A Key Recovery Attack on Streamlined NTRU Prime

Chen Li

[1] School of Telecommunications Engineering, Xidian University
(lichen@xidian.edu.cn)
[2] Temasek Laboratory, National University of Singapore

Abstract. For years, researchers have been engaged in finding new cryptography schemes with high security and efficiency that can resist against the attacking from quantum computers. Lattice-based cryptography scheme is believed as a promising candidate. But to achieve both high efficiency and high security is not easy. Until recently, some Lattice-based schemes with enough efficiency have been proposed and submitted to the post-quantum cryptography standardization project that initiated by NIST. Streamlined NTRU Prime is one of them. Basing on a new"strong" ring and applying the "modern key encapsulation mechanism" approach, Streamlined NTRU Prime aims to provide IND-CCA security.

However, in this paper, we identify a simple property of the new "strong" ring. Using this property and also taking advantage of the information leakage from the decapsulation feedback, we provide an efficient key recovery attack on the Streamlined NTRU Prime. Our attack does not only break most instances of Streamlined NTRU Prime, but also shows an evidence that modifying a public key encryption scheme into a key encapsulation mechanism scheme does not naturally provide higher security.

Keywords: NTRU Prime, key encapsulation mechanism, IND-CCA security, post-quantum cryptography.

1 Introduction

NIST has kept an eye on Post-Quantum Cryptography (PQC) for many years. In 2016, the PQC standardization project was launched by NIST. The aim is to find new cryptography schemes with high security to resist against quantum computers and high efficiency for implementation in real world. By the end of 2017, there were 59 Public Key Encryption (PKE) or Key Encapsulation Mechanism (KEM) were submitted for the initial round submission and by April 2018, 45 schemes of them remained and were presented on the first NIST PQC standardization conference. Streamlined NTRU Prime scheme is one of them. Streamlined NTRU Prime – a KEM scheme – was firstly proposed in [1], then published in [2]. Streamlined NTRU Prime scheme has two features: (1) using a new ring structure; (2) using a modern "KEM+DEM" approach. The original NTRU [3] is based on the ring $(\mathbb{Z}/q)[x]/(x^p - 1)$, where p is a prime and q is a power of 2. Some recently proposed Ring-LWE-based scheme such as [4] is based on the ring $(\mathbb{Z}/q)[x]/(x^p + 1)$, where p is a power of 2 and $q \in 2p\mathbb{Z} + 1$ is a prime. As pointed in [2], these rings have small Galois group, and potentially suffer from attacks such as in[5] and [6]. Although these attacks may not straightly work on these special ring structure, using a stronger ring structure to remove the potential weakness is not a bad thing. The new ring used by Streamlined NTRU Prime is $(\mathbb{Z}/q)[x]/(x^p - x - 1)$, where p, q $(q > p)$ are two primes. This ring is of prime-degree, large-Galois-group and inert modulus, and is believed as a building block for designing efficient-implementation and high-security ideal-lattice-based cryptography.

It should be noted that Streamlined NTRU Prime is designed to achieve IND-CCA security [7]. However, known as a standard security notion for PKE, IND-CCA security is not easy to achieve efficiently. A general roadmap is to firstly design a PKE scheme, which is relatively weaker in security but high in efficiency, and then use a generic method to turn the weakly secure scheme into one with higher security, say IND-CCA security. Several methods have been proposed to turn a PKE scheme with weaker security into one with IND-CCA security. Fujisaki and Okamoto [8, 9] proposed a generic transformation – FO transformation – combining a One-Way secure asymmetric encryption scheme with a one-time secure symmetric encryption scheme into a hybrid encryption scheme which is proved with IND-CCA security under the random oracle model. However, FO transformation has been pointed out not tight in the security reduction, and consequently is believed that cannot provide an efficient and secure PKE scheme in practice. The KEM is another approach that may achieve IND-CCA security. It was firstly introduced by Shoup [10], and was originally used for padding RSA. Being generalized by Dent [11], KEM approach is generally regard as a " more modern" and "much nicer" approach to turn a weakly secure PKE scheme into an IND-CPA secure one. Due to the using of cryptographic hash function in KEM, any modification of the ciphertext will be caught by challenger via verifying the hash value on the corresponding plaintext. So if an adversary attempts to modify the ciphertext and query for its decryption, the challenger will find its attempt and return "$False$". Thus people believed that by modifying a PKE scheme into KEM scheme and combining with a secure symmetric encryption, an IND-CCA secure PKE could be achieved. It has also been proved in [11] that any genetic-hash chosen-ciphertext attack on the modified KEM scheme is as difficult as inverting the original encryption function. Streamlined NTRU Prime scheme follows the genetic KEM construction introduced by Dent [11], and attempt to achieve IND-CCA security.

Although Streamlined NTRU Prime is designed with these two features, and its security receives evidences from both mathematical and cryptographic theory, we still found an efficient key recovery attack on it. Our attack exactly takes advantage of the two features of Streamlined NTRU Prime. Briefly, we use a simple property associated to the new ring adopted by Streamlined NTRU Prime to construct the querying ciphertexts, then by analysis the information leakage from the feedback of "False", we recover the private key of Streamlined NTRU Prime. Our attack is not like the attacks proposed in[5] and [6], because indeed we haven't found any special structure in the new ring that can be used to reduce the dimension of the corresponding lattice attack. Our attack is more similar to the attacks [12, 13] in principle, it exploits the dependence between the private key and the failure in decryption.

The rest of this paper is organized as follows. In Section 2, we give the notations used in this paper and a brief review of Streamlined NTRU Prime, we also introduce some tools used in our attack and describe the outline of our attack. In Section 3, we use two algorithms to describe our attack, and use two theorems to show its correctness, we also discuss the parameter setting and the future work about our attack. In Section 4, we make a conclusion.

2 Notations, Brief Review and Preliminaries

2.1 Notations:

Let $\mathbb{Z}[x]$ be the polynomial ring over the integers ring $\mathbb{Z}$. Let p, q be two primes, we use $\mathcal{R}, \mathcal{R}/3, \mathcal{R}/q$ to respectively denote the ring $\mathbb{Z}[x]/(x^p - x - 1), \mathbb{Z}[x]/(x^p - x - 1, 3), \mathbb{Z}[x]/(x^p - x - 1, q)$. We use lowercase letter, e.g. g, to denote a polynomial in $\mathcal{R}$ ($\mathcal{R}/3, \mathcal{R}/q$). We use lowercase letter with an overline, e.g. $\overline{g}$ to denote string of the corresponding polynomial e.g. g, which is used as the input of a hash function. Given two polynomial $f, g \in \mathcal{R}$, we use fg and $f + g$ to respectively denote the multiplication and addition in $\mathcal{R}$, and we use $fg \bmod q$ and $f + g \bmod q$ to denote the corresponding operations in $\mathcal{R}/q$. We use lowercase letter with a subscript i, e.g. g_i, to denote the coefficient of the i-degree term of g, i.e., $g = g_0 + g_1 x + \cdots + g_{p-1} x^{p-1}$. For the product and sum of two polynomial, say f and g, we also use $(fg)_i$ and $(f + g)_i$ to denote the coefficient of the i-degree term of fg and $f + g$. Given an integer a and a prime q, $a \bmod q$ is defined as the unique integer $a' \in [-\frac{q-1}{2}, \frac{q-1}{2}]$, such that $q | a - a'$. Therefore, the coefficients of a polynomial in $\mathcal{R}/q$ ($\mathcal{R}/3$) are in $\{-\frac{q-1}{2}, \cdots, 0, \cdots, \frac{q-1}{2}\}$ $\{-1, 0, 1\}$). A polynomial $g \in \mathcal{R}$ is called small, if $\forall\ i \in \{0, 1, \cdots, p-1\}$, $g_i \in \{-1, 0, 1\}$. Given an integer $t > 0$, g is called t-small, if: (1) g is small; (2) $\sum_{i=0}^{p-1} |g_i| = 2t$, i.e., there are exactly $2t$ non-zero coefficients. We use ϕ to denote the standard isomorphism from $\mathcal{R}$ to $\mathbb{Z}^p$, i.e., $\phi(g) = (g_0, g_1, \cdots, g_{p-1})$, then we refer to the norm of g as the norm of $\phi(g)$. We use notation $\|g\|_{l_\infty}$ to represent the l_∞-norm of the polynomial g.

2.2 Brief review of Streamlined NTRU Prime

As a KEM scheme Streamlined NTRU Prime includes three algorithms: key generation, encapsulation, and decapsulation.

Key Generation The receiver generates the public key and private key in the following steps:

1) Choose uniformly at random a small polynomial $g \in \mathcal{R}$ with g being invertible in $\mathcal{R}_3$.
2) Choose uniformly at random a t-small polynomial $f \in \mathcal{R}$, such that $t \geq 1$, and f is invertible in $\mathcal{R}_q$.
3) Compute $h = g/(3f) \bmod q$.
4) The public key is h. The private key is f in $\mathcal{R}$ and $1/g$ in $\mathcal{R}_3$.

Encapsulation The sender generates a ciphertext as follows:

1) Choose uniformly at random a t-small polynomial $r \in \mathcal{R}$.
2) Compute $v = hr \bmod q$.
3) Round each coefficient of v to the nearest multiple of 3 to product $c \in \mathcal{R}$. This can be viewed as choosing the small polynomial m, such that $c = v + m$ and $3|c$.
4) Compute $Hash(\overline{r})$, obtaining a left half $\overline{C}$ (key confirmation) and a right half $\overline{K}$ (session key). Where $Hash(\cdot)$ denote a cryptographic hash function.
5) Output the concatenation $\overline{C}||\overline{c}$, keep the session key $\overline{K}$.

Decapsulation The receiver decapsulates a ciphertext $\overline{C}||\overline{c}$ as follows:

1) Compute $w = 3fc \bmod q$.
2) Compute $e = w \bmod 3$.
3) Compute $r' = e(1/g) \bmod 3$.
4) Compute $Hash(\overline{r'})$, obtaining a left half $\overline{C'}$ and a right half $\overline{K'}$. In case of r' is t-small and $\overline{C'} = \overline{C}$, output $\overline{K'}$. Otherwise output "$False$".

The encapsulation can be viewed as two steps. The first step is **encryption**. It chooses uniformly at random a t-small polynomial r as plaintext, and encrypts it to obtain the ciphertext $c = hr + m \bmod q$. The second step is hashing. It takes as input the string of randomly chosen plaintext r, and generates the session key and key confirmation, which are respectively the right half and left half of $Hash(\overline{r})$. Finally, it outputs the ciphertext with the key confirmation, and keeps the session key.

Correspondingly, the decapsultion can also be viewed as two steps. The first step is **decryption**. It decrypts the received ciphertext c to recover a plaintext r'. The second step is hashing and checking. It computes $Hash(\overline{r'})$ to obtain the right half $\overline{K'}$ and left half $\overline{C'}$, and verifies the legality of the session key $\overline{K'}$ by checking whether $\overline{C'} = \overline{C}$.

2.3 Computations in $\mathcal{R}$

We use ϕ to denote the standard isomorphism from $\mathcal{R}$ to $\mathbb{Z}^p$, i.e., $\phi(g) = (g_0, g_1, \cdots, g_{p-1})$. Given a polynomial g, there is a corresponding matrix

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{p-2} & g_{p-1} \\ g_{p-1} & g_{p-1} + g_0 & g_1 & \cdots & f_{p-3} & g_{p-2} \\ g_{p-2} & g_{p-2} + g_{p-1} & g_{p-1} + g_0 & \cdots & g_{p-3} & g_{p-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ g_1 & g_1 + g_2 & g_2 + g_3 & \cdots & g_{p-2} + g_{p-1} & g_{p-1} + g_0 \end{bmatrix}$$

such that the i-th (i from 0 to $p-1$) row is exactly $\phi(gx^i)$. Then we have

$$\phi(gr) = \phi(r) \cdot G$$

We consider the relation between g and gx. We have $(gx)_j = g_{(j-1 \bmod p)}$ for $j = 0, 2, \cdots, p-1$, and $(gx)_1 = g_0 + g_{p-1}$. Suppose g is small, it is obvious that $|(gx)_j| \leq 1$ for $j = 0, 2, \cdots, p-1$, and $|(gx)_1| \leq 2$. The following property is also easy to obtain.

Property 1. Let $g \in \mathcal{R}$ be a small polynomial, suppose L is the smallest integer such that $\|gx^L\|_{l_\infty} \geq 2$, then let $u = gx^L$, it must hold $\|gx^L\|_{l_\infty} = 2$ and

$$\begin{cases} |u_1| = 2, \\ |u_i| \leq 1, \text{ for } i = 0, 2, \cdots, p-1. \end{cases} \tag{1}$$

2.4 Hoeffding's inequality

Lemma 1 (Hoeffding's inequality[14]). *Let $x_1, x_2, \cdots, x_n$ be n independent variables, satisfying* $\Pr[x_i \in [\alpha_i, \beta_i]] = 1$, *for $1 \leq i \leq n$. Let $X = x_1 + x_2 + \cdots + x_n$ and $E(X)$ be the expected value of X. Then for any $\lambda > 0$, we have*

$$\Pr[X - E(X) \geq \lambda] \leq e^{-\frac{2\lambda^2}{\sum_{i=1}^n (\beta_i - \alpha_i)^2}}$$

and

$$\Pr[X - E(X) \leq -\lambda] \leq e^{-\frac{2\lambda^2}{\sum_{i=1}^n (\beta_i - \alpha_i)^2}}$$

and therefore

$$\Pr[|X - E(X)| < \lambda] > 1 - 2e^{-\frac{2\lambda^2}{\sum_{i=1}^n (\beta_i - \alpha_i)^2}}$$

Given a small polynomial $g \in \mathcal{R}$ and a t-small polynomial $r \in \mathcal{R}$. As we shown before, each coefficient of gr can be viewed as the sum of at most $4t$ variables in $[-1, 1]$, and obviously its expected value is 0. So, by Hoeffding's inequality, we can bound the l_∞ norm of $gr \in \mathcal{R}$ as:

$$\Pr[\|gr\|_{l_\infty} < s] > 1 - 2e^{-\frac{s^2}{8t}}$$

Similarly, given a t-small polynomial $f \in \mathcal{R}$ an a small polynomial $m \in \mathcal{R}$, we can bound $\|gr + 3fm\|_{l_\infty}$ by:

$$\Pr[\|gr + 3fm\|_{l_\infty} < s] > 1 - 2e^{-\frac{s^2}{80t}}$$

2.5 Attack Model, Decapsulation Oracle and Outline

Attack Model Our attack is under the chosen-ciphertext attack model. The adversary plays the role of a sender and the receiver plays as the challenger. Received a cihphertext, the challenger should honestly decapsulate it and feed back to the adversary. By analyzing the feedback the adversary aims to recover the challenger's private key. Notice that Streamlined NTRU Prime scheme is a KEM scheme and is believed to achieve IND-CCA security. This is because: (1) the using of hash function remove the malleability of the ciphertext; (2) by checking the hash value on the corresponding plaintext the challenger could find out any modification of the queried ciphertext, and will return to the querying nothing but a "*False*". We need to emphasize that even a feedback of "*False*" will reveal information which at least shows that the queried ciphertext lead to an illegal plaintext after decryption. As we will show in this paper, the feedback of False is equivalent to the "*Failure*" of decryption on the querying ciphertext. By cleverly designing, we embed the relation between the private key and the "*Failure*" of decryption into the querying ciphertext. After received enough feedbacks of "*False*", an adversary can learn the private key form these information leakages.

Decapsulation Oracle A basic query-response procedure used in our attack is described as follows. The adversary chooses a t-small polynomial $r \in \mathcal{R}$, and computes $v = hr \bmod q$. Then the adversary chooses the small polynomial $m \in \mathcal{R}$, such that $c = v + m \bmod q$ and $3|c$, and chooses another polynomial m', such $c' = c + m' \bmod q$ and $3|c'$. The adversary computes $Hash(\overline{r})$ to obtain the left half $\overline{C}$ and the right half $\overline{K}$. Finally the adversary sends $\overline{C}||\overline{c'}$ to the challenger and waits for the feedback. We denote the above procedure as "$\mathcal{D}(c')$". This procedure is almost the same as an ordinary encapsulation. The only difference is that a true sender will choose $m' = 0$, while the adversary chooses m' more freely.

To decapsulate $\overline{C}||\overline{c'}$, the challenger needs firstly to decrypt c'. Note that the first step of decryption on c' is computing $w' = 3fc' \bmod q$. If m' is chosen such that $\|gr + 3fm + 3fm'\|_{l_\infty} \leq \frac{q-1}{2}$, then $w' = gr + 3fm + 3fm'$, and the decrypted plaintext r' is equal to r. After computing $Hash(r')$ to obtain the left half $\overline{C'}$ and the right half $\overline{K'}$, challenger will find that r' is t-small, and $\overline{C'} = \overline{C}$. Finally, the session key is accepted by the challenger. We denote this procedure by $\mathcal{D}(c') \Rightarrow$ "*Pass*". If the m' is chosen such that $\|gr + 3fm + 3fm'\|_{l_\infty}\| > \frac{q-1}{2}$, the following lemma guarantees that the decrypted plaintext r' is no long equal to r.

Lemma 2. *Let $gr \in \mathcal{R}$ and $\|gr\|_{l_\infty} \leq \frac{q-1}{4}$, let $\alpha \in \mathcal{R}$ and $\|gr + 3\alpha\|_{l_\infty} \leq q - 1$, then there does not exist $\beta \in \mathcal{R}$ such that $\|gr + 3\beta\|_{l_\infty} < \frac{q-1}{2}$ and $gr + 3\alpha \equiv gr + 3\beta \bmod q$.*

Proof. Suppose there exists $\beta \in \mathcal{R}$ such that $gr + 3\alpha \equiv gr + 3\beta \bmod q$, we have $q|3(\alpha - \beta)$. Since $\gcd(q, 3) = 1$, it implies that $q|\alpha - \beta$. Note that $\|gr\|_{l_\infty} \leq \frac{q-1}{4}$ and $\|gr + 3\alpha\|_{l_\infty} < q - 1$, we have $\|\alpha\|_{l_\infty} \leq \frac{5(q-1)}{12}$. Suppose it also holds that $\|gr + 3\beta\|_{l_\infty} < \frac{q-1}{2}$, similarly, we have $\|\beta\|_{l_\infty} \leq \frac{3(q-1)}{12}$. It is easy to check that $\|\alpha - \beta\|_{l_\infty} \leq \frac{8}{12}(q - 1) < (q - 1)$, then $q|(\alpha - \beta)$ implies that $\alpha = \beta$, which is contradictory to $\|gr + 3\beta\|_{l_\infty} \leq \frac{q-1}{2}$. Therefore there does not exist such β. □

Lemma 3. *Let $c' = hr + m + m' \bmod q$, and $\|gr\|_{l_\infty} \leq \frac{q-1}{4}$, suppose that $|(gr + 3fm + 3fm')_j| \leq \frac{q-1}{2}$ for all $j = 0, 2, \cdots, p - 1$, then $\mathcal{D}(c') \Rightarrow$ "$False$" if and only if $|(gr + 3fm + 3fm')_1| > \frac{q-1}{2}$.*

Proof. The sufficiency is obvious, since if $|(gr + 3fm + 3fm')_1| \leq \frac{q-1}{2}$, then $\|gr + 3fm + 3fm'\|l_\infty \leq \frac{q-1}{2}$. The decryption on c' will obtain r, which implies $\mathcal{D}(c') \Rightarrow$ "$Pass$".

Suppose for $j = 0, 2, \cdots, p - 1$, $|(gr + 3fm + 3fm')_j| \leq \frac{q-1}{2}$, and $|(gr + 3fm + 3fm')_1| > \frac{q-1}{2}$, then we have $w' = gr + 3fm + 3fm' \bmod q = gr + 3fm + 3fm' + \xi \cdot qx$. By lemma 2, we also have $3 \nmid \xi \cdot qx$. The decryption on c' will obtain $r' = w'g^{-1} \bmod 3 = r \pm xg^{-1}$. Note that x is invertible in $\mathcal{R}/3$, so $xg^{-1} \neq 0$ and $r' \neq r$. This implies $\mathcal{D}(c') \Rightarrow$ "$False$". □

In the rest of this paper, every polynomial $m' \in \mathcal{R}$ chosen by the adversary to construct the querying cipheretxt will satisfy the conditions required by lemma 1 and lemma 2. Noted that g is small polynomial and r is t-small polynomial, and considered that the parameters satisfy $q - 1 \geq 32t$, so we have $\|gr\|_{l_\infty} \leq \frac{q-1}{4}$. Therefore, it holds that $\mathcal{D}(c') \Rightarrow$ "$False$" if and only if $|(gr + 3fm + 3fm')_1| > \frac{q-1}{2}$.

Attack Outline The core of our attack is the construction of the querying ciphertext $c' = hr + m + m' \in \mathcal{R}/q$. Since there is no much freedom for the adversary on the choice of **basic ciphertext** $hr + m$, so the most important is the choice of m'. In our attack m' consists of two part, say $m'^{(1)}$ and $m'^{(2)}$. We call $m'^{(1)}$ the **impulse ciphertext**, and call $m'^{(2)}$ the **key sensitive ciphertext**. Based on the constitution of m', our attack includes three main steps:

i) Find an impulse ciphertext $m'^{(1)}$, such that the value $|(gr+3fm+3fm'^{(1)})_1|$ reaches to a peak, while for the rest position $j \in \{0, 2, \cdots, p - 1\}$, $|(gr + 3fm + 3fm'^{(1)})_j|$ remains low and keeps a big enough gap to $|(gr + 3fm + 3fm'^{(1)})_1|$.

ii) Design a key sensitive ciphertext, such that the value $|(3fm'^{(2)})_1|$ determines a linear relation about the private key, and when $|(3fm'^{(2)})_k|$ takes different value, it satisfies that either $|(gr + 3fm + 3fm'^{(1)} + 3fm'^{(2)})_1| \leq \frac{q-1}{2}$ or $|(gr + 3fm + 3fm'^{(1)} + 3fm'^{(2)})_1| > \frac{q-1}{2}$.

iii) Query the challenger with $\overline{C}||c'$ and receive the feedback. The feedback $\mathcal{D}(c')$ determines the value of $|(3fm'^{(2)})_1|$, and consequently determines a linear relation about the private key. With enough such linear relations, the adversary will finally recover the private key.

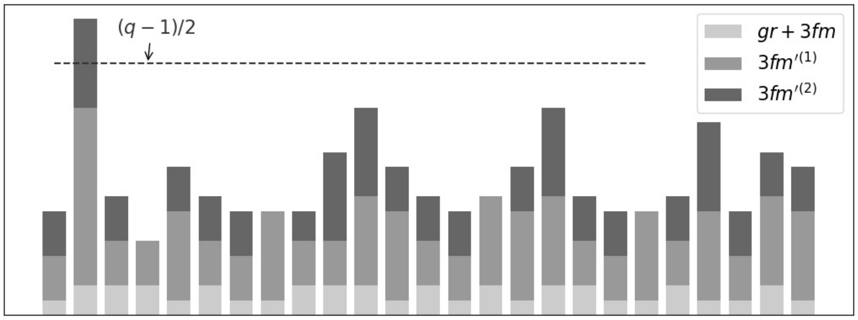

Fig. 1. Basic, impulse and key sensitive plaintexts

More specifically, the impulse ciphertext is of the form $\theta^{(1)} \cdot x^L$, where $\theta^{(1)}$ is an integer, L is the smallest integer such that $\|fx^L\|_{l_\infty} = 2$. According to the decryption step in decapsulation, $|(gr + 3fm + 3fm'^{(1)})_1| = |(gr + 3fm + \theta^{(1)} \cdot fx^L)_1|$. By property 1, we know that $|(fx^L)_1| = 2$ and for $j = 0, 2, \cdots, p-1$, $|(fx^L)_j| \leq 1$. Thus, as shown in Fig. 1, by properly selecting $\theta^{(1)}$, $|(gr + 3fm + 3fm'^{(1)})_1|$ will reaches to a peak, and keeps a big gap to $|(gr+3fm+3fm'^{(1)})_j|$, for $j = 0, 2, \cdots, p-1$.

The key sensitive ciphertext is of the form $\theta^{(2)} \cdot x^{L+i}$, where $\theta^{(2)}$ is an integer, $i \in \{0, 1, \cdots, p-1\}$. Noted that x is invertible in $\mathcal{R}$, so if we get fx^L, we can obtain f by multiplying x^{-L} to fx^L. Let $u = fx^L \in \mathcal{R}$, it is easy to check that for $i = 1, \cdots, p-1$, $(fx^{L+i})_1 = u_{p-i} + u_{p-i+1}$ (define $u_p = u_0$), and $(fx^L)_1 = u_1$. As shown in Fig.1, when $(fx^{L+i})_1$ takes some specific value, it will result in $|(gr + 3fm + 3fm'^{(1)} + 3fm'^{(2)})_1| > \frac{q-1}{2}$, and therefore $\mathcal{D}(c') \Rightarrow$ "*False*".

3 Attack on Streamlined NTRU Prime

3.1 Attack

Our attack includes two algorithms. The first one is to determine the smallest integer L such that $\|fx^L\|_{l_\infty} = 2$, the second one is to query to the challenger with the elaborately fabricated ciphertexts, and to obtain the linear equations about the coefficients of fx^L. Theorem 1 and theorem 2 respectively show that the algorithm 1 and algorithm 2 will correctly output what we need with a proper probability. The details are as follows.

```
Algorithm 1:
Input: An intance of the Streamlined NTRU Prime with paramerter
    $(p, q, t)$, and a parameter $s$ such that $s \leq \frac{q-1}{6} - 4$.
Output: $(L, r, m)$.
Choose an integer $\gamma \in [\frac{q-1}{12} + \frac{s}{6} + 1, \frac{q-1}{6} - \frac{s}{3} - 2]$;
Choose uniformly at random a $t$-small polynomial $r \in \mathcal{R}$. Compute
  $v = hr \bmod q$. Choose a small polynomial $m \in \mathcal{R}$, such that
  $c = v + m \in \mathcal{R}/q$ and $3|c$.
Loop (1): for $(i = 1; i++)$ do
    Compute $c^{(i)} = c + \rho^{(i)} \cdot x^i + \gamma \cdot x^i \bmod q$, where $\rho^{(i)} \in \{-1, 0, 1\}$ such
      that $3|c^{(i)}$;
    if $\mathcal{D}(c^{(i)})$ returns "False" then
        $L \leftarrow i$, break Loop (1);
return $(L, r, m)$;
```

Theorem 1. *Let (L, r, m) be the output of algorithm 1, let $u = fx^L \in \mathcal{R}$, then,*

(I) $\Pr[\|gr + 3fm\|_{l_\infty} < s] > 1 - 2e^{-\frac{s^2}{80t}}$*;*

(II) when $\Pr[\|gr+3fm\|_{l_\infty} < s]$*, L is the smallest integer such that* $\|u\|_{l_\infty} = 2$.

Proof. $\Pr[\|gr + 3fm\|_{l_\infty} < s] > 1 - 2e^{-\frac{s^2}{80t}}$ follows directly by Hoeffding's inequality.

Note $\rho^{(i)} \in \{-1, 0, 1\}$, $\|3\rho^{(i)} \cdot fx^i\|_{l_\infty} \leq 6$. Let $m^{(i)} = c + \rho^{(i)} \cdot x^i$, by triangle inequality, we have

$$\|gr + 3fm^{(i)}\|_{l_\infty} \leq \|gr + 3fm\|_{l_\infty} + \|3\rho^{(i)} \cdot fx^i\|_{l_\infty} < s + 6.$$

Let $w'^{(i)} = gr + 3fm^{(i)}$, and $w^{(i)} = w'^{(i)} + 3\gamma \cdot fx^i$. Consider the l_∞ norm, we have

$$-\|w'^{(i)}\|_{l_\infty} + 3\gamma\|fx^i\|_{l_\infty} \leq \|w^{(i)}\|_{l_\infty} \leq +\|w'^{(i)}\|_{l_\infty} + 3\gamma\|fx^i\|_{l_\infty}$$

Since $\|w'^{(i)}\|_{l_\infty} < s + 6$ holds for any $i = 1, 2, \cdots, L$, so we have

$$-s - 6 + 3\gamma\|fx^i\|_{l_\infty} < \|w^{(i)}\|_{l_\infty} < s + 6 + 3\gamma\|fx^i\|_{l_\infty}.$$

Let $u = fx^L$, then $w^{(L)} = w'^{(L)} + 3\gamma \cdot u$. Since $\mathcal{D}(c^{(L)})$ returns "*False*", it must hold that $\|u\|_{l_\infty} \geq 2$. Otherwise, suppose $\|u\|_{l_\infty} \leq 1$, it implies

$$\|w^{(L)}\|_{l_\infty} < s + 6 + 3(\frac{q-1}{6} - \frac{s}{3} - 2) = \frac{q-1}{2}$$

which is contradictory to $\mathcal{D}(c^{(L)})$ returns "*False*".

It also needs to show that when $\|u\|_{l_\infty} = 2$, it must hold $\mathcal{D}(c^{(L)})$ returns "*False*". Given $\|u\|_{l_\infty} = 2$,

$$\|w^{(L)}\|_{l_\infty} > -s - 6 + 6(\frac{q-1}{12} + \frac{s}{6} + 1) = \frac{q-1}{2}.$$

Suppose there exists $L' < L$ such that L' is the smallest integer that satisfies $\|fx^{L'}\|_{l_\infty} = 2$. By property 1, let $u' = fx^{L'}$, we have

$$\begin{cases} |u'_1| = 2, \\ |u'_k| \leq 1, \text{ for } k = 0, 2, \cdots, p-1. \end{cases}$$

Therefore

$$|(w^{(L')})_1| > -s - 6 + 6(\tfrac{q-1}{12} + \tfrac{s}{6} + 1) = \tfrac{q-1}{2},$$
$$|(w^{(L')})_j| < s + 6 + 3(\tfrac{q-1}{6} - \tfrac{s}{3} - 2) = \tfrac{q-1}{2}, \text{ for } i = 0, 2, \cdots, p-1.$$

By lemma 3, it follows that $\mathcal{D}(c^{(L')}) \Rightarrow$ "$False$", which is contradictory to $L' < L$. Therefore, L is the smallest integer such that $\|u\|_{l_\infty} = 2$. □

Algorithm 2:

```
Input: An intance of Streamlined NTRU Prime with paramerter $(p, q, t)$.
Output: $\{(\sigma_1, \cdots, \sigma_{p-1}), s\}$.
Choose a parameter $\delta$, such that $\delta = \lfloor \frac{q-1}{27} \rceil$. Let $s = \frac{3\delta}{2} - 21$;
$\{L, r, m\} \leftarrow$ algorithm $1(p, q, t, s)$;
Compute $v = hr \bmod q$, $c = v + m \bmod q$ (note that $3|c$);
Loop (1): for $i = 1; i \leq p - 2$ do
    Initiate $\sigma_i = 0$;
    Loop (2): for $j = 1, -1, 2, -2$ (by order) do
        case $j = 1$ do
            Choose $\eta^{(i,j)} = \lfloor \frac{q-1-9\delta}{12} \rceil$, Set
             $c^{(i,j)} = c + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i} + \eta^{(i,j)} \cdot x^L + \delta \cdot x^{L+i} \bmod q$,
             where $\rho^{(i,j,1)}, \rho^{(i,j,2)} \in \{-1, 0, 1\}$ such that $3|c^{(i,j)}$;
        case $j = -1$ do
            Choose $\eta^{(i,j)} = \lfloor \frac{q-1-9\delta}{12} \rceil$, Set
             $c^{(i,j)} = c + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i} + \eta^{(i,j)} \cdot x^L - \delta \cdot x^{L+i} \bmod q$,
             where $\rho^{(i,j,1)}, \rho^{(i,j,2)} \in \{-1, 0, 1\}$ such that $3|c^{(i,j)}$;
        case $j = 2$ do
            Choose $\eta^{(i,j)} = \lfloor \frac{q-1-3\delta}{12} \rceil$, Set
             $c^{(i,j)} = c + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i} + \eta^{(i,j)} \cdot x^L + \delta \cdot x^{L+i} \bmod q$,
             where $\rho^{(i,j,1)}, \rho^{(i,j,2)} \in \{-1, 0, 1\}$ such that $3|c^{(i,j)}$;
        case $j = -2$ do
            Choose $\eta^{(i,j)} = \lfloor \frac{q-1-3\delta}{12} \rceil$, Set
             $c^{(i,j)} = c + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i} + \eta^{(i,j)} \cdot x^L - \delta \cdot x^{L+i} \bmod q$,
             where $\rho^{(i,j,1)}, \rho^{(i,j,2)} \in \{-1, 0, 1\}$ such that $3|c^{(i,j)}$;
        if $\mathcal{D}(c^{(i,j)})$ returns "$False$" then
            $\sigma_i \leftarrow \frac{2}{j}$, break Loop (2);
for $i = p - 1$ do
    Initiate $\sigma_i = 0$;
    Loop (3): for $j = 1, 2$ (by order) do
        case $j = 1$ do
            Choose $\eta^{(i,j)} = \lfloor \frac{q-1-15\delta}{12} \rceil$, Set
             $c^{(i,j)} = c + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i} + \eta^{(i,j)} \cdot x^L + \delta \cdot x^{L+i} \bmod q$,
             where $\rho^{(i,j,1)}, \rho^{(i,j,2)} \in \{-1, 0, 1\}$ such that $3|c^{(i,j)}$;
        case $j = 2$ do
            Choose $\eta^{(i,j)} = \lfloor \frac{q-1-9\delta}{12} \rceil$, Set
             $c^{(i,j)} = c + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i} + \eta^{(i,j)} \cdot x^L + \delta \cdot x^{L+i} \bmod q$,
             where $\rho^{(i,j,1)}, \rho^{(i,j,2)} \in \{-1, 0, 1\}$ such that $3|c^{(i,j)}$;
        if $\mathcal{D}(c^{(i,j)})$ returns "$False$" then
            $\sigma_i \leftarrow \lfloor \frac{3}{j} \rceil$, break Loop (3);
return $\{(\sigma_1, \cdots, \sigma_{p-1}), s\}$;
```

Theorem 2. *Let $\{(\sigma_1, \cdots, \sigma_{p-1}), s\}$ be the output of algorithm 2, let $u'_0, u'_1, \cdots, u'_{p-1}$ be the unique solution of the equations*

$$\begin{aligned} u'_{p-i} + u'_{p-i+1} &= \sigma_i \ (\ i = 1, \cdots, p-1.) \\ u'_1 &= 2 \\ u'_0 &= u'_p \end{aligned} \tag{2}$$

over $\mathbb{Z}/3$. Let $u' = \phi^{-1}(u'_0, u'_1, \cdots, u'_{p-1}) \in \mathcal{R}$ and $f' = u'x^{-L} \in \mathcal{R}$ (x is invertible in $\mathcal{R}$), then

- *(I)* $\Pr[\|gr + 3fm\|_{l_\infty} < s] > 1 - 2e^{-\frac{s^2}{80t}}$*;*
- *(II) when $\|gr + 3fm\|_{l_\infty} < s$, we have either $f = g'$ or $f = -f'$, where f is the corresponding private of the Streamlined NTRU Prime instance input to algorithm 2.*

Proof. $\Pr[\|gr + 3fm\|_{l_\infty} < s] > 1 - 2e^{-\frac{s^2}{80t}}$ follows directly by Hoeffding's inequality.

For any $i \in \{1, \cdots, p-1\}$ and $j \in \{1, -1, 2, -2\}$ (when $i \neq q-1$) or $j \in \{1, 2\}$ (when $i = q-1$), let

$$w'^{(i,j)} = gr + 3f(m + \rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i}).$$

It is easy to check that $\|\rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i}\|_{l_\infty} \leq 3$. So $\|f(\rho^{(i,j,1)} \cdot x^L + \rho^{(i,j,2)} \cdot x^{L+i})\|_{l_\infty} \leq 6$, and $\|w'^{(i,j)}\|_{l_\infty} \leq \|gr + 3fm\|_{l_\infty} + 18$.

Let

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot fx^L + 3\delta \cdot fx^{L+i}$$

we have $w^{(i,j)} \equiv 3fc^{(i,j)} \bmod q$. Let $u = fx^L$, by theorem 1 and property 1, we have $\|u\|_{l_\infty} = 2$ and

$$\begin{cases} |u_1| = 2, \\ |u_k| \leq 1, \text{ for } k = 0, 2, \cdots, p-1. \end{cases}$$

Suppose $\|w'^{(i,j)}\|_{l_\infty} = s'$, then for $k = 0, 2, \cdots, p-1$, we have

$$|w_k^{(i,j)}| \leq s' + 3\eta^{(i,j)} + 6\delta.$$

Note $s' \leq s + 18 < \frac{3\delta}{2} - 3$, and for any choice of $\eta^{(i,j)}$, it is easy to check that

$$|w_k^{(i,j)}| \leq \frac{q-1}{2} \text{ for } k = 0, 2, \cdots, p-1.$$

According to lemma 3, $\mathcal{D}(c'^{(i,j)}) \to$ "*False*" if and only if

$$|w_1^{(i,j)}| > \frac{q-1}{2}.$$

Suppose $u_1 = 2$, it is easy to check that $w_1^{(i,j)} - w_1'^{(i,j)} > 0$. Then we discuss as follows;

For each $i \in \{1, \cdots, p-2\}$, noted $(ux^i)_1 = u_{p-i} + u_{p-i+1} \in \{-2, -1, 0, 1, 2\}$ (here $u_p = u_0$), we discuss in the following cases:

(i). Assume that loop (2) ends when $j = 1$, then

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot u + 3\delta \cdot ux^i,$$

where $u = fx^L$. Note $u_1 = 2$, we have $w_1^{(i,j)} = w_1'^{(i,j)} + 6\eta^{(i,j)} + 3\delta(ux^i)_1$. According to lemma 3, $\mathcal{D}(c^{(i,j)}) \to$ "*False*" if an only if $w_1^{(i,j)} > \frac{q-1}{2}$. If $(ux^i)_1 \leq 1$, it implies that

$$\begin{aligned} w_1^{(i,j)} &\leq |w_1'^{(i,j)}| + 6(\tfrac{1}{2} + \tfrac{q-1-9\delta}{12}) + 3\delta \\ &< \tfrac{3\delta}{2} - 3 + 3 + \tfrac{q-1}{2} - \tfrac{9\delta}{2} + 3\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

This is contradictory to the assumption, so $(ux^i)_1 \geq 2$. Since $\|ux^i\|_{l_\infty} \leq 2$ for $i = 1, \cdots, p-2$, so $(ux^i)_1 = 2$.

It also needs to show that when $(ux^i)_1 = 2$, it must hold that $\mathcal{D}(c^{(i,j)}) \to$ "*False*". Given $(ux^i)_1 = 2$, then

$$\begin{aligned} w_1^{(i,j)} &\geq -|w_1'^{(i,j)}| + 6(-\tfrac{1}{2} + \tfrac{q-1-9\delta}{12}) + 6\delta \\ &> -\tfrac{3\delta}{2} + 3 - 3 + \tfrac{q-1}{2} - \tfrac{9\delta}{2} + 6\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

Note that in this case we set $\sigma_i = 2/j = 2$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

(ii). Assume that loop (2) ends when $j = -1$, then

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot fx^L - 3\delta \cdot fx^{L+i},$$

where $u = fx^L$. Note $u_1 = 2$, we have $w_1^{(i,j)} = w_1'^{(i,j)} + 6\eta^{(i,j)} - 3\delta(ux^i)_1$. According to lemma 3, $\mathcal{D}(c^{(i,j)}) \to$ "*False*" if an only if $w_1^{(i,j)} > \frac{q-1}{2}$. If $(ux^i)_1 \geq -1$, it implies that

$$\begin{aligned} w_1^{(i,j)} &\leq |w_1'^{(i,j)}| + 6(\tfrac{1}{2} + \tfrac{q-1-9\delta}{12}) + 3\delta \\ &< \tfrac{3\delta}{2} - 3 + 3 + \tfrac{q-1}{2} - \tfrac{9\delta}{2} + 3\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

This is contradictory to the assumption, so $(ux^i)_1 \leq -2$. Since $\|ux^i\|_{l_\infty} \geq -2$ for $i = 1, \cdots, p-2$, so $(ux^i)_1 = -2$.

It also needs to show that when $(ux^i)_1 = -2$, it must hold that $\mathcal{D}(c^{(i,j)}) \to$ "*False*". Given $(ux^i)_1 = -2$, then

$$\begin{aligned} w_1^{(i,j)} &\geq -|w_1'^{(i,j)}| + 6(-\tfrac{1}{2} + \tfrac{q-1-9\delta}{12}) + 6\delta \\ &> -\tfrac{3\delta}{2} + 3 - 3 + \tfrac{q-1}{2} - \tfrac{9\delta}{2} + 6\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

Note that in this case we set $\sigma_i = 2/j = -2$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

(iii). Assume that loop (2) ends when $j = 2$, then

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot u + 3\delta \cdot ux^i,$$

where $u = fx^L$. Note $u_1 = 2$, we have $w_1^{(i,j)} = w_1'^{(i,j)} + 6\eta^{(i,j)} + 3\delta(ux^i)_1$. According to lemma 3, $\mathcal{D}(c^{(i,j)}) \to$ "*False*" if an only if $w_1^{(i,j)} > \frac{q-1}{2}$. If $(ux^i)_1 < 1$, it implies that

$$\begin{aligned} w_1^{(i,j)} &\leq |w_1'^{(i,j)}| + 6(\tfrac{1}{2} + \tfrac{q-1-3\delta}{12}) \\ &< \tfrac{3\delta}{2} - 3 + 3 + \tfrac{q-1}{2} - \tfrac{3\delta}{2} \\ &= \tfrac{q-1}{2} \end{aligned}$$

This is contradictory to the assumption, so $(ux^i)_1 \geq 1$. Since $(ux^i)_1 < 2$, otherwise loop (2) end when $j = 1$, so we have $(ux^i)_1 = 1$.
It also needs to show that when $(ux^i)_1 = 1$, it must hold that $\mathcal{D}(c^{(i,j)}) \to$ "*False*". Given $(ux^i)_1 = -2$, then

$$\begin{aligned} w_1^{(i,j)} &\geq -|w_1'^{(i,j)}| + 6(-\tfrac{1}{2} + \tfrac{q-1-3\delta}{12}) + 3\delta \\ &> -\tfrac{3\delta}{2} + 3 - 3 + \tfrac{q-1}{2} - \tfrac{3\delta}{2} + 3\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

Note that in this case we set $\sigma_i = 2/j = 1$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

(iv). Assume that loop (2) ends when $j = -2$, then

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot u - 3\delta \cdot ux^i,$$

where $u = fx^L$. Note $u_1 = 2$, we have $w_1^{(i,j)} = w_1'^{(i,j)} + 6\eta^{(i,j)} - 3\delta(ux^i)_1$. According to lemma 3, $\mathcal{D}(c^{(i,j)}) \to$ "*False*" if an only if $w_1^{(i,j)} > \frac{q-1}{2}$. If $(ux^i)_1 > -1$, it implies that

$$\begin{aligned} w_1^{(i,j)} &\leq |w_1'^{(i,j)}| + 6(\tfrac{1}{2} + \tfrac{q-1-3\delta}{12}) \\ &< \tfrac{3\delta}{2} - 3 + 3 + \tfrac{q-1}{2} - \tfrac{3\delta}{2} \\ &= \tfrac{q-1}{2} \end{aligned}$$

This contradicts to the assumption, so $(ux^i)_1 \leq -1$. Since $(ux^i)_1 > -2$, otherwise loop (2) end when $j = -1$, so we have $(ux^i)_1 = -1$.

It also needs to show that when $(ux^i)_1 = -1$, it must hold that $\mathcal{D}(c^{(i,j)}) \to$ "$False$". Given $(ux^i)_1 = -1$, then

$$\begin{aligned} w_1^{(i,j)} &\geq -|w_1'^{(i,j)}| + 6(-\tfrac{1}{2} + \tfrac{q-1-3\delta}{12}) + 3\delta \\ &> -\tfrac{3\delta}{2} + 3 - 3 + \tfrac{q-1}{2} - \tfrac{3\delta}{2} + 3\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

Note that in this case we set $\sigma_i = 2/j = -1$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

(v). Else if loop (2) ends but no $\mathcal{D}(c'^{(i,j)})$ returns "$False$", then $(ux^i)_1 \notin \{-2, -1, 1, -2\}$. However $(ux^i)_1 \in \{-2, -1, 0, 1, -2\}$, so it must be $(ux^i)_1 = 0$. Noted it initiates $\sigma_i = 0$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

For $i = p - 1$, noted that $(ux^i)_1 = (ux^{p-1})_1 = u_1 + u_2 \in \{1, 2, 3\}$, we discuss in the following cases:

(vi). Assume that loop (3) ends when $j = 1$, then

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot u + 3\delta \cdot ux^{ui},$$

where $u = fx^L$. Noted $u_1 = 2$, we have $w_1^{(i,j)} = w_1'^{(i,j)} + 6\eta^{(i,j)} + 3\delta(ux^i)_1$. According to lemma 3, $\mathcal{D}(c^{(i,j)}) \to$ "$False$" if an only if $w_1^{(i,j)} > \frac{q-1}{2}$. If $(ux^i)_1 \leq 2$, it implies that

$$\begin{aligned} w_1^{(i,j)} &\leq |w_1'^{(i,j)}| + 6(\tfrac{1}{2} + \tfrac{q-1-15\delta}{12}) + 6\delta \\ &< \tfrac{3\delta}{2} - 3 + 3 + \tfrac{q-1}{2} - \tfrac{15\delta}{2} + 66\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

This is contradictory to the assumption, so $(ux^i)_1 = 3$.
It also needs to show that when $(ux^i)_1 = 3$, it must hold that $\mathcal{D}(c^{(i,j)}) \to$ "$False$". Given $(ux^i)_1 = 3$, then

$$\begin{aligned} w_1^{(i,j)} &\geq -|w_1'^{(i,j)}| + 6(-\tfrac{1}{2} + \tfrac{q-1-3\delta}{12}) + 9\delta \\ &> -\tfrac{3\delta}{2} + 3 - 3 + \tfrac{q-1}{2} - \tfrac{15\delta}{2} + 9\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

Note that in this case we set $\sigma_i = \lceil 3/j \rceil = 3$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

(vii). Assume that loop (3) ends when $j = 2$, then

$$w^{(i,j)} = w'^{(i,j)} + 3\eta^{(i,j)} \cdot u + 3\delta \cdot ux^i,$$

where $u = fx^L$. Note that $u_1 = 2$, we have $w_1^{(i,j)} = w_1'^{(i,j)} + 6\eta^{(i,j)} + 3\delta(ux^i)_1$.
According to lemma 3, $\mathcal{D}(c^{(i,j)}) \rightarrow$ "*False*" if an only if $w_1^{(i,j)} > \frac{q-1}{2}$. If $(ux^i)_1 \leq 1$, it implies that

$$\begin{aligned} w_1^{(i,j)} &\leq |w_1'^{(i,j)}| + 6(\tfrac{1}{2} + \tfrac{q-1-9\delta}{12}) + 3\delta \\ &< \tfrac{3\delta}{2} - 3 + 3 + \tfrac{q-1}{2} - \tfrac{9\delta}{2}3\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

This is contradictory to the assumption, so $(ux^i)_1 = 2$.
It also needs to show that when $(ux^i)_1 = 2$, it must hold that $\mathcal{D}(c^{(i,j)}) \rightarrow$ "*False*". Given $(ux^i)_1 = 2$, then

$$\begin{aligned} w_1^{(i,j)} &\geq -|w_1'^{(i,j)}| + 6(-\tfrac{1}{2} + \tfrac{q-1-3\delta}{12}) + 6\delta \\ &> -\tfrac{3\delta}{2} + 3 - 3 + \tfrac{q-1}{2} - \tfrac{9\delta}{2} + 6\delta \\ &= \tfrac{q-1}{2} \end{aligned}$$

Note that in this case we set $\sigma_i = \lceil 3/j \rceil = 3$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

(viii). Else if loop (3) ends but no $\mathcal{D}(c'^{(i,j)})$ returns "*False*", then $(ux^i)_1 \notin \{2, 3\}$. However $(ux^i)_1 \in \{1, 2, 3\}$, so it must be $(ux^i)_1 = 1$. Noted that it initiates $\sigma_i = 1$, it follows that

$$u_{p-i} + u_{p-i+1} = \sigma_i.$$

Suppose $u_1 = -2$, it is easy to check that the coefficients of $-fx^L$ satisfy the equations 2.

Let $u' = \phi^{-1}(u'_0, u'_1, \cdots, u'_{p-1})$, we have either $u' = fx^L$ or $u' = -fx^L$. Since x is invertible in $\mathcal{R}$, we have either $f = u'x^{-L}$ or $f = -u'x^{-L}$.

□

It remains to show that there exists available integers δ, s, such that the probability $(1 - 2e^{-\frac{s^2}{80t}})$ is big enough. First, we consider an instance – Streamlined NTRU Prime 4591^{761}, which appears in [2] as an example. Its parameter setting is $(p, q, t) = (761, 4591, 143)$. We choose $(\delta, s) = (170, 234)$, then the probability is about $(1 - 2e^{-\frac{234^2}{80 \cdot 143}}) \approx 0.9833$. In general, the parameter (p, q, t) of an instance of Streamlined NTRU Prime should follows the restriction: $t \geq 1$; $p \geq 3t$; $q \geq 32t+1$, and p, q are two primes. If we take $q = 32t$, $\delta \approx \frac{32t}{27}$ and $s \approx \frac{32t}{18} - 21$, then $(1-2e^{-\frac{s^2}{80t}}) \approx (1-2e^{-\frac{16(t-12)^2}{405t}})$. It is easy to check that this probability increase with increasing of t. In all the suggested parameter sets listed in [2], the smallest three values for the t are $27, 39, 44$. By simple calculation, we have $(1-2e^{-\frac{16(44-12)^2}{405\cdot 44}}) \approx 0.2024$.

In Algorithm 2, to guarantee each querying ciphertext $c^{(i,j)}$ satisfying $3|c^{(i,j)}$, we introduce $\rho^{(i,j,1)} \cdot x^L$ and $\rho^{(i,j,2)} \cdot x^{L+i}$. In order to bound $\|w'^{(i,j)}\|_{l_\infty} < \frac{3\delta}{2} - 3$, the parameter s must satisfy $s < \frac{3\delta}{2} - 21$. This reduces the advantage of our attack. Another impact to the advantage of our attack is the parameter δ. In order to bound $|w_k^{(i,j)}| < \frac{q-1}{2}$, for $k = 0, 2, \cdots, p-1$, the parameter δ must satisfy $\delta \leq \frac{q-1}{27} + 2$. If the parameters can be improved, our attack will gain more advantages. The following methods can be taken into consideration to improve the attack:

1). Reduce the upper bound of $\|gr + 3fm\|_{l_\infty}$. For example, use some lattice-based or code-based algorithm to find some r such that the corresponding m has small l_1 norm.

2). Adaptively collect the equations. For example, only collect the equations with the right side $\sigma_i \leq 2$, this will allow a bigger δ.

4 Conclusion

In this paper, we proposed an attack on Streamlined NTRU Prime. This attack is under the chosen-ciphertext attack model, and aims to recover the private key. Our attack has the following meanings:

1). It recovers the private key for most parameter setting of Streamlined NTRU Prime.

2). It discloses an interesting fact that the security of Streamlined NTRU Prime decreases with the increasing of the parameter t.

3). It shows an evidence that the "KEM" approach does not always transform a weakly secure PKE to an IND-CPA one.

References

1. D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "Ntru prime." *IACR Cryptology ePrint Archive*, vol. 2016, p. 461, 2016.
2. ——, "Ntru prime: reducing attack surface at low cost," in *International Conference on Selected Areas in Cryptography.* Springer, 2017, pp. 235–260.
3. J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in *International Algorithmic Number Theory Symposium.* Springer, 1998, pp. 267–288.
4. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange-a new hope." in *USENIX Security Symposium*, vol. 2016, 2016.
5. M. Albrecht, S. Bai, and L. Ducas, "A subfield lattice attack on overstretched ntru assumptions," in *Annual Cryptology Conference.* Springer, 2016, pp. 153–178.

6. P. Kirchner and P.-A. Fouque, "Comparison between subfield and straightforward attacks on ntru." *IACR Cryptology ePrint Archive*, vol. 2016, p. 717, 2016.
7. C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Annual International Cryptology Conference*. Springer, 1991, pp. 433–444.
8. E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Annual International Cryptology Conference*. Springer, 1999, pp. 537–554.
9. ——, "Secure integration of asymmetric and symmetric encryption schemes," *Journal of cryptology*, vol. 26, no. 1, pp. 80–101, 2013.
10. V. Shoup, "A proposal for an iso standard for public key encryption (version 2.1)," *IACR e-Print Archive*, vol. 112, 2001.
11. A. W. Dent, "A designers guide to kems," in *IMA International Conference on Cryptography and Coding*. Springer, 2003, pp. 133–151.
12. N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. Whyte, "The impact of decryption failures on the security of ntru encryption," in *Annual International Cryptology Conference*. Springer, 2003, pp. 226–246.
13. Q. Guo, T. Johansson, and P. Stankovski, "A key recovery attack on mdpc with cca security using decoding errors," in *International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT*. Springer, 2016, pp. 789–815.
14. W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American statistical association*, vol. 58, no. 301, pp. 13–30, 1963.