EURASIP Journal on Information Security

RESEARCH Open Access

A new method of generating hard random lattices with short bases

Chengli Zhang[1,2*], Wenping Ma[1], Hefeng Chen[3] and Feifei Zhao[1]

Abstract

This paper first gives a regularity theorem and its corollary. Then, a new construction of generating hard random lattices with short bases is obtained by using this corollary. This construction is from a new perspective and uses a random matrix whose entries obeyed Gaussian sampling which ensures that the corresponding schemes have a wider application future in cryptography area. Moreover, this construction is more specific than the previous constructions, which makes it can be implemented easier in practical applications.

Keywords: Cryptography, Gaussian distribution, Hard random lattices, Short bases

1 Introduction

A lattice has a typical linear structure and some problems about it have been proven to be NP-hard. Many exciting developments in lattice-based cryptography have occurred in the past few years [1–10], and there has been renewed interest in lattice-based cryptography as prospects for a real quantum computer improve. As is well known, some lattice-based cryptosystems can be resistant to attack by both classical and quantum computers. But the basic problems about short bases and short vector are studied in only a few papers [11–14]. But such problems occupy an important place in the study on lattice-based cryptography. And more researches are based on these basic problems.

Ajtai's seminal work [15] in the lattice-based cryptography demonstrated a random class of lattice whose elements could be generated along with a short vector in them for which finding a short nonzero vector in the random lattice is at least as hard as finding the length of a shortest nonzero vector for any random lattice, and is at least as hard as finding a basis for the random lattice in 1996. And he showed how to generate a hard random lattice with knowledge of one relatively short nonzero lattice vector which can be used as secret information in cryptography applications. In addition, Ajtai also had given the reductions of some hard problems on the lattice.

In 1999, Ajtai also demonstrated an entirely different method of generating a random lattice along with a short basis based on his previous studies [11]. His algorithm had an important property that the resulting lattice is drawn, under the appropriate distribution, from the hard family defined in [15]. Interestingly, the algorithm apparently went without application until recently, when Gentry, Peikert, and Vaikuntanathan constructed several provably secure cryptographic schemes that crucially use the short bases as the secret keys [16].

Alwen and Perkert revisited the problem of generating a hard random lattice with a relatively short basis [12] in 2011. They elucidated and modularized Ajtai's basic approach for generating a hard random lattice with a relatively short basis. They endeavored to give a top-down exposition of the key aspects of the problem and the techniques. They have based the algorithm around the concept of the Hermite normal form.

Micciancio and Peikert then gave the methods for generating and using "strong trapdoors" in cryptographic lattices [7]. Their methods involved a kind of trapdoor and included specialized algorithms for inverting LWE, randomly sampling SIS preimages, and securely delegating trapdoors. The trapdoor generator strictly subsumed the prior ones of [11, 12], in that it proves the main theorems from those works.

We construct a new hard random lattice together with a relatively short basis from a new perspective in this

* Correspondence: zcl0719@163.com
[1]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi 710071, People's Republic of China
[2]Department of Mathematics, Xi'an Polytechnic University, Xi'an, Shaanxi 710048, People's Republic of China
Full list of author information is available at the end of the article

paper. Firstly, we give and demonstrate a useful theorem called regularity theorem, which plays an important role in the cryptography area. Before this, we get that after proper matrix elementary transformations, any random matrix uniformly on $Z_q^{k\times l_1}$ can be written a special matrix whose first k columns consist an identity matrix and the other columns are uniformly on Z_q^k. Furthermore, we can learn from the theorem that the result matrix of the above special matrix right multiplied by a matrix whose entries follow Gaussian distribution is a uniform matrix. Then, by using the regularity theorem, we give our simple, wider applied, and more particular algorithm in which Gaussian distribution is used. Then, the concrete expression of each matrix in our algorithm is given. Lastly, we give the analysis of the short basis in our algorithm.

2 Preliminaries

Some notations are given in this section that will be used throughout the paper. We denote the integer ring by Z and the modular q residue ring by Zq. For any real x, the largest integer not greater than x is denoted by $\lfloor x \rfloor$. For a vector $\mathbf{x} = (\times 1, \cdots, \mathrm{xn})$, $\lfloor \mathbf{x} \rfloor$ is defined as $(\lfloor \times 1 \rfloor, \cdots, \lfloor \mathrm{xn} \rfloor)$. We write log for the logarithm to the base 2, and $\log_q$ when the base q is any number possibly different from 2. A negligible amount in n is defined as an amount that is asymptotically smaller than n^{-c} for any constant $c > 0$. Also, when we say that an expression is exponentially small in n, we mean that it is at most $2^{-\Omega(n)}$. Finally, when we say that an expression is exponentially close to 1, we mean that it is $1 - 2^{-\Omega(n)}$.

All the k-dimensional vectors over a domain D are written by D^k. Similarly, $(\mathrm{D})^{m\times n}$ denotes all m by n matrices whose entries belong to D. The Euclidean norm of a vector $x = (\mathrm{x}_1, \cdots, \mathrm{x}_n) \in \mathrm{R}^n$ is $\|x\| = \sqrt{\sum_i x_i^2}$, and the associated distance of two vectors x and y is $\mathrm{dist}(x, y) = \|x - y\|$. The distance function is extended to sets in a customary way: $\mathrm{dist}(x, S) = \mathrm{dist}(S, x) = \min_{y\in S} \mathrm{dist}(x, y)$ where x is a point, S is a set, and $y \in S$. We often use matrix notation to denote sets of vectors. For example, the matrix $S \in \mathrm{R}^{n\times m}$ represents the set of n-dimensional vectors $\mathrm{s}_1, \cdots, \mathrm{s}_m$, where $\mathrm{s}_1, \cdots, \mathrm{s}_m$ are the columns of S. $[A \mid B]$ denotes a block matrix whose left part is A and the right part is B. We denote the maximum norm of the column vectors in S by $\|S\|$ and the number of all elements in S by $|S|$. For the vectors $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$ in R^{n}, $\langle \mathbf{x}, \mathbf{y} \rangle$ denotes the inner product of x and y, that is, $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_i x_i y_i$. The linear space spanned by a set S of m vectors $\mathrm{s}_1, \cdots, \mathrm{s}_m$ is denoted by $\mathrm{span}(S) = \{\sum_i x_i s_i : x_i \in R for \ \ 1 \le i \le m\}$. For any set of n linearly independent vectors in S, we define the half-open parallelepiped as $P(S) = \{\sum_i x_i s_i : 0 \le x_i < 1 for \ \ 1 \le i \le n\}$.

Random matrix is a matrix whose each entry is chosen randomly from some set.

We now review some basic definitions of lattice. A lattice in R^{n} is defined as the set of all integer combinations of n linearly independent vectors. This set of vectors is known as a basis of the lattice and it is not unique.

Definition 21. [15] An n-dimensional lattice A is the set of all integer combinations

$$\Lambda = L(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in Z \text{ for } \quad 1 \le i \le n \right\}$$

of n linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ in R^{n}.

The set of vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ is called a basis for the lattice. A basis can be represented by the matrix $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n) \in \mathrm{R}^{n\times n}$ having the basis vectors as its columns. The lattice generated by $\mathbf{B}$ is denoted $L(\mathbf{B})$. Notice that $L(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in Z^n\}$, where $\mathbf{Bx}$ is the usual matrix-vector multiplication.

For any lattice basis $\mathbf{B}$ B and point $\mathbf{x}$, there exists a unique vector $\mathbf{y} \in P(\mathbf{B})$ such that $\mathbf{y} - \mathbf{x} \in L(\mathbf{B})$. This vector is denoted by $\mathbf{y} = \mathbf{x} \bmod \mathbf{B}$, and it can be computed in polynomial time when given $\mathbf{B}$ and $\mathbf{x}$.

The dual of a lattice Λ in R^{n}, denoted Λ^{V}, is the lattice given by the set of all vectors $\mathbf{y} \in R^n$ such that $\langle \mathbf{x}, \mathbf{y} \rangle \in Z$ for all vectors $\mathbf{x} \in \Lambda$.

We now recall some about Gaussian measures.

Definition 22. [17] For any vectors $\mathbf{c}$, $\mathbf{x}$ and any $r > 0$, let

$$\rho_{r,c}(\mathbf{x}) = \mathrm{e}^{-\pi \|(\mathbf{x}-\mathbf{c})/\mathrm{r}\|^2}$$

be a Gaussian function centered in $\mathbf{c}$ scaled by a factor of r and normally let $\mathbf{c} = \mathbf{0}$.

Note that $\int_{\mathbf{x}\in R^n} \rho_{r,c}(\mathbf{x}) = r^n$. Hence, Gaussian distribution around $\boldsymbol{c}$ with parameter r can be defined as its probability density function

$$(\forall \mathbf{x} \in \mathrm{R}^n) \mathrm{D}_{r,c}(\mathbf{x}) = \frac{\rho_{r,c}(\mathbf{x})}{r^n}.$$

We know that the expected square distance from $\mathbf{c}$ of a vector chosen from the distribution is $nr^2/(2\pi)$. So $D_{r,\,c}$ can be seen as a sphere of radius $r\sqrt{n/(2\pi)}$ centered around $\mathbf{c}$. Notice that a sample from the above Gaussian distribution can be obtained by taking n independent samples from the 1-dimensional Gaussian distribution.

For any vector $\mathbf{c}$, real $\mathrm{r} > 0$, and lattice L, define the probability distribution $D_{L,\,r,\,c}$ over L by

$$(\forall \mathbf{x} \in L) \mathrm{D}_{L,r,c}(\mathbf{x}) = \frac{\mathrm{D}_{r,c}(\mathbf{x})}{\mathrm{D}_{r,c}(L)} = \frac{\rho_{r,c}(\mathbf{x})}{\rho_{r,c}(L)}.$$

We refer to $\mathrm{D}_{L,\,r,\,c}(\mathbf{x})$ as a discrete Gaussian distribution. And for a large enough r, $\mathrm{D}_{L,\,r,\,c}$ behaves in many

respects like the continuous Gaussian distribution $D_{r,\ c}$. In particular, vectors distributed according to $D_{L,\ r,\ c}$ have an average value which is very close to the center **c** and the expected squared distance from the vector c is very close to $nr^2/(2\pi)$. The center vector is zero sometimes and is omitted.

We give the definition of smoothing parameter introduced by Micciancio and Regev.

Definition 23. [17] For a lattice Λ and a positive real $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\Lambda)$ is the smallest s such that

$$\rho_{1/s}(\Lambda^{\mathbf{v}} \backslash \{0\}) \le \varepsilon.$$

Lemma 24. [17] For any lattice Λ, real $\varepsilon > 0$ and $s \ge \eta_\varepsilon(\Lambda)$, and $\mathbf{c} \in \mathbf{H}$, we have $\rho_s(\Lambda + \mathbf{c}) \in [1 \pm \varepsilon] s^n \det(\Lambda)^{-1}$.

3 New hard random lattice

We will give a new method of generating a hard random lattice along with short bases by using our regularity theorem in this section. On the topic of hard random lattice with short bases, the large hard random matrix and its corresponding short base are required simultaneously in cryptography to ensure the security. But the matrix in our regularity theorem needs to be a special form, that is, the left part is an identity matrix and the right part is a random matrix. So we must first transform the hard random matrix into the special form matrix.

We now describe our basic framework for constructing our new hard random lattice and the corresponding short basis.

Firstly, we must ensure that the large hard random matrix contains an invertible submatrix, and we will prove that any $k \times l_1$ random matrix **A** uniformly chosen from $(Z_q)^{k \times l_1}$, with very great probability, contains k independent column vectors, that is, A contains an invertible submatrix.

Secondly, our regularity theorem, which can be extended a useful corollary, will be constructed and be proved. Moreover, an effective parameter will be calculated in the regularity theorem which ensures that our hard random lattice with a short basis is generated.

Thirdly, we will give the new construction of generating the hard random lattice with a short basis and the framework of our algorithm by using the fact in the first part of this section and the regularity in the second part of this section.

Fourthly, the concrete expression of each matrix in the algorithm is given.

Finally, the quality of the short basis S will be analyzed.

3.1 Generate a random matrix containing an invertible submatrix

Let q be an integer and Z_q be a modular q residue ring. Let $\mathbf{A} \in (Z_q)^{k \times l_1}$ be a random matrix where k, $l_1 \in Z$ whose entries are chosen randomly from Z_q.

Case 1: Let p be a prime integer and $q = p^{\overline{k}}$ be an integer for some integer $\overline{k}$. It is obvious that a submatrix on $(Z_q)^{k \times k}$ contained in **A** is invertible if and only if the submatrix mod p is invertible.

Firstly, we choose a k-dimensional vector on $Z_q{}^k$ randomly and the probability that the vector can be one column of the invertible submatrix of **A** is $\frac{(p^k-1)p^{k(\overline{k}-1)}}{q^k} = \frac{p^k-1}{p^k}$. Then we let this column be the first column of **A**.

After fixing the first column of **A**, we choose a k-dimensional vector randomly on Z_q^k again and the probability that this vector can be another column of the invertible submatrix of **A** is $\frac{(p^k-p)p^{k(\overline{k}-1)}}{q^k} = \frac{p^k-p}{p^k}$.Similarly, we let this column be the second column of **A**.

And so on, after fixing the first $k-1$ columns of **A**, the probability that a vector is chosen randomly can be the kth column of the invertible submatrix of **A** is $\frac{p^k-p^{k-1}}{p^k}$.

Thus, we choose a matrix **A** randomly on $(Z_q)^{k \times l_1}$, the probability that **A** contains an invertible submatrix is $\prod_{i=1}^{k}(1-\frac{1}{p^i})$.

Case 2: From another perspective, let $q = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, where each p_i is a prime and $k_i \in Z(\mathrm{i} = 1, 2, \cdots, \mathrm{t})$. Similarly, the probability of generating a random matrix on $(Z_q)^{k \times l_1}$ which contains an invertible submatrix in t steps is $\prod_{s=1}^{t}\prod_{i=1}^{k}(1-\frac{1}{p_s^i})$.

If $l_1 \gg k$, then any $k \times l_1$ random matrix **A** uniformly chosen from $(Z_q)^{k \times l_1}$, with very great probability, contains k independent column vectors, and we suppose these columns are the first k columns of **A**. After proper elementary matrix transformations, **A** can be written as $(\mathbf{I}|\overline{\mathbf{A}})$, where **I** is a $k \times k$ identity matrix and $\overline{\mathbf{A}}$ is a $k \times (l_1 - k)$ uniformly random matrix on $(Z_q)^{k \times (l_1-k)}$. And the columns of **A** generate all of the $Z_q{}^k$.

3.2 Regularity

We will construct a theorem called "Regularity Theorem" and the proof also will be given in this subsection. The regularity theorem can be widely used into cryptography applications, who gives an important property that a special matrix being multiplied by a vector sampled from Gaussian distribution, with great probability, produces a uniform vector.

Suppose that $\mathbf{A} \in (Z_q)^{k \times l_1}$, we define

$$\Lambda^{\perp}(\mathbf{A}) = \left\{\mathbf{z}\in \mathrm{Z}^{l_1} : \mathbf{A}\mathbf{z} = \mathbf{0} \bmod q\mathrm{Z}\right\}.$$

Then, we give our regularity theorem on integer lattice as following:

Theorem 31. Let z be an integer and $q \geq 2$ be an integer. Let $\mathbf{A} = (\mathbf{I}_k|\overline{\mathbf{A}})\in(\mathrm{Z}_q)^{k\times l_1}$, where $\mathbf{I}_k \in (\mathrm{Z}_q)^{k\times k}$ is identity matrix and $\overline{\mathbf{A}}\in(\mathrm{Z}_q)^{k\times(l_1-k)}$ is a uniformly random matrix. Then, for all r ($\sqrt{l_1} < r < \sqrt{l_1}g_s$), $E_{\overline{\mathbf{A}}}[\rho_{1/r}(\Lambda^{\perp}(\mathrm{A})^{\mathrm{V}})] \leq 1 + 2^{-\Omega(k)}$.

Proof For any $\mathbf{A}\in(\mathrm{Z}_q)^{k\times l_1}$, the dual lattice of $\Lambda^{\perp}(\mathbf{A})$ is

$$(\Lambda^{\perp}(\mathbf{A}))^{\mathrm{V}} = Z^{l_1} + \left\{\frac{1}{q}\mathbf{A}^T\mathbf{s} : \mathbf{s}\in \mathrm{Z}_q^k\right\}.$$

Then, we have

$$\begin{aligned}
&\mathrm{E}_{\overline{\mathbf{A}}}\left[\rho_{1/r}(\Lambda^{\perp}(\mathbf{A}))^{\mathrm{V}}\right] \\
&= \sum_{\mathbf{s}\in Z_q^k} \mathrm{E}_{\overline{\mathbf{A}}}\left[\rho_{1/r}\left(Z^{l_1} + \frac{1}{q}\mathbf{A}^T\mathbf{s}\right)\right] \\
&= \sum_{\mathbf{s}\in Z_q^k} \rho_{1/r}\left(Z^k + \frac{\mathbf{s}}{q}\right) + E_{\mathbf{a}}\left[\rho_{1/r}\left(Z + \frac{\langle \mathbf{a}, \mathbf{s}\rangle}{q}\right)\right]^{l_1-k}
\end{aligned}$$

where $\mathbf{a}$ is chosen uniformly from $\mathrm{Z}_{\mathrm{q}}^{\mathrm{k}}$. For any $\mathbf{s} = (\mathrm{s}_1, \cdots, \mathrm{s}_k)^T \in Z_q^k$, let $\mathrm{h}_{\mathbf{s}} = \gcd(\mathrm{s}_1, \cdots, \mathrm{s}_k, \mathrm{q})$ and define the ideal

$$\mathbf{I}\mathbf{s} = (\mathrm{hs}\cdot \mathrm{Z}) = \mathrm{s}_1\mathrm{Z} + \cdots + \mathrm{s}_k\mathrm{Z} + \mathrm{qZ}\boxtimes\mathrm{Z}.$$

Let $|\frac{\mathrm{I}_s}{qZ}| = \mathrm{g}_{\mathbf{s}} = \mathrm{q}/\gcd(\mathrm{s}_1, \cdots, \mathrm{s}_k, \mathrm{q})$. Note that $\langle a, s\rangle$ is uniformly random on $\frac{\mathrm{I}_s}{qZ}$. Then

$$E_{\mathbf{a}}\left[\rho_{1/r}\left(Z + \frac{\langle \mathbf{a}, \mathbf{s}\rangle}{q}\right)\right] = \left|\frac{\mathrm{I}_s}{qZ}\right|^{-1} \rho_{1/r}\left(\frac{\mathrm{I}_s}{q}\right)$$

Then, the expectation is

$$\begin{aligned}
&\mathrm{E}_{\overline{\mathbf{A}}}\left[\rho_{1/r}(\Lambda^{\perp}(\mathbf{A}))^{\mathrm{V}}\right] \\
&= \sum_{\mathbf{s}\in Z_q^k} \rho_{1/r}\left(Z^k + \frac{\mathbf{s}}{q}\right) + E_{\mathbf{a}}\left[\rho_{1/r}\left(Z + \frac{\langle \mathbf{a}, \mathbf{s}\rangle}{q}\right)\right]^{l_1-k} \\
&= \rho_{1/r}Z^{l_1} + \sum_{\mathbf{s}\in Z_q^k, \mathbf{s}\neq 0 \bmod q} \rho_{1/r}\left(Z^k + \frac{s}{q}\right) \\
&+ E_{\mathbf{a}}\left[\rho_{1/r}\left(Z + \frac{\langle \mathbf{a}, \mathbf{s}\rangle}{q}\right)\right]^{l_1-k} \\
&\leq \rho_{1/r}Z^{l_1} + \sum_{I_{\mathbf{s}}, \mathbf{s}\neq 0 \bmod q} \left|\frac{I_{\mathbf{s}}}{qZ}\right|^{-(\mathrm{l}_1-\mathrm{k})} \\
&\cdot \rho_{1/r}\left(\frac{I_{\mathbf{s}}}{q}\right)^{(\mathrm{l}_1-\mathrm{k})} \cdot \left(\rho_{1/r}\left(\frac{I_{\mathbf{s}}}{q}\right)^k - 1\right) \\
&\leq \rho_{1/r}Z^{l_1} \\
&+ \sum_{I_{\mathbf{s}}, \mathbf{s}\neq 0 \bmod q} \left|\frac{I_{\mathbf{s}}}{qZ}\right|^{-(\mathrm{l}_1-\mathrm{k})} \cdot \left(\rho_{1/r}\left(\frac{I_{\mathbf{s}}}{q}\right)^{\mathrm{l}_1} - 1\right) \\
&= 1 + \sum_{I_{\mathbf{s}}} \left|\frac{I_{\mathbf{s}}}{qZ}\right|^{-(\mathrm{l}_1-\mathrm{k})} \cdot \left(\rho_{1/r}\left(\frac{I_{\mathbf{s}}}{q}\right)^{\mathrm{l}_1} - 1\right) \\
&\leq 1 + \sum_{\mathbf{s}} (\mathrm{g}_s)^{-(\mathrm{l}_1-\mathrm{k})} \cdot \left(\rho_{1/r}\left(\frac{Z}{g_s}\right)^{\mathrm{l}_1} - 1\right) \\
&\leq 1 + \sum_{\mathbf{s}} (\mathrm{g}_s)^{-(\mathrm{l}_1-\mathrm{k})} \left(\frac{\eta}{r}\right)^{l_1} (\mathrm{g}_s)^{l_1} \left(\rho_{1/\eta}(Z^{\mathrm{l}_1}) - 1\right) \\
&\left(\text{Let} \quad \eta > \frac{r}{g_s}\right) \\
&\leq 1 + \sum_{\mathbf{s}} (\mathrm{g}_s)^{\mathrm{k}} \left(\frac{\eta}{r}\right)^{l_1} \left(\rho_{1/\eta}(Z^{\mathrm{l}_1}) - 1\right)
\end{aligned}$$

Because $q = p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$. So we have

$$\begin{aligned}
&\sum_{\mathbf{s}} (\mathrm{g}_s)^{\mathrm{k}} \\
&= \prod_{i=1}^{t} \left(1 + \mathrm{p}_i^k + \mathrm{p}_i^{2k} + \cdots + \mathrm{p}_i^{k_i k}\right) \\
&= \prod_{i=1}^{t} \frac{1 - \mathrm{p}_i^{\mathrm{k}(k_i+1)}}{1 - \mathrm{p}_i^k} \\
&\leq \prod_{i=1}^{t} \frac{\mathrm{p}_i^{\mathrm{k}k_i}}{1 - \mathrm{p}_i^{-k}} \\
&= q^k \cdot \prod_{i=1}^{t} \left(1 - \mathrm{p}_i^{-k}\right)^{-1} \\
&= q^k \cdot e^{\ln \prod_{i=1}^{t} \left(1-\mathrm{p}_i^{-k}\right)^{-1}} \\
&= q^k \cdot e^{\sum_{i=1}^{t} \ln\left(1 + \frac{1}{p_i^k - 1}\right)} \\
&\leq e \cdot q^k.
\end{aligned}$$

So the above expectation is as the following

$$\begin{aligned}
&1 + \sum_{\mathbf{s}} (\mathrm{g}_s)^{\mathrm{k}} \left(\frac{\eta}{r}\right)^{l_1} \left(\rho_{1/\eta}(Z^{\mathrm{l}_1}) - 1\right) \\
&\leq 1 + q^k \cdot e\left(\frac{\eta}{r}\right)^{l_1} \left(\rho_{1/\eta}(Z^{\mathrm{l}_1}) - 1\right) \\
&\leq 1 + eq^k \cdot \left(\frac{\sqrt{l_1}}{r}\right)^{l_1} 2^{-2l_1} \left(\textit{Let} \quad \eta = \sqrt{l_1}\right) \\
&\leq 1 + 2^{-\Omega(k)} \left(\sqrt{l_1} < r < \sqrt{l_1}g_s\right)
\end{aligned}$$

Because of the fact that the matrix $\mathbf{A}$ contains an identity submatrix and Lemma24, then we can get the following more applicative corollary.

Corollary 32. Let Z, q, t, k, and l_1 be as in Theorem 31. Assume that $\mathbf{A} = (\mathbf{I}_k|\overline{\mathbf{A}}) \in (Z_q)^{k\times l_1}$ is chosen as in Theorem 31. Then, with probability $1-2^{-\Omega(k)}$ over the choice of $\mathbf{A}$, the distribution of $\mathbf{Ax} \in (Z_q)^k$, where each coordinate of $\mathbf{x} \in (Z_q)^{l_1}$ is chosen from a discrete Gaussian distribution with parameter r ($\sqrt{l_1} < r < \sqrt{l_1}g_s$) over Z, satisfies that the probability of each of the possible outcomes is within statistical distance $2^{-\Omega(k)}$ of the uniform distribution over $(Z_q)^k$.

Therefore, any random matrix $\mathbf{A}'$ chosen uniformly from ${Z_q}^{k\times l_1}$, after proper matrix elementary transformations, with great probability, can be written as the special formal $(\mathbf{I}|\overline{\mathbf{A}})$ where $\overline{\mathbf{A}} \in {Z_q}^{k\times(l_1-k)}$ is a uniformly random matrix. That is, $\mathbf{A}'\mathbf{T} =_c \mathbf{A} = (\mathbf{I}|\overline{\mathbf{A}}) \in {Z_q}^{k\times l_1}$, where $\mathbf{T}$ is the product of the proper elementary transformation matrices. Similarly, for a matrix $\mathbf{R} \in Z_q^{l_1\times l_2}$ whose entries are chosen from Gaussian distribution with parameter r ($\sqrt{l_1} < r < \sqrt{l_1}g_s$), we know that $\mathbf{AR}$ is a uniformly random matrix on $Z_q^{k\times l_2}$.

3.3 Framework of our new algorithm

By using the regularity theorem and its corollary obtained in the previous subsection, the algorithm for constructing a hard random lattice with a short basis is given in this subsection. Also, our construction is simple and guaranteed bound on basis quality.

Now we will give the common framework in Table 1.

$$\begin{aligned}&\mathbf{G}\cdot\mathbf{S}\\&= (\mathbf{I}\overline{\mathbf{A}}|\mathbf{A}_1)\begin{pmatrix}\mathbf{I}-\mathbf{RP} & -(\mathbf{R}+\mathbf{F})\mathbf{B}\\ \mathbf{P} & \mathbf{B}\end{pmatrix}\\&= \mathbf{0}\ \mathrm{mod}q\end{aligned}$$

Let $l = l_1 + l_2$ for some sufficiently large dimensions l_1 and l_2. Before discussing our algorithm, we first give a uniformly random matrix $\mathbf{A}' \in Z_q^{k\times l_1}$ and then using the proper elementary transformation matrices, we can obtain the special form matrix $\mathbf{A} = (\mathbf{I}|\overline{\mathbf{A}})$, where $\mathbf{A}$ is a uniformly random matrix with great probability.

Table 1 The framework for constructing the hard random lattice with a short basis

Algorithm 1. Framework for constructing the matrix $\mathbf{G} \in \mathbb{Z}_q^{k\times l}$ and the basis $\mathbf{S}$ of $\wedge^{\perp}(\mathbf{G})$.
Input: The random matrix $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times(l_1-k)}$
Output: $\mathbf{A}_1 \in \mathbb{Z}_q^{k\times l_2}$ and basis $\mathbf{S}$ of $\wedge^{\perp}(\mathbf{G})$, where $\mathbf{G} = [\mathbf{I} \mid \overline{\mathbf{A}} \mid \mathbf{A}_1] \in \mathbb{Z}_q^{k\times l}$ for $l = l_1 + l_2$
1. Generate component matrices $\mathbf{F}, \mathbf{R} \in \mathbb{Z}^{l_1\times l_2}$; $\mathbf{P} \in \mathbb{Z}^{l_2\times l_1}$; $\mathbf{B} \in \mathbb{Z}^{l_2\times l_2}$ such that $\mathbf{B}$ is nonsingular and $\mathbf{FP} + \mathbf{I} \subset \wedge^{\perp}(\mathbf{A})$ where $\mathbf{A} = [\mathbf{I} \mid \overline{\mathbf{A}}]$;
2. Let $\mathbf{A}_1 = \mathbf{A}(\mathbf{R}+\mathbf{F})$;
3. Let $\mathbf{S} = \begin{bmatrix}\mathbf{I}-\mathbf{RP} & -(\mathbf{R}+\mathbf{F})\mathbf{B}\\ \mathbf{P} & \mathbf{B}\end{bmatrix}$;
4. Return $\mathbf{A}_1$ and $\mathbf{S}$.

Our algorithm for constructing a hard random lattice with a short basis is given, where the input of the algorithm is the uniformly random matrix $\overline{\mathbf{A}} \in Z_q^{k\times(l_1-k)}$.

and $\overline{\mathbf{A}}$ can be extended to the matrix $\mathbf{G} = (\mathbf{A}|\mathbf{A}_1) = (\mathbf{I}|\overline{\mathbf{A}}|\mathbf{A}_1) \in Z_q^{k\times l}$ by generating $\mathbf{A}_1 \in Z_q^{k\times l_2}$ together with some short basis $\mathbf{S} = \begin{pmatrix}\mathbf{I}-\mathbf{RP} & -(\mathbf{R}+\mathbf{F})\mathbf{B}\\ \mathbf{P} & \mathbf{B}\end{pmatrix} \in Z^{l\times l}$ of $\wedge^{\perp}(\mathbf{G})$.

From Table 1, we can see that the output matrix $\mathbf{S}$ has a block structure, which contains four component matrices **B, F, P,** and **R**. The properties of the four matrices are as following:

- **B** is nonsingular and typically unimodular;
- **F** has entries that grow geometrically, which is a relationship to the parameter q and the special matrix **A**;
- **P** is a short matrix depending on **F** such that **FP** is short;
- **R** is a randomly short matrix whose entries are from Gaussian distribution with the parameter r where $\sqrt{l_1} < r < \sqrt{l_1}g_s$.

The matrix $\mathbf{A}'$ is uniformly random matrix on $Z^{k\times l_1}$, then the matrix $\mathbf{A}'\mathbf{T}$ is also uniformly random matrix which follows from the uniformity of $\mathbf{A}'$. We have the matrix $(\mathbf{A}'\mathbf{T}|\ \mathbf{A}'\mathbf{T}(\mathbf{R}+\mathbf{F})) = (\mathbf{A}|\ \mathbf{A}(\mathbf{R}+\mathbf{F}))$ is near-uniformly random because of random choice of **R** whose entries from Gaussian distribution by Theorem 3.1 and its corollary.

Since the matrix $\mathbf{A} = (\mathbf{I}|\overline{\mathbf{A}}) \in Z_q^{k\times l_1}$, and let $\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{x} : \mathbf{x} \in Z^{l_1}, \mathbf{Ax} = \mathbf{0}\ \mathrm{mod}q\}$. Obviously, the basis matrix of the lattice $\Lambda^{\perp}(\mathbf{A})$ can be obtained, that is, $\mathbf{H} = \begin{pmatrix}q\mathbf{I} & -\overline{\mathbf{A}}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}$.

Let $\mathbf{D} = \mathbf{R} + \mathbf{F}$, then we can get that

$$(\mathbf{A}|\mathbf{0})\begin{pmatrix}\mathbf{I} & \mathbf{D}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{I} & -\mathbf{D}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{H} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}\end{pmatrix} = \mathbf{0}\ \mathrm{mod}q,$$

That is,

$$(\mathbf{A}|\mathbf{AD})\begin{pmatrix}\mathbf{H} & -\mathbf{D}\\ \mathbf{0} & \mathbf{I}\end{pmatrix} = \mathbf{0}\ \mathrm{mod}q,$$

and we let the matrix $\mathbf{B}$ be a nonsingular matrix, then the block matrix $\begin{pmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{P} & \mathbf{B}\end{pmatrix}$ is also a nonsingular matrix, so we can get that

$$(\mathbf{A}|\mathbf{A}(\mathbf{R}+\mathbf{F}))\begin{pmatrix}\mathbf{H} & -(\mathbf{R}+\mathbf{F})\\ \mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{P} & \mathbf{B}\end{pmatrix} = \mathbf{0}\ \mathrm{mod}q,$$

that is,

$$(\mathbf{A}|\mathbf{A}(\mathbf{R}+\mathbf{F}))\begin{pmatrix}\mathbf{H}-(\mathbf{R}+\mathbf{F})\mathbf{P} & -(\mathbf{R}+\mathbf{F})\mathrm{B}\\ \mathbf{P} & \mathbf{B}\end{pmatrix} = \mathbf{0}\ \mathrm{modq},$$

Because the entries of the short random matrix **R** are from Gaussian distribution which leads to the matrix (**A**| **A**(**R** + **F**)) is uniformly random with great probability. Furthermore, **H** is the basis of $\Lambda^{\perp}(\mathbf{A})$ and **I** is the identity matrix, thus we have that

$$\begin{pmatrix}\mathbf{H}-(\mathbf{R}+\mathbf{F})\mathbf{P} & -(\mathbf{R}+\mathbf{F})\mathrm{B}\\ \mathbf{P} & \mathbf{B}\end{pmatrix} = \begin{pmatrix}\mathbf{I}-\mathbf{RP} & -(\mathbf{R}+\mathbf{F})\mathrm{B}\\ \mathbf{P} & \mathbf{B}\end{pmatrix}$$

is a nonsingular matrix.

In the block structure, we know the matrices **P**, **B**, and **R** are short matrices and so are the matrices **RP** and **RB**. But the norm of **F** is large, so we must use **B** to reduce the norm of the block matrix, such that the matrix **FB** is also short. Then, the block matrix $\begin{pmatrix}\mathbf{I}-\mathbf{RP} & -(\mathbf{R}+\mathbf{F})\mathbf{B}\\ \mathbf{P} & \mathbf{B}\end{pmatrix}$ is short. Simultaneously, we must ensure that the matrix equation **I** + **FP** = **H** is correct.

Lemma 33. The algorithm shows that if $\mathbf{I}+\mathbf{FP}\subset\Lambda^{\perp}(\mathbf{A})$, we have $\mathbf{S}\subset\Lambda^{\perp}(\mathbf{G})$. Moreover, **S** is a basis of $\Lambda^{\perp}(\mathbf{G})$ if and only if **I** + **FP** is a basis of $\Lambda^{\perp}(\mathbf{A})$.

Proof It is obvious that **A(I** + **FP) = 0** mod *q* implies **GS = 0** mod *q*, that is, $\mathbf{I}+\mathbf{FP}\subset\Lambda^{\perp}(\mathbf{A})$, implies $\mathbf{S}\subset\Lambda^{\perp}(\mathbf{G})$.

By the block structure of **S**, the determinant of **S** is

$$|\mathbf{S}| = \begin{vmatrix}\mathbf{I}-\mathbf{RP} & -(\mathbf{R}+\mathbf{F})\mathbf{B}\\ \mathbf{P} & \mathbf{B}\end{vmatrix} = |\mathbf{I}+\mathbf{FP}||\mathbf{B}|$$

Since the matrix **B** is nonsingular, that is $|\mathbf{B}|\neq\mathbf{0}$, then we have that the block matrix **S** is nonsingular if and only if the matrix **I** + **FP** is nonsingular. Because all the columns of $\mathbf{A}_1 = \mathbf{A}(\mathbf{R}+\mathbf{F})$ can be linearly represented by the columns of **A**, we have that the additive subgroup **G** $\boxtimes Z_q^n$ generated by the columns of **A** is exactly the subgroup generated by the columns of **G** = (**A**| **A1**). Therefore,

$$\det(\Lambda^{\perp}(\mathbf{G})) = |\mathbf{G}| = \det(\Lambda^{\perp}(\mathbf{A}))$$

Then **S** is a basis of $\Lambda^{\perp}(\mathbf{G})$ exactly when **I** + **FP** is a basis of $\Lambda^{\perp}(\mathbf{A})$.

Now, we know that the block matrix **S** is the basis of $\Lambda^{\perp}(\mathbf{G})$, then the remaining problem is that **S** must be relatively short. By the above discussion, we know that the matrices **B** and **R** are short, where **B** is unimodular and **R** is chosen from Gaussian distribution on $Z^{l_1\times l_2}$; moreover, the matrix **P** must be short and the columns of **I** + **FP** is ensured to be nontrivial vectors in $\Lambda^{\perp}(\mathbf{A})$. So a part of the matrix **F** should be long. Simultaneously, the matrix **FB** must be short because it is a part of −(**R** + **F**)**B** where **R** and **R** are short or a part of the block matrix **B**.

3.4 Concrete expression

The framework of our algorithm for constructing the hard random lattice with a short basis was given in the previous subsection. In this subsection, the concrete expression of each matrix in our algorithm will be shown as follows.

Given any random matrix **A'** uniformly on ${Z_q}^{k\times l_1}$, after proper matrix elementary transformations, **A'** can be written as $(\mathbf{I}|\overline{\mathbf{A}})$ where $\overline{\mathbf{A}}$ is uniformly matrix on ${Z_q}^{k\times(l_1-k)}$ with great probability. The chosen uniformly random matrix **A'** corresponds to the formal $\mathbf{A} = (\mathbf{I}|\overline{\mathbf{A}})$ where $\overline{\mathbf{A}}$ is uniformly random. So we can give $\overline{\mathbf{A}}$. By the discussion in the last subsection, **H** is the basis of $\Lambda^{\perp}(\mathbf{A})$, and let **H**=**I** + **FP**. So **FP**=**H**−**I**= $\begin{pmatrix}(q-1)\mathbf{I} & -\mathbf{A}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}$. Let *d* be an integer and $m = \log_d q$.

Definition of **F**: The matrix **F** has the formal

$$\mathbf{F} = \left(\mathbf{F}^{(1)}|\mathbf{F}^{(2)}|\cdots|\mathbf{F}^{(\mathrm{l}_1)}|\mathbf{0}\right)\in Z^{l_1\times l_2},$$

which has $l_1 + 1$ blocks containing l_1 blocks $\mathbf{F}^{(\mathrm{i})}(\mathrm{i} = 1, 2, \cdots, \mathrm{l}_1)$, each of which has m columns, and one zero block having remaining $l_2 - l_1 m$ columns. The first *k* blocks have the structure that the vector $\mathbf{f} = (f_1, f_2, \cdots, f_m) = (\lfloor\frac{q-1}{d^{m-1}}\rfloor, \lfloor\frac{q-1}{d^{m-2}}\rfloor, \cdots, \lfloor\frac{q-1}{d}\rfloor, q-1)$ is the *i*th row in $\mathbf{F}^{(i)}(i = 1, 2, \cdots, k)$ and other rows are zero vectors. The other $\mathrm{l}_1 - k$ blocks have the structure that $\mathbf{F}^{(k+i)} = (\lfloor\frac{-\mathbf{a}^{(i)}}{d^{m-1}}\rfloor, \lfloor\frac{-\mathbf{a}^{(i)}}{d^{m-2}}\rfloor, \cdots, \lfloor\frac{-\mathbf{a}^{(i)}}{d}\rfloor, -\mathbf{a}^{(\mathrm{i})})\ (i = 1, 2, \cdots, l_1-k)$ where $\mathbf{a}^{(i)}$ denotes the *i*th column of $\overline{\mathbf{A}}$. We can get that the entry of f_1 in each $\mathbf{F}^{(i)}$ is in the range [0,*r*−1].

Definition of **P:** The columns of the matrix $\mathbf{P} = (p_1, p_2, \cdots, p_{l_1})\in Z^{l_2\times l_1}$ are some identity vectors which are written as $\mathbf{p}_j = \mathbf{e}_{jm}\in Z^{l_2}$ where $j = 1, 2, \cdots, l_1$. This construction of **P** guarantees that **FP**=**H**−**I** and $\|\mathbf{p}_j\|^2 = 1(\mathrm{j} = 1, 2, \cdots, l_1)$.

Definition of **B:** Let the matrix $\mathbf{B}\in Z^{l_2\times l_2}$ be a unimodular matrix such that **FB** is short. Let $\mathbf{B}_m\in Z^{m\times m}$ be the unimodular matrix whose diagonal entries are 1, upper diagonal entries are −*d*, and zero entries elsewhere, that is,

$$\mathbf{B}_m = \begin{pmatrix}1 & -d & 0 & \cdots & 0 & 0\\ 0 & 1 & -d & \cdots & 0 & 0\\ 0 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & -d\\ 0 & 0 & 0 & \cdots & 0 & 1\end{pmatrix}.$$

Then define $\mathbf{B}\in Z^{l_2\times l_2}$ to be a block-diagonal matrix consisting of l_1 the block $\mathbf{B}_m$ and one identity matrix block $\mathbf{I}\in Z^{(l_2-l_1m)\times(l_2-l_1m)}$ in the main diagonal, and other blocks are zero matrices, that is,

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}_m & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_m & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{B}_m & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{I} \end{pmatrix}$$

and we can learn that $\|\mathbf{b}_i\|^2 \le d^2 + 1 (j = 1, 2, \cdots, l_2)$.

Then, $\mathbf{FB} = (\mathbf{F}^{(1)}\mathbf{B}_m|\mathbf{F}^{(2)}\mathbf{B}_m|\cdots|\mathbf{F}^{(l_1)}\mathbf{B}_m|\mathbf{0}) \in Z^{l_1 \times l_2}$, and all the entries of **FB** are in the range [0,d]. So the norm of each column of **FB** is less than or equal to $d\sqrt{l_1}$ and **FB** is short.

Definition of **R:** The entries of the matrix $\mathbf{R} \in Z^{l_1 \times l_2}$ are chosen randomly from Gaussian distribution with the parameter r where $\sqrt{l_1} < r < \sqrt{l_1} g_s$. Then by the Theorem 3.1, the entries of $(\mathbf{I}|\mathbf{A})\mathbf{R}$ are uniformly on Z_q with great probability. Because the parameter r is relatively large, we have that the vectors distributed according to Gaussian distribution have an average value very close to zero and expected squared distance from zero very close to $r^2 l_1/(2\pi)$. So the norm of **R** is less than or equal to $r\sqrt{l_1/(2\pi)}$.

The above discussion in this subsection shows that our algorithm for constructing the hard random lattice with a short basis is reasonable, and the basis of the dual lattice is indeed short. We will analyze the quality of the basis matrix **S** to prove the advantage of short in the next subsection.

3.5 Analysis and comparison

We analyze the norm of the basis matrix **S** in this subsection. Firstly, we have that

$$\|\mathbf{S}\|^2 \le \max\left\{\|\mathbf{I}-\mathbf{RP}\|^2 + \|\mathbf{P}\|^2, (\|\mathbf{RB}\| + \|\mathbf{FB}\|)^2 + \|\mathbf{B}\|^2\right\}$$

From the discussion in the previous subsection, we know that $\|\mathbf{P}\|^2 = 1$ and $\|\mathbf{I}-\mathbf{RP}\|^2 \le (r\sqrt{l_1/(2\pi)} + 1)^2$. Then,

$$\|\mathbf{I}-\mathbf{RP}\|^2 + \|\mathbf{P}\|^2 \le 2r^2 l_1/(2\pi).$$

Then we consider the other part, $\|\mathbf{FB}\|^2 \le l_1 d^2$, $\|\mathbf{RB}\|^2 \le (d+1)^2 r^2 l_1/(2\pi)$, and $\|\mathbf{B}\|^2 \le d^2 + 1$. So we have

$$\begin{aligned} &(\|\mathbf{RB}\| + \|\mathbf{FB}\|)^2 + \|\mathbf{B}\|^2 \\ &\le 4\|\mathbf{RB}\|^2 \\ &\le 4(d+1)^2 r^2 l_1/(2\pi) \end{aligned}$$

Our construction for generating a hard random lattice with a short basis was from a new perspective and our algorithm in the construction first used a random matrix whose entries were obeyed Gaussian distribution, not an independent $\{0, \pm 1\}$-valued random variable in [12] or uniform distribution from the set {0,1} in [11] as shown in Table 2, and the parameter q is a large regular, which ensure that our algorithm has a wider application future in cryptography area. Moreover, our construction is more specific than the previous constructions which makes our construction be implemented easier in practical applications. What is more, the problem we discussed is the basis of lattice-based cryptograph, so it can resist the attack by quantum computers.

Table 2 The comparison on distribution of random matrix *R*

R	distribution of **R**
[11]	uniform distribution from the set $\{0, 1\}$
[12]	independent $\{0, \pm 1\}$-valued random variable
ours	Gaussian distribution

4 Conclusion

In this paper, we firstly have proved a fact that a uniformly random matrix contains an invertible submatrix and using elementary transformations the uniformly random matrix can be transformed into the special matrix which contains two parts, an identity matrix part and a uniform matrix part. Secondly, a useful regularity theorem and its corollary on Z_q has been proved and the useful parameters could be obtained. Thirdly, using the above fact and corollary, a new construction of hard random lattice with a short basis have been proposed, and then we have given the framework of our algorithm. Fourthly, the concrete expression of our construction, that is the concrete form of the matrices in our algorithm, has been given. Lastly, we have analyzed the quality of the short basis **S**, which shows that the quality of the short basis in our algorithm is as same as the Alwen and Peikert algorithm.

Acknowledgements

This work is supported by National Key R&D Program of China (no. 2017YFB0802400), National Science Foundation of China (no. 61373171) and the 111 Project (no. B08038).

Funding

This work is supported by National Key R&D Program of China No. 2017YFB0802400, National Science Foundation of China under grant no. 61373171 and the 111 Project under grant no. B08038.

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Authors' contributions

All authors actively participated in the discussions, and read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Author details
[1]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi 710071, People's Republic of China. [2]Department of Mathematics, Xi'an Polytechnic University, Xi'an, Shaanxi 710048, People's Republic of China. [3]Computer Engineering College, Jimei University, Xiamen, Fujian 361021, People's Republic of China.

Received: 22 January 2019 Accepted: 16 April 2019
Published online: 10 June 2019

References

1. C. Peikert, in *Annual Cryptology Conference*. An efficient and parallel Gaussian sampler for lattices (Springer, Berlin, 2010), pp. 80–97
2. Z. Brakerski, V. Vaikuntanathan, in *Adannces in Cryptology -CRYPTO 2011*. Fully homomorphic encryption from ring-LWE and security for key dependent message (2011), pp. 505–524
3. S. Dov Gordon, J. Katz, V. Vaikuntanathan, in *Advances in cryptology -ASIACRYPT 2010*, Lecture Notes in Computer Science. A group signature scheme from lattice assumptions, vol 6477 (2010), pp. 395–412
4. V. Lyubashevsky, C. Peikert, O. Regev, in *Advances in Cryptology C EUROCRYPT 2010*. On ideal lattices and learning with errors over rings (2010), pp. 1–23
5. V. Lyubashevsky, C. Peikert, O. Regev, in *Advances in Cryptology C EUROCRYPT 2013*. A Toolkit for Ring-LWE Cryptography (2013), pp. 35–54
6. S. Ling, K. Nguyen, D. Stehl, et al., in *Public-Key CryptographyCPKC 2013*. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications (Springer, Berlin, 2013), pp. 107–124
7. D. Micciancio, C. Peikert, in *Advances in Cryptology C EUROCRYPT 2012*. Trapdoor for lattices: simpler, tighter, faster, smaller (2012), pp. 700–718
8. O. Regev, Lattice-based cryptography[C]. Annual International Cryptology Conference. (Springer, Berlin, Heidelberg, 2006), pp. 131–141
9. C. Peikert, B. Waters, Lossy trapdoor functions and their applications[J]. SIAM J. Comput. **40**(6), 1803–1844 (2011)
10. T. Poppelmann, Efficient implementation of ideal lattice-based cryptography. Inf. Technol. **59**(6), 305–309 (2017)
11. M. Ajtai, in *International Colloquium on Automata, Languages, and Programming*. Generating hard instances of the short basis problem (1999), pp. 1–9
12. J. Alwen, C. Peikert, Generating shorter bases for hard random lattices. Theory Comput. Syst. **48**(3), 535–553 (2011)
13. V. Lyubashevsky, D. Micciancio, in *Advances in Cryptology-CRYPTO 2009*. On bounded distance decoding, unique shortest vectors, and the minimum distance problem (2009), pp. 577–594
14. T. Laarhoven, M. Mosca, J. Van De Pol, Finding shortest lattice vectors faster using quantum search. Des. Codes Crypt. **77**(2–3), 375400 (2015)
15. M. Ajtai, in *ACM Symposium on Theory of Computing -STOC*. Generating hard instances of lattice problem-s (1996), pp. 99–108
16. C. Gentry, C. Peikert, V. Vaikuntanathan, in *Proceedings of the fortieth annual ACM symposium on Theory of computing*. Trapdoors for hard lattices and new cryptographic constructions (2008), pp. 197–206
17. D. Micciancio, O. Regev, Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. **37**(1), 267–302 (2007)