A Variant of NTRU with Non-Invertible Polynomials

William D. Banks[1] and Igor E. Shparlinski[2]

[1] Department of Mathematics, University of Missouri
Columbia, MO 65211, USA
bbanks@math.missouri.edu
[2] Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract. We introduce a generalization of the NTRU cryptosystem and describe its advantages and disadvantages as compared with the original NTRU protocol. This extension helps to avoid the potential problem of finding "enough" invertible polynomials within very thin sets of polynomials, as in the original version of NTRU. This generalization also exhibits certain attractive "pseudorandomness" properties that can be proved rigorously using bounds for exponential sums.

1 A Generalization of NTRU

In this generalization of the original *NTRU cryptosystem* [5, 6], one selects integer parameters (N, p, q) and four sets $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\varphi, \mathcal{L}_m$ of polynomials in the ring $\mathcal{R} = \mathbb{Z}[X]/(X^N - 1)$ as in the standard version of NTRU. We denote by $\odot$ the operation of multiplication in the ring $\mathcal{R}$. The parameters q and p are distinct prime numbers such that $\gcd(N, q) = 1$, and the sets $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\varphi, \mathcal{L}_m$ are chosen to satisfy the "width condition"

$$\|p\,\varphi \odot g + f \odot m\| < q$$

for all polynomials $f \in \mathcal{L}_f$, $g \in \mathcal{L}_g$, $\varphi \in \mathcal{L}_\varphi$, $m \in \mathcal{L}_m$, where for any polynomial

$$F(X) = F_0 + F_1 X + \ldots + F_{N-1} X^{N-1},$$

we define the *width* of F by

$$\|F\| = \max_{0 \le \nu \le N-1} F_\nu - \min_{0 \le \nu \le N-1} F_\nu.$$

Our extension of the original NTRU scheme can be described as follows.

Key Creation. Alice randomly selects polynomials $f \in \mathcal{L}_f$, $g \in \mathcal{L}_g$ and $G \in \mathcal{R}$ such that G has an inverse modulo q and f has an inverse modulo p. This is easily accomplished since G is allowed to range over all of $\mathcal{R}$, and p will be very small

in any practical implementation of this scheme. *Alice* first computes inverses G_q^* and f_p^* that satisfy

$$G \odot G_q^* \equiv 1 \pmod{q}, \qquad f \odot f_p^* \equiv 1 \pmod{p}, \tag{1}$$

then *Alice* computes the products

$$h \equiv G_q^* \odot g \pmod{q}, \qquad H \equiv G_q^* \odot f \pmod{q}. \tag{2}$$

Alice publishes the pair of polynomials (h, H) as her public key, retaining (f, g, G) as her private key. The polynomial f_p^* is simply stored for later use, and the polynomial G_q^* may be discarded.

Encryption. Suppose *Bob* (the encrypter) wants to send a secret message to *Alice* (the decrypter). *Bob* selects a message m from the set of plaintexts $\mathcal{L}_m$. Next, *Bob* selects a random polynomial $\varphi \in \mathcal{L}_\varphi$ and uses *Alice*'s public key (h, H) to compute

$$e \equiv p\,\varphi \odot h + H \odot m \pmod{q}.$$

Bob then transmits e to *Alice*.

Decryption. *Alice* has received e from *Bob*. To decrypt the message, she first computes

$$a \equiv G \odot e \equiv p\,\varphi \odot g + f \odot m \pmod{q},$$

choosing the coefficients of a to lie in the interval from $-q/2$ to $q/2$. The remainder of our procedure now follows the standard version of NTRU; that is, *Alice* treats a as a polynomial with *integer* coefficients and recovers the message by computing

$$m \equiv f_p^* \odot a \pmod{p}.$$

One easily verifies that the case $G = f$ corresponds to the classical NTRU cryptosystem (in this case, $H = 1$, so the public key consists solely of the polynomial h). Moreover, if f (and therefore H) is invertible modulo q, then this generalization is equivalent to the original scheme. Indeed, instead of decrypting e the attacker can try to decrypt

$$e \odot H_q^* \equiv p\,\varphi \odot \left(H_q^* \odot h\right) + m \pmod{q},$$

where $H_q^* H \equiv 1 \pmod{q}$. On the other hand, if f is a zero-divisor in the ring $\mathcal{R}$, then our construction seems to produce a new scheme.

The main *disadvantage* of this scheme versus the classical NTRU scheme is that the public key size and the encryption time are roughly doubled.

The *advantages* are:

- This scheme provides more flexibility in the choice of parameters. In particular, it is likely that this generalization is more robust against some of the known attacks on classical NTRU. In particular, for a lattice attack (which is by far the most "dangerous" threat to NTRU), in this setting one must work with more general lattices than in the original scheme.

- One can *prove* some theoretical results about the set of inverses G_q^*. In particular, although the issue has never been doubted in practice, it is not clear how to prove rigorously that there exist "enough" invertible polynomials $f \in \mathcal{L}_f$ in the NTRU scheme. In our scheme, G is selected from the entire ring $\mathcal{R}$, and the density of invertible polynomials has been explicitly evaluated in [11]. One can also prove some rigorous statements concerning the distribution of h and H, and also about the distribution of e (thus showing that the ciphertext e and the plaintext message m are *uncorrelated*).
- One can select G to have very small degree, which will speed-up the decryption procedure as compared with the original NTRU scheme.
- It is possible to select h once and for all as a universal quantity (thus reducing the public key size), or it can be selected to have a certain special form (to speed-up the encryption), although it is not clear whether or not these choices might compromise the security of this scheme; this question should be studied in more detail. With such a modification, G would be computed in terms of f, g, and h, and the public key size be roughly the same as for classical NTRU.

In what follows, we present rigorous proofs of some of the theoretical results alluded to above. In particular, we show that for almost all $G \in \mathcal{R}^*$, the set of polynomials $\{p\,\varphi \odot h\}$, where h is defined by (1) and (2) and φ runs over the set $\mathcal{L}_\varphi$ (which can be rather arbitrary), is uniformly distributed. This means that for almost all G, the message m (or, equivalently, the product $H \odot m$) is reliably concealed by adding $\{p\,\varphi \odot h\}$.

Acknowledgement. We thank Jeffrey Hoffstein, Daniel Lieman and Joe Silverman for attracting our interest in this problem and for many fruitful discussions. Work supported in part by NSF grant DMS-0070628 (W. Banks) and by ARC grant A00000184 (I. Shparlinski).

2 Character Sums

Let $\mathcal{R}_q$ be the reduction of $\mathcal{R}$ modulo q, and let $\mathcal{R}_q^*$ be the set of invertible polynomials in $\mathcal{R}_q$. We use $\odot$ for multiplication in the ring $\mathcal{R}_q$.

Recall that the cardinality of $\mathcal{R}_q^*$ is given by an analogue of the *Euler function*

$$|\mathcal{R}_q^*| = q^N \prod_{j=1}^{r} (1 - q^{-n_j}) \tag{3}$$

where $n_1, \ldots, n_r$ are the degrees of the $r \geq 1$ irreducible divisors of $X^N - 1$. Though we will not need this, a more explicit expression for n_j's (hence also for $|\mathcal{R}_q^*|$) is given in [11]; see also Section 6.5 of [3] and Section 7.5 of [10].

Let $X^N - 1 = \Psi_1(X) \ldots \Psi_r(X)$ be the complete factorization of $X^N - 1$ into irreducible polynomials in the ring $\mathcal{R}_q$. Because $\gcd(N, q) = 1$, we see that $X^N - 1$ is square-free in $\mathcal{R}_q$, hence all of these factors are pairwise distinct.

We recall that $\mathbb{F}_q[X]/\Phi(X) \cong \mathbb{F}_{q^m}$ for any irreducible polynomials $\Phi(X) \in \mathbb{F}_q[X]$ with $\deg \Phi = m$. For each $j = 1, \ldots, r$, we fix a root α_j of $\Psi_j(X)$, and denote

$$\mathbb{K}_j = \mathbb{F}_{q^{n_j}} = \mathbb{F}_q(\alpha_j) \cong \mathbb{F}_q[X]/\Psi_j(X). \tag{4}$$

where $n_j = \deg \Psi_j$. For each j, let

$$\mathrm{Tr}_j(z) = \sum_{k=0}^{n_j-1} z^{q^k}$$

be the trace of $z \in \mathbb{K}_j$ to $\mathbb{F}_q$.

We denote by $\mathcal{A}$ the direct product of fields

$$\mathcal{A} = \mathbb{K}_1 \times \ldots \times \mathbb{K}_r,$$

and we have a natural isomorphism

$$\mathcal{R}_q \cong \mathbb{K}_1 \times \ldots \times \mathbb{K}_r = \mathcal{A} \tag{5}$$

given by the map that sends $f \in \mathcal{R}_q$ to $\mathbf{a}_f = (f(\alpha_1), \ldots, f(\alpha_r)) \in \mathcal{A}$. In particular, the relation (3) from immediately from (5).

For every vector $\mathbf{a} = (a_1, \ldots, a_r) \in \mathcal{A}$, let $\chi_{\mathbf{a}}$ be the character of $\mathcal{R}_q$ given by

$$\chi_{\mathbf{a}}(f) = \prod_{j=1}^{r} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j f\left(\alpha_j\right)\right)\right), \qquad f \in \mathcal{R}_q,$$

where

$$\mathbf{e}(z) = \exp(2\pi i z/q).$$

It is easy to shown that $\{\chi_{\mathbf{a}} \,|\, \mathbf{a} \in \mathcal{A}\}$ is the complete set of additive characters of $\mathcal{R}_q$. In particular, for any polynomial $f \in \mathcal{R}_q$, one has

$$\sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(f) = \begin{cases} 0, & \text{if } f \neq 0, \\ q^N, & \text{if } f = 0. \end{cases} \tag{6}$$

Our main results rely on an upper bound for character sums of the form

$$W_{\mathbf{a}}(\mathcal{L}) = \sum_{Q \in \mathcal{R}_q^*} \left| \sum_{\varphi \in \mathcal{L}} \chi_{\mathbf{a}}(Q \odot \varphi) \right|, \qquad \mathbf{a} \in \mathcal{A}.$$

To estimate these sums, we need the following identity (see Section 1 of Chapter 5 of [9])

$$\sum_{x_j \in \mathbb{K}_j} \mathbf{e}(\mathrm{Tr}_j(x_j\, c)) = \begin{cases} 0, & \text{if } c \neq 0, \\ q^{n_j}, & \text{if } c = 0, \end{cases} \tag{7}$$

which holds for any $c \in \mathbb{K}_j$, $j = 1, \ldots, r$.

Lemma 1. *Let* $\mathbf{a} = (a_1, \ldots, a_r) \in \mathcal{A}$ *and let* $\mathcal{J} \subseteq \{1, \ldots, r\}$ *be the set of* j *with* $a_j \neq 0$. *Then the bound*

$$W_{\mathbf{a}}(\mathcal{L}) \leq |\mathcal{R}_q^*|^{1/2} |\mathcal{L}|^{1/2} q^{N/2} \prod_{j \notin \mathcal{J}} q^{n_j/2}$$

holds.

Proof. Using the Cauchy inequality and extending the summation over all polynomials $Q \in \mathcal{R}_q$, we derive

$$\begin{aligned} W_{\mathbf{a}}(\mathcal{L})^2 &\leq |\mathcal{R}_q^*| \sum_{Q \in \mathcal{R}_q} \left| \sum_{\varphi \in \mathcal{L}} \chi_{\mathbf{a}} \left(Q \odot \varphi\right) \right|^2 \\ &= |\mathcal{R}_q^*| \sum_{Q \in \mathcal{R}_q} \sum_{\varphi_1, \varphi_2 \in \mathcal{L}} \chi_{\mathbf{a}} \left(Q \odot (\varphi_1 - \varphi_2)\right) \\ &\leq |\mathcal{R}_q^*| \sum_{\varphi_1, \varphi_2 \in \mathcal{L}} \sum_{Q \in \mathcal{R}_q} \prod_{j=1}^{r} \mathbf{e}\left(\mathrm{Tr}_j \left(a_j Q(\alpha_j) \left(\varphi_1(\alpha_j) - \varphi_2(\alpha_j)\right)\right)\right). \end{aligned}$$

From the isomorphism (5), we see that as Q runs over the set $\mathcal{R}_q$ the vector $\left(Q\left(\alpha_1\right), \ldots, Q\left(\alpha_r\right)\right)$ runs through the set $\mathbb{K}_1 \times \ldots \times \mathbb{K}_r$. Therefore

$$\begin{aligned} W_{\mathbf{a}}(\mathcal{L})^2 &\leq |\mathcal{R}_q^*| \sum_{\varphi_1, \varphi_2 \in \mathcal{L}} \prod_{j=1}^{r} \sum_{x_j \in \mathbb{K}_j} \mathbf{e}\left(\mathrm{Tr}_j \left(a_j x_j \left(\varphi_1(\alpha_j) - \varphi_2(\alpha_j)\right)\right)\right) \\ &= |\mathcal{R}_q^*| \prod_{j \notin \mathcal{J}} q^{n_j} \sum_{\varphi_1, \varphi_2 \in \mathcal{L}} \prod_{j \in \mathcal{J}} \sum_{x_j \in \mathbb{K}_j} \mathbf{e}\left(\mathrm{Tr}_j \left(a_j x_j \left(\varphi_1(\alpha_j) - \varphi_2(\alpha_j)\right)\right)\right). \end{aligned}$$

From (7) we see that the product vanishes if $\varphi_1(\alpha_j) \neq \varphi_2(\alpha_j)$ for some $j \in \mathcal{J}$, and

$$\prod_{j \in \mathcal{J}} \sum_{x_j \in \mathbb{K}_j} \mathbf{e}\left(\mathrm{Tr}_j \left(a_j x_j \left(\varphi_1(\alpha_j) - \varphi_2(\alpha_j)\right)\right)\right) = \prod_{j \in \mathcal{J}} q^{n_j}$$

otherwise. Since $\{\Psi_j \,|\, j = 1, \ldots, r\}$ are *irreducible* polynomials, the condition $\varphi_1(\alpha_j) = \varphi_2(\alpha_j)$ is equivalent to $\Psi_j \big| (\varphi_1 - \varphi_2)$. Hence

$$W_{\mathbf{a}}(\mathcal{L})^2 \leq |\mathcal{R}_q^*| q^N M(\mathcal{J}),$$

where $M(\mathcal{J})$ is the number of pairs $\varphi_1, \varphi_2 \in \mathcal{L}$ with

$$\varphi_1 \equiv \varphi_2 \pmod{\prod_{j \in \mathcal{J}} \Psi_j}.$$

For each $\varphi_1 \in \mathcal{L}$ there are at most

$$q^N \prod_{j \in \mathcal{J}} q^{-n_j} = \prod_{j \notin \mathcal{J}} q^{n_j}$$

such values for φ_2. Consequently

$$M(\mathcal{J}) \le |\mathcal{L}| \prod_{j \notin \mathcal{J}} q^{n_j},$$

and the lemma follows. □

3 Uniformity of Distribution

If we assume for simplicity that $g \in \mathcal{L}_g$ is invertible modulo q, it follows that $Q = p\, G_q^* \odot g$ runs through the entire set $\mathcal{R}_q^*$ together with G. Thus it suffices to study the distribution of $\{Q \odot \varphi \,|\, \varphi \in \mathcal{L}\}$ "on average" for $Q \in \mathcal{R}_q^*$. We remark that the condition $g \in \mathcal{R}_q^*$ is equivalent to $\gcd(g, X^N - 1) = 1$, and we will always need a condition of this type in any case; otherwise, the number of possible values for h becomes too small, and the cryptosystem is then vulnerable to a brute force attack.

Given polynomials $S \in \mathcal{R}_q$ and $Q \in \mathcal{R}_q^*$, a set $\mathcal{L} \subseteq \mathcal{R}_q$, and an integer d, we denote by $N_d(S, Q, \mathcal{L})$ the number of polynomials $\varphi \in \mathcal{L}$ such that the inequality $\deg(S - Q \odot \varphi) < d$ holds.

Thus, roughly speaking, $N_d(S, Q, \mathcal{L})$ counts how many products $Q \odot \varphi$ with $\varphi \in \mathcal{L}$ are "close" to the given polynomial S. Our main result claims that this number is very close to the expected value for almost all polynomials $Q \in \mathcal{R}_q^*$. In particular, this means that for almost all polynomials $Q \in \mathcal{R}_q^*$, the encryptions e (of the same message m) in our modification of NTRU, obtained with randomly chosen polynomials $\varphi \in \mathcal{L}_\varphi$, are uniformly distributed in $\mathcal{R}$.

Theorem 1. *For $q \ge 5$, the bound*

$$\frac{1}{|\mathcal{R}_q^*|} \sum_{Q \in \mathcal{R}_q^*} \left| N_d(S, Q, \mathcal{L}) - \frac{|\mathcal{L}|}{q^{N-d}} \right| \le 3^{Nq^{-1/2}} |\mathcal{L}|^{1/2}$$

holds.

Proof. Clearly, $N_d(S, Q, \mathcal{L}) = q^{-d}\, T_d(S, Q, \mathcal{L})$, where $T_d(S, Q, \mathcal{L})$ is the number of representations $Q \odot \varphi = S + \psi_1 - \psi_2$ with $\varphi \in \mathcal{L}$ and polynomials $\psi_1, \psi_2 \in \mathcal{R}_q$ of degree at most $d - 1$. From the identity (6) we derive

$$\begin{aligned} T_d(S, Q, \mathcal{L}) &= \frac{1}{q^N} \sum_{\varphi \in \mathcal{L}} \sum_{\substack{\psi_1, \psi_2 \in \mathcal{R}_q \\ \deg \psi_1, \deg \psi_2 \le d-1}} \sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(Q \odot \varphi - S - \psi_1 + \psi_2) \\ &= \frac{1}{q^N} \sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(-S) \sum_{\varphi \in \mathcal{L}} \chi_{\mathbf{a}}(Q \odot \varphi) \sum_{\substack{\psi_1, \psi_2 \in \mathcal{R}_q \\ \deg \psi_1, \deg \psi_2 \le d-1}} \chi_{\mathbf{a}}(\psi_2 - \psi_1) \\ &= \frac{1}{q^N} \sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(-S) \sum_{\varphi \in \mathcal{L}} \chi_{\mathbf{a}}(Q \odot \varphi) \left| \sum_{\substack{\psi \in \mathcal{R}_q \\ \deg \psi \le d-1}} \chi_{\mathbf{a}}(\psi) \right|^2 . \end{aligned}$$

The term corresponding to $\mathbf{a} = \mathbf{0}$ is equal to $q^{2d-N}|\mathcal{L}|$. For any nonempty set $\mathcal{J} \subseteq \{1, \dots, r\}$, let $\mathcal{A}_{\mathcal{J}}$ be the subset of $\mathcal{A}$ consisting of all $\mathbf{a} = (a_1, \dots, a_r)$ such that $a_j = 0$ whenever $j \notin \mathcal{J}$. Then we obtain

$$\left| T_d(S, Q, \mathcal{L}) - \frac{|\mathcal{L}|}{q^{N-2d}} \right| \leq \frac{1}{q^N} \sum_{\substack{\mathcal{J} \subseteq \{1,\dots,r\} \\ \mathcal{J} \neq \emptyset}} \sum_{\substack{\mathbf{a} \in \mathcal{A}_{\mathcal{J}} \\ \mathbf{a} \neq \mathbf{0}}} \left| \sum_{\varphi \in \mathcal{L}} \chi_{\mathbf{a}}(Q \odot \varphi) \right| \left| \sum_{\substack{\psi \in \mathcal{R}_q \\ \deg \psi \leq d-1}} \chi_{\mathbf{a}}(\psi) \right|^2.$$

Applying Lemma 1, it follows that

$$\begin{aligned} &\sum_{Q \in \mathcal{R}_q^*} \left| T_d(S, Q, \mathcal{L}) - \frac{|\mathcal{L}|}{q^{N-2d}} \right| \\ &\qquad \leq |\mathcal{R}_q^*|^{1/2} |\mathcal{L}|^{1/2} q^{-N/2} \sum_{\substack{\mathcal{J} \subseteq \{1,\dots,r\} \\ \mathcal{J} \neq \emptyset}} \prod_{j \notin \mathcal{J}} q^{n_j/2} \sum_{\substack{\mathbf{a} \in \mathcal{A}_{\mathcal{J}} \\ \mathbf{a} \neq \mathbf{0}}} \left| \sum_{\substack{\psi \in \mathcal{R}_q \\ \deg \psi \leq d-1}} \chi_{\mathbf{a}}(\psi) \right|^2. \end{aligned}$$

It is easy to see that

$$\begin{aligned} &\sum_{\substack{\mathbf{a} \in \mathcal{A}_{\mathcal{J}} \\ \mathbf{a} \neq \mathbf{0}}} \left| \sum_{\substack{\psi \in \mathcal{R}_q \\ \deg \psi \leq d-1}} \chi_{\mathbf{a}}(\psi) \right|^2 \\ &\qquad = -q^{2d} + \sum_{\mathbf{a} \in \mathcal{A}_{\mathcal{J}}} \left| \sum_{\substack{\psi \in \mathcal{R}_q \\ \deg \psi \leq d-1}} \chi_{\mathbf{a}}(\psi) \right|^2 \\ &\qquad = -q^{2d} + \sum_{\substack{\varphi, \psi \in \mathcal{R}_q \\ \deg \varphi, \deg \psi \leq d-1}} \sum_{\mathbf{a} \in \mathcal{A}_{\mathcal{J}}} \chi_{\mathbf{a}}(\varphi - \psi) \\ &\qquad = -q^{2d} + \sum_{\substack{\varphi, \psi \in \mathcal{R}_q \\ \deg \varphi, \deg \psi \leq d-1}} \sum_{\mathbf{a} \in \mathcal{A}_{\mathcal{J}}} \prod_{j \in \mathcal{J}} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j\left(\varphi\left(\alpha_j\right) - \psi\left(\alpha_j\right)\right)\right)\right) \\ &\qquad = -q^{2d} + U \prod_{j \in J} q^{n_j}, \end{aligned}$$

where U is the number of pairs of $\varphi, \psi \in \mathcal{R}_q$ with $\deg \varphi, \deg \psi \leq d-1$ and such that $\varphi\left(\alpha_j\right) = \psi\left(\alpha_j\right)$ for all $j \in \mathcal{J}$. Since this condition is equivalent to the polynomial congruence

$$\varphi(X) \equiv \psi(X) \pmod{\prod_{j \in J} \Psi_j(X)},$$

we derive that

$$U = \begin{cases} q^{2d} \prod_{j \in J} q^{-n_j}, & \text{if } d \geq \sum_{j \in J} n_j, \\ q^d, & \text{otherwise.} \end{cases}$$

Hence, in either case

$$0 \le -q^{2d} + U \prod_{j\in J} q^{n_j} \le q^d \prod_{j\in J} q^{n_j},$$

and consequently

$$\sum_{\substack{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}\\ \mathbf{a}\neq\mathbf{0}}} \left| \sum_{\substack{\varphi\in\mathcal{R}_q\\ \deg\varphi\le d-1}} \chi_{\mathbf{a}}(\psi) \right|^2 \le q^d \prod_{j\in J} q^{n_j}.$$

Therefore, we have

$$\begin{aligned}
&\frac{1}{|\mathcal{R}_q^*|} \sum_{Q\in\mathcal{R}_q^*} \left| T_d(S,Q,\mathcal{L}) - \frac{|\mathcal{L}|}{q^{N-2d}} \right| \\
&\quad \le |\mathcal{R}_q^*|^{-1/2} |\mathcal{L}|^{1/2} q^{d-N/2} \sum_{\substack{\mathcal{J}\subseteq\{1,\dots,r\}\\ \mathcal{J}\neq\emptyset}} \prod_{j\notin\mathcal{J}} q^{n_j/2} \prod_{j\in J} q^{n_j} \\
&\quad = |\mathcal{R}_q^*|^{-1/2} |\mathcal{L}|^{1/2} q^{d} \sum_{\substack{\mathcal{J}\subseteq\{1,\dots,r\}\\ \mathcal{J}\neq\emptyset}} \prod_{j\in J} q^{n_j/2} \\
&\quad = |\mathcal{R}_q^*|^{-1/2} |\mathcal{L}|^{1/2} q^{d} \left(\prod_{j=1}^{r} \left(1 + q^{n_j/2}\right) - 1 \right) \\
&\quad < |\mathcal{R}_q^*|^{-1/2} |\mathcal{L}|^{1/2} q^{d} \prod_{j=1}^{r} \left(1 + q^{n_j/2}\right) \\
&\quad = |\mathcal{L}|^{1/2} q^{d-N/2} \prod_{j=1}^{r} \left(1 - q^{-n_j}\right)^{-1/2} \left(1 + q^{n_j/2}\right) \\
&\quad = |\mathcal{L}|^{1/2} q^{d} \prod_{j=1}^{r} \left(1 - q^{-n_j}\right)^{-1/2} \left(1 + q^{-n_j/2}\right).
\end{aligned}$$

Since $(1-x^2)^{-1/2}(1+x) < 3^x$ for every x in the open interval $0 < x < 1/2$, and each term $q^{-n_j/2}$ lies in this interval since $q \ge 5$, we have

$$\prod_{j=1}^{r} \left(1 - q^{-n_j}\right)^{-1/2} \left(1 + q^{-n_j/2}\right) < \prod_{j=1}^{r} 3^{q^{-n_j/2}} \le \prod_{j=1}^{r} 3^{q^{-1/2}} \le 3^{Nq^{-1/2}}.$$

Consequently

$$\frac{1}{|\mathcal{R}_q^*|} \sum_{Q\in\mathcal{R}_q^*} \left| T_d(S,Q,\mathcal{L}) - \frac{|\mathcal{L}|}{q^{N-2d}} \right| < q^d\, 3^{Nq^{-1/2}}\, |\mathcal{L}|^{1/2},$$

and the theorem follows immediately. □

4 Remarks

We remark that for the special set $\mathcal{L}_\varphi$ considered in [5], the bound on $M(\mathcal{J})$ in Lemma 1 can be improved, which leads to a stronger bound in Theorem 1.

We have already mentioned that using polynomials G of small degree can speed up the decryption procedure. It has been shown in [1] that using the method of [7, 8] (see also [4]), one can obtain an analogue of Theorem 1 for polynomials G of the form $G = G_1G_2$ where G_1, G_2 are irreducible polynomials of very small degree; see also [2].

The above result is just one out of many other statements of similar nature which can be proved for the generalization of NTRU introduced in this paper.

Finally, we remark that an analogue of Theorem 1 can be obtained in any polynomial ring of the form $\mathbb{F}_q[X]/F(X)$, where $F(X) \in \mathbb{F}_q[X]$ is a square-free polynomial.

References

1. W. Banks, A. Harcharras and I. E. Shparlinski, 'Short Kloosterman sums for polynomials over finite fields', *Canad J. Math.*, (to appear).
2. W. Banks and I. E. Shparlinski, 'Distribution of inverses in polynomial rings', *Indag. Math.*, **12** (2001), 303–315.
3. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
4. J. Friedlander and H. Iwaniec, 'The Brun–Titchmarsh theorem', *Analytic Number Theory*, Lond. Math. Soc. Lecture Note Series **247**, 1997, 363–372.
5. J. Hoffstein, J. Pipher and J. H. Silverman, 'NTRU: A ring based public key cryptosystem', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1433** (1998), 267–288.
6. J. Hoffstein and J. H. Silverman, 'Optimizations for NTRU', *Proc. the Conf. on Public Key Cryptography and Computational Number Theory, Warsaw, 2000*, Walter de Gruyter, 2001, 77–88.
7. A. A. Karatsuba, 'Fractional parts of functions of a special form', *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **55**(4) (1995), 61–80 (in Russian).
8. A. A. Karatsuba, 'Analogues of Kloosterman sums', *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **55**(5) (1995), 93–102 (in Russian).
9. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
10. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
11. J. H. Silverman, 'Invertibility in truncated polynomial rings', *NTRU Cryptosystem Tech. Report 9*, 1998, 1–8.