International Journal of Cryptology Research 10(1): 1 - 21 (2020)

NTRU Public-Key Cryptosystem and Its Variants: An Overview

Nurshamimi Salleh*[1] and **Hailiza Kamarulhaili**[1]

[1]*School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia*

E-mail: mymy_nsbs@yahoo.mail.com.my, hailiza@usm.my
**Corresponding author*

ABSTRACT

NTRU is a lattice-based public-key cryptosystem which operates in a polynomial ring with integer coefficients. The encryption algorithm, namely NTRUEncrypt has been widely studied due to its resistance to quantum computer-based attacks. There are various NTRUEncrypt variants proposed since NTRU was introduced in 1996. This paper gives an overview and the compilation of several developments of NTRUEncrypt and its variants.

Keywords: NTRUEncrypt, polynomial ring, encryption, decryption.

1 INTRODUCTION

In the modern world today, the development of communication networks happen so rapidly and this is a result of the ever-expanding internet network usage. Consequently, security becomes essential to keep communication data safe and secure from any internet threats. The security lacking leave the system vulnerable to attacks and miss use of important data by an adversary. This can be overcome by exploiting public-key cryptography (PKC) which has features such as confidentiality, data integrity, authentication, and non-repudiation. With these features, PKC can provide security for communication networks, especially for ensuring the privacy and confidentiality of important information.

Public-key cryptosystems are designed based on hard computational problems. Public-key cryptosystems, such as Diffie Hellman key exchange protocol (Diffie and Hellman, 1976) is based on discrete logarithm problem, RSA cryptosystem (Rivest et al., 1978) is based on factorization problem, McEliece cryptosystem (McEliece, 1978) is based on a coding problem, ElGamal cryptosystem (ElGamal, 1985) is based on discrete logarithm problem, Elliptic Curves Cryptosystem (ECC) (Koblitz, 1987, Miller, 1985) is based on elliptic curves discrete logarithm problems and NTRU cryptosystem (Hoffstein, 1996) is based on lattice problems. These are several examples of well-known public-key cryptosystems. Remarkably, a public-key cryptosystem that is designed based on the hard computational problem is intractable in practice. And yet, all those public-key cryptosystems are vulnerable to the quantum computer except for the NTRU cryptosystem. For this reason, the NTRU cryptosystem is more preferred compared to others mentioned above.

This paper begins with a description of NTRU including its mathematical aspect, construction, and comparisons with RSA (and ECC) in Section 2. Followed by a brief overview of NTRUEncrypt variants in Section 3. Finally, Section 4 concludes.

2 THE NTRU CRYPTOSYSTEM

NTRU that stands for Nth-Degree Truncated Polynomial Ring was invented by three mathematicians from the Department of Mathematics, Brown University, that are Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman. They presented NTRU at rump session Crypto96 but the preprint (Hoffstein, 1996) was rejected by the organizing committee of Crypto97. In 1998, they successfully published NTRU (Hoffstein et al., 1998), which is the NTRU-1996 with some added information based on comments from several mathematicians as well as from the article by Coppersmith and Shamir (1997). NTRU-1998 is also known as NTRUEncrypt. Indeed, NTRUEncrypt refers to the encryption algorithm of NTRU. Note that NTRU also consists of the digital signature algorithm, namely NTRUSign but will not be discussed in this paper.

In 2009, NTRUEncrypt was officially being standardized for the IEEE Std 1363.1 where IEEE 1363.1 is the lattice-based code for public-key cryptography in the Institute of Electrical and Electronics Engineers (IEEE) standardization project. A year later, NTRUEncrypt received another encryption standard, namely the X9.98 standard from the Accredited Standards Committee X9 in the financial services industry. NTRUEncrypt also has been issued for the National Institute of Standards Technology (NIST) post-quantum cryptography standardization in 2017.

2.1 Mathematical Aspect of NTRUEncrypt

NTRUEncrypt exploits the algebraic structure of the polynomial ring, $R = \mathbb{Z}[X]/(X^N - 1)$. To be more specific, the ring R, is the ring of truncated (or convolution) polynomials of degree $N-1$ with integer coefficients in the form of $a_0 + a_1X + a_2X^2 + \cdots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$. In modulo p and q, the ring R can be respectively defined by

$$R_p = \frac{(\mathbb{Z}/p\mathbb{Z})[X]}{X^N - 1}, \qquad \text{and} \qquad R_q = \frac{(\mathbb{Z}/q\mathbb{Z})[X]}{X^N - 1}.$$

Let an element $F \in R$ be a polynomial with the vector of its coefficients as $F = \sum_{i=0}^{N-1} F_iX^i \equiv [F_0, F_1, \ldots, F_{N-1}]$. Then the addition and multiplication of two elements in R are given by

$$F + G = \sum_{i=0}^{N-1} F_iX^i + \sum_{j=0}^{N-1} G_jX^j,$$

and

$$F * G = \left(\sum_{i=0}^{N-1} F_iX^i\right) * \left(\sum_{j=0}^{N-1} G_jX^j\right) = \sum_{k=0}^{N-1} \left(\sum_{i+j\equiv k \ (mod\ N)} F_iG_j\right)X^k,$$

respectively. Next, the width (or size) of F is defined by

$$\|F\| = \sqrt{\sum_{i=0}^{N-1} \left(F_i - \bar{F}\right)^2} = \sqrt{\sum_{i=0}^{N-1} F_i^2 - \frac{1}{N}\left(\sum_{i=0}^{N-1} F_i\right)^2},$$

where $\bar{F} = (\sum_{i=0}^{N-1} F_i)/N$ is the coefficients average of F. Then the width of two elements in R is given by the quasi-multiplicative norm, $\|F * G\| \approx \|F\| \cdot \|G\|$.

As for security, the underlying hard problem for NTRUEncrypt is based on the Shortest Vector Problem (SVP) in a special class of lattices, namely NTRU convolutional modular lattices, $\mathcal{L}_h^{NTRU}$. SVP is one of the well-known computational lattice problems.

Definition 2.1. *(SVP (Galbraith, 2012)) Given a basis matrix B for lattice $\mathcal{L}$, compute a shortest non-zero vector $u \in \mathcal{L}(B)$ such that $\|u\|$ is minimal.*

Specifically, the security of NTRUEncrypt is based on the difficulty of finding reasonably shortest vectors $[f, g] = [f_0, f_1, \ldots, f_{N-1}, g_0, g_1, \ldots, g_{N-1}]$ in $\mathcal{L}_h^{NTRU}$ that is defined by

$$\mathcal{L}_h^{NTRU} = \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right) \subset \mathbb{Z}^{2N},$$

where $h(X) \equiv g(X)/f(X)\ (mod\ q)$.

2.2 Construction of NTRUEncrypt

The construction of NTRUEncrypt can be described by the following phases.

I. Parameter Creation

The creation of parameter divides into two parts which are the creation of parameter (N, p, q) and the creation of spaces L_f, L_g, L_φ and L_m. Parameter (N, p, q) consists of the parameter N that represents the degree of R and the parameters p and q that uses the reduction of coefficients of R. Next, space $L_f = L(d_f, d_f - 1), L_g = L(d_g, d_g)$ and $L_\varphi = L(d, d)$ are obtained from the set of ternary polynomial

$$L(d_1, d_2) = \left\{ A \in R \textit{ has } \begin{array}{l} d_1 \textit{ coefficients equal to } 1, \\ d_2 \textit{ coefficients equal to } -1, \\ \textit{all other coefficients equal to } 0 \end{array} \right\}.$$

Whereas space L_m is obtained from the space

$$L_m = \left\{ m \in R \textit{ has coefficients lying between } -\frac{p-1}{2} \quad \textit{and} \quad \frac{p-1}{2} \right\}.$$

II. Key Generation

The generation of keys includes the generation of private keys and a public key. To be more specific, the private keys are generated by polynomial $g(X) \in L_g$ and polynomial $f(X) \in L_f$ where f must be invertible in modulo p and q, and its inverses, that is, F_p and F_q satisfying the following:

$$F_p(X) * f(X) = f_p^{-1}(X) * f(X) \equiv 1 \ (mod\, p),$$

and

$$F_q(X) * f(X) = f_q^{-1}(X) * f(X) \equiv 1 \ (mod\, q),$$

respectively. While, the public key is generated by polynomial $h(X) = F_q(X) * g(X) = f_q^{-1}(X) * g(X) \ (mod\, q)$.

III. Encryption

The encryption phase involves the use of public key h in the calculation of encrypted message $e(X) = p\varphi(X) * h(X) + m(X) \ (mod\, q)$ where polynomial φ is a random polynomial in L_φ and polynomial m is a message in L_m. The mod q here means the coefficients are reducing into the interval $[-q/2, q/2]$.

IV. Decryption

The decryption phase involves the aid of temporary polynomial a in the recovery of the message m from the encrypted message e by using the private key

f. Firstly, calculate a temporary polynomial $a(X) = f(X) * e(X)\ (mod\ q)$. Next, compute $F_p(X) * a(X) = f_p^{-1}(X) * a(X) = m(X)\ (mod\, p)$ to recover the message m with the mod p here means the coefficients are reducing into the interval $[-p/2, p/2]$.

In the decryption process, the calculation of temporary polynomial a yields the inequality $p\varphi(X) * g(X) + f(X) * m(X)$ which lies in the interval of $[-q/2, q/2]$. Indeed, $\|p\varphi(X) * g(X) + f(X) * m(X)\|_\infty = \max_{1 \le i \le N}\{p\varphi_i(X) * g_i(X) + f_i(X) * m_i(X)\} - \min_{1 \le i \le N}\{p\varphi_i(X) * g_i(X) + f_i(X) * m_i(X)\}$. Therefore, when given by

$$\|p\varphi(X) * g(X) + f(X) * m(X)\|_\infty \le q, \quad \text{(the wrap failure)}$$

or

$$\|p\varphi(X) * g(X) + f(X) * m(X)\|_\infty > q, \quad \text{(the gap failure)}$$

occurs, the decryption process is failing to work. But the decryption process is working properly when $\|p\varphi(X) * g(X) + f(X) * m(X)\|_\infty < q$.

The construction of NTRUEncrypt can be simply illustrated by the following example. Consider the parameter $(N, p, q) = (7, 3, 43)$ and the following polynomials:

$$\begin{aligned} f(X) &= X^6 - X^4 + X^2 - X + 1 \in L(3, 2), \\ g(X) &= X^6 - X^4 - X^2 + X \in L(2, 2), \\ \varphi(X) &= X^6 + X^5 - X^3 - 1 \in L(2, 2), \\ m(X) &= X^5 + X^4 - X^3 - X + 1. \end{aligned}$$

Then the inverses of f and the public key h are given by

$$\begin{aligned} F_q(X) &= 8X^6 + 25X^5 + 11X^4 + 30X^3 + 42X^2 + 9X + 5 \in R_{43}, \\ F_p(X) &= 2X^6 + X^4 + X^3 + 2X^2 + 2X + 2 \in R_3, \\ h(X) &= 20X^6 + 23X^5 + 8X^4 + 36X^3 + 9X^2 + 28X + 5 \quad (mod\, 43). \end{aligned}$$

For the encryption, the calculation of encrypted message e yield

$$e(X) = 17X^6 + 23X^5 + 22X^4 + 12X^3 + 2X^2 + 24X + 30 \quad (mod\, 43).$$

For the decryption, firstly calculate a temporary polynomial a as

$$a(X) = X^6 + 6X^5 + 5X^4 + 39X^3 + 40X^2 + 34X + 5 \quad (mod\, 43),$$

and center-lifting it modulo 43 obtain

$$\text{center} - \text{lift of } a(X) = X^6 + 6X^5 + 5X^4 - 4X^3 - 3X^2 - 9X + 5 \quad (mod\, 43).$$

where its coefficients are chosen from $\{-21, -20, \ldots, 20, 21\}$. Next, compute

$$F_p(X) * a(X) = X^5 + X^4 + 2X^3 + 2X + 1 \quad (mod\, 3),$$

and center-lifting it modulo 3 with its coefficients are chosen from $\{-1, 0, 1\}$ to recover the message, $m(X) = X^5 + X^4 - X^3 - X + 1 \quad (mod\, 3)$.

2.3 Comparison with Other Public-Key Cryptosystems

NTRU is the fastest public-key cryptosystem among that of other cryptosystems. To verify this fact, a comparison are made between NTRU and RSA in terms of encryption and decryption execution timings for different text sizes.

Text sizes	NTRU		RSA	
(bits)	Encryption	Decryption	Encryption	Decryption
128	0.0000001	0.0000001	0.0549	0.0549
265	0.0000001	0.05490	0.1098	0.1098
512	0.05490	0.05490	0.2197	0.1648
1024	0.10989	0.05490	0.3846	0.3296
2048	0.27472	0.05490	0.7142	0.6593
5120	0.65934	0.16484	1.7032	1.7032
10240	1.31868	0.36100	3.4020	3.4020

Table 1: NTRU and RSA encryption and decryption execution timings (Challa and Pradhan, 2007).

Table 1 above indicates that the execution timings of NTRU are much shorter than the execution timings of RSA for both encryption and decryption which means that NTRU is more speedy than RSA. Therefore, NTRU is proven to be faster than RSA and this also implies that NTRU (possible) to be the fastest cryptosystem among that of other cryptosystems.

Furthermore, another comparison will be made between NTRU and RSA together with ECC in terms of public key sizes. This comparison is made from some lowest security level to some higher security level, which is at 80, 122, 128, 160, 192 and 256 bits security level (Howgrave-Graham et al., 2005). In general, the minimum for the lowest security level is recommended at 112 bits instead of at 80 bits because 112 bits security level offers stronger security than 80 bits security level.

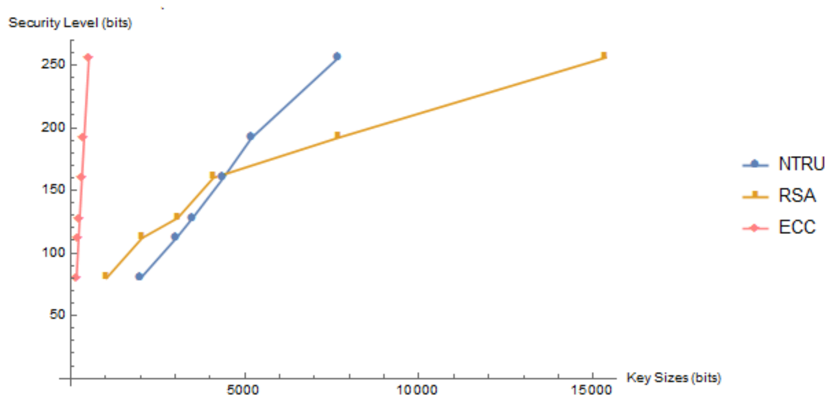

Figure 1: Graph security level versus public key sizes for NTRU, RSA, and ECC.

Figure 1 above shows that among these cryptosystems, ECC is having the best performance and NTRU is having the worst performance. Despite it, the performance of NTRU become better when the security level is getting higher.

Other than that, NTRU can be a lattice-based alternative to RSA and ECC because the lattices can become the best replacement for factorization and elliptic curves in the structure of the public-key cryptosystem for security purposes. Furthermore, the advantage of NTRU being a lattice-based cryptosystem is its resistance to quantum computer-based attacks compared to RSA and ECC which are likely to fail when implemented on quantum computers.

3 NTRUENCRYPT VARIANTS

Recall that NTRU-1998 is the improved version of NTRU-1996 due to a lack of information on the security proof and is also known as NTRUEncrypt. NTRU-Encrypt (or NTRU-1998) has been considered as the main reference for those who intend to study NTRU. In the interest of this fact, the investigations were been carried out on NTRUEncypt to improve its security as well as its performances. There are various NTRUEncrypt variants proposed over the past 20 years. The following table summarizes those NTRUEncrypt variants.

Year	Name of variants	Ring-based structure	Description
2002	NTRU with non-invertible polynomials	$\frac{\mathbb{Z}[X]}{X^N-1}$	NTRU with non-invertible polynomials (Banks and Shparlinski, 2002) extends NTRUEncrypt to non-invertible polynomial as a way to overcome the problem of finding an invertible polynomial in NTRUEncrypt.
2002	CTRU	$\frac{\mathbb{F}_2[T][X]}{X^N-1}$	CTRU (Gaborit et al., 2002) designs NTRUEncrypt over binary finite field $\mathbb{F}_2$ which is secure against Popov normal form attack but it was completely insecure against linear algebra-based attacks. Therefore, CTRU has a non-commutative and secure variant, namely NETRU (Atani et al., 2018).

Table 2. (Continued)

2005	MaTRU	$\frac{M_k(\mathbb{Z})[X]}{X^n - I_{k\times k}}$	MaTRU (Coglianese and Goi, 2005) operates in the ring of k by k matrices of a polynomial in R with the linear transformation of two-sided matrix multiplication. For $nk^2 = N$, MaTRU is having the same number of bits per message as NTRUEncrypt.
2006	GNTRU	$\frac{\mathbb{Z}[i][X]}{X^N - 1}$	GNTRU (Kouzmenko, 2006) proposes NTRUEncrypt over the ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}, i^2 = -1\}$. GNTRU is slightly more secure to lattice attack than NTRUEncrypt but it still not as efficient as NTRUEncrypt.
2008	Matrix NTRU	$\frac{M(\mathbb{Z})[X]}{X^n - I}$	Matrix NTRU (Nayak et al., 2008) represents NTRUEncrypt in the matrix formulation form. This is because the matrix formulation form is proven more secure when the matrix is invertible or its determinant exists. Also, it can ensure that the encryption and decryption working properly without having to fix the choice of the parameters p and q.
2008	GB-NTRU	$\frac{\mathbb{Z}[X,Y]}{(X^N - 1, Y^N - 1)}$	GB-NTRU (Caboara et al., 2008) generalizes NTRUEncrypt to multivariate polynomial, that is, a bivariate polynomial in its system.

Table 2. (Continued)

2009	NNRU	$\frac{M_k(\mathbb{Z})[X]}{X^n - I_{k\times k}}$	NNRU (Vats, 2009) operates in the ring of k by k matrices of a polynomial in R. NNRU is said to be secure to lattice-based attack compared to NTRUEncrypt. By setting $N = n(k^2)$, NTRUEncrypt and NNRU are having the same size of plaintext blocks.
2010	GTRU	$\frac{\mathcal{D}[X]}{X^N - 1}$	GTRU (Malekian and Zakerolhosseini, 2010a) generalizes NTRUEncrypt over some broader algebra than Dedekind domain, $\mathcal{D}$. The underlying algebra of GTRU can be non-commutative (quaternion algebra or algebra of dimension four) or even non-associative (octonion algebra or algebra of dimension eight).
2010	OTRU	$\frac{\mathbb{Z}[X]}{X^N - 1}$	OTRU (Malekian and Zakerolhosseini, 2010b) proposes the octonion version of NTRUEncrypt. The operation of OTRU involve a non-associative octonion algebra, $\mathbb{A} := \left\{a_0(x) + \sum_{i=1}^{7} a_i(x) \cdot e_i \| a_0(x), \cdots, a_7(x) \in R\right\}$ where $R = \mathbb{Z}[X]/(X^N - 1)$. OTRU is faster than NTRUEncrypt.
2011	QTRU	$\frac{(-1,-1)}{\mathbb{Z}[X]/(X^N - 1)}$	QTRU (Malekian et al., 2011) presents the quaternion version of NTRUEncrypt. The operation of QTRU involve a non-commutative quaternion algebra, $\mathbb{H} = \{a + ib + jc + kd \| a, b, c, d \in \mathbb{Z}, i^2 = j^2 = k^2 = ijk = -1\}$. QTRU is more efficient and secure than NTRUEncrypt.

Table 2. (Continued)

2015	DBTRU	$\frac{GF(2)[x]}{x^N-1}\Big\vert N$	DBTRU (Thang and Binh, 2015) designs NTRUEncrypt over the ring of dual special kinds of binary truncated polynomial with positive integer coefficients, $R_N[x] = GF(2)[x]/(x^N-1)\vert N \in Z^+$. DBTRU is having better theoretical performances and security than NTRUEncrypt.
2015	ETRU	$\frac{\mathbb{Z}[\omega][X]}{X^N-1}$	ETRU (Jarvis and Nevins, 2015) presents NTRUEncrypt over the ring of Eisenstein integers, $\mathbb{Z}[\omega] = \left\{a+\omega b \vert a,b \in \mathbb{Z}, i^2 = -1, \omega = e^{2i\frac{\pi}{3}}\right\}$. ETRU is having smaller key sizes than NTRUEncrypt and it also faster than NTRUEncrypt. In additions, the properties of ETRU have been used by the ILTRU (Karbasi and Atani, 2015) in its security proof that based on ideal lattices under an assumption of a worst-case hardness of standard R-SIS (*Ring Small Integer Solution*) and R-LWE (*Ring Learning with Errors*) problem.
2015	GR-NTRU	$\frac{\mathbb{Z}[G][X]}{X^N-1}$	GR-NTRU (Yasuda et al., 2015) derives NTRUEncrypt over group ring, $\mathbb{Z}[G] = \left\{\sum_{g\in G} a_g[g] \vert a_g \in \mathbb{Z}(\forall g \in G)\right\}$. The security comparison shows that GR-NTRU is less secure than NTRUEncrypt.

Table 2. (Continued)

2016	BITRU	$\frac{\mathbb{Z}[X]}{X^N-1}$	BITRU (Alsaidi and Yassein, 2016) proposes NTRUEncrypt over binary algebra, $BN_R = \{a + bj \mid j^2 = 1, a, b \in \mathbb{R}\}$. BITRU is a multidimensional cryptosystem with two public keys h and k where it can encrypt two independent messages from two different origins. BITRU is having better security than NTRUEncrypt.
2016	CQTRU	$\frac{A[X]}{X^N-1}$	CQTRU (Alsaidi et al., 2016) presents NTRUEncrypt over commutative quaternion ring, $A = \{a + bi + cj + dk \mid a, b, c, d \in K, i^2 = a, j^2 = b, ij = k\}$. CQTRU can encrypt and decrypt four messages at the same time and resistant to the alternate key attack, brute force attack and lattice attack. CQTRU is more secure than NTRUEncrypt.
2016	HXDTRU	$\frac{\mathbb{Z}[X]}{X^N-1}$	HXDTRU (Yassein and Alsaidi, 2016) derives NTRUEncrypt over hexadecnion algebra, $\Psi = \{r_0 + \sum_{i=1}^{15} r_i x_i \mid r_0, r_1, \ldots, r_{15} \in K\}$ where $K = \mathbb{Z}[X]/(X^N - 1)$. HXDTRU with N dimension is sixteen times faster than NTRUEncrypt with $16N$ dimension.
2016	BTRU	$\frac{B[x]}{x^N-1}$	BTRU (Thakur and Tripathi, 2016) extends NTRUEncrypt over a rational field in variable α or $Q[\alpha] = B$. BTRU is faster and secure than NTRUEncrypt.

Table 2. (Continued)

2016	KTRU	$\frac{\mathbb{Z}[\tau][X]}{X^N-1}$	KTRU (Thakur et al., 2016) designs NTRUEncrypt over the ring of Kleinian integers, $\mathbb{Z}[\tau]=\{q=m+n\tau : \lvert q^2\rvert = m^2+2n^2+mn, \tau=\left(1+i\sqrt{7}\right)/2, m,n \in Q\}$. The ring $\mathbb{Z}[\tau]$ is said to have a higher significance than the ring of integers, $\mathbb{Z}$.
2016	mini-NTRU	$\frac{\mathbb{Z}[X]}{X^N-1}$	mini-NTRU (Gaithuru et al., 2016) provides a mini version of NTRUEncrypt that uses smaller parameter sets based on the binary representation. However, those parameter sets are insecure for practical application.
2017	ITRU	$\frac{(\mathbb{Z}/n\mathbb{Z})[X]}{X^N-1}$	ITRU (Gaithuru and Salleh, 2017) presents NTRUEncrypt over the ring of integers modulo n that denoted by $\mathbb{Z}/n\mathbb{Z}$. As the comparison in terms of key generation, ITRU is only required $O(N^2)$ whereas NTRUEncrypt is required $O\left(N^2(log^2p+log^2q)\right)$.
2017	SQTRU	$\frac{(-1,-1)}{\mathbb{Z}[x]/(x^N-1)}$	SQTRU (Thakur and Tripathi, 2017) proposes NTRUEncrypt over coquaternions (also known as spit quaternion algebra), $\hat{H}=\{q=q_0+q_1i+q_2j+q_3k; q_0,q_1,q_2,q_3 \in R\}$ where $R=\mathbb{Z}[x]/(x^N-1)$. SQTRU can reduce the decryption failure through its non-commutative nature and due to its multidimensional nature, SQTRU is more secure to lattice-based attack than NTRUEncrypt.

Table 2. (Continued)

2018	PairTRU	$\frac{M(k,\mathbb{Z}\times\mathbb{Z})[x]}{(I_{k\times k},I_{k\times k})x^N-(I_{k\times k},I_{k\times k})}$	PairTRU (Karbasi et al., 2018) establishes NTRUEncrypt over the non-commutative matrix ring of $k \times k$ matrices of polynomials for $\mathbb{Z} \times \mathbb{Z}$. PairTRU is more secure to linear algebra-based attack and lattice-based attack than NTRUEncrypt.
2018	D-NTRU	$\frac{\mathbb{Z}[X]}{X^N-1}$	D-NTRU (Wang et al., 2018) uses NTRUEncrypt as a reference to introduce its definition of the truncated polynomial ring. D-NTRU also uses another cryptosystem, namely C-NTRU as an aid to complete its security proof of IND-CPA (*Indistinguishability under Chosen Plaintext Attack*). D-NTRU is more efficient than all the provably secure NTRUEncrypt variants.
2018	DTRU1	$\frac{\mathbb{D}[X]}{X^N-1}$	DTRU1 (Camara et al., 2018) designs NTRUEncrypt over the ring of Dual Integers (or the ring with zero divisors), $\mathbb{D} = \mathbb{Z} + \epsilon\mathbb{Z}, \epsilon^2 = 0$. At the equivalent security level, DTRU1 is less efficient than NTRUEncrypt.

Table 2. (Continued)

2018	BQTRU	$\frac{(-1,-1)}{\mathbb{Z}[x,y]/(x^n-1,y^n-1)}$	BQTRU (Bagheri et al., 2018) generalizes NTRUEncrypt to bivariate polynomial over quaternion algebras, $\mathbb{H} = \{s_0 + s_1 i + s_2 j + s_3 k : s_0, s_1, s_2, s_3 \in \mathbb{R}\}$. At an equivalent set of the parameter, BQTRU more secure to lattice-based attack, brute force attack and Gentry attack than NTRUEncrypt. BQTRU also has a smaller public key size than NTRUEncrypt.
2019	NTRU-type public-key cryptosystem	$\frac{\mathbb{Z}_2[X]}{X^N-1}$	(Gu et al., 2019) proposes an NTRU-type public-key cryptosystem over a binary field, $\mathbb{Z}_2$ where its security is based on the difficulty of decisional unbalanced sparse polynomial ratio (DUSPR) problem. The NTRU-type public-key cryptosystem is relatively practical and efficient.

Table 2: NTRUEncrypt Variants.

4 CONCLUSION

The NTRUEncrypt variants discussed here were constructed based on several different type of algebraic structures. Deviating from the original NTRUEncrypt which was based on polynomial ring of $\mathbb{Z}$, to some other types of rings, algebra and vector spaces. Indeed, with different established properties for each variant has offered in some ways, a more secure and efficient scheme as compared to NTRUEncrypt. The data obtained from the survey also showed that NTRU and its variants can be used as an alternative method to replace the RSA in future. Looking at the prospect of lattice-based public-key cryptosystem, as a better resolution to quantum computer-based attacks, further revisions on NTRU and its variants are expected to take place in an extensive manner. Therefore, this paper provides a good start and reference to NTRU for future development.

ACKNOWLEDGMENTS

The work presented here was supported in part by a research university grant from Universiti Sains Malaysia, account no: 1001/PMATHS/8011121

REFERENCES

Alsaidi, N. M. and Yassein, H. R. (2016). Bitru: Binary version of the ntru public key cryptosystem via binary algebra. *International Journal of Advanced Computer Science & Applications*, 1:1–6.

Alsaidi, N. M. G., Sadiq, A. T., and Majid, A. A. (2016). Cqtru: A commutative quaternions rings based public key cryptosystem. *Engineering and Technology Journal*, 34(6 Part (B) Scientific):901–911.

Atani, R. E., Atani, S. E., and Karbasi, A. H. (2018). Netru: A non-commutative and secure variant of ctru cryptosystem. *The ISC International Journal of Information Security*, 10(1):45–53.

Bagheri, K., Sadeghi, M. R., and Panario, D. (2018). A non-commutative cryptosystem based on quaternion algebras. *Designs, Codes and Cryptography*, 86(10):2345–2377.

Banks, W. D. and Shparlinski, I. E. (2002). A variant of ntru with non-invertible polynomials. In *International Conference on Cryptology in India*, pages 62–70, Berlin Heidelberg. Springer.

Caboara, M., Caruso, F., and Traverso, C. (2008). Gröbner bases for public key cryptography. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 315–324, Hagenberg Austria. ACM.

Camara, M. G., Sow, D., Sow, D., and et Informatique, E. D. D. (2018). Dtru1: First generalization of ntru using dual integers. *International Journal of Algebra*, 12(7):257–271.

Challa, N. and Pradhan, J. (2007). Performance analysis of public key cryptographic systems rsa and ntru. *International Journal of Computer Science and Network Security*, 7(8):87–96.

Coglianese, M. and Goi, B. M. (2005). Matru: A new ntru-based cryptosystem. In et al., S. M., editor, *International Conference on Cryptology in India*, pages 232–243, Berlin Heidelberg. Springer.

Coppersmith, D. and Shamir, A. (1997). Lattice attacks on ntru. In Fumy, W., editor, *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 52–61, Berlin Heidelberg. Springer Verlag.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472.

Gaborit, P., Ohler, J., and Solé, P. (2002). Ctru, a polynomial analogue of ntru. *Institut National de Recherche en Informatique et en Automatique (INRIA)*, Theme 2(4621):1–12.

Gaithuru, J. N. and Salleh, M. (2017). Itru: Ntru-based cryptosystem using ring of integers. *International Journal of Innovative Computing*, 7(1):33–38.

Gaithuru, J. N., Salleh, M., and Mohamad, I. (2016). Mini n-th degree truncated polynomial ring (mini-ntru): A simplified implementation using binary polynomials. In *2016 IEEE 8th International Conference on Engineering Education (ICEED)*, pages 270–275. IEEE.

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

Gu, Y., Xie, X., and Gu, C. (2019). A new ntru-type public-key cryptosystem over the binary field. *Computers, Materials & Continua*, 60(1):305–316.

Hoffstein, J. (1996). Ntru: a new high speed public key cryptosystem. presented at the rump session of Crypto 96.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). Ntru: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288, Berlin Heidelberg. Springer.

Howgrave-Graham, N., Silverman, J. H., and Whyte, W. (2005). Choosing parameter sets for ntruencrypt with naep and sves-3. In *Cryptographers Track at the RSA Conference*, pages 118–135, Berlin Heidelberg. Springer.

Jarvis, K. and Nevins, M. (2015). Etru: Ntru over the eisenstein integers. *Designs, Codes and Cryptography*, 74(1):219–242.

Karbasi, A. H. and Atani, R. E. (2015). Iltru: An ntru-like public key cryptosystem over ideal lattices. *IACR Cryptology ePrint Archive*, 2015:549–557.

Karbasi, A. H., Atani, R. E., and Atani, S. E. (2018). Pairtru: Pairwise non-commutative extension of the ntru public key cryptosystem. *International Journal of Information Security Science*, 1(1):11–19.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209.

Kouzmenko, R. (2006). *Generalizations of the NTRU Cryptosystem*. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland. Diploma Project.

Malekian, E. and Zakerolhosseini, A. (2010a). Ntru-like public key cryptosystems beyond dedekind domain up to alternative algebra. In *Transactions on computational science X*, pages 25–41. Springer, Berlin Heidelberg.

Malekian, E. and Zakerolhosseini, A. (2010b). Otru: A non-associative and high speed public key cryptosystem. In *2010 15th CSI International Symposium on Computer Architecture and Digital Systems*, pages 83–90. IEEE.

Malekian, E., Zakerolhosseini, A., and Mashatan, A. (2011). Qtru: quaternionic version of the ntru public-key cryptosystems. *The ISC International Journal of Information Security*, 3(1):29–42.

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116.

Miller, V. S. (1985). Use of elliptic curves in cryptography. In Wiliams, H. C., editor, *Conference on the theory and application of cryptographic techniques*, pages 417–426, Berlin Heidelberg. Springer-Verlag.

Nayak, R., Sastry, C. V., and Pradhan, J. (2008). A matrix formulation for ntru cryptosystem. In *2008 16th IEEE International Conference on Networks*, pages 1–5. IEEE.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Thakur, K. and Tripathi, B. P. (2016). Btru, a rational polynomial analogue of ntru cryptosystem. *International Journal of Computer Applications*, 145(12):22–24.

Thakur, K. and Tripathi, B. P. (2017). A variant of ntru with split quaternions algebra. *Palestine Journal of Mathematics*, 6(2):598–610.

Thakur, K., Tripathi, B. P., and Yadav, M. R. (2016). Ktru: Ntru over the kleinian integers. *Journal of international academy of physical sciences*, 20(3):177–183.

Thang, C. M. and Binh, N. (2015). Dbtru, a new ntru-like cryptosystem based on dual binary truncated polynomial rings. In *2015 2nd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS)*, pages 11–16. IEEE.

Vats, N. (2009). Nnru, a noncommutative analogue of ntru. *arXiv preprint arXiv:0902.1891*, pages 1–14.

Wang, B., Lei, H., and Hu, Y. (2018). D-ntru: More efficient and average-case ind-cpa secure ntru variant. *Information Sciences*, 438:15–31.

Yassein, H. R. and Alsaidi, N. (2016). Hxdtru cryptosystem based on hexadecnion algebra. In *5th International Cryptology and Information Security Conference*, pages 1–14.

Yasuda, T., Dahan, X., and Sakurai, K. (2015). Characterizing ntru-variants using group ring and evaluating their lattice security. *IACR Cryptology ePrint Archive*, 2015:1170–1186.