数理解析研究所講究録
第1649巻 2009年 217-221

NFALSE: 多項式環に基づくより高速な公開鍵暗号

NFALSE: Another Ring-Based Public Key Cryptosystem with Faster Encryption

Keita Xagawa * Keisuke Tanaka *

Abstract— We propose a variant of NTRU, whose main feature is fast encryption and decryption; the time complexity is almost linear time in a security parameter. While NTRU is defined over a ring $\mathbb{Z}[X]/\langle X^n - 1\rangle$, ours over $\mathbb{Z}[X]/\langle X^n + 1\rangle$, where n is the power of 2. This change admits us to use FFT and prevents Gentry's folding attack.

Keywords: NTRU, almost linear-time encryption, lattice-based cryptography.

1 Introduction

At the beginning of the research on public-key encryption, many researchers studied fast encryption procedure, since the encryption procedure costs $\tilde{O}(n^3)$ steps in the RSA and the ElGamal cryptosystems, where n is the security parameter.

In 1996, Hoffstein, Pipher, and Silverman proposed a fast ring-based encryption scheme, NTRU [8]. The ring is mainly $\mathbb{Z}_q[X]/\langle X^n - 1\rangle$, denoted by $\mathcal{R}_{X^n-1,q}$. The public key in NTRU is $\boldsymbol{h} \in \mathcal{R}_{X^n-1,q}$. For a plaintext $\boldsymbol{m} \in \mathcal{L}(d)$ and a randomness $\boldsymbol{r} \in \mathcal{L}(d)$, the ciphertext is obtained by

$$\boldsymbol{c} = \boldsymbol{h} \otimes \boldsymbol{r} + \boldsymbol{m},$$

where $\mathcal{L}(d)$ denotes the set of $\{0,1\}$-coefficient polynomials of degree at most $n-1$ with exactly d coefficients set to 1 and $\otimes$ denotes the multiplicative operation in $\mathcal{R}_{X^n-1,q}$. The main feature of NTRU is faster encryption and decryption than that of the RSA and the ElGamal cryptosystems. In precise, time complexity of each algorithm for encryption and decryption is $O(n^2 \log^2 q)$ in NTRU.

On real implementations, Bailey, Coffin, Elbirt, Silverman, and Woodbury implemented NTRU in constrained devices with encryption taking $O(n^2 \log q)$ costs. Lee, Kim, Song, and Park [12], and Buchmann, Döring, and Lindner [2] reported efficient software implementations for NTRU, whose encryption cost is $O(dn \log q)$ in the worst case.

There were attempts for faster encryption for NTRU by modifying the parameters. In [17], Silverman observed that setting $n = 2^k$ allows us to use FFT and the encryption cost is reduced to $\tilde{O}(n \log^2 q)$. Gentry observed that $X^{2^k} - 1 = (X^{2^{k-1}} - 1)(X^{2^{k-1}} + 1)$ over $\mathbb{Z}$ and this induces a ring homomorphism. By this observation, he succeeded an attack for NTRU with $n = 256$ in [6] and recommended that n should be a prime.

There were also attempts for NTRU by modifying a ring. In [5], Gaborit, Ohler, and Solé proposed a variant of NTRU, named CTRU and claimed that this variant allows setting $n = 2^k$, where a ring is $(\mathbb{F}_2[T])[X]/\langle X^n - 1\rangle$. After one month from this proposal, Arnault cryptanalysed CTRU [1]. Independently, Kouzmenko gave the analysis of CTRU in his master thesis [11], which was based on simple linear algebra. In 2008, Vats also cryptanalysed CTRU in 2008 [18]: he gave the same algebraic attack as Kouzmenko's one, and extended the results by giving a faster attack.

Coglianese and Goi [3] gave another variant of NTRU which is defined over a $k \times k$ matrix ring over $\mathbb{Z}_q[X]/\langle X^{n'} - 1\rangle$, MaTRU, where $n = n'k^2$. The complexity for encryption of MaTRU is $O(n'^2 k^3 \log^2 q) = O(n^2 \log^2 q/k)$.

Our work: We attempt to set $n = 2^k$, which enables us to use FFT in encryption. Differently from Silverman's attempt, we use a ring $\mathbb{Z}_q[X]/\langle X^n + 1\rangle$. This change of a base of a ring prevents Gentry's attack, since a polynomial $X^n + 1$ is irreducible over $\mathbb{Z}$ if $n = 2^k$.

Organization: In Section 2, we define the basic notions and notations. We briefly review NTRU in Section 3. Section 4 gives the definition of lattices and NTRU lattices. Section 5 reviews Gentry's folding attack. In Section 6, we recall the properties of the polynomial $X^n + 1$. We propose our new variant of NTRU in Section 7.

2 Preliminaries

We say a function $\epsilon(n)$ is negligible in n if $\epsilon(n) = 2^{-\omega(\log n)}$. We denote by $\boldsymbol{v}_1 \circ \boldsymbol{v}_2$ the concatenation of two vectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$. Let $\langle a_1, \ldots, a_l\rangle$ denote an ideal generated by $a_1, \ldots, a_l$.

Let $\boldsymbol{b}(X) \in \mathbb{Z}[X]$ denote a monic polynomial of degree n. $\mathcal{R}_{\boldsymbol{b}}$ denotes $\mathbb{Z}[X]/\langle \boldsymbol{b}\rangle$. For a positive integer n, NTRU is defined on a quotient ring $\mathcal{R}_{X^n-1} = \mathbb{Z}[X]/\langle X^n - 1\rangle$. For a monic polynomial $\boldsymbol{b}(X)$ of degree n, we identify $\mathcal{R}_{\boldsymbol{b}}$ with $\mathbb{Z}^n$ by identifying $\boldsymbol{f} = \sum_{i=0}^{n-1} f_i X^i \in \mathcal{R}_{\boldsymbol{b}}$ with $\boldsymbol{f} = {}^t(f_0, \ldots, f_{n-1}) \in \mathbb{Z}^n$.

* Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan. {xagawa5,keisuke}@is.titech.ac.jp. Supported in part by NTT Information Sharing Platform Laboratories and KAKENHI No.19-55201.

Name	Ring	n	q and p	Ref.
NTRU	$\mathbf{Z}[X]/\langle X^n - 1\rangle$	Primes	$q, p \in \mathbf{Z}$	[8]
NTRU-Composite	$\mathbf{Z}[X]/\langle X^n - 1\rangle$	2^k	$q, p \in \mathbf{Z}$	[17]
CTRU	$(\mathbb{F}_2[T][X])/\langle X^n - 1\rangle$	Any	$q, p \in \mathbb{F}_2[T]$	[5]
MaTRU	$M_{k,k}(\mathbf{Z}[X]/\langle X^n - 1\rangle)$	Any	$q, p \in \mathbf{Z}$	[3]
NFALSE (Ours)	$\mathbf{Z}[X]/\langle X^n + 1\rangle$	2^k	$q, p \in \mathbf{Z}$	..

Table 1: Variants of NTRU.

Let $\mathcal{B}$ denote $\{0,1\}^n$, and $\mathcal{B}(d)$ the set of all polynomials of degree at most $n-1$ with exactly d coefficients set to 1 and all the other coefficients set to 0. We define $\mathcal{T}$ as $\{-1,0,+1\}^n$. $\mathcal{T}(d_1, d_2)$ denotes the subset of $\mathcal{T}$ such that each polynomial in $\mathcal{T}(d_1, d_2)$ has exactly d_1 coefficients set to 1 and d_2 coefficients set to -1. We define $\mathcal{X}(d_F)$ as $\{f_1 \otimes f_2 + f_3 : f_i \in \mathcal{B}(d_F)$ for all $i\}$. For an integer a and a subset $S \subseteq \mathcal{R}_q$, we define aS as $\{af : f \in S\}$. For a subset $S \subseteq \mathcal{R}_q$, S^* denotes the set of the polynomials in S which have the inverses in $\mathcal{R}_q$, i.e., $S^* = \{f \in S : \exists f^{-1} \in \mathcal{R}_q\}$.

3 Brief Sketch of NTRU

In this section, we briefly review NTRU. For details, see the original paper [8] and proposals of the parameters [9, 10, 7, 19].

Let $b(X) = X^n - 1$. The subsets of $\mathcal{R}_{b,q}$, $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$, $\mathcal{L}_r$, and $\mathcal{L}_F$ are defined later. They are used for key generation and encryption. The parameter p may be a polynomial $2+\alpha$ rather than small prime such as 2 or 3.

Key Generation:

1. Choose $f \in \mathcal{L}_f$ and $g \in \mathcal{L}_g$ uniformly at random. f must be invertible in $\mathcal{R}_{b,q}$ and $\mathcal{R}_{b,p}$.
2. Set $F_q = f^{-1}$ in $\mathcal{R}_{b,q}$.
3. Compute $h = p \otimes g \otimes F_q$.
4. The public key is h and the secret key is f.

Encryption: A plaintext is $m \in \mathcal{L}_m$.

1. Select $r \in \mathcal{L}_r$ uniformly at random.
2. Compute $c = h \otimes r + m$.
3. The ciphertext is c.

Decryption: A ciphertext is $c \in \mathcal{R}_{b,q}$.

1. Compute $a' = f \otimes c$ in $\mathcal{R}_{b,q}$.
2. Compute $a = p \otimes g \otimes r + f \otimes m$ in $\mathcal{R}_b$ from a' by using a centering algorithm.
3. Compute $F_p = f^{-1}$ in $\mathcal{R}_{b,p}$.
4. Compute $m' = F_p \otimes a$ in $\mathcal{R}_{b,p}$.
5. The obtained plaintext is m'.

Remark 3.1. We first confirm the following equation:

$$a' = f \otimes (h \otimes r + m) = p \otimes g \otimes r + f \otimes m \text{ in } \mathcal{R}_{b,q}.$$

The centering algorithm sets the coefficients of a into $[A - q/2, A + q/2)$ for some A. Using the centering algorithm, we have, with high probability,

$$a = p \otimes g \otimes r + f \otimes m \text{ in } \mathcal{R}_b.$$

Thus, we obtain

$$m' = F_p \otimes a = F_p \otimes (p \otimes g \otimes r + f \otimes m) = F_p \otimes f \otimes m = m \text{ in } \mathcal{R}_{b,p}.$$

In order for the decryption process to work correctly, it is necessary that $|a|_\infty < q/2$, where, for any $x \in \mathcal{R}_b$, $|x|_\infty$ is defined as $\max_i\{x_i\} - \min_i\{x_i\}$ and called width. The subsets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_r$, $\mathcal{L}_m$, and $\mathcal{L}_F$ are carefully chosen to satisfy the above norm bound with overwhelming probability.

There are five instantiations of NTRU, NTRU-1998 [8], NTRU-2001 [9], NTRU-2005 [10], NTRU-2007 [7], and NTRU-2008 [19]. Table 2 summarizes the parameter sets of these instantiations. Table 3 reports example parameters of NTRU-2008.

Parameter Sets	n	d_F & d_r	d_g	Expected Security
ees449ep1	449	134	149	128-bit
ees613ep1	613	55	204	128-bit
ees761ep1	761	42	253	128-bit
ees853ep1	853	268	284	256-bit
ees1171ep1	1171	106	394	256-bit
ees1499ep1	1499	79	499	256-bit

Table 3: Example of the parameter sets in NTRU-2008 [19].

4 NTRU Lattices

Lattices: In this paper, we use the basic notions and notations of lattices. A lattice is an additive discrete subgroup of $\mathbb{R}^m$. A lattice $L \subseteq \mathbb{R}^m$ of rank n has a basis $B \in \mathbb{R}^{m \times n}$ such that $L(B) = \{Bx : x \in \mathbf{Z}^n\}$, where the rank of B is n. For details on lattices and cryptography based on lattice problems, see, e.g., the textbook by Micciancio and Goldwasser [15] and the latest survey by Micciancio and Regev [16].

4.1 NTRU lattices

Let p^{-1} be the inverse of p in $\mathbf{Z}_q$. An NTRU lattice [4] is generated by a basis

$$H := \begin{bmatrix} \mathrm{Rot}(1) & \mathrm{Rot}(0) \\ \mathrm{Rot}(p^{-1}h) & \mathrm{Rot}(q) \end{bmatrix}.$$

As noted by Coppersmith and Shamir [4], the lattice $L(H)$ includes a short vector $f \circ g$ containing a secret key since $p^{-1}h \equiv f^{-1} \otimes g \pmod{q}$.

Parameter Sets	q	p	$\mathcal{L}_f$	$\mathcal{L}_g$	$\mathcal{L}_m$	$\mathcal{L}_r$	$\mathcal{L}_F$	Ref.
NTRU-1998	2^k	3	$\mathcal{T}(d_f, d_f-1)^*$	$\mathcal{T}(d_g, d_g)$	$\mathcal{T}$	$\mathcal{T}(d_r, d_r)$	-	[8]
NTRU-2001	prime	$2+X$	$\{1+p\otimes F : F\in\mathcal{L}_F\}^*$	$\mathcal{B}(d_g)$	$\mathcal{B}$	$\mathcal{B}(d_r)$	$\mathcal{B}(d_F)$	[9]
NTRU-2005	prime	2	$\{1+p\otimes F : F\in\mathcal{L}_F\}^*$	$\mathcal{B}(N/2)^*$	$\mathcal{B}$	$\mathcal{X}(d_r)$	$\mathcal{X}(d_F)$	[10]
NTRU-2007	2^k	3	$\{1+p\otimes F : F\in\mathcal{L}_F\}^*$	$\mathcal{T}(d_f, d_f-1)^*$	$\mathcal{T}(d_f, d_f-1)$	$\mathcal{T}(d_f, d_f-1)$	$\mathcal{T}(d_f, d_f-1)$	[7]
NTRU-2008	2^k	3	$\{1+p\otimes F : F\in\mathcal{L}_F\}^*$	$\mathcal{T}(d_g, d_g)$	$\mathcal{T}$	$\mathcal{T}(d_r, d_r)$	$\mathcal{T}(d_F)$	[19]

Table 2: Parameter sets. In NTRU-1998, f must be invertible in $\mathcal{R}_p$.

5 Gentry's Folding Attack

In [6], Gentry proposed an attack against NTRU-Composite. Let us assume that n is a composite number. The factor of n will be denoted by d.

For $f = (f_0, \ldots, f_{n-1}) \in \mathbb{Z}[X]/\langle X^n - 1\rangle$, the d-dimensional folded polynomial of f is defined by

$$\theta_d(f) = \left(\sum_{i=0 \bmod d}^{0\le i<n} f_i, \sum_{i=1 \bmod d}^{0\le i<n} f_i, \ldots, \sum_{i=d-1 \bmod d}^{0\le i<n} f_i \right).$$

This mapping θ_d is a ring homomorphism from $\mathbb{Z}[X]/\langle X^n - 1\rangle$ to $\mathbb{Z}[X]/\langle X^d - 1\rangle$ (see [6, Theorem 1]). We mention that θ_d has a good property with respect to norms. For the ℓ_∞-norm, we have that $\|\theta_d(f)\|_\infty \le (n/d)\|f\|_\infty$ obviously.

Let us set $n = 2^k$ and $d = n/2$. Gentry considered the following folded NTRU lattices of rank n instead of the NTRU lattices of rank $2n$: Since (f, g) is in the NTRU lattice spanned by h and its norm is short, so $(\theta_d(f), \theta_d(g))$ is relatively short in the folded NTRU lattice L of rank n. Thus, using the LLL algorithm, one may obtain $(\theta_d(f), \theta_d(g))$. We omit the details of extracting (f, g) from $(\theta_d(f), \theta_d(g))$. For the details, see [6].

5.1 Another Foldings

As noted in [6, Section 5.1], we have another folding by a ring homomorphism $\theta : \mathbb{Z}[X]/\langle b(X)\rangle \to \mathbb{Z}[X]/\langle s(X)\rangle$ for some $b(X) = s(X)\cdot t(X)$, which is given by $\theta(f) = f(X) + \langle s(X)\rangle$. Gentry's folding attack may be useful if the following two conditions hold: (1) the degree of s is relatively high, that is, N/c for some constant c and (2) the mapping θ preserves a good norm bound, i.e., there exists a constance c' such that for any $f \in \mathcal{R}_b$, $\|\theta(f)\|_\infty \le c\|f\|_\infty$.

6 The properties of $X^n + 1$

In the hash function SWIFFT [14], the polynomial $X^n + 1$ serves a fast computation and a security proof. We employ the polynomial to use it in the encryption scheme.

In this section, we review the properties of the polynomial, its expansion factor and FFT-like computations.

6.1 Small Expansion Factor

The expansion factor of a polynomial f captures the relation of the norms in the ring $\mathcal{R}$ and the quotient ring $\mathcal{R}_f$.

We define an expansion factor, which is a restricted version of that proposed by Lyubashevsky and Micciancio [13]:

$$\mathrm{EF}(f) = \max_{g\in\mathbb{Z}[x], \deg(g)\le 2(\deg(f)-1)} \|g \bmod f\|_\infty / \|g\|_\infty .$$

A simple calculation shows that $\mathrm{EF}(x^n \pm 1, 2) = 2$.

Since the expansion factor of $X^n + 1$ is 2, we have that, for any two polynomials f and g of degree at most $n-1$, $\|f \otimes g\|_\infty \le 2\|fg\|_\infty$.

6.2 Serving a FFT-like computation

Mathematical backgrounds: Let q be a prime. Recall that for an element in $\mathbb{Z}_q^*$, its multiplicative order divides $q-1$. Thus, there is a subgroup of order $2n$ in $\mathbb{Z}_q^*$. Let w denote an element of multiplicative order $2n = 2^{k+1}$ in $\mathbb{Z}_q$. By setting w as the above, the polynomial $X^n + 1$ has n roots, $w^1, w^3, \ldots, w^{2n-1}$, that is, $X^n + 1 = \prod_{i=1}^{n}(X - w^{2i-1})$ over $\mathbb{Z}_q$. By the Chinese remainder theorem, we have a ring homomorphism

$$\mathbb{Z}_q[X]/\langle b'\rangle \simeq \mathbb{Z}_q[X]/\langle X - w\rangle \times \mathbb{Z}_q[X]/\langle X - w^3\rangle \times \cdots \times \mathbb{Z}_q[X]/\langle X - w^{2n-1}\rangle.$$

For a polynomial $f \in \mathcal{R}_{X^n+1,q}$, we define

$$\tilde{f} = \mathrm{DFT}_{n,w}(f) = (f(w), f(w^3), \ldots, f(w^{2n-1})).$$

Let $\odot$ denote a component-wise multiplication. So, DFT induces the above ring homomorphism from $(\mathcal{R}_{X^n+1,q}, \otimes, +)$ to $(D, \odot, +)$.

Computational backgrounds: It is well-known that $\mathrm{DFT}(f)$ can be computed by $O(n \log n)$ additions and multiplications. From the definition, it is easy to verify that

$$\mathrm{DFT}_{n,w}(f) = \begin{pmatrix} w^0 & w^1 & w^2 & \cdots & w^{n-1} \\ w^0 & w^3 & w^6 & \cdots & w^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ w^0 & w^{2n-1} & w^{4(n-1)} & \cdots & w^{(n-1)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix}.$$

By reordering, we obtain the following equation.

$$\mathrm{DFT}_{n,w}(f) = \begin{pmatrix} \mathrm{DFT}_{n/2,w^2}(f_e) + (w, w^3, \ldots, w^{2n-1}) \odot \mathrm{DFT}_{n/2,w^2}(f_o) \\ \mathrm{DFT}_{n/2,w^2}(f_e) - (w, w^3, \ldots, w^{2n-1}) \odot \mathrm{DFT}_{n/2,w^2}(f_o) \end{pmatrix},$$

where $f_e = (f_0, f_2, \ldots, f_{n-2})$ and $f_o = (f_1, f_3, \ldots, f_{n-1})$. Computing recursively, we can obtain $\mathrm{DFT}_{n,w}(f)$ with $O(n \log n)$ additions and multiplications.

7 Our Proposal

In order to use a FFT-like computation to compute multiplications, n should be the power of 2, say 2^k for some k. However, since $X^{2^k} - 1$ has a factor $X^{2^{k-1}} - 1$, Gentry's folding attack works well in practical. To prevent the attack, we set the base polynomial $b'(X) = X^{2^k} + 1$ which is irreducible over $\mathbf{Z}$. Additionally, the polynomial $X^{2^k} + 1$ serves FFT-like computations in $\mathbf{Z}_q[X]/\langle X^{2^k} + 1\rangle$ for suitable q.

7.1 Proposal

Our proposal is as follows:

Key Generation:

1. Choose $F \in \mathcal{L}_F$ and $g \in \mathcal{L}_g$ uniformly at random. $1 + 3F$ must be invertible in $\mathcal{R}_q$.
2. Set $F_q = f^{-1}$ in $\mathcal{R}_q$.
3. Compute $\tilde{F}_q = \mathrm{DFT}(F_q)$ and $\tilde{g} = \mathrm{DFT}(g)$.
4. Compute $\tilde{h} = 3(\tilde{g} \odot \tilde{F}_q)$.
5. The public key is $\tilde{h}$ and the secret key is $\tilde{f} = \mathrm{DFT}(1 + 3F)$.

Encryption: A plaintext is $m \in \mathcal{L}_m$.

1. Select $r \in \mathcal{L}_r$ uniformly at random.
2. Compute $\tilde{r} = \mathrm{DFT}(r)$ and $\tilde{m} = \mathrm{DFT}(m)$.
3. Compute $\tilde{c} = \tilde{h} \odot \tilde{r} + \tilde{m}$.
4. The ciphertext is $\tilde{c}$.

Decryption: A ciphertext is $\tilde{c}$.

1. Compute $\tilde{a}' = \tilde{f} \odot \tilde{c}$.
2. Compute $a' = \mathrm{DFT}^{-1}(\tilde{a}')$
3. Compute a by using the centering algorithm as in NTRU.
4. Compute $m' = a$ in $\mathcal{R}_p$.
5. The obtained plaintext is m'.

Notes: In encryption, the ciphertext is $\tilde{c}$ rather than c. This enables us to decrease the number of DFT in decryption.

7.2 Correctness

As in NTRU, we have that

$$a' = f \otimes (h \otimes r + m) = 3 \otimes g \otimes r + f + m \text{ in } \mathcal{R}_{b',q}.$$

If we have that

$$a = 3 \otimes g \otimes r + f \otimes m \text{ in } \mathcal{R}_{b'},$$

we can obtain that

$$m' = a = 3 \otimes g \otimes r + f \otimes m = 3 \otimes g \otimes r + (1 + 3F) \otimes m = m \text{ in } \mathcal{R}_{b',3}.$$

We note that

$$\|a\|_\infty \leq 2\|3 \cdot g \cdot r + f \cdot m\|_\infty,$$

where $\cdot$ denote the multiplicative operation in $\mathcal{R}$. Thus, if $\|3 \cdot g \cdot r + f \cdot m\|_\infty \leq q/4$, we have that $a = 3 \otimes g \otimes r + f \otimes m$ in $\mathcal{R}_{b'}$. Hence, the expansion factor of the base polynomial b' plays a key role for correct decryptions. This is one of the reason that we set b' as $X^n + 1$.

7.3 On Gentry's attack

NFALSE prevents Gentry's folding attacks and its extensions by choosing the ring $\mathbf{Z}[X]/\langle X^n + 1\rangle$, since $X^n + 1$ is irreducible over $\mathbf{Z}$ if n is the power of 2.

References

[1] Arnault, F. Cryptanalyse de CTRU, December 2002.

[2] Buchmann, J., Döring, M., and Lindner, R. Efficiency improvement for NTRU. In *Sicherheit 2008: Sicherheit, Schutz und Zuverlässigkeit* (April 2008), A. Alkassar and J. H. Siekmann, Eds., vol. 128 of *Lecture Note in Informatics*, GI, pp. 163–178.

[3] Coglianese, M., and Goi, B.-M. MaTRU: A new NTRU-based cryptosystem. In *Progress in Cryptology – INDOCRYPT 2005* (Bangalore, India, December 2005), S. Maitra, C. E. Veni Madhavan, and R. Venkatesan, Eds., vol. 3797 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 232–243.

[4] Coppersmith, D., and Shamir, A. Lattice attacks on NTRU. In *Advances in Cryptology – EUROCRYPT '97* (Konstanz, Germany, May 1997), W. Fumy, Ed., vol. 1233 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 52–61.

[5] Gaborit, P., Ohler, J., and Solé, P. CTRU, a polynomial analogue of NTRU. INRIA, RR-4621, November 2002. Available at `http://www.inria.fr/rrrt/rr-4621.html`.

[6] Gentry, C. Key recovery and message attacks on NTRU-composite. In *Advances in Cryptology – EUROCRYPT 2001* (Innsbruck, Austria, May 2001), B. Pfitzmann, Ed., vol. 2045 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 182–194.

[7] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H., and Whyte, W. Hybrid lattice reduction and meet in the middle resistant parameter selection for NTRUEncrypt, 2007.

[8] Hoffstein, J., Pipher, J., and Silverman, J. H. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III* (Portland, Oregon, USA, June 1998), J. Buhler, Ed., vol. 1423 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 267–288.

[9] Hoffstein, J., and Silverman, J. Optimizations for NTRU, 2000. Available at `http://www.ntru.com/cryptolab/articles.htm`.

[10] Howgrave-Graham, N., Silverman, J. H., and Whyte, W. Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3, 2005. Available at `http://www.ntru.com/cryptolab/articles.htm`.

[11] KOUZMENKO, R. Generalizations of the NTRU cryptosystem. Master's thesis, Ecole Polytechnique Fédérale de Lausanne, 2006.

[12] LEE, M.-K., KIM, J. W., SONG, J. E., AND PARK, K. Sliding window method for NTRU. In *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007* (Zhuhai, China, June 2007), J. Katz and M. Yung, Eds., vol. 4521 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 432–442.

[13] LYUBASHEVSKY, V., AND MICCIANCIO, D. Generalized compact knapsacks are collision resistant. In *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Part II* (Venice, Italy, July 2006), M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds., vol. 4052 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 144–155.

[14] LYUBASHEVSKY, V., MICCIANCIO, D., PEIKERT, C., AND ROSEN, A. SWIFFT: A modest proposal for FFT hashing. In *Fast Software Encryption, 15th International Workshop, FSE 2008* (Lausanne, Switzerland, February 2008), K. Nyberg, Ed., vol. 5086 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 54–72.

[15] MICCIANCIO, D., AND GOLDWASSER, S. *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

[16] MICCIANCIO, D., AND REGEV, O. Lattice-based cryptography. In *Post-quantum Cryptography*, D. J. Bernstein and J. Buchmann, Eds. Springer-Verlag, 2008.

[17] SILVERMAN, J. H. Wraps, gaps, and lattice constants. Tech. Rep. 11, version 2, NTRU Cryptosystems, 2001. Available at `http://www.ntru.com/cryptolab/tech_notes.htm`.

[18] VATS, N. Algebraic cryptanalysis of CTRU cryptosystem. In *Computing and Combinatorics, 14th Annual International Conference, COCOON 2008* (Dalian, China, June 2008), X. Hu and J. Wang, Eds., vol. 5092 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 235–244.

[19] WHYTE, W., HOWGRAVE-GRAHAM, N., HOFFSTEIN, J., PIPHER, J., SILVERMAN, J. H., AND HIRSCHHORN, P. IEEE P1363.1/D10 draft standard for public-key cryptographic techniques based on hard problems over lattices, July 2008. Available at `http://eprint.iacr.org/2008/361`.