Chosen-Ciphertext Attacks on Optimized NTRU

Jin Hong, Jae Woo Han, Daesung Kwon, and Daewan Han

December 9, 2002

Abstract

NTRU([3]) is an efficient public-key cryptosystem proposed by Hoffstein, Pipher, and Silverman. In [4], some modifications were made to the original scheme to make the system even faster. We give three chosen-ciphertext attacks on the un-padded version of this *optimized* NTRU cryptosystem. Any one of the three attacks will recover the private key with just a few queries to the decryption machine.

1 Introduction

In the work [3], Hoffstein, Pipher, and Silverman presented a new public-key cryptosystem named NTRU. Security of the NTRU cryptosystem comes from the interaction of polynomial mixing systems and the independence of reduction modulo two numbers p and q. Efficiency of this system is one of its biggest merits, and the system is being considered by organizations for standards([1, 6]).

The NTRU cryptosystem depends on several parameters and in the original work, the value $p = 3$ was suggested. With this choice, the message space is defined by polynomials with coefficients in the set $\{-1, 0, 1\}$. This certainly is not friendly to computer systems, which are binary in nature. Hence, in [4], it was suggest that $\mathbf{p} = x + 2$ be used. The message space now consists of binary polynomials. Special form for the private key was also introduced. It is set to be

$$\mathbf{f} = 1 + \mathbf{p} * \mathbf{F}.$$

It removes the need for an inversion calculation during key setup and also simplifies the decryption process. We shall call this the *optimized* NTRU cryptosystem.

While there are many reports on the security of the original NTRU cryptosystem, the optimized NTRU system has not gone through much analysis. It is generally believed that the security of the optimized NTRU cryptosystem is equivalent to the original one. We show in this paper that without padding, the optimized NTRU system is much weaker than the original system from the viewpoint of chosen-ciphertext attacks. The optimizations, especially, the choice of special forms for the private key, has introduced new weakness into the NTRU cryptosystem.

In practice, the polynomial $\mathbf{F}$, used in defining the private key $\mathbf{f}$, is also set to be of special form. It is taken to be either

1. a binary polynomial, or
2. of the form $a * b + c$, where a, b, and c are sparse binary polynomials.

It is even suggested in [4] that polynomial satisfying both conditions be used for $\mathbf{F}$.

We present three chosen-ciphertext attacks in this paper. Under realistic values of various parameters, our first two attacks will recover the private key up to one of a few candidates, if $\mathbf{F}$ is binary. At most 4 (usually just 2) trial texts will be needed for the first attack and the second attack makes just one query to the decryption machine. The two attacks are still applicable when $\mathbf{F}$ is not binary, although with smaller strength.

The third attack is the strongest of our three attacks. Under normal conditions, it uses just one query to the decryption machine and completely determines the private key. It does not depend on the form of $\mathbf{F}$.

The paper is organized as follows. Section 2 describes the un-padded version of optimized NTRU cryptosystem. This will set the grounds of our attack. Section 3, 4, and 5 explains the three chosen-ciphertext attacks. The last section closes the paper with some comments.

2 Description of the NTRU cryptosystem

Review of the NTRU cryptosystem is given in this section. We mostly follow [1, 4] ignoring the padding part.

Let N be an odd prime. We will be working over the ring $\mathcal{R} = \mathbf{Z}[x]/(x^N - 1)$. The ring $\mathcal{R}$ is identified with the set of integer polynomials of degree less than N. Multiplication in $\mathcal{R}$ is denoted by $*$. We set $\mathbf{p} = x + 2 \in \mathcal{R}$ and fix a positive integer q relatively prime to $\mathbf{p}$.

2.1 Key generation

The private key

$$\mathbf{f} = 1 + \mathbf{p} * \mathbf{F} \in \mathcal{R} \tag{1}$$

is chosen so that it is invertible modulo q. The inverse will be denoted by $\mathbf{f}_q$ so that

$$\mathbf{f} * \mathbf{f}_q \equiv 1 \pmod{q}. \tag{2}$$

The polynomial $\mathbf{F}$, used in defining the private key $\mathbf{f}$ is either

1. a binary polynomial with d_F-many nonzero coefficients, or
2. of the form $\mathbf{F}_1 * \mathbf{F}_2 + \mathbf{F}_3$ with each $\mathbf{F}_i$ a binary polynomial with d_{F_i}-many nonzero coefficients.

The values d_F and d_{F_i} are predefined public values. We shall name the first case *binary*-$\mathbf{F}$, and call the second one *LHW*-$\mathbf{F}$(low Hamming weight).

Another random binary polynomial $\mathbf{g}$ with d_g coefficients equal to 1 is chosen, and the public key is set to

$$\mathbf{h} = \mathbf{p} * \mathbf{f}_q * \mathbf{g} \pmod{q}. \tag{3}$$

N	q	d_F	d_{F_1}	d_{F_2}	d_{F_3}	d_g	d_r
251	128	72	8	8	8	72	72
347	128	64	7	8	8	173	64
503	256	420	20	20	20	251	170

Table 1: Realistic parameter values

Realistic values for various parameters are given in Table 1([1]). Notice that $d_F = d_{F_1} \cdot d_{F_2} + d_{F_3}$ in all cases.

2.2 Encryption

To encrypt a binary message $\mathbf{m} \in \mathcal{R}$, a random binary polynomial $\mathbf{r} \in \mathcal{R}$ is chosen with d_r coefficients equal to 1. The value

$$\mathbf{e} = \mathbf{r} * \mathbf{h} + \mathbf{m} \pmod{q} \tag{4}$$

is calculated to be the ciphertext.

2.3 Decryption

To explain the decryption process, we first need to explain the notion of taking residue modulo $\mathbf{p}$. Given a polynomial $f(x) \in \mathcal{R}$, there (almost) always exists a unique binary polynomial $g(x) \in \mathcal{R}$ satisfying

$$f(-2) \equiv g(-2) \pmod{2^N + 1}.$$

We denote by $\mathrm{Mod}_{\mathbf{p}}(f(x))$, this unique binary polynomial. There is one exception to the existence of such a binary polynomial, which is when $f(-2) = \frac{2^{N+1}+2}{3} \pmod{2^N + 1}$. In this case, we take $\mathrm{Mod}_{\mathbf{p}}(f(x)) = 2 + x^2 + x^4 + \cdots + x^{N-1}$. In short, the operator $\mathrm{Mod}_{\mathbf{p}}$ chooses a specific representative of a given polynomial modulo $\mathbf{p}$.

We also define the operator $\mathrm{Mod}_q^{\mathcal{A}}$ for any real number $\mathcal{A}$. Given n in either $\mathbf{Z}_q$ or $\mathbf{Z}$, the value $\mathrm{Mod}_q^{\mathcal{A}}(n)$ will be the unique integer congruent to n modulo q, contained in the interval $(\mathcal{A} - \frac{q}{2}, \mathcal{A} + \frac{q}{2}]$. The operator $\mathrm{Mod}_q^{\mathcal{A}}$ will also be applied to polynomials with coefficients in $\mathbf{Z}_q$ or $\mathbf{Z}$.

Given a ciphertext $\mathbf{e}$, the decryption process is done as follows.

1. $I \leftarrow \mathrm{Mod}_q^{\frac{N}{2}}(\mathbf{e}(1) - \mathbf{r}(1) \cdot \mathbf{h}(1))$.
2. $\mathcal{A} \leftarrow \frac{1}{N}(\mathbf{p}(1) \cdot \mathbf{r}(1) \cdot \mathbf{g}(1) + I \cdot \mathbf{f}(1))$.
3. $\mathbf{a} \leftarrow \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{f} * \mathbf{e})$.
4. Output $\mathrm{Mod}_{\mathbf{p}}(\mathbf{a})$.

We refer the readers to [9] for explanation on why this works.

Remark 2.1. Since $\mathbf{r}(1) = d_r$, $\mathbf{g}(1) = d_g$, and $\mathbf{f}(1) = 1 + 3 \cdot d_F$, the values I and $\mathcal{A}$ may be calculated from just $\mathbf{e}$ and public values.

Remark 2.2. The value I is calculated as

$$I = \mathrm{Mod}_q^{\frac{N}{2}} \left(\mathbf{f}_q(1) \cdot (\mathbf{a}(1) - \mathbf{p}(1) \cdot \mathbf{r}(1) \cdot \mathbf{g}(1))\right)$$

in [1, 6, 10]. This may seem different from what is done in step 1. Furthermore, in this form, knowledge of the secrete information $\mathbf{f}_q$ also seems to be required. But both are calculating the same value $\mathbf{m}(1)$, assuming that it is close to $\frac{N}{2}$.

3 Attack exploiting modulo q reduction

The chosen-ciphertext attacks on NTRU presented up to now ([2, 5, 7]) has focused on the *wrapping* behavior of the modulo q reduction process done during decryption. We apply this idea to the $\mathbf{p} = x+2$ case, but our method is different from previous methods in two aspects. First is that, in our method, the choice of ciphertext does not depend on previous queries to the decryption machine. The second point is that our attack is no longer a *reaction attack*. We do need to see the decrypted output of our chosen ciphertext.

The ciphertexts to be inserted in the decryption machine are determined for each public key through pre-computations. The number of queries to the decryption machine needed is less than twice the size of the coefficient set for $\mathbf{f}$. If the coefficient set for $\mathbf{f}$ is small, the number of queries needed could be much smaller. We shall determine $\mathbf{f}$ completely.

Remark 3.1. Reaction attacks still seem to be applicable to the un-padded *optimized* NTRU cryptosystem. No new idea is needed in doing this, but the process does become much more complicated. We shall not deal with it here.

3.1 The attack

We shall explain the chosen-ciphertext attack with a concrete example. Take the value $N = 251$ and $q = 128$ from Table 1 and assume that the coefficient set of $\mathbf{f}$ is $\{0, 1, 2\}$. Application of this method to bigger coefficient set will be straightforward. We propose to run the constant polynomial $\mathbf{e} = e$ (for some $0 \le e < q$) through the decryption machine. As stated by Remark 2.1, given $\mathbf{e}$ and a specific public key $\mathbf{h}$, anybody may find the value $\mathcal{A}$. Let us fix a public key $\mathbf{h}$ and write $\mathcal{A}(e)$ to denote the value $\mathcal{A}$ corresponding to the constant polynomial $\mathbf{e} = e$.

For the parameter values given in the $N = 251$ row of Table 1 we can calculate

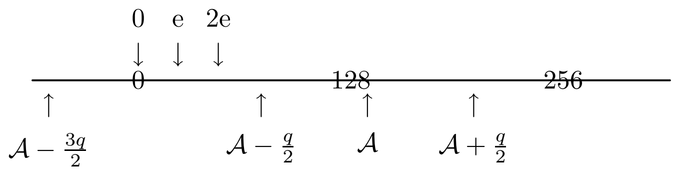
$$\begin{aligned}
&\mathbf{f}(1) = 1 + (1+2) \cdot \mathbf{F}(1) = 1 + 3 \cdot d_F = 217, \\
&\mathbf{f}_q(1) \equiv \mathbf{f}(1)^{-1} \equiv 105 \pmod{q}, \\
&\mathbf{r}(1) \cdot \mathbf{h}(1) \equiv d_r \cdot 3 \cdot \mathbf{f}_q(1) \cdot d_g \equiv 64 \pmod{q}.
\end{aligned}$$

With this, we can find the I and $\mathcal{A}$ values for various $\mathbf{e} = e$. Gather terms of the private key $\mathbf{f}$ according to their coefficients and write

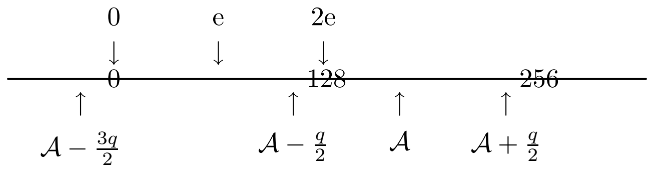
$$\mathbf{f} = 0 \cdot \mathbf{f}_0 + 1 \cdot \mathbf{f}_1 + 2 \cdot \mathbf{f}_2. \tag{5}$$

The coefficients of $\mathbf{f} * \mathbf{e}$ will belong to the set $\{0, e, 2e\}$. Below, we have drawn their position relative to $\mathcal{A}(e)$ for some chosen e values.

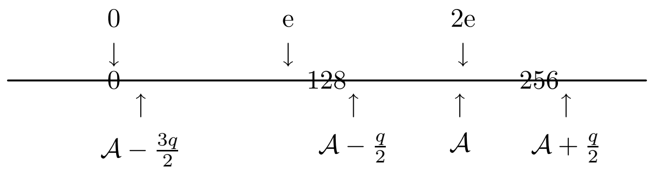
• $e = 24$, $\mathcal{A}(e) \fallingdotseq 138.04$


0
e
2e
0
128
256
$\mathcal{A} - \frac{3q}{2}$
$\mathcal{A} - \frac{q}{2}$
$\mathcal{A}$
$\mathcal{A} + \frac{q}{2}$

• $e = 63$, $\mathcal{A}(e) \fallingdotseq 171.76$


0
e
2e
0
128
256
$\mathcal{A} - \frac{3q}{2}$
$\mathcal{A} - \frac{q}{2}$
$\mathcal{A}$
$\mathcal{A} + \frac{q}{2}$

• $e = 105$, $\mathcal{A}(e) \fallingdotseq 208.07$


0
e
2e
0
128
256
$\mathcal{A} - \frac{3q}{2}$
$\mathcal{A} - \frac{q}{2}$
$\mathcal{A}$
$\mathcal{A} + \frac{q}{2}$

Let us fix $e = 63$ and follow through the decryption steps with the help of the above drawing.

$$\begin{aligned}
\mathbf{a}(e) &= \mathrm{Mod}_q^{\mathcal{A}(e)}(\mathbf{f} * \mathbf{e}) \\
&= \mathrm{Mod}_q^{\mathcal{A}(e)}(0 \cdot \mathbf{f}_0 + e \cdot \mathbf{f}_1 + 2e \cdot \mathbf{f}_2) \\
&= (0 + q) \cdot \mathbf{f}_0 + (e + q) \cdot \mathbf{f}_1 + 2e \cdot \mathbf{f}_2 \\
&= e \cdot \mathbf{f} + q \cdot (\mathbf{f}_0 + \mathbf{f}_1).
\end{aligned}$$

Let us do this once more with $e' = 105$.

$$\begin{aligned}
\mathbf{a}(e') &= \mathrm{Mod}_q^{\mathcal{A}(e')}(\mathbf{f} * \mathbf{e}') \\
&= \mathrm{Mod}_q^{\mathcal{A}(e')}(0 \cdot \mathbf{f}_0 + e' \cdot \mathbf{f}_1 + 2e' \cdot \mathbf{f}_2) \\
&= (0 + 2q) \cdot \mathbf{f}_0 + (e' + q) \cdot \mathbf{f}_1 + 2e' \cdot \mathbf{f}_2 \\
&= e' \cdot \mathbf{f} + q \cdot (2\mathbf{f}_0 + \mathbf{f}_1).
\end{aligned}$$

We may observe that the difference of the outputs from the decryption machine satisfies

$$\begin{aligned}
D(e, e') &:= \mathrm{Mod}_{\mathbf{p}}(\mathbf{a}(e)) - \mathrm{Mod}_{\mathbf{p}}(\mathbf{a}(e')) \\
&\equiv \mathbf{a}(e) - \mathbf{a}(e') \pmod{\mathbf{p}} \\
&= (e - e') \cdot \mathbf{f} - q \cdot \mathbf{f}_0 \\
&= (e - e') \cdot (1 + \mathbf{p} \cdot \mathbf{F}) - q \cdot \mathbf{f}_0 \\
&\equiv (e - e') - q \cdot \mathbf{f}_0 \pmod{\mathbf{p}}.
\end{aligned}$$

Denote the modulo $\mathbf{p}$ inverse of q by $q_{\mathbf{p}}$ so that $q_{\mathbf{p}} \cdot q \equiv 1 \pmod{\mathbf{p}}$. We may now obtain

$$\mathrm{Mod}_{\mathbf{p}}\big(-q_{\mathbf{p}} \cdot \big(D(e,e') - (e-e')\big)\big) = \mathrm{Mod}_{\mathbf{p}}\big(q_{\mathbf{p}} \cdot q \cdot \mathbf{f}_0\big) = \mathrm{Mod}_{\mathbf{p}}(\mathbf{f}_0) = \mathbf{f}_0.$$

We stress that all three equalities above are true equalities in the ring $\mathcal{R}$. They are stronger than just modulo $\mathbf{p}$ equivalence relations. The last equality follows since $\mathbf{f}_0$ is a binary polynomial. We have found all terms of $\mathbf{f}$ having coefficients equal to 0 with just two queries to the decryption machine.

The above argument obtained $\mathbf{f}_0$ because the value 0 crossed over the value $\mathcal{A} - \frac{3q}{2}$ as we changed e to e' and since neither e nor $2e$ went over any $\mathrm{Mod}_q^{\mathcal{A}}$ operation boundary. If we work with $e = 24$ and $e' = 63$, we can similarly obtain $\mathbf{f}_2$. The remaining terms will now have coefficient equal to 1 and we have found the private key $\mathbf{f}$ with just three queries to the decryption machine.

Remark 3.2. In the above calculations, we've used the fact $\mathbf{f} \equiv 1 \pmod{\mathbf{p}}$. Hence this attack is not applicable to the original NTRU cryptosystem.

3.2 Feasibility of attack

We shall use the notation

$$\mathrm{dc}(n, \mathcal{A}) = \frac{1}{q}(n - \mathrm{Mod}_q^{\mathcal{A}}(n)) \tag{6}$$

for any integer n and centering value $\mathcal{A}$. An equivalent definition would be

$$\mathrm{Mod}_q^{\mathcal{A}}(n) = n - q \cdot \mathrm{dc}(n, \mathcal{A}).$$

It measures how far n is from the *representative interval.* When the value $\mathcal{A}$ is clear from context, $\mathrm{dc}(n)$ will be used.

Let the coefficient set of $\mathbf{f}$ be $\{0, 1, \ldots, t\}$. To argue that the previous section is a meaningful attack on un-padded version of optimized NTRU, it remains to consider how likely it is to find an (e, e') pair with $\mathrm{dc}(i \cdot e, \mathcal{A}(i \cdot e))$ and $\mathrm{dc}(i \cdot e', \mathcal{A}(i \cdot e'))$ differing at just one $0 \leq i \leq t$. We have no proof that enough such pairs may always be found, but will give an informal argument showing that this is highly possible. Also, a complete solution for the $N = 251$ case is provided in the Appendices as an example.

Examine what happens to the dc-values when we increase e by just 1. If we study the procedure for calculating $\mathcal{A}(e)$, we find that setting $e \leftarrow e + 1$ increases $\mathcal{A}(e)$, in most cases (exception occurs when I goes over the modulo q boundary), by $\frac{\mathbf{f}(1)}{N}$. For the parameter values given in Table 1, this value is roughly 0.86 ($N = 251$), 0.56 ($N = 347$), and 2.51 ($N = 503$) for each case. Of course, setting $e \leftarrow e + 1$ increase $i \cdot e$ by the amount i. We want to point out that not all $t + 1$ of these values i can be close to $\frac{\mathbf{f}(1)}{N}$ at the same time.

The second point we want to make is that, as we change e from 0 to $q - 1$, the values $i \cdot e$ all start as being equal to 0 and end up spreading out over an interval of length $t \cdot q$. So the $t + 1$ dc-values will start out as the same and end up as different.

These two points convince us that not all of the dc-values can stay constant over the change of e from 0 to $q-1$.

Finally, we want to call to attention one more point. Since the distance between $i \cdot e$ and $(i+1) \cdot e$ is less than q, if e is big enough, it is almost impossible (again, the same exception apply) for two adjacent dc-values to change simultaneously, as we increase e by 1. Non-adjacent dc-values have a better chance of changing simultaneously, but since they have to be apart by a multiple of q for this to happen, this is not too frequent.

If this does not convince the reader, we can just roughly say that we have about q equations in hand to solve for $t+1$ variables.

For the case $N = 251$, we have given a table of dc-values in Appendix A. As we have already seen, for the parameter values given in the first row of Table 1, we have $\mathbf{r}(1)\mathbf{h}(1) = 64$. Notice that the maximum possible value for the coefficient of $\mathbf{f}$, in either the binary-$\mathbf{F}$ or the LHW-$\mathbf{F}$ case, is $28 = 3 \cdot (8+1)+1$. So, for each $e = 0, 1, \ldots, q-1$, we've listed the values $\mathrm{dc}(i \cdot e, \mathcal{A}(i \cdot e))$ for $i = 0, 1, \ldots, 28$.

In Appendix B, we used these values to give an explicit instruction for determining the private key $\mathbf{f}$ completely with 52 queries to the decryption machine. In practice, we do not expect $\mathbf{f}$ to contain coefficients as large as 28. So the process would be a lot shorter.

If the coefficient set of $\mathbf{f}$ is just $\{0, 1, 2, 3\}$, which is highly probable in the binary-$\mathbf{F}$ case, Appendix C explains how one could obtain $\mathbf{f}$ completely with just one or two queries to the decryption machine.

4 Attack using $\mathbf{p}_q$

In this section, we assume the private key is given by a binary-$\mathbf{F}$. We present a chosen-ciphertext attack which makes one query to the decryption machine and recovers the private key completely. Remarks on implications of this method on the LHW-$\mathbf{F}$ case is given at the end of this section.

Let us denote the modulo q inverse of $\mathbf{p}$ by $\mathbf{p}_q$, so that

$$\mathbf{p}_q * \mathbf{p} \equiv 1 \pmod{q}.$$

If $q = 2^k$, we may specifically set

$$\mathbf{p}_q = \sum_{i=1}^{k} (-2)^{i-1} x^{N-i} \pmod{q}. \tag{7}$$

4.1 Simple case

If we insert $\mathbf{p}_q$ into the decryption machine, it will calculate

$$\begin{aligned}\mathbf{a} &= \mathrm{Mod}_q^{\mathcal{A}(\mathbf{p}_q)}(\mathbf{f} * \mathbf{p}_q) \\ &= \mathrm{Mod}_q^{\mathcal{A}}\left((1 + \mathbf{p} * \mathbf{F}) * \mathbf{p}_q\right) \\ &= \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q + \mathbf{F}).\end{aligned}$$

Since all the coefficients of $\mathbf{F}$ are either 0 or 1, with high probability, we will have

$$\mathbf{a} = \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q) + \mathbf{F}. \tag{8}$$

Assume for the moment that this is true. Then, we have

$$\mathrm{Mod}_{\mathbf{p}}(\mathbf{a}) - \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q) \equiv \mathbf{a} - \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q) \equiv \mathbf{F} \pmod{\mathbf{p}}.$$

Notice that the first term on the left is the output of the decryption machine, and that the second term on the left may readily be computed. Hence we may obtain

$$\mathrm{Mod}_{\mathbf{p}}\left(\mathrm{Mod}_{\mathbf{p}}(\mathbf{a}) - \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q)\right) = \mathrm{Mod}_{\mathbf{p}}(\mathbf{F}) = \mathbf{F}.$$

The second equality holds, since $\mathbf{F}$ is a binary polynomial. We have obtained the private key $\mathbf{f} = 1 + \mathbf{p} * \mathbf{F}$ with just one query.

Remark 4.1. This attack obviously relies on the form of the private key $\mathbf{f} = 1 + \mathbf{p} * \mathbf{F}$. Hence this attack may not be applied to the original NTRU scheme.

It remains to justify equation (8). For parameters given in Table 1, we have calculated various values.

N	$\mathbf{f}(1)$	$\mathbf{f}_q(1)$	$\mathbf{r}(1)\mathbf{h}(1)$	$\mathbf{p}_q(1)$	$I(\mathbf{p}_q)$	$\mathcal{A}(\mathbf{p}_q)$
251	217	105	64	43	107	154.47
347	193	65	64	43	235	226.43
503	1261	229	242	171	185	718.28

Some of these values are defined only up to modulo q. Now, using equation (7) and this table, we list all coefficients (including the one corresponding to zero) of $\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q)$ in the following table. We've also written down the lower and upper boundaries (LB,UB) of the *representative interval.* Last column contains the distance between UB and the coefficient maximum.

N	LB	coefficients	UB	headroom
251	91	129, 126, 132, 120, 144, 96, 192, 128	218	26
347	163	257, 254, 260, 248, 272, 224, 192, 256	290	18
503	591	769, 766, 772, 760, 784, 736, 832, 640, 768	846	14

So at least, for the parameter values given in Table 1, equation (8) is always satisfied.

4.2 Wrapping case

Assumption of the previous subsection, namely, equation (8), fails if and only if

1. some coefficient c of $\mathrm{Mod}_q^{\mathcal{A}(\mathbf{p}_q)}(\mathbf{p}_q)$ satisfies $c \leq \mathcal{A}(\mathbf{p}_q) + \frac{q}{2} < c + 1$,
2. and the corresponding coefficient of $\mathbf{F}$ is equal to 1.

Since we know the exact polynomial $\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q)$, we know which coefficients satisfy the first of the above conditions. Suppose some coefficient c_i of the

x^i term in $\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q)$ satisfies both conditions. Suppose further that such a coefficient is unique. Then

$$\begin{aligned}\mathbf{a} &= \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q + \mathbf{F}) \\ &= \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q) - qx^i + \mathbf{F}.\end{aligned}$$

And the output of the decryption machine satisfies

$$\mathrm{Mod}_{\mathbf{p}}(\mathbf{a}) \equiv \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q) - qx^i + \mathbf{F} \pmod{\mathbf{p}}.$$

As before, we may obtain the private key by computing

$$\mathrm{Mod}_{\mathbf{p}}\left(\mathrm{Mod}_{\mathbf{p}}(\mathbf{a}) - \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{p}_q) + qx^i\right) = \mathrm{Mod}_{\mathbf{p}}(\mathbf{F}) = \mathbf{F}.$$

In conclusion, if $\mathbf{p}_q$ contains t-many coefficients satisfying the above condition 1, with just one query to the decryption machine, we may find 2^t candidates for $\mathbf{F}$, one of which corresponds to the true private key $\mathbf{f} = 1 + \mathbf{p} * \mathbf{F}$.

Remark 4.2. If $q = 2^k$, we know from equation (7) that all of the coefficients of $\mathbf{p}_q$ are distinct modulo q. (Read next remark to see why this isn't strictly true.) Hence there can be at most one coefficient satisfying the first of the above two conditions.

Remark 4.3. In the $q = 2^k$ case, if it happens that some coefficient $c \equiv 0 \pmod{q}$ satisfies the first condition, application of this method is not feasible. But with some modifications we could use $-\mathbf{p}_q$ or even $2\mathbf{p}_q$ in a similar attack.

4.3 LHW-F with small coefficients

We consider application of the above method to LHW-$\mathbf{F}$ case. The attack on this case is not as strong as the above, but is still meaningful.

Suppose that the coefficients of $\mathbf{F}$ belong to the set $\{0, 1, \ldots, \ell\}$. For the parameter values given in Table 1 and LHW-$\mathbf{F}$, we may take ℓ to be $\min(d_{F_1}, d_{F_2}) + 1 = 9, 8, 21$ for N equal to 251, 347, 503, respectively. Then we should start by checking for coefficients c of $\mathrm{Mod}_q^{\mathcal{A}(\mathbf{p}_q)}(\mathbf{p}_q)$ satisfying

$$c \leq \mathcal{A}(\mathbf{p}_q) + \frac{q}{2} < c + \ell.$$

For the case $q = 2^k$, we've seen that the coefficients of $\mathbf{p}_q$ are relatively far apart from each other, so that for small ℓ, the number of such coefficients will be small. Actually, referring to the *headroom* column of the above table, we see that this is wholly impossible for the $N = 251$ case $(9 \leq 26)$ and $N = 347$ case $(8 \leq 28)$. For $N = 503$ case, we only need to worry about the possibility of $\mathbf{F}$ coefficient corresponding to the $832 \cdot x^{N-7}$ term of $\mathbf{p}_q$ being greater than 14. This should be rare enough.

In any case, we can obtain a small number of candidates for $\mathrm{Mod}_{\mathbf{p}}(\mathbf{F})$, one of which is a correct value. We have not obtained the private key itself, but know $\mathbf{F}$ up to modulo $\mathbf{p}$.

We shall now restrict to the case $N = 251$ with LHW-$\mathbf{F}$. We have

$$\mathbf{F} = \mathbf{F}_1 * \mathbf{F}_2 + \mathbf{F}_3 \tag{9}$$

with each $\mathbf{F}_i$ having $d_{F_i} = 8$ coefficients equal to 1. We shall provide two lines of thought for this case.

The first is somewhat artificial. For LHW-$\mathbf{F}$, there is a non-dismissible possibility of it satisfying the following two conditions.

1. The coefficients of $\mathbf{F}$ belong to the set $\{0, 1, 2\}$.
2. If the term $2x^i$ appears in $\mathbf{F}$, the x^{i+1} and x^{i+2} terms are zero.

We shall continue under this assumption. It is clear that

$$2 \cdot x^i + 0 \cdot x^{i+1} + 0 \cdot x^{i+2} \equiv 0 \cdot x^i + x^{i+1} + x^{x+2} \pmod{\mathbf{p}}.$$

Hence for every occurrence of consecutive coefficients $(0, 1, 1)$ in $\mathrm{Mod}_{\mathbf{p}}(\mathbf{F})$, the corresponding coefficients of $\mathbf{F}$ could either have been $(0, 1, 1)$ or $(2, 0, 0)$. It is clear that these two cases cover the whole possibility. So if there are t occurrence of $(0, 1, 1)$ in $\mathbf{F}$, we obtain 2^t candidates for $\mathbf{F}$, one of which is the true value under the above two assumptions. The number t will usually be small. Of course, we could relax the two condition and find a bigger set of candidates which would contain $\mathbf{F}$ with a higher probability.

The second idea is to do an (almost) exhaustive search. The number of $\mathbf{F}$ of the form (9) is about

$$N \cdot ({}_N C_7)^2 \cdot {}_N C_8.$$

But now, we may just run $\mathbf{F}_1$ and $\mathbf{F}_2$ through all possible binary polynomials with $d_{F_1} = d_{F_2} = 8$ nonzero terms, and use the $\mathrm{Mod}_{\mathbf{p}}(\mathbf{F})$ value to find the uniquely corresponding $\mathbf{F}_3$. Probability of the obtained $\mathbf{F}_3$ having $d_{F_1} = 8$ coefficients equal to 1 is about $\mathbf{p}(1)/N$ and this reduces the size of key space to just

$$N \cdot ({}_N C_7)^2 \cdot \frac{\mathbf{p}(1)}{N} = 3 \cdot ({}_N C_7)^2.$$

While this is not a feasible attack, it is still a huge improvement over an exhaustive search.

5 Attack using the public key h

This section contains the simplest, and perhaps, the strongest of our attacks on un-padded NTRU. Using just one query to the decryption machine, we shall obtain completely, the binary polynomial $\mathbf{g}$ used in defining the public key, with probability $(q-1)/q$. Since the public key is given by $\mathbf{h} = \mathbf{p} * \mathbf{f}_q * \mathbf{g}$, this is (almost) equivalent to having obtained the private key $\mathbf{f}$.

As before, let $\mathbf{p}_q$ be the modulo q inverse of $\mathbf{p}$. We run $\mathbf{e} = \mathbf{p}_q * \mathbf{h}$ through the decryption machine. The output of the machine will be

$$\begin{aligned}\mathrm{Mod}_{\mathbf{p}} \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{f} * \mathbf{e}) &= \mathrm{Mod}_{\mathbf{p}} \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{f} * \mathbf{p}_q * \mathbf{p} * \mathbf{f}_q * \mathbf{g}) \\ &= \mathrm{Mod}_{\mathbf{p}} \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{g}).\end{aligned}$$

Recall the notation (6). With probability $(q-1)/q$, we can expect to have $\mathrm{dc}(0) = \mathrm{dc}(1)$. For the parameter values of Table 1, we may easily check that they are equal.

N	$I(\mathbf{p}_q * \mathbf{h})$	$\mathcal{A}(\mathbf{p}_q * \mathbf{h})$	LB	UB	dc(0)	dc(1)
251	72	124.21	61	188	-1	-1
347	173	191.95	128	255	-1	-1
503	149	628.03	501	756	-2	-2

Assume $\mathrm{dc}(0) = \mathrm{dc}(1)$ and let d denote the common value. Set

$$S(x) = 1 + x + \cdots + x^{N-1}.$$

Then, we may write

$$\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{g}) = \mathbf{g} - d \cdot q \cdot S(x).$$

Hence

$$\mathrm{Mod}_{\mathbf{p}}\left(\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{f} * \mathbf{e})\right) + d \cdot q \cdot S(x) \equiv \mathrm{Mod}_q^{\mathcal{A}}(\mathbf{g}) + d \cdot q \cdot S(x) \equiv \mathbf{g} \pmod{\mathbf{p}}$$

and we may obtain

$$\mathrm{Mod}_{\mathbf{p}}\Big(\mathrm{Mod}_{\mathbf{p}}\left(\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{f} * \mathbf{e})\right) + d \cdot q \cdot S(x)\Big) = \mathbf{g}$$

from just one query to the decryption machine. The value

$$\mathbf{f} * \mathbf{h} \equiv \mathbf{f} * \mathbf{p} * \mathbf{f}_q * \mathbf{g} \equiv \mathbf{p} * \mathbf{g} \pmod{q}$$

is in our hands. Now, if $\mathbf{h}$ is invertible modulo q, or equivalently, if $\mathbf{g}$ is invertible module q, we can obtain $\mathbf{f}$ modulo q. We know the form of $\mathbf{f}$, so can find $\mathbf{f}$ exactly. Furthermore, the random binary polynomial $\mathbf{g}$ is invertible with a very high probability. Even if it is not, we still have the possibility of using a pseudo inverse of $\mathbf{h}$ to obtain $\mathbf{f}$.

Remark 5.1. Attack presented in this section cannot be applied to the original NTRU scheme. Fundamentally, this attack is only possible because we have chosen $\mathbf{f}$ to satisfy $\mathbf{f}_{\mathbf{p}} = 1$

Remark 5.2. In the case $\mathrm{dc}(0) \neq \mathrm{dc}(1)$, we may use $-\mathbf{p}_q * \mathbf{h}$ in a similar attack. Again, we have about $1/q$ chance of encountering the same problem.

Remark 5.3. Suppose $\mathrm{dc}(0) \neq \mathrm{dc}(1)$, or equivalently, $\mathrm{dc}(0) + 1 = \mathrm{dc}(1)$. We may write $\mathbf{g} = 0 \cdot \mathbf{g}_0 + 1 \cdot \mathbf{g}_1$ with $S(x) = \mathbf{g}_0 + \mathbf{g}_1$. Then

$$\begin{aligned}
&\mathrm{Mod}_{\mathbf{p}}\left(\mathrm{Mod}_q^{\mathcal{A}}(\mathbf{g})\right) + q \cdot \mathrm{dc}(0) \cdot S(x) \\
&\qquad \equiv \mathbf{g} - q \cdot \mathrm{dc}(0) \cdot \mathbf{g}_0 - q \cdot \mathrm{dc}(1) \cdot \mathbf{g}_1 + q \cdot \mathrm{dc}(0) \cdot (\mathbf{g}_0 + \mathbf{g}_1) \pmod{\mathbf{p}} \\
&\qquad = 0 \cdot \mathbf{g}_0 + (1 - q) \cdot \mathbf{g}_1 \\
&\qquad = (1 - q) \cdot (0 \cdot \mathbf{g}_0 + 1 \cdot \mathbf{g}_1) = (1 - q) \cdot \mathbf{g}.
\end{aligned}$$

Hence, if $1 - q$ is invertible modulo $\mathbf{p}$ in $\mathcal{R}$, we may find $\mathbf{g}$. This is true for the values $N = 251$ with $q = 128$ and $N = 347$ with $q = 128$.

6 Conclusion

We've seen three chosen-ciphertext attacks on the un-padded version of *optimized* NTRU cryptosystem. The first of these, given in Section 3, uses the *wrapping* idea of previous reaction attacks. Other two attacks presented here, given in Section 4 and Section 5, are new. Using practical values of various parameters, in many cases, we could obtain the private key with just one query to the decryption machine. Since chosen-ciphertext attacks are realistic in some situations, for example, with smart cards, optimized NTRU should never be used without padding.

All three attacks presented depend on the private key being of the form

$$\mathbf{f} = 1 + \mathbf{p} * \mathbf{F}.$$

None of these attacks are applicable to the original NTRU cryptosystem. So, while the choice of such a private key does make the NTRU cryptosystem more efficient, it also greatly weakens the system. This weakness fundamentally originates from having made the modulo $\mathbf{p}$ inverse of $\mathbf{f}$ equal to 1. Hence, without abandoning the central idea used in the *optimization*, the scheme itself cannot be re-strengthened to the previous level.

However, we believe any reasonable padding scheme will provide the optimized NTRU cryptosystem protection from our attacks. Of course, with explicit hash functions chosen to be used in the padding schemes, the story could be different. This part still remains to be considered.

References

[1] Consortium for Efficient Embedded Security, Efficient embedded security standards #1: Implementation aspects of NTRUEncrypt and NTRUSign. Draft version 5. Available from `http://www.ceesstandards.org`.

[2] Daewan Han, Jae Woo Han, Daesung Kwon, and Jin Hong, A new chosen ciphertext attack against NTRU. Submitted.

[3] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, NTRU: A ring-based public key cryptosystem. In *Proc. of ANTS III*, LNCS 1423. Springer-Verlag, 1998.

[4] Jeffrey Hoffstein and Joseph Silverman, Optimizations for NTRU. In *Public-Key Cryptogrphy and Computational Number Theory.* DeGruyter, 2002. Available from [9].

[5] Jeffrey Hoffstein and Joseph H. Silverman, Reaction attacks against the NTRU public key cryptosystem. Techinal report, NTRU Cryptosystems, Report #015. Available from [9]

[6] IEEE Standard P1363.1/D4, Standard specifications for public key cryptography : Techniques based on hard problems over lattices, IEEE. Available from `http://grouper.ieee.org/group/1363`.

[7] Éliane Jaulmes and Antoine Joux, A chosen-ciphertext attack against NTRU. *Advances in Cryptology - CRYPTO 2000*, LNCS 1880. Springer-Verlag, 2000.

[8] Phong Q. Nguyen and David Pointcheval, Analysis and improvements of NTRU encryption paddings. *Advances in Cryptology - CRYPTO 2002*, LNCS 2442. Springer-Verlag, 2002.

[9] NTRU Cryptosystems, Technical reports. Available from `http://www.ntru.com`.

[10] NTRU Cryptosystems, The NTRU public key cryptosystem - A tutorial. Available from `http://www.ntru.com`.

Appendix A

We have used $N = 251$, $q = 128$, and $d_F = d_g = d_r = 72$ in the following. We list $\mathcal{A}(i \cdot e)$ and values $\mathrm{dc}(i \cdot e, \mathcal{A}(i \cdot e))$ for each $i = 0, 1, \ldots, 28$ and $e = 0, 1, \ldots, q-1$.

```
 N = 251,  q = 128,  r(1)h(1) = 64

 e    A(e)   0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

 0, 117.29, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1
 1, 118.16, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1
 2, 119.02, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1  0
 3, 119.88, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0
 4, 120.75, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  0  0
 5, 121.61, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
 6, 122.48, -1 -1 -1 -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
 7, 123.34, -1 -1 -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  1  1
 8, 124.21, -1 -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  1  1  1  1  1
 9, 125.07, -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1
10, 125.94, -1 -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  1  1
11, 126.80, -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  1  1  1
12, 127.67, -1 -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  1  1  1  2  2
13, 128.53, -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  1  1  2  2  2  2
14, 129.39, -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  1  2  2  2  2  2  2
15, 130.26, -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  1  2  2  2  2  2  2  2
16, 131.12, -1 -1 -1 -1 -1  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  2  2  2  2  2  2  2  2
17, 131.99, -1 -1 -1 -1  0  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  2  2  2  2  2  2  2  3  3
18, 132.85, -1 -1 -1 -1  0  0  0  0  0  0  0  1  1  1  1  1  1  1  1  2  2  2  2  2  2  2  3  3  3
19, 133.72, -1 -1 -1 -1  0  0  0  0  0  0  0  1  1  1  1  1  1  1  2  2  2  2  2  2  3  3  3  3  3
20, 134.58, -1 -1 -1 -1  0  0  0  0  0  0  1  1  1  1  1  1  1  2  2  2  2  2  2  3  3  3  3  3  3
21, 135.45, -1 -1 -1 -1  0  0  0  0  0  0  1  1  1  1  1  1  2  2  2  2  2  2  3  3  3  3  3  3  4
22, 136.31, -1 -1 -1 -1  0  0  0  0  0  0  1  1  1  1  1  2  2  2  2  2  2  3  3  3  3  3  3  4  4
23, 137.18, -1 -1 -1 -1  0  0  0  0  0  1  1  1  1  1  1  2  2  2  2  2  3  3  3  3  3  3  4  4  4
24, 138.04, -1 -1 -1 -1  0  0  0  0  0  1  1  1  1  1  2  2  2  2  2  2  3  3  3  3  3  4  4  4  4
25, 138.90, -1 -1 -1  0  0  0  0  0  0  1  1  1  1  1  2  2  2  2  2  3  3  3  3  3  4  4  4  4  4
26, 139.77, -1 -1 -1  0  0  0  0  0  1  1  1  1  1  2  2  2  2  2  3  3  3  3  3  4  4  4  4  4  5
27, 140.63, -1 -1 -1  0  0  0  0  0  1  1  1  1  1  2  2  2  2  2  3  3  3  3  4  4  4  4  4  5  5
28, 141.50, -1 -1 -1  0  0  0  0  0  1  1  1  1  2  2  2  2  2  3  3  3  3  3  4  4  4  4  5  5  5
29, 142.36, -1 -1 -1  0  0  0  0  0  1  1  1  1  2  2  2  2  3  3  3  3  3  4  4  4  4  5  5  5  5
30, 143.23, -1 -1 -1  0  0  0  0  1  1  1  1  1  2  2  2  2  3  3  3  3  4  4  4  4  5  5  5  5  5
31, 144.09, -1 -1 -1  0  0  0  0  1  1  1  1  2  2  2  2  3  3  3  3  3  4  4  4  4  5  5  5  5  6
32, 144.96, -1 -1 -1  0  0  0  0  1  1  1  1  2  2  2  2  3  3  3  3  4  4  4  4  5  5  5  5  6  6
33, 145.82, -1 -1 -1  0  0  0  0  1  1  1  1  2  2  2  2  3  3  3  4  4  4  4  5  5  5  5  6  6  6
34, 146.69, -1 -1 -1  0  0  0  0  1  1  1  2  2  2  2  3  3  3  3  4  4  4  4  5  5  5  5  6  6  6
35, 147.55, -1 -1 -1  0  0  0  0  1  1  1  2  2  2  2  3  3  3  3  4  4  4  5  5  5  5  6  6  6  7
36, 148.41, -1 -1 -1  0  0  0  1  1  1  1  2  2  2  2  3  3  3  4  4  4  4  5  5  5  6  6  6  6  7
37, 149.28, -1 -1 -1  0  0  0  1  1  1  1  2  2  2  3  3  3  3  4  4  4  5  5  5  5  6  6  6  7  7
38, 150.14, -1 -1 -1  0  0  0  1  1  1  1  2  2  2  3  3  3  4  4  4  4  5  5  5  6  6  6  7  7  7
39, 151.01, -1 -1 -1  0  0  0  1  1  1  2  2  2  2  3  3  3  4  4  4  5  5  5  6  6  6  6  7  7  7
40, 151.87, -1 -1 -1  0  0  0  1  1  1  2  2  2  3  3  3  4  4  4  4  5  5  5  6  6  6  7  7  7  8
41, 152.74, -1 -1 -1  0  0  0  1  1  1  2  2  2  3  3  3  4  4  4  5  5  5  6  6  6  6  7  7  7  8
42, 153.60, -1 -1 -1  0  0  0  1  1  1  2  2  2  3  3  3  4  4  4  5  5  5  6  6  6  7  7  7  8  8
43, 154.47, -1 -1 -1  0  0  0  1  1  1  2  2  2  3  3  3  4  4  5  5  5  6  6  6  7  7  7  8  8  8
44, 155.33, -1 -1 -1  0  0  1  1  1  2  2  2  3  3  3  4  4  4  5  5  5  6  6  6  7  7  7  8  8  8
45, 156.20, -1 -1 -1  0  0  1  1  1  2  2  2  3  3  3  4  4  4  5  5  5  6  6  7  7  7  8  8  8  9
46, 157.06, -1 -1 -1  0  0  1  1  1  2  2  2  3  3  3  4  4  5  5  5  6  6  6  7  7  7  8  8  8  9
47, 157.92, -1 -1  0  0  0  1  1  1  2  2  2  3  3  4  4  4  5  5  5  6  6  6  7  7  8  8  8  9  9
48, 158.79, -1 -1  0  0  0  1  1  1  2  2  3  3  3  4  4  4  5  5  6  6  6  7  7  7  8  8  9  9  9
49, 159.65, -1 -1  0  0  0  1  1  1  2  2  3  3  3  4  4  4  5  5  6  6  6  7  7  8  8  8  9  9  9
50, 160.52, -1 -1  0  0  0  1  1  1  2  2  3  3  3  4  4  5  5  5  6  6  7  7  7  8  8  9  9  9 10
51, 161.38, -1 -1  0  0  0  1  1  2  2  2  3  3  4  4  4  5  5  6  6  6  7  7  8  8  8  9  9  9 10
52, 162.25, -1 -1  0  0  0  1  1  2  2  2  3  3  4  4  4  5  5  6  6  6  7  7  8  8  8  9  9 10 10
53, 163.11, -1 -1  0  0  0  1  1  2  2  2  3  3  4  4  5  5  5  6  6  7  7  7  8  8  9  9  9 10 10
54, 163.98, -1 -1  0  0  0  1  1  2  2  3  3  3  4  4  5  5  5  6  6  7  7  8  8  8  9  9 10 10 11
55, 164.84, -1 -1  0  0  0  1  1  2  2  3  3  3  4  4  5  5  6  6  6  7  7  8  8  9  9  9 10 10 11
56, 165.71, -1 -1  0  0  0  1  1  2  2  3  3  4  4  4  5  5  6  6  7  7  7  8  8  9  9 10 10 11 11
57, 166.57, -1 -1  0  0  0  1  1  2  2  3  3  4  4  4  5  5  6  6  7  7  8  8  8  9  9 10 10 11 11
58, 167.43, -1 -1  0  0  1  1  1  2  2  3  3  4  4  5  5  5  6  6  7  7  8  8  9  9 10 10 10 11 11
```

```
 59, 168.30, -1 -1  0  0  1  1  1  2  2  3  3  4  4  5  5  6  6  7  7  7  8  8  9  9 10 10 11 11 12
 60, 169.16, -1 -1  0  0  1  1  1  2  2  3  3  4  4  5  5  6  6  7  7  8  8  9  9  9 10 10 11 11 12
 61, 170.03, -1 -1  0  0  1  1  2  2  2  3  3  4  4  5  5  6  6  7  7  8  8  9  9 10 10 11 11 12 12
 62, 170.89, -1 -1  0  0  1  1  2  2  3  3  4  4  4  5  5  6  6  7  7  8  8  9  9 10 10 11 11 12 12
 63, 171.76, -1 -1  0  0  1  1  2  2  3  3  4  4  5  5  6  6  7  7  8  8  9  9  9 10 10 11 11 12 12
 64, 172.62, -1 -1  0  0  1  1  2  2  3  3  4  4  5  5  6  6  7  7  8  8  9  9 10 10 11 11 12 12 13
 65, 173.49, -1 -1  0  0  1  1  2  2  3  3  4  4  5  5  6  6  7  7  8  8  9  9 10 10 11 11 12 12 13
 66, 174.35, -1 -1  0  0  1  1  2  2  3  3  4  4  5  5  6  6  7  7  8  8  9  9 10 10 11 12 12 13 13
 67, 175.22, -1 -1  0  0  1  1  2  2  3  3  4  4  5  5  6  6  7  8  8  9  9 10 10 11 11 12 12 13 13
 68, 176.08, -1 -1  0  0  1  1  2  2  3  3  4  4  5  6  6  7  7  8  8  9  9 10 10 11 11 12 12 13 13
 69, 176.94, -1 -1  0  0  1  1  2  2  3  3  4  5  5  6  6  7  7  8  8  9  9 10 10 11 12 12 13 13 14
 70, 177.81, -1 -1  0  0  1  1  2  2  3  4  4  5  5  6  6  7  7  8  8  9 10 10 11 11 12 12 13 13 14
 71, 178.67, -1 -1  0  0  1  1  2  2  3  4  4  5  5  6  6  7  7  8  9  9 10 10 11 11 12 12 13 14 14
 72, 179.54, -1 -1  0  0  1  1  2  3  3  4  4  5  5  6  6  7  8  8  9  9 10 10 11 12 12 13 13 14 14
 73, 180.40, -1 -1  0  0  1  1  2  3  3  4  4  5  5  6  7  7  8  8  9  9 10 11 11 12 12 13 13 14 15
 74, 181.27, -1 -1  0  0  1  1  2  3  3  4  4  5  6  6  7  7  8  8  9 10 10 11 11 12 12 13 14 14 15
 75, 182.13, -1 -1  0  0  1  2  2  3  3  4  4  5  6  6  7  7  8  9  9 10 10 11 11 12 13 13 14 14 15
 76, 183.00, -1 -1  0  0  1  2  2  3  3  4  5  5  6  6  7  7  8  9  9 10 10 11 12 12 13 13 14 15 15
 77, 183.86, -1 -1  0  0  1  2  2  3  3  4  5  5  6  6  7  8  8  9  9 10 11 11 12 12 13 14 14 15 15
 78, 184.73, -1 -1  0  0  1  2  2  3  3  4  5  5  6  6  7  8  8  9 10 10 11 11 12 13 13 14 14 15 16
 79, 185.59, -1 -1  0  0  1  2  2  3  3  4  5  5  6  7  7  8  8  9 10 10 11 12 12 13 13 14 15 15 16
 80, 186.45, -1 -1  0  0  1  2  2  3  4  4  5  5  6  7  7  8  9  9 10 10 11 12 12 13 14 14 15 15 16
 81, 187.32, -1 -1  0  0  1  2  2  3  4  4  5  5  6  7  7  8  9  9 10 11 11 12 12 13 14 14 15 16 16
 82, 188.18, -1 -1  0  0  1  2  2  3  4  4  5  6  6  7  7  8  9  9 10 11 11 12 13 13 14 15 15 16 16
 83, 189.05, -1 -1  0  0  1  2  2  3  4  4  5  6  6  7  8  8  9 10 10 11 11 12 13 13 14 15 15 16 17
 84, 189.91, -1 -1  0  0  1  2  2  3  4  4  5  6  6  7  8  8  9 10 10 11 12 12 13 14 14 15 16 16 17
 85, 190.78, -1 -1  0  1  1  2  2  3  4  4  5  6  6  7  8  8  9 10 10 11 12 12 13 14 14 15 16 16 17
 86, 191.64, -1 -1  0  1  1  2  3  3  4  5  5  6  7  7  8  9  9 10 11 11 12 13 13 14 15 15 16 17 17
 87, 192.51, -2 -1  0  1  1  2  3  3  4  5  5  6  7  7  8  9  9 10 11 11 12 13 13 14 15 15 16 17 18
 88, 193.37, -2 -1  0  1  1  2  3  3  4  5  5  6  7  7  8  9  9 10 11 12 12 13 14 14 15 16 16 17 18
 89, 194.24, -2 -1  0  1  1  2  3  3  4  5  5  6  7  8  8  9 10 10 11 12 12 13 14 14 15 16 17 17 18
 90, 195.10, -2 -1  0  1  1  2  3  3  4  5  6  6  7  8  8  9 10 10 11 12 13 13 14 15 15 16 17 17 18
 91, 195.96, -2 -1  0  1  1  2  3  3  4  5  6  6  7  8  8  9 10 11 11 12 13 13 14 15 16 16 17 18 18
 92, 196.83, -2 -1  0  1  1  2  3  3  4  5  6  6  7  8  9  9 10 11 11 12 13 14 14 15 16 16 17 18 19
 93, 197.69, -2 -1  0  1  1  2  3  4  4  5  6  6  7  8  9  9 10 11 12 12 13 14 14 15 16 17 17 18 19
 94, 198.56, -2 -1  0  1  1  2  3  4  4  5  6  7  7  8  9  9 10 11 12 12 13 14 15 15 16 17 18 18 19
 95, 199.42, -2 -1  0  1  1  2  3  4  4  5  6  7  7  8  9 10 10 11 12 13 13 14 15 16 16 17 18 18 19
 96, 200.29, -2 -1  0  1  1  2  3  4  4  5  6  7  7  8  9 10 10 11 12 13 13 14 15 16 16 17 18 19 19
 97, 201.15, -2 -1  0  1  1  2  3  4  4  5  6  7  8  8  9 10 11 11 12 13 14 14 15 16 17 17 18 19 20
 98, 202.02, -2 -1  0  1  1  2  3  4  5  5  6  7  8  8  9 10 11 11 12 13 14 14 15 16 17 18 18 19 20
 99, 202.88, -2 -1  0  1  2  2  3  4  5  5  6  7  8  8  9 10 11 12 12 13 14 15 15 16 17 18 19 19 20
100, 203.75, -2 -1  0  1  2  2  3  4  5  5  6  7  8  9  9 10 11 12 12 13 14 15 16 16 17 18 19 20 20
101, 204.61, -2 -1  0  1  2  2  3  4  5  6  6  7  8  9  9 10 11 12 13 13 14 15 16 17 17 18 19 20 20
102, 205.47, -2 -1  0  1  2  2  3  4  5  6  6  7  8  9 10 10 11 12 13 14 14 15 16 17 18 18 19 20 21
103, 206.34, -2 -1  0  1  2  2  3  4  5  6  6  7  8  9 10 10 11 12 13 14 14 15 16 17 18 19 19 20 21
104, 207.20, -2 -1  0  1  2  2  3  4  5  6  7  7  8  9 10 11 11 12 13 14 15 15 16 17 18 19 20 20 21
105, 208.07, -2 -1  0  1  2  2  3  4  5  6  7  7  8  9 10 11 11 12 13 14 15 16 16 17 18 19 20 21 21
106, 208.93, -2 -1  0  1  2  3  3  4  5  6  7  7  8  9 10 11 12 12 13 14 15 16 17 17 18 19 20 21 22
107, 209.80, -2 -1  0  1  2  3  3  4  5  6  7  8  8  9 10 11 12 13 13 14 15 16 17 18 18 19 20 21 22
108, 210.66, -2 -1  0  1  2  3  3  4  5  6  7  8  8  9 10 11 12 13 14 14 15 16 17 18 19 19 20 21 22
109, 211.53, -2 -1  0  1  2  3  3  4  5  6  7  8  9  9 10 11 12 13 14 15 15 16 17 18 19 20 20 21 22
110, 212.39, -2 -1  0  1  2  3  3  4  5  6  7  8  9 10 10 11 12 13 14 15 16 16 17 18 19 20 21 22 22
111, 213.25, -2 -1  0  1  2  3  4  4  5  6  7  8  9 10 10 11 12 13 14 15 16 17 17 18 19 20 21 22 23
112, 214.12, -2 -1  0  1  2  3  4  4  5  6  7  8  9 10 11 11 12 13 14 15 16 17 18 18 19 20 21 22 23
113, 214.98, -2 -1  0  1  2  3  4  5  5  6  7  8  9 10 11 12 12 13 14 15 16 17 18 19 20 20 21 22 23
114, 215.85, -2 -1  0  1  2  3  4  5  5  6  7  8  9 10 11 12 13 13 14 15 16 17 18 19 20 21 21 22 23
115, 216.71, -2 -1  0  1  2  3  4  5  5  6  7  8  9 10 11 12 13 14 14 15 16 17 18 19 20 21 22 23 23
116, 217.58, -2 -1  0  1  2  3  4  5  6  6  7  8  9 10 11 12 13 14 15 16 16 17 18 19 20 21 22 23 24
117, 218.44, -2 -1  0  1  2  3  4  5  6  7  7  8  9 10 11 12 13 14 15 16 17 17 18 19 20 21 22 23 24
118, 219.31, -2 -1  0  1  2  3  4  5  6  7  8  8  9 10 11 12 13 14 15 16 17 18 19 19 20 21 22 23 24
119, 220.17, -2 -1  0  1  2  3  4  5  6  7  8  9  9 10 11 12 13 14 15 16 17 18 19 20 21 22 22 23 24
120, 221.04, -2 -1  0  1  2  3  4  5  6  7  8  9 10 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
121, 221.90, -2 -1  0  1  2  3  4  5  6  7  8  9 10 11 12 12 13 14 15 16 17 18 19 20 21 22 23 24 25
122, 222.76, -2 -1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 14 15 16 17 18 19 20 21 22 23 24 25
123, 223.63, -2 -1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 17 18 19 20 21 22 23 24 25
124, 224.49, -2 -1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 21 22 23 24 25
125, 225.36, -2 -1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
126, 115.56, -1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
127, 116.43, -1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
```

Appendix B

For the parameters given by the $N = 251$ row of Table 1, we give an explicit set of instructions for determining the private key $\mathbf{f}$ assuming that it is given by a LHW-$\mathbf{F}$. The first column contains the e values. Applying methods of Section 3 with e and $e' = e + 1$, we can obtain the term or sum of terms given in the third column. Using this together with information already obtained in higher rows, the term given in the last column is obtained. This is constructed from information given in Appendix A.

e	e'		
1	2	$\mathbf{f}_{28}$	$\mathbf{f}_{28}$
15	16	$\mathbf{f}_{21}$	$\mathbf{f}_{21}$
48	49	$\mathbf{f}_{23}$	$\mathbf{f}_{23}$
51	52	$\mathbf{f}_{27}$	$\mathbf{f}_{27}$
56	57	$\mathbf{f}_{20}$	$\mathbf{f}_{20}$
84	85	$\mathbf{f}_{3}$	$\mathbf{f}_{3}$
102	103	$\mathbf{f}_{25}$	$\mathbf{f}_{25}$
23	24	$\mathbf{f}_{14} + \mathbf{f}_{25}$	$\mathbf{f}_{14}$
26	27	$\mathbf{f}_{22} + \mathbf{f}_{27}$	$\mathbf{f}_{22}$
33	34	$\mathbf{f}_{10} + \mathbf{f}_{14}$	$\mathbf{f}_{10}$
40	41	$\mathbf{f}_{18} + \mathbf{f}_{21}$	$\mathbf{f}_{18}$
41	42	$\mathbf{f}_{24} + \mathbf{f}_{27}$	$\mathbf{f}_{24}$
54	55	$\mathbf{f}_{16} + \mathbf{f}_{23}$	$\mathbf{f}_{16}$
59	60	$\mathbf{f}_{19} + \mathbf{f}_{21}$	$\mathbf{f}_{19}$
61	62	$\mathbf{f}_{8} + \mathbf{f}_{10}$	$\mathbf{f}_{8}$
86	87	$\mathbf{f}_{0} + \mathbf{f}_{28}$	$\mathbf{f}_{0}$
116	117	$\mathbf{f}_{9} + \mathbf{f}_{20}$	$\mathbf{f}_{9}$
120	121	$\mathbf{f}_{13} + \mathbf{f}_{14}$	$\mathbf{f}_{13}$
121	122	$\mathbf{f}_{15} + \mathbf{f}_{16}$	$\mathbf{f}_{15}$
5	6	$\mathbf{f}_{10} + \mathbf{f}_{11}$	$\mathbf{f}_{10}$
10	11	$\mathbf{f}_{6} + \mathbf{f}_{18}$	$\mathbf{f}_{6}$
17	18	$\mathbf{f}_{11} + \mathbf{f}_{19} + \mathbf{f}_{26}$	$\mathbf{f}_{26}$
19	20	$\mathbf{f}_{10} + \mathbf{f}_{17} + \mathbf{f}_{23}$	$\mathbf{f}_{17}$
4	5	$\mathbf{f}_{12} + \mathbf{f}_{13} + \mathbf{f}_{14}$	$\mathbf{f}_{12}$
8	9	$\mathbf{f}_{7} + \mathbf{f}_{22} + \mathbf{f}_{23}$	$\mathbf{f}_{7}$
74	75	$\mathbf{f}_{5} + \mathbf{f}_{17} + \mathbf{f}_{24}$	$\mathbf{f}_{5}$
57	58	$\mathbf{f}_{4} + \mathbf{f}_{13} + \mathbf{f}_{22} + \mathbf{f}_{24}$	$\mathbf{f}_{4}$
46	47	$\mathbf{f}_{2} + \mathbf{f}_{13} + \mathbf{f}_{24} + \mathbf{f}_{27}$	$\mathbf{f}_{2}$

The reader can check that the only term not appearing in the last column is $\mathbf{f}_1$. It may readily be set to all remaining terms.

Careful counting will show that 52 queries were needed to determine $\mathbf{f}$ completely. Since we've been very lazy in making this table, there would be ways to reduce this number.

Appendix C

Content of this section may not qualify as an attack on NTRU, but contains information which could be useful when used together with some form of attack.

We assume that the private key (1), is given by a binary-$\mathbf{F}$ and that the constant term of $\mathbf{f}$ is not 4, so that the coefficient set of $\mathbf{f}$ is $\{0, 1, 2, 3\}$.

Let us denote by $(f_0, f_1, \ldots, f_{N-1})$, the coefficients of $\mathbf{f}$. Likewise, the coefficients of $\mathbf{F}$ will be denoted with $(F_0, \ldots, F_{N-1})$. Notice

$$f_i = 2 \cdot F_i + F_{i-1}$$

for all $i \neq 0$. So the parity (E/O) of f_i determines F_{i-1} completely. Similarly, knowing whether f_i belongs to the set $L = \{0, 1\}$ or $H = \{2, 3\}$ determines F_i completely. Once more, if f_i belongs to $I = \{1, 2\}$, then $F_i = 1 - F_{i-1}$ and if f_i belongs to $B = \{0, 3\}$, then $F_i = F_{i-1}$.

We may use this argument as follows. Suppose we know that $\mathbf{f}$ is of the form

$$\mathbf{f} = (?, L, H, H, H, L, L, H, L, H, \ldots).$$

Then we must have

$$\mathbf{F} = (?, 0, 1, 1, 1, 0, 0, 1, 0, 1, \ldots)$$

and hence

$$\mathbf{f} = (?, ?, 2, 3, 3, 1, 0, 2, 1, 2, \ldots)$$

We may conclude that, even though the coefficient set of $\mathbf{f}$ is of size 4, knowing one bit of information for each f_i $(i \neq 0)$, in the form of E/O, L/H, or I/B, is enough to determine $\mathbf{f}$ almost completely.

This may not have any impact on the security of NTRU cryptosystem by itself, but may be useful when combined with other methods of attacks. For example, for the $N = 251$ case, still assuming that the coefficients of $\mathbf{f}$ belong to the set $\{0, 1, 2, 3\}$, using Appendix A, we see that

$$\mathbf{a}(70) = 70 \cdot \mathbf{f} + q(\mathbf{f}_0 + \mathbf{f}_1),$$

in the notation of Section 3. Hence, with just one query to the decryption machine, we can obtain

$$\mathrm{Mod}_{\mathbf{p}}\left(q_{\mathbf{p}}\big(\mathrm{Mod}_{\mathbf{p}}(\mathbf{a}(70)) - 70\big)\right) = \mathbf{f}_0 + \mathbf{f}_1.$$

This determines whether each f_i belongs to L or H, so determines $\mathbf{f}$ almost completely.

If we are not so lucky as to find such an e, we could use the difference of two queries to the decryption machine in a similar attack.