Scientific Research Publishing

Journal of Information Security, 2022, 13, 165-180
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Generalization of NTRUEncrypt

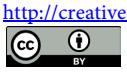
—Cryptosystem Based on Ideal Lattice

Zhiyong Zheng[1], Fengxia Liu[2], Wenlin Huang[1], Jie Xu[1], Kun Tian[1*]

[1]Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering, Renmin University of China, Beijing, China
[2]Artificial Intelligence Research Institute, Beihang University, Beijing, China
Email: *tkun19891208@ruc.edu.cn

How to cite this paper: Zheng, Z.Y., Liu, F.X., Huang, W.L., Xu, J. and Tian, K. (2022) A Generalization of NTRUEncrypt. *Journal of Information Security*, **13**, 165-180.
https://doi.org/10.4236/jis.2022.133010

Received: April 27, 2022
Accepted: July 10, 2022
Published: July 13, 2022



Abstract

The purpose of this article is to extend the theory of circulant matrix to general ideal matrix, and to construct more general NTRU cryptosystem combined with the ϕ-cyclic code. To understand our construction, first we discuss a more general form of the ordinary cyclic code, namely ϕ-cyclic code, which firstly appeared in [1] and [2], thus we give a more generalized NTRUEncrypt by replacing finite field with real number field $\mathbb{R}$.

Keywords

ϕ-Cyclic Code, Ideal Matrices, Convolutional Modular Lattice, NTRU

1. Introduction

Lattice theory based cryptography is a representative technology of post quantum cryptography, which is recognized by the academic community as being able to resist quantum computing attacks. Cyclic code and the number theory research unit (NTRU) cryptosystem are two representatives of the post quantum cryptography. Both the two cryptosystems are based on the theory of circulant matrix. Cyclic code plays a central role in algebraic coding theory (see Chapter 6 of [3]). An important class of cyclic code named BCH code was discovered in 1960 [4]. After that, many other codes were developed based on cyclic code, such as polynomial code, Goppa code and so on [5]. The ϕ-cyclic code was firstly introduced in [1], which was applied to McEliece and Niederriter's cryptosystems.

NTRU cryptosystem is a new public key cryptosystem based on lattice hard problem proposed in 1996 by three digit theorists Hoffstein, Piper and Silverman of Brown University in the United States [6]. Its main feature is that the key

generation is very simple, and the encryption and decryption algorithm is much faster than the commonly used RSA and elliptic curve cryptography. In particular, NTRU can resist quantum computing attacks and is considered to be a potential public key cryptography that can replace RSA in the post quantum cryptography era. The essence of NTRU cryptographic design is the generalization of RSA on polynomials, so it is called the cryptosystem based on polynomial rings. However, NTRU can give a completely equivalent form by using the concept of q-ary lattice, so NTRU is also a lattice based cryptosystem.

Many researchers have presented some variations of NTRU by changing its algebraic structure. In 2002, Gaborit introduced an NTRU-like cryptosystem called CTRU by replacing the base ring of the NTRU with a polynomial ring over a binary field $F_2[x]$ [7]. They proved that their system is successfully decrypted. In 2005, Kouzmenko showed that CTRU is weak under a time attack and proposed the GNTRU cryptosystem based on Gaussian integers $Z[i]$ [8]. In the same year, Coglianese introduced an analog to the NTRU cryptosystem called MaTRU [9]. MaTRU is based on a ring of all square matrices with polynomial entries. In 2009, Malekian introduced the QTRU cryptosystem based on quaternion algebra [10]. They also introduced the OTRU cryptosystem in 2010 based on Octonion algebra [11]. In 2016, Alsaidi proposed a public key cryptosystem BITRU based on binary algebra [12]. However, all of the above variations of NTRU have limitations. The purpose of this article is to extend the theory of circulant matrix to general ideal matrix, and to construct more general NTRU cryptosystem combined with the ϕ-cyclic code. The motivation of this research is to adapt the distributed scenario of blockchain architecture and apply the post quantum cryptography in it.

2. ϕ-Cyclic Code

Let F_q be a finite field with q elements and q be a power of a prime number, $F_q[x]$ be the polynomial ring of F_q with variable x. Let F_q^n be the n-dimensional linear space over F_q, and $a=(a_0,a_1,\cdots,a_{n-1})\in F_q^n$ be a fixed vector in F_q^n with $a_0\neq 0$, the associated polynomial of a given by

$$\phi(x)=\phi_a(x)=x^n-a_{n-1}x^{n-1}-\cdots-a_1x-a_0\in F_q[x],\ a_0\neq 0. \tag{1.1}$$

Let $\langle\phi(x)\rangle$ be the principal ideal generated by $\phi(x)$ in $F_q[x]$. There is a one to one correspondence between F_q^n and the quotient ring $R=F_q[x]/\langle\phi(x)\rangle$, given by

$$c=(c_0,c_1,\cdots,c_{n-1})\in F_q^n \rightleftarrows c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in R. \tag{1.2}$$

In fact, this correspondence is also an isomorphism of Abel groups. One may extend this correspondence to subsets of F_q^n and R by

$$C\subset F_q^n \rightleftarrows C(x)=\{c(x)\,|\,c\in C\}\subset R. \tag{1.3}$$

If $C\subset F_q^n$ is a linear subspace of F_q^n of dimension k, then C is called a linear code in coding theory and written by $C=[n,k]$ as usual. Each vector

$c=(c_0,c_1,\cdots,c_{n-1})\in C$ is called a codeword of length n. Obviously, $C=[n,0]$ and $C=[n,n]$ are two trivial codes. Another one is called constant codes, which is almost trivial given by

$$C=\{(b,b,\cdots,b)\mid b\in F_q\},\ \text{and}\ C=[n,1].$$

According to the given polynomial $\phi(x)=\phi_a(x)$, we may define a linear transformation τ_ϕ in F_q^n,

$$\tau_\phi(c)=\tau_\phi((c_0,c_1,\cdots,c_{n-1}))=(a_0c_{n-1},c_0+a_1c_{n-1},\cdots,c_{n-2}+a_{n-1}c_{n-1}) \tag{1.4}$$

It is easily seen that $\tau_\phi:F_q^n\to F_q^n$ is a linear transformation.

Definition 1.1. Let $C\subset F_q^n$ be a linear code. It is called a ϕ-cyclic code, if

$$\forall c\in C\Rightarrow\tau_\phi(c)\in C. \tag{1.5}$$

In other words, a linear code C is a ϕ-cyclic code, if and only if C is closed under linear transformation τ_ϕ. Clearly, if $a=(1,0,\cdots,0)$, and $\phi_a(x)=x^n-1$, then the ϕ-cyclic code is precisely the ordinary cyclic code (see Chapter 6 of [1]).

Remark The ϕ-cyclic code we give here is polycyclic code in fact, which firstly appeared in [1] [2], but we mainly concern for its application to McEliece and Niederriter's cryptosystems. We first show that there is a one to one correspondence between ϕ-cyclic codes in F_q^n and ideals in $R=F_q[x]/\langle\phi(x)\rangle$.

Theorem 1. Let $C\subset F_q^n$ be a subset, then C is a ϕ-cyclic code, if and only if $C(x)$ is an ideal of R.

Proof: We use column notation for vector in F_q^n, then linear transformation τ_ϕ may be written as

$$\tau_\phi\begin{pmatrix}c_0\\c_1\\\vdots\\c_{n-1}\end{pmatrix}=\begin{pmatrix}a_0c_{n-1}\\c_0+a_1c_{n-1}\\\vdots\\c_{n-2}+a_{n-1}c_{n-1}\end{pmatrix},\quad\forall c=\begin{pmatrix}c_0\\c_1\\\vdots\\c_{n-1}\end{pmatrix}\in F_q^n.$$

Let T_ϕ be a $n\times n$ square matrix over F_q,

$$T_\phi=\begin{pmatrix}0&\cdots&0&a_0\\&&&a_1\\&I_{n-1}&&\vdots\\&&&a_{n-1}\end{pmatrix}\in F_q^{n\times n}. \tag{1.6}$$

where I_{n-1} is the $(n-1)\times(n-1)$ unit matrix. The matrix expression of τ_ϕ as follows

$$\tau_\phi\begin{pmatrix}c_0\\c_1\\\vdots\\c_{n-1}\end{pmatrix}=T_\phi\begin{pmatrix}c_0\\c_1\\\vdots\\c_{n-1}\end{pmatrix}=\begin{pmatrix}a_0c_{n-1}\\c_0+a_1c_{n-1}\\\vdots\\c_{n-2}+a_{n-1}c_{n-1}\end{pmatrix}. \tag{1.7}$$

Suppose $C\subset F_q^n$ and $C(x)$ is an ideal of R, it is clear that C is a linear code of F_q^n. To prove C is a ϕ-cyclic code, we note that for any polynomial $c(x)\in C(x)$, then $xc(x)\in C(x)$ if and only if $\tau_\phi(c)\in C$, namely, if

$c(x) \in C(x)$, then

$$xc(x) \in C(x) \Leftrightarrow \tau_\phi(c) \in C \Leftrightarrow T_\phi c \in C. \tag{1.8}$$

Therefore, if $C(x)$ is an ideal of R, then we have immediately that C is a ϕ-cyclic code of F_q^n.

Conversely, if $C \subset F_q^n$ is a ϕ-cyclic code, then for all $k \geq 1$, we have

$$\forall c \in C \Rightarrow T_\phi^k c \in C,\ k \geq 1.$$

It follows that

$$\forall c(x) \in C(x) \Rightarrow x^k c(x) \in C(x),\ 0 \leq k \leq n-1,$$

which implies $C(x)$ is an ideal of R. This is the proof of Theorem 1. □

By Theorem 1, to find a ϕ-cyclic code, it is enough to find an ideal of R. There are two trivial ideals $C(x) = 0$ and $C(x) = R$, the corresponding ϕ-cyclic codes are $C = [n, 0]$ and $C = F_q^n$ respectively, which are called trivial ϕ-cyclic code. To find non-trivial ϕ-cyclic codes, we make use of homomorphic theorems, which is a standard technique in Algebra. Let π be the natural homomorphism from $F_q[x]$ to its quotient ring $R = F_q[x]/\langle \phi(x) \rangle$, $\ker \pi = \langle \phi(x) \rangle$,

$$\langle \phi(x) \rangle \subset N \subset F_q[x] \xrightarrow{\pi} R = F_q[x]/\langle \phi(x) \rangle, \tag{1.9}$$

where N is an ideal of $F_q[x]$, which is containing $\ker \pi = \langle \phi(x) \rangle$. Since $F_q[x]$ is a principal ideal domain, then $N = \langle g(x) \rangle$ is a principal ideal generated by a monic polynomial $g(x) \in F_q[x]$. It is easy to see that

$$\langle \phi(x) \rangle \subset \langle g(x) \rangle \Leftrightarrow g(x) \mid \phi(x).$$

It follows that all ideals N satisfying (1.9) are given by

$$\{\langle g(x) \rangle \mid g(x) \in F_q[x] \text{ is monic and } g(x) \mid \phi(x)\}.$$

We write by $\langle g(x) \rangle \mod \phi(x)$, the image of $\langle g(x) \rangle$ under π, it is easy to check

$$\langle g(x) \rangle \bmod \phi(x) = \{h(x)g(x) \mid h(x) \in F_q[x] \text{ and } \deg h(x) + \deg g(x) < n\}, \tag{1.10}$$

more precisely, which is a representative elements set of $\langle g(x) \rangle \mod \phi(x)$, by homomorphism theorem in ring theory, all ideals of R given by

$$\{\langle g(x) \rangle \bmod \phi(x) \mid g(x) \in F_q[x] \text{ is monic and } g(x) \mid \phi(x)\}. \tag{1.11}$$

Let d be the number of monic divisors of $\phi(x)$ in $F_q[x]$, we can get the following corollary immediately.

Corollary 1. The number of ϕ-cyclic code in F_q^n is d.

To compare the ϕ-cyclic code and ordinary cyclic code, we see a simple example.

Example 1. Constant code C is always a cyclic code for $1 + x + \cdots + x^{n-1} \mid x^n - 1$, and its generated polynomial is just $1 + x + \cdots + x^{n-1}$. But constant code C in F_q^n is not always a ϕ-cyclic code, it is a ϕ-cyclic code if and only if

$1+x+\cdots+x^{n-1} \mid \phi(x)$, an equivalent condition for $1+x+\cdots+x^{n-1} \mid \phi(x)$ is

$$a_{n-1}=a_{n-2}=\cdots=a_1=b, \text{ and } a_0=1+b.$$

Definition 1.2. Let C be a ϕ-cyclic code and $C(x)=g(x) \mod \phi(x)$. We call $g(x)$ is the generated polynomial of C, where $g(x)$ is monic and $g(x) \mid \phi(x)$.

Lemma 1.1. Let $g(x)=g_0+g_1x+\cdots+g_{n-k-1}x^{n-k-1}+x^{n-k}$ be the generated polynomial of a ϕ-cyclic code C, where $1 \le k \le n-1$, and $g(x) \mid \phi(x)$, then $C=[n,k]$ and a generated matrix for C is the following block matrix

$$G=\begin{pmatrix} g \\ \tau_\phi(g) \\ \tau_\phi^2(g) \\ \vdots \\ \tau_\phi^{k-1}(g) \end{pmatrix}_{k\times n}, \tag{1.12}$$

where $g=(g_0,g_1,\cdots,g_{n-k-1},1,0,\cdots,0) \in C$ is the corresponding codeword of $g(x)$, and $\tau_\phi^i(g)=\tau_\phi^{i-1}(\tau_\phi(g))$ for $1 \le i \le n-1$.

Proof: By assumption, $C(x)=\langle g(x) \rangle \mod \phi(x)$, then $\{g,\tau_\phi(g),\cdots,\tau_\phi^{k-1}(g)\} \subset C$, we are to prove it is a basis of C. First, these vectors are linearly independent. Otherwise, we have

$$\sum_{i=0}^{k-1} b_i \tau_\phi^i(g)=0, \text{ for some } b_i \in F_q, \tag{1.13}$$

and the corresponding polynomial is zero, namely

$$\left(\sum_{i=0}^{k-1} b_i x^i\right) g(x)=0.$$

It follows that

$$\sum_{i=0}^{k-1} b_i x^i=0 \Rightarrow b_i=0 \text{ for all } i,\ 0 \le i \le k-1.$$

Next, if $c \in C$, and $c(x) \in C(x)$, by (1.10), there is a polynomial $b(x)=b_0+b_1x+\cdots+b_{k-2}x^{k-2}+x^{k-1}$ such that

$$c(x)=b(x)g(x)=\left(\sum_{i=0}^{k-1} b_i x^i\right) g(x), \text{ where } b_{k-1}=1.$$

Thus we have the corresponding codeword of $C(x)$

$$c=\sum_{i=0}^{k-1} b_i \tau_\phi^i(g).$$

This shows that $\{g,\tau_\phi(g),\cdots,\tau_\phi^{k-1}(g)\}$ is a basis of C, and a generated matrix for C is

$$G=\begin{pmatrix} g \\ \tau_\phi(g) \\ \tau_\phi^2(g) \\ \vdots \\ \tau_\phi^{k-1}(g) \end{pmatrix}_{k\times n}.$$

We have lemma 1.1 at once. □

To describe a parity check matrix for a ϕ-cyclic code, for any $c=(c_0,c_1,\cdots,c_{n-1})\in F_q^n$, we write

$$\overline{c}=(c_{n-1},c_{n-2},\cdots,c_1,c_0)\in F_q^n.$$

Lemma 1.2. Suppose C is a ϕ-cyclic code with generated polynomial $g(x)$, where $g(x)\mid\phi(x)$ and $\deg g(x)=n-k$. Let $h(x)g(x)=\phi(x)$, where $h(x)=h_0+h_1x+\cdots+h_{k-1}x^{k-1}+x^k$. Then a parity check matrix for C is

$$H=\begin{pmatrix}\overline{h}\\ \tau_\phi(\overline{h})\\ \vdots\\ \tau_\phi^{n-k-1}(\overline{h})\end{pmatrix}_{(n-k)\times n}. \tag{1.14}$$

Proof: Since $h(x)g(x)=\phi(x)$, it means that $h(x)g(x)=0$ in $R=F_q[x]/\langle\phi(x)\rangle$, thus we have

$$g_0h_i+g_1h_{i-1}+\cdots+g_{n-k}h_{i-n+k}=0,\ \forall 0\le i\le n-1.$$

It follows that $GH'=0$, where G is a generated matrix for C given by (1.12). Therefore, H is a parity check matrix for C. □

A separable polynomial in Algebra means that it has no multiple roots in its splitting field. The following lemma shows that there is a unit element in any non-zero ideal of R, when $\phi(x)$ is a separable polynomial.

Lemma 1.3. Suppose $\phi(x)$ is a separable polynomial of F_q, and $C(x)=g(x) \mod \phi(x)$ is an ideal of R with $\deg g(x)\le n-1$, then there exists an element $d(x)\in C(x)$ such that

$$c(x)d(x)=c(x),\ \text{for all } c(x)\in C(x).$$

Proof: Let $h(x)g(x)=\phi(x)$. Since $\phi(x)$ is a separable polynomial, then gcd $(g(x),h(x))=1$, and there are two polynomial $a(x)$ and $b(x)$ in $F_q[x]$ such that

$$a(x)g(x)+b(x)h(x)=1.$$

Let

$$d(x)=a(x)g(x)=1-b(x)h(x)\in C(x).$$

If $c(x)\in C(x)$, by (1.10), we write $c(x)=g(x)g_1(x)$, it follows that

$$\begin{aligned}c(x)d(x)&\equiv a(x)g(x)g(x)g_1(x)\equiv(1-b(x)h(x))g(x)g_1(x)\\&\equiv g(x)g_1(x)\equiv c(x)(\mathrm{mod}\,\phi(x)).\end{aligned}$$

Thus we have $c(x)d(x)=c(x)$ in R. □

Next, we discuss maximal ϕ-cyclic code. Let $C(x)=g(x) \mod \phi(x)$, and $g(x)$ be an irreducible polynomial in $F_q[x]$, we call the corresponding ϕ-cyclic code C a maximal ϕ-cyclic code, because $\langle g(x)\rangle$ is a maximal ideal in $F_q[x]$.

Lemma 1.4. Let C be a maximal ϕ-cyclic code with generated polynomial

$g(x)$, β be a root of $g(x)$ in some extensions of F_q, then

$$C(x)=\{a(x)\mid a(x)\in R \text{ and } a(\beta)=0\}. \tag{1.15}$$

Proof: If $a(x)\in C(x)$, by (1.10) we have $a(\beta)=0$ immediately. Conversely, if $a(x)\in F_q[x]$ and $a(\beta)=0$, since $g(x)$ is irreducible, thus we have $g(x)\mid a(x)$, and (1.15) follows at once. □

An important application of maximal ϕ-cyclic code is to construct an error-correcting code, so that we may obtain a modified McEliece-Niederriter's cryptosystem. To do this, let $1\le m<\sqrt{n}$, and F_{q^m} be an extension field of F_q of degree m. Suppose $F_{q^m}=F_q(\theta)$, where θ is a primitive element of F_{q^m} and $F_q(\theta)$ is the simple extension containing F_q and θ. Let $g(x)\in F_q[x]$ be the minimum polynomial of θ, then $g(x)$ is an irreducible polynomial of degree m of $F_q[x]$. It is well-known that F_{q^m} is a Galois extension of F_q, so that all roots of $g(x)$ are in F_{q^m}. Let $\beta_1,\beta_2,\cdots,\beta_m$ be all roots of $g(x)$, the Vandermonde matrix $V(\beta_1,\beta_2,\cdots,\beta_m)$ defined by

$$H=V(\beta_1,\beta_2,\cdots,\beta_m)=\begin{pmatrix}1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1}\\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \beta_m & \beta_m^2 & \cdots & \beta_m^{n-1}\end{pmatrix}_{m\times n}, \tag{1.16}$$

where $\beta_1=\theta$ and each β_i is a vector of $(F_q)^m$. For arbitrary monic polynomial $h(x)\in F_q[x]$, $\deg h(x)=n-m$, let $\phi(x)=h(x)g(x)$ and C be a maximal ϕ-cyclic code generated by $g(x)$. It is easy to verify that

$$c\in C \Leftrightarrow cH'=0.$$

Therefore, H is a parity check matrix for C. If we choose the primitive element θ, so that any $d-1$ columns in H are linearly independent, then the minimum distance of C is greater than d, and C is a t-error-correcting code, where $t=\left[\frac{d}{2}\right]$.

The public key cryptosystems based on algebraic coding theory were created by R. J. McEliece [13] and H. Niederriter [14], a suitable t-error-correcting code plays a key role in their construction. The error-correcting code C should satisfy the following requirements:

1) C should have a relatively large error-correcting capability so that a reasonable number of message vectors can be used;

2) C should allow an efficient decoding algorithm so that the decryption can be carried out in a short time.

Our results supply a different way to choose an error-correcting code by selecting arbitrary irreducible polynomials $g(x)\in F_q[x]$ of degree m and roots of $g(x)$ rather than an irreducible factor of x^n-1 and the roots of unit such as ordinary BCH code and Gappa code.

In fact, for any positive integer m, there is at least an irreducible polynomial $g(x)\in F_q[x]$ with degree m. Let $N_q(m)$ be the number of irreducible polynomials of degree m in $F_q[x]$, then we have (see Theorem 3.25 of [15])

$$N_q(m)=\frac{1}{m}\sum_{d|m}u\left(\frac{m}{d}\right)q^d=\frac{1}{m}\sum_{d|m}u(d)q^{\frac{m}{d}},$$

where $u(d)$ is Mobius function.

Assuming one has selected two monic and irreducible polynomials $g(x)$ and $h(x)$ with $\deg g(x)=m$ and $\deg h(x)=n-m$, let $\phi(x)=g(x)h(x)$, then one may obtain ϕ-cyclic code C generated by $g(x)$ or $h(x)$, which is more convenient and more flexible than the ordinary methods.

Remark It's difficult to compare the error-correcting capability between ϕ-cyclic code with existing cyclic codes of the same length and dimension. However, we believe that the advantages of ϕ-cyclic code will become more clear when q increases. We will discuss this carefully in another paper later.

3. A Generalization of NTRUEncrypt

The public key cryptosystem NTRU proposed in 1996 by Hoffstein, Pipher and Silverman, is the fastest known lattice based encryption scheme, although its description relies on arithmetic over polynomial quotient ring $Z[x]/\langle x^n-1\rangle$, it was easily observed that it could be expressed as a lattice based cryptosystem (see [16]). For the background materials, we refer to [3] [6] [17] [18] [19] and [20]. Our strategy in this section is to replace $Z[x]/\langle x^n-1\rangle$ by more general polynomial ring $Z[x]/\langle\phi(x)\rangle$ and obtain a generalization of NTRUEncrypt, where $\phi(x)$ is a monic polynomial of degree n with integer coefficients.

In this section, we denote $\phi(x)$ and R by

$$\phi(x)=x^n-a_{n-1}x^{n-1}-\cdots-a_1x-a_0\in Z[x],\ R=Z[x]/\langle\phi(x)\rangle,\ a_0\neq 0. \quad (2.1)$$

Let $H_\phi\in Z^{n\times n}$ be a square matrix given by

$$H=H_\phi=\begin{pmatrix}0 & \cdots & 0 & a_0\\ & & & a_1\\ & I_{n-1} & & \vdots\\ & & & a_{n-1}\end{pmatrix}_{n\times n}, \quad (2.2)$$

where I_{n-1} is $(n-1)\times(n-1)$ unit matrix. Obviously, $\phi(x)$ is the characteristic polynomial of H, and H defines a linear transformation of $\mathbb{R}^n\to\mathbb{R}^n$ by $x\to Hx$, where $\mathbb{R}$ is real number field, x is a column vector of $\mathbb{R}^n$. We may extend this transformation to $\mathbb{R}^{2n}$ and denote σ by

$$\sigma\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}H\alpha\\ H\beta\end{pmatrix},\ \text{where}\ \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\in\mathbb{R}^{2n}. \quad (2.3)$$

Of course, σ is again a linear transformation of $\mathbb{R}^{2n}\to\mathbb{R}^{2n}$.

According to [20], a q-ary lattice is a lattice L such that $qZ^n\subset L\subset Z^n$, where q is a positive integer.

Definition 2.1. A q-ary lattice L is called convolutional modular lattice, if L is in even dimension $2n$ satisfying

$$\forall\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\in L\Rightarrow\sigma\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}H\alpha\\ H\beta\end{pmatrix}\in L. \quad (2.4)$$

In other words, a convolutional modular lattice is a q-ary lattice in even dimension and is closed under the linear transformation σ.

Recalling the secret key $\begin{pmatrix} f \\ g \end{pmatrix}$ of NTRU is a pair of polynomials of degree $n-1$, we may regard f and g as column vectors in Z^n. To obtain a convolutional modular lattice containing $\begin{pmatrix} f \\ g \end{pmatrix}$, we need some help of ideal matrices. An ideal matrix generated by a vector f is defined by

$$H^*(f) = H_\phi^*(f) = \left[f, Hf, H^2 f, \cdots, H^{n-1} f \right]_{n\times n}, \tag{2.5}$$

which is a block matrix in terms of each column $H^k f\ (0 \le k \le n-1)$. It is easily seen that $H^*(f)$ is a generalization of the classical circulant matrices (see [21]), in fact, let $\phi(x) = x^n - 1$, and $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in Z[x]$, the ideal matrix $H_\phi^*(f)$ generated by f is given by

$$H^*(f) = H_\phi^*(f) = \begin{pmatrix} f_0 & f_{n-1} & \cdots & f_1 \\ f_1 & f_0 & \cdots & f_2 \\ \vdots & \vdots & & \vdots \\ f_{n-1} & f_{n-2} & \cdots & f_0 \end{pmatrix},\ \phi(x) = x^n - 1,$$

which is known as a circulant matrix. On the other hand, ideal matrix and ideal lattice play an important role in Ajtai's construction of a collision resistant Hash function, the related materials we refer to [3] [22] [23] [24] [25] and [26].

First, we have to establish some basic properties for an ideal matrix $H^*(f)$, most of them are known when $H^*(f)$ is a circulant matrix.

Lemma 2.1. Suppose H and $H^*(f)$ are given by (2.2) and (2.5) respectively, then for any $f \in \mathbb{R}^n$ we have

$$H \cdot H^*(f) = H^*(f) \cdot H,\ \forall f \in \mathbb{R}^n.$$

Proof: Since $\phi(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$ is the characteristic polynomial of H, by Hamilton-Cayley theorem, we have

$$H^n = a_0 I_n + a_1 H + \cdots + a_{n-1} H^{n-1}. \tag{2.6}$$

Let

$$b = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix},\ \text{and } H = \begin{pmatrix} 0 & a_0 \\ I_{n-1} & b \end{pmatrix}.$$

By (2.5) we have

$$\begin{aligned} H^*(f)H &= \left[f, Hf, \cdots, H^{n-1} f \right] \begin{pmatrix} 0 & a_0 \\ I_{n-1} & b \end{pmatrix} \\ &= \left[Hf, H^2 f, \cdots, H^{n-1} f, a_0 f + a_1 Hf + \cdots + a_{n-1} H^{n-1} f \right] \\ &= \left[Hf, H^2 f, \cdots, H^{n-1} f, H^n f \right] \\ &= H\left[f, Hf, \cdots, H^{n-1} f \right] = H \cdot H^*(f). \end{aligned}$$

the lemma follows. □

Lemma 2.2. For any $f=\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n$ we have

$$H^*(f) = f_0 I_n + f_1 H + \cdots + f_{n-1} H^{n-1}. \tag{2.7}$$

Proof: We use induction on n to show this conclusion. If $n=1$, it is trivial. Suppose it is true for n, we consider the case of $n+1$. For this purpose, we write $H = H_n$, $e_1, e_2, \cdots, e_n$ the n column vectors of unit in $\mathbb{R}^n$, namely

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \cdots,\ e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

and

$$H_{n+1} = \begin{pmatrix} 0 & A_0 \\ e_1 & H_n \end{pmatrix},$$

where $A_0 = (0, 0, \cdots, a_0) \in \mathbb{R}^n$ is a row vector. For any k, $1 \le k \le n-1$, it is easy to check that

$$H_n e_k = e_{k+1},\ H_n^k e_1 = e_{k+1} \text{ and } H_{n+1}^k = \begin{pmatrix} 0 & A_0 H_n^{k-1} \\ e_k & H_n^k \end{pmatrix}.$$

Let $f=\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \\ f_n \end{pmatrix} \in \mathbb{R}^{n+1}$, we denote f' by

$$f' = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} \in \mathbb{R}^n, \text{ and } f = \begin{pmatrix} f_0 \\ f' \end{pmatrix}.$$

By the assumption of induction, we have

$$H_n^*(f') = \left[f', H_n f', \cdots, H_n^{n-1} f' \right] = f_1 I_n + f_2 H_n + \cdots + f_n H_n^{n-1}.$$

It follows that

$$\begin{aligned} H_{n+1}^*(f) &= \left[\begin{pmatrix} f_0 \\ f' \end{pmatrix}, H_{n+1} \begin{pmatrix} f_0 \\ f' \end{pmatrix}, \cdots, H_{n+1}^n \begin{pmatrix} f_0 \\ f' \end{pmatrix} \right] \\ &= f_0 I_n + f_1 H_{n+1} + \cdots + f_n H_{n+1}^n. \end{aligned}$$

We complete the proof of lemma 2.2. □

We always suppose that $\phi(x) \in Z[x]$ is a separable polynomial and $w_1, w_2, \cdots, w_n$ are complex number roots of $\phi(x)$, of which are different from each other. The Vandermonde matrix V_ϕ generated by $\{w_1, w_2, \cdots, w_n\}$ is

$$V_\phi = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ w_1 & w_2 & \cdots & w_n \\ \vdots & \vdots & & \vdots \\ w_1^{n-1} & w_2^{n-1} & \cdots & w_n^{n-1} \end{pmatrix}, \text{ and } \det\left(V_\phi\right) \neq 0.$$

Lemma 2.3. Let $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \mathbb{R}[x]$, then we have

$$H^*(f) = V_\phi^{-1} \operatorname{diag}\left\{f(w_1), f(w_2), \cdots, f(w_n)\right\} V_\phi, \tag{2.8}$$

where $\operatorname{diag}\left\{f(w_1), f(w_2), \cdots, f(w_n)\right\}$ is the diagonal matrix.

Proof: By Theorem 3.2.5 of [21], for H, we have

$$H = V_\phi^{-1} \operatorname{diag}\left\{w_1, w_2, \cdots, w_n\right\} V_\phi. \tag{2.9}$$

By lemma 2.2, it follows that

$$H^*(f) = V_\phi^{-1} \operatorname{diag}\left\{f(w_1), f(w_2), \cdots, f(w_n)\right\} V_\phi. \quad \square$$

Now, we summarize some basic properties for ideal matrix as follows.

Theorem 2. Let $f \in \mathbb{R}^n$, $g \in \mathbb{R}^n$ be two column vectors and $H^*(f)$ be the ideal matrix generated by f, then we have:

(i) $H^*(f)H^*(g) = H^*(g)H^*(f)$.

(ii) $H^*(f)H^*(g) = H^*\left(H^*(f)g\right)$.

(iii) $\det\left(H^*(f)\right) = \prod_{i=1}^{n} f(w_i)$.

(iv) $H^*(f)$ is an invertible matrix if and only if $\phi(x)$ and $f(x)$ are co-prime, *i.e.* $\gcd\left(\phi(x), f(x)\right) = 1$.

Proof: (i) and (ii) follow from lemma 2.2 immediately, (iii) and (iv) follow from lemma 2.3. Here we only give an equivalent form of (ii). Let

$$f * g = H^*(f)g. \tag{2.10}$$

then by (ii) we have

$$H^*(f * g) = H^*(f)H^*(g). \tag{2.11}$$

$\square$

To construct a convolutional modular lattice containing vector $\begin{pmatrix} f \\ g \end{pmatrix}$, let $\begin{pmatrix} f \\ g \end{pmatrix} \in Z^{2n}$, $\left(H^*(f)\right)'$ be the transpose of $H^*(f)$, and

$$A = \left[\left(H^*(f)\right)', \left(H^*(g)\right)'\right] = \begin{pmatrix} f' & g' \\ f'H' & g'H' \\ f'(H')^2 & g'(H')^2 \\ \vdots & \vdots \\ f'(H')^{n-1} & g'(H')^{n-1} \end{pmatrix}_{n\times 2n}, \tag{2.12}$$

$$A' = \begin{pmatrix} H^*(f) \\ H^*(g) \end{pmatrix} = \begin{pmatrix} f & Hf & \cdots & H^{n-1}f \\ g & Hg & \cdots & H^{n-1}g \end{pmatrix}_{2n\times n}. \tag{2.13}$$

We consider A and A' as matrices over Z_q, *i.e.* $A \in Z_q^{n\times 2n}$, $A' \in Z_q^{2n\times n}$, a

q-ary lattice $\Lambda_q(A)$ is defined by (see [20])

$$\Lambda_q(A)=\left\{y\in Z^{2n} \mid \text{there exists } x\in Z^n \Rightarrow y\equiv A'x(\bmod q)\right\}. \tag{2.14}$$

Under the above notations, we have

Theorem 3. For any column vectors $f\in Z^n$ and $g\in Z^n$, then $\Lambda_q(A)$ is a convolutional modular lattice, and $\begin{pmatrix} f \\ g \end{pmatrix}\in\Lambda_q(A)$.

Proof: It is known that $\Lambda_q(A)$ is a q-ary lattice, *i.e.*

$$qZ^{2n}\subset\Lambda_q(A)\subset Z^{2n}.$$

We only prove that $\Lambda_q(A)$ is fixed under the linear transformation σ given by (2.4). If $y\in\Lambda_q(A)$, then $y\equiv A'x(\bmod q)$ for some $x\in Z^n$, by lemma 2.1, we have

$$\sigma(y)\equiv\begin{pmatrix} HH^*(f)x \\ HH^*(g)x \end{pmatrix}=\begin{pmatrix} H^*(f)Hx \\ H^*(g)Hx \end{pmatrix}\equiv A'Hx(\bmod q).$$

It means that $\sigma(y)\in\Lambda_q(A)$ whenever $y\in\Lambda_q(A)$. Let

$$e=\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\in Z^n\Rightarrow H^*(f)e=f, \text{ and } H^*(g)e=g.$$

We have $\begin{pmatrix} f \\ q \end{pmatrix}\in\Lambda_q(A)$, and Theorem 3 follows. □

Since $\Lambda_q(A)\subset Z^{2n}$, then there is a unique Hermite Normal Form of basis N, which is an upper triangular matrix given by

$$N=\begin{pmatrix} I_n & H^*(h) \\ 0 & qI_n \end{pmatrix}, \text{ where } h\equiv\left(H^*(f)\right)^{-1}g(\bmod q). \tag{2.15}$$

Next, we consider parameters system of NTRU. To choose the parameters of NTRU, let d_f be a positive integer and $\{p,0,-p\}^n\subset Z^n$ be a subset of Z^n, of which has exactly d_f+1 positive entries and d_f negative ones, the remaining $n-2d_f-1$ entries will be zero. We take some assumption conditions for choice of parameters as follows:

(i) $\phi(x)=x^n-a_{n-1}x^{n-1}-\cdots-a_1x-a_0\in Z[x]$ with $a_0\neq 0$, and $\phi(x)$ is separable polynomial, n,p,q,d_f are positive integers with n prime, $1<p<q$ and $\gcd(p,q)=1$.

(ii) $f(x)$ and $g(x)$ are two polynomials in $Z[x]$ of degree $n-1$, the constant term of $f(x)$ is 1, and

$$f(x)-1\in\{p,0,-p\}^n,\ g\in\{p,0,-p\}^n.$$

(iii) $H^*(f)$ is invertible modulo q.

(iv) $d_f<\left(\frac{q}{2}-1\right)\Big/4p-\frac{1}{2}$.

Under the above conditions, by lemma 2.2 we have

$$H^*(f) \equiv I_n \pmod{p}, \text{ and } H^*(g) \equiv 0 \pmod{p}. \tag{2.16}$$

Now, we state a generalization of NTRU as follows.

- Private key. The private key in generalized NTRU is a short vector $\begin{pmatrix} f \\ q \end{pmatrix} \in Z^{2n}$. The lattice associated with a private key is $\Lambda_q(A)$, which is a convolutional modular lattice containing private key.
- Public key. The public key of the generalized NTRU is the HNF basis N of $\Lambda_q(A)$, which is given by (2.15).
- Encryption. An input message is encoded as a vector $m \in \{1, 0, -1\}^n$ with exactly $d_f + 1$ positive entries and d_f negative ones. Here the reason for restricting $d_f + 1$ positive and d_f negative entries of vector m is to improve the efficiency of encryption and decryption and it's not necessary. The vector m is concatenated with a randomly chosen vector $r \in \{1, 0, -1\}^n$ also with exactly $d_f + 1$ positive entries and d_f negative ones, to obtain a short error vector $\begin{pmatrix} m \\ r \end{pmatrix} \in \{1, 0, -1\}^{2n}$. Let

$$\begin{pmatrix} c \\ 0 \end{pmatrix} = N \begin{pmatrix} m \\ r \end{pmatrix} \equiv \begin{pmatrix} m + H^*(h) r \\ 0 \end{pmatrix} \pmod{q}, \tag{2.17}$$

where h is given by (2.15). Then, the n-dimensional vector c

$$c \equiv m + H^*(h) r \pmod{q},$$

is the ciphertext.

- Decryption. Suppose the entries of n-dimensional vector c are belong to interval $\left[-\frac{q}{2}, \frac{q}{2}\right]$, then ciphertext c is decrypted by multiplying it by the secret matrix $H^*(f) \mod q$, it follows that

$$H^*(f) c \equiv H^*(f) m + H^*(f) H^*(h) r \equiv H^*(f) m + H^*(g) r \pmod{q}. \tag{2.18}$$

Here, we use the identity (ii) of Theorem 2, namely,

$$H^*(f) H^*(g) = H^*\left(H^*(f) g\right).$$

If the above conditions (iv) is satisfied, it is easily seen that the coordinates of vector $H^*(f) m + H^*(g) r$ are all bounded by $\frac{q}{2}$ in absolute value, or, with high probability, even for larger value of d_f. The decryption process is completed by reducing (2.18) modulo p, to obtain

$$H^*(f) m + H^*(g) r \equiv m I_n \pmod{p}.$$

Thus one gets plaintext m from ciphertext c.

Example 2. Let $n = 3$, $p = 3$, $q = 7$, $\phi(x) = x^3 + x^2 + x + 1$, $f(x) = 3x^2 + 1$, $g(x) = 3x^2$, *i.e.* the private key is $\begin{pmatrix} f \\ g \end{pmatrix}$ with $f = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}$, $g = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}$. It is easy to get

$$H^*(f)=\begin{pmatrix}1 & -3 & 3\\ 0 & -2 & 0\\ 3 & -3 & 1\end{pmatrix},\ \text{and}\ H^*(g)=\begin{pmatrix}0 & -3 & 3\\ 0 & -3 & 0\\ 3 & -3 & 0\end{pmatrix}.$$

By (2.15), we compute the public key N as follows

$$h=\begin{pmatrix}2\\ 0\\ -3\end{pmatrix},\ H^*(h)=\begin{pmatrix}2 & 3 & -3\\ 0 & 5 & 0\\ -3 & 3 & 2\end{pmatrix},\ \text{and}\ N=\begin{pmatrix}I_3 & H^*(h)\\ 0 & 7I_3\end{pmatrix}.$$

Assume the input message $m=\begin{pmatrix}1\\ 0\\ 0\end{pmatrix}$, random vector $r=\begin{pmatrix}0\\ 1\\ 0\end{pmatrix}$, by (2.17) we get the ciphertext

$$c\equiv m+H^*(h)r\equiv\begin{pmatrix}-3\\ -2\\ 3\end{pmatrix}(\mathrm{mod}\,7).$$

By (2.18), we have

$$H^*(f)c\equiv\begin{pmatrix}-2\\ -3\\ 0\end{pmatrix}(\mathrm{mod}\,7).$$

Since

$$\begin{pmatrix}-2\\ -3\\ 0\end{pmatrix}\equiv\begin{pmatrix}1\\ 0\\ 0\end{pmatrix}(\mathrm{mod}\,3),$$

one can get the plaintext $m=\begin{pmatrix}1\\ 0\\ 0\end{pmatrix}$ from ciphertext c.

4. Conclusion

In this study, we first discuss a more general form of the ordinary cyclic code, namely ϕ-cyclic code. Then we give a generalized construction of NTRU based on ideal matrix and q-ary lattice theory. Compared with other variations of NTRU, such as CTRU, GNTRU, QTRU and BITRU, our extended NTRU cryptosystem is constructed with general ideal matrix rather than some special algebraic structures. Our purpose is to apply post quantum cryptography in distributed scenarios of blockchain future.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Lopez-Permouth, S.R., Parra-Avila, B.R. and Szabo, S. (2009) Dual Generalizations of the Concept of Cyclicity of Codes. *Advances in Mathematics of Communica-*

tions, **3**, 227-234. https://doi.org/10.3934/amc.2009.3.227

[2] Shi, M., Li, X., Sepasdar, Z. and Solé, P. (2020) Polycyclic Codes as Invariant Subspaces. *Finite Fields and Their Applications*, **68**, Article ID: 101760. https://doi.org/10.1016/j.ffa.2020.101760

[3] Lint, J.H.V. (1999) Introduction to Coding Theory. Volume 86 of GTM. Springer-Verlag, Berlin.

[4] Bose, R.C. and Ray-Chaudhuri, D.K. (1960) On a Class of Error Correcting Binary Group Codes. *Information and Control*, **3**, 68-79. https://doi.org/10.1016/S0019-9958(60)90287-4

[5] Goppa, V.D. (1970) A New Class of Linear Error-Correcting Codes. *Problemy Peredachi Informatsii*, **6**, 24-30.

[6] Hoffstein, J., Pipher, J. and Silverman, J.H. (1998) NTRU: A Ring Based Public Key Cryptosystem. In: Buhler, J.P., Ed., *Algorithmic Number Theory*, Lecture Notes in Computer Science, Vol. 1423, Springer, Berlin, 267-288. https://doi.org/10.1007/BFb0054868

[7] Gaborit, P., Ohler, J. and Soli, P. (2002) CTRU, a Polynomial Analogue of NTRU. Hal Inria, RR 4621.

[8] Kouzmenko, R. (2006) Generalizations of the NTRU Cryptosystem. Diploma Project, Ecole Polytechnique Federale de Lausanne.

[9] Coglianese, M. and Goi, B. (2005) MaTRU: A New NTRU Based Cryptosystem. Springer Verlag, Berlin, 232-243. https://doi.org/10.1007/11596219_19

[10] Malecian, E., Zakerolhsooeini, A. and Mashatan, A. (2011) QTRU: A Lattice Attack Resistant Version of NTRU PCKS Based on Quaternion Algebra. *The ISC Intrtnational Journal of Information Security*, **3**, 29-42.

[11] Malecian, E. and Zakerolhsooeini, A. (2010) OTRU: A Non-Associative and High Speed Public Key Cryptosystem. *IEEE* 15*th CSI International Symposium on Computer Architecture and Digital Systems* (*CADS*), Tehran, 23-24 September 2010, 83-90. https://doi.org/10.1109/CADS.2010.5623536

[12] Alsaidi, M.G. and Yassein R. (2016) BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra. *International Journal of Advanced Computer Science & Applications*, **7**, 1-6. https://doi.org/10.14569/IJACSA.2016.071101

[13] Lyubashevsky, V. and Micciancio, D. (2006) Generalized Compact Knapsacks Are Collision Resistant. In: Bugliesi, M., Preneel, B., Sassone, V. and Wegener, I., Eds., *Automata, Languages and Programming*, Lecture Notes in Computer Science, Vol. 4052, Springer, Berlin, 144-155. https://doi.org/10.1007/11787006_13

[14] Micciancio, D. and Regev, O. (2009) Lattice-Based Cryptography. In: Bernstein, D.J., Buchmann, J. and Dahmen, E., Eds., *Post-Quantum Cryptography*, Springer Berlin, 147-191. https://doi.org/10.1007/978-3-540-88702-7_5

[15] Lidl, R. and Niederreiter, H. (1983) Finite Fields. In: Doran, R., Ismail, M., Lam, T.-Y. and Lutwak, E., Eds., *Encyclopedia of Mathematics and Its Applications*, Vol. 20, Cambridge University Press, Cambridge.

[16] IEEE Computer Society. (2000) IEEE Standard Specifications for Public-Key Cryptography. IEEE Std 1363-2000, 1-228.

[17] Coppersmith, D. and Shamir A. (1997) Lattice Attacks on NTRU. In: Fumy, W., Ed., *Advances in Cryptology*, Lecture Notes in Computer Science, Vol. 1233, Springer, Berlin, 52-61. https://doi.org/10.1007/3-540-69053-0_5

[18] Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W. and Zhang, Z. (2017) Choosing Parameters for NTRUEncrypt. In: Handschuh, H., Ed., *Topics in*

Cryptology, Lecture Notes in Computer Science, Vol. 10159, Springer, Berlin, 3-18. https://doi.org/10.1007/978-3-319-52153-4_1

[19] McEliece, R.J. (1978) A Public-Key Cryptosystem Based on Algebraic Coding Theory. DSN Progress Report, Jet Propulsion Laboratory, Pasadena, 42-44.

[20] Micciancio, D. (2001) Improving Lattice Based Cryptosystems Using the Hermite Normal Form. In: Silverman, J.H., Ed., *Cryptography and Lattices*, Lecture Notes in Computer Science, Vol. 2146, Springer, Berlin, 126-145. https://doi.org/10.1007/3-540-44670-2_11

[21] Davis, P.J. (1994) Circulant Matrices. 2nd Edition, Chelsea Publishing, New York.

[22] Ajtai, M. (1996) Generating Hard Instances of Lattice Problems. *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, Philadelphia, 22-24 May 1996, 99-108. https://doi.org/10.1145/237814.237838

[23] Ajtai, M. and Dwork, C. (1997) A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence. *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing*, El Paso, 4-6 May 1997, 284-293. https://doi.org/10.1145/258533.258604

[24] Niederreiter, H. (1986) Knapsack-Type Cryptosystems and Algebraic Coding Theory. *Problems of Control and Information Theory*, **15**, 159-166.

[25] Plantard T. and Schneider, M. (2013) Creating a Challenge for Ideal Lattices. *IACR Cryptology ePrint Archive*, **39**, 1-17.

[26] Pradhan, P.K., Rakshit, S. and Datta, S. (2019) Lattice Based Cryptography: Its Applications, Areas of Interest and Future Scope. *Proceedings of the Third International Conference on Computing Methodologies and Communication*, Erode, 27-29 March 2019, 988-993. https://doi.org/10.1109/ICCMC.2019.8819706