RESEARCH ARTICLE OPEN ACCESS

A Theoretical Aspect of Lattice Based Cryptography

Manoj Kumar
Srinivasa Ramanujan Department of Mathematics,
Central University of Himachal Pradesh,Dharamshala,Kangra,
Himachal Pradesh-176215, India.

ABSTRACT
The gap factor γ of lattice problems (e.g., SVP, CVP, SIVP etc.) and sampling technique have an importance in lattice-based cryptography. In the ideal lattices, we introduce similar problems and expansion factor (like the gap factor in lattice problems). We also state some results related to ideal lattices.

Keywords-Lattice, cryptographic primitive, hash function, expansion factor.

I. INTRODUCTION

Public key cryptography has a vital role in our daily life. The first idea is DH-Key Exchange Protocol introduced by W. Diffie and M. Hellman in 1976[3], which is based on the Discrete Logarithmic Problem (DLP) over a finite field, say$\mathbb{Z}_q$, where q is a prime number.

The best and well-known public key encryption scheme based on the factorization of integers known as RSA was introduced in 1978[17]. ElGamal[4] studied public key cryptosystem and a signature scheme based on discrete logarithms. Elliptic Curve Cryptography (ECC) was introduced independently by Miller in 1985[14], and later by Koblitz in 1987[7] using the Elliptic Curve Discrete Logarithmic Problem (ECDLP) over a finite field. Most of these problems (factorization of integers, DLP and elliptic curve version of DLP) are based on number theoretic transformation.

C. Gentry, C. Peikert and V. Vaikuntanathan[2] invented preimage sampleable trapdoor functions. They considered the value of error term large enough so that many preimages exist. M. Ajitai in 1996[1] proposed the first worst-case to average-case reduction for a lattice problem. Ajtai proved that solving some NP-hard lattice problems, e.g., Shortest Vector Problem (SVP), in the average case is as hard as solving the worst-case assumption and also formulated the SIS problem.

However, the applications of cryptography that are related to SIS are inherently inefficient due to the size of the associated key or public data, whichmeans such schemes are essentially unable to achieve its maximum potential. In 1998, Hoffstein, Pipher and later by J. H. Silverman [6] developed the NTRU cryptosystem, which is a milestone in the history of cryptography.

Also, in 2005 [18], O. Regev has proposed the LWE problem (Learning with Error) which is based on uniform distribution and error distribution) and have many applications and also used in public key cryptography and CCA secure cryptosystem. The secret key s (say) is chosen uniformly at random from $\mathbb{Z}_q^n$ and error distribution like a Discrete Gaussian Distribution. If we choose the secret key s from the polynomial ring, then we have another version of LWE, called R-LWE problem.

II. ALGEBRAICNOTATIONS

By $L \subset \mathbb{R}^n$, we mean a lattice. The ring of polynomials with integer coefficients is denoted by $\mathbb{Z}[x]$ and the quotient ring of polynomials is denoted by $R = \frac{\mathbb{Z}[x]}{(f(x))}$, where $f(x)$ is monic irreducible polynomial of degree n. Every equivalence class $(g + (f)) \in \frac{\mathbb{Z}[x]}{(f(x))}$ has a unique representative $g' \in (g + (f))$ of degree less than n. This representative is denoted by $(g \bmod f)$ and can be efficiently computed using the standard division algorithm. Every polynomial $g(x) = g_0 + g_1 x^1 + \cdots + g_{n-1} x^{n-1}$ have a representation in an n-dimensional vector $(g_0, g_1, \dots, g_{n-1})$.

The ring $\frac{\mathbb{Z}[x]}{(f(x))}$ is endowed with the (infinity)norm $||g+(f)||_f = ||g\mathrm{mod}f||_\infty$. The function $||.||_f$ also well-defined, that is, it does not depend on the choice of representative g. Further, we consider q as a prime power of 2, where q is a prime number.

III. LATTICES

In this section, we define the concept of minimum distance in lattices and a brief discussion of q-ary lattices.

Definition: 3.1*The m-dimensional lattice L is a discrete additive subgroup of R^m. Formally, L is the set of all integer linear combinations $\sum_{i=1}^{\infty} x_i\, z_i : x_i \in \mathbb{Z}$ of n linearly independent vectors $z_1, z_2, \ldots, z_n \in \mathbb{R}^m$, where $n \leq m$. The set of linearly independent vectors $z_1, \ldots, z_n$ is called a basis for the lattice, and can be compactly represented by the matrix B having the basis vectors as columns.*

We analogously define the notions of determinant, rank and the dual lattice, which are defined in vector spaces and also similar results of vector spaces, e.g., a lattice have more than one basis, that is, basis are not unique in the lattices. Lattices can also be represented as $Bx : x \in \mathbb{Z}^n$, where Bx is matrix-vector multiplication. The lattice generated by B is denoted $L(B)$.

The minimum distance in $L(B)$

The minimum distance of a lattice $L(B)$ is the minimum distance between any two (distinct) lattice vector and equals the length of shortest nonzero lattice vector. The minimum distance can be defined with respect to any norm.

For any $p \geq 1$,the $l_p$norm of a vector$x$is defined by

$$\left||x|\right|_p = \sqrt[p]{\sum_i |x_i|^p}$$

and the corresponding minimum distance is defined as

$$\lambda_1^p \min = ||x-y||_p : x \neq y \in L(B)$$

$$= \min\{||x||_p : x \in L(B)\backslash\{0\}\}.$$

The notion of minimum distance can be generalized to define the i^{th} successive minimum (in the $l_p$norm) $\lambda_i^p\left(L(B)\right)$ as the smallest radius r such that the closed sphere $S_p[0,r] = \{x : ||x||_p \leq r\}$ contains i linearly independent lattice vectors, that is,

$\lambda_i^p\left(L(B)\right) = \min\{r : dim\left(span\left(L(B) \cap\right.\right.$ *Sp0,r≥i}.*

Recall that, the infinity norm is defined as

$$\left||x|\right|_\infty = \lim_{p\to\infty}\left||x|\right|_p = \max|x_i|.$$

Also, the infinity norm is most natural and convenient norm when dealing with polynomials. It is easy to see that $\lambda_1^p \leq \lambda_2^p \leq, \ldots, \leq \lambda_n^p$.

q-array Lattices

The lattices $L(B)$ which satisfying the condition $q\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$ for a prime (possible) integer q. In other words, the membership of a vector x in lattice $L(B)$ is determined by x mod$q$.

Definition: 3.2(q-ary Lattices)*Given a matrix $M \in \mathbb{Z}_q^{n\times m}$, where q, n and m are positive integers. The two m dimensional q-ary lattice is defined as follows:*

$$L_q(M) = \{y \in \mathbb{Z}^m : y \equiv M^t s\ modq\}$$

for some s in $\mathbb{Z}^n$. And

$$L_q^\perp(M) = \{y \in \mathbb{Z}^m : My \equiv 0\ modq\}.$$

Note that the first q-ary lattice is generated by the rows of M, while the second contains all vectors that are orthogonal mod$q$ to the rows of M.

The dual of the Lattices $L(B)$ in $\mathbb{R}^m$, denoted by L^*, which is the lattice given by set of all vectors $z \in \mathbb{R}^m$ satisfying $\langle x, z\rangle \in \mathbb{Z}$ for all $x \in L$.

IV. THE GAUSSIAN SAMPLER

The Gaussian Sampler is the most and well-known sampling algorithm in lattice based digital signature scheme are defined by

$$D_{L,s,c} = \exp\left(\frac{-\pi||v-c||^2}{s^2}\right),$$

where $s > 0$ and $c \in \mathbb{R}^n$ are parameters of the Discrete Gaussian Sampler akin to its standard deviation and mean. Here v is the point of lattice L. If $B = \{b_1, \ldots, b_n\}$ is the basis of the lattice L, then the Gaussian Sampler depends only on the maximal length of $B's$ Gram-Schmidt vectors.

The Sampler Component

The quality of a discrete Gaussian sampler is determined by a tuple of three parameters s, λ, and

τ, where s is the standard deviation (adjusts dispersal of data from the mean), λ is the precision parameter (controls statistical difference between a perfect and implemented discrete Gaussian sampler), and τ is the distribution tail-cut (determines amount of the distribution that we would like to ignore). Each of these parameters affects the security and efficiency of the sampler. For encryption/decryption schemes, the value of $s = 3.33$ is suggested. Digital signature sampling from a Gaussian Sampler involves a large value of deviation $s = 215$.

V. LATTICE PROBLEMS, PROBLEMS OF RING AND REDUCTION ALGORITHMS

In this section, we study lattice problems, which are useful in the security proof of lattice based digital signature scheme. There are several lattices' problems, we discuss some problems. Further, we study problems of ring and lattice reduction algorithms. We assume that all the lattice vectors are non-zero.

Worst Case Lattice Problems

Definition: 5.1(Shortest Vector Problem (SVP))

Find a lattice vector x whose length is shortest among all the lattice vectors, that is,

$$||x|| \leq ||y|| \; for\ all,\ y \in L(B).$$

Definition: 5.2(Closest Vector Problem (CVP))

Suppose $p \in \mathbb{R}^n$ is the target vector, not necessarily lies in the lattices.Then find a vector $x \in L(B)$ such that

$$||x-p|| \leq ||y-p|| \; for\ all\ y \in L(B).$$

The SVP and CVP problems are considered to be computationally hard to solve, with both classical and quantum algorithm. In the regard of these lattice problem, we state a conjecture.

Conjecture: 5.3*There does not exist any probabilistic polynomial time algorithm that approximates lattice problem to within polynomial factors.*

Thus, approximate versions of these problems are also considered. Let B be the basis of the lattice L.

Definition: 5.4(Approximate SVP)

The approximate variation of SVP is to allow the gap function $\gamma \geq 1$ in the sense, to find a non zero lattice vector $x \in L(B)$ such that

$$||x|| \leq \gamma||y|| \; for\ all\ y \in L(B).$$

Definition: 5.5(Approximate CVP)

Find a non-zero lattice vector $x \in L(B)$ such that

$$||x-p|| \leq \gamma||y-p|| \; for\ all\ y \in L(B).$$

Definition: 5.6(Shortest Independent Vector Problem (SIVP))

Find a set $S \subset L(B)$ of n linearly independent vectors such that $||S|| \leq \lambda_n$.

We also define Approximate SIVP (using γ in SIVP). The approximate version, say, Approximate SVP should be significant easier than the SVP and CVP. Even the best algorithms are often impractical for sufficiently large value of the gap factor γ.

Problems of Ring

We give the notion of R-SIS (also called f-SIS) over the ring $R = \frac{\mathbb{Z}_q[x]}{(f)}$.

Definition: 5.7(f-SIS)

Suppose m uniformly random polynomials $a_1, \dots, a_m$ are given, then to find the elements $y_1, \dots, y_m$ with small coefficients such that $\sum_{i=1}^{m} a_i\, y_i = 0$ in the ring $\frac{\mathbb{Z}_q[x]}{(f)}$.

We also define another problem of rings R as follows:

Definition: 5.8(Generalized Compact Knapsack Problem)

Given m random elements $a_1, \dots, a_m$ in the ring R and a target $t \in R$, find $z_1, \dots, z_m \in D$ such that $\sum_{i=1}^{m} a_i\, z_i = t$. where D is a fixed subset of R.

Lattice Reduction Algorithm

The Fundamental theorem of linear algebra states that any finite dimensional vector space has a basis. Also, we know that every finite dimensional Euclidean space has an orthogonal basis. On the other hand, a lattice may not have an orthogonal basis. The goal of lattice reduction is to get a lattice basis, which is not far from being orthogonal.

A. LLL Algorithm

The best reduction algorithm for lattice problem is the LLL algorithm, developed in 1982 [8], an approximation algorithm to the shortest vector problem (SVP), by A. K.

Lenstra, H. W. Lenstra and L. Lovasz. This algorithm takes as input a basis of a lattice and outputs a lattice basis consisting of smaller vectors called a reduced basis. The LLL algorithm is a polynomial time algorithm for SVP and for most other basic lattice problems that achieves an approximation factor of $2^{O(n)}$, where n is the dimension of the lattices. In 1987, C. P. Schnorr presented an extension of the LLL algorithm with a better approximation factor.

B. Babai's Nearest Plane Algorithm

The Babai's nearest plane algorithm uses induction on the dimension n of the lattice. The idea is as follows, consider a plane (vector space) generated by $(n-1)$ lattice vectors. Find the translated plane at each lattice point. Choose the one which is nearest to the target vector. Inductively apply the algorithm to the sub-lattice generated by those $(n-1)$ vectors and to the new translated target vector.

More precisely, let $U = \text{span}\ \{b_1, \dots, b_{n-1}\}$ and let $L^{'} = L \cap U$ be the sub-lattice spanned by $\{b_1, \dots, b_{n-1}\}$. Now to find a vector v such that plane U+v is nearest to the target vector w. Now take the new target vector w'' = w' - v, where w' is projection of w to the plane U+v. Inductively work out closest vector v' to w'' in $L^{'}$ and output v + v'.

The GGH Cryptosystem

Goldreich, Goldwasser and Halevi (GGH) proposed a cryptosystem [5] using the closest vector problem (CVP), that is, GGH's security depends on the difficulty of the CVP. Intuitively, CVP involves finding the lattice point to an arbitrary point. In a GGH key pair, a public key is a “bad" basis and a private key is a “good" basis. A “good " basis is close to orthogonal with short basis vectors. There exist algorithms for approximating CVP for a “good" basis. One such algorithm is called Babai's closest vector algorithm.

Babai's algorithm takes a point w and a set of basis vector $[v_1, \dots, v_n]^t$ as input, where t denotes the transpose. The algorithm then solves$w = t_1 \star v_1 + \cdots + t_n \star v_n$, where $[t_1, \dots, t_n]^t$ are real number coefficients. Babai's algorithm then approximates a solution to CVP by rounding all coefficients $t_1, \dots, t_n$ to their nearest integer.

For short and approximately orthogonal bases, Babai's algorithm work well and likely returns the closest lattice point to w and for “bad" bases, Babai's algorithm is likely to return a lattice point that is not close to w.

How does GGH use CVP?

GGH takes advantage CVP's assumed difficulty for “bad" bases to create an asymmetric key pair. GGH key pair consists of two bases for the same lattice, one public basis and one private basis. A plaintext message is encoded as a vector with integer coefficients and ciphertext is a vector that is not a lattice point.

1. STRUCTURES OF IDEAL LATTICES

In this section, we give brief details of various kind of lattices using the quotient polynomial ring. The properties of ideal lattices are studied in many papers, for example see [9,10,11,12,15,16]. First, we state the hash function and collision resistant hash function. We also define the expansion factor in the quotient polynomial ring, which is a powerful tool in the ideal lattices.

Hash Function

Given a ring $R = \frac{\mathbb{Z}_q[x]}{(f)}$, where $f \in \mathbb{Z}[x]$ is a monic, irreducible polynomial of degree n and q is a prime integer of order roughly n^2, generate m random elements $a_1, \dots, a_m \in R$, where m is a constant. The order m-tuple $h = (a_1, \dots, a_m) \in R^m$ is our hash function. It will map elements in D^m, where D is a strategically chosen subset of R.

For an element $b = (b_1 \dots b_m) \in D^m$, the hash value is $h(b) = \sum_{i=1}^{m} a_i\, b_i$. Notice that the size of the key (hash function) is $O(mn \log p) = O(n \log n)$, and the operation $a_i . b_i$ can be done in time $O(n \log n \operatorname{loglog} n)$ by using the fast Fourier transform, for appropriate choice of the polynomial f. Since m is a constant, hashing requires time $O(n \log n \operatorname{loglog} n)$.

To prove, our hash function is collision resistant, we will show that, if there is a polynomial time algorithm that succeeds with some non-negligibly probability in finding $b \neq b^{'} \in D^m$ such that $h(b) = h(b^{'})$, for a randomly chosen hash function $h \in R^m$. Then a certain problem called the shortest polynomial problem, which is solvable in polynomial time for every ideal of the ring $\frac{\mathbb{Z}[x]}{(f)}$.

Ideal Lattices

Suppose $f(x)$ be a monic polynomial of degree n in $\mathbb{Z}[x]$ and we consider the quotient polynomial ring

$\frac{\mathbb{Z}[x]}{(f)}$. This becomes a lattice via the coordinate embedding. Fix a basis $x_0, x_1, \dots, x_{n-1}$ for $\mathbb{R}^n$ and consider the linear map ϕ defined by $\phi\colon \frac{\mathbb{Z}[x]}{(f)} \to \mathbb{R}^n$ such that $\phi(x^i) = x_i$. Since, we can pick any coefficients from $\mathbb{Z}$ to define a polynomial in $\frac{\mathbb{Z}[x]}{(f)}$, then the image $L = \phi(J) \subset \mathbb{R}^n$ is called an ideal lattice, where J is an ideal of the ring $\frac{\mathbb{Z}[x]}{(f)}$. As the name suggests, this is also a lattice and has rank n.

Cyclic Lattices

D. Micciancio[13] defined a cyclic lattice to be a lattice L such that if the vector $(a_1, \dots, a_{n-1}, a_n) \in L$ then the vector $(a_n, a_1 \dots, a_{n-1})$ is also in the lattice L. Such lattices correspond to ideals in $\frac{\mathbb{Z}[x]}{(x^n-1)}$. Micciancio gave a construction of an efficient family of one-way functions with security based on the worst-case hardness of approximating $\lambda_1(L)$ in cyclic lattices. The ring $\frac{\mathbb{Z}[x]}{(x^n-1)}$ is called cyclotomic ring and has several useful properties enabling fast computation. The cyclotomic ring is also a basis for the NTRU cryptosystem [6].

Integer Lattices

Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n and consider the quotient polynomial ring $\frac{\mathbb{Z}[x]}{(f)}$. Using the standard set of representatives $(g \bmod f)\colon g \in \mathbb{Z}[x]$ and our identification of polynomials with vectors, the quotient ring $\frac{\mathbb{Z}[x]}{(f)}$ is isomorphic (as an additive group) to the integer lattice $\mathbb{Z}^n$. Any ideal $J \subseteq \frac{\mathbb{Z}[x]}{(f)}$ defines a corresponding integer sub lattice $L(J) \subseteq \mathbb{Z}^n$. Note that, not every integer lattice $L(B) \subseteq \mathbb{Z}^n$ can be represented in this form. Thus, we define ideal lattices as lattice that admit suchrepresentation.

<u>Definition: 6.1(Integer Lattices)</u>

An ideal lattice is an integer lattice $L(B) \subset \mathbb{Z}^n$ such that, $L(B) = \{g \bmod f\colon g \in J\}$ for a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n and an ideal $J \subseteq \frac{\mathbb{Z}[x]}{(f)}$.

It turns out that, the relevant properties of f for the resulting function to be collision resistant are:

a. f should be an irreducible polynomial.

b. The ring norm $||g||_f$ is not much bigger than $||g||_\infty$ for any polynomial g.

The first property implies that every ideal of the ring $\frac{\mathbb{Z}[x]}{(f)}$ defines a full-rank lattice in $\mathbb{Z}^n$.

<u>Remark: 6.2</u>*If $f(x) = x^n - 1$ be a reducible polynomial then the corresponding lattice is not an ideal lattice.*

Consider the ideal lattice $L(B) = \{g \bmod f\colon g \in J\}$ and the ideal $J \subseteq \frac{Z[x]}{(f(x))}$. Then a vector is in the ideal lattice if and only if its corresponding polynomial is in the ideal, that is,

$$(f_0, \dots, f_{n-1}) \subseteq L(B) \Leftrightarrow f_0 + f_1 x + \dots + f_{n-1} x^{n-1} \in J.$$

Now, we give a result [11, Lemma 3.2] related to a property of ideal lattices.

<u>Lemma: 6.3</u>*Every ideal lattice of $\frac{\mathbb{Z}[x]}{(f)}$, where f is a monic irreducible integer polynomial of degree n, is isomorphic to a full rank lattice in $\mathbb{Z}^n$.*

The second property is crucial for the security purpose, if the ratio $\frac{||g||_f}{||g||_\infty}$ have small value, then it is suitable for the cryptographic function. We elaborate on the second property by defining a quantitative parameter (the expansion factor) that captures the relation between $||.||_f$ and$||.||_\infty$

The Expansion Factor

We note that, when we reduce a polynomial $g \bmod f$, the maximum coefficients of g can increase by quite a bit, and thus $||g||_f$ could be a lot bigger than $||g||_\infty$. For example, if $f(x) = x^n - 2x^{n-1}$, then $x^{2n} = 2^{n+1}x^{n-1} (\bmod f)$.

On the other hand, if $f(x) = x^n - 1$, we can never have such an exponential growth of coefficients. We capture this property of $f(x)$ by defining the expansion factor of $f(x)$ as follows:

$$EF(f,k) = \max_{g \in \mathbb{Z}[x], deg\,(g) \leq k(deg\,(f)-1)} \frac{||g||_f}{||g||_\infty}.$$

Now, we give a theorem related to expansion factor, which gives a tight bounds for $EF(.)$ of certain polynomial.

<u>Theorem: 6.4</u>*The following conditions hold:*

a. $EF(1 + x + \dots + x^{n-1}, k) \leq 2k.$

b. $EF(1 + x^n, k) \leq k.$

Ideal Lattice Problem

Definition: 6.5In the approximate Shortest Polynomial Problem $\left(SPP_{\gamma}(I)\right)$, we are given an ideal $I \subset \frac{\mathbb{Z}[x]}{f(x)}$ where f is a monic polynomial of degree n and we are asked to find a $g \in I$ such that $g \neq 0$ and $||g||_f \leq \gamma\lambda_1^{\infty}(I)$.*

As for the shortest vector problem, we can consider the restriction of SPP to specific classes of ideals. We will write f-SPP for SPP restricted to ideals of the ring $\frac{\mathbb{Z}[x]}{f(x)}$. Now, we define the incremental version of SPP. In this version, we are not looking for the shortest polynomial, but for a polynomial that is smaller than the one given to us.

Definition: 6.6In the approximate Incremental Shortest Polynomial Problem $\left(IncSPP_{\gamma}(I,g)\right)$, we are given an ideal I and a $g \in I$ such that $||g||_f \geq \gamma\lambda_1^{\infty}(I)$ and are asked to return an $h \in I$ such that $||h||_f \neq 0$ and $||h||_f \leq \frac{||g||_f}{2}$.*

We define the restricted version of IncSPP in the same way as the restricted version for SPP. Let us give a lemma which shows that if I is an ideal of $\frac{\mathbb{Z}[x]}{(f)}$, where f is monic and irreducible polynomial then $\lambda_n^{\infty}(I)$cannot be much bigger than $\lambda_1^{\infty}(I)$.

Lemma: 6.7For all ideals I of $\frac{\mathbb{Z}[x]}{(f)}$, where f is monic, irreducible, polynomial of degree n, we have*

$\lambda_n^{\infty}(I) \leq EF(f,2)\lambda_1^{\infty}(I)$.

*Proof:*Let g be a polynomial in I of degree less than n such that $||g||_{\infty} = \lambda_1^{\infty}(I)$. Consider the polynomial $g, gx, \ldots, gx^{n-1}$. By Lemma 6.3, these polynomials are linearly independent. Since the maximum degree of any of this polynomial is $2n-2$,

$$||gx^i||_f \leq EF(f,2)||gx^i||_{\infty} \leq EF(f,2)||g||_{\infty} = EF(f,2)\lambda_1^{\infty}(I)$$

for all $0 \leq i \leq n-1$.

Remark: 6.8 The collision resistant hash function has importance in cryptographic application under some suitable choices of parameters. Sometimes, we call these parameters as instantiation parameters.*

REFERENCES

[1] M. Ajtai, Generating hard instances of lattices problems, In: Proc. STOC. (1996), p. 99–108.

[2] G. Craig, P. Chris and V. Vinod, Trapdoors for hard lattices and new cryptographic constructions, STOC'08 ACM (2008), p. 197–206.

[3] W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory IT-22 (6) (1976), p. 644–654.

[4] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transaction Information Theory 31(4) (1985), p. 469–472.

[5] O. Goldreich, S. Goldwasser and S. Halevi, Collision-free hashing from lattice problems, IACR Cryptol. ePrint Arch. (1996), p. 9.

[6] J. Hoffstein, J. Pipher and J. H. Silverman, NTRU: A ring-based public key cryptosystem, In International Algorithmic Number Theory Symposium (1998), p. 267-288.

[7] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48(177) (1987), p. 203-209.

[8] A. K. Lenstra, H. W. Lenstra Jr. and L.Lovasz, Factoring polynomials with rational coefficients, MathematischeAnnalen 261 (1982), p. 513-534.

[9] V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, In Annual International Conference on the Theory and Applications of Cryptographic Techniques (2010), p. 1–23.

[10] V. Lyubashevsky, Digital signatures based on the hardness of ideal lattice problems in all rings, In International Conference on the Theory and Application of Cryptology and Information Security (2016), p.196–214.

[11] D. Micciancio and V. Lyubashevsky, Generalized compact knapsack are collision resistent, In International Colloquium on Automata, Languages, and Programming (2006), p. 144-155.

[12] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one way functions from worst- case complexity assumptions, In FOCS (2002), p. 356-365.

[13] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions, Computational Complexity 16(4) (2007), p. 365-411.

[14] V. S. Miller, Use of elliptic curves in cryptography, In Conference on The Theory and Application of Cryptographic Techniques (1985), p. 417–426.

[15] C. Peikert, A decade of lattice cryptography, Foundations and Trends in Theoretical Computer Science 10(4) (2016), p. 283–424.

[16] C. Peikert and A. Rosen, Efficient collision-resistant hashing from worst- case

assumptions on cyclic lattices, In Theory of Cryptography Conference (2006), p. 145–166.

[17] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of The ACM 21(2) (1978), p. 120–126.

[18] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, STOC'05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing (2005), p. 84–93.