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,chenjingwei,wuwenyuan,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 $\mathbf{s}$, where $\mathbf{A}$ is chosen by the adversary. 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 application of the above results, we improved the multi-key fully homomorphic encryption [6] 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) [18], Threshold fully homomorphic encryption (ThFHE) and Multi-key fully homomorphic encryption (MKFHE) [13] 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

T. Zhu and Y. Li (Eds.): ACISP 2024, LNCS 14896, pp. 44–63, 2024.
https://doi.org/10.1007/978-981-97-5028-3_3

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 [6], 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 [4], 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 [1] 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 [6], assuming there are k parties, in order to support subsequent *ciphertext 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 $\{\mathbf{b}_i = \mathbf{sA}_i\}_{i\in[k-1]}$ 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 $\{\mathbf{b}_i = \mathbf{sA}_i\}_{k-1}$, the leakage in the worst case was estimated. For $\mathbf{b}_i \in \mathbb{Z}_q^n$, $\{\mathbf{b}_i = \mathbf{sA}_i\}_{i\in[k-1]}$ leaks $\mathbf{s}$ with a maximum of $(k-1)n\log q$ bits. According to the proof in [6], 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 at least satisfy $m - (k-1)n\log q \geq \log q + 2\lambda$.

In [4], 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 [4] 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? One method is to bit-decomposition the key before encrypting it. For example, the work [8,12] adopt binary key to fill into the plaintext space in order to realize bootstrapping more quickly and control the growth of noise. Another approach is to limit the norm of the $\mathbf{s}$ to a small range. Therefore, [2] reduced the LWE samples with discrete Gaussian secrets to the LWE samples with uniform secrets. MKFHE scheme [7] 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, [17] proved that Regev's encryption scheme is leakage-resilient when the private key $\mathbf{s}$ is taken from a small uniform range. The work [17] only provided a reduction for $\mathbf{s} \in \{0,1\}^*$, but the result holds for all sufficiently small $\mathbf{s}$. In addition, the paper [1] utilizes the result of [4] 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 [6], resulting in shorter keys and smaller ciphertexts. We present our results in the following section.

1.2 Our Results

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

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

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

For LWE samples whose secrets and noise are sampled from bounded uniform distribution, we have the following result.

Theorem 2. *Let n, q, d, $m = O(n \log q)$ and $d < q$ be integers. For a given matrix $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m}$, let $\mathbf{t} \leftarrow \mathbb{Z}_q^n, \mathbf{s} \leftarrow \mathbb{Z}_d^n, \mathbf{e} \leftarrow \mathbb{Z}_d^m, \bar{\mathbf{b}} = \mathbf{t}\bar{\mathbf{A}} - \mathbf{s}$, $\mathbf{b} = \mathbf{tA} + \mathbf{e}$, $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$. It holds that*

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

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

For the LWE samples whose secrets are sampled from bounded uniform distribution while noise are sampled from discrete Gaussian distribution, we present a more general results of Lemma 3.2 in [4] (Lemma 3.2 is a special case of our Theorem 3).

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*

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

Clearly, when $d = q$, the above Theorem degenerates to Lemma 3.2 in [4]. 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) in the full version [10] of this work. 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 [6]. In particular, combined with the proof trick of [17] for the LWE variant of binary keys, we provide a positive answer to the question raised at the end of [6]: the ciphertext of our improved scheme is constructed in a GSW-like manner, rather than Dual GSW. In addition, compared with [6] and [14], our ciphertext and key are shorter, as shown in Table 1.

Table 1. Complexity

Scheme	Key size	Ciphertext size	Hom-multiplication	Communication in setup	Setup
[14]	$O(n^2 \log^2 q)$	$O(n^2 \log^2 q)$	$O(k^3 n^3 \log^2 q)$	-	CRS
[6]	$O(kn^2 \log^2 q)$	$O(k^2 n^2 \log^4 q)$	$O(k^6 n^3 \log^5 q)$	$O(kn^2 \log^2 q)$	-
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-multiplication 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 [5] 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 [17], which proved that when the key $\mathbf{s}$ is taken from $\{0, 1\}$, and $\tilde{H}_\infty(\mathbf{s})$ is large enough, the binary LWE is anti-leakage). We must point out that our work is dedicated to characterizing the lower bound of $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$, where $\mathbf{A}$ may not be uniformly distributed. This 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.

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 $\mathbf{GG}^{-1}(\mathbf{M}) = \mathbf{M}$.

Average Conditional Min-Entropy (in [4]). 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

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

2.2 Some Result on the Lattice

Theorem 4. *Let Λ be a lattice, V be the Voronoï-cell of Λ, $\mathbf{t}, \mathbf{t}'$ are two vectors in span(Λ), 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* $\mathbf{t}$.

Theorem 5 (in [3]). *For any lattice $\Lambda \in \mathbb{R}^m$, parameter $\sigma > 0$ and $u \geq \frac{1}{\sqrt{2\pi}}$ it holds that*

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

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

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

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

Theorem 6 (The Gaussian Heuristic). *Let $\mathcal{L}$ be a random lattice, for all sufficiently large $S \subset \mathbb{R}^n$, it holds that*

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

2.3 Leakage Model

The concept of leakage models evolved from leakage-resistant encryption. Anti-leakage encryption focuses on the semantic security of ciphertext when the key is lossy. It mainly prevents side-channel attacks and is of great significance to the specific implementation of cryptographic schemes. The leakage model mainly quantifies the lower bound of the conditional entropy of key $\mathbf{s}$ in various leakage scenarios, which is a precondition for leakage-resistant encryption. There are currently two main leakage models. One is a hash function-like leakage model $\mathbf{s}|\mathbf{sA}$ introduced by [17], where $\mathbf{A}$ is generated by the adversary, $\mathbf{s} \leftarrow \{0,1\}^*$. The other is the LWE-like leakage model $\mathbf{s}|\mathbf{sA} + \mathbf{e}$ introduced by [4], where A is generated by the adversary, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$.

2.4 Learning with Errors

The Learning With Errors (LWE) problem was introduced by Regev [16]. In general, we are primarily interested in its decision version.

Definition 1 (Decision-LWE). *For $n, m, q \in \mathbb{N}$ and for a distribution χ supported over $\mathbb{Z}$, the $\mathsf{DLWE}_{n,m,q,\chi}$ 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 $\mathsf{DLWE}_{n,m,q,\chi}$ for any $m = \mathsf{poly}(n \log q)$. The matrix version of this problem ask to distinguish $(\mathbf{A}, \mathbf{SA} + \mathbf{E})$ from $(\mathbf{A}, \mathbf{U})$ where $\mathbf{S} \leftarrow \mathbb{Z}_q^{k\times m}$, $\mathbf{E} \leftarrow \chi^{k\times m}$ and $\mathbf{U} \leftarrow \mathbb{Z}_q^{k\times m}$, whose hardness for any $k = \mathsf{poly}(n)$ can be established from $\mathsf{DLWE}_{n,m,q,\chi}$ via a routine hybrid-argument.

As shown in Regev [16], for certain module q and discrete Gaussian error distribution χ with parameter $\sigma = \alpha q \geq 2\sqrt{n}$, the $\mathsf{DLWE}_{n,m,q,\chi}$ is true as long as certain worst-case lattice problem is hard to solve using a quantum algorithm.

2.5 Road-Map

In Sect. 3, we outline our approach and techniques. In Sect. 4, we proved a more general result for $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$. In Sect. 5, 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 2.1

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

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 [4] notes that when $\mathbf{s}$ is uniformly chosen from $\mathbb{Z}_q^n$, by Bayes' rule,

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

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 Fig. 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 $\Pr(\mathbf{e}\in V) < \frac{1}{\rho_\sigma(\Lambda_q(\mathbf{A}))}$ [4], when $\mathbf{s}$ is drawn from the discrete Gaussian distribution, we can quantify the conditional entropy of $\mathbf{s}$.

LWE with Bounded Uniform Secrets and Noise. Let $d<q$ be an integer, when the secret $\mathbf{s}$ is sampled uniformly from $\mathbb{Z}_d^n$. We cannot apply the above method directly. This is because $\mathbf{sA} \mod q$ cannot traverse all lattice points. Let

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

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 Fig. 2, we interpret it in a two-dimensional lattice.

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 [4] to obtain the $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}+\mathbf{e})$ lower bound. This is because $\mathbf{sA} \mod q$ does not necessarily traverse all the lattice points when limiting $\mathbf{s}$ to a small range. This is the challenge of determining the

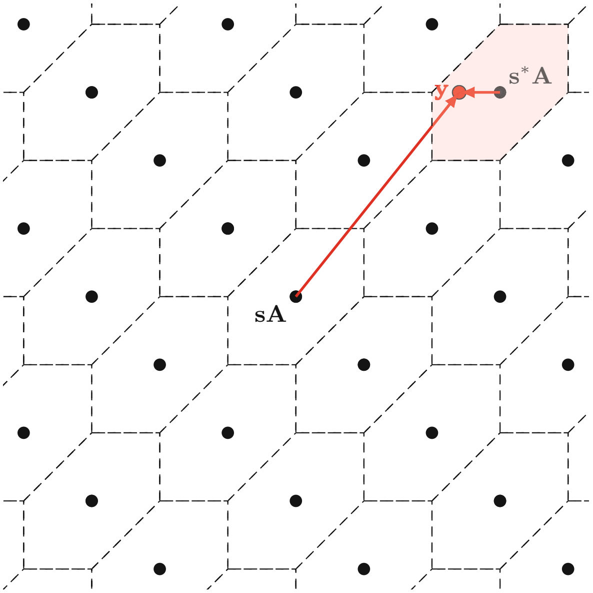

Fig. 1. $\mathbf{s}^*\mathbf{A}$ is the lattice point closest to $\mathbf{y}$, at this time, $\mathbf{e}^*$ happens to fall in the *Voronoï cell* of $\mathbf{s}^*\mathbf{A}$

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.

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

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 and Discrete Gaussian Noise. 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 $\mathbb{Z}_d^n$ and $\mathbf{e}$ is sampled from discrete Gaussian distribution.

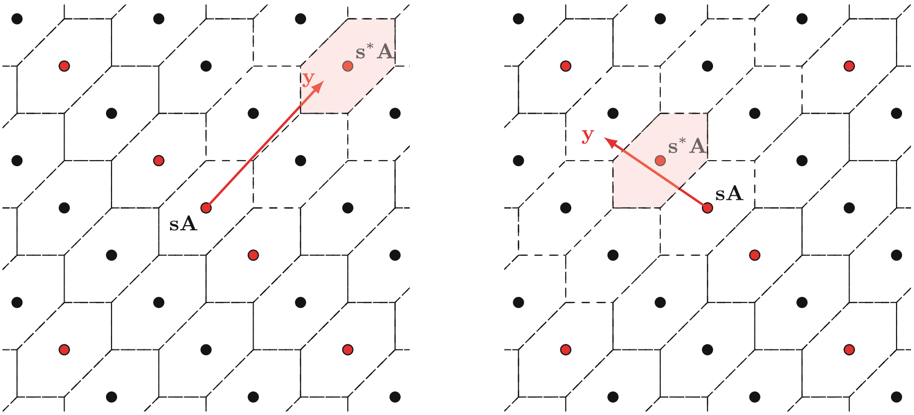

Fig. 2. Cases of the nearest point to $\mathbf{y}$: Red points are in S. The left panel shows that the closest point to $\mathbf{y}$ is on S, but the right panel clearly shows that the closest point to $\mathbf{y}$ is not on S. (Color figure online)

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 [4].

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. It is actually a d-ary lattice defined over $\frac{q}{d}\mathbb{Z}^m$. Therefore, for such a lattice, 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 above three results tell us that when $\mathbf{A}$ is generated by an adversary, how much entropy of $\mathbf{s}$ remains after $\mathbf{sA} + \mathbf{e}$ is disclosed. When $\mathbf{s}$ is lossy, in order to prove that the ciphertext generated by $\mathbf{s}$ is semantically secure, it is further necessary to prove the regularity of the hash function mapped to the prime-order group. In this way, we can convert the LWE sample with lossy secret $\mathbf{s}$ into a low-dimensional LWE sample (need to introduce the circular security assumption). We use Theorem 3 to characterize the conditional entropy of $\mathbf{s}$ because when $\mathbf{s}$ is taken from a discrete Gaussian distribution, we do not know how to prove the regularity of the hash function defined by it. This explains why our scheme is constructed on $\frac{q}{d}\mathbb{Z}$.

The improvement on the MKFHE scheme [6] 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 [17] 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). We give the proof in the full version of this work [10]. Therefore, we can still use the GSW type to construct MKFHE.

4 Lattice-Based, More General Anti-leakage Model

In Sect. 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 Sect. 4.2, we consider the case when $\mathbf{s}$ is drawn from a bounded uniform distribution. In Sect. 4.3, we describe a lattice contained in $\frac{q}{d}\mathbb{Z}^m$, then in Sect. 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 [4]. At this time, we need to use the reduction technique [2] from the LWE with discrete Gaussian secrets to the LWE with uniform secrets.

Consider the following game

- Alice picks matrix $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m}$, where $\bar{\mathbf{A}}$ is invertible, sends $\tilde{\mathbf{A}}$ it to Bob.
- After receiving $\tilde{\mathbf{A}}$, Bob generates $\mathbf{t} \leftarrow \mathbb{Z}_q^n$, $\mathbf{s} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$, $\bar{\mathbf{b}} = \mathbf{t}\bar{\mathbf{A}} - \mathbf{s}$, $\mathbf{b} = \mathbf{tA} + \mathbf{e}$, $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, 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 $(\mathbf{A}', \mathbf{b}' = \mathbf{sA}' + \mathbf{e})$ are the LWE samples with discrete Gaussian secrets, but $\mathbf{A}'$ may not be uniform because $\tilde{\mathbf{A}}$ is chosen by Alice. Now, we quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}' + \mathbf{e})$.

Theorem 7. *Let n, q, $m = O(n \log q)$ be integers, and $0 < \sigma < \frac{q}{2\sqrt{m+n}}$. For the given matrix $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m}$, where $\bar{\mathbf{A}}$ is invertible, let $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, $\mathbf{s} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$. It holds that*

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

Proof. Let $\tilde{\mathbf{e}} = (-\mathbf{s}, \mathbf{e})$, $\mathbf{t} \leftarrow \mathbb{Z}_q^n$, $\bar{\mathbf{b}} = \mathbf{t}\bar{\mathbf{A}} - \mathbf{s}$, $\mathbf{b} = \mathbf{t}\mathbf{A} + \mathbf{e}$, $\tilde{\mathbf{b}} = (\bar{\mathbf{b}}, \mathbf{b})$. According to the definition of average min-entropy, we have

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

Obviously, $\tilde{\mathbf{e}}$ that maximizes the conditional probability $\Pr[\tilde{\mathbf{e}} = \tilde{\mathbf{e}}^*|\tilde{\mathbf{b}} = \mathbf{t}\tilde{\mathbf{A}} + \tilde{\mathbf{e}}]$ must fall in the *Voronoï cell* of the lattice point that nearest to $\tilde{\mathbf{b}}$, that is $\tilde{\mathbf{e}}^* = \tilde{\mathbf{b}} - \mathbf{t}^*\tilde{\mathbf{A}}$ ($\mathbf{t}^*\tilde{\mathbf{A}}$ is the nearest lattice point to $\tilde{\mathbf{b}}$). By Theorem 4, it holds that $\Pr[\tilde{\mathbf{e}} = \tilde{\mathbf{e}}^*|\tilde{\mathbf{b}} = \mathbf{t}\tilde{\mathbf{A}} + \tilde{\mathbf{e}}] = \Pr[\tilde{\mathbf{e}} \mod q \in V]$, where $V \in \mathbb{Z}^{m+n}$ is the discretized *Voronoï cell* of $\Lambda_q(\tilde{\mathbf{A}})$. By Theorem 5, 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 the Lemma 3.1 in [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

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

Because $\mathbf{A}'$ is public, thus $\tilde{H}_\infty(\mathbf{e}|(-\mathbf{s}, \mathbf{s}\mathbf{A}' + \mathbf{e})) = 0$. By the chain rule, we have

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

Combining (2), (3) we have

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

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

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

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

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

■

4.2 The Leakage-Resilient of LWE Samples with Bounded Uniform Secrets and Noise

In this section, we first define the problem of distinguishing between LWE samples and uniform distributions where the secret and noise are taken from a bounded uniform distribution. It is no less hard than distinguishing standard LWE samples and uniform distribution (we give the proof in the full version [4]). Then we consider the anti-leakage properties of such LWE samples.

Definition 2. *Let n, m, q be integers, χ be the noise distribution in the standard problem $\mathsf{DLWE}_{n,m,q,\chi}$ bounded by B_χ. Let λ be the security parameter, $d \leq q$ be an integer, satisfying $\frac{B_\chi}{d} = \mathsf{negl}(\lambda)$. The $\mathsf{Bounded\text{-}DLWE}_{n,m,d,q,\chi}$ problem is to distinguish the following distribution*

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

Consider the following game

- Alice picks matrix $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m}$, where $\bar{\mathbf{A}}$ is invertible, sends $(\mathbf{A}, \bar{\mathbf{A}})$ it to Bob.
- After receiving $\tilde{\mathbf{A}}$, Bob generates $\mathbf{t} \leftarrow \mathbb{Z}_q^n$, $\mathbf{s} \leftarrow \mathbf{Z}_d^n$, $\mathbf{e} \leftarrow \mathbb{Z}_d^m$, $\bar{\mathbf{b}} = \mathbf{t}\bar{\mathbf{A}} - \mathbf{s}$, $\mathbf{b} = \mathbf{tA} + \mathbf{e}$, $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$, sends $(\mathbf{A}', \mathbf{b}' = \mathbf{b} + \bar{\mathbf{b}}\mathbf{A}')$ to Alice.

Apparently $(\mathbf{A}', \mathbf{b}' = \mathbf{sA}' + \mathbf{e})$. The above game essentially transforms the LWE samples with bounded noise to the LWE samples with bounded secrets, but $\mathbf{A}'$ may not be uniform since $\tilde{\mathbf{A}}$ is chosen by Alice. Now, we quantify $\tilde{H}_\infty(\mathbf{s}|\mathbf{sA}' + \mathbf{e})$.

Theorem 8. *Let n, q, d, $m = O(n \log q)$ be integers. For a given matrix $\tilde{\mathbf{A}} = (\bar{\mathbf{A}}, \mathbf{A}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m}$, let $\mathbf{t} \leftarrow \mathbb{Z}_q^n, \mathbf{s} \leftarrow \mathbb{Z}_d^n, \mathbf{e} \leftarrow \mathbb{Z}_d^m, \bar{\mathbf{b}} = \mathbf{t}\bar{\mathbf{A}} - \mathbf{s}$, $\mathbf{b} = \mathbf{tA} + \mathbf{e}$, $\mathbf{A}' = -\bar{\mathbf{A}}^{-1}\mathbf{A}$. It holds that*

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

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

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

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

By Bayes's rule, we have

$$\begin{aligned}
&\Pr_{\mathbf{t},\tilde{\mathbf{e}}}[\mathbf{t}=\mathbf{t}^*|\tilde{\mathbf{b}}=\mathbf{t}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}] = \Pr_{\mathbf{t},\tilde{\mathbf{e}}}\left[\tilde{\mathbf{b}}=\mathbf{t}\tilde{\mathbf{A}}+\tilde{\mathbf{e}} \mid \mathbf{t}=\mathbf{t}^*\right]\cdot\frac{\Pr\left[\mathbf{t}=\mathbf{t}^*\right]}{\Pr_{\mathbf{t},\tilde{\mathbf{e}}}[\tilde{\mathbf{b}}=\mathbf{t}\tilde{\mathbf{A}}+\tilde{\mathbf{e}}]}\\
&=\Pr_{\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{t}^*\tilde{\mathbf{A}}\right]\cdot\frac{\Pr\left[\mathbf{t}=\mathbf{t}^*\right]}{\sum_{\mathbf{t}'}\Pr_{\tilde{\mathbf{e}}}\left[\tilde{\mathbf{b}}=\mathbf{t}\tilde{\mathbf{A}}+\tilde{\mathbf{e}} \mid \mathbf{t}=\mathbf{t}'\right]\Pr\left[\mathbf{t}=\mathbf{t}'\right]}\\
&=\Pr_{\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{t}^*\tilde{\mathbf{A}}\right]\cdot\frac{d^{-n}}{\sum_{\mathbf{t}'}\Pr_{\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{t}\tilde{\mathbf{A}}\right]\cdot d^{-n}}\\
&=\frac{\Pr_{\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{t}^*\tilde{\mathbf{A}}\right]}{\sum_{\mathbf{t}'}\Pr_{\tilde{\mathbf{e}}}\left[\tilde{\mathbf{e}}=\tilde{\mathbf{b}}-\mathbf{t}'\tilde{\mathbf{A}}\right]}=\frac{1}{|\Lambda_q(\tilde{\mathbf{A}})\bigcap V_{\tilde{\mathbf{b}}}(d)|}
\end{aligned}$$

Thus, we have

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

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

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

Thus, it holds that

$$\tilde{H}_\infty(\mathbf{s}|\mathbf{s}\mathbf{A}'+\mathbf{e})=\tilde{H}_\infty(\tilde{\mathbf{e}}|\mathbf{s}\mathbf{A}'+\mathbf{e})\geq\tilde{H}_\infty(\tilde{\mathbf{e}}|\tilde{\mathbf{b}}=\mathbf{t}\tilde{\mathbf{A}}+\tilde{\mathbf{e}})=\log(|\Lambda_q(\tilde{\mathbf{A}})\bigcap V_{\tilde{\mathbf{b}}}(d)|)$$

■

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

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[1]

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

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 $\mathbf{A}\in\frac{q}{d}\mathbb{Z}^{n\times m}$,

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

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 The Leakage-Resilient of LWE Samples with Bounded Uniform Secrets and Gaussian Noise

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

Theorem 9. *Let q, $0 < d \le q$, $m = O(n\log d)$ be integers. For a given matrix $\mathbf{A} \in \frac{q}{d}\mathbb{Z}^{n\times m}$, let $0 \le \sigma \le \frac{d}{2\sqrt{m}}$, $\mathbf{s} \leftarrow \mathbb{Z}_d^n$ and $\mathbf{e} \leftarrow \mathcal{D}_{\frac{q}{d}\mathbb{Z}^m,\sigma}$. It holds that*

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

If $d = q$, the above Theorem degenerates into Lemma 3.2 in [4]. Its proof is the same as [4]; for the sake of completeness, we list it in Appendix A.

5 Optimized Multi-key Fully Homomorphic Encryption Scheme

As an application of our result in the previous section, we give an optimized MKFHE scheme based on [6]. It must be pointed out that such optimization can also be applied to [9,11,14,15] and other GSW-based MKFHE (constructed on $\mathbb{Z}$, can use the Leftover Hash Lemma to remove CRS). We choose [6] as an example because it requires fewer changes, and the improved result is better.

5.1 An Improved "GSW-Style" MKFHE Based on [6]

Our optimized scheme is similar to [6], 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 $\mathbf{s}|\mathbf{s}\mathbf{A}$, while ours is $\mathbf{s}|\mathbf{s}\mathbf{A} + \mathbf{e}$. 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 the $\mathsf{rational\text{-}DLWE}_{n,m,d,q,\chi}$ problem (Definition 7 in [10]) 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 $u = \lfloor\frac{\gamma}{q/2}\rceil$.

5.2 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

Theorem 10. *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 the Theorem 11 in the full version [10], 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 9, if $0 < \sigma < \frac{d}{2\sqrt{m(k-1)}}$ we have

$$\tilde{H}_\infty(\mathbf{s}_i|\mathbf{s}_i\bar{\mathbf{A}} + \bar{\mathbf{e}}) \geq -\log(\frac{1}{\rho_\sigma(\mathit{\Lambda}_q(\bar{\mathbf{A}}))} + 2^{-m(k-1)}) \tag{6}$$

Let $\gamma > 0$ be real, $\mathcal{B}$ be a sphere of radius 1, by the Lemma 4.3 in [4], if $\mathsf{rank}(\mathit{\Lambda}_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$ and $\sigma > 4\gamma$, it holds that $\rho_\sigma(\mathit{\Lambda}_q(\bar{\mathbf{A}})) > 2^{n+2}$ (satisfying $\frac{1}{\rho_\sigma(\mathit{\Lambda}_q(\bar{\mathbf{A}}))} \leq 2^{-n} - 2^{m(k-1)}$, thus $\tilde{H}_\infty(\mathbf{s}_i|\{\mathbf{b}_{i,j}\}_{j\in[k]/i}) \geq n$). We observe from [1] that one way to satisfy $\mathsf{rank}(\mathit{\Lambda}_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$ is to make $\bar{\mathbf{A}}$ have structure as

$$\bar{\mathbf{A}} = \begin{pmatrix} \mathbf{B}_2 & \mathbf{B}_3 & \cdots & \mathbf{B}_k \\ \mathbf{S}\mathbf{B}_2 + \mathbf{E}_2, & \mathbf{S}\mathbf{B}_3 + \mathbf{E}_3, & \cdots, & \mathbf{S}\mathbf{B}_k + \mathbf{E}_k \end{pmatrix}$$

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 it holds that

$$\begin{pmatrix} \mathbf{I} & \\ \mathbf{S} & \mathbf{I} \end{pmatrix}^{-1} \cdot \bar{\mathbf{A}} = \begin{pmatrix} \mathbf{B}_2, \mathbf{B}_3, \cdots, \mathbf{B}_k \\ \mathbf{E}_2, \mathbf{E}_3, \cdots, \mathbf{E}_k \end{pmatrix} \in \mathit{\Lambda}_q(\bar{\mathbf{A}})$$

Thus, $\mathsf{rank}(\mathit{\Lambda}_q(\bar{\mathbf{A}}) \bigcap \gamma\mathcal{B}) \geq \frac{n}{2}$. 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 $\mathsf{rational\text{-}DLWE}_{\frac{n}{2},m,d,q,\bar{\chi}}$ assumption, $\bar{\mathbf{A}}$ 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 9, for (6) 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 Theorem 10, we require $||\mathbf{eR}/\mathbf{e}'||_\infty = \mathsf{negl}(\lambda)$. To sum up, we get the parameters of $\bar{\chi}$ and χ respectively as follows

$$\bar{\sigma} > 2\sqrt{n}, \quad 8\sqrt{mn(k-1)} < \sigma < \frac{d}{2\sqrt{m(k-1)}} \tag{7}$$

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

5.3 Comparison

The main distinction between our optimized scheme and the scheme [6] 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 [14], 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).

Table 2. Complexity

Scheme	Key size	Ciphertext size	Hom-multiplication	Communication in setup	Setup
[14]	$O(n^2 \log^2 q)$	$O(n^2 \log^2 q)$	$O(k^3 n^3 \log^2 q)$	-	CRS
[6]	$O(kn^2 \log^2 q)$	$O(k^2 n^2 \log^4 q)$	$O(k^6 n^3 \log^5 q)$	$O(kn^2 \log^2 q)$	-
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-multiplication 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.

Acknowledgement. The authors would like to thank anonymous reviewers for their helpful comments and suggestions. This study was funded by Academicians in Chongqing lead the scientific and technological innovation guidance project (2022YSZX-JCX0011CSTB, CSTB2023YSZX-JCX0008), Key scientific issues of the Ministry of Science and Technology on transformative technologies (2020YFA0712300), Chongqing Natural Science Foundation (cstc2021jcyj-msxmX0821), Chongqing Talents Plan Youth Top-Notch Project (2021000263), Western Young Scholars Program of CAS.

Appendix

A The Proof of Theorem 9

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

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

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 4, it holds that $\Pr[\mathbf{s} = \mathbf{s}^*|\mathbf{y} = \mathbf{sA} + \mathbf{e}] = \Pr[\mathbf{e} \mod q \in V]$. By Theorem 5, 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 the Lemma 3.1 in [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

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

■

References

1. Ananth, P., Jain, A., Jin, Z., Malavolta, G.: Unbounded multi-party computation from learning with errors. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12697, pp. 754–781. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77886-6_26
2. 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 (2009). https://doi.org/10.1007/978-3-642-03356-8_35
3. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Math. Ann. **296**, 625–635 (1993)

4. Brakerski, Z., Döttling, N.: Two-message statistically sender-private OT from LWE. In: Beimel, A., Dziembowski, S. (eds.) TCC 2018. LNCS, vol. 11240, pp. 370–390. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03810-6_14
5. Brakerski, Z., Döttling, N.: Hardness of LWE on general entropic distributions. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12106, pp. 551–575. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45724-2_19
6. Brakerski, Z., Halevi, S., Polychroniadou, A.: Four round secure computation without setup. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10677, pp. 645–677. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70500-2_22
7. Chen, H., Dai, W., Kim, M., Song, Y.: Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, pp. 395–412. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3319535.3363207
8. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: Faster fully homomorphic encryption: bootstrapping in less than 0.1 seconds. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 3–33. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_1
9. Clear, M., McGoldrick, C.: Multi-identity and multi-key leveled FHE from learning with errors. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 630–656. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_31
10. Dai, X., Chen, J., Wu, W., Feng, Y.: Lattice-based, more general anti-leakage model and its application in decentralization. Cryptology ePrint Archive, Paper 2023/699 (2023). https://eprint.iacr.org/2023/699
11. 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
12. Ducas, L., Micciancio, D.: FHEW: bootstrapping homomorphic encryption in less than a second. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 617–640. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_24
13. López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, STOC 2012, pp. 1219–1234. Association for Computing Machinery, New York (2012). https://doi.org/10.1145/2213977.2214086
14. Mukherjee, P., Wichs, D.: Two round multiparty computation via multi-key FHE. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 735–763. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_26
15. Peikert, C., Shiehian, S.: Multi-key FHE from LWE, revisited. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 217–238. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_9
16. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6) (2009). https://doi.org/10.1145/1568318.1568324
17. Shafi, G., Yael, K., Chris, P., Vinod, V.: Robustness of the learning with errors assumption. In: Gennaro, R., Robshaw, M. (eds.) Innovations in Computer Science, pp. 230–240 (2010)
18. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science, SFCS 1982, pp. 160–164 (1982)