Cryptanalysis of NTRU with Two Public Keys

Abderrahmane Nitaj
(Corresponding author: Abderrahmane Nitaj)
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse Normandie, France
(Email: abderrahmane.nitaj@unicaen.fr)
(Received July 20, 2012; revised and accepted Mar. 10, 2013)

Abstract

NTRU is a fast public key cryptosystem presented in 1996 by Hoffstein, Pipher and Silverman. It operates in the ring of truncated polynomials. In NTRU, a public key is a polynomial defined by the combination of two private polynomials. In this paper, we consider NTRU with two different public keys defined by different private keys. We present a lattice-based attack to recover the private keys assuming that the public keys share polynomials with a suitable number of common coefficients.

Keywords: Cryptanalysis, lattice attacks, NTRU cryptosystem

1 Introduction

The NTRU Public Key Cryptosystem is a ring-based cryptosystem that was first introduced in the rump session at Crypto'96 [5]. It is one of the fastest public-key cryptosystems, offering both encryption (NTRUencrypt) and digital signatures (NTRUSign). It is a relatively new cryptosystem that appears to be more efficient than the current and more widely used public-key cryptosystems, such as RSA [9] and ElGamal [4]. It is well known that the security of RSA and ElGamal relies on the difficulty of factoring large composite integers or computing discrete logarithms. However, in 1994, Shor [11] showed that quantum computers can be used to factor integers and to compute discrete logarithms in polynomial time. Since NTRU does not rely on the difficulty of factoring or computing discrete logarithms and is still considered secure even against quantum computer attacks, it is a promising alternative to the more established public key cryptosystems. In [5], Hoffstein, Pipher and Silverman have studied different possible attacks on NTRU. The brute force and the meet-in-the-middle attacks may be used against the private key or against a single message but will not succeed in a reasonable time. The multiple transmission attack also will fail for a suitable choice of parameters. However, we notice that NTRU suggests that the public key should be changed very frequently, for each transmission if possible. The most important attack, presented by Coppersmith and Shamir [3] in 1997 makes use of the LLL algorithm of Lenstra, Lenstra and Lovász [6]. Coppersmith and Shamir constructed a lattice generated by the public key and found a factorization of the public key that could be used to break the system if the NTRU parameters are poorly set.

The NTRU cryptosystem depends on three integer parameters (N, p, q) and four sets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_r$, $\mathcal{L}_m$ of polynomials of degree $N-1$ with small integer coefficients. Let $\mathbb{Z}_q$ denote the ring of integers modulo q. The operations of NTRU took place in the ring of truncated polynomials $\mathbb{Z}_q[X]/\left(X^N-1\right)$. In this ring, the addition of two polynomials is defined as pairwise addition of the coefficients of the same degree and multiplication, noted " $*$ " is defined as convolution multiplication. In NTRU, to create a public key h, one chooses a private key (f, g) composed with two polynomials f and g and computes

$$h = f_q^{-1} * g \in \mathbb{Z}_q[X]/\left(X^N-1\right),$$

where f_q^{-1} is the inverse of f in $\mathbb{Z}_q[X]/\left(X^N-1\right)$.

In this paper, we consider NTRU with two public keys h, h' defined by the private keys (f, g) and (F', G') with

$$h' = F_q'^{-1} * G' \pmod q.$$

Since f is invertible in $\mathbb{Z}_q[X]/\left(X^N-1\right)$, then we can define $g' = f * h' \pmod q$ so that

$$h' = f_q^{-1} * g' \mod q.$$

The main objective of this paper is to show how to find the private key (f, g) when

$$\|g - g'\| < \min(\|g\|, \|g'\|).$$

Using h and h', we construct a lattice $\mathcal{L}(h, h')$ of dimension $2N$, and applying the lattice basis reduction algorithm LLL, we show that short vectors in $\mathcal{L}(h, h')$ can be used to find the private polynomials f, g, g' when $\|g - g'\| < \min(\|g\|, \|g'\|)$. Under this condition, it is important to notice that our method is more efficient than

the method of Coppersmith and Shamir to recover the private key (f, g) using the public key h.

We note that when the polynomials g, g' are generated randomly and independently, then with overwhelming probability the condition $\|g - g'\| < \min(\|g\|, \|g'\|)$ is not satisfied. So in practice one can easily avoid this inequality.

Similarly, assume that $h' = F_q'^{-1} * G' \pmod q$ is invertible in $\mathbb{Z}_q[X]/\left(X^N - 1\right)$. Then we can define a polynomial f' as

$$f' = h_q'^{-1} * g \pmod q,$$

where $h_q'^{-1}$ is the inverse of h' in $\mathbb{Z}_q[X]/\left(X^N - 1\right)$. Using lattice reduction techniques, we show that it is possible to recover the private key (f, g) assuming that the condition $\|f - f'\| < \min(\|f\|, \|f'\|)$ is fulfilled.

The paper is organized as follows. In Section 2, we give motivation for our work. Section 3 gives a brief mathematical description of NTRU and introduces the LLL algorithm as well as the attack of Coppersmith and Shamir on NTRU. In Section 4, we present our new attack on NTRU with two private keys (f, g) and (f, g') with $\|g - g'\| < \min(\|g\|, \|g'\|)$ and compare it with the attack of Coppersmith and Shamir. In Section 5, we present our new attack on NTRU when h and h' are invertible and $\|f - f'\| < \min(\|f\|, \|f'\|)$. We conclude the paper in Section 6.

2 Motivation

RSA, the most commonly used public-key cryptosystem [9] has stood up remarkably well to years of extensive cryptanalysis and is still considered secure by the cryptographic community (see [1] for more details). Various schemes and digtal signatures are based on the same problem behind RSA (see e.g. [2] and [13]). Indeed, RSA derives its security from the difficulty of factoring large numbers of the shape $N = pq$ where p, q are large unknown primes of the same bit-size. In some cases, the problem can be slightly easier given two RSA modulus $N = pq$, $N' = p'q'$. If $p = p'$, then it is trivial to factor N and N' by computing $\gcd(N, N')$. However, it is possible to factor N and N' when p and p' share a certain amount of bits (see [8, 10]).

The first paper studying NTRU was written by Coppersmith and Shamir [3] in 1997. In that paper, they noted that the best way to attack the NTRU cryptosystem was via the techniques of lattice reduction. Nevertheless, the security of NTRU is also based on the following factorization problem: Given a polynomial $h \in \mathbb{Z}[X]/\left(X^N - 1\right)$, find two short polynomials $f \in \mathbb{Z}[X]/\left(X^N - 1\right)$ and $g \in \mathbb{Z}[X]/\left(X^N - 1\right)$ such that $h = f_q^{-1} * g \pmod q$, where f_q^{-1} is the inverse of f in $\mathbb{Z}_q[X]/\left(X^N - 1\right)$.

Similarly to RSA with two modulus, consider NTRU with two public keys h and h' defined by the same parameters (N, p, q). Assume that $h = f_q^{-1} * g \pmod q$. Then, h' can be expressed as $h' = f_q^{-1} * g' \pmod q$ where $g' = f * h' \pmod q$. The main contribution of this paper is to show how to find the private keys (f, g) when g and g' satisfy $\|g - g'\| < \min(\|g\|, \|g'\|)$.

We notice that lattice-based cryptography is currently seen as one of the most promising alternatives to cryptography based on number theory. Given recent advances in lattice-based cryptography (see [7] and [12]), studying NTRU and related schemes is both useful and timely. In this direction, our work shows that using the same f or the same g in generating public keys h, h' is likely to reduce the security of NTRU.

3 Mathematical Background

In this section, we give a brief description of the NTRU encryption and the LLL algorithm for lattice reduction and the well known attack of Coppersmith and Shamir on NTRU. Further details can be found in [3] and [5].

3.1 Definitions and Notations

We start by introducing the ring

$$\mathcal{R} = \mathbb{Z}[X]/(X^N - 1),$$

upon which NTRU operates. We use $*$ to denote a polynomial multiplication in $\mathcal{R}$, which is the cyclic convolution of two polynomials. If

$$\begin{aligned} f &= (f_0, f_1, \cdots, f_{N-1}) = \sum_{i=0}^{N-1} f_i X^i, \\ g &= (g_0, g_1, \cdots, g_{N-1}) = \sum_{i=0}^{N-1} g_i X^i, \end{aligned}$$

are polynomials of $\mathcal{R}$, then $h = f * g$ is given by $h = (h_0, h_1, \cdots, h_{N-1})$, where h_k is defined for $0 \le k \le N-1$ by

$$\begin{aligned} h_k &= \sum_{i+j \equiv k \mod N} f_i g_j \\ &= \sum_{i=0}^{k} f_i g_{k-i} + \sum_{i=k+1}^{N-1} f_i g_{N+k-i}. \end{aligned}$$

The Euclidean norm or the length of a polynomial $f = (f_0, f_1, \cdots, f_{N-1})$ is defined as

$$\|f\| = \sqrt{\sum_{i=0}^{N-1} f_i^2}.$$

One more notation is the binary set of polynomials $\mathcal{B}(d)$ defined for a positive integers d by

$$\mathcal{B}(d) = \{f(X) = \sum_{i=0}^{N-1} f_i X^i, \text{ where } f_i \in \{0, 1\}, \sum_{i=0}^{N-1} f_i = d\}.$$

In other words, $\mathcal{B}(d)$ is the set of polynomials of $\mathcal{R}$ with d coefficients equal to 1 and all the other coefficients equal to 0.

Different descriptions of NTRU Encrypt and different proposed parameter sets have been in circulation since 1996. The 2005 instantiation of NTRU is set up by six public integers N, p, q, d_f, d_g, d_r and four public spaces $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$, $\mathcal{L}_r$ such that

- N is prime and sufficiently large to prevent lattice attacks.
- p and q are relatively prime.
- q is much larger than p.
- $\mathcal{L}_f$ is a set of small polynomials from which the private keys are selected.
- $\mathcal{L}_g$ is a similar set of small polynomials from which other private keys are selected.
- $\mathcal{L}_m$ is the plaintext space. It is a set of polynomials $m \in \mathbb{Z}_p[X]/(X^N - 1)$ that represent encrypted table messages.
- $\mathcal{L}_r$ is a set of polynomials from which the blinding value used during encryption is selected.

3.2 The NTRU Encryption Scheme

3.2.1 Key Pair Generation

To create a NTRU key, one randomly chooses a polynomial $f \in \mathcal{L}_f$ and a polynomial $g \in \mathcal{L}_g$. The polynomial f must satisfy the additional requirement that it has an inverse f_p^{-1} modulo p and an inverse f_q^{-1} modulo q, that is

$$f * f_p^{-1} = 1 \pmod{p}, \qquad f * f_q^{-1} = 1 \pmod{q}.$$

Then the private key is f and the public key is the polynomial

$$h = f_q^{-1} * g \pmod{q}.$$

We recall that N, p, q are also public.

3.2.2 Encryption.

To encrypt a message $m \in \mathcal{L}_m$, one randomly chooses a polynomial $r \in \mathcal{L}_r$. The ciphertext is the polynomial

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

3.2.3 Decryption

To decrypt an encrypted message e using the private key f, one computes

$$a = f * e \mod q,$$

where the coefficients of a lie between $-q/2$ and $q/2$. The message m is then obtained from a by reducing the coefficients of $f_p^{-1} * a$ modulo p.

3.3 The LLL Algorithm

Since lattice reduction is an essential tool for our attack, let us recall a few facts about lattices and reduced basis. Let $u_1, \ldots, u_n \in \mathbb{R}^m$ be linearly independent vectors with $n \leq m$. The lattice L spanned by $(u_1, \ldots, u_n)$ consists of all integral linear combinations of $u_1, \ldots, u_n$, that is

$$L = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n = \left\{ \sum_{i=1}^{n} b_i u_i, \;\middle|\; b_i \in \mathbb{Z} \right\}.$$

The set $(u_1, \ldots, u_n)$ is called a lattice basis. A lattice can be conveniently represented by a matrix B whose rows are the vectors $u_1, \ldots, u_n$. The determinant of the lattice L is defined as

$$\det(L) = \sqrt{\det(BB^T)}.$$

Any two bases of the same lattice L are related by some integral matrix of determinant ± 1.

There are several natural computational problems relating to lattices. An important problem is the shortest vector problem (SVP): given a basis matrix B for L, compute a non-zero vector $v \in L$ such that $\|v\|$ is minimal.

In 1982, Lenstra et al. [6] introduced the LLL reduction algorithm which produces an LLL-reduced basis $b_1, \ldots, b_n$ of L with the following property

$$\|b_1\| \leq \|b_2\| \leq \ldots \leq \|b_i\| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \det(L)^{\frac{1}{n+1-i}},$$

for $i = 1, \ldots, n$. With $i = 1$, this implies that $\|b_1\|$ satisfies $\|b_1\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}$. In comparison, a theorem of Minkowski asserts that any lattice L of dimension n contains a non-zero vector v with

$$\|v\| \leq \sqrt{\frac{2n}{e\pi}} \det(L)^{\frac{1}{n}}.$$

On the other hand, the Gaussian heuristic says that the length of the shortest non-zero vector is usually approximately $\sigma(L)$ where

$$\sigma(L) = \sqrt{\frac{n}{2\pi e}} \det(L)^{\frac{1}{n}}.$$

3.4 The Attack of Coppersmith and Shamir on NTRU

In [3] Coppersmith and Shamir presented a lattice attack on NTRU. They defined a lattice determined by the parameters N, q, h of the system and showed that recovering the secret key (f, g) from the public key h is reduced to finding a shortest vector of the lattice. Let $h = (h_0, h_1, \cdots, h_{N-1})$ be the public key. The NTRU lattice L is the lattice of dimension $2N$ generated by the

row vectors of a matrix of the following form

$$M(L) = \begin{bmatrix} lI_N & H \\ 0 & qI_N \end{bmatrix} = \left[\begin{array}{cccc|cccc} l & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & l & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & l & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right].$$

Since $h = f_q^{-1} * g \pmod q$, then $f * h - qu = g$ for some $u \in \mathcal{R}$ and

$$(f, -u) * M(L) = (f, -u) * \begin{bmatrix} lI_N & H \\ 0 & qI_N \end{bmatrix} = (lf, g).$$

So the vector (lf, g) is a short vector in the NTRU lattice L, which is with high probability the shortest vector of L. Hence, an attacker uses lattice reduction algorithms to find (f, g) from L, then he can recover the private keys. More precisely, the Gaussian heuristic says that the length of the shortest non-zero vector is usually approximately $\sigma(L)$ where

$$\begin{aligned} \sigma(L) &= \sqrt{\frac{\dim(L)}{2\pi e}} (\det L)^{1/\dim(L)} \\ &= \sqrt{\frac{2N}{2\pi e}} (lq)^{\frac{N}{2N}} \\ &= \sqrt{\frac{lqN}{\pi e}}. \end{aligned}$$

Hence, in order to maximize the probability of breaking the NTRU system using lattice reduction, the attacker should choose l to minimize the ratio

$$c = \frac{\|(lf, g)\|}{\sigma(L)} = \frac{\sqrt{l^2\|f\|^2 + \|g\|^2}}{\sqrt{\frac{lqN}{\pi e}}}.$$

This occurs for $l = \|g\|/\|f\|$ which leads to

$$c = \sqrt{\frac{2\pi e \|g\| \|f\|}{qN}}. \quad (1)$$

The ratio c measures how much smaller the key is compared to the expected smallest vector. If c is very small then we expect a lattice reduction algorithm as LLL to have an easier time finding it.

4 The New Attack when $\|g - g'\| < \min(\|g\|, \|g'\|)$

4.1 The New Lattice

Let

$$h(X) = \sum_{i=0}^{N-1} h_i X^i, \quad h'(X) = \sum_{i=0}^{N-1} h'_i X^i,$$

be two NTRU public keys created by the private polynomials (f, g) and (F', G') with the same parameters $(N, p, q, d_f, d_g, d_r, d_m)$, that is

$$\begin{aligned} h &= f_q^{-1} * g \pmod q, \\ h' &= F_q'^{-1} * G' \pmod q. \end{aligned}$$

Let $g' = f * h' \pmod q$. Then

$$h' = f_q^{-1} * g' \pmod q.$$

For a positive constant l, define the lattice

$$\begin{aligned} &\mathcal{L}(h, h') \\ &= \{(lv, w) \in \mathcal{R}^2 : \\ &\text{where } w = v * (h - h') \pmod q\}. \end{aligned}$$

This is a $2N$-dimension lattice spanned by the matrix

$$M(h, h') = \begin{bmatrix} lI_N & H - H' \\ 0 & qI_N \end{bmatrix},$$

where $H - H'$ is the circulant matrix

$$\begin{bmatrix} h_0 - h'_0 & h_1 - h'_1 & \cdots & h_{N-1} - h'_{N-1} \\ h_{N-1} - h'_{N-1} & h_0 - h'_0 & \cdots & h_{N-2} - h'_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 - h'_1 & h_2 - h'_2 & \cdots & h_0 - h'_0 \end{bmatrix}.$$

The matrix $M(h, h')$ has the following property.

Proposition 1. *Let h, h' be two NTRU public keys. Assume that*

$$f * h = g + qu, \qquad f * h' = g' + qu'.$$

Then the vector $(lf, g - g')$ is in the lattice $\mathcal{L}(h, h')$ and

$$(f, -u + u') * M(h, h') = (lf, g - g').$$

Proof. Assume that $f * h = g + qu$ and $f * h' = g' + qu'$. Substracting the two equalities, we get

$$f * h - f * h' = f * (h - h') = g - g' \pmod q.$$

This implies that the vector $(lf, g - g')$ is in $\mathcal{L}(h, h')$. Next, we have

$$\begin{aligned} &(f, -u + u') * M(h, h') \\ &= (f, -u + u') * \begin{bmatrix} lI_N & H - H' \\ 0 & qI_N \end{bmatrix} \\ &= (lf, g - g'). \end{aligned}$$

This terminates the proof. □

4.2 The Gaussian Heuristics

For a random lattice L, the Gaussian heuristic says that the length of the shortest non-zero vector is approximately

$$\sigma(L) = \sqrt{\frac{\dim(L)}{2\pi e}} \det L^{1/\dim(L)}.$$

The dimension and determinant of $\mathcal{L}(h,h')$ are given by

$$\dim(\mathcal{L}(h,h')) = 2N, \qquad \det(\mathcal{L}(h,h')) = l^N q^N.$$

Hence for the lattice $\mathcal{L}(h,h')$, we have

$$\sigma(\mathcal{L}(h,h')) = \sqrt{\frac{lNq}{\pi e}}.$$

Let us define the ratio

$$c_1 = \frac{\|(lf, g-g')\|}{\sigma(\mathcal{L}(h,h'))}.$$

So c_1 is the ratio of the length of the target vector to the length of the expected shortest vector. The smaller the value of c_1, the easier it will be to find the target vector. Thus, the idea to increase the chances of LLL to find $(lf, g-g')$ is to choose l such that $\|(lf, g-g')\|$ is as small as possible compared to $\sigma(\mathcal{L}(h,h'))$. In $\mathcal{L}(h,h')$, we have

$$\|(lf, g-g')\| = \sqrt{l^2\|f\|^2 + \|g-g'\|^2}.$$

It turns out that we should choose

$$l = \frac{\|g-g'\|}{\|f\|}.$$

This implies that the ratio c_1 satisfies

$$c_1 = \sqrt{\frac{2\pi e\|g-g'\|\|f\|}{qN}}.$$

Let us compare the ratio c_1 and the ratio c as defined by (1) in the the attack of Coppersmith and Shamir. Our attack will be more efficient when $c_1 < c$. This leads to the following condition

$$\|g-g'\| < \min(\|g\|, \|g'\|).$$

5 The New Attack when $\|f-f'\| < \min(\|f\|, \|f'\|)$

5.1 The New Lattice

Let $h = f_q^{-1} * g \pmod q$ and $h' = F_q'^{-1} * G' \pmod q$ be two NTRU public keys with the same parameters $(N, p, q, d_f, d_g, d_r, d_m)$. In this section, we assume that h, h' are invertible in $\mathbb{Z}_q[X]/\left(X^N-1\right)$. Let h_q and h'_q be their inverses. Define $f' = g * h'_q$. We have

$$g * h_q = f \pmod q, \qquad g * h'_q = f' \pmod q.$$

Let

$$h_q(X) = \sum_{i=0}^{N-1} h_{q,i}X^i, \qquad h'_q(X) = \sum_{i=0}^{N-1} h'_{q,i}X^i,$$

be the representations of $h_q(X)$ and $h'_q(X)$ in $\mathbb{Z}_q[X]/\left(X^N-1\right)$. For a positive constant l, define the $2N$ dimension lattice

$$\mathcal{L}_q(h,h') = \left\{(lv, w) \in \mathcal{R}^2 : w = v * \left(h_q - h'_q\right) \pmod q\right\}.$$

The lattice is generated by the row vectors of the matrix $M_q(h,h')$ given below

$$M_q(h,h') = \begin{bmatrix} lI_N & H_q - H'_q \\ 0 & qI_N \end{bmatrix},$$

where $H_q - H'_q$ is the circulant matrix

$$\begin{bmatrix} h_{q,0} - h'_{q,0} & \cdots & h_{q,N-1} - h'_{q,N-1} \\ h_{q,N-1} - h'_{q,N-1} & \cdots & h_{q,N-2} - h'_{q,N-2} \\ \vdots & \ddots & \vdots \\ h_{q,1} - h'_{q,1} & \cdots & h_{q,0} - h'_{q,0} \end{bmatrix}.$$

The matrix $M_q(h,h')$ has the following property.

Proposition 2. *Let h, h' be two NTRU public keys and h_q, h'_q their inverses in $\mathbb{Z}_q[X]/\left(X^N-1\right)$. Assume that*

$$g * h_q = f + qv, \qquad g * h'_q = f' + qv'.$$

Then the vector $(lg, f-f')$ is in the lattice $\mathcal{L}_q(h,h')$ and

$$(g, -v+v') * M_q(h,h') = (lg, f-f').$$

Proof. Assume that $g * h_q = f + qv$ and $g * h'_q = f' + qv'$. Then $g * h_q = f \pmod q$ and $g * h'_q = f' \pmod q$. This gives $g * (h_q - h'_q) = f - f' \pmod q$ and it follows that the vector $(lg, f-f')$ is in $\mathcal{L}_q(h,h')$. More precisely,

$$\begin{aligned} &(g, -v+v') * M_q(h,h') \\ &= (g, -v+v') * \begin{bmatrix} lI_N & H_q - H'_q \\ 0 & qI_N \end{bmatrix} \\ &= (lg, f-f'). \end{aligned}$$

This terminates the proof. □

5.2 The Gaussian Heuristics

We can apply the the Gaussian heuristic to the lattice $\mathcal{L}_q(h,h')$. The shortest non-zero vector is approximately

$$\begin{aligned} &\sigma(\mathcal{L}_q(h,h')) \\ &= \sqrt{\frac{\dim(\mathcal{L}_q(h,h'))}{2\pi e}} \det \mathcal{L}_q(h,h')^{1/\dim(\mathcal{L}_q(h,h'))} \\ &= \sqrt{\frac{lNq}{\pi e}}. \end{aligned}$$

To compare the length of the target vector $(lg, f-f')$ to the length of the expected shortest vector $\sigma(\mathcal{L}_q(h,h'))$, we consider the ratio

$$c_2 = \frac{\|(lg, f-f')\|}{\sigma(\mathcal{L}_q(h,h'))}.$$

In order to increase the chances of LLL to find the vector $(lg, f-f')$, the attacker chooses the balancing constant l to make c_2 as small as possible. For the lattice $\mathcal{L}_q(h,h')$, we have

$$\|(lg, f-f')\| = \sqrt{l^2\|g\|^2 + \|f-f'\|^2}.$$

Hence the optimal choice for l is

$$l = \frac{\|f - f'\|}{\|g\|}.$$

which leads to

$$c_2 = \sqrt{\frac{2\pi e \|f - f'\| \|g\|}{qN}}.$$

To increase the chance of this attack to find $(lg, f - f')$ comparatively to the attack of Coppersmith and Shamir, we should have $c_2 < c$ where c is the constant defined by (1). This gives the condition

$$\|f - f'\| < \min\left(\|f\|, \|f'\|\right).$$

6 Conclusion

We have shown that choosing two NTRU public keys $h = f_q^{-1} * g \pmod q$ and $h' = F_q'^{-1} * G' \pmod q$ could be insecure in some cases. Rewriting h' as $h' = f_q^{-1} * g' \pmod q$, where $g' = f * h' \pmod q$, we have shown, that using lattice reduction techniques, it is possible to find the private key (f, g) when $\|g - g'\| < \min\left(\|g\|, \|g'\|\right)$. We have shown that the same techniques apply when h' is invertible modulo q and $\|f - f'\| < \min\left(\|f\|, \|f'\|\right)$. Here f' is defined by the equality $f' * h' = g \pmod q$. For implementations of NTRU key pair generation we recommend to build in a check for $\|g - g'\| > \min\left(\|g\|, \|g'\|\right)$ and $\|f - f'\| > \min\left(\|f\|, \|f'\|\right)$. This is very easy to implement, and will only in extremely rare cases imply that the key pair is to be rejected. The main reason is that when f, g, F' and G' are generated randomly, the probability that g and $g' = f * h' \pmod q$ share an important amount of monomials is negligible. Similarly, the probability that f and $f' = g * h'^{-1} \pmod q$ share an important amount of monomials is also negligible.

References

[1] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices of the American Mathematical Society*, vol. 46, no. 2, pp. 203–213, 1999.

[2] Z. Cao, "Universal encrypted deniable authentication protocol," *International Journal of Network Security*, vol. 8, no. 2, pp. 151–158, 2009.

[3] D. Coppersmith and A. Shamir, "Lattice attacks on NTRU," in *Advances in Cryptology-Eurocrypt '97*, LNCS 1233, pp. 52–61, Springer-Verlag, 1997.

[4] T. El Gamal, "A public key cryptosystem and signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 496–473, 1985.

[5] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring based public key cryptosystem in algorithmic number theory," in *Algorithmic Number Theory*, LNCS 1423, pp. 267–288, Springer-Verlag, 1998.

[6] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 513–534, 1982.

[7] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology-Eurocrypt 2010*, LNCS 6110, pp. 1–23, Springer-Verlag, 2010.

[8] A. May and M. Ritzenhofen, "Implicit factoring: On polynomial time factoring given only an implicit hint," in *Stanislaw Jarecki and Gene Tsudik, editors, Public Key Cryptography*, LNCS 5443, pp. 1–14, Springer-Verlag, 2009.

[9] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[10] S. Sarkar and S. Maitra, "Further results on implicit factoring in polynomial time," *Advances in Mathematics of Communications*, vol. 3, no. 2, pp. 205–217, 2009.

[11] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Computing*, vol. 26, no. 2, pp. 1484–1509, 1997.

[12] D. Stehlé and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices," in *Advances in Cryptology - Eurocrypt '11*, LNCS 6632, pp. 27–47, Springer-Verlag, 2011.

[13] B. Yang, H. Ma, and S. Zhu, "A traitor tracing scheme based on the RSA system," *International Journal of Network Security*, vol. 5, no. 2, pp. 182–186, 2007.

Abderrahmane Nitaj received his Ph.D. degree from Caen University, Basse Normandie in 1994. Now he is an associate researcher at Caen University, Basse Normandie and mainly interested in cryptography, information security, designing secure and efficient cryptographic schemes and number theory.