entropy

MDPI

*Article*

# Random Integer Lattice Generation via the Hermite Normal Form

**Gengran Hu [1,2,*], Lin You [1], Liang Li [1], Liqin Hu [1] and Hui Wang [1]**

[1] School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China; mryoulin@gmail.com (L.Y.); liangli@hdu.edu.cn (L.L.); huliqin@hdu.edu.cn (L.H.); h.wang@hdu.edu.cn (H.W.)

[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

* Correspondence: grhu@hdu.edu.cn

**Abstract:** Lattices used in cryptography are integer lattices. Defining and generating a "random integer lattice" are interesting topics. A generation algorithm for a random integer lattice can be used to serve as a random input of all the lattice algorithms. In this paper, we recall the definition of the random integer lattice given by G. Hu et al. and present an improved generation algorithm for it via the Hermite normal form. It can be proven that with probability $\geq$0.99, this algorithm outputs an $n$-dim random integer lattice within $O(n^2)$ operations.

**Keywords:** random integer lattice; Hermite normal form; generation algorithm



**Citation:** Hu, G.; You, L.; Li, L.; Hu, L.; Wang, H. Random Integer Lattice Generation via the Hermite Normal Form. *Entropy* **2021**, *23*, 1509. https://doi.org/10.3390/e23111509

Academic Editor: T. Aaron Gulliver

Received: 27 August 2021
Accepted: 10 November 2021
Published: 14 November 2021



## 1. Introduction

Lattices are discrete subgroups in $\mathbb{R}^n$. Since Ajtai's discovery of the average-case/worst-case connection in lattice problems [1], lattice-based cryptography has attracted much attention [2–5]. Up to now, lattice-based cryptographic schemes have been considered to be a promising alternative to more traditional ones based on the factoring and discrete logarithm problems since lattice-based schemes can be resistant to efficient quantum algorithms [6]. Lattice algorithms such as LLL [7] and BKZ [8,9] are commonly used in analyzing these lattice-based schemes' security. The lattices used in cryptography and lattice algorithms are integer lattices (discrete subgroups of $\mathbb{Z}^n$). Thus, the problem of suitably defining and generating a random integer lattice is a meaningful topic. In [10], P. Q. Nguyen found that for dimensions up to 50, LLL almost outputs the shortest lattice vector, while in theory, LLL's output is just an approximately short vector. Once we are able to generate a random integer lattice, such a generation algorithm can be used to serve as a random input for all lattice algorithms to obtain their output qualities on average.

In [1], M. Ajtai defined a family of "random integer lattices" in terms of the worst-case to average-case connection and showed how to generate one from this lattice family. For uniform $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the lattice family is defined as $\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{Ax} \in \mathbb{Z}^m : \mathbf{Ax} = \mathbf{0} \in \mathbb{Z}_q^n\}$. In [10], P. Q. Nguyen and D. Stehle gave a definition of the "random integer lattice" in the sense of the Haar measure, which was approximated by the Goldstein–Mayer method [11]. For large number $N$, this "random integer lattice" is uniformly chosen from the set of all $n \times n$ Hermite normal forms with the determinant equal to $N$. When $N$ is prime, to generate such a random integer lattice, one only needs to set $h_{nn} = N$, $h_{in} \in [0, N)$ uniformly and $h_{ii} = 1$ for $i < n$. This type of "random integer lattice" is used in many cryptographic applications. From the perspective of mathematics, studying whether the requirement that $N$ be a prime can be removed is also a meaningful issue.

In [12], G. Maze studied the probabilistic distribution of the random HNF with a special diagonal structure, where the randomness was derived from a random square matrix whose elements were all chosen uniformly from $[-B, B]$ for large enough $B$. In [13],

G. Hu et al. introduced a different definition of randomness, in which the definition "random integer lattice" means the lattice's HNF is chosen uniformly from all $n \times n$ HNFs whose determinants are upper bounded by a large number $M$. In the same paper [13], G. Hu et al. also presented a complete random integer lattice generation algorithm. In this algorithm, the first step is to generate a determinant. To make the final output uniform, it is necessary to compute the total number of HNFs with fixed determinant $N$. Since the total number can be figured out only in the case that the factorization of $N$ is known, a subroutine to factor integers is necessary in this algorithm. In this paper, we improved this algorithm with the help of the diagonal elements' distribution in the random HNF. This improved algorithm first generates the diagonal elements $h_{11}, \cdots, h_{n-1,n-1}$ without computing the total number of HNFs with a fixed determinant, then it uses the reverse sampling method to generate the final diagonal element $h_{nn}$. Thus, the factorization subroutine is no longer needed in this improved algorithm, which makes it more efficient.

The remainder of the paper is organized as follows. In Section 2, we give some necessary preliminaries. In Section 3, we recall the definition of the random integer lattice given by G. Hu et al. and discuss the distribution of all the diagonal elements in the random integer lattice's HNF. For the next section, we present our improved algorithm to generate the random integer lattice via the HNF. Finally, we give our conclusion in Section 5.

## 2. Preliminaries

We denote by $\mathbb{Z}$ the integer ring and $\mathbb{R}$ the real number field. We use $GL_n(\mathbb{Z})$ to denote the general linear group over $\mathbb{Z}$. For convenience, we denote the set of all $n \times n$ nonsingular integer matrices by $GL_n(\mathbb{R}) \cap \mathbb{Z}^{n \times n}$.

*Lattice and the HNF*

Given a matrix $B = (b_{ij}) \in \mathbb{R}^{n \times m}$ with rank $n$, the lattice $\mathcal{L}(B)$ spanned by the rows of $B$ is:

$$\mathcal{L}(B) = \{xB = \sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z}\},$$

where $b_i$ is the $i$-th row of $B$. We call $m$ the dimension of $\mathcal{L}(B)$ and $n$ its rank. The determinant of $\mathcal{L}(B)$, say $\det(\mathcal{L}(B))$, is defined as $\sqrt{\det(B^T B)}$. It is easy to see that when $B$ is full-rank ($n = m$), its determinant becomes $|\det(B)|$.

Two lattices $\mathcal{L}(B_1)$ and $\mathcal{L}(B_2)$ are exactly the same when there exists a matrix $U \in GL_n(\mathbb{Z})$ s.t. $B_1 = UB_2$. Lattices used in cryptography are usually "integer lattices", whose basis matrices are over $\mathbb{Z}$ instead of $\mathbb{R}$. Thus, the space of all full-rank integer lattices is actually $(GL_n(\mathbb{R}) \cap \mathbb{Z}^{n \times n})/GL_n(\mathbb{Z})$.

The Hermite Normal Form (HNF) is a useful tool to study integer matrices:

**Definition 1.** *A square nonsingular integer matrix $H \in \mathbb{Z}^{n \times n}$ is called in the HNF if:*

- *$H$ is upper triangular, i.e., $h_{ij} = 0$ for all $i > j$;*
- *All diagonal elements are positive, i.e., $h_{ii} > 0$ for all $i$;*
- *All nondiagonal elements are reduced modulo the corresponding diagonal element at the same column, i.e., $0 \leq h_{ij} < h_{jj}$ for all $i < j$.*

There exists a famous result for the HNF [14] (Chapter 2, page 66):

**Theorem 1.** *For every $A \in GL_n(\mathbb{R}) \cap \mathbb{Z}^{n \times n}$, there exists a unique $n \times n$ matrix $B \in S_{n,\mathbb{Z}}$ (HNF) of the form $B = UA$ with $U \in GL_n(\mathbb{Z})$.*

By this theorem, an integer lattice corresponds to its unique HNF, implying that generating an integer lattice is actually equivalent to generating an HNF.

## 3. Random Integer Lattice

### *3.1. Definition*

In this part, we refer to [13] to recall some results related to the random integer lattice. First, for $M, N \in \mathbb{Z}^+$,

$$H_n^{\leq}(M) \triangleq \{H \text{ is } n\text{-dim HNF} | \det(H) \leq M\},$$

$$H_n(N) \triangleq \{H \text{ is } n\text{-dim HNF} | \det(H) = N\}.$$

Gruber [15] counted the size of $|H_n(N)|$:

**Theorem 2.** *If $N$ has prime decomposition $N = p_1^{r_1} \dots p_t^{r_t}$, then:*

$$|H_n(N)| = \prod_{i=1}^{t} \prod_{j=1}^{n-1} \frac{p_i^{r_i+j} - 1}{p_i^j - 1}.$$

There exists an asymptotic estimation for $|H_n^{\leq}(M)|$ in [13]:

**Theorem 3.** *For large positive integer $M$,*

$$|H_n^{\leq}(M)| = \frac{\prod_{s=2}^{n} \zeta(s)}{n} M^n + O(M^{n-1} \log M).$$

$H$ is called an $n$-dim random nonsingular HNF if for large integer $M > 0$, $H$ is chosen from $H_n^{\leq}(M)$ uniformly, and the lattice $\mathcal{L}(H)$ generated by such an $H$ is called a random integer lattice.

### *3.2. Diagonal Distribution*

In [13], Hu et al. studied the expectation and variance of every entry and the probability distribution of every diagonal entry:

**Theorem 4.** *Let $H = (h_{ij})$ be an $n$-dim random nonsingular HNF with the determinant bounded by $M > 0$ and $t$ be an integer in $[1, n-1]$, given an increasing subset $\{i_1, \cdots, i_t\}$ of $\{1, \cdots, n\}$ and its increasing complementary subset $\{j_1, \cdots, j_{n-t}\}$, for positive integers $b_1 \cdots b_t$; when $M \to +\infty$, we have:*

$$P(h_{i_k,i_k} = b_k \text{ for all } k) = \begin{cases} 0 & (i_t = n) \\ \frac{\prod_{k=1}^{n-t-1} \zeta(n+1-j_k)}{\prod_{s=2}^{n} \zeta(s)} \prod_{l=1}^{t} b_l^{i_l - n - 1} & (i_t < n) \end{cases} \quad (1)$$

If we take $t = 1$, a one-element set $T = \{i\} (i \in [1, n-1])$, and positive integers $b$, then the increasing complementary subset of $T$ in $\{1, 2, \cdots, n\}$ is $\{1, \cdots, i-1, i+1, \cdots, n\}$. We apply the above theorem and obtain the following corollary:

**Corollary 1.** *Let $H = (h_{ij})$ be an $n$-dim random nonsingular HNF with the determinant bounded by $M > 0$, then for $i \in [1, n-1]$ and positive integer $b$, when $M \to +\infty$, we have:*

$$P(h_{ii} = b) = \frac{1}{\zeta(n+1-i) \cdot b^{n+1-i}} \ (b = 1, 2, \cdots).$$

*We denote this distribution of $h_{ii}$ by $\mathbb{D}(n, i)$.*

**Remark 1.** *Notice that in Theorem 4, when $i_t < n$ and $M \to \infty$, both cases: $t = 1$ and $1 < t < n$ are valid conditions, which corresponds to the joint distribution of $h_{i_k,i_k} (k = 1, \cdots, t)$ for $1 < t < n$ or a marginal distribution of the single variable $h_{i_1,i_1}$ for $t = 1$ as in Corollary 1. Considering*

*Theorem 4 and Corollary 1, it can be deduced that when $M \to \infty$, the first $n-1$ diagonal elements $h_{11}, \cdots, h_{n-1,n-1}$ are independent variables.*

## 4. Generating the Random Integer Lattice via the HNF

In this section, we present our random integer lattice generation algorithm via the HNF. Firstly, we introduce the inverse sampling method in probability theory to generate all the diagonal elements. Then, we generate all the nondiagonal elements accordingly.

### *4.1. Inverse Sampling Method*

Given a distribution $\mathbb{D}$ over some ordered set $A$, we can use the inverse sampling method to generate a random variable according to the distribution $\mathbb{D}$. We present two versions of the inverse sampling method: continuous-ISM and discrete-ISM.

**Theorem 5.** (Continuous-ISM) *For distribution $\mathbb{D}$ over interval $[a,b]$ with cumulative distribution function $F_X(x)$, choose a random $y$ uniformly from $[0,1]$ and compute $z$ s.t. $F(z) = y$, then the resulting variable $Z$ has distribution $\mathbb{D}$.*

**Proof.** Our goal is to prove $Z$ has $F_X$ as its cumulative distribution function. Namely, for any $x \in [a,b]$, we have to prove $P(Z \leq x) = F_X(x)$. Since $F$ is a monotonically increasing function, we have:

$$P(Z \leq x) = P(F_Z(z) \leq F_X(x)) = P(y \leq F_X(x)) = F_X(x)$$

where the second equality comes from $F(z) = y$ and the last one is a direct result of $y$'s uniformity in $[0,1]$. Thus, the cumulative distribution function of $Z$ is actually $F_X$, which completes the proof. □

**Theorem 6.** (Discrete-ISM) *For distribution $\mathbb{D}$ over finite-ordered set $A = \{a_k\}_{k=1}^n \subseteq \mathbb{Z}$ with corresponding density $f_k = P(X = a_k)$, choose a random number $y$ uniformly from $[0,1]$ and compute the minimum $j$ s.t. $\sum_{k=1}^{j} f_k \geq y$; then, we let $Z = a_j$, and $Z$ will have distribution $\mathbb{D}$.*

**Proof.** For any $a_j \in A$, we need to prove $P(Z = a_j) = f_j$. Since $j$ is the minimum value s.t. $\sum_{k=1}^{j} f_k \geq y$, we know that $\sum_{k=1}^{j-1} f_k < y$. Then, we have:

$$\begin{aligned} P(Z = a_j) &= P(\sum_{k=1}^{j} f_i \geq y, \sum_{k=1}^{j-1} f_i < y) \\ &= P(\sum_{k=1}^{j} f_k \geq y) - P(\sum_{k=1}^{j-1} f_k \geq y)) \\ &= \sum_{k=1}^{j} f_k - \sum_{k=1}^{j-1} f_k \text{ (since } y \text{ is uniform in } [0,1]) \\ &= f_j \end{aligned}$$

which completes the proof. □

### *4.2. Generating the Random Integer Lattice via the HNF*

From Section 3.1, we can generate a random integer lattice by equivalently generating a random nonsingular HNF. To begin with, we generate the first $n-1$ diagonal elements $h_{11}, h_{22}, \cdots, h_{n-1,n-1}$. Then, we generate the last diagonal element $h_{nn}$. Finally, all the nondiagonal elements are generated, and we output the matrix $H$ as a lattice basis for our random integer lattice.

4.2.1. Generating $h_{11}, h_{22}, \cdots, h_{n-1,n-1}$

From Corollary 1, we know that for an $n$-dim nonsingular HNF, when $i \in [1, n-1]$, the distribution of $h_{ii}$ is:

$$\mathbb{D}(n,i) : P(X = x) = \frac{1}{\zeta(n+1-i)} \cdot x^{-(n+1-i)} \ (x = 1, 2 \dots). \tag{2}$$

Therefore, we generate these diagonal elements $h_{11}, h_{22}, \cdots, h_{n-1,n-1}$ according to $\mathbb{D}(n,i)$ by discrete-ISM (Theorem 6).

For $i \in [1, n-1]$, we choose $y$ uniformly randomly from $[0,1]$ and increasingly iterate $j_i$ starting from 1 until it satisfies $\frac{1}{\zeta(n+1-i)} \sum_{k=1}^{j_i} k^{-(n+1-i)} \geq y$. Then, we set $h_{ii} = j_i$. By Theorem 6, each diagonal $h_{ii}$ has distribution $\mathbb{D}(n,i)$, which is what we need.

4.2.2. Generating $h_{nn}$

After generating the first $n-1$ diagonal elements $h_{ii}$, we set $D_{n-1} \triangleq \prod_{i=1}^{n-1} h_{ii}$. Since the determinant upper bound is $M$, the last diagonal element $h_{nn}$ should be in $[1, \lfloor \frac{M}{D_{n-1}} \rfloor]$. We point out that $D_{n-1}$ is a small number compared to $M$ with high probability. More specifically, the following theorem can be proven.

**Theorem 7.** *Let $H = (h_{ij})$ be an $n$-dim random nonsingular HNF with the determinant bounded by $M > 0$; for $D_{n-1} \triangleq \prod_{i=1}^{n-1} h_{ii}$, we have:*

$$E(D_{n-1}) = \frac{1}{\zeta(n)} \log M + O(1).$$

*Moreover, by Markov's inequality, we find that:*

$$P(D_{n-1} \geq (\log M)^2) \leq \frac{1}{\log M}.$$

To prove Theorem 7, the following lemma from [13] is needed.

**Lemma 1.** *Given an integer $n \geq 4$ and a large integer $M > 0$, for any non-negative increasing sequence $(s_i)_{1 \leq i \leq n}$ s.t. $s_n - s_{n-3} \geq 2, s_n - s_{n-2} \geq 1$ and a respective summation:*

$$S(M, s_1 \dots s_n) \triangleq \sum_{a_i \in \mathbb{Z}^+, \prod_{i=1}^{n} a_i \leq M} a_1^{s_1} \cdots a_n^{s_n},$$

*we have the following Table 1 on asymptotic formulas for $S(M, s_1 \dots s_n)$.*

**Table 1.** Asymptotic formulas of $S(M, s_1 \dots s_n)$ in different cases.

| $S(M, s_1 \dots s_n)$ | If |
|---|---|
| $\frac{\prod_{j=1}^{n-1} \zeta(s_n+1-s_j)}{s_n+1} M^{s_n+1} + O(M^{s_n} \log M)$ | $s_{n-3} \leq s_{n-2} < s_{n-1} < s_n$ |
| $\frac{\prod_{j=1}^{n-1} \zeta(s_n+1-s_j)}{s_n+1} M^{s_n+1} + O\big(M^{s_n} (\log M)^2\big)$ | $s_{n-3} < s_{n-2} = s_{n-1} < s_n$ |
| $\frac{\prod_{j=1}^{n-2} \zeta(s_n+1-s_j)}{s_n+1} M^{s_n+1} \log M + O(M^{s_n+1})$ | $s_{n-3} \leq s_{n-2} < s_{n-1} = s_n$ |

*where $\zeta(s) = \sum_{i=1}^{\infty} i^{-s}$ is the well-known Riemann zeta function and the constant in the $O$ notation is only relevant to $n$.*

Now, we start to prove Theorem 7.

**Proof.** For the expectation of $D_{n-1} = \prod_{i=1}^{n-1} h_{ii}$, we find that:

$$\begin{aligned}
E(D_{n-1}) &= \sum_{k\le M} k \cdot P(D_{n-1} = k) \\
&= \frac{\sum\limits_{k\le M} k \cdot |H_{n-1}(k)| \cdot \sum\limits_{a_n \le M/k} a_n^{n-1}}{|H_n^{\le}(M)|} \\
&= \frac{\sum\limits_{k\le M} \prod_{j=1}^{n-1} a_j \sum\limits_{\prod_{j=1}^{n-1} a_j = k} \prod_{j=1}^{n-1} a_j^{j-1} \sum\limits_{a_n \le M/k} a_n^{n-1}}{|H_n^{\le}(M)|} \\
&= \frac{\sum\limits_{k\le M} \sum\limits_{\prod_{j=1}^{n-1} a_j = k} \prod_{j=1}^{n-1} a_j^{j} \sum\limits_{a_n \le M/k} a_n^{n-1}}{|H_n^{\le}(M)|} \\
&= \frac{\sum\limits_{\prod_{j=1}^{n} a_j \le M} \prod_{j=1}^{n-1} a_j^{j} \cdot a_n^{n-1}}{\sum\limits_{\prod_{j=1}^{n} a_j \le M} \prod_{j=1}^{n} a_j^{j-1}} \\
&= \frac{S(M, 1, 2, \cdots, n-2, n-1, n-1)}{S(M, 0, 1, \cdots, n-2, n-1)} \text{(as in Lemma 1)} \\
&= \frac{\frac{\prod_{s=2}^{n-1} \zeta(s)}{n} \cdot M^n \log M + O(M^n)}{\frac{\prod_{s=2}^{n-1} \zeta(s)}{n} M^n + O(M^{n-1} \log M)} \text{(by Lemma 1)} \\
&= \frac{\frac{\prod_{s=2}^{n-1} \zeta(s)}{n} \cdot \log M + O(1)}{\frac{\prod_{s=2}^{n-1} \zeta(s)}{n} + O(\log M / M)} \\
&= \frac{1}{\zeta(n)} \log M + O(1),
\end{aligned}$$

which completes the first part of Theorem 7.

For the second part, recall that for any non-negative random variable $X$, Markov's inequality tells us that:

$$P(X \ge a) \le E(X)/a.$$

Since $D_{n-1}$ is non-negative, we apply Markov's inequality to it by setting $a = (\log M)^2$ and obtain:

$$P(D_{n-1} \ge (\log M)^2) \le (\frac{1}{\zeta(n)} \log M + O(1))/(\log M)^2 \le \frac{1}{\log M}$$

which completes the second part of the proof. □

From Theorem 7, we know that $D_{n-1}$ is small compared to $M$ with high probability; thus, $\lfloor \frac{M}{D_{n-1}} \rfloor$ is still large enough for us to obtain a similar result for $h_{nn}$. We think this is a relatively reasonable way to describe the distribution of $h_{nn}$. Thus, for the random nonsingular HNF with the determinant bounded by $M$, on the condition that $\prod_{i=1}^{n-1} h_{ii} = D_{n-1}$, the distribution of $h_{nn}$ is the following:

$$\begin{aligned}
\tilde{\mathbb{D}}(n, M, D_{n-1}): \quad & P(X = x) \\
&= \frac{1}{\sum_{k=1}^{\lfloor M/D_{n-1} \rfloor} k^{n-1}} \cdot x^{n-1} \\
&= \frac{1}{\frac{1}{n} \lfloor \frac{M}{D_{n-1}} \rfloor^n + O(\lfloor \frac{M}{D_{n-1}} \rfloor^{n-1})} \cdot x^{n-1} \ (x = 1, 2 \ldots, \lfloor \frac{M}{D_{n-1}} \rfloor).
\end{aligned} \tag{3}$$

Moreover, the corresponding cumulative distribution function is:

$$\begin{aligned} F_X(x) &= P(X \le x) \\ &= \frac{1}{\frac{1}{n}\lfloor\frac{M}{D_{n-1}}\rfloor^n + O(\lfloor\frac{M}{D_{n-1}}\rfloor^{n-1})} \cdot \sum_{k=1}^{x} k^{n-1} \\ &= \frac{\frac{1}{n}x^n + O(x^{n-1})}{\frac{1}{n}\lfloor\frac{M}{D_{n-1}}\rfloor^n + O(\lfloor\frac{M}{D_{n-1}}\rfloor^{n-1})} \ (x = 1, 2 \ldots, \lfloor\frac{M}{D_{n-1}}\rfloor). \end{aligned} \tag{4}$$

Since $\lfloor\frac{M}{D_{n-1}}\rfloor$ is still super large, we know that:

$$F_X(x) \approx \frac{x^n/n}{\lfloor M/D_{n-1}\rfloor^n/n} = (\frac{x}{\lfloor M/D_{n-1}\rfloor})^n \triangleq G_X(x).$$

As a result, $G_X(x)$ is a rather good estimation for $F_X(x)$. In fact, if we define the distribution $\tilde{\mathbb{D}}_0(n, M, D_{n-1})$ by the cumulative distribution function $G_X(x)$ as follows:

$$\begin{aligned} \tilde{\mathbb{D}_0}(n, M, D_{n-1}): \ & P(X \le x) \\ & = (\frac{x}{\lfloor M/D_{n-1}\rfloor})^n \ (x = 1, 2 \ldots, \lfloor\frac{M}{D_{n-1}}\rfloor), \end{aligned} \tag{5}$$

then we have the following theorem.

**Theorem 8.** *For large enough $M \in \mathbb{Z}^+$ and positive integer $D_{n-1} = o(M)$, the statistical distance between $\tilde{\mathbb{D}}(n, M, D_{n-1})$ and $\tilde{\mathbb{D}}_0(n, M, D_{n-1})$ is at most $n \cdot O(\frac{D_{n-1}}{M})$.*

**Proof.** According to (4), the cumulative distribution function of $\tilde{\mathbb{D}}(n, M, D_{n-1})$ is $F_X(x) = \frac{\frac{1}{n}x^n + O(x^{n-1})}{\frac{1}{n}\lfloor\frac{M}{D_{n-1}}\rfloor^n + O(\lfloor\frac{M}{D_{n-1}}\rfloor^{n-1})}$, since the cumulative distribution function of $\tilde{\mathbb{D}}_0(n, M, D_{n-1})$ is $G_X(x) = (\frac{x}{\lfloor M/D_{n-1}\rfloor})^n$; denote $\lfloor\frac{M}{D_{n-1}}\rfloor$ by $\tilde{M}$, then $x \le \tilde{M}$, and for every $x \in [1, \tilde{M}]$, we have:

$$\begin{aligned} & |F_X(x) - G_X(x)| \\ =& |\frac{\frac{1}{n}x^n + O(x^{n-1})}{\frac{1}{n}\tilde{M}^n + O(\tilde{M}^{n-1})} - (\frac{x}{\tilde{M}})^n| \\ =& |\frac{x^n + n \cdot O(x^{n-1})}{\tilde{M}^n + n \cdot O(\tilde{M}^{n-1})} - (\frac{x}{\tilde{M}})^n| \\ =& |\frac{(x^n + n \cdot O(x^{n-1}))\tilde{M}^n - (\tilde{M}^n + n \cdot O(\tilde{M}^{n-1}))x^n}{\tilde{M}^{2n} + n \cdot O(\tilde{M}^{2n-1})}| \\ =& |\frac{n \cdot O(x^{n-1})\tilde{M}^n - n \cdot O(\tilde{M}^{n-1})x^n}{\tilde{M}^{2n} + n \cdot O(\tilde{M}^{2n-1})}| \\ =& |\frac{n \cdot O(\tilde{M}^{n-1})\tilde{M}^n - n \cdot O(\tilde{M}^{n-1})\tilde{M}^n}{\tilde{M}^{2n} + n \cdot O(\tilde{M}^{2n-1})}| (\text{since } x \le \tilde{M}) \\ =& |\frac{n \cdot O(\tilde{M}^{2n-1})}{\tilde{M}^{2n} + n \cdot O(\tilde{M}^{2n-1})}| \\ =& |\frac{n \cdot O(\frac{1}{\tilde{M}})}{1 + n \cdot O(\frac{1}{\tilde{M}})}| = n \cdot O(\frac{1}{\tilde{M}}) = n \cdot O(\frac{D_{n-1}}{M}) \end{aligned}$$

which implies that the statistical distances $\tilde{\mathbb{D}}(n, M, D_{n-1})$ and $\tilde{\mathbb{D}}_0(n, M, D_{n-1})$ are bounded by $n \cdot O(\frac{D_{n-1}}{M})$. □

Since $\lfloor M/D_{n-1} \rfloor$ is still super large, we can generate $h_{nn}$ according to $\tilde{\mathbb{D}}_0(n, M, D_{n-1})$ (close enough to $\tilde{\mathbb{D}}(n, M, D_{n-1})$) by continuous-ISM (Theorem 5).

We choose $y$ uniformly randomly from $[0, 1]$ and compute $z \in \mathbb{R}^+$ s.t.:

$$(\frac{z}{\lfloor M/D_{n-1} \rfloor})^n = y.$$

Then, we set $h_{nn} = \lfloor z \rfloor$. By Theorems 6 and 8, the diagonal $h_{nn}$ has distribution $\tilde{\mathbb{D}}_0(n, M, D_{n-1})$, which is close enough to $\tilde{\mathbb{D}}(n, M, D_{n-1})$.

#### 4.2.3. Generating $h_{ij}(i \neq j)$

This part is relatively easier. For $i, j = 1, \ldots, n$, let $h_{ij}$ be chosen from $[0, h_{jj})$ uniformly randomly if $i < j$ and let $h_{ij} = 0$ if $i > j$.

#### 4.2.4. Correctness

By the discussion above, for large enough $M > 0$, the distribution of the diagonal $h_{11}, \cdots, h_{nn}$ generated by this algorithm is close enough to its distribution as a random nonsingular HNF. For $i < j \in [1, n]$, since a random nonsingular HNF's $h_{ij}$ is uniform in $[0, h_{jj})$ and $h_{ij}$ is generated in the same way, we know that the output of this algorithm is also close enough to a real random nonsingular HNF, which implies the correctness of this algorithm.

### *4.3. Algorithm 1: Generate Random Integer Lattice*

Now we present the Algorithm 1 to generate a random integer lattice.

**Algorithm 1** Random Integer Lattice Generation

**Require:** Dimension $n$, large integer $M$
**Ensure:** $n$-dim random integer lattice $\mathcal{L}$ with $\det(\mathcal{L}) \leq M$
  **Step 1:** Generate $h_{11}, \cdots, h_{n-1,n-1}$
  $D_0 = 1$
  **for** $i = 1$ to $n - 1$ **do**
    $j_i = 1, s_i = 1$
    choose $y_i \in [0, 1]$ uniformly
    **while** $s_i < \zeta(n + 1 - i) \cdot y_i$ **do**
      $j_i = j_i + 1$
      $s_i = s_i + j_i^{-(n+1-i)}$
    **end while**
    $D_i = D_{i-1} \cdot j_i$
    set $h_{ii} = j_i$
  **end for**
  **Step 2:** Generate $h_{nn}$
  choose $y \in [0, 1]$ uniformly
  $z = y^{1/n}$
  $z = z \cdot \lfloor \frac{M}{D_{n-1}} \rfloor$
  set $h_{nn} = \lfloor z \rfloor$
  **Step 3:** Generate $h_{ij}(i \neq j)$
  **for** $j = 1$ to $n$ **do**
    **for** $i = 1$ to $j - 1$ **do**
      choose $h_{ij} \in [0, h_{jj})$ uniformly
    **end for**
    **for** $i = j + 1$ to $n$ **do**
      set $h_{ij} = 0$
    **end for**
  **end for**
  **Step 4:** Set $H = (h_{ij})$, and output $\mathcal{L}(H)$

*4.4. Time Complexity of Algorithm 1*

Now, we analyze the time complexity of Algorithm 1. Obviously, the most time-consuming part of Algorithm 1 is the floating-point operations $s_i = s_i + j_i^{-(n+1-i)}$ inside the while iteration for each $i$ in Step 1. Denote the number of computing $s_i = s_i + j_i^{-(n+1-i)}$ in the $i$-th while iteration by $T(i)$. Notice that:

$$P(h_{ii} = 1) = \frac{1}{\zeta(n+1-i)};$$

since $\zeta(s)$ converges to one quite fast as $s$ grows, the majority of $h_{ii}$ will be set to one. In fact, by the numerical results, we have following result:

**Fact 1**: For any integer $n \geq 10$,

$$\frac{1}{\prod_{s=10}^{n} \zeta(s)} \geq 0.999.$$

By this fact, for $i \leq n-10$, all the $h_{ii}$ are very likely to be set to one, implying that $T(1), T(2), \cdots, T(n-10) = 0$ with probability $\geq 0.999$. Then, we consider $T(n-9), T(n-8), \cdots, T(n-1)$. If we set the probability bound for each $T(i)$ to be 0.999, then by accurate numerical results, we have the following Table 2:

**Table 2.** Upper bound for $T(i)$ with probability$\geq 0.999$.

| T(i) | Upper Bound |
|---|---|
| $T(n-9)$ | 0 |
| $T(n-8)$ | 1 |
| $T(n-7)$ | 1 |
| $T(n-6)$ | 1 |
| $T(n-5)$ | 2 |
| $T(n-4)$ | 3 |
| $T(n-3)$ | 6 |
| $T(n-2)$ | 19 |
| $T(n-1)$ | 607 |

Thus, we have the following theorem:

**Theorem 9.** *The number of floating-point operations performed in Algorithm 1 is bounded by* 1300 *with probability* $\geq 0.99$.

**Proof.** By the above table, $\sum_{i=n-9}^{n-1} T(i)$ is bounded by 640 with probability $\geq 0.999^9$. Since $T(1), T(2), \cdots, T(n-10) = 0$ with probability $\geq 0.999$, we know that $\sum_{i=1}^{n-1} T(i)$ is bounded by 640 with probability $\geq 0.999^{10} \geq 0.99$. Notice that each $s_i = s_i + j_i^{-(n+1-i)}$ needs two floating-point operations, and it also needs another four floating-point operations to generate $h_{nn}$ in Step 2; thus, with probability $\geq 0.99$, the total number of floating-point operations performed in Algorithm 1 is bounded by $640 \times 2 + 4 = 1284 < 1300$, which completes the proof. □

**Remark 2.** *We point out that the accuracy of the floating-point affects the actual running time of Algorithm 1. By experiments,* 150 *bit are a suitable option.*

It is not hard to see that in Algorithm 1, besides the floating-point operations, the remaining parts of Step 1, Step 2, and Step 3 take $O(n^2), O(1)$, and $O(n^2)$ operations, respectively. Combining this with Theorem 9, we have the following result:

**Theorem 10.** *Algorithm 1 outputs a random integer lattice within $O(n^2)$ operations with probability $\geq 0.99$.*

## 5. Conclusions

In this paper, we presented an improved algorithm for generating random integer lattices and discussed its time complexity. We proved that with probability $\geq$0.99, this algorithm outputs an $n$-dim random integer lattice within $O(n^2)$ operations. We pointed out that there is still space for improvement of our algorithm, and we leave this as an open problem.

**Author Contributions:** Conceptualization, G.H.; formal analysis, L.Y.; funding acquisition, G.H. and L.Y.; investigation, G.H.; methodology, G.H.; validation, L.L.; writing—original draft, G.H.; writing—review and editing, L.L., L.H., and H.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded in part by the National Natural Science Foundation of China (No. 61602143, No. 61772166) and in part by the Natural Science Foundation of Zhejiang Province of China (No. LZ17F020002).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** We thank Yanbin Pan for his wonderful suggestions about this paper, and we thank the referees for putting forward their excellent advice on how to improve the presentation of this paper.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Ajtai, M. Gennerating hard instances of lattice problems. In Proceedings of the STOC '96 Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; Miller, G., Ed.; ACM Press: New York, NY, USA, 1996; pp. 99–108.
2. Ajtai, M.; Dwork, C. A public-key cryptosystem with worst-case/average-case equivalence. In Proceedings of the STOC '97 Twenty-Ninth Annual ACM Symposium on Theory of Computing, El Paso, TX, USA, 4–6 May 1997; Leighton, F.T., Shor, P., Eds.; ACM Press: New York, NY, USA, 1997; pp. 284–293.
3. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A Ring-Based Public Key Cryptosystem. In Proceedings of the ANTS-III Third International Symposium on Algorithmic Number Theory, Portland, OR, USA, 21–25 June 1998; Buhler, J.P., Ed.; Springer: Heidelberg, Germany, 1998; Volume 1423, pp. 267–288.
4. Regev, O. On lattices, learning with errors, random linear codes, and cryptography, In Proceedings of the STOC '05 Thirty-Seventh Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, 22–24 May 2005; Gabow, H.N., Fagin, R., Eds.; ACM Press: New York, NY, USA, 2005; pp. 84–93.
5. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In Proceedings of the STOC '08 Fortieth Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 17–20 May 2008; Ladner, R., Dwork, C., Eds.; ACM Press: New York, NY, USA, 2008; pp. 197–206.
6. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
7. Lenstra, A.K.; Lenstra, H.W., Jr.; Lovasz, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 513–534. [CrossRef]
8. Schnorr, C.P.; Euchner, M. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Math. Program.* **1994**, *66*, 181–199. [CrossRef]
9. Chen, Y.; Nguyen, P.Q. BKZ 2.0: Better Lattice Security Estimates. In Proceedings of the ASIACRYPT 2011 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, Korea, 4–8 December 2011; Lee, D.H., Wang, X., Eds.; Springer: Heidelberg, Germany, 2011; Volume 7073, pp. 1–20.
10. Nguyen, P.Q.; Stehle, D. LLL on the average. In Proceedings of the ANTS-XII 7th International Symposium on Algorithmic Number Theory, Berlin, Germany, 23–28 July 2006; Hess, F., Pauli, S., Pohst, M.E., Eds.; Springer: Heidelberg, Germany, 2006; Volume 4076, pp. 238–256.
11. Goldstein, D.; Mayer, A. On the equidistribution of Hecke points. *Forum Math.* **2003**, *15*, 165–189. [CrossRef]

12. Maze, G. Natural density distribution of Hermite normal forms of integer matrices. *J. Number Theory* **2011**, *131*, 2398–2408. [CrossRef]
13. Hu, G.; Pan, Y.; Liu, R.; Chen, Y. On Random Nonsingular Hermite Normal Form. *J. Number Theory* **2016**, *164*, 66–86. [CrossRef]
14. Cohen, H. *A Course in Computational Algebraic Number Theory*; Springer-Verlag: Berlin/Heidelberg, Germany, 1993; Volume 138, p. 66.
15. Gruber, B. Alternative formulae for the number of sublattices. *Acta Cryst.* **1997**, *A53*, 807–808. [CrossRef]