for certain module q and discrete Gaussian error distribution χ with parameter $\sigma = \alpha q \geq 2\sqrt{n}$, the 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 Section 3, we outline our approach and techniques. In Section 4, we proved a more general result for $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$. In Section 5, 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 Section 6, we proved the leakage-resilient property of LWE defined on $\frac{q}{d}\mathbb{Z}^m$. In Section 7, we presented our improved MKFHE scheme.

3 Technical overview

In this section, we will briefly outline our technical approach, focusing on our ideas and providing readers with some intuition. A detailed description will be given in the subsequent section. For the given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and $\mathbf{y} = \mathbf{sA} + \mathbf{e}$, where $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$, by the definition of Average Conditional Min-Entropy 2.2

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

where $\mathbf{s}^*$ is the point maximizes the conditional probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}]$. The work [9] notes that when $\mathbf{s}$ is uniformly chosen from $\mathbb{Z}_q^n$, by Bayes' rule,

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

the denominator is a constant, that is, when $\mathbf{s}^*\mathbf{A}$ is the point closest to $\mathbf{y}$, conditional probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s}=\mathbf{s}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}]$ is the largest. The events that $\mathbf{s}^*\mathbf{A}$ is the lattice point closest to $\mathbf{y}$ and $\mathbf{e}\in V$, are equivalent, where V is the discrete *Voronoï cell* of $\mathbf{s}^*\mathbf{A}$. Therefore, they can transform the problem from finding the probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s}=\mathbf{s}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}]$ to finding the probability $\Pr(\mathbf{e}\in V)$.

LWE with discrete Gaussian secrets. However, when $\mathbf{s}$ is sampled from a discrete Gaussian distribution, we cannot directly apply the above method to quantify the probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s}=\mathbf{s}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}]$. The reason is as follows, also according to Bayes' rule

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

We cannot proceed to the next step because, when $\mathbf{s}$ is drawn from a discrete Gaussian distribution, we cannot determine the probability that $\mathbf{s}$ equals $\mathbf{s}^*$. At this time, the point $\mathbf{s}^*\mathbf{A}$ that maximizes the probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s}=\mathbf{s}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}]$ is not necessarily the lattice point closest to $\mathbf{y}$. This is the challenge of determining the probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s}=\mathbf{s}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}]$ when $\mathbf{s}$ is drawn from a discrete Gaussian distribution.

By the reduction from the LWE with uniform secrets to the LWE with Gaussian secrets, the noise of the former becomes the secrets of the latter. Therefore, in order to quantify the entropy of the latter secrets, we can turn to the entropy of the noise. By definition

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

where $\mathbf{e}^*$ is the point that maximizes the conditional probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{e}=\mathbf{e}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}]$. Given $\mathbf{A}$ and $\mathbf{y}$, when $\mathbf{s}^*\mathbf{A}$ is the closest lattice point to $\mathbf{y}$, $||\mathbf{e}|| = ||\mathbf{y}-\mathbf{s}^*\mathbf{A}||$ is minimized. As $\mathbf{e}$ is discrete Gaussian, it holds that $\mathbf{e}^*=\mathbf{y}-\mathbf{s}^*\mathbf{A}$. Events $\mathbf{e}=\mathbf{e}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}$ and $\mathbf{s}=\mathbf{s}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}$ are equivalent, as shown in Figure 1. Furthermore, it holds that $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{e}=\mathbf{e}^*|\mathbf{y}=\mathbf{sA}+\mathbf{e}] = \Pr[\mathbf{e}\in V]$, where V is the *Voronoï cell* of the lattice point $\mathbf{s}^*\mathbf{A}$. Therefore, based on the previous result $\Pr(\mathbf{e}\in V) < \frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))}$ [9], when $\mathbf{s}$ is drawn from the discrete Gaussian distribution, we can quantify the conditional entropy of $\mathbf{s}$.

LWE with bounded uniform secrets. Let $d=\mathsf{suppoly}(\lambda)<q$[3] be an integer. When the secret $\mathbf{s}$ is sampled uniformly from $\mathbb{Z}_d^n$. We cannot apply the above method directly. The reason is as follows. This is because $\mathbf{sA} \mod q$ cannot traverse all lattice points. Let

[3] $\mathsf{suppoly}(\lambda)$ is the superpolynomial of λ

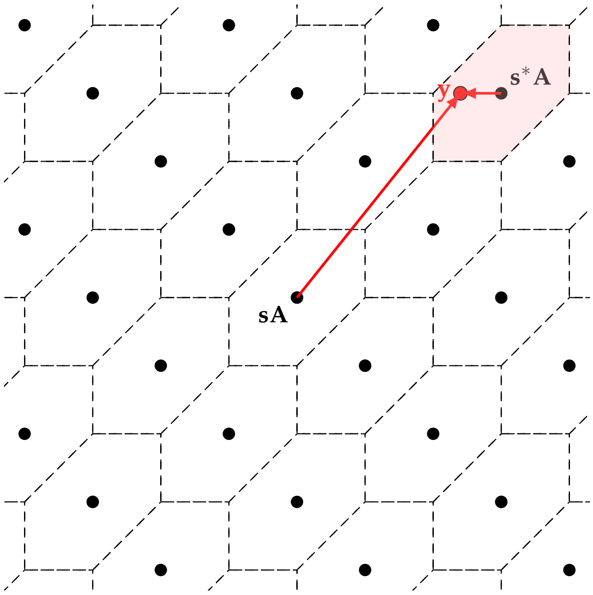

Fig. 1: $\mathbf{s}^*\mathbf{A}$ is the lattice point closest to $\mathbf{y}$, at this time, $\mathbf{e}^*$ happens to fall in the *Voronoï cell* of $\mathbf{s}^*\mathbf{A}$

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

obviously, S is a subset of the 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 $\mathbf{s} \leftarrow \mathbb{Z}_d^n$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$, according to 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 Figure 2, we interpret it in a two-dimensional lattice.

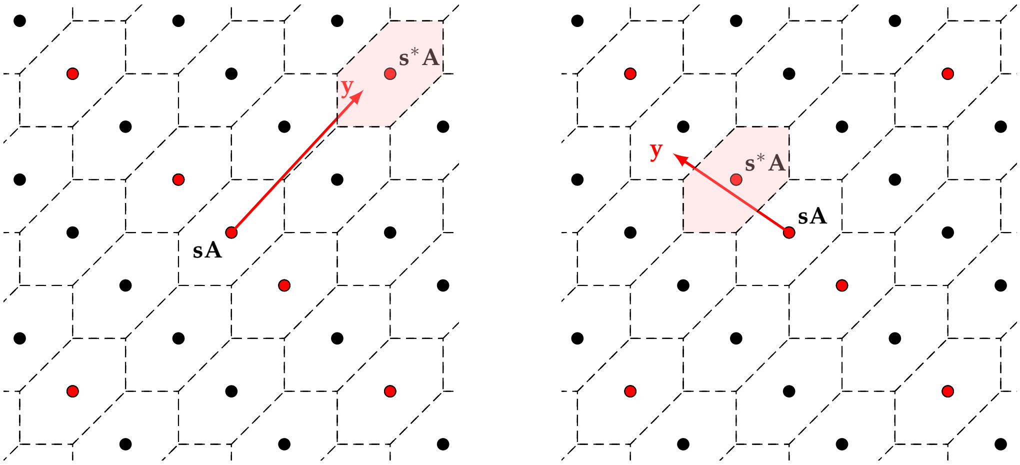

Fig. 2: Cases of the nearest point to $\mathbf{y}$: Red points are in S. The left panel shows that the closest point to $\mathbf{y}$ is on S, but the right panel clearly shows that the closest point to $\mathbf{y}$ is not on S.

Obviously, in the second case, $\mathbf{y}$ falls outside the *Voronoï cell* of $\mathbf{s}^*\mathbf{A}$ and $\mathbf{e} \notin V$. Therefore, we cannot use Lemma 3.2 in [9] to obtain the $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA} + \mathbf{e})$ lower bound. The point is that $\mathbf{sA} \mod q$

does not necessarily traverse all the lattice points when limiting $\mathbf{s}$ to a small range. This is the challenge of determining the probability $\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}]$ when $\mathbf{s}$ is sampled from a bounded uniform distribution.

Similar to the case where the secret is drawn from a discrete Gaussian distribution, we can use the reduction from LWE with a uniform secret to LWE with a Gaussian secret. Given the LWE samples whose noise is taken from a bounded uniform distribution, we can convert it into the LWE samples whose secret is taken from a bounded uniform distribution. Similarly, in order to quantify the secret's entropy, we can refer to the entropy of the noise. By the chain rule of entropy, $H(X,Y) = H(X) + H(Y|X)$. Therefore, for the given $\mathbf{A}$ and $\mathbf{y}$, the entropy of the $\mathbf{e}$ is equal to the entropy of the secret $\mathbf{s}$. By Bayes' rule, the entropy of the key can be determined directly, as the noise is both bounded and uniform.

$$\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}] = \frac{\Pr_{\mathbf{s},\mathbf{e}}[\mathbf{e} = \mathbf{y} - \mathbf{s}^*\mathbf{A}]}{\sum_{\mathbf{s}'} \Pr_{\mathbf{s},\mathbf{e}}[\mathbf{e} = \mathbf{y} - \mathbf{s}'\mathbf{A}]} = \frac{1}{|\Lambda_q(\mathbf{A}) \bigcap V_{\mathbf{y}}(d)|}$$

The hypercube $V_{\mathbf{y}}(d)$ is defined as the cube with $\mathbf{y}$ as the center point and d as the side length.

LWE with bounded uniform secrets for any $d < q$. Note that in the above case, d cannot be too small, at least suppoly(λ). This is because for the LWE samples with smaller d, we do not know how to reduce them to the standard LWE samples. We want to quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{y} = \mathbf{sA} + \mathbf{e})$ for any integer $d \leq q$, when $\mathbf{s}$ is chosen uniformly from $\mathbb{Z}_d^n$. Compromises must be made at this point; the lattice $\Lambda_q(\mathbf{A})$ is dynamic. If $S = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x} = \mathbf{sA} \mod q, \mathbf{s} \in \mathbb{Z}_d^n\}$ is a lattice, a similar conclusion can be obtained from Lemma 3.2 in [9].

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. This is similar to $\Lambda_q(\mathbf{A}')(\mathbf{A}' \in \mathbb{Z}^{n\times m}$, being a q-ary lattice defined over $\mathbb{Z}^m$, and $\Lambda_q(\mathbf{A})$ being a d-ary lattice defined over $\frac{q}{d}\mathbb{Z}^m$. Therefore, for such a lattice $\Lambda_q(\mathbf{A})$, when $\mathbf{s} \leftarrow \mathbb{Z}_d^n(d \leq q)$, we can still quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{y} = \mathbf{sA} + \mathbf{e} \mod q)$.

More efficient MKFHE. The improvement on the MKFHE scheme [12] requires us to show that $\mathbf{sA} + \mathbf{e}$ remains pseudorandom even 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 [20] from binary LWE samples to low-dimensional standard LWE samples. Let $\mathbf{A} = \mathbf{BC} + \mathbf{E}$, where $\mathbf{B} \leftarrow \frac{q}{d}\mathbb{Z}^{n\times l}$, $\mathbf{C} \leftarrow \mathbb{Z}_d^{l\times m}$, and $\mathbf{E} \leftarrow \mathcal{D}^{n\times m}_{\frac{q}{d}\mathbb{Z},\sigma'}$. 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, it is sufficient to show that the hash function determined by $\mathbf{B}$ is universal and that $\mathbf{s}$ has enough conditional entropy. This implies 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 typically *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 denoted as $(\mathbf{B}, \mathbf{t})$, $\mathbf{s}$, and $\mathbf{sE}$, respectively. In other words, 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 [12], 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 Section 7.2.

4 Lattice-based, more general anti-leakage model

In Section 4.1, we first quantify the anti-leakage properties of LWE, where the secrets are drawn from a discrete Gaussian distribution. However, when the secrets are uniform in a small range, the situation is different. In Section 4.2, we consider the case when $\mathbf{s}$ is drawn from a bounded uniform distribution $\mathbb{Z}_d^n$, where d cannot be small. In Section 4.3, for any integer $d < q$, We describe a lattice contained on $\frac{q}{d}\mathbb{Z}^m$, then in Section 4.4, we prove the anti-leakage property of the LWE samples on this lattice.

4.1 The leakage-resilient of LWE samples with discrete Gaussian secrets

When $\mathbf{s}$ is drawn from a discrete Gaussian distribution, we cannot directly apply the proof in [9]. At this time, we need to use the reduction technique [3] from the LWE with discrete Gaussian secrets to the 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 $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, and $\bar{\mathbf{e}} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$. Let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e}, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$, sends $(\mathbf{A}', \mathbf{b}' = \mathbf{b} + \bar{\mathbf{b}}\mathbf{A}')$ to Alice.

The above game essentially reduces 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 8 *Let n, q, $m = O(n\log q)$ be integers, and $0 < \sigma < \frac{q}{2\sqrt{m+n}}$. For a given matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, 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 :*

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

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 Theorem 5, 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 Theorem 6, 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 Lemma 4, 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 :

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

Because $\mathbf{A}'$ is public, thus $\tilde{H}_\infty(\mathbf{e}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}, \bar{\mathbf{e}}) = 0$, 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 :

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

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

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

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

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

■

4.2 The leakage-resilient of LWE samples with bounded uniform secrets

In this section, we first describe the indistinguishability of the LWE samples whose $\mathbf{s}$ and error $\mathbf{e}$ are sampled from a bounded uniform distribution. We then quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{s}\mathbf{A} + \mathbf{e})$, where $\mathbf{A}$ may not be uniform.

Let χ be the discrete Gaussian distribution over $\mathbb{Z}$ bounded by B_χ. Let λ be the security parameter, d be an integer, χ' be the uniform distribution over $\mathbb{Z}_d$, satisfying $\frac{B_\chi}{d} = \mathsf{negl}(\lambda)$. Let $\mathbf{s}' \leftarrow \chi'^n$, almost obvious, $A_{\mathbf{s}',\chi'}$ is indistinguishable from a uniform distribution. The proof is easy; we only need to note two facts. First, the LWE samples, whose errors are sampled from a bounded uniform distribution, are indistinguishable from a uniform distribution. Let $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $(\mathbf{A}, \mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e})$ be m samples of $A_{\mathbf{s},\chi}$. Let $\mathbf{e}' \leftarrow \chi'^m$, $\mathbf{b}' = \mathbf{b} + \mathbf{e}'$, by Lemma 1, we have $\mathbf{b}' \approx_s \mathbf{b}' - \mathbf{e}$. Thus, given any m $A_{\mathbf{s},\chi}$ samples, we can transform them into $A_{\mathbf{s},\chi'}$ samples by adding a large noise $\mathbf{e}'$. Thus, by the $\mathsf{DLWE}_{n,m,q,\chi}$ assumption, we have $A_{\mathbf{s},\chi'} \approx_c \mathbf{U}$. Second, by reducing the standard LWE to the discrete Gaussian version of LWE, we can transform the samples of $A_{\mathbf{s},\chi'}$ to the samples of $A_{\mathbf{s}',\chi'}$. Again, based on the $\mathsf{DLWE}_{n,m,q,\chi}$ assumption, we have $A_{\mathbf{s}',\chi'} \approx_c \mathbf{U}$.

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 samples $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \mathbf{s}\bar{\mathbf{A}}, +\bar{\mathbf{e}})$ from $A_{\mathbf{s},\chi'}$. Let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\mathbf{e} \leftarrow \chi'^m$, $\mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e}$, sends $(\mathbf{A}', \mathbf{b}' = \mathbf{b} + \bar{\mathbf{b}}\mathbf{A}')$ to Alice.

The game above essentially transforms from $A_{\mathbf{s},\chi'}$ to $A_{\mathbf{s}',\chi'}$. Apparently $(\mathbf{A}', \mathbf{b}' = \bar{\mathbf{e}}\mathbf{A}' + \mathbf{e})$ are the m samples of $A_{\mathbf{s}',\chi'}$, but $\mathbf{A}'$ may not be uniform since $\mathbf{A}$ is chosen by Alice. Now, we quantify $\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e})$.

Theorem 9 *Let λ, n, q, d, $m = O(n \log q)$ be integers, χ be the discrete Gaussian distribution over $\mathbb{Z}$ bounded by B_χ. Let χ' be the uniform distribution over $\mathbb{Z}_d$ satisfrying $\frac{B_\chi}{d} = \mathsf{negl}(\lambda)$. For a given matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, let $(\bar{\mathbf{A}}, \bar{\mathbf{b}} = \mathbf{s}\bar{\mathbf{A}} + \bar{\mathbf{e}})$ be n samples of $A_{\mathbf{s},\chi'}$, let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\mathbf{e} \leftarrow \chi'^m$, $\mathbf{b} = \mathbf{s}\mathbf{A} + \mathbf{e}$. It holds that :*

$$\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}' + \mathbf{e}) \geq \log(|\Lambda_q(\tilde{\mathbf{A}}) \bigcap V_{\tilde{\mathbf{b}}}(d)|)$$

where $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A})$, $\tilde{\mathbf{b}} = (\bar{\mathbf{b}}, \mathbf{b})$, $V_{\tilde{\mathbf{b}}}(d)$ is the hypercube with $\tilde{\mathbf{b}}$ as the center point and d as the side length.

Proof. Let $\tilde{\mathbf{e}} = (\bar{\mathbf{e}}, \mathbf{e})$, according to the definition of average min-entropy, it holds that

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

By Bayes's rule, we have

$$\begin{aligned}
&\Pr_{\mathbf{s},\tilde{\mathbf{e}}}[\mathbf{s}=\mathbf{s}^*|\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}] = \Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}} \mid \mathbf{s}=\mathbf{s}^*\right]\cdot \frac{\Pr\left[\mathbf{s}=\mathbf{s}^*\right]}{\Pr_{\mathbf{s},\tilde{\mathbf{e}}}[\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}]} \\
&= \Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{s}^*\tilde{\mathbf{A}}\right]\cdot \frac{\Pr\left[\mathbf{s}=\mathbf{s}^*\right]}{\sum_{\mathbf{s}'}\Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}} \mid \mathbf{s}=\mathbf{s}'\right]\Pr\left[\mathbf{s}=\mathbf{s}'\right]} \\
&= \Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{s}^*\tilde{\mathbf{A}}\right]\cdot \frac{q^{-n}}{\sum_{\mathbf{s}'}\Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{s}'\tilde{\mathbf{A}}\right]\cdot q^{-n}} \\
&= \frac{\Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{s}^*\tilde{\mathbf{A}}\right]}{\sum_{\mathbf{s}'}\Pr_{\mathbf{s},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{s}'\tilde{\mathbf{A}}\right]} = \frac{1}{|\Lambda_q(\tilde{\mathbf{A}})\bigcap V_{\tilde{\mathbf{b}}}(d)|}
\end{aligned}$$

Thus, we have

$$\tilde{H}_\infty(\mathbf{s}|\tilde{\mathbf{b}}) = \tilde{H}_\infty(\mathbf{s}|\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}) = \log(|\Lambda_q(\tilde{\mathbf{A}})\bigcap V_{\tilde{\mathbf{b}}}(d)|)$$

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

$$\tilde{H}_\infty(\mathbf{s}|\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}) = \tilde{H}_\infty(\tilde{\mathbf{e}}|\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}})$$

Thus, it holds that

$$\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}'+\mathbf{e}) = \tilde{H}_\infty(\tilde{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}'+\mathbf{e}) \geq \tilde{H}_\infty(\tilde{\mathbf{e}}|\tilde{\mathbf{b}}=\mathbf{s}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}) = \log(|\Lambda_q(\tilde{\mathbf{A}})\bigcap V_{\tilde{\mathbf{b}}}(d)|)$$

■

We can use the Gaussian heuristic $|\Lambda_q(\tilde{\mathbf{A}})\bigcap V_{\tilde{\mathbf{b}}}(d)| \approx \mathsf{vol}(V_{\tilde{\mathbf{b}}}(d))/\det(\Lambda_q(\tilde{\mathbf{A}}))$ to estimate $\tilde{H}_\infty(\bar{\mathbf{e}}|\bar{\mathbf{e}}\mathbf{A}'+\mathbf{e})$.

4.3 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 [4]

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

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 $\frac{q}{d}\mathbb{Z}^m$.

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 $\Lambda_d(\mathbf{A}')=\{\mathbf{x}'\in\mathbb{Z}^m : \mathbf{x}'=\mathbf{s}\mathbf{A}' \mod d, \mathbf{s}\leftarrow\mathbb{Z}_d^n\}$ 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 $\mathbf{x}=\frac{q}{d}\mathbf{v}+q\cdot\mathbf{c}$.

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

4.4 Lossy model for d-ary lattices

For any $d\leq q$, we provide the corresponding result when $\mathbf{s}$ is uniformly distributed on $\mathbb{Z}_d^n$. As a compromise, the lattice $\Lambda_q(\mathbf{A})$ should also be adjusted accordingly.

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

Theorem 10 *Let q, $0 < d \leq q$, $m = O(n \log d)$ be integers. For a given matrix $\mathbf{A} \in \frac{q}{d}\mathbb{Z}^{n\times m}$, let $0 \leq \sigma \leq \frac{d}{2\sqrt{m}}$, $\mathbf{s} \leftarrow \mathbb{Z}_d^n$ and $\mathbf{e} \leftarrow \mathcal{D}_{\frac{q}{d}\mathbb{Z}^m,\sigma}$. 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 [9]. Its proof is the same as [9]; for the sake of completeness, we list it in Appendix B.

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

The work([27], Claim 5.3)proved that the hash function family $\{\mathcal{H}_G = h_{\mathbf{g}} : \mathbf{g} \in G^m\}$ is universal, where

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

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 will prove that the following hash function family is universal $\mathcal{H}_G = \{h_{\mathbf{g}} : \mathbf{g} \in G^m\}$

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

Below, we will prove Lemma 6 and then extend it 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 $g_1, \cdots, g_m \in G$, $b_i \leftarrow \mathbb{Z}_d$ and $u \leftarrow G$, 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 :

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

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 with 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 Lemma 2, 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 [30]. 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 the *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 $\mathsf{Exp}_{\mathbf{g}\leftarrow G^m}\left[\Delta(\sum_i b_i g_i, u)\right] \geq \frac{1}{2}\sqrt{\frac{q}{d^m}}$, 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, we 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

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

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, it holds that

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

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 Lemma 6, 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 $\frac{1}{a}$.

6 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.

6.1 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 $\mathsf{DLWE}_{n,m,q,\bar{\chi}}$ is defined on $\mathbb{Z}$, where $\bar{\chi}$ 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 $\mathsf{DLWE}_{n,m,d,\bar{\chi}}$ to $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$.

Claim 1 *If an adversary can distinguish the* $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ *problem with an advantage of* ϵ *in time* T*, then he can also distinguish the standard* $\mathsf{DLWE}_{n,m,d,\bar{\chi}}$ *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 $\mathsf{DLWE}_{n,m,d,\bar{\chi}}$ and $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ samples. For any given standard $\mathsf{LWE}_{n,m,d,\bar{\chi}}$ 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 $(\mathbf{A}', \mathbf{b}')$ are samples of $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$.

Therefore, for $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$, 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 $\mathsf{DLWE}_{n,m,d,\bar{\chi}}$.

■

6.2 Leakage resistance of rational LWE samples

Goldwasser et al. [20] 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 utilizes the anti-leakage property of the Leftover Hash Lemma and reduces it to low-dimensional LWE samples.

Next, we will prove that the $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ samples we defined also possess anti-leakage properties. This proof needs to utilize the regularity result of the hash function family on the prime order group (Corollary 2), and unlike [20], we need to use the *Circular Security* assumption.

Theorem 11 *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* $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ *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 the 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 Claim 1, 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 $\frac{q}{d}\mathbb{Z}_d^r$.

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

By Corollary 2, we have that the family of hash functions $\mathcal{H}_{\frac{q}{d}\mathbb{Z}_d^r}$ is universal. Furthermore, by the Leftover Hash Lemma 2, 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 [20], 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 Lemma 1. 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 [11] and the bootstrapping in [18] [13] [19]. 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).

■

7 Optimized multi-key fully homomorphic encryption scheme

Multi-key fully homomorphic encryption (MKFHE) was proposed by López-Alt *et al.* [23], 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 [16], Mukherjee and Wichs [24], Peikert and Shiehian [25] constructed the GSW type MKFHE. Chen [15] and Chen [14] constructed the MKFHE based on RLWE and applied it to privacy-preserving neural network training with multiple parties. The work [12] 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. [1] 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 goal.

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 address the above problems, Dai et al. [17] introduced the *keylifting* operation during 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 those 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 [12] [24] [2] 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 [12]. It must be pointed out that such optimization can also be applied to [16] [24] [25] [17] and other GSW-based MKFHE (constructed on $\mathbb{Z}$, can use the Leftover Hash Lemma to remove CRS). We choose [12] as an example because it requires fewer changes, and the improved result is better.

7.1 An improved "GSW-style" MKFHE based on [12]

Our optimized scheme is similar to [12], except that their scheme was based on Dual-GSW (on $\mathbb{Z}$), while ours 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, $m = n\lceil \log d \rceil$, $q = d \cdot \mathsf{poly}(\lambda)$. 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 $u_i \in \{0,1\}$, 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 $||\mathbf{eR}/\mathbf{e}'||_\infty = \mathsf{negl}(\lambda)$, $\mathbf{R} \leftarrow \{0,1\}^{m\times(n+1)l}$, $l = \lceil \log d \rceil$, $\mathbf{G}$ is a gadget matrix as defined in preliminary.
- $u \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathbf{C})$: Input ciphertext $\mathbf{C}$, private key sk, let $\mathbf{t} = \mathsf{sk}$, $\mathbf{w}^T = (0, \cdots, 0, \lfloor \frac{d}{2} \rceil \cdot \frac{q}{d}) \in \frac{q}{d}\mathbb{Z}_d^{n+1}$, $\gamma = \mathbf{t}\cdot\mathbf{C}\mathbf{G}^{-1}(\mathbf{w}^T)$, output $u = \lfloor \frac{\gamma}{q/2} \rceil$.

7.2 The encoding check

Since our improved scheme is based on $\frac{q}{d}\mathbb{Z}$, we will now describe the correctness of decryption, homomorphic addition, and multiplication. It must be pointed out that the initial ciphertext does not undergo homomorphic evaluation because it is encrypted using different public keys. It is the "expanded" ciphertext that actually undergoes homomorphic evaluation. Because the "expanded" ciphertext and the initial ciphertext maintain the same decryption paradigm: $\mathbf{tC} \approx u\mathbf{tG}$, they 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

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

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

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

where $|\Delta| < 0.5$, thus if $\langle \mathbf{eR} + \mathbf{e}', \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + \frac{q}{d}\Delta < \frac{q}{4}$, 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

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

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

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

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

Homomorphic multiplication : 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

$$\begin{aligned}\gamma = \mathbf{t}\mathbf{C}_{\mathsf{mult}}\mathbf{G}^{-1}(\mathbf{w}^T) = \langle &\mathbf{tM} + u_2\mathbf{eR}_1 + u_2\mathbf{e}_1'\\ &+ u_1\mathbf{eR}_2 + u_1\mathbf{e}_2', \quad \mathbf{G}^{-1}(\mathbf{w}^T)\rangle + u_1u_2\mathbf{tGG}^{-1}(\mathbf{w}^T)\end{aligned}$$

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

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

  it holds that $\lfloor \frac{\gamma}{q/2} \rceil = 0$
- if $u_1 = u_2 = 1$, we have :

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

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

7.3 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 the other $k-1$ parties. Under the semi-honest adversary, $\{\mathbf{A}_j\}_{j\in[k]/i}$ are uniformly distributed over $\frac{q}{d}\mathbb{Z}_d^{n\times m}$. Under the $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ assumption, Auxk_i is indistinguishable from the uniform distribution, and the security of the scheme is now obvious.

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 differ significantly. 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 sufficiently large. 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 $\mathbf{c}_1 = \mathbf{s}_i\mathbf{A}_i\mathbf{R} + \mathbf{eR} + \mathbf{e}' = \mathbf{s}_i\mathbf{C}_0 + \mathbf{eR} + \mathbf{e}'$. By our parameter settings, we have $||\mathbf{eR}/\mathbf{e}'|| = \mathsf{negl}(\lambda)$, 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 Theorem 11, 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 Theorem 10, 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 Lemma 5, 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 [2] 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 [2] constructed the Unbounded MPC protocol and used it against semi-malicious receivers). Thus it holds that :

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

where $\mathbf{B}_i \leftarrow \frac{q}{d}\mathbb{Z}_d^{\frac{n}{2}\times m}$, $\mathbf{S} \leftarrow \mathbb{Z}_d^{\frac{n}{2}\times\frac{n}{2}}$, $\mathbf{E}_i \leftarrow \bar{\chi}^{\frac{n}{2}\times m}$, $\bar{\chi}$ is defined over $\frac{q}{d}\mathbb{Z}$ with standard deviation $\bar{\sigma}$ satisfying $\sqrt{m(k-1)} \cdot \bar{\sigma} \leq \gamma$. Thus, $\mathsf{rank}(\Lambda_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$. Let $\sigma > 4\gamma$, 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 rational-$\mathsf{DLWE}_{\frac{n}{2},m,d,q,\bar{\chi}}$, $\bar{\mathbf{A}}$ looks random.

Put things together : We bring together the previous parameter requirements, in particular, the range of standard deviations for several discrete Gaussian distributions. By Theorem 10, 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 Lemma 7, 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 $[-2^\lambda\sigma, 2^\lambda\sigma]$.

7.4 Ciphertext expansion

In order to convert the ciphertext under different keys into ciphertext under the same key, the GSW-type ciphertext needs to undergo a "ciphertext expansion" operation. The private key corresponding to the expanded ciphertext is the concatenation of private keys. A typical ciphertext expansion was the masking scheme defined in [24] [26] [16] : 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 applies the homomorphic property of the GSW scheme to output the ciphertext $\mathbf{X} \in \mathbb{Z}_q^{(n+1)\times(n+1)l}$ of $\mathbf{vR}$ under $\mathbf{t}$(satisfying $\mathbf{tX} \approx \mathbf{vR}$), where the function of $\mathbf{X}$ is to eliminate the redundant items produced by decrypting $\mathbf{C}$ with the 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 that our scheme is defined over $\frac{q}{d}\mathbb{Z}$). Below, for the sake of completeness, we informally describe the process of ciphertext expansion.

A masking scheme for GSW ciphertext (defined in [24] [16] adapted to our scheme) : There exist a pair of algorithm (UniEnc, Extend)

- UniEnc(u, pk) : On input a message $u \in \{0,1\}$ 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 $\mathcal{U} \in \{0,1\}^*$
- 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 $u_{i,j} \in \{0,1\}$ 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 : $\bar{\mathbf{t}} \cdot \mathbf{C}_{\mathsf{mult}} \approx u_1u_2\bar{\mathbf{t}}\bar{\mathbf{G}}$

Accumulation of noise : 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 :

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

Therefore, the initial noise $||\mathbf{e}_{\mathsf{init}}||_\infty$ obtained by decrypting $\bar{\mathbf{C}}_1$ is bounded by $(m + (n+1)^4 l^4)B_\chi + B_{\chi'}$. 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 [19], 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 $\bar{\mathbf{w}}^T = (0, \cdots, 0, \lfloor \frac{d}{2} \rceil \cdot \frac{q}{d}) \in \frac{1}{d}\mathbb{Z}_d^{k(n+1)}$, we have:

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

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

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

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) $\leq \frac{q}{4}$.

7.5 Comparison

The main distinction between our optimized scheme and the scheme [12] is similar to the difference between the GSW scheme and the Dual-GSW scheme. Furthermore, the sizes of the key and ciphertext in their schemes are related to k. Furthermore, we have a smaller key and ciphertext size and computation compared to the scheme [24], noting that $d = q/\mathsf{poly}(\lambda)$. The computation complexity of our scheme is proportional to k^3. The communication complexity in the setup phase is independent of k. The total communication amount should be the ciphertext size multiplied by the input length of the circuit.

Table 2: Complexity

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

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. 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)
2. 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)

3. 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)
4. 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)
5. Attrapadung, N., Hanaoka, G., Hiromasa, R., Matsuda, T., Schuldt, J.C.: Maliciously circuit-private multikey fhe and mpc based on lwe. Designs, Codes and Cryptography pp. 1–40 (2022), https://doi.org/10.1007/s10623-022-01160-x
6. 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)
7. 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)
8. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen 296, 625–635 (1993)
9. 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)
10. 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)
11. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: Goldwasser, S. (ed.) ITCS 2012. pp. 309–325. ACM (Jan 2012)
12. 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)
13. 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)
14. 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)
15. 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)
16. 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)
17. 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
18. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Mitzenmacher, M. (ed.) 41st ACM STOC. pp. 169–178. ACM Press (May / Jun 2009)
19. 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)
20. 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)
21. 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)
22. 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)
23. 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)
24. 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)
25. 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)
26. Peikert, C., Shiehian, S.: Multi-key FHE from LWE, revisited. Cryptology ePrint Archive, Report 2016/196 (2016), https://eprint.iacr.org/2016/196
27. 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)
28. Reyzin, L.: Extractors and the leftover hash lemma. Lecture notes, available at https://www.cs.bu.edu/~reyzin/teaching/s11cs937/notes-leo-1.pdf

29. Vadhan, S.P.: Pseudorandomness. Foundations and Trends® in Theoretical Computer Science 7(1–3), 1–336 (2012), http://dx.doi.org/10.1561/0400000010
30. Xagawa, K.: Cryptography with lattices. Ph.D. thesis (2010), available at http://xagawa.net/pdf/2010Thesis.pdf
31. 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

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, the number of red dot marks in each book would be less than $\frac{N}{3}$. This would result in the total number of red dot marks in the library being less than $\frac{NB}{3}$, which leads to a contradiction. ■

B The proof of Theorem 10

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 $\mathbf{A}$ and $\mathbf{y}$, $\sum_{\mathbf{s}'} \Pr[\mathbf{e} = \mathbf{y} - \mathbf{s}'\mathbf{A}]$ 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 Theorem 5, it holds that $\Pr[\mathbf{s} = \mathbf{s}^* | \mathbf{y} = \mathbf{sA} + \mathbf{e}] = \Pr[\mathbf{e} \mod q \in V]$. By Theorem 6, it holds that $||\mathbf{e}|| \leq \frac{q}{d} \cdot \sigma \cdot \sqrt{m} < q/2$ except with probability 2^{-m}, thus $\Pr[\mathbf{e} \mod q \in V] \leq \Pr[\mathbf{e} \in V] + 2^{-m}$. By Lemma 4, 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 :

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

■