The ISC Int'l Journal of Information Security

January 2018, Volume 10, Number 1 (pp. 45–53)

http://www.isecure-journal.org

NETRU: A Non-commutative and Secure Variant of CTRU Cryptosystem

Reza Ebrahimi Atani [1,*], Shahabaddin Ebrahimi Atani [2], and Amir Hassani Karbasi [2]

[1] *Department of Computer Engineering, University of Guilan, Rasht, Iran*

[2] *University Campus 2, Department of Mathematics, University of Guilan, Rasht, Iran*

ARTICLE INFO.

Article history:
Received: 8 February 2016
First Revised: 26 December 2016
Last Revised: 16 October 2017
Accepted: 5 December 2017
Published Online: 10 December 2017

Keywords:
Lattice-based Cryptography, CTRU, Matrix Rings, Finite Fields.

Abstract

In this paper we present a new finite field-based public key cryptosystem (*NETRU*) which is a non-commutative variant of CTRU. The original CTRU is defined by the ring of polynomials in one variable over a finite field $\mathbb{F}_2$. This system works in the ring $R = \mathbb{F}_2[x]/\langle x^N - 1\rangle$ and is already broken by some attacks such as linear algebra attack. We extend this system over finite fields $\mathbb{Z}_p$, where p is a prime (or prime power) and it operates over the non-commutative ring $\mathbf{M} = M_k(\mathbb{Z}_p)[T,x]/\langle X^n - I_{k*k}\rangle$, where $\mathbf{M}$ is a matrix ring of k by k matrices of polynomials in $R = \mathbb{Z}_p[T,x]/\langle x^n - 1\rangle$. In the proposed NETRU, the encryption and decryption computations are non-commutative and hence the system is secure against linear algebra attack as lattice-based attacks. NETRU is designed based on the CTRU core and exhibits high levels of security with two-sided matrix multiplication.

1 Introduction

Some secure communications are provided by the concept of public key cryptography over non-secure channels. Public key cryptography was first presented by Diffie and Hellman in 1976 [1]. So far several public key cryptosystems have been proposed that their underlying security is based on solving some number theoretic and group theoretic problems such as: the integer factoring problem (IFP), the discrete logarithm problem (DLP) in a certain finite group [2], algebraic coding theory [3], the intractability of elliptic curve and the variants of Matsumoto-Imai cryptosystems [4], multivariable polynomials and presumed hardness of lattice problems, the most basic of which are the shortest vector problem (SVP) and the closest vector problem (CVP) [6]. Lattice-based cryptography as a post-quantum field in cryptography has some advantages such as: very strong security proofs, efficient implementations, great simplicity, as well as efficiency in terms of computational and space complexity.

In the recent years, some lattice-based constructions have been presented that their security comes from the conjectured worst-case hardness of lattice problems which are the foundations for public-key encryption [7], digital signatures [9–11], identity-based encryption [12, 13], fully homomorphic encryption [14], and authors' schemes [34–37], and much more.

The NTRU public key cryptosystem officially introduced in 1998 [15]. NTRU is classified as a lattice-based cryptosystem since its security is based on intractability of solving shortest vector problem and closest vector problem in a particular type of lattices called Convolutional Modular Lattices (CML) related to the quotient ring $\mathbb{Z}[x]/\langle x^N - 1\rangle$. Thus, most in-

* Corresponding author.
Email addresses: rebrahimi@guilan.ac.ir (R. Ebrahimi Atani), ebrahimi@guilan.ac.ir (S. Ebrahimi Atani), karbasi@phd.guilan.ac.ir (A. Hassani Karbasi)
ISSN: 2008-2045

volved attacks against NTRU are based on lattice reduction techniques [16] and Chinese Remainder Theorem (CRT) [17]. In a lattice attack, the attacker is trying to find the original key or an alternative key which can be applied instead of original key to decrypt ciphertext with some more computational complexity. In NTRU, every element of the mentioned ring is a polynomial, hence the multiplication of two polynomials is based on linear transformation with $O(N^2)$ operations. Note that one can use *Fast Fourier Transforms* (FFT's) for optimization since these operations are on small integers, allowing for further speed optimizations. Therefore, the speed of NTRU is one of its considerable features. NTRU executes drastically faster than both RSA and ECC at relatively the same security levels [15].

The standard number (version) of NTRU is IEEE P1363.1 [18]. NTRU encryption mainly consists of vector multiplications which is called vector convolutions, a very simple operation without extra computations. This operation is fundamentally different from both RSA and elliptic curve cryptography, and NTRU has some efficiency advantages over them. NTRU has been cryptanalyzed heavily by the cryptographic community, and some interesting results can be found in [17, 19] and some extensions based on non-commutative algebra were proposed in [20]. For improving the security of NTRU, some variants have been proposed using polynomial rings with coefficients in rings other than $\mathbb{Z}$. The most important of these is QTRU, based on Quaternion algebra [21] and authors' lattice-based schemes [34, 35]. In [22], we can find a generalization of NTRU by the ring of polynomials over the binary field $\mathbb{F}_2$ which is called CTRU. Although CTRU is based on $GF(2^k)[x]$, in [22] never had a desirable result and was broken soon after [23], it showed the idea of replacing NTRU algebraic structure with other rings and algebras. We believe that the basic concept on which the CTRU cryptosystem pivots is totally abstract and can be extended to a broader finite fields than $\mathbb{F}_2$ such as $\mathbb{Z}_p$, where p is prime (or prime power).

The CTRU scheme can be summarized as follows [22]:

Let $A := \mathbb{F}_2[T]$ be polynomials in one variable T over the binary finite field $\mathbb{F}_2$ and let $R = A[x]/\langle x^N - 1\rangle$ be the convolution polynomial ring defined over $\mathbb{F}_2[T]$. Hence, an element of R is reflected as: $f(x) = f_0(T) + f_1(T)x + \ldots + f_{N-1}(T)x^{N-1}$ where the coefficient of $x^{i'}s$ for each $0 \leq i \leq N-1$ are: $f_i(T) = f_{i0} + f_{i1}T + \ldots + f_{iki}T^{ki}$ that for all $0 \leq j \leq ki$, we have: $f_{ij} \in \mathbb{F}_2$. Assume that $\langle P\rangle$ and $\langle Q\rangle$ are ideals generated by irreducible polynomials P and Q with degrees s and t, respectively where $\gcd(s,t) = 1$ and $2s \leq s < t$, such that $\mathbb{F}_2 s \cap \mathbb{F}_2 t = \mathbb{F}_2$. Obviously, we have the quotient rings $A_P := A/\langle P\rangle$ and $A_Q := A/\langle Q\rangle$ are isomorphic to finite fields of order 2^s and 2^t, respectively. Thus the quotient rings $R_P := R/\langle P\rangle$ and $R_Q := R/\langle Q\rangle$ are isomorphic to $\mathbb{F}_2 s[T,x]/\langle x^N - 1\rangle$ and $\mathbb{F}_2 t[T,x]/\langle x^N - 1\rangle$, respectively. Suppose the set of all coset representatives for each equivalence class modulo $\langle Q\rangle$ by $l \subset R$. If certain restrictions are imposed on the coefficients of f, g, Φ and m such that the result of $P \cdot g \cdot \Phi + m \cdot f$ lies exactly in l (i.e., $P \cdot g \cdot \Phi + m \cdot f \bmod \langle Q\rangle$ is exactly equal to $P \cdot g \cdot \Phi + m \cdot f \in R$), then one can easily switch from $R/\langle Q\rangle$ to $R/\langle P\rangle$ and follow the rest of the encryption and decryption calculations. The security of CTRU relies on a special instance of the shortest pair of vectors problem (SPVP), that is, it's security is heuristic.

In this paper, we present a non-commutative extension of CTRU, called NETRU. Our focus involves extension to non-commutative groups instead of using group algebra over $\mathbb{Z}_2$. We will prove that our proposed NETRU based on non-commutative algebra is not only feasible but also it has higher security compared to commutative version of CTRU and NTRU encryption scheme.

The NETRU cryptosystem uses a more efficient linear transformation while providing a security level higher than that of CTRU. NETRU operates with appropriate selection of prime p for finite field $\mathbb{Z}_p$. It works in the non-commutative ring $\mathbf{M} = M_k(\mathbb{Z}_p)[T,x]/\langle X^n - I_{k*k}\rangle$, where $\mathbf{M}$ is a matrix ring of k by k matrices of polynomials in $R = \mathbb{Z}_p[T,x]/\langle x^n - 1\rangle$. As matrix multiplication in NETRU is strictly non-commutative and because of two-sided matrix multiplication, search space will be square times than that of CTRU, and then the lattice attack will be extremely hard due to the high dimension of lattice. We can compare an instance of CTRU with NETRU when $nk^2 = N$. Encryption and decryption in CTRU requires $O(N^2t^2)$ or $O(n^2k^4t^2)$ operations for a message block with length of N, but in NETRU for the same bit of information we need $O(n^2k^{2.807}t^2)$ or $O(n^2k^{2.376}t^2)$ operations if we use Strassen's or Coppersmith algorithms for matrix multiplication, respectively. Also since RSA requires $O(N^3)$ operations in the best case for encryption and decryption, so NETRU will be faster than RSA crypto scheme.

The rest of this paper is organized as follows: Section 2 presents some notations, constructions of irreducible polynomials over finite fields and degree estimation for analysis. In Section 3, the main parameter constraints which are required for a reliable encryption/decryption is presented and the proposed

NETRU cryptosystem is described. Details of the security analysis of NETRU is given in Section 4. Section 5 shows performance analysis and comparison with CTRU and NTRU. Finally, the paper concludes in Section 6.

2 Notations

NETRU cryptosystem operates over the ring $\mathbf{M} = M_k(\mathbb{Z}_p)[T,x]/\langle X^n - I_{k*k}\rangle$ of k by k matrices of elements in the ring $R = \mathbb{Z}_p[T,x]/x^n - 1\rangle$. Let n be a positive integer so a typical element of R can be represented as:

$$f(x) = f_0(T)+f_1(T)x+f_2(T)x^2+\cdots+f_{n-1}(T)x^{n-1} \quad (1)$$

where for each $0 \le i \le n-1$ the coefficient of $x^{i'}$ is:

$$f_i(T) = f_{i0} + f_{i1}T + f_{i2}T^2 + \ldots + f_{iz}T^z$$
$$f_{ij} \in \mathbb{Z}_p = \{0,1,\ldots,P-1\}, \text{ where } 0 \le j \le z. \quad (2)$$

Addition (+) in R is performed component wise, and multiplication is a circular convolution. Let P and Q be two irreducible polynomials of $\mathbb{Z}_p[T,x]$ of degree s and t, respectively such that $2 \le s \le t$ and $\gcd(s,t) = 1$. It is worth observing that the quotient rings $A_P := \mathbb{Z}_p[T,x]/\langle P\rangle$ and $A_Q := \mathbb{Z}_p[T,x]/\langle Q\rangle$ are isomorphic to finite fields of order p^s and p^t,respectively. Since P and Q are irreducible polynomials then $\langle P\rangle$ and $\langle Q\rangle$ are maximal ideals, therefore $\mathbb{Z}_p[T,x]/\langle P\rangle$ and $\mathbb{Z}_p[T,x]/\langle Q\rangle$ are finite fields then the existence of a division algorithm gives us several useful properties. Thus the quotient rings $R_P := R/\langle P\rangle$ and $R_Q := R/\langle Q\rangle$ are isomorphic to $\mathbb{Z}_p^s[T,x]/\langle x^n - 1\rangle$ and $\mathbb{Z}_p^t[T,x]/\langle x^n - 1\rangle$ respectively. By the arithmetic constraint $\gcd(s,t) = 1$ we see that $\mathbb{Z}_p^s \cap \mathbb{Z}_p^t = \mathbb{Z}_p$.

For any polynomial $f \in R$, let $\deg_T(f)$ denote the maximum degree of the coefficients of x in T. In other words, $\deg_T(f)$ is computed for f as a polynomial in t . Note that since $\deg(f+g) = \max\{\deg(f),\deg(g)\}$, the function "deg" over $\mathbb{Z}_p[T,x]$ is a Euclidean norm which gives unique quotient and remainder.

2.1 Irreducibility Tests Over Finite Fields $\mathbb{Z}_P$

For a prime (or prime power) p and an integer $n \ge 2$, let $\mathbb{Z}_p$ be a finite field with p elements, and $\mathbb{Z}_p^n$ be its extension of degree n. Extensions of finite fields are important in implementing cryptosystems and error correcting codes such as our proposed NETRU. As an example, a probabilistic algorithm for finding irreducible polynomials that works well in practice is presented in [24]. Let $f \in \mathbb{Z}_p[T,x]$, $\deg_T(f) = n$, be a polynomial to be tested for irreducibility. Assume that $p_1,\ldots,p_k$ are the distinct prime divisors of n. In practice, there are two general approaches for this problem:

- Rabin: f is irreducible iff $\gcd(f, x^{p^{n/p_i}} - x) = 1$ for all $1 \le i \le k$, and $x^{p^n} - x \equiv 0 \mod f$ (see [24]).
- Butler: f is irreducible iff $\dim \ker(\Phi - I) = 1$, where Φ is the Frobenius map on $\mathbb{Z}_p[T,x]/\langle f\rangle$ that sends $\in \mathbb{Z}_p[T,x]/\langle f\rangle$ to $h^p \in \mathbb{Z}_p[T,x]/\langle f\rangle$, and i is the identity map on $\mathbb{Z}_p[T,x]/\langle f\rangle$ (see [25]).

Other irreducibility tests can be found in [26, 27]. We concentrate on Rabin's test and its variant presented in [28].

Theorem 1 ([28]). *The proposed variant of Rabin's algorithm correctly tests for polynomial irreducibility, and uses $O(nM(n)\log p)$ operations in $\mathbb{Z}_p$, where $M(n) = n\log n\log\log n$.*

2.2 Degree Estimation

We define length of an element $\Psi \in \mathbf{M} = M_k(\mathbb{Z}_p)[T,x]/\langle X^n - I_{k*k}\rangle$ to be:

$$|\Psi| = \max\{\deg_T(polys \cdot m \in \Psi)\} \quad (3)$$

The length of matrices $\Psi \in \mathbf{M}$ is the maximum degree in any of k^2 polynomials of it. We say a matrix $\Psi \in \mathbf{M}$ is small if $|\Psi|\deg_T(P)$. When small matrices are multiplied together, we get a matrix which has a length greater than P but is still almost certainly smaller than Q. The definitions for length and shortness apply similarly to polynomials in R. For $f \in R$:

$$|f| = \max\{\deg_T(f)\} \quad (4)$$

The polynomial f is said to be small if $f|\deg_T(P)$. We also define the degree of an element $\Psi \in \mathbf{M}$ to be:

$$\mathrm{Deg}(\Psi) = \{deg_T(polys \cdot m \in \Psi)\} \quad (5)$$

3 NETRU Cryptosystem

3.1 Parameter Creation

NETRU cryptosystem depends on six positive integer parameters (n,k,d_f,d_g,d_b,d_Φ). Let P and Q be two irreducible polynomials of $\mathbb{Z}_p[T,x]$ of degree s and t respectively such that $2 \le s < t$ and $\gcd(s,t) = 1; d_f,d_g,d_b,d_\Phi \le t$, and six sets of matrices $(L_f,L_g,L_b,L_\Phi,L_w,L_m) \subset \mathbf{M}$. The set of matrices $(L_f,L_g,L_b,L_\Phi,L_w,L_m)$ consists of all matrices of polynomials in the ring $R = \mathbb{Z}_p[T,x]/\langle x^{n-1}\rangle$. Define the set $L(d)$ as:

$$L(d) = \{f \in R \,|\, \deg_T(f) < d\} \quad (6)$$

Lemma 1. *The set $L(d)$ has p^{nd} elements.*

Proof. A typical element of $L(d)$ looks like:

$$f(x) = f_0(T)+f_1(T)x+f_2(T)x^2+\ldots+f_{N-1}(T)x^{n-1} \quad (7)$$

where for each $0 \leq i \leq n-1$ the coefficient of x^i's are:

$$f_i(T) = f_{i0} + f_{i1}T + f_{i2}T^2 + \ldots + f_{iz}T^z$$
$$f_{ij} \in \mathbb{Z}_p = \{0, 1, \ldots, p1\}, \text{ where } 0 \leq j \leq z.$$

Hence, applying the elementary counting techniques, we get exactly p^d choices for each f_i. Since the degree in x of f is at most $n-1$, there are p^{nd} different possibilities for f. □

3.2 Key Generation

Suppose that Bob wants to create his set of public and private keys. He randomly chooses $f \in L_f := L(d_f + 1), g \in L_g := L(d_g + 1), b \in L_b := L(d_b + 1)$, and $w \in L_w$, where L_w is a short matrix. Note that matrices f should be invertible modulo both P and Q. Matrices g and b should also have inverse modulo P. We denote these inverses by notation F_P, F_Q, G_P, B_P respectively.

$$\begin{aligned} fFQ &\equiv I \pmod{Q}, \\ gGP &\equiv I \pmod{P}, \\ G_Q g &\equiv I \pmod{Q}, \\ B_P b &\equiv I \pmod{P}. \end{aligned} \tag{8}$$

Then Bob computes the matrices h and H as follows:

$$h \equiv wG_Q \pmod{Q} \tag{9}$$
$$H \equiv F_Q b \pmod{Q} \tag{10}$$

Therefore $(h, H) \in \mathbf{M}$ and (f, g, b) are Bob's sets of public and private keys.

3.3 Parameter Constraint

There are some requirements for true parameter selection that we describe them as follows:

In order to eliminate decryption failure, $f\Phi w$ and bmg should be small. For preventing a private key attack, we choose f, g and b similar to NTRU method. Appropriate selection of Φ and m prevent plain text attack.

It is important in decryption that $f\Phi w$ and bmg are not chosen too large so we should keep $|Pf\Phi w + bmg|$ small. For security reasons, it is the key point that w, remains secret from attacker. Also:

$$\begin{aligned} \mathrm{Deg}(w) &\simeq \mathrm{Deg}(m) \\ \mathrm{Deg}(Pf\Phi w) &\simeq \mathrm{Deg}(bmg) \end{aligned} \tag{11}$$

As already described, we are selecting f from L_f, g from L_g, b from L_b, w from L_w, and m from L_m which gives $d_f = d_\Phi = d_g = d_b = [t - 2s - 1/4]$, that ensures to maximize the number of possible choices for polynomials of these matrices.

3.4 Encryption

Alice chooses her message $m \in L_m := L(s)$ and then she randomly chooses a matrix $\Phi \in L_\Phi := L(d_\Phi + 1)$. She encrypts the message as:

$$e \equiv P\Phi h + Hm \pmod{Q} \tag{12}$$

and then she sends e to Bob.

3.5 Decryption

In order to decrypt the cipher text, Bob first needs to compute:

$$\begin{aligned} a &\equiv feg \pmod{Q} \\ &\equiv f(P\Phi h + Hm)g \pmod{Q} \\ &\equiv fP\Phi hg + fHmg \pmod{Q} \\ &\equiv Pf\Phi wG_Q g + fF_Q bmg \pmod{Q} \\ &\equiv Pf\Phi w + bmg \pmod{Q} \end{aligned} \tag{13}$$

If a is equal to the non-modular expression $Pf\Phi w + bmg$, Bob can compute the matrix C:

$$\begin{aligned} C &\equiv a \pmod{Q}, \\ C &\equiv bmg \pmod{P}. \end{aligned} \tag{14}$$

Finally, Bob uses his other private keys B_P and G_P to recover m as:

$$\begin{aligned} D &\equiv B_P bmg G_P \pmod{P}, \\ D &\equiv m \pmod{P}. \end{aligned} \tag{15}$$

Clearly, D and the non-modular m are equal if and only if each coefficient in the latter has degree less than $\deg_T(Q)$.

Lemma 2. *It is enough to have $2s + d_f + d_\Phi \leq t$ and $d_b + s + d_g \leq t$ simultaneously, for the decryption process to be successful.*

Proof. If $\deg_T(Pf\Phi w + bmg)$ is less than $\deg_T(Q)$, reduction modulo polynomial Q would not change $Pf\Phi w + bmg$. Since it has two components, we need each of them to be of degree less than t. Using, $d(a + b) \leq \max\{d(a), d(b)\}$ for all $a, b \in \mathbb{Z}_p[T, x]$, we conclude:

$$\begin{aligned} &\deg_T(Pf\Phi w + bmg) \leq \deg_T(Q) = t \\ \Leftrightarrow\ &\deg_T(Pf\Phi w) \leq t \text{ and } \deg_T(bmg) \leq t \\ &s + d_f + d_\Phi + s \leq t \text{ and } d_b + s + d_g \leq t \\ \Leftrightarrow\ &2s + d_f + d_\Phi \leq t \text{ and } d_b + s + d_g \leq t. \end{aligned}$$

which completes the proof. □

4 Security Analysis

4.1 Brute Force Attack

To conduct a brute force attack against NETRU, attackers who know the public parameters, including the public key $h \equiv wG_Q$ and $H \equiv F_Q b$ and also,

$b, n, k, d_f, d_g, d_b, d_\Phi, P$ and Q. For obtaining the entire possible keys in $f \in L_f$ and $g \in L_g$ so that $hg \pmod Q$, $fH \pmod Q$ and $b \pmod Q$, it is necessary to find the private keys f, g and b correctly and a short key using these private keys. Therefore, searching pair of (f, g) that f and g are determined by $2k^2$ polynomials are needed. The size of the key space $L_f (\simeq L_g)$ is calculated as follows:

$$\#L_f = \binom{n}{d_f}^{2k^2}\binom{n-d_f}{d_f}^{2k^2} = \left[\frac{n!}{(d_f!)^2(n-2d_f)!}\right]^{2k^2},$$
$$\#L_g = \binom{n}{d_g}^{2k^2}\binom{n-d_g}{d_g}^{2k^2} = \left[\frac{n!}{(d_g!)^2(n-2d_g)!}\right]^{2k^2}. \quad (16)$$

Here d_f and d_Φ are defined by assuming L_f and L_Φ contains polynomials from the set of polynomials $L(d_f + 1)$ and $L(d_\Phi + 1)$, respectively. Note that just like CTRU, f, g and all of their scalar rotations $(x^i \cdot f, x^i \cdot g)$ can be served as decryption key. Using Meet-in-The-Middle attack [29] the search time could be reduced to $\sqrt{\#L_f/nk^2}$ if sufficient memory is provided. Since the total state space which an attacker has to search for an encryption key is about $\#L_f/nk^2$. Similarly, the same attack can also be done against a given message by testing all possible $\Phi \in L_\Phi$ and search for the matrices $e - \Phi h \pmod Q$ which contains polynomials with small entries. Thus, the message security is $\#L_\Phi/nk^2$ for brute force attack and $\sqrt{\#L_\Phi/nk^2}$ for Meet-in-The-Middle attack, where:

$$\#L_\Phi = \left[\frac{n!}{(d_\Phi!)^2\,(n-2d_\Phi)\,!}\right]^{2k^2} \quad (17)$$

Based on parameter choosing method in NTRU and by applying it in the NETRU, our proposed cryptosystem seems to be completely secure against the brute-force attack. Meet-in-The-Middle attack cannot be operated on NETRU because computations involved in decryption are non-commutative.

4.2 Chosen Ciphertext Attacks

Because of similarity among NETRU, CTRU and NTRU, the security and survivability of our proposed cryptosystem against adaptively chosen ciphertext attacks [30] is exactly equivalent to NTRU, then one can use prevention techniques [31] for NETRU.

4.3 Message Expansion

In NETRU the length of the encrypted message is the same as CTRU and is more than the original message and that is part of the price one has to pay for gaining more speed in both cryptosystems. We compute the degree parameters d_f, d_g, d_b and d_Φ in Section 4, therefore the expansion ratio can be easily calculated as $\log |C|/\log|P| = \log|Q|/\log|P| = t/s$, where C is the state space for the encrypted message and P is the state space for plaintext. This should not be a problem if the system is used in conjunction with a symmetric cipher, merely to exchange keys.

4.4 Multiple Transmission Attack

In order to conduct Multiple Transmission Attack, a single message m is sent multiple times by Alice using same public key but different error values $\Phi\,'s$, it is then possible to obtain information on the $\Phi\,'s$. Suppose Alice transmits different encrypted massages $e_i \equiv \Phi_i h + Hm \pmod Q$, then attacker can compute $(e_i - e_1)h \pmod Q$. Therefore recovering $\Phi_i - \Phi_1 \pmod Q$ by repeating this operation with different e_i, attacker will recover enough bits of Φ_1 to allow a brute force attack on the remaining coordinates. Due to this attack we suggest not to use multiple transmissions with further scrambling of particular (underlying) message. However, this attack will work for a single message not for any subsequent messages. We can refer to [21] for more information about this attack.

4.5 Algebraic Attack as a Lattice Attack

Shamir in [16] concluded if one designs a variant of NTRU where the calculations involved during encryption and decryption are non-commutative then the system will be secure against lattice-based attacks. In this paper, our method involves extension of CTRU to broader finite fields and non-commutative algebra together for obtaining robust security against linear algebra attack. In this section we prove that the security of NETRU relies on the intractability of the SPVP. We can attack this cryptosystem if we find a suitable key for decryption by expanding public key pair h, H in which vector (fw, bg) lies as a system of linear equations and form a lattice of dimension $2nk^2$ by $2nk^2$. In other words, we show vectors fw and bg are the same linear transformation of public key vectors for attack. In the following theorem we prove that the security of the proposed scheme relies on the intractability of SPVP in a certain type of lattice and non-linear equations.

Theorem 2. *Let $(h, H) \subset \mathbf{M} = M_k(\mathbb{Z}_p)[T, x]/\langle X^n - I_{k*k}\rangle$, and suppose there exist a transformation $\theta_{f,g}$ which has at least a pair of solutions fw and bg in M, then attacker cannot make a lattice by h and H, which contains the vectors (fw, bg).*

Proof. It is clear that fw and bg are produced from encrypted message by multiplying it by f and g from left and right respectively. We can define the linear map $\theta_{f,g}$ as follows:

$$\theta_{f,g} : M \to M$$
$$h \to fhg \quad \text{or} \quad (h \to fw) \tag{18}$$
$$H \to fHg \quad \text{or} \quad (H \to bg) \tag{19}$$

The private key (fw, bg) viewed as a vector of length $2nk^2$ over $\mathbb{Z}_p[T, x]$ belongs to the lattice L_{NETRU} of dimension and rank nk^2. Let basis vectors produced by the cyclic shift of the coefficients of polynomial of the matrices h and H. The lattice L_{NETRU} is the $\mathbb{Z}_p[T, x]$ span of the rows of the matrix M_{NETRU} defined as:

$$M_{NETRU} = \begin{pmatrix} [I]_{nk^2 \times nk^2} & \begin{bmatrix} h & H \end{bmatrix}_{nk^2 \times nk^2} \\ [0]_{nk^2 \times nk^2} & [Q(T)I]_{nk^2 \times nk^2} \end{pmatrix}_{2nk^2 \times 2nk^2} \tag{20}$$

One can conclude by linear transformation shown in Equations (18) and (19) that the lattice attack is possible if and only if one can make a lattice with public key vectors (h, H) which contains vector (fw, bg) or if following transformation is linear:

$$(h, H) \to (fw, bg) \tag{21}$$

We show in the following analysis that transformation $h \to fhg$ is not linear. Similarly, one can prove $H \to fHg$ and $(h, H) \to (fw, bg)$ are not linear. Consider the multiplication of the matrices $f \cdot h \cdot g = fw$, where each matrix (f, g, h, fw) having k^2 short polynomials as elements:

$$\begin{bmatrix} f_1 & \dots & f_k \\ \dots & \dots & \dots \\ f_{k(k-1)} & \dots & f_{k^2} \end{bmatrix} \cdot \begin{bmatrix} h_1 & \dots & h_k \\ \dots & \dots & \dots \\ h_{k(k-1)} & \dots & h_{k^2} \end{bmatrix} \cdot \begin{bmatrix} g_1 & \dots & g_k \\ \dots & \dots & \dots \\ g_{k(k-1)} & \dots & g_{k^2} \end{bmatrix}$$
$$= \begin{bmatrix} fw_{1,1} & \dots & fw_{1,k} \\ \dots & \dots & \dots \\ fw_{k,1} & \dots & fw_{k,k} \end{bmatrix} \tag{22}$$

Now we can show system of equations as follows:

$$g_1 f_1 h_1 + g_{k+1} f_1 h_2 + g_{2k+1} f_1 h_3 + \ldots +$$
$$g_{k(k-1)+1} f_1 h_k + g_1 f_2 h_{k+1} + \ldots + g_{k(k-1)+1} f_2 h_{2k} +$$
$$\ldots + g_{k(k-1)+1} f_k h_k^2 = (fw)_{1,1}$$
$$g_2 f_1 h_1 + \ldots + g_{k(k-1)+2} f_k h_k^2 = (fw)_{1,2}$$
$$\vdots$$
$$g_k h_1 f_{k(k-1)+1} + g_{2k} h_2 f_{k(k-1)+1} + \ldots +$$
$$g_k^2 h_k f_{k(k-1)+1} + \ldots + g_k^2 h_k^2 f_k^2 = (fw)_{k,k}$$

So general term can be represented as:

$$(fw)_{i,j} = \sum_{m=k(i-1)+1}^{ki} \sum_{s=0}^{k-1} f_m (g_{j+sk})(h_{(1+s)(m-k(i-1))}) \tag{23}$$

Or, another form is: $(fw)_{i,j} = \sum f_l g_m h_z = \sum U_z h_z$, where, $i, j, l, m \in [1, k^2]$; $z \in [1, k^4]$.

As all U_z are different so we cannot find a row vector $X_i = (x_1, x_2, \ldots, x_k^2)$ that will produce vector fw on multiplying with a Lattice represented by the cyclic shift of the coefficients of polynomial of h. In other words, we cannot find different vector X_i to multiply $M_{NETRU}(V)$ with $v_1, v_2, \ldots, v_{nk}^2$ to get fw as a short lattice vector and system (23) is a hard non-linear system of equation. We therefore conclude:

$$fw \neq X_i L_{NETRU}(v_1, v_2, \ldots, v_{nk}^2) \tag{24}$$

which completes the proof. □

Thus we proved that one cannot make a lattice by h and H, which contains the vectors (fw, bg). So lattice attack will not work for NETRU cryptosystem. Note that, in a lattice of relatively small dimension, we can enumerate all short vectors using exhaustive search, but beyond dimension 100, exhaustive search is practically infeasible [32, 33]. Therefore, attacker can use polynomial-time lattice-reduction algorithms such as LLL algorithm or linear algebra attack. CTRU simply replaces the role played by $\mathbb{Z}$ in NTRU by $\mathbb{F}_2[T]$. The role of LLL algorithm is played by Popov form. It can be presumed that the hard lattice problem underlying NTRU becomes the elementary linear algebra problem for CTRU cryptosystem. Notice that NETRU like CTRU enjoys the security against attacks based on LLL algorithm or Chinese Remainder Theorem which are the biggest threat to original NTRU cryptosystem. But CTRU neither give any speed improvement over NTRU, nor security against polynomial time linear algebra attacks.

5 Performance Analysis and Comparison with CTRU and NTRU

We compare the theoretical operating characteristics of NETRU with those of CTRU and NTRU, as shown in Table 1. NETRU cryptosystem depends on four positive integer parameters (n, k, s, t) with s and t relatively prime and six sets of matrices $(L_f, L_g, L_b, L_\Phi, L_w, L_m) \subset \mathbf{M}$. The properties are listed in terms of the parameters (N, s, t) for CTRU and (N, p, q) for NTRU. These should be compared by setting $N = nk^2$, since this equates to plaintext message blocks of the same size.

In Table 1, since NETRU perform two-sided multiplication during decryption process, the constant factor will be about twice higher than of CTRU and NTRU. For popov normal form attack, NETRU needs two public keys that each of them has double length than that of CTRU and NTRU public keys while the size of private keys are the same. NETRU gives significant speed improvement over CTRU and NTRU. We can further reduce the number of encryption and decryption operations to $O(n \log nk^{2.376} t^2)$, if we use

Table 1. Comparison of NETRU, NTRU and CTRU.

Characteristic	**CTRU [22]**	**NTRU [15]**	**NETRU**
Plain Text Block	Ns (bits)	$N \log_2 p$ (bits)	nk^2s (bits)
Encrypted Text Block	Nt (bits)	$N \log_2 q$ (bits)	nk^2t (bits)
Encryption Speed	$O(N^2t^2)$ operations	$O(N^2)$ operations	$O(n^2k^3t^2)$ operations
Decryption Speed	$O(N^2t^2)$ operations	$O(N^2)$ operations	$O(n^2k^3t^2)$ operations
Message Expansion	t-to-1	$\log_p q$-to-1	t-to-1
Private Key Length	$2Ns$ (bits)	$2N \log_2 p$ (bits)	$2nk^2s$ (bits)
Public Key Length	Nt (bits)	$N \log_2 q$ (bits)	$2nk^2t$ (bits)
Key Security	$\frac{N!}{(d_g!)^2(N-2d_g)!}$	$\frac{N!}{(d_g!)^2(N-2d_g)!}$	$\left[\frac{n!}{(d_g!)^2(n-2d_g)!}\right]^{2k^2}$ $(d_g = d_f)$
Message Security	$\frac{N!}{(d_\Phi!)^2(N-2d_\Phi)!}$	$\frac{N!}{(d_\Phi!)^2(N-2d_\Phi)!}$	$\left[\frac{n!}{(d_\Phi!)^2(n-2d_\Phi)!}\right]^{2k^2}$
Total Security	Broken	Secure	Totally Secure

FFT for polynomial multiplication, which is considerable speed improvement over CTRU and NTRU.

6 Conclusion

The CTRU scheme, a variant of NTRU encrypt over ring $R = \mathbb{F}_2[x]/\langle x^N - 1\rangle$, is secure against Popov Normal Form attack but completely insecure against linear algebra attacks as a different form of lattice attacks. We extend this system over finite fields $\mathbb{Z}_p$, that it operates in the non-commutative matrix ring of k by k matrices of polynomials in $R = \mathbb{Z}_p[T, x]/\langle x^n - 1\rangle$. NETRU security level is comparable to CTRU with respect to several well-known attacks with significant speed improvement. Also, we have shown that NETRU cryptosystem is more secure than CTRU, because of its lattice structure and robustness against linear algebra attack. In this paper, we proved that using non-commutativity in a lattice-based cryptosystem is not only possible, but also if we design a non-commutative public key cryptosystem similar to NETRU, it will be secure and efficient. In the end, we would like to point out that NETRU is the first step in extension of the CTRU public key cryptosystems with a non-commutative matrix rings in broader finite fields. Furthermore, NETRU can be generalized to different types of rings, modules, and vector spaces, or different kinds of algebras in order to design new lattice-based cryptosystems and explore their possible advantages.

References

[1] W. Diffie, and M.E. Hellman, *New directions in cryptography*, In IEEE Trans. On Information Theory, (1976), Vol. 22, pages 644-654.

[2] N. Koblitz, and A.J. Menezes, *A Survey of Public Key Cryptosystems*, SIAM Review, (2004), Vol. 46, No. 4, pages 599-634.

[3] R.J. McEliece, *A public key cryptosystem based on algebraic coding theory*, JPL DSN Progress Report, (1978), No. 42-44, pages 114-116.

[4] T. Matsumoto, and H. Imai, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, In Proceeding of Eurocrypt '88, (1988), LNCS of vol. 330, Springer-Verlag, pages 419-453.

[5] J. Ding, *A new variant of the Matsumoto-Imai cryptosystem through perturbation*, In Proceeding of PKC '04, (2004), LNCS of vol. 2947, Springer-Verlag, pages 305-318.

[6] O. Regev, *Lattice-based cryptography*, In Advances in cryptology-CRYPTO, (2006), pages 131–141.

[7] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, J. ACM, (2005), Vol. 56, No. 6, pages 1–40. Preliminary version in STOC 2005.

[8] C. Peikert, V. Vaikuntanathan, and B. Waters, *A framework for efficient and composable oblivious transfer*, In CRYPTO, (2008), pages 554–571.

[9] X. Boyen, *Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more*, In Public Key Cryptography, (2010), pages 499–517.

[10] C. Gentry, C. Peikert, and V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, In STOC, (2008), pages 197–206.

[11] V. Lyubashevsky, *Lattice signatures without trapdoors*, In EUROCRYPT, (2012), pages 738–755.

[12] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, *Bonsai trees, or how to delegate a lattice basis*, In EUROCRYPT, (2010), pages 523–552.

[13] S. Agrawal, D. Boneh, and X. Boyen, *Lattice basis delegation in fixed dimension and shorter ciphertext hierarchical IBE*, In CRYPTO, (2010), pages 98–115.

[14] Z. Brakerski and V. Vaikuntanathan, *Efficient*

fully homomorphic encryption from (standard) LWE, In FOCS, (2011), pages 97–106.

[15] J. Hoffstein, J. Pipher, and J.H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, In Proceedings of the 3rd International Symposium on Algorithmic Number Theory (ANTS-III), (1998), pages 267-288.

[16] D. Coppersmith, and A. Shamir, *Lattice attacks on NTRU*, in *EUROCRYPT*, (1997), pages 52–61.

[17] C. Gentry, *Key recovery and message attacks on NTRU-composite*, Eurocrypt 01, (2001), Springer LNCS 2045, pages 182-194.

[18] Standard Specifications for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. IEEE P1363, 2008. Available at http://grouper.ieee.org/groups/1363/.

[19] D. Han, J. Hong, J.W. Han, and D. Kwon, *Key recovery attacks on NTRU without ciphertext validation routine*, In Proceeding of ACISP '03, (2003), LNCS of vol. 2727, Springer-Verlag, pages 274-284.

[20] M. Coglianese, and B. M. Go, *MaTRU: A New NTRU-Based Cryptosystem*, INDOCRYPT, Lecture Notes in Computer Science, (2005), No. 3797 pages 232-243.

[21] E. Malekian, A. Zakerolhosseini, and A. Mashatan, *QTRU: Quaternionic Version of the NTRU Public Key Cryptosystems*, The int'l Journal of information Security (ISeCure), (2011), Vol. 3, No. 1, pages 29-42.

[22] P. Gaborit, J. Ohler, and P. Sole, *CTRU, a polynomial analogue of NTRU*, Technical report, INRIA, (2002).

[23] R. Kouzmenko, *Generalizations of the NTRU Cryptosystem*, Master's thesis, Polytechnique Montreal, Canada, (2006).

[24] M. O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comp., (1980), No. 9, pages 273-280.

[25] M. Butler, *On the reducibility of polynomials over a finite field*, Quart. J. Math. Oxford 5 (1954), pages 102-107.

[26] J. von zur Gathen, and V. Shoup, *Computing Frobenius maps and factoring polynomials*, Comput complexity, (1992), No. 2, pages 187-224.

[27] V. Shoup, *Fast construction of irreducible polynomials over finite fields*, J. Symb. Comp., (1995), No. 17, pages 371-391.

[28] M. Ben-Or, *Probabilistic algorithms in finite fields*, In Proc. 22nd IEEE Symp. Foundations Computer Science, (1981), pages 394-398.

[29] N. Howgrave-Graham, J.H. Silverman, and W. Whyte, *A Meet-In-The-Middle Attack on an NTRU Private Key*, Technical report, Security Innovation Inc., Boston, MA, USA, (2002). Available at http://securityinnovation.com/cryptolab/pdf/NTRUTech004v2.pdf.

[30] E. Jaulmes, and A. Joux, *A Chosen Ciphertext Attack against NTRU*, In Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology-CRYPTO, (2000), pages 20-36.

[31] J. Hoffstein, and J. Silverman, *Optimizations for NTRU*, Technical Report 015, NTRU Cryptosystems, (2000). Available at http://www.sisecure.com/cryptolab/pdf/ TECH_ARTICLE_OPT.pdf.

[32] P.Q. Nguyen, and D. Stehle, *LLL on the Average*, In Proceedings of the 7th International Symposium on Algorithmic Number Theory (ANTS-VII), (2006), pages 238-256.

[33] P.Q. Nguyen, and D. Stehle, *Low Dimensional Lattice Basis Reduction Revisited*, ACM Transactions on Algorithms, (2009), Vol. 5, No. 4, pages 1-48.

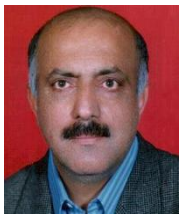
[34] R.E. Atani, S.E. Atani, and A.H. Karbasi, *EEH: A GGH-Like Public Key Cryptosystem Over The Eisenstein Integers Using Polynomial Representation*, The ISC International Journal of Information Security, (2015), Vol. 7, No. 2, pages 115-126.

[35] A.H. Karbasi, and R.E. Atani, *ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices*, IACR Cryptology ePrint Archive 2015: 549, (2015).

[36] A.H. Karbasi, R.E. Atani, and S.E. Atani, *A New Ring-Based SPHF and PAKE Protocol On Ideal Lattices*, Submitted.

[37] S.E. Atani, R.E. Atani, and A.H. Karbasi, *PairTRU: Pairwise Non-commutative Extension of The NTRU Public key Cryptosystem*, Submitted.

Reza Ebrahimi Atani studied electronics engineering at University of Guilan, Rasht, Iran and obtained his B.S. in 2002. He followed his masters and Ph.D. studies at Iran University of Science & Technology in Tehran, and received Ph.D. in 2010. He has an associated professor position in department of computer engineering at University of Guilan. His main research interests focuses on design and implementation of cryptographic algorithms and protocols as well as their applications in computer and network security and mobile communications.



Shahabaddin Ebrahimi Atani got his B.S. and M.S. in Mathematics. In 1996, he obtained his Ph.D. from mathematical science department of University of Manchester, England, UK. He is now a professor at the faculty of mathematical sciences of University of Guilan. His research interests include rings and semi-ring theory and cryptography.

Amir Hassani Karbasi studied his B.S. in applied mathematics at University of Tabriz in Tabriz, Iran. He received his B.S. degree in 2010. He was accepted to follow his Masters study at the University of Guilan in Rasht, Iran. He received his M.S. in computer networks in 2013. He is now a Ph.D. candidate working on "design, analysis and implementation of lattice-based cryptography". He is a student member of IEEE and Iranian Society of Cryptology. His main research interests include lattice-based cryptography, digital signatures, network security, rings and semi-ring theory and pullback of rings.