Improving the Stability of Cryptographic Algorithms on Algebraic Lattices

Olha Petrenko [1], Oleksii Petrenko [2]

[1] *Kharkiv National University of Radio Electronics, Nauky Ave. 14, Kharkiv, 61166, Ukraine*
[2] *Ivan Kozhedub Kharkiv National Air Force University, Sumska Str. 77/79, Kharkiv, 61023, Ukraine*

Abstract

The paper considers a way to increase the stability of the NTRU Encrypt algorithm by replacing the uniform distribution with a normal one when generating encryption keys to increase the stability of transformations. The use of fast Fourier sampling to reduce the number of operations when performing encryption is justified.

Keywords

Algebraic lattices, NTRU Encrypt algorithm, fast Fourier transform, normal distribution.

1. Introduction

With the constant process of improving quantum computers, which leads to increase in the number of qubits, the classic encryption algorithms can be rapidly hacked. [1] Given this, there is a necessity of developing and further improving of the algorithms, which are able to counteract cryptanalysis in the post-quantum period. The question of defining and substantiating the size of their parameters and conditions of application for solving various applied problems remains relevant. With the practical application of the algorithms, there are problems associated with end-to-end encryption, such as encrypting messages between the UAV and the ground workstation. In solving the tasks, it is necessary to use fast algorithms that can work effectively in the post-quantum period. Finding new solutions to protect information in the post-quantum period and improving existing algorithms by increasing their cryptographic stability is a task that is relevant today.

Algorithms that use transformations on algebraic lattices, the stability of which is based on solving NP-complexity problems, have become an alternative to classical algorithms in fields and rings.

NP-complexity problems include the following tasks: finding the shortest lattice vector (SVP - Shortest Vector Problem) or finding the (approximately) shortest independent vectors (SIVP – Shortest Independent Vectors Problem) [2]. The essence of these problems is to find in a given basis of the algebraic lattice of a nonzero vector that close to a certain normal.

The aim of this article is developing tools of increasing the stability of the algorithm on algebraic lattices, the NTRU algorithm exactly, without effect on its performance

2. Algebraic lattices and fast Fourier transform.

Algebraic lattices have become a convenient tool for cryptographic transformations in modern conditions. An algebraic lattice of dimension m means a set of all possible combinations of linearly independent vectors from a space of dimension n with integer coefficients. [3].

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: olha.petrenko@nure.ua (A. 1); alexwgs78@gmail.com (A. 2)
ORCID: orcid.org/0000-0002-7862-5399 (A. 1); orcid.org/0000-0001-9903-7388 (A. 2)

The basis of a lattice $b_1, b_{2,\dots,} b_n$ is a set of linearly independent vectors that generates the specified lattice. Coordinates of basis vectors are $b_i = \{x_{11}, x_{12}, \dots x_{1m}\}\ i = \overline{1, n}.$

The lattice can be associated with a matrix which rows are the coordinates of the basis vectors that form it. It is well known that any lattice can be defined by several bases and build a matrix of transition from one basis to another. This property allows to implement stable algorithms on algebraic lattices by constructing a basis that consisting of the shortest vectors. Using polynomials of degree n, it is possible to specify a basic vector of dimension n, the coordinates of which are equal to the coefficients of the polynomial. These properties allow to apply the fast Fourier transform to represent the basis vectors and build cryptographic transformations with their help. According to [4], the fast Fourier transform can be applied when developing an algorithm on algebraic lattices in a ring of a class of surpluses modulo some number q. In addition, the fast Fourier transform can be represented in matrix form, which allows in the field of surpluses modulo q to move from the values of the polynomial from the original roots from one to its coefficients according to formula 1.

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} = \\ = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & w_n & \cdots & w_n^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & w_n^{n-1} & \cdots & w_n^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}, \qquad (1)$$

where y_j is the value of the polynomial from the degrees of the original root of unity, w_n^i is the value of the original root of unity degree i, a_i are polynomial coefficients that determine the coordinates of the basis vectors.

For any prime number q in the field of surpluses modulo q there is a root g of degree $(q-1)$of unity, which satisfies the following formula:

$$q - 1 = m2^k, \qquad (2)$$

where g^m is the root of degree of unity. Formula 2 allows the application of fast Fourier transform algorithms for polynomials of degree . It can be shown that for any natural number k such a prime number q exists. This follows from Dirichlet's theorem on prime numbers [5]. To apply Dirichlet's theorem for cryptographic transformations on lattices, the number q and the degree of the polynomial on which the transformations are performed must correspond to the formula 2. Using the inverse Fourier transform, it is possible to determine the coordinates of the basis vectors with the formula:

$$a_j = \frac{1}{n} \sum_{j=0}^{n-1} y_j w_n^{-jk} \qquad (3)$$

where n is the number of basis vectors, k is the degree of the original element, ϖ is the value of the original root of unity, y_j is the value of the polynomial from the degrees of the original root of unity.

This mathematical apparatus allows with performing transformations on algebraic lattices to reduce the number of operations due to the properties of the original roots of unity, such as $w_n^0 = w_n^n = 1$. In addition, $w_n^j \cdot w_n^k = w_n^{j+k} = w_n^{(j+k) mod n}$. So, it is enough to use the condition $w_n^{n-1} = w_n^{-1}$ to find the inverse element then.

With the help of fast Fourier transform it is possible to solve a problem which consists in search from a numerical matrix of the big size of extraction of the small size block with the specified properties.

Under the block means the submatrix of the initial matrix. The idea of this algorithm, based on the fast Fourier transform, is to find some pattern $p_0, p_1, \dots \dots p_{m-1}$ in a range $t_0, t_1, \dots, t_{n-1}$, where p_i, t_j are some numbers. It is well known that the subrange enters from the i-th position, if $p_j = t_{i+j}, j = 0,1,2, \dots, m-1$. Entry of the subrange of the i-th position is equivalent to the fulfillment of the condition:

$$B_i = \sum_{j=0}^{m-1} \left(p_j - t_{i+j}\right)^2 = 0. \qquad (4)$$

Calculating the array B_i allows to determine all entries of subranges into the range. This property is used to construct one-sided functions with a trapdoors, which are used in cryptographic transformations on algebraic lattices [6].

The algorithm for calculating B_i according to [6] is to perform the following steps:

1. Polynomial calculations are performed $C(x) = T(x)P(x)$, where $T(x) = t_{n-1} x^{n-1} + \dots + t_1 x + t_0$, $P(x)$=$p_0 x^{m-1} + \dots + p_{m-1}$ the coefficient of the specified polynomial at x^{m-1+i} is equal to $c_{m-1+i} = p_0 t_i + p_1 t_{i+1} + \dots + p_{m-1} t_{m-1} = \sum_{j=0}^{m-1} p_j t_{j+i}$.
2. Calculations of $S = \sum_{j=0}^{m-1} p_j^2$ are performed and this addend is present in every B_i;
3. Calculations $H = \sum_{j=0}^{m-1} t_j^2$ are performed;

4. Calculations of the recurrent formula: $B_0 = S - 2c_{m-1} + H,$ $B_1 = S - 2c_m + \sum_{j=0}^{m-1} t_{j+1}^2 = B_0 - 2c_{m-1} - 2c_m - t_1^2 + t_m^2,$ $B_i = B_{i-1} + 2(c_{m-2+i} + c_{m-1+i}) - t_{i-1}^2 - t_{m-1+i}^2$ are performed.

This algorithm allows to determine vectors with certain properties, such as to find the shortest lattice vector.

3. NTRU algorithm

NTRU Encrypt algorithm [7] today is one of the most researched and widespread algorithms. The asymmetric cryptosystem which built on its basis is based on transformations on algebraic lattices. NTRU is a probabilistic stable system, i.e. a random element is used to encrypt messages. Under this condition, each message has a lot of ciphertext. The stability of the cryptosystem NTRU Encrypt [7] was determined experimentally and is based on the fact of the difficulty of finding the shortest vector of the algebraic lattice [2]. The advantage of this system is the fact that encryption and decryption of the message and key generation process is quick and easy for implementing. NTRU Algebraic Lattice Algorithm is an attractive algorithm for encrypting data in the communication channel between the UAV and the ground workstation. The advantage of the algorithm on the one hand is the ability to perform asymmetric encryption, and on the other to provide fast software implementation. The complexity of the algorithm can be reduced by applying a fast Fourier transform [4] from $O(n^2)$ to $O(nlogn)$. The NTRU Encrypt algorithm depends on parameters that are integers and can be represented in polynomial form. In order for the parameters not to contribute to the occurrence of random errors during decryption, it is necessary to include control bits in each message block.

The following parameters are used to build a mathematical model of the algorithm:

- N – the dimension of the ring of polynomials which used in encrypting messages;
- p – a natural number involved in encrypting and decrypting of the message;
- q – a natural number that participates in encrypting, decrypting of the message and determining the public key;
- k – the key security on which resistance to attacks depends;
- d_i (i=1,2) – distributions of polynomial coefficients used in the formation of the public and secret keys.

When generating keys, consider a ring of truncated polynomials $R = Z[x]/(x^N - 1)$. Each element of the ring can be represented in polynomial form $f = \sum_{s=0}^{N-1} f_s x^s$ or in vector form $(f_1, f_2, \ldots, f_{N-1})$. All coefficients of a polynomial are integers. To reduce the complexity of calculating the operation of multiplication of polynomials in a ring of truncated polynomials is possible by applying the operation of "convolution" according to the following rule: let it be necessary to multiply 2 polynomials $f = \sum_{s=0}^{N-1} f_s x^s$ and $g = \sum_{s=0}^{N-1} g_s x^s$ in a ring of truncated polynomials $R = Z[x]/(x^N - 1)$. The result of multiplication $h = f \otimes g$ is a polynomial of the form: $h = \sum_{s=0}^{N-1} h_s x^s$, which coefficients are calculated by the formula:

$$h_s = \sum_{i=0}^{s} f_i g_{s-i} + \sum_{i=s+1}^{N-1} f_i g_{N+s-i}.$$

This formula allows to reduce the computational complexity of multiplying polynomials in $R = Z[x]/(x^N - 1)$ due to the lack of a summation of $mod(x^N - 1)$ terms which degree are greater than *N*.

The parameters *p* and *q* do not have to be prime numbers, but they must satisfy the conditions: *НСД (p, q) = 1* and parameter *p* should be much smaller than *q*. Using the values of the parameters *p* and *q*, two polynomials f and g are randomly selected. A polynomial f belongs to a ring of truncated polynomials $R = Z[x]/(x^N - 1)$ with the distribution of coefficients with the parameter d_1. This means that the polynomial f contains d_1 coefficients equal to 1, d_1 -1 coefficients equal to -1 and all other coefficients equal to 0. This distribution of coefficients is due to the presence of an inverse polynomial to the polynomial f. A polynomial g belongs to a ring of truncated polynomials $R = Z[x]/(x^N - 1)$ with the distribution of coefficients with the parameter d_2. This means that the polynomial g contains d_2 coefficients equal to 1, d_2 -1 coefficients equal to -1 and all other coefficients equal to 0. Using polynomial f coefficients, polynomials $f_p \equiv f(mod\, p)$ and $f_q \equiv f(mod\, q)$ are constructed.

The obtained polynomials have inverse polynomials in the ring of truncated polynomials $R_p = Z_p[x]/(x^N - 1)$ and $R_q = Z_q[x]/(x^N - 1)$. As for polynomials obtained by reducing a polynomial modulo *p* and *q*, they do not have inverse polynomials in the ring of truncated polynomials $R_p = Z_p[x]/(x^N - 1)$ and $R_q = Z_q[x]/(x^N - 1)$.

The public key is calculated according to the rule: $h \equiv pf_q^{-1} \otimes g(mod\, q)$. It should be noted that the polynomial h and the numbers p and q are open parameters, and the polynomial f and f_q^{-1} are secret. To encrypt messages a polynomial r, that has a distribution of coefficients d_3 in the ring of truncated polynomials $R = Z[x]/(x^N - 1)$, and a public key h are randomly selected. This means that the polynomial h contains d_3 coefficients equal to 1, d_3 -1 coefficients equal to -1 and all other coefficients equal to 0.

The message m is encrypted as follows: $c \equiv r \otimes h + m(mod\, q)$.

The message is decrypted in two stages.

First, calculate the polynomial p with integer coefficients from the interval $\left(\frac{-q}{2}, \frac{q}{2}\right)$ by the formula: $a \equiv f \otimes c(mod\, q)$. Then calculate $f_q^{-1} \otimes a$.

The specified encryption algorithm has a disadvantage, which is associated with the appearance of parameters that contribute to errors. Therefore, it is necessary to include control bits for each message block. The cause of such errors is incorrect message centering. It is possible to get rid of it by calculating a polynomial $a \equiv f \otimes c(mod\, q)$ with integer coefficients in the interval $\left(\frac{-q}{2} + x, \frac{q}{2} + x\right)$ for a small value of negative or positive x. If this algorithm does not work, then the encryption procedure is repeatable.

From the decryption procedure, it can be concluded that the NTRU cryptosystem is probabilistic, so the plaintext is not always restored correctly from the encrypted text. The correct choice of polynomials *f*, *g*, *r* allows to reduce the probability of such an error to .

4. Means to increase the stability of the NTRU algorithm and its speed

Given the advantages and disadvantages of the NTRU Encrypt algorithm and the existing specific attacks [8-10],]it is possible to increase the stability of the algorithm by applying not uniform but normal distribution law when encrypting a message, namely when choosing polynomial r coefficients.

To determine the coefficients of the polynomial r, it is proposed to use a random number generator and the density of the normal distribution with predetermined mathematical expectations and standard deviation. The standard deviation in this algorithm is the value of safety level control and is a decisive factor. This is due to the fact that the stability of algorithms on algebraic lattices is based on the solution of the SPV problem (the problem of finding a short lattice vector) [11]. The specified value of the parameter should be chosen under the requirements of the stability of transformations, namely the standard deviation should be equal to the shortest vector of the algebraic lattice. As for the mathematical expectation, it can be zero. This point is due to the fact that for successful cryptanalysis it is necessary to find the lattice points within the probable radius $s\sqrt{N}$, where N is the degree of the polynomial, the modulus of which is transformed, s is the Euclidean norm of the shortest lattice vector. The higher the rate of the vector, the greater the freedom of action of the cryptanalyst to carry out attacks. In view of this, it is proposed to choose the standard deviation equal to the Euclidean norm of the shortest lattice vector. It is possible to obtain the shortest lattice vector among the basis vectors with using the algorithm proposed in the paper [8]. This algorithm allows to obtain a basis using the Gram-Schmidt orthogonalization process [12] with predetermined restrictions on the lengths of vectors.

Next, using the obtained value of the standard deviation and a mathematical expectation equal to zero a random sequence is formed according to the following algorithm:

1. a sequence (c_n) of random numbers is generated;
2. divide the field of real numbers into intervals according to the following condition: $I_1 = (-\infty, -3\sigma)$, $I_2 = (-3\sigma, 0)$ $I_3 = (0,3\sigma)$ $I_4 = (3\sigma, +\infty)$;
3. check in what interval the generated number got c_i. If $c_i \in I_1, c_i \in I_4$, then i - member of the sequence is equal to 0. If $c_i \in I_2$, Then i - member of the sequence is equal to -1. If $c_i \in I_3$, then i - member of the sequence is equal to 1. This sequence is the coefficient of the polynomial r, which is used for encryption.

The sequence proposed by this rule allows to increase the resistance of the algorithm on the algebraic lattices of NTRU Encrypt to the attack described in [12,13].

To find the shortest lattice vector, we use a one-way function with a trapdoor, which allows us to find the shortest lattice vector from an array based on the fast Fourier transform. Next, the

Euclidean norm of this vector is calculated, which allows to set the density function of the normal distribution and on the basis of the calculations to obtain a polynomial r .

It is possible to increase the speed of algorithms, as mentioned above, by applying a fast Fourier transform. $R = Z[x]/(x^N - 1)$.

According to formula 2 to determine the modulus q it is necessary to find such a simple value of q that corresponds to the condition $q - 1 = m \cdot 2^7$. It is proposed to apply to cryptographic transformations that provide a high level of stability the value of $q = 3 \cdot 2^7 + 1 = 769$. This parameter gives possibility to apply the fast Fourier transform algorithm for polynomials of degree N. In a accordance with Dirichlet's theorem on a prime number for a prime number 769 in the field of the class of surpluses there is a root g of degree 768 of unity. Then $\omega = g^3$ is a root g of degree of unity. This fact gives possibility to apply formula 3 and reduce the complexity of the calculation.

5. Conclusion

Based on the analysis of the NTRU Encrypt algorithm, the paper proposes the application of the normal distribution law to determine the coefficients of the polynomial by which encryption is performed. The application of its parameters, namely mathematical expectation and heart-square deviation, is determined and substantiated. The choice of the original root for the representation of the base vectors of the algebraic lattice using fast Fourier transform is substantiated. It allows to reduce the encryption complexity for a high level of stability of transformations based on the NTRU Encrypt algorithm.

6.References

[1] Gorbenko, Ju. I. Analiz shljahiv rozvitku kriptografiї pislja pojavi kvantovih komp'juteriv / Komp'juterni sistemi ta merezhi: Visnik nacional'nogo universitetu «L'vivs'ka politehnika» 806 (2014): 40–49.

[2] Subhash Khot. Hardness of approximating the Shortest Vector Problem in lattices.Journalof the AC M, 52(5) (2005) 789–808.

[3] J. M. Pollard, "The Fast Fourier Transform in a Finite Field," Mathematics of Computation, vol. 25, 1971, pp. 365–374.

[4] Ju. V. Linnik, A. O. Gel'fand. Jelementarnye metody v analiticheskoj teorii chisel. — Fizmatgiz, 1962.

[5] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In EUROCRYPT, 2012, pp. 700–718.

[6] Hoffstein J., Lieman D., Pipjer J., Silverman J. NTRU: A public key cryptosystem. Conference International Algorithmic Number Theory Symposium Springer, Berlin, Heidelberg, 1998, pp. 267-288.

[7] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lov ́asz. Factoring polynomials with rational coefficients. Math. Ann., 261(4), 1982, pp. 515–534.

[8] J. Hoffstein, J.H. Silverman, Protecting NTRU Against Chosen Ciphertext and Reaction Attacks, NTRU Technical Report #016, June 2000, www.ntru.com

[9] E. Jaulmes, A. Joux, A chosen-ciphertext attack against NTRU, in Proceedings of CRYPTO, Lecture Notes in Comp ter Science, Springer-Verlag, 2000.

[10]. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In STOC, 2009, pp. 333–342.

[11] Howgrave-Graha N., Silverman J., Whyte W. Meet-in-the-middle attack on an NTRU private key // NTRU Cryptosystems Technical Report #004. Version 2.

[12] Xuexin Zheng, An Wang, Wei Wei First-order collision attack on protected NTRU cryptosystem, Affiliations Microprocessors & Microsystems Volume 37, 2013, pp. 601–609.