NTRU Modulo p Flaw

Anas Ibrahim, Alexander Chefranov
Computer Engineering Department
Eastern Mediterranean University
Famagusta, North Cyprus

Abstract

NTRU encryption is a standardized public-key cryptosystem which is considered faster than RSA and ECC. For encryption, NTRU adds the product of $p, h, r$ to the plaintext, where $p$ is a predefined public parameter, $h$ is the public key, and $r$ is a pseudo-randomly generated blinding polynomial. For decryption, NTRU uses two private keys. We prove that for some parameters NTRU has the modulo $p$ flaw, so NTRU-encrypted plaintext can be disclosed just by applying modulo $p$ operation to the ciphertext without the need of using any of NTRU secret keys. We provide also statistical estimates of the probability of having NTRU modulo $p$ flaw cases for different values of $N$, where $N$ is the order of polynomial ring used in NTRU. The probabilities show that NTRU modulo $p$ flaw may take place rather often. NTRU amendment to withstand the flaw is proposed.

1. Introduction

The NTRU is proposed in [1], and standardized as IEEE-1363 [2]. NTRU is faster than RSA and ECC in encryption and decryption [3]. NTRU imposes certain constraints on its parameters. We show that there exist some cases when NTRU-encrypted plaintext can be revealed without knowledge of its private keys, just applying modulo $p$ operation to the ciphertext[4]. The rest of the paper is organized as follows. In Section 2 we provide a brief description of NTRU and give an example of NTRU encryption-decryption. In Section 3 the NTRU modulo $p$ flaw is shown by example; explanations are given for the example. In Section 4, we present statistics of cases when NTRU has modulo $p$ flaw for different $N$ values. In Section 5, NTRU amendment is proposed to fix the flaw. In Section 6, conclusion is given.

2. NTRU Description and Example of Encryption-Decryption

We describe NTRU according to [5].

2.1 NTRU Description

NTRU has four positive integer parameters, $(N, p, q, d)$, and uses polynomials modulo $P(x) = x^N - 1$ (1) with integer coefficients from the ring $R = \mathbb{Z}[x]/(x^N - 1)$, (2)

where $\mathbb{Z}[x]$ is the set of polynomials with integer coefficients. A polynomial, $a(x) \in R$, looks as follows:

$$a(x) = \sum_{i=0}^{n-1} a_i x^i = [a_0, a_1, ..., a_{n-1}]$$. (3)

NTRU assumes that

$$\text{gcd}(p, q) = \text{gcd}(N, q) = 1, q > (6d + 1)p, \quad (4)$$

$p > 2$ is prime, $d$ is an integer defining structure of used by NTRU polynomials, $f(x)$, $g(x)$, $r(x)$, introduced in Subsections 2.1.1 and 2.1.2 farther. NTRU uses subrings, $R_k \subset R$, with coefficients restricted to $\mathbb{Z}/k\mathbb{Z}$, where $R_k$ is:

$$R_k = \left(\frac{\mathbb{Z}/k\mathbb{Z}[x]}{x^N - 1}\right).$$ (5)

where $\mathbb{Z}/k\mathbb{Z}$ is a set of integers in the range $0, 1, ..., k-1$ for any positive $k \in \mathbb{Z}$.
2.1.1. NTRU Private and Public Keys Generation.

For key generation, NTRU uses polynomials from $T(d_1,d_2)$ defined as follows (see (1), (2)):

$$a \in T(d_1,d_2) = \begin{cases} a(x) \in R: \text{a has } d_1 \text{ coefficients equal to } 1, \\ \text{a has } d_2 \text{ coefficients equal to } -1, \\ \text{the rest coefficients equal to } 0 \end{cases}$$

(6)

NTRU uses four private keys:

$f(x), F_q(x), F_p(x), g(x)$. The first private key, $f(x)$, is generated as follows (see (3), (6)):

$$f(x) = [f_0, f_1, ..., f_{d_1-1}] \in T(d+1,d).$$

(7)

The private key (7), $f(x)$, must have inverses modulo $p$ and $q$, that is, $F_q(x), F_p(x)$, respectively, used as the second and third private keys:

$$f \cdot F_q \equiv 1 \pmod{q} \quad \text{and} \quad f \cdot F_p \equiv 1 \pmod{p},$$

(8)

where '*' denotes polynomial multiplication in $R$ (see (2)). The fourth private key, $g(x)$, is randomly chosen as follows (see (6)):

$$g(x) \in T(d,d).$$

(9)

The public key, $h(x)$, is computed using (8), (9) as follows:

$$h = F_q \cdot g \pmod{q}.$$  

(10)

2.1.2. NTRU Encryption.

The plaintext message $m(x)$, is assumed to meet the following condition:

$$m(x) \in R_p.$$  

(11)

Moreover, the coefficients of $m$ are assumed to be center-lifted, i.e. to be in $(-\frac{1}{2}p, \frac{1}{2}p]$. For example, if $p$ is odd equal to 5, then normally the coefficients are from 0, ..., 4 but after center-lifting, they are in $-2, ..., 2$. And if $p$ is equal to 4, then center-lifted coefficients are in $-1, ..., 2$. A pseudo-randomly generated blinding polynomial, $r(x)$, is chosen as follows:

$$r(x) \in T(d,d).$$  

(12)

Ciphertext, $e(x)$, is computed using (10) -(12) as

$$e = pr \cdot h + m \pmod{q}.$$  

(13)

2.1.3. NTRU Decryption.

Decryption in NTRU consists of Steps 1 and 2 described below.

Step 1: The first private key, $f(x)$, is applied to (13):

$$a = f \cdot e \pmod{q} = pr \cdot g + f \cdot m \pmod{q}$$  

where (8) and (10) are used.

Step 2: The second private key, $F_p$ is applied to (14) after $a$ is center-lifted:

$$m = a \cdot F_p \pmod{p}$$  

(15)

where (8) is used and the contributor with factor $p$ in (14) vanishes due to the constraints (4), (7)-(9), (12) imposed which guarantee that sum in the rightmost expression in (14) is a polynomial with coefficients strictly less than $q$, so that mod $q$ operation, applied last in (14), does not change the coefficients.

2.2 Example of NTRU Key Generation and Encryption-Decryption

Example 1. Let according to (4),

$$N = 5; d = 1; p = 3; q = 32 > (6d + 1)p = 21 .$$

Let according to (7),

$$f(x) = x^3 + x^2 - 1 = [-1,0,1,0].$$

(17)

Then, according to (8),

$$F_q = x^4 + x + 31$$

$$F_p = x^4 + x + 2.$$  

(18)

Let us check (18) using (17):

$$f(x) \cdot F_q(x) = (x^3 + x^2 - 1)(x^4 + x + 31) = x^7 + x^6 + 31x^5 + 31x + 1 \equiv 1 \pmod{x^5 - 1} \pmod{q}$$
\[ f(x) \ast F_p(x) = (x^3 + x^2 - 1)(x^3 + x + 2) = x^6 + x^4 + 2x^2 + x + 1 + 1 \mod (x^5 - 1) \mod p \]

Let according to (9), (11) and (12), \( g(x) \), \( r(x) \), and \( m(x) \) are selected as,
\[
 r(x) = x-1, \quad g(x) = x - 1, \quad m(x) = x^2 + x + 1 \in R_p. \tag{20}
\]

Public key, \( h \), according to (10), (18), (19) is
\[
 h = F^*g \mod q = (x^3 + x + 31)^*(x-1) = x^6 + 31x^4 + x^2 + 30x + 1 \mod (x^5 - 1) \mod 32 = 31x^4 + x^2 + 30x + 2 \tag{21}
\]

Ciphertext according to (13), (19)-(21), is:
\[
 e = (p \cdot r \ast h + m) \mod q = (3(x-1)*31x^4 + x^3 + 30x + 1 + x) + x + 1 \mod 32 = 3x^4 + 3x^3 + 24x^2 + 13x + 24 \tag{22}
\]

To decrypt ciphertext (22), apply Step 1 (14) using (17)
\[
 a = f \ast e \mod q = (x^3 + x^2 - 1)(3x^4 + 3x^3 + 24x^2 + 13x + 24) \mod 32 = 2x^4 + 2x^3 + 3x^2 + 3x + 25 \tag{23}
\]

In Step2, the message (20) is retrieved using (15), (18), and center-lifted \( a \) with respect to \( q \) from (23):
\[
 m = F^*a \mod p = (x^3 + x + 2)(2x^4 + 2x^3 + 3x^2 - 7x + 3) \mod 3 \tag{24}
\]

Thus, in (24), we get back the plaintext, \( m(x) \), from (20). We see that NTRU encryption-decryption procedure \( (11)-(15) \) from [5], works correctly in the Example.

3. NTRU Modulo \( p \) Flaw Example and Its Explanation

3.1. NTRU Modulo \( p \) Flaw Example

Consider again the Example 1 of NTRU encryption-decryption from Section 2.2. First, we center-lift the ciphertext (22) with respect to \( q = 32 \).

\[
 e = 3x^4 + 3x^3 + 24x^2 + 13x + 24 \mod q = 3x^4 + 3x^3 - 8x^2 + 13x - 8 \mod q \tag{25}
\]

Then applying modulo \( p \) operation directly to the center-lifted ciphertext (25), we also disclose the original plaintext, \( m(x) \), from (20), as follows
\[
 m = e \mod p = (3x^4 + 3x^3 - 8x^2 + 13x - 8) \mod 3 \tag{26} = x^2 + x + 1
\]

Comparing (26) and (20), we see that actually, the plaintext is restored without any key, by knowledge of the public value of public parameter \( p \) only. Thus, the example represents NTRU flaw that we call “modulo \( p \) flaw”.

3.2. NTRU Modulo \( p \) Flaw Example Explanation

The reason of NTRU modulo \( p \) flaw is that in the encryption (13) it might happen that the polynomial used for hiding the plaintext, \( m(x) \), from (11),
\[
 A = p \cdot r \ast h = [a_0, ..., a_{N-1}] \tag{27}
\]
has all its coefficients by absolute value less than \( q \).
\[
 \text{for } \forall i \in \{0, ..., N-1\}, \quad |a_i| < q, \tag{28}
\]

In such a case, modulo \( q \) operation used in (22), preserves \( A \) being a multiple of \( p \) that can be eliminated from (22) just by modulo \( p \) operation applied to the ciphertext, \( e \), as we exactly made in (26).

For the NTRU modulo \( p \) flaw realization, we need finding such inverse of (7) that the products (10), (27) used in (13), have coefficients by absolute value less than \( q \) (see (28)). Hence, we need finding dependence of the products’ coefficients on the coefficients of (7). It is done in the next Subsection 3.2.1. Then, in Subsection 3.2.2, we find such polynomial (7) that the product (27) be more likely to have coefficients by absolute value less than \( q \).

3.2.1. Finding Inverse of the Polynomial \( f(x) \)

Modulo \( x^N - 1 \)

Consider finding of an inverse, \( f^{-1}(x) = [h_0, b_1, ..., b_{N-1}] \), of (7) in \( R \).
\[
P_N(x) = x^N - 1. \tag{29}
\]
By definition,
\[ f(x) \cdot f^{-1}(x) = c(x) \cdot P_b(x) + 1, \quad (30) \]
\[ c(x) = \sum_{i=0}^{N-2} c_i x^i. \quad (31) \]

From (7), (29) - (31):
\[ \sum_{i=0}^{2N-2} (\sum_{b_i \in \mathbb{J}, i \neq N} f b_i) x^i = \sum_{i=0}^{i=N} c_{i-N} x^i - \sum_{i=0}^{N} c_i x^i + 1. \quad (32) \]

Equating coefficients near respective powers, we get from (32) the following system of linear algebraic equations with respect to unknowns \( b_0, b_{N-1}, c_0, \ldots, c_{N-2} \),
\[ \sum_{j=0}^{N-i} f b_{i,j} = c_{i-N}, \quad \text{for} \quad i = N, \ldots, 2N - 2, \quad (33) \]
\[ \sum_{j=0}^{N-1} f b_{N-1,j} = 0, \quad (34) \]
\[ \sum_{j=0}^{i} f b_{i,j} = -c_i, \quad i = 1, \ldots, N - 2, \quad (35) \]
\[ 1 - f_0 b_0 = c_0. \quad (36) \]

Preserving \( b_0, \ldots, b_{N-1} \), only, from (33) - (36), we get
\[ \sum_{j=0}^{N-i} f b_{i,j} + \sum_{j=0}^{N-i} f b_{j} = 0, \quad \text{for} \quad i = 2N - 2, \ldots, N + 1, \quad (37) \]
\[ f_0 b_0 + \sum_{j=0}^{N-i} f b_{j} = 1, \quad (38) \]
\[ \sum_{j=0}^{N-i} f b_{N-1,j} = 0 \quad (39) \]

For \( N = 5 \), the matrix of coefficients in (37) - (39) is as follows
\[
\Delta = \begin{bmatrix}
    f_3 & f_2 & f_1 & f_0 & f_4 \\
    f_2 & f_1 & f_0 & f_4 & f_3 \\
    f_1 & f_0 & f_4 & f_3 & f_2 \\
    f_0 & f_4 & f_3 & f_2 & f_1 \\
    f_4 & f_3 & f_2 & f_1 & f_0
\end{bmatrix}
\]

Determinant of (40), \( \det(\Delta) \), calculated using Maple® 12, is as follows (Figure 1):

Figure 1. Definition of matrix (40), and its determinant, in Maple 12®

Right hand side, RHS, of equations (37) - (39), for \( N = 5 \) is as follows
\[ RHS = (0,0,0,1,0). \quad (41) \]

Using Cramer’s rule[6], find
\[ b_i = \frac{\det(\Delta_j)}{\det(\Delta)}, \quad \text{for} \quad i = 0, \ldots, N - 1, \quad (42) \]
where the matrix \( \Delta_i \) is the matrix \( \Delta \) with column \( i \) replaced by \( RHS = (0,0,0,1,0) \), which is the right side of (45).

Division in (42) is made modulo \( p \) or \( q \) to find \( F_p \) or \( F_q \) from (8) respectively. For correctness of the division in (42), determinant in the denominator shall have multiplicative inverse modulo \( p \) or \( q \), and shall be co-prime to them. For arbitrary determinants, their inverses may be rather large integers resulting in large coefficients \( b_i \) in (42), hence, leading to large coefficients in \( h \) (10), and, thus, to violation of (28). To minimize the coefficients, we need the absolute value of the determinant value, \( \det(\Delta) \) (see (40)), equal to 1. Such a case is considered in the next Subsection 3.2.2 and was used in the Example 1 in Section 2.2.

3.2.2 Getting \( |\det(\Delta)| = 1 \). For the polynomial (17) used in Example 1 in section 2.2, from (40) and Figure 1, we have,
\[ |\det(\Delta)| = 1; \quad (43) \]
\[ \det(\Delta_0) = -1; \quad \det(\Delta_1) = 1; \quad \det(\Delta_2) = 0; \quad \det(\Delta_3) = 0; \quad \det(\Delta_4) = 1. \quad (44) \]

By substituting (43), (44) into (41),
\[ f^{-1}(x) = x^4 + x - 1. \quad (45) \]
From (8), (45), we get (18).
4. Estimate of the Probability of NTRU Modulo $p$ Flaw

As discussed in Section 3.2.1, we need the determinant value, $\det(\Delta)$, be equal to 1 in order to minimize coefficients (42). The crucial question is how probably a user will choose permutation of $\pm 1$ coefficients of (7) that ends up with $|\det(\Delta)|=1$ (40), to answer this question we conducted statistical experiment for ($N=5,7,11$), results of which are shown in Table 1 and Figure 2. These probabilities estimate roughly probability of the NTRU modulo $p$ flaw since (28) most likely might happen in the cases when (43) holds. However, in Example 2 below, we show that (28) may be not true and NTRU modulo $p$ flaw is not applicable for the case of (43) holding.

Table1. Probability of $|\det(\Delta)|=1$

<table>
<thead>
<tr>
<th>$N$</th>
<th>No. of permutations with $\det(\Delta)=1$</th>
<th>Total Number of permutations</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>10</td>
<td>40</td>
<td>25%</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
<td>350</td>
<td>12%</td>
</tr>
<tr>
<td>11</td>
<td>382</td>
<td>24057</td>
<td>1.5%</td>
</tr>
</tbody>
</table>

![Figure 2. Probability of $|\det(\Delta)|=1$ Dependence on $N$.](image)

As we can notice from Table 1 and Figure 2, the probability of choosing permutation of $\pm 1$ coefficients of (7) that ends up with (43) holding is very high at low value of $N=5$, where probability is 25% and we see that probability of (43) holding drops to 1.5% when $N=11$, i.e. the probability of (43) holding decreases with the growth of $N$. Choosing permutation of $\pm 1$ coefficients of (7), that ends up with (43) holding, doesn’t guarantee (28) to hold since the product (27) depends on the value of polynomial (9) used in (10) and polynomial (12) used in (27). In the following Example 2, we show a case when (43) holds but (28) doesn’t hold and NTRU modulo $p$ flaw is not applicable in that case.

**Example 2.** Let us consider Example 1 but instead of (19), $g(x)$ and $r(x)$ are as follows,

$$r(x) = -x^4 + x^3$$

$$g(x) = x^4 - 1$$

We also update (16) to be as follows,

$$N = 5; d = 1; p = 3; q = 23 > (6d + 1)p = 21,$$  

We have shown in Section 3.2.2 that (43) holds for the polynomial $f(x)$ (17) from Example 1. Public key, $h$, according to (10), (18), (45) is

$$h = F_q * g \mod q$$

$$= (x^4 + x + 22)(x^4 - 1)$$

$$= (x^4 + x^2 + 21x^2 + 22x + 1) \mod (x^5 - 1) \mod 23$$

$$= 21x^4 + x^3 + 22x + 2$$

Ciphertext according to (13), (18), (46), (47) is:

$$e = (p \cdot r * h + m) \mod q$$

$$= (3 \cdot (-x^4 + x^3) \ast (21x^4 + x^3 + 22x + 2)$$

$$+ x^2 + x + 1) \mod 23$$

$$= 14x^4 + 12x^3 + 15x^2 + 4x + 4$$

After obtaining ciphertext, $e(x)$ in (48), we try to apply NTRU modulo $p$ flaw steps introduced in Subsection 3.1. First, we center-lift the ciphertext (48) with respect to $q = 23$.

$$e = 14x^4 + 12x^3 + 15x^2 + 4x + 4 \mod q$$

$$= -9x^4 - 11x^3 - 8x^2 + 4x + 4 \mod q.$$  

(50)

Then applying modulo $p$ operation directly to the center-lifted ciphertext (49), we get message, $m'$, that is not same as the plaintext message, $m(x)$, from (20), and, hence, the NTRU modulo $p$ flaw doesn’t work in that case:

$$m' = e \mod p$$

$$= (-9x^4 - 11x^3 - 8x^2 + 4x + 4) \mod 3$$

$$= x^3 + x + 1 \neq x^3 + x + 1.$$  

(51)
Thus, Example 2 shows that in spite of (48) holding, condition (28) for NTRU modulo p applicability does not hold, and applying modulo p operation to the ciphertext (49) after center-lifting in (48), we do not get back the plaintext (20) in (50).

5. NTRU Amendment to Fix NTRU Modulo p Flaw

NTRU constraints (4) guarantee correctness of decryption process (14), (15). But these constraints donot guarantee that at least one of the product (27) coefficients is exceeding the value of $q$ in absolute value. To fix the NTRU modulo p flaw specified in the present paper, an amendment must be made so that in addition to (4), it is necessary that the following condition shall hold:

$$M = pF_q \equiv [M_0, \ldots, M_{N-1}]$$

for $\exists i \in \{0, \ldots, N-1\}$, $|M_i| > q$.

Thus, the product, $p \cdot F_q$, shall have at least one coefficient exceeding $q$ by the absolute value. If condition (51) holds, eliminating of the product, $A$, from equation (27) by modulo $p$ operation is generally not possible because at least one term in the product maybe not a multiple of $p$. However, in spite of the condition of applicability of the modulo p flaw is violated if (51) holds, it is not excluded an opportunity that modulo p operation reveals a plaintext, and this question needs further investigation.

6. Conclusion

In this paper, we presented NTRU modulo $p$ flaw by construction of an example of a plaintext decryption just applying modulo $p$ operation to the ciphertext. We explained that the flaw happens when all coefficients of (27) are less than $q$ in absolute value. In this case, $A$ from (27) has coefficients that are multiples of $p$ which can be eliminated by modulo $p$ operation. We also presented statistics of probability of the determinant (39) absolute value getting equal to 1 that in many cases allows application of NTRU modulo $p$ flaw. We considered dependence of the probability on $N$, the order of the polynomial (1). These statistics shows that the probability decreases with the growth of $N$. To fix the NTRU modulo $p$ flaw, we proposed an amendment to NTRU by extending condition (4) by condition (51) guaranteeing that at least one coefficient of (27) is exceeding $q$ in absolute value so that plaintext generally cannot be revealed using modulo $p$ operation.

7. References


