Cryptanalysis of ITRU

Hayder R. Hashim

Dept. of Algebra and Number Theory
Institute of Mathematics
University of Debrecen
hashim.hayder.raheem@science.unideb.hu
(This is a joint work with Dr. Sz. Tengely and A. Molnár)

20th Central European Conference on Cryptology

June 24-26, 2020

Summary of the talk

What is ITRU?

What is ITRU?

ITRU cryptosystem, is a public key cryptosystem and one of the known variants of NTRU (N^{th} Degree Truncated Polynomial Ring) cryptosystem, which was proposed in 2017 by Gaithuru, Salleh, and Mohamad [1].

What is ITRU?

What is ITRU?

ITRU cryptosystem, is a public key cryptosystem and one of the known variants of NTRU (N^{th} Degree Truncated Polynomial Ring) cryptosystem, which was proposed in 2017 by Gaithuru, Salleh, and Mohamad [1].

What is NTRU?

1996, Hoffstein, Pipher and Silverman [2] proposed a class of fast public key cryptosystems called NTRU cryptosystem (Classical NTRU cryptosystem). This cryptosystem has the following features:

- It is considered as a lattice-based public key cryptosystem, and it is the first asymmetric cryptosystem based on the polynomial ring $\frac{\mathbb{Z}[X]}{(X^N-1)}$.

What is NTRU?

- It has very good features comparing to other public key cryptosystems such as reasonably short, easily created keys, high speed, and low memory requirements.

What is NTRU?

- 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.

What is NTRU?

- 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).

Back to What is ITRU?

Structure of ITRU

The authors proposed this cryptosystem in the way that 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 the small modulus (an integer).

Back to What is ITRU?

Structure of ITRU

The authors proposed this cryptosystem in the way that 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 the small modulus (an integer).
- Random integers f, g and r are chosen such that f is invertible modulo p.

Back to What is ITRU?

Structure of ITRU

The authors proposed this cryptosystem in the way that 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 the small modulus (an integer).
- 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 (assuming that the message is comprised of English alphabetical characters based on *ASCII* conversion tables, that is the one with $a \rightarrow 97$.)

What is ITRU?

Structure of ITRU (continued (2))

- 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.

What is ITRU?

Structure of ITRU (continued (2))

- 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

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

What is ITRU?

Structure of ITRU (continued (2))

- 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
$$h \equiv p \cdot F_q \cdot g \pmod{q}.$$
- The encryption procedure is similar to the one applied in NTRU cryptosystem [2], one generates a random integer r and computes
$$e \equiv r \cdot h + m \pmod{q}.$$

What is ITRU?

Structure of ITRU (continued (3))

- To get the plaintext from the ciphertext one determines

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

What is ITRU?

Structure of ITRU (continued (3))

- To get the plaintext from the ciphertext one determines

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

- Recovering the message is done by computing

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

What is ITRU?

Comparison between NTRU and ITRU

According to results of [1], the authors claimed that ITRU has better features comparing to the classical NTRU such as

- ITRU has a simple parameter selection algorithm comparing to the one of NTRU.

What is ITRU?

Comparison between NTRU and ITRU

According to results of [1], the authors claimed that ITRU has better features comparing to the classical NTRU such as

- ITRU has a simple parameter selection algorithm comparing to the one of NTRU.
- ITRU has a successful message decryption, while the classical NTRU cryptosystem has a probability of decryption failure of 2^{-145}.

What is ITRU?

Comparison between NTRU and ITRU

According to results of [1], the authors claimed that ITRU has better features comparing to the classical NTRU such as

- ITRU has a simple parameter selection algorithm comparing to the one of NTRU.
- ITRU has a successful message decryption, while the classical NTRU cryptosystem has a probability of decryption failure of 2^{-145}.
- ITRU has a better security than NTRU. In fact, ITRU is based on integer rings as opposed to the lattice structure of the classical NTRU. The security of ITRU is based on the integer factorization problem.

Attacking/ Breaking ITRU cryptosystem

What are the used tools to attack this cryptosystem ?

Used tools to attack ITRU

- From the construction, ITRU presents a substitution cipher, and one of the best effective attacks against the substitution ciphers in general presented by the frequency analysis technique.
- Therefore, by using a simple frequency analysis this attack is preformed with help of SageMath Software in which the plaintext is completely recovered only from the ciphertext and the public key with no need to have the private key.

We preform the attack with the following Steps:

Step 1: ITRU Cryptosystem Implementation

- 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 (*ASCII* conversion tables).
- In the following SageMath implementation we can use different bounds. With the following example, we use 255 to preform our implementation on the arbitrary message: Cryptanalysis.

ITRU Implementation Input

```
s ='Cryptanalysis'
pretty_ print('The message is:', s)
r = 8
p = 1000
```

ITRU Implementation Input

```
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))
```

Step 1: ITRU Cryptosystem Implementation (continued 3)

ITRU Implementation Input

```
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))
```

The output is as follows:

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

ITRU Implementation

We may preform our implementation with the bound 4999 as the largest possible value of the representations on the arbitrary message: Implementation of ITRU cryptosystem.

Output

The message is: Implementation of ITRU cryptosystem
The ASCII code of the message: [73, 109, 112, 108,101,109,101, 110, 116, 97, 116, 105, 111, 110, 32, 111, 102, 32, 73, 84, 82, 85, 32, 99, 114, 121, 112, 116, 111, 115, 121, 115, 116, 101, 109]
Large modulus : 3212849
Public key : 3160038
Private key pair :$(177, 113)$
The encrypted message: [2790434, 2790470, 2790473, 2790469, 2790462, 2790470, 2790462, 2790471, 2790477, 2790458, 2790477, 2790466, 2790472, 2790471, 2790393, 2790472

Output

2790463, 2790393, 2790434, 2790445, 2790443, 2790446, 2790393, 2790460, 2790475, 2790482, 2790473, 2790477, 2790472, 2790476, 2790482, 2790476, 2790477, 2790462, 2790470]

$f \cdot e \pmod q$ is:[2340921, 2347293, 2347824, 2347116, 2345877, 2347293, 2345877, 2347470, 2348532, 2345169, 2348532, 2346585, 2347647, 2347470, 2333664, 2347647, 2346054, 2333664, 2340921, 2342868, 2342514, 2343045, 2333664, 2345523, 2348178, 2349417, 2347824, 2348532, 2347647, 2348355, 2349417, 2348355, 2348532, 2345877, 2347293]

$F_p \cdot a \pmod p$ is: [73, 109, 112, 108,101,109,101, 110, 116, 97, 116, 105, 111, 110, 32, 111, 102, 32, 73, 84, 82, 85, 32, 99, 114, 121, 112, 116, 111, 115, 121, 115, 116, 101, 109]

The original message: Implementation of ITRU cryptosystem

Step 2: ITRU Plaintext Recovery

Performing the attack: 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 [1] (without spaces):

′ThegoalofthisstudyistopresentavariantofNTRUwhichis basedontheringofintegersasopposedtousingthepolynomial ringwithintegercoefficients.WeshowthatNTRUbasedonthe ringofintegers(ITRU),hasasimpleparameterselection algorithm,invertibilityandsuccessfulmessagedecryption. Wedescribeaparameterselectionalgorithmandalsoprovide animplementationofITRUusinganexample.ITRUisshown tohavesuccessfulmessagedecryption,whichprovidesmore assuranceofsecurityincomparisontoNTRU.′

Step 2: ITRU Plaintext Recovery

Remarks:

- If this paragraph is encrypted with the large modulus $q = 8170933$ and the public key $h = 3942626$ (this key is created in case of having 4999 as an upper bound for the representations), then the ciphertext starts as

7028293, 7028313, 7028310, 7028312, 7028320, 7028306, 7028317, 7028320, 7028311, 7028325,....

- In fact, there are 32 different numbers appearing in the ciphertext these are between 7028249 and 7028330.
- A simple frequency analysis with the SageMath function: `frequency_distribution()` provides the following data:

Obtained data:

$$[(7028249, 0.00223713646532438), (7028250, 0.00223713646532438),$$
$$(7028253, 0.00671140939597315), (7028255, 0.00894854586129754),$$
$$(7028282, 0.00671140939597315), (7028287, 0.00671140939597315),$$
$$(7028291, 0.0134228187919463), (7028293, 0.0156599552572707),$$
$$(7028294, 0.0134228187919463), (7028296, 0.00447427293064877),$$
$$(7028306, 0.0693512304250559), (7028307, 0.00894854586129754),$$
$$(7028308, 0.0357941834451902), (7028309, 0.0246085011185682),$$
$$(7028310, \boxed{0.109619686800895}), (7028311, 0.0223713646532438),$$
$$(7028312, 0.0290827740492170), (7028313, 0.0380313199105145),$$
$$(7028314, 0.0850111856823266), (7028317, 0.0313199105145414),$$
$$(7028318, 0.0290827740492170), (7028319, 0.0648769574944072),$$
$$(7028320, 0.0738255033557047), (7028321, 0.0313199105145414),$$

$$(7028323, 0.0536912751677852), (7028324, 0.0850111856823266), (7028325, 0.0693512304250559), (7028326, 0.0201342281879195), (7028327, 0.0111856823266219), (7028328, 0.0111856823266219), (7028329, 0.0022371364653243 8), (7028330, 0.0134228187919463)]$$

We see that the number 7028310 appears the most in the ciphertext. Therefore, 7028310 represents either $'e','a'$ or $'t'$. If it is $'e' = 101$, then we apply the formula

$$c_i - 7028209,$$

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,....

which corresponds to the original plaintext.

References:

J. N. Gaithuru, M. Salleh, and I. Mohamad, *ITRU: NTRU-Based Cryptosystem Using Ring of Integers*, International Journal of Innovative Computing, 7(1),(2017).

J. Hoffstein, J. Pipher and J. H. Silverman , *NTRU: A ring-based public key cryptosystem*,Algorithmic number theory. 3rd international symposium, ANTS-III, Portland, OR, USA, June 21–25, 1998. Proceedings, Berlin: Springer, (1998).

Thank you for your attention!