საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 11, №2, 2017
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 2, 2017

Informatics

Analysis of Post-Quantum Cryptography Use in Practice

Avtandil Gagnidze*, Maksim Iavich*, Giorgi Iashvili*

* *Bank of Georgia University, Tbilisi, Georgia*

(Presented by Academy Member Archil Prangishvili)

ABSTRACT. Quantum computers are able to destroy most, if not absolutely all conventional cryptosystems that are widely used in practice, specifically, systems based on the problem of factoring integers (e.g., RSA). Some cryptosystems like RSA system with 4 000- bit keys are considered useful to protect classic computers from attacks, but probably absolutely useless against attacks on quantum computers. One of the alternatives are post-quantum systems, systems based on lattices. These systems are known for high security levels based on the worst-case hardness. They are based on the complexity of the problems grids, the main of which is the problem of the shortest vector (SVP). In fact, we consider the approximate option when we find a lattice vector, with the length of $\alpha(n)$ times more than the shortest nonzero vector. $\pm(n)$ is the approximation coefficient, n is the lattice size. The best known algorithm for grids problems is LLL algorithm. This algorithm needs polynomial time with approximation factor $2^{O(n)}$. In 1987, Schnorr extended LLL algorithm and improved this approximation ratio, but he increased the performance of the algorithm. Schnorr replaced core of LLL algorithm by blocks of larger size. We analyze the advantages and disadvantages of the lattice based crypto systems. We consider the attacks on these systems and propose defenses against these attacks. These defenses decrease the efficiency of the systems and make the systems inefficient. Cryptosystems based on NTRU allow to implement a directional encryption as well as the digital signature, so it is possible to build a public key infrastructure, which will be fully based on the NTRU cryptosystem. It makes this cryptosystem very important for practical use. So in the article we analyze whether NTRU can be implemented in practice. From our results we can conclude that crypto-system NTRU has such advantages as faster encryption and decryption of the messages, faster key generation and cryptographic resistance compared to RSA. The main advantage of this cryptographic system is resistance to quantum computer attacks. Thus, it can be argued that the crypto system NTRU is prospective. But it is also evident from these results that the key in NTRU system is bigger than in RSA that causes loss of efficiency. It should be also noted that the size of the signature in NTRU is not constant. It is also necessary to use concrete parameters for NTRU safety. It is also worth to note that even the right formed signature does not always pass the verification. In the article we also check the safety of NTRUsign without perturbation techniques before it has lost its efficiency in different threat models and show that the system is not secure in CPA model. So, we show that despite the fact that lattice-based cryptosystems for post-quantum period are proposed, the attacks on them are still fixed, and they are not effective enough. Thus, for the creation and implementation of safe and effective lattice-based post-quantum cryptosystems, it is necessary to conduct quite a big work.

Key words: attacks, security, cryptosystems, post-quantum, lattice, encryption

Quantum computers are able to destroy most, if not absolutely all conventional cryptosystems that are widely used in practice. Specifically, systems based on the problem of factoring integers (e.g., RSA). One of the alternatives are post-quantum systems, systems based on lattices. They are based on the complexity of the problems grids, the main of which is the problem of the shortest vector (SVP). The best known algorithm for grids problems is LLL algorithm[1]. This algorithm needs polynomial time with approximation factor $2^{O(n)}$. In 1987, Schnorr extended LLL algorithm and improved this approximation ratio, but he increased the time of performance of the algorithm[2]. Collision resistant hash functions based on lattices were proposed.

Hash Functions

Ajtai suggested the family of one-way functions [3] the security of which is based on the worst case of the SVP with the approximation ratio of n^c, where n is constant. Later Goldreich showed that these functions are resistant to the collision. To construct a family of hash functions the following integers are used as parameters: n, m, q and d. Selection of parameter *n* defines the safety of hash function. The key to a hash function specified by the matrix M is chosen uniformly from $Z_q^{n\times m}$. Hash function is $f_M : \{0, \ldots, d\text{-}1\}^m \to Z_q^n$. The function maps mlogd bits to nlogq bits for input compression, m> log q / log d. This hash function is very easy to implement, because we use only addition and multiplication modulo *q*, whose size is O (log n). However, it should be noted that the problem of effectiveness of these functions is that the size of their key grows quadratically in *n*, so that functions are ineffective. Due to the attacks on these functions by combinatorial method [4,5], for the security of 100-bit, you need to use a key of 500,000 bits size. To increase effectiveness, matrix M can be changed by block matrix, each block of which is circulant matrix: $M = [M^{(1)} | \ldots | M^{(m/n)}]$. Changing the structure of the matrix allows us to find the collision. When multiplying each block by constant vector v_i *1 = (v_i, . . . , v_i), the output of f_M function is also constant vector c * 1. Since *c* can take *q* different values, the collision can be found in polynomial time q or even in $O(\sqrt{q})$. This problem was solved by Peikert and Rosen and by Lyubashevsky and Micciancio, using ideal matrixes. To construct a family of hash functions as parameters are used integers: *n, m, q, d* and the vector $f \in Z_n$. As the key we take m/n number of vectors $a_1, \ldots, a_{m/n,}$ chosen uniformly from Z_q^n. Hashing takes place as follows: $f_M : \{0, \ldots, d\text{-}1\}^m \to Z_q^n$, where $f_M(y) = [F*a_1 | \ldots | F*a_{m/n}]y \bmod q$. As M is taken as a block matrix with structured blocks $M^{(i)} = F*a^{(i)}$. For security, based on the "worst case", vector f must satisfy the following conditions: 1. For two unit vectors u_1, u_2 vector $[F*u_1]\, u_2$ must have a small norm. 2. The polynomial $f(x) = x^n + f_n x^{n-1} + \cdots + f_1 \in Z[x]$ should be irreducible over integers. In [6] the values of f are proposed, satisfying the both conditions: $f = (1, \ldots, 1) \in Z_n$, where n + 1 is prime; f= (1, 0, . . . , 0) ∈ Zn, where n is power of two. The family of hash functions SWIFFT is an optimized version of the hash function described above, and is rather efficient due to the use of FFT in Z_q.

Public Key Encryption Schemes

The lattice based public key encryption schemes were proposed. Goldreich, Goldwasser, and Halevi offered cryptosystem: GGH, which is analogous of the cryptosystem McEliece, based on algebraic coding theory [7]. In 1999, Nguyen published an attack on the GGH, able to break the system for the matrix size up to 350. The attack is successful because of two vulnerabilities: The first one is that the error vectors are always very short compared to the lattice vectors. It makes easier to solve the closest vector problem, CVP. Second vulnerability is in the choice of the error vector. Nguyen offered several options for correcting the second vulnerability, but they all increase the first one. Because of this attack it is necessary to increase the size of the matrix, which makes the system inefficient. It should be also noted that this system is not semantically secure. In 1996 Hoffstein, Pipher and Silverman offered cryptosystem NTRU. NTRU is usually described as the ring polyno-

mials cryptosystem. Nevertheless, the relationship between the public and private keys determines the grid, which is called a lattice NTRU. The basis of this lattice can be obtained from the public key. In addition, the private key of cryptosystem corresponds to certain short-vectors in this lattice. Thus, the natural attack on this system is an attempt to solve the problem of the shortest vector in the lattice. However, it is not necessary to use the lattice during encryption and decryption. The private key is a short vector $(f, g) \in Z^{2n}$. Public Key - $h = p[R*f]^{-1}g \bmod q$, where p - is a small modulus, R is a cyclic rotation, transforming the vector $(x_1, x_2, \dots, x_n)^T$ в $(x_n, x_1, \dots, x_{n-1})^T$, p - is a big modulus. Encryption takes place in the following way: a message is encrypted as a vector $m \in \{1,0,-1\}^n$, for randomness vector $r \in \{1,0,-1\}^n$ is used, containing d_r records - 1, and all the rest - 0. d_r is the boundary of an integer for r. Cypher is calculated: $c = m + [R"h]r \bmod q$. To decrypt: $red = [R*f]c \pmod q$; all red coefficients should lie in the range: $[-q / 2; q / 2]$.

The message we calculate: $m = [R*f]_p^{-1} red \pmod p$. Coppersmith and Shamir carried out an attack on the private key of the system. The aim of the attack is to find the vectors f and g or vectors that are close to them, which can be used for cipher decryption. Vector (f, g) and its pairwise rotations are the vectors in NTRU Lattice. The Euclidean norm of this vector is $(2d_f - 1 + 2d_g)^{1/2}$. NTRU lattice volume is defined as $Det(L) = q^n$ and lattice dimension is 2n. It is expected that the shortest vector has a length approximately $\det(L)^{1/2n} = q^{1/2}$. Because $(2d_f - 1 + 2d_g)^{1/2} << q^{1/2}$, with a high probability vector (f, g) is the shortest vector of the lattice, so its pairwise rotations are also candidates for the shortest vector. These vectors can also be used to decrypt the cipher. Coppersmith and Shamir have shown that if the resultant vector is greater than (f, g) at some constant value, it is possible to combine several of these vectors and to decrypt the cipher. When using modern lattice reduction algorithms the approximation coefficient of the shortest vector problem is still exponential in n. Howgrave-Graham has shown that it is possible to improve the attack, if it is combined with combinatorial attack. To resist this attack, it is necessary to increase the parameters of the system. A public key of the system has the size of $n \log_2(q)$. Algorithm execution time depends on *n* and on the boundaries of integers. To increase the efficiency of the system as the private key we can take $f = u + pf_r$, where *u* is the first unit vector and records f_r are randomly selected from (1, 0, -1) depending on the d_f. In this way we increase efficiency as we get rid of the multiplication step.

NTRU cryptosystem is much more effective than the GGH and AD. AD cryptosystem was proposed by Ajtai-Dwork in 1997. This system is defined in the Euclidean setting of vector space, using the standard Euclidean norm. Later Nguyen and Stern carried out an attack on the private key of the system. Regev proposed cryptosystem LWE [8], this cryptosystem is the most effective system based on lattices. The private key of the system is matrix $S \in Zq^{nxl}$, chosen randomly. q, n and l are integers. The public key is $(A, P = AS+E) \in Z_q^{mxn} \times Z_q^{mxl}$, where $A \in Z_q^{mxn}$, chosen randomly. $E \in Z_q^{mxl}$, where data is selected according to the distribution Ψ_α, over Z_q, obtained by choosing a standard variable with a mean value 0 and with deviation $\pm q/(2A)^{1/2}$, approximating the result to the nearest integer and decreasing it modulo q. Encryption takes place as follows: given an element from the message space $e \in Z_t^l$ messages and the public key (A, P), vector $v \in \{-d, -d+1, \dots, d\}^m$ is selected randomly, d - is integer, and the cypher is issued: $(u = A^T v, c = P^T v + f(e)) \in Z_q^n \times Z_q^l$ is issued. Decryption takes place as follows: given cypher (u,c) $Z_q^n \times Z_q^l$ and private key: $S \in Zq^{nxl}$ and $f^{-1}(C - S^T u)$ is issued. The above given is implemented rather easily using only addition and multiplication modulo *q*. To optimize the execution time, it is possible to set *t* as the power of two and delay the operation modular reduction operations. This system has the following properties: Public key size: nl log q; Private key size: m(n+l) log q; Message size: l log t; Cypher size: (n+l) log q; Encryption blowup factor: (1+n/l)loq/logt; Operations needed for one bit encryption: O(m(1+n/l)); Operations needed for one bit decryption: O(n)

Digital Signature Schemes

Digital signature system based on lattices were also offered. Digital signature systems GGH and NTRUSign were offered [9]. The private key is the secret matrix S, whose columns form the basis of lattice L, the base consists of short, almost orthogonal vectors. The public key is an open matrix B, which forms a bad basis of the same matrix. Best of all is to use HNF (Hermite Normal Form) of matrix S. To encrypt the message we map it to the point $m \in R^n$, using the secret basis, then we approximate m to the nearby point $n \in L(S)$, using the secret basis. It takes place using Babai's round-off procedure. $n = S[S^{-1}m]$. To verify the signature and message pair (*m, n*) we must verify that $n \in L(B) = L(S)$, using the public key B, and that the distance from *n* to *m* is small. Gentry and Szydlo noticed that each signature leaks information about the secret key. In some years Nguyen and Regev showed that this leak leads to the attack on secret key. The main idea of the attack is that *m-n* difference is distributed uniformly. Therefore, considering a sufficient number of such pairs, we finally get to the algorithmic problem - so-called hidden parallelepiped problem. The solution of this problem leads to this attack. To protect against these attacks the most effective measures are the perturbation techniques. Hidden parallelepiped is replaced by more complex figures that helps to prevent the given attacks. These protection techniques slow down the generation of the signature, and increase the size of the private key. Gentry, Peikert and Vaikuntanathan identified a scheme called «preimage sampleable trapdoor functions» and showed how to construct it on the basis of the "worst case" lattice problems. This construction can be used as an option of GGH with the security proof. This scheme does not leak information about the secret base. This is achieved by replacing Babai's round-off procedure with Gaussian sampling procedure. System has quadratic complexity, as in the size of the key, also in the case of verification time. Lyubashevsky and Micciancio proposed a scheme of an electronic signature with security, based on the "worst case" lattice problems, the scheme is asymptotically efficient as in the case of the key size, also in the case of the verification time it has a linear complexity [10]. This system uses a new one-time signature system based on hashing. This type of schemes can be converted into full signature schemes using standard tree construction with only logarithmic loss of efficiency. One-time signature scheme is based on a hash function, collision resistant, based on ideal lattices. The hash function *h*, may be selected during key generation, or be a fixed parameter. The input data of function are vectors $v_1, \ldots v_{m/n} \in Zq^n$. The private key of the function is randomly chosen pair $x_1, \ldots x_{m/n} \in Zq^n$ и $v_1, \ldots v_{m/n} \in Zq^n$, selected in accordance with the relevant distribution, which generates short vectors with high probability. Public key is the image of these two given input values: $X = h(x_1, \ldots x_{m/n})$ и $V = h(v_1, \ldots v_{m/n})$. Messages are presented in the form of short vectors: $m \in Zq^n$. Signature is calculated as follows: $sig = (sig_1, \ldots x_{m/n}) = ([F*m]x_{1+}v_1, \ldots [F*m]x_{m/n+}v_{m/n}) \bmod q$. To verify the signature, it is checked whether sig is the sequence of short vectors which is hashed to $[F*m]X + V \bmod q$. Security of the scheme is based on the fact that even after the attacker sees the signature, private key value is hidden from him.

NTRU Use in Practice.

Cryptosystems based on NTRU allow to implement a directional encryption as well as the digital signature, so it is possible to build a public key infrastructure, which will be fully based on the NTRU cryptosystem. It makes this ctyptosystem very important for practical use.

From our results we can conclude that crypto-system NTRU has such advantages as faster encryption and decryption of the messages, faster key generation and cryptographic resistance compared to RSA. The main advantage of this cryptographic system is resistance to quantum computer attacks. Thus, it can be argued that the crypto system NTRU is perspective.

To check the possibility of NTRU use in practice, we compared it with RSA system which is widely used in practice. Table 1 provides a comparison of time needed for key generation in the cases of RSA and NTRU.

Table 1. Relation between key length and generation time

Cryptosystem	Key length	Generation time (ms)
RSA	512	360
	1024	1280
	2048	4195
NTRU	1169	4
	1841	7.5
	4024	17.5

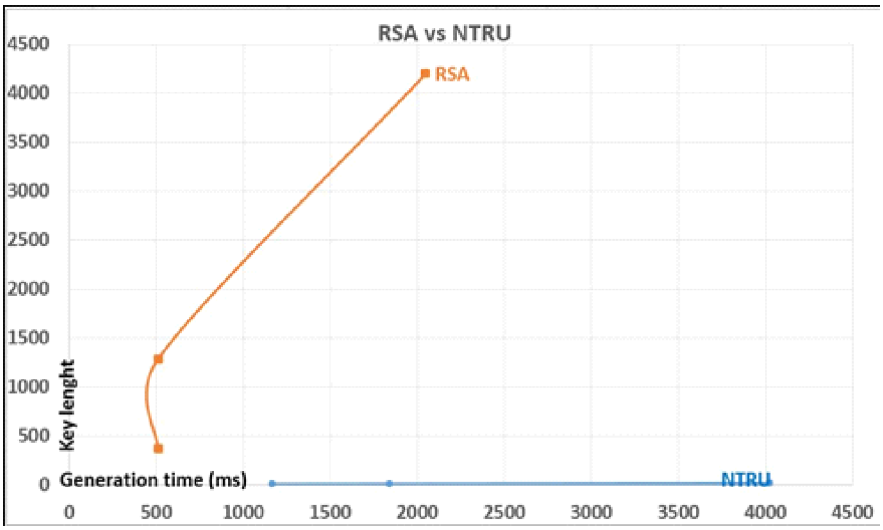

Fig. 1. Illustrates a comparison of time needed for key generation in the cases of RSA and NTRU. Dependence of key length of generation time

Table 2. Encryption and decryption time

Cryptosystem	Key length	Message encryption (block/s)	Message Decryption (block/s)
RSA	512	2440	120
	1024	930	20
	2048	310	3
NTRU	1169	5940	2820
	1841	3680	1620
	4024	1470	610

Table 2 provides a comparison of time needed for encryption and decryption of message block in RSA and NTRU cases.

Table 3 provides comparison of security in RSA and NTRU cases.

Table 4 provides comparison of efficiency between RSA and NTRU.

From our results we can conclude that crypto-system NTRU has such advantages as faster encryption and decryption of the messages, faster key generation and cryptographic resistance compared to RSA. The main advantage of this cryptographic system is resistance to quantum computer attacks. Thus, it can be argued that crypto system NTRU is perspective.

Table 3. Security of NTRU and RSA

Cryptosystem	Key length	Security (MIPS per year)
RSA	512	$4*10^5$
	1024	$3*10^{12}$
	2048	$3*10^{21}$
NTRU	1169	$2*10^6$
	1841	$4.6*10^{14}$
	4024	$3.4*10^{35}$

Table 4. Efficiency of RSA and NTRU

Cryptosystem	NTRU	RSA
KEY	L>l	l
ENC	l^2	l^2
DEC	L^2	L^3
MESSAGE	different	L

But it is also evident from these results that the key in NTRU system is bigger than in RSA that causes loss of efficiency. It should be also noted that the size of the signature in NTRU is not constant. It is also necessary to use concrete parameters for NTRU safety. It is also worth to note that even the right-formed signature does not always pass the verification.

Analysis of NTRUsign in Different Threat Models.

Let us analyze NTRUsign without perturbation techniques before it has lost its efficiency in different threat models.

In the treat model "ciphertext-only attack" (coa), attacker sees only the plain text and he cannot say anything about *m* and *n*, so the difference between *n* and *m* does not give him any information. So in this treat model the scheme is secure.

To get computational indistinguishability in the treat model "Known-plaintext attack" (KPA), we fix alg - algorithm, a – attacker and define a randomized experiment: 1. $a(1^n)$ outputs $m_0, m_1 \in \{0,1\}^*$ of equal length; 2. ans' $\leftarrow$ A(c); at *succeeds* if ans = ans', and experiment evaluates to 1 in this case. The scheme is secure if : $Pr[Exp_{a,alg}(n) = 1] \leq 1/2 + \varepsilon(n)$. In this case attacker signs two messages, and the oracle encrypts one of them, the experiment succeeds, if the attacker provides a correct guess with probability more than $1/2 + \varepsilon(n)$. $\varepsilon(n)$ is negligible, n is security parameter. In the treat model "Chosen-plaintext attack", CPA, the attacker can encrypt as many messages as he wants and only afterwards can apply the experiment. In this case according [11], 400 tries will be absolutely enough to break the system, so the system is not secure in CPA threat model.

Conclusion

As we can see, despite the fact that on the proposed lattice-based cryptosystems for post-quantum period the attacks are fixed and they are not effective. Thus, for the creation and implementation of safe and effective lattice-based post-quantum cryptosystems, it is necessary to conduct quite a big work.

Acknowledgement:

The work was conducted as a part of research Grant of "Shota Rustaveli National Science Foundation" [№ ys15_2.1.2_9].

ინფორმატიკა

პოსტ-კვანტური კრიპტოგრაფიის პრაქტიკაში გამოყენების ანალიზი

ა. გაგნიძე*, მ. იავიჩი*, გ. იაშვილი*

* *საქართველოს ბანკის უნივერსიტეტი, თბილისი, საქართველო*

(წარმოდგენილია აკადემიის წევრის ა. ფრანგიშვილის მიერ)

კვანტურ კომპიუტერებს აქვს შესაძლებლობა გაანადგუროს უმრავლესობა, თუ არა ყველა ტრადიციული კრიპტოსისტემა, რომლებიც ფართოდ გამოიყენება პრაქტიკაში. კონკრეტულად, სისტემები, რომლებიც ეფუძნება მთელი რიცხვების ფაქტორიზაციის ფუნქციას (მაგალითად RSA). ზოგი კრიპტოსისტემა როგორიც არის RSA ოთხიათას ბიტიანი გასაღებით ითვლება გამოსადეგად კლასიკური კომპიუტერების თავდასხმებისგან დასაცავად, მაგრამ შესაძლოა აბსოლუტურად უმოქმედო გახდეს კვანტური კომპიუტერების თავდასხმების შემთხვევაში. ერთ-ერთ ალტერნატივას პოსტ-კვანტური სისტემებისა წარმოადგენს მესრებზე დაფუძნებული სისტემები, რომლებიც ცნობილია უსაფრთხოების მაღალი დონით, და დაფუძნებულია უარეს შემთხვევებზე (worst-case hardness). სისტემები ეფუძნება მესრების პრობლემების სირთულეს, მათგან ძირითად პრობლემას კი უმოკლესი ვექტორის პრობლემა (SVP) წარმოადგენს. რეალურად, როდესაც მესრის ვექტორს ვპოულობთ, ჩვენ ვიზილავთ მიახლოებულ ვარიანტს, რისი სიგრძეც $\alpha(n)$-ჯერ უფრო მეტია ვიდრე უმოკლესი ნულოვანი ვექტორის სიგრძე. $\alpha(n)$ წარმოადგენს აპროქსიმაციის კოეფიციენტს, n კი, მესრის ზომაა. მესრების პრობლემების ყველაზე ცნობილი ალგორითმი გახლავთ LLLალგორითმი, რომელიც მიმდინარეობს პოლინომალურ დროში და მისი აპროქსიმაციის კოეფიციენტი გახლავთ $2^{O(n)}$. 1987 წელს შნორმა გააფართოვა LLL ალგორითმი, რის შედეგადაც გააუმჯობესა აპროქსიმაციის კოეფიციენტი, მაგრამ ამავდროულად ალგორითმის შესრულების დროც გაზარდა. შნორმა LLL ალგორითმის ბირთვი დიდი ზომის ბლოკებით ჩაანაცვლა. ჩვენ გავაანალიზეთ მესრებზე დაფუძნებული კრიპტოსისტემების სუსტი და ძლიერი მხარეები. ვიზილავთ თავდასხმებს ამ სისტემებზე, და ვთავაზობთ დაცვას წარმოდგენილ თავდასხმების წინააღმდეგ. ეს დაცვითი მექანიზმები ამცირებს სისტემების ეფექტურობას და ხდის უეფექტოს. NTRU-ზე დაფუძნებული კრიპტოსისტემები გვაძლევენ როგორც ელექტრონული ხელმოწერების რეალიზაციის, ასევე მიმართული შიფრირების საშუალებას. აქედან გამომდინარე, შესაძლებელი ხდება ღია გასაღების ინფრასტრუქტურის შექმნა, რომელიც მთლიანად იქნება დაფუძნებული NTRU კრიპტო-სისტემაზე, რაც ამ სისტემას ხდის ძალიან მნიშვნელოვანს პრაქტიკაში გამოყენებისთვის. წარმოდ-გენილ სტატიაში ჩვენ ვაანალიზებთ, შესაძლოა თუ არა NTRU-ს რეალიზაცია პრაქტიკაში. ჩვენი შედეგებიდან გამომდინარე დავასკვნით, რომ კრიპტოსისტემა NTRU-ს გააჩნია უპირატესობები შეტყობინების შიფრირებასა და გაშიფრვაში, გასაღების უფრო სწრაფი გენერირება და კრიპტო-გრაფიული მდგრადობა RSA-თან შედარებით. ძირითადი უპირატესობა სისტემისა არის მდგრადობა პოსტკვანტური კომპიუტერების შეტევების წინააღმდეგ. აქედან გამომდინარე ჩანს, რომ NTRU არის პერსპექტიული კრიპტოსისტემა. მაგრამ, ასევე ჩვენი შედეგებიდან გამომდინარე ჩანს, რომ გასაღები NTRU-სისტემაში არის უფრო დიდი ვიდრე RSA კრიპტოსისტემაში, რაც იწვევს ეფექტურობის დაკარგვას. აღსანიშნავია, რომ NTRU ხელმოწერის ზომა არ არის მუდმივი. აგრეთვე,

მნიშვნელოვანია კონკრეტული პარამეტრების გამოყენება NTRU სისტემის უსაფრთხოებისთვის. აღსანიშნავია ის ფაქტიც, რომ სწორად ფორმირებული ხელმოწერაც ყოველთვის ვერ გადის შემოწმებას. სტატიაში ჩვენ აგრეთვე ვამოწმებთ NTRUsign-ის უსაფრთხოებას „მღელვარების“ ტექნიკის გარეშე, მანამდე, სანამ იგი დაკარგავს ეფექტურობას სხვადასხვა threat მოდელში, და ვაჩვენებთ, რომ ზემოხსენებული სისტემა არ არის უსაფრთხო CPA მოდელის შემთხვევაში. მიუხედავად იმისა, რომ მესრებზე დაფუძნებული კრიპტოსისტემები არის შეთავაზებული პოსტ-კვანტური ეპოქისათვის, მათზე ფიქსირდება თავდასხმები, და ეს სისტემები არ არიან საკმარისად ეფექტურები. აქედან გამომდინარე, ეფექტურ და უსაფრთხო მესრებზე დაფუძნებული კრიპტოსისტემების შესაქმნელად საჭიროა ძალიან დიდი სამუშაოს ჩატარება.

REFERENCES

1. Lenstra A. K., Lenstra Jr., H.W. and Lovász L. (1982) Factoring polynomials with rational coefficients. *L Math. Ann*., **261**(4):515–534.
2. Schnorr C.P. (1987) A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, **53**(2-3):201–224.
3. Ajtai M. (2004) The LLL algorithm: survey and applications. *Complexity of computations and proofs*, **13**: 1–32. Napoli, Caserta.
4. Wagner D. (2002) Tweakable Block Ciphers. *Advances in Cryptology* (CRYPTO), **2442**: 288–303. Springer.
5. Blum A., Kalai A. and Wasserman H. (2003) Noise-Tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*, **50**(4):506–519.
6. Lyubashevsky V. and Micciancio D. (2006) Automata, languages and programming, In: 33rd International Colloquium.
7. Gagnidze A.G., Iavich M.P., Iashvili G.U. (2016) Post-Kvantovye kriptosistemy. *Modern scientific researches and innovations*, 5, URL (in Russian).
8. Regev O. (2006) Lattice-based cryptography. *Advances in cryptology* (CRYPTO), 131–141.
9. Hoffstein J., Graham N.A.H., Pipher J., Silverman J.H. and Whyte W. (2003) Digital signatures using the NTRU lattice. *Advances in Cryptology*, **2612:** 122–140. Springer-Verlag.
10. Lyubashevsky V. and Micciancio D. (2008) Asymptotically efficient lattice-based digital signatures. *In: Fifth Theory of Cryptography Conference* (TCC), **4948**, Springer.
11. Nguyen P.Q. & Regev O. J (2009) Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, **22:** 139–160.

Received December, 2017