RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 25 = 546 (2021): 181-193
DOI: https://doi.org/10.21857/yrvgqtexl9

CRYPTANALYSIS OF ITRU

Hayder R. Hashim, Alexandra Molnár and Szabolcs Tengely

Abstract. ITRU cryptosystem is a public key cryptosystem and one of the known variants of NTRU cryptosystem. Instead of working in a truncated polynomial ring, ITRU cryptosystem is based on the ring of integers. The authors claimed that ITRU has better features comparing to the classical NTRU, such as having a simple parameter selection algorithm, invertibility, and successful message decryption, and better security. In this paper, we present an attack technique against the ITRU cryptosystem, and it is mainly based on a simple frequency analysis on the letters of ciphertexts.

1. History of NTRU and its variants

1.1. *Introduction.*

The study of cryptography has been interested to cryptologists for long time because the necessity of transferring important information secretly, which established the existence of many types of cryptosystems. It is well-known that there are two types of cryptography, which are symmetric cryptography and asymmetric cryptography (or, public key cryptography). In the symmetric cryptosystem, the same key being used in the encryption and decryption procedures. However, in the asymmetric cryptosystem two different keys are used; the public key that should be announced to everyone and the corresponding private key has to be secret. In fact, many models of these cryptosystems have been established by several cryptologists. Indeed, symmetric key cryptography is by far more efficient; we only use public key cryptography to establish secret communication and the shared secret keys of symmetric encryption. The security of many public key cryptosystems such as Rivest, Shamir and Adelman (RSA) cryptosystem [37], McEliece cryptosystem [27], ElGamal cryptosystem [7], or elliptic curve cryptosystem (ECC) [23] is based on different intractable mathematical problems. In practice, all of these public key cryptosystems are far slower than symmetric cryptosystems such as

2020 *Mathematics Subject Classification.* 94B40, 94A60, 68P25.
Key words and phrases. NTRU, ITRU, public key cryptography, cryptanalysis.

Data Encryption Standard (DES) cryptosystem [33] or Advanced Encryption Standard (AES) cryptosystem [34] in terms of space and computational complexity and for this reason they are often simply used to solve the problem of sharing a secret key for use in a symmetric cryptosystem (for more details, see e.g. [15], [44] and the references given there). Therefore, the main target for cryptologists is the discovery of a fast public key cryptosystem based on different hard problems. Thus, in the following we introduce such public key cryptosystem and its variants.

1.2. *NTRU cryptosystem and its variants.*

In 1996, Hoffstein, Pipher and Silverman [16] proposed a class of fast public key cryptosystems called NTRU (N^{th} Degree Truncated Polynomial Ring) cryptosystem, which was published in 1998. This cryptosystem is considered as a lattice-based public key cryptosystem, and it is the first asymmetric cryptosystem based on the polynomial ring $\frac{\mathbb{Z}[X]}{(X^N-1)}$. Indeed, it has very good features comparing to other public key cryptosystems such as reasonably short, easily created keys, high speed, and low memory requirements. Its encryption and decryption procedures rely on a mixing system presented by polynomial algebra combined with a clustering principle based on elementary probability theory. From its lattice-based structure, the security of the NTRU cryptosystem is based on the hardness of solving the Closest Vector Problem (CVP), which is a computational problem on lattices closely related to Shortest Vector Problem (SVP) and considered to be NP hard (non-deterministic polynomial-time hardness) (for more details, see [29] and the references given there). In fact, the inventors [16] proved that the NTRU cryptosystem preforms much faster than other public key cryptosystems. For instance, the encryption and decryption procedure of a message block of length N takes $\mathcal{O}(N^2)$ operations using the NTRU cryptosystem and this is considerably faster than the $\mathcal{O}(N^3)$ operations required by RSA cryptosystem. Further, the key lengths of NTRU cryptosystem are $\mathcal{O}(N)$, which is very good comparing to the $\mathcal{O}(N^2)$ key lengths required by other fast public key cryptosystems presented in [14] and [27]. Furthermore, preliminary experimental results by Shen, Du, and Chen [41] showed that the speed of the NTRU cryptosystem is much faster than that of the RSA cryptosystem in which the key generation is more than 200 times faster, the encryption is almost 3 times faster, and the decryption is about 30 times faster. These results show the applicable possibility of NTRU cryptosystem in mobile Java systems.

For further enhancement of the security of the NTRU cryptosystem, researchers have been proposing several variants of NTRU cryptosystem. Starting with a generalization of NTRU cryptosystem proposed by Banks and Shparlinski [1] with non-invertible polynomials on the same ring as NTRU. The

main advantage of this variant is that it is more secure against some of the known attacks on the original NTRU cryptosystem such as lattice attack. On the other hand, it is less efficient than NTRU since the lengths of its public key and the ciphertext are twice the ones in the classical NTRU cryptosystem. Another analogue of NTRU cryptosystem was introduced by Gaborit, Ohler, and Solé [10] called CTRU cryptosystem in which the ring $\mathbb{Z}$ in NTRU cryptosystem is replaced by the ring of polynomials $\mathbb{F}_2[T]$. A new variant of the NTRU cryptosystem was presented by Coglianese and Goi [5] called MaTRU cryptosystem. However, it operates under the same general principles as the NTRU cryptosystem, it works in a different ring with a different linear transformation in the encryption and decryption procedures. As a result, MaTRU cryptosystem is more efficient and has a better security level comparing to NTRU cryptosystem. Kouzmenko [24] used Gaussian integers instead of the ring $\mathbb{Z}$ in NTRU cryptosystem to propose a generalization of NTRU cryptosystem. However, it is not as efficient as NTRU, this scheme is slightly more secure against lattice attack than NTRU cryptosystem. By replacing the ring $\mathbb{Z}$ in NTRU cryptosystem by the Eisenstein integers $\mathbb{Z}[\zeta_3]$, Nevins, KarimianPour, and Miri [31] proposed another variant, which we they called it by ETRU cryptosystem, which presents a more difficult lattice problem for lattice attacks, for the same level of decryption failure security. Malekian, Zakerolhosseini, and Mashatan [26] presented a new variant called QTRU cryptosystem based on using the ring of quaternions instead of the ring $\mathbb{Z}$ in NTRU cryptosystem. They showed that the structure of QTRU cryptosystem gives more resistant to some lattice-based attacks comparing to the classical NTRU cryptosystem. Other variants have been introduced by many authors such ILTRU cryptosystem, which is a modification of ETRU cryptosystem, introduced by Karbasi and Atani [21]. The security of this cryptosystem is based on the worst case hardness of the approximate both SVP and CVP in ideal lattices. Last but not least, we mention one of the known variants of NTRU cryptosystem called ITRU cryptosystem, which was presented in 2017 by Gaithuru, Salleh, and Mohamad [11]. Instead of working in a truncated polynomial ring, ITRU cryptosystem is based on the ring of integers. The authors claimed that ITRU has better features comparing to the classical NTRU such as having a simple parameter selection algorithm, invertibility, and successful message decryption. Indeed, the classical NTRU cryptosystem has a probability of decryption failure of 2^{-145}. Moreover, they claimed that the ITRU has a better security than NTRU, since its security is based on the integer factorization problem. Other variants of NTRU cryptosystem can be found, e.g. in [4], [22], [32], [35], [42], [46]. However, the inventors of NTRU cryptosystem ensured that it is extremely unlikely to several potential attacks against the scheme to succeed (particularly, the standard lattice-based attack) since the secret key was surrounded by a "cloud" of exponentially many unrelated lattice vectors. Many attacks have been preformed against

the NTRU and its variants, and in the following we mention some of these attacks (mainly attacks against NTRU) .

1.3. *Attacks.*

In 2001, Coppersmith and Shamir [6] showed that the security of NTRU cryptosystem is not necessarily based on the difficulty of reducing the NTRU lattice since the lattice reduction can be one of the practical attacks against NTRU cryptosystem. In fact, they presented a lattice-based attack, which can either find the original secret key k or an alternative key k' which can be used instead of k to obtain the plaintexts by decrypting the corresponding ciphertexts with only slightly higher computational complexity. After that, many types of lattice-based attacks on the NTRU cryptosystem and its variants have been occurred. It is important to mention that all of these attacks have focused primarily on the "secret key recovery" problem. For instance, Gentry [12] proposed lattice-based attacks that are especially effective when N, in the polynomial ring that used in the classical NTRU cryptosystem, is composite. He used low-dimensional lattices to find a folded version of the private key, where this key has d coefficients where d dividing N. This folded private key is used to recover a folding of the plaintext, or it helps to recover the original private key. However, a chosen ciphertext attack is another type of attacks, which was already used in [13] or [19] against other public key cryptosystems. Here, the attacker constructs invalid cipher messages. By knowing the plaintexts corresponding to his messages, she can get some information about the private key or even recover it. Such an attack was used against the NTRU cryptosystem by Jaulmes and Joux [18]. Similar attack to the later one was proposed by Meskanen and Renvalla [28]. Another attack on NTRU cryptosystem hardware implementations, that employ scan based Design-for-Test (DFT) techniques, was proposed by Kamal and Youssef [20], and they called it a scan-based side channel attack. This attack determines the scan chain structure of the polynomial multiplication circuits used in the decryption algorithm which allows the cryptanalyst to efficiently retrieve the secret key. In case of CTRU cryptosystem, Kouzmenko [24] showed that CTRU was completely vulnerable to a simple attack. More attack techniques against NTRU cryptosystem and its variants can be found, i.e. [17], [25], [30], [36], [38] and the references given there.

In fact, most of the attacks against the NTRU cryptosystem especially the ones mentioned above focus primarily on the "secret key recovery" problem. Therefore, in this paper we present an attack technique to break the ITRU cryptosystem proposed in [11]. Indeed, the construction of ITRU (see Section 2) shows that ITRU is a substitution cipher. Therefore, we use one of the best effective attacks against substitution ciphers presented by the frequency analysis technique. This attack is mainly based on a simple frequency analysis

on the letters of ciphertexts using a function implemented in SageMath [43] as `frequency_distribution()`. As a result, this techniques will recover the corresponding plaintexts immediately with no need of having the private keys.

2. The ITRU Cryptosystem

As mentioned earlier, instead of working in a truncated polynomial ring ITRU cryptosystem is based on the ring of integers. The parameters and the main steps of ITRU cryptosystem are as follows.

- ☐ The value of p is suggested to be 1000.
- ☐ Random integers f, g and r are chosen such that f is invertible modulo p.
- ☐ A prime q is fixed satisfying $q > p \cdot r \cdot g + f \cdot m$, where m is the representation of the message in decimal form. The suggested conversion is based on $ASCII$ conversion tables, that is the one with $a \to 97$.
- ☐ One computes $F_p \equiv f^{-1} \pmod{p}$ and $F_q \equiv f^{-1} \pmod{q}$. These computations can be done by using the extended Euclidean algorithm.
- ☐ The public key is consisted of h and q such that

$$h \equiv p \cdot F_q \cdot g \pmod{q}. \tag{2.1}$$

- ☐ The encryption procedure is similar to the one applied in NTRU cryptosystem [16], one generated a random integer r and computes

$$e \equiv r \cdot h + m \pmod{q}. \tag{2.2}$$

- ☐ To get the plaintext from the ciphertext, one determines

$$a \equiv f \cdot e \pmod{q}. \tag{2.3}$$

- ☐ Recovering the message is done by computing

$$F_p \cdot a \pmod{p}. \tag{2.4}$$

In order to show this later recovery leads to the original plaintext at the end, one can show that as follows. Combining equation (2.3) with (2.2) and (2.1), with use of the fact that $f \cdot F_q \equiv 1 \pmod{q}$ we obtain that

$$a \equiv f \cdot e \equiv f \cdot (r \cdot h + m) \equiv f \cdot (r \cdot p \cdot F_q \cdot g + m) \equiv r \cdot p \cdot g + f \cdot m \pmod{q}. \tag{2.5}$$

It remains to compute $F_p \cdot a \pmod{p}$ by substituting (2.5) in (2.4) and using the fact that $f \cdot F_p \equiv 1 \pmod{p}$. We obtain that

$$F_p \cdot a \equiv F_p \cdot (r \cdot p \cdot g + f \cdot m) \equiv F_p \cdot f \cdot m \equiv m \pmod{p}.$$

We also emphasize that the only reason that we can switch from mod q to mod p is because of the hypothesis in the third step above (i.e. $q > p \cdot r \cdot g + f \cdot m$), which ensures that the integer value of that string is less than q and so when we do mod q we have selected the correct coset.

3. ITRU Cryptosystem Implementation

We note that to fix q one needs a bound for the largest possible value of the representation, so here if one only uses the letters from 'A' to 'Z' and 'a' to 'z', then the maximum is 122. In the following SageMath implementation we will use 255, however one can use a greater upper bound for the representations. In fact, we preform our implementation on the arbitrary message: Cryptanalysis.

ITRU Implementation Input

```
s ='Cryptanalysis'
pretty_ print('The message is:', s)
r = 8
p = 1000
F = Set([k for k in range(2, 1000) if gcd(k, 1000) == 1])
f = F. random_element()
S =Set([2..1000])
g = S. random_element()
m =[ord(k) for k in s]
 pretty_print(' The ASCII code of the message :', m)
 q =next_prime(p * r * g + 255 * f)
 F_p = (1/f)%p
 Fq = (1/f)%q
 h = (p * Fq * g)%q
 pretty_print(' Large modulus :', q)
 pretty_print(' Public key :', h)
 pretty_print(' Private key pair :', (f, Fp))
 e = [((r * h) + m[i])%q for i in [0..len(m) − 1]]
 pretty_print(' The encrypted message :', e)
 a = [(f * e[i])%q for i in [0..len(e) − 1]]
 pretty_print(html(r'$f\cdot e \pmod{q}$ is: $%s$'%latex(a)))
 C = [(F_p * a[l])%p for l in [0..len(a) − 1]]
pretty_print(html(r'$F_p \cdot a \pmod {q}$ is: $%s$'% latex(C)))
 D =[chr(k) for k in C]
 pretty_print(' The original message: ','.join(D))
```

Output

The message is: Cryptanalysis
The ASCII code of the message: [67, 114, 121, 112, 116, 97, 110, 97, 108, 121, 115, 105, 115]
Large modulus: 6186617
Public key: 180058
Private key pair: (73, 137)
The encrypted message: [1440531, 1440578, 1440585, 1440576, 1440580, 1440561, 1440574, 1440561, 1440572, 1440585, 1440579, 1440569, 1440579]
$f \cdot e \pmod{q}$ is: [6172891, 6176322, 6176833, 6176176, 6176468, 6175081, 6176030, 6175081, 6175884, 6176833, 6176395, 6175665, 6176395]
$F_p \cdot a \pmod{p}$ is: [67, 114, 121, 112, 116, 97, 110, 97, 108, 121, 115, 105, 115]
The original message: Cryptanalysis

4. ITRU Plaintext Recovery

By using the frequency analysis technique, we can recover the corresponding plaintexts of any ciphertext encrypted using ITRU with no need of recovering the private keys. This technique mainly focuses on studying of the frequency of letters or groups of letters and counting their appearance in a ciphertext. More precisely, the frequency analysis is based on the fact that, in any given piece of text, certain letters and combinations of letters occur with varying frequencies. For example, in any typical text in English language, letters E, T, A and O are the most common, while letters Z, Q and X are not as frequently used. For more details about the frequency of letters in English, see e.g. Table 1 in [2]. In this section, we therefore present an attack technique against the ITRU cryptosystem, it is mainly based on a simple frequency analysis preformed with SageMath Software. As a result, this technique will recover the corresponding plaintexts immediately with no need of having the private keys. Indeed, the attack is via eavesdropping on some encrypted messages. If the message is too short, then the attack fails. Moreover, according to the index of coincidence introduced by Friedman [8] the language of the plaintext can be identified (e.g. in case of English it is about 0.0686). Therefore, once we identify the language correctly, then the frequency analysis works very well in practice. However, it is assumed that most samples of text written in English would have a similar distribution of letters only if the text is long enough, one may ask the following question: what is the minimum length of a ciphertext for which this attack operates efficiently? A brief answer to this question is presented in the following remark. Indeed, it is interpreted formally with more details in ([45, pp. 110-119]) and ([3, pp. 283-285]).

REMARK 4.1. Given a ciphertext C in a symmetric key cryptosystem (particularly, a substitution cipher), it seems reasonable to suppose that the longer that C is, the fewer the number of intelligible plaintext messages M there are corresponding to C. Shannon [39], [40] showed that there exists a critical length U called the unicity point such that if the length of ciphertext C is longer than this length then there is likely to be just one corresponding plaintext M. In fact, Shannon showed that U can be calculated as roughly the point where the message entropy plus the key entropy is less than or equal to the cipher text entropy. More precisely, the unicity point is calculated as the following:

$$U = \frac{H(K)}{\log|\Gamma| - H(\Gamma)} = \frac{\log|K|}{\log|\Gamma| - H(\Gamma)}, \tag{4.1}$$

where $H(K) = \log|K|$ represents the entropy of the key-space such that $|K|$ forms the number of permutations of the letters in the key K (it is usually assumed that all the keys are equally likely to be chosen), $H(\Gamma)$ denotes the the entropy per symbol of the language Γ being used, and $|\Gamma|$ is the number of the letters in the language Γ.

Since we are interested in substitution ciphers over the English alphabet, let us here calculate the unicity point. Since the English language contains 26 letters, then there are 26! possible keys, i.e. $|K| = 26!$. Taking $\log|\Gamma| = \log(26) = 4.7$ and the entropy of English to be 2 bits per letter (which is probably a little high), i.e. $H(\Gamma) = 2$. From (4.1) we get that

$$U = \frac{\log(26!)}{4.7 - 2} = \frac{88.4}{2.7} \approx 32.$$

This means if the ciphertext C has length of 32 letters or more we expect there to be just one meaningful plaintext M. This is fairly good agreement with the empirical observation of Shannon [40], who claimed that the unicity point can be shown experimentally to lie between 20 and 30. In the same ballpark, Friedman [9] claimed that 'practically every example of 25 or more characters representing monoalphabetic encipherment of a "sensible" message in English can be readily solved'.

However, this attack technique can be applied on any encrypted message using the ITRU cryptosystem, let us preform this technique on the following paragraph from the article describing ITRU cryptosystem [11] (without spaces):

′ThegoalofthisstudyistopresentavariantofNTRUwhichisbased ontheringofintegersasopposedtousingthepolynomialringwith integercoefficients.WeshowthatNTRUbasedontheringofintegers (ITRU),hasasimpleparameterselectionalgorithm,invertibility andsuccessfulmessagedecryption.Wedescribeaparameter selectionalgorithmandalsoprovideanimplementationofITRU usinganexample.ITRUisshowntohavesuccessfulmessage decryption,whichprovidesmoreassuranceofsecurityin comparisontoNTRU.′

If this paragraph is encrypted with the large modulus $q = 1104427$ and the public key $h = 37619$, then the ciphertext starts as

$$301036, 301056, 301053, 301055, 301063, 301049, 301060, 301063, 301054, ...$$

In fact, there are 32 different numbers appearing in the ciphertext these are between 300992 and 301073. A simple frequency analysis with the function `frequency_distribution()` provides the following data:

$$\begin{aligned}[&(301056, 0.0380313199105145), (301057, 0.0850111856823266),\\ &(301060, 0.0313199105145414), (301061, 0.0290827740492170),\\ &(301062, 0.0648769574944072), (301063, 0.0738255033557047),\\ &(301064, 0.0313199105145414), (301066, 0.0536912751677852),\\ &(301067, 0.0850111856823266), (301068, 0.0693512304250559),\\ &(301069, 0.0201342281879195), (301070, 0.0111856823266219),\\ &(301071, 0.0111856823266219), (301072, 0.00223713646532438),\\ &(301073, 0.0134228187919463), (300992, 0.00223713646532438),\\ &(300993, 0.00223713646532438), (300996, 0.00671140939597315),\\ &(300998, 0.00894854586129754), (301025, 0.00671140939597315),\\ &(301030, 0.00671140939597315), (301034, 0.0134228187919463),\\ &(301036, 0.0156599552572707), (301037, 0.0134228187919463),\\ &(301039, 0.00447427293064877), (301049, 0.0693512304250559),\\ &(301050, 0.00894854586129754), (301051, 0.0357941834451902),\\ &(301052, 0.0246085011185682), (301053, 0.109619686800895),\\ &(301054, 0.0223713646532438), (301055, 0.0290827740492170)]\end{aligned}$$

We see that the number 301053 appears the most in the ciphertext. Therefore, 301053 represents either $′e′$,$′a′$ or $′t′$. If it is $′e′$, then we apply the

formula

$$c_i - 300952,$$

where c_i represents the ciphertext blocks in the ASCII character code for all i. Thus, we get a sequence of numbers starting with

$$84, 104, 101, 103, 111, 97, 108, 111, 102, ...$$

Finally, if we consider it as a sequence of ASCII codes and determine the corresponding plaintext, then we get the encoded message.

5. Can ITRU be fixed?

Our main aim of this paper is in fact to show that the ITRU cryptosystem is only a substitution cipher in which the authors proposed to encode each letter individually using the same key. As consequence, this cipher can be attacked easily using a simple frequency analysis technique as described earlier. Nevertheless, we could propose some corrections that make ITRU secure against such attacks. First, we can either use a different r for each letter of the ciphertext, or we encode the message not as a sequence of integers but as one absolutely huge integer. Moreover, in practice we use PKC to encode a bit string that will be used in a subsequent symmetric cipher, like AES, so we could assume that m is the number corresponding to this bit string (so a number of size 2^N where e.g. $N = 128$).

Acknowledgements.

The authors would like to express their sincere gratitude to the referee for the careful reading of the manuscript and many useful comments which improve the quality of the paper. The research was supported in part by the NKFIH grants 115479, 128088 and 130909 and by the project EFOP-3.6.1-16-2016-00022, co-financed by the European Union and the European Social Fund.(Sz.T.). The work of H. R. Hashim was supported by the Stipendium Hungaricum Scholarship.

References

[1] W. D. Banks and I. E. Shparlinski, *A variant of NTRU with non-invertible polynomials,* in: Progress in Cryptology – INDOCRYPT 2002, Lecture Notes in Comput. Sci. **2551**, Springer, Berlin, pp. 62–70.

[2] H. Beker and F. Piper, Cipher systems: The protection of communications, A New Electronics Communications International Book, Northwood Books, London, 1982.

[3] A. A. Bruen and M. A. Forcinito, Cryptography, information theory, and error-correction. A handbook for the 21st century, John Wiley & Sons, Hoboken, 2005.

[4] M. G. Camara, De. Sow and Dj. Sow, *DTRU1: First generalization of NTRU using dual integers,* International Journal of Algebra **12 (7)** (2018), 257–271.

[5] M. Coglianese and B. M. Goi, *MaTRU: A new NTRU-based cryptosystem,* in: Progress in Cryptology – INDOCRYPT 2005, Lecture Notes in Comput. Sci. **3797**, Springer, Berlin, 2005. pp. 232–243.

[6] D. Coppersmith and A. Shamir, *Lattice attacks on NTRU*, in: Advances in Cryptology — EUROCRYPT '97, Lecture Notes in Comput. Sci. **1233**, Springer, Berlin, 1997, pp. 52–61.
[7] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms,* IEEE Trans. Inform. Theory **31 (4)** (1985), 469–472.
[8] W. F. Friedman, The index of coincidence and its applications in cryptography, Department of Ciphers. Publ 22. Riverbank Laboratories, Geneva, Illinois, 1922.
[9] W. F. Friedman, *Codes And Ciphers (CRYPTOLOGY),* Encyclopaedia Britannica, 1961, pp. 1–8.
[10] P. Gaborit, J. Ohler and P. Solé, *CTRU, a polynomial analogue of NTRU,* INRIA, 2002.
[11] J. N. Gaithuru, M. Salleh and I. Mohamad, *ITRU: NTRU-based cryptosystem using ring of integers,* International Journal of Innovative Computing **7 (1)** (2017), 33–38.
[12] C. Gentry, *Key recovery and message attacks on NTRU-composite,* in: Advances in Cryptology – EUROCRYPT 2001, Lecture Notes in Comput. Sci. **2045**, Springer, Berlin, 2001, pp. 182–194.
[13] H. Gilbert, D. Gupta, A. Odlyzko and J. J. Quisquater, *Attacks on Shamir's 'RSA for paranoids',* Inf. Process. Lett. **68 (4)** (1998), 197–199.
[14] O. Goldreich, S. Goldwasser and S. Halevi, *Public-key cryptosystems from lattice reduction problems,* in: Advances in Cryptology – CRYPTO '97, Lecture Notes in Comput. Sci. **1294**, Springer, Berlin, 1997, pp. 112–131.
[15] S. Gurpreet and K. Supriya, *A study of encryption algorithms (RSA, DES, 3DES and AES) for information security,* International Journal of Computer Applications **67 (19)** (2013), 33–38.
[16] J. Hoffstein, J. Pipher and J. H. Silverman, *NTRU: A ring-based public key cryptosystem,* in: Algorithmic number theory, ANTS-III, Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, 1998, pp. 267–288.
[17] N. Howgrave-Graham, *A hybrid lattice-reduction and meet-in-the-middle attack against NTRU,* in: Advances in Cryptology – CRYPTO 2007, Lecture Notes in Comput. Sci. **4622**, Springer, Berlin, 2007, pp. 150–169.
[18] É. Jaulmes and A. Joux, *A Chosen-Ciphertext Attack against NTRU,* in: Advances in Cryptology — CRYPTO 2000, Lecture Notes in Comput. Sci. **1880**, Springer, Berlin, 2000, pp. 20–35.
[19] M. Joye and J. J. Quisquater, *On the importance of securing your bins: The garbage-man-in-the-middle attack,* in: Proceedings of the 4th ACM conference on Computer and communications security, 1997, pp. 135–141.
[20] A. A. Kamal and A. M. Youssef, *A scan-based side channel attack on the NTRUEncrypt cryptosystem,* in: 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp. 402–409.
[21] A. H. Karbasi and R. E. Atani, *ILTRU: An NTRU-like public key cryptosystem over ideal lattices,* IACR Cryptology ePrint Archive, 2015.
[22] A. H. Karbasi, R. E. Atani and S. E. Atani, *PairTRU: Pairwise non-commutative extension of the NTRU public key cryptosystem,* International Journal of Computer Applications **7 (1)** (2018), 11–19.
[23] N. Koblitz, *Elliptic curve cryptosystems,* Math. Comp. **48** (1987), 203–209.
[24] R. Kouzmenko, Generalizations of the NTRU cryptosystem, Diploma Project, École Polytechnique Fédérale de Lausanne (2005–2006).
[25] Z. Liu, Y. Pan and Z. Zhang, *Cryptanalysis of an NTRU-based proxy encryption scheme from ASIACCS'15,* in: Post-quantum cryptography, Lecture Notes in Comput. Sci. **11505** (2019), pp. 153–166.

[26] E. Malekian, A. Zakerolhosseini and A. Mashatan, *QTRU: Quaternionic version of the NTRU public-key cryptosystems,* ISeCure **3 (1)** (2011), 28–42.
[27] R. J. McEliece, *A public-key cryptosystem based on algebraic coding theory,* Deep Space Network Progress Report **44** (1978), 114–116.
[28] T. Meskanen and A. Renvall, *A wrap error attack against NTRUEncrypt,* Discrete Appl. Math. **154** (2006), 382–391.
[29] D. Micciancio, *Closest Vector Problem,* in: H.C.A. van Tilborg (ed.), Encyclopedia of Cryptography and Security, Springer, New York, 2005, pp. 79–80.
[30] P. Mol and M. Yung, *Recovering NTRU secret key from inversion oracles,* in: Public key cryptography – PKC 2008, Lecture Notes in Comput. Sci. **4939**, Springer, Berlin, 2008, pp. 18–36.
[31] M. Nevins, C. KarimianPour and A. Miri, *NTRU over rings beyond $\mathbb{Z}$,* Des. Codes Cryptogr. **56** (2010), 65–78.
[32] D. Nuñez, I. Agudo and J. Lopez, *NTRUReEncrypt: An efficient proxy re-encryption scheme based on NTRU,* in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Association for Computing Machinery, 2015, pp. 179–189.
[33] National Bureau of Standards, *Data Encryption Standard*, FIPS Publication 46, U.S. Department of Commerce, 1977.
[34] National Institute of Standards and Technology, *Advanced Encryption Standard,* FIPS Publication 197, U.S. Department of Commerce, 2001.
[35] Y. Pan and Y. Deng, *A general NTRU-like framework for constructing lattice-based public-key cryptosystems,* in: Information Security Applications, Lecture Notes in Comput. Sci. **7115**, Springer, Berlin, 2012, pp. 109–120.
[36] J. Proos, *Imperfect decryption and an attack on the NTRU encryption scheme,* IACR Eprint archive, 2003.
[37] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems,* Comm. ACM **21 (2)** (1978), 120–126.
[38] T. E. Seidel, D. Socek and M. Sramka, *Parallel symmetric attack on NTRU using non-deterministic lattice reduction,* Des. Codes Cryptogr. **32**(2004), 369–379.
[39] C. E. Shannon, *A mathematical theory of communication,* Bell System Tech. J. **27** (1948), 623–656.
[40] C. E. Shannon, *Communication theory of secrecy systems,* Bell System Tech. J. **28** (1949), 656–715.
[41] X. Shen, Z. Du and R. Chen, *Research on NTRU algorithm for mobile Java security,* in: 2009 International Conference on Scalable Computing and Communications; Eighth International Conference on Embedded Computing, 2009, pp. 366–369.
[42] S. Singh and S. Padhye, *Generalisations of NTRU cryptosystem,* Security Comm. Network **9** (2016), 6315–6334.
[43] W. A. Stein and others, *Sage Mathematics Software (Version 9.0),* The Sage Development Team, 2020, `http://www.sagemath.org`.
[44] J. Talbot and D. Welsh, Complexity and cryptography, Cambridge University Press, Cambridge, 2006.
[45] D. Welsh, Codes and cryptography, Clarendon Press, Oxford University Press, New York, 1988.
[46] H. Yassein and N. Al-Saidi, *BITRU: Binary version of the NTRU public key cryptosystem via binary algebra,* International Journal of Advanced Computer Science and Applications **7 (11)** (2016), 1–6.

Kriptoanaliza ITRU kriptosustava

Hayder R. Hashim, Alexandra Molnár i Szabolcs Tengely

Sažetak. Kriptosustav ITRU je kriptosustav s javnim ključem i jedna od poznatih inačica kriptosustava NTRU. Umjesto na prstenu krnjih polinoma, ITRU kriptosistem zasnovan je na prstenu cijelih brojeva. Njegovi autori su tvrdili da ITRU ima bolje značajke u odnosu na klasični NTRU, poput jednostavnog algoritma za odabir parametara, invertibilnosti, uspješnog dešifriranja poruka i bolje sigurnosti. U ovom članku predstavljamo tehniku napada na ITRU kriptosustav, koja se uglavnom temelji na jednostavnoj frekvencijskoj analizi slova šifrata.

Hayder R. Hashim
Institute of Mathematics
University of Debrecen
P. O. Box 400, 4002 Debrecen, Hungary
and
Faculty of Computer Science and Mathematics
University of Kufa
P.O.Box 21, 54001 Al Najaf, Iraq
E-mail: hashim.hayder.raheem@science.unideb.hu
hayderr.almuswi@uokufa.edu.iq

Alexandra Molnár
Institute of Mathematics
University of Debrecen
P. O. Box 400, 4002 Debrecen, Hungary
E-mail: alexandra980312@freemail.hu

Szabolcs Tengely
Institute of Mathematics
University of Debrecen
P. O. Box 400, 4002 Debrecen, Hungary
E-mail: tengely@science.unideb.hu

Received: 11.8.2020.
Revised: 4.1.2021.
Accepted: 19.1.2021.