TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2022) 46: 59 – 70
© TÜBİTAK
doi:10.3906/mat-2102-116

Efficient Nyberg-Rueppel type of NTRU digital signature algorithm

Ferdi ELVERDİ[1], **Sedat AKLEYLEK**[2,*], **Barış Bülent KIRLAR**[3]

[1]Department of Mathematics, Graduate School of Natural and Applied Sciences, Süleyman Demirel University, Isparta, Turkey

[2]Department of Computer Engineering, Faculty of Engineering, Ondokuz Mayıs University, Samsun, Turkey

[3]Department of Mathematics, Faculty of Arts and Sciences, Süleyman Demirel University, Isparta, Turkey

Received: 27.02.2021 • **Accepted/Published Online:** 29.11.2021 • **Final Version:** 19.01.2022

Abstract: Message recovery is an important property in Nyberg-Rueppel type digital signature algorithms. However, the security of Nyberg-Rueppel type digital signature algorithms depends on the hard problems which might be vulnerable to quantum attacks. Therefore, quantum resistant Nyberg-Rueppel type digital signature algorithms with message recovery property are needed. Since NTRU-based cryptosystems are one of the best studied quantum-resistant schemes, using traditional NTRU encryption scheme has several advantages on the message recovery property. In this paper, we define Nyberg-Rueppel type of NTRU digital signature algorithm. It is carried out by combining NTRU-based encryption and signature algorithms. In the proposed scheme, efficient message recovery property is achieved with the help of NTRU. Then, we compare the computational cost of our Nyberg-Rueppel type signature scheme with the others in terms of the arithmetic complexity. According to the asymptotic complexity results, the proposed scheme has better arithmetic complexity than Nyberg-Rueppel type schemes. We also discuss the security properties of the proposed scheme by modifying attacks on Nyberg-Rueppel type algorithms and lattice-based algorithms.

Key words: Message recovery, Post-quantum cryptography, NTRU, Digital signature

1. Introduction

New public-key cryptosystems alternative to traditional ones such as RSA and ECC have recently received widespread attention due to the unpredictable but possibly threat of constructing a quantum computer. Besides, Shor [39] proved that the cryptosystems, depending on the computationally hard integer factorization, discrete logarithm problem (DLP) over different groups, are not secure in quantum era. Then, it is obvious that asymmetric cryptographic systems based on these problems cannot be used in the long term [6]. As a consequence, it is necessary to propose alternative problems and related algorithms that are considered secure in quantum computers. In 2017, Post-Quantum Cryptography project, a call for quantum secure cryptosystems, was started by NIST [33]. There are several cryptosystem families in quantum safe world. Of these, lattice-based ones are the most attractive due to the security and performance properties. There are many lattice-based cryptosystems in the literature [3, 14, 16]. The NTRU public-key encryption algorithm (NTRUEncrypt) [16], is the most up-and-coming algorithm among quantum secure encryption systems (so-called post-quantum cryptography). The NTRU encryption algorithm was standardized by IEEE [22] and ASC X9 [2] in 2008 and 2010, respectively. The NTRU is not only quantum-resistant, it is also an efficient public-key cryptosystem.

*Correspondence: sedat.akleylek@bil.omu.edu.tr

2010 *AMS Mathematics Subject Classification:* 81P94, 94A60

NTRU has better time complexity when we consider traditional public-key cryptosystems. The security of this scheme relies on the intractability of related problems for convolutional lattices over a ring [42]. There are some variants of NTRU in the literature; some of them are based on square matrices of polynomials [8], quaternion algebra [29], ring of Eisenstein integers [31], ideal lattices [24] and group-ring structure [43]. Survey papers on NTRU-based cryptosystems were in the literature [41, 42]. Besides, there exist several lattice-based signature schemes that depend on the security of the NTRU lattice [16], such as BLISS [12] and pqNTRUSign [20]. The NTRU signature scheme (NSS) [17] was proposed in 2001. NSS has similar structure to the NTRUEncrypt. Both of them rely on the same hard problem which is so-called finding the closest vector problem. In 2001, Gentry and Szydlo [13] revealed that the original NSS scheme would not be resistant to the transcript attack. In 2003, a novel "semibased" NTRU digital signature algorithm, NTRUSign, was proposed in [16]. Then, it was shown that how to prevent transcript attacks using distributions in [11, 32]. Thereafter, how to implement distributions to NTRU-based signature schemes was introduced in [20, 37]. In 2019, some improvements were made to transcript attack-resistant signature schemes in [10]. A signature scheme of ElGamal type, having message recovery and key exchange properties in one protocol, was introduced in [34]. This was followed by several other proposals [1, 30, 35, 44]. However, in [30], it was shown that there is a security weakness such as not resistant to forgery attacks in some cases.

1.1. Our contribution

Quantum resistant cryptosystems have received attention due to the security reasons. Thus, traditional public key cryptosystems will be replaced with postquantum cryptographic schemes. Lattice-based cryptosystems are one of the best alternatives among them. Since NTRU-based cryptosystems have been widely studied, hybrid versions of NTRU-based cryptosystems will be attractive. Therefore, we focus on the traditional NTRU scheme to modify Nyberg-Rueppel digital signature algorithm. In this paper, we describe a new signature scheme (NR-NTRU-DSA) by using Nyberg-Rueppel digital signature algorithm (NR-DSA) and NTRU. The proposed scheme has message recovery property. Moreover, the proposed scheme uses NTRU encryption and it is resistant to some well-known forgery attacks and other related lattice attacks. The proposed scheme has better arithmetic complexity than the others having similar properties such as message recovery.

1.2. Organization

The rest is organized as follows: In Section 2, we recall basic definitions to construct the proposed signature scheme. In Section 3, the proposed NR-NTRU-DSA is discussed in detail. Correctness and security analysis are provided. This paper is concluded in Section 4.

2. Mathematical background

In this section we give the mathematical infrastructures for the proposed scheme (Algorithm 1), which uses NTRU-based primitives. NTRU is running over convolutional polynomial rings [16]. We first choose a fix prime integer N and determine modulo odd prime p satisfying $\gcd(p, N) = 1$ and modulo q satisfying $q \gg p$ and $\gcd(p, q) = 1$. Then, we have the convolutional polynomial rings $\mathcal{R}$, $\mathcal{R}_p$ and $\mathcal{R}_q$ defined by

$$\mathcal{R} = \frac{\mathbb{Z}[x]}{x^N - 1}, \quad \mathcal{R}_p = \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{x^N - 1} \quad \text{and} \quad \mathcal{R}_q = \frac{(\mathbb{Z}/q\mathbb{Z})[x]}{x^N - 1},$$

respectively. Due to the division algorithm for polynomials, any element $a(x) \in \mathcal{R}, \mathcal{R}_p$ or $\mathcal{R}_q$ is uniquely represented as

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} \tag{2.1}$$

where $a_0, a_1, \ldots a_{N-1} \in \mathbb{Z}, \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/q\mathbb{Z}$, respectively. Note that there is an isomorphism between polynomial ring and vector space. Then, addition of polynomials is the standard addition of vectors in coefficients. In order for working in the polynomial ring $X^N - 1$, one can define convolution product of the polynomials denoted by $\circledast$ for multiplication in $\mathcal{R}, \mathcal{R}_p$ and $\mathcal{R}_q$ [19]. For any positive integers d_1 and d_2, we define

$$\mathcal{T}(d_1, d_2) = \left\{ \begin{array}{ll} & a(x) \text{ has } d_1 \text{ coefficients equal to } 1, \\ a(x) \in \mathcal{R}: & a(x) \text{ has } d_2 \text{ coefficients equal to } -1, \\ & a(x) \text{ has all other coefficients equal to } 0. \end{array} \right\}.$$

Polynomials in $\mathcal{T}(d_1, d_2)$ are called ternary (or trinary - $\{-1, 0, 1\}$) polynomials. They are extended versions of binary polynomials, which have only 0's and 1's as coefficients. Then $\mathcal{T}(d+1, d)$ be the set of ternary polynomials having $2d+1$ coefficients. The sup-norm of the polynomial (2.1) is denoted by

$$\|a\|_\infty = \max\{|a_0|, |a_1|, |a_2|, \cdots, |a_{N-1}|\}.$$

Moreover, norm is an important issue $\mathcal{R}(k) = \{\, a \in \mathcal{R} : \|a\|_\infty \leq k \,\}$, where k is the sup-norm ball of radius. For instance, $\mathcal{R}(3/2)$ is the set of the ternary polynomials. Let

$$L_h = \{\, (f, g) \in \mathcal{R}^2 : g \equiv h \circledast f \pmod q \,\}$$

be the convolution modular lattice associated to h. The vectors in L_h are in the bounded norm as:

$$\begin{aligned} L_h(k_1, k_2) &= L_h \cap \big(\mathcal{R}(k_1) \times \mathcal{R}(k_2)\big) \\ &= \{\, (f, g) \in \mathcal{R}^2 : g \equiv h \circledast f \pmod q, \|f\|_\infty \leq k_1, \|g\|_\infty \leq k_2 \,\}. \end{aligned}$$

The lifted coefficients satisfy $-q/2 \leq a_i \leq q/2$ for even q and $\lfloor -q/2 \rfloor \leq a_i \leq \lfloor q/2 \rfloor$ for odd q. Note that $\lfloor x \rfloor$ is the floor function giving the greatest integer smaller than x (or equal). B_s and B_t are norm constraints parameters that allow to make the balance between security and performance. Typical values of B_s and B_t satisfying $B_s = pB_t$ and

$$\|a \circledast b\|_\infty \leq B_t \quad \text{for all } a, b \in \mathcal{R}(p/2).$$

Reducing B_s and B_t may cause to get a smaller q, but this is a possible problem to verify the signature. To overcome this situation, the signer can add one more control mechanism during the signature generation. In order to make it simple, one can choose $B = \lceil p^2 N/4 \rceil$ with $B = B_t = B_s$ [20]. For more details about mathematical background, the interested readers are referred to the studies in [19, 20].

3. Nyberg-Rueppel type of NTRU digital signature algorithm

In this section, we describe the details for the proposed signature scheme (Algorithm 1) called NR-NTRU-DSA. This is a combination of NTRU encryption [16] and Nyberg-Rueppel DSA [34], the first ElGamal type signature scheme. We show that the proposed algorithm is resistant to attacks on Nyberg-Rueppel type algorithms and lattice-based algorithms, especially the transcript attack [19]. Then, we make a comparison including

the computational cost of our scheme with the others in terms of the arithmetic complexity. In order to do these, we briefly describe necessary NTRU parameters (for more details [19]). First of all, $\mathcal{A}$ gets the public parameters (N, p, q, d, B) with an integer d satisfying $q > (2p^2 + 4p)d + p$ due to the efficiency reasons which are stated in Remark 3.5. She randomly selects $g(x) \in \mathcal{R}(p/2)$ and $f(x) \in p\mathcal{R}(3/2)$, where $f(x) = pF(x)$ with $F(x) \in \mathcal{T}(d+1, d) \subset \mathcal{R}(3/2)$. She has to check whether the inverses of F and g under modulo p and modulo q exist; if they are not, she selects a new pair. She then computes the inverse $f_q^{-1}(x) \in \mathcal{R}_q$, $g_p^{-1}(x) \in \mathcal{R}_p$ satisfying

$$f_q^{-1}(x) \circledast f(x) \equiv 1 \pmod{q}, \quad g_p^{-1}(x) \circledast g(x) \equiv 1 \pmod{p}.$$

Remark 3.1 *If the factorization of $(x^N - 1)/(x - 1)$ does not include polynomials with small degrees after reducing modulo p and q, then the probability of invertible elements is relatively high [19].*

Remark 3.2 *If we choose $F(x) \in \mathcal{T}(d+1, d)$, "Almost Inverse Algorithm" helps to efficiently compute the inverse of the polynomial $F(x)$ in the ring $\mathcal{R}_p$ or $\mathcal{R}_q$ provided that $\gcd(F(x), x^N - 1) = 1$ [40].*

She next calculates the public key $h(x)$ as

$$h(x) = f_q^{-1}(x) \circledast g(x) \text{ in } \mathcal{R}_q.$$

$\mathcal{B}$ randomly selects $v(x) \in \mathcal{R}$ and $u(x) \in p\mathcal{T}(d+1, d) \subset \mathcal{R}$, where $u(x) = 1 + pU(x)$ with $U(x) \in \mathcal{T}(d, d)$, then computes the inverse $u_q^{-1}(x) \in \mathcal{R}_q$ satisfying

$$u_q^{-1}(x) \circledast u(x) \equiv 1 \pmod{q}.$$

He computes the public key $l(x)$ as

$$l(x) = u_q^{-1}(x) \circledast v(x) \text{ in } \mathcal{R}_q.$$

Assume that $\mathcal{A}$ would like to send a signed and encrypted message $m(x) \in \mathcal{R}_p$ to $\mathcal{B}$ and then they proceed in Algorithm 1.

Remark 3.3 *In Algorithm 1, we fix the hash function H as follows:*

$$\begin{aligned} H \ : \ \mathcal{R}(p/2) \times \{0,1\}^\star &\longrightarrow \mathcal{R}(p/2) \times \mathcal{R}(p/2) \\ (h, \mu) &\longmapsto H(h, \mu) = (s_p, t_p). \end{aligned}$$

Remark 3.4 (Verification of Algorithm 1) *The first step of verification part of Algorithm 1 is true so that*

$$\begin{aligned} h \circledast s &= h \circledast (s_0 + a \circledast f) && (\textit{output (7) of signature}) \\ &= h \circledast s_0 + h \circledast a \circledast f && (\textit{distributive property}) \\ &\equiv t_0 + a \circledast g \pmod{q} && (\textit{output (5) of signature and public key of } \mathcal{A}) \\ &\equiv t \pmod{q}. && (\textit{output (7) of signature}) \end{aligned}$$

Algorithm 1: NR-NTRU-DSA

Public Parameters.

- N: a prime integer dimension of the ring.
- p: a relatively small odd prime.
- q: an integer satisfying $q \gg p$, $\gcd(p,q)=1$ and $\gcd(p,N)=1$.
- d: an integer satisfying $q > (2p^2+4p)d+p$.
- B: norm constraint with $B = \lceil p^2 N/4 \rceil$.

Private Keys.

- $f \in p\mathcal{R}(3/2)$ and $g \in \mathcal{R}(p/2)$ are the private keys of $\mathcal{A}$, where $f = pF$ with $F \in \mathcal{T}(d+1,d) \subset \mathcal{R}(3/2)$.
- f_q^{-1}, g_p^{-1} are the private keys of $\mathcal{A}$ satisfying $f_q^{-1} \circledast f \equiv 1 \pmod q$, $g_p^{-1} \circledast g \equiv 1 \pmod p$.
- $u \in p\mathcal{R}(3/2)$ and $v \in \mathcal{T}(d,d)$ are the private keys of $\mathcal{B}$, where $u = 1+pU$ with $U \in \mathcal{T}(d,d)$.
- u_q^{-1} is a private key of $\mathcal{B}$ satisfying $u_q^{-1} \circledast u \equiv 1 \pmod q$.

Public Keys.

- $h \equiv f_q^{-1} \circledast g \pmod q$ is a public key of $\mathcal{A}$.
- $l \equiv u_q^{-1} \circledast v \pmod q$ is a public key of $\mathcal{B}$.

Signature.

Input : $m \in \mathcal{R}_p$

Output: $(c,(s,t)) \in \mathcal{R} \times \mathcal{L}_h(\frac{q}{2}-B, \frac{q}{2}-B)$

(1) $\mathcal{A}$ randomly chooses an ephemeral key $r \in \mathcal{T}(d,d)$.
(2) $\mathcal{A}$ computes $c \equiv pr \circledast l + m \pmod q$ using $\mathcal{B}$'s public key l.
(3) $\mathcal{A}$ calculates the Hash value $H(h,c) = (s_p, t_p)$.
(4) $\mathcal{A}$ chooses a random ephemeral key $k \in \mathcal{R}\left(\left\lfloor \frac{q}{2p} + \frac{1}{2} \right\rfloor\right)$.
(5) $\mathcal{A}$ computes $s_0 = s_p + pk$ and then $t_0 \equiv h \circledast s_0 \pmod q$ with $t_0 \in \mathcal{R}(q/2)$.
(6) $\mathcal{A}$ computes $a \equiv g_p^{-1} \circledast (t_p - t_0) \pmod p$ with $a \in \mathcal{R}(p/2)$.
(7) $\mathcal{A}$ computes $(s,t) = (s_0 + a \circledast f, t_0 + a \circledast g)$.
(8) **If** $\|a \circledast f\|_\infty > B$, $\|a \circledast g\|_\infty > B$, $\|s\|_\infty > \frac{q}{2} - B$ and $\|t\|_\infty > \frac{q}{2} - B$ **then** go to Step 4 **end if**
(9) $\mathcal{A}$ sends the signature $(c,(s,t)) \in \mathcal{R} \times \mathcal{L}_h(\frac{q}{2}-B, \frac{q}{2}-B)$ to $\mathcal{B}$.

Verification.

Input : $(c,(s,t)) \in \mathcal{R} \times \mathcal{L}_h(\frac{q}{2}-B, \frac{q}{2}-B)$

Output: $m \in \mathcal{R}_p$

(1) $\mathcal{B}$ verifies that $t \equiv h \circledast s \pmod q$, otherwise rejects.
(2) $\mathcal{B}$ verifies that $\|s\|_\infty \le \frac{q}{2} - B$ and $\|t\|_\infty \le \frac{q}{2} - B$, otherwise rejects.
(3) $\mathcal{B}$ calculates the Hash value $H(h,c) = (s_p, t_p)$.
(4) $\mathcal{B}$ verifies that $(s,t) \equiv (s_p, t_p) \pmod p$, otherwise rejects.
(5) $\mathcal{B}$ computes $z \equiv u \circledast c \pmod q$ and then centerlifts z to $\mathbb{Z}^N$ with coefficients $|z_i| \le \frac{1}{2}q$.

Moreover, $z \equiv m \pmod p$.

The pair (s,t) is also congruent to $(s_p, t_p) \pmod p$ so that

$$\begin{aligned} s &= s_0 + a \circledast f && (\textit{output (7) of signature}) \\ &= s_p + pk + p(a \circledast F) && (\textit{output (5) of signature and } f = pF) \\ &\equiv s_p \pmod p && (\textit{modulo p reduction}) \end{aligned}$$

and

$$\begin{aligned} t &= t_0 + a \circledast g && (\textit{output (7) of signature}) \\ &\equiv t_0 + \cancel{g_p^{-1}} \circledast (t_p - t_0) \circledast \cancel{g} \pmod p && (\textit{output (6) of signature}) \\ &= \cancel{t_0} + t_p - \cancel{t_0} \pmod p \\ &= t_p \pmod p. \end{aligned}$$

In the last step, the verification of m is true so that

$$\begin{aligned} z &\equiv u \circledast c \pmod q \\ &\equiv u \circledast (pr \circledast l + m) \pmod q \\ &\equiv u \circledast (pr \circledast u_q^{-1} \circledast v + m) \pmod q \\ &\equiv p(\cancel{u \circledast u_q^{-1}} \circledast v \circledast r) + u \circledast m \pmod q \\ &\equiv p(v \circledast r) + (1 + pU) \circledast m \pmod q \\ &\equiv p(v \circledast r) + m + (pU \circledast m) \pmod q \\ &\equiv p(v \circledast r) + p(U \circledast m) + m \pmod q, \end{aligned}$$

then

$$\begin{aligned} z &\equiv \cancel{p(v \circledast r)} + \cancel{p(U \circledast m)} + m \pmod p \\ &\equiv m \pmod p. \end{aligned}$$

Remark 3.5 *NR-NTRU-DSA paramaters (N, p, q, d) are satisfied*

$$q > (2p^2 + 4p)d + p, \tag{3.1}$$

because of the following reasons: We consider $z(x)$ from $\mathcal{B}$'s side. Thus,

$$\begin{aligned} z(x) &\equiv u(x) \circledast c(x) \pmod q \\ &\equiv u(x) \circledast \big(pr(x) \circledast l(x) + m(x)\big) \pmod q \\ &\equiv u(x) \circledast \big(pr(x) \circledast u_q^{-1}(x) \circledast v(x) + m(x)\big) \pmod q \\ &\equiv p\big(\cancel{u(x) \circledast u_q^{-1}(x)} \circledast v(x) \circledast r(x)\big) + u(x) \circledast m(x) \pmod q \\ &\equiv p\big(v(x) \circledast r(x)\big) + u(x) \circledast m(x) \pmod q. \end{aligned}$$

If we think about the polynomial

$$p\big(v(x) \circledast r(x)\big) + u(x) \circledast m(x), \tag{3.2}$$

it is necessary to put an upper bound for the possible coefficients. Due to the polynomial $v(x), r(x) \in \mathcal{T}(d, d)$, the coefficients of $v(x) \circledast r(x)$ are bounded by $2d$. In a similar manner, let $U(x) \in \mathcal{T}(d, d)$ and then $u(x) = 1 + pU(x)$.

The coefficients of $m(x)$ *are in* $[-\frac{1}{2}p, \frac{1}{2}p]$*, thus the upper bound for the coefficients of* $u(x) \circledast m(x)$ *is given by* $(2pd+1)\frac{1}{2}p$*. Then, the magnitude of the largest coefficient of (3.2) is bounded by*

$$p(2d) + (2pd+1)\frac{1}{2}p = \left(p^2 + 2p\right) d + \frac{1}{2}p.$$

Thus, the assumption given in (3.1) tells us that the magnitude of the each coefficient of (3.2) is not larger than $\frac{1}{2}q$*.*

Remark 3.6 *It should be noted that we have proposed the rejection criterion in Step 8 of Algorithm 1. If a created signature does not meet the required norm criteria, the signature scheme returns to Step 4 and generates a new key. Then, we have a new signature. This phase is repeated until a signature that meets the norm constraints is generated. Moreover, the probability of generating a valid signature resulting from the rejection criteria contained in NR-NTRU-DSA is given in [20].*

Remark 3.7 *During the review process, it is suggested to use NTRU-HRSS [7] instead of NTRUEncrypt [16]. However, since there is no signature scheme which can efficiently work in this NR-type structure, i.e. message recovery property, we could not use NTRU-HRSS. We believe that constructing NTRU-based scheme for message recovery property is a nice problem to study.*

3.1. Computational cost

In Table , the comparison is provided in terms of the cost of signature generation (Sign), signature verification (Verify), throughput and message recovery property. Throughput is a measure of how many actions are completed within a given time frame. A signature scheme with message recovery is one where some or all of the message is embedded in the signature. The efficiency of the proposed scheme is discussed in Theorem 3.8.

Theorem 3.8 *The proposed scheme (Algorithm 1) has better signature generation and verification performance compared with similar schemes in terms of arithmetic complexity.*

Proof In GH-NR-DSA [5] and GH-DSA [15], double exponentiation in $\mathbb{F}_q$ where the order $Q|q^2+q+1$ in $\mathbb{F}_{q^3}$ is the main operation. In XTR-NR-DSA [34], double exponentiation is performed in $\mathbb{F}_q$ with $q = p^2$, where $Q|p^2 - p + 1$ in $\mathbb{F}_{p^6}$. GH-NR-DSA requires fewer operations than GH-DSA [15] and ECDSA [23] in terms of the computational cost and the message recovery. On the other hand, for twisted Edwards curves NR-DSA using the accelerated ECDSA verification algorithm is more efficient than GH-NR-DSA. The proposed scheme requires convolutional products. Then, to have a fair comparison, we compute the required number of arithmetic operations by considering the field sizes.

In Table , DS and CP stand for double-scalar and convolution product (in general polynomial multiplication), respectively. Q is the period of the corresponding irreducible polynomial. M and S stand for the cost of field multiplication and squaring in 2048-bit for 80-bit security level, respectively. Recall that the cost of polynomial multiplication is $\mathcal{O}(N \log N)$ for the polynomials having $N+1$ elements. In NTRU case, for 80-bit security level, $N = 509$ is given in [7]. Then, for the proposed scheme, the number of the modular multiplication to sign the message is $5 \cdot 509 \log 509\mathbf{M}$ in the field of 11-bit size. Recall that the integer multiplication can

Table . Comparison of the related DSAs.

	Sign	Verify	Throughput	Message recovery
GH-NR-DSA [5]	1 DS $(s_{f+eh}, s_{-(f+eh)})$	1 DS $(6\log Q\ \mathbf{M})$	m	Yes
GH-DSA [15]	1 DS $(s_{c(h-dl)}, s_{-c(h-dl)})$	1 DS $(16\log Q\ \mathbf{M} + 16\log Q\ \mathbf{S})$	m_1, m_2	No
EC-DSA[23]	1 DS $(u_1 + u_2 d)P$	1 DS $(7\log Q\ \mathbf{M} + 3.7\log Q\ \mathbf{S})$	m	No
NR-DSA with JSF algorithm [25]	1 DS $(u_1 + u_2 d)P$	1 DS $(7.1\log Q\ \mathbf{M})$	m	Yes
NR-DSA with the accelerated ECDSA verification algorithm [25]	1 DS $(u_1 + u_2 d)P$	1 DS $(4.7\log Q\ \mathbf{M})$	m	Yes
XTR-NR-DSA [34]	1 DS (s_{f+eh})	1 DS $(6\log Q\ \mathbf{M})$	m	Yes
Ours	5 CP	2 CP	m	Yes

be performed with n^2 multiplications (AND operations) in bits, where n is the bit size (at most 11-bit). The cost of double-scalar depends on the period (Q). For 80-bit security level, the period should be at least 80-bit. Then, the number of modular multiplication is $1280\mathbf{M} + 16\mathbf{S}$ in the field of 2048-bit size for [15]. By using the same idea, the lowest cost for the previous studies is $480\mathbf{M}$ in the field of 2048-bit size for [34]. Recall that multiplication of two 2048-bit integers requires much more time than multiplication of two 11-bit integers since the cost is computed with $\mathcal{O}(n^2)$. For instance, the cost for $1280\mathbf{M} + 16\mathbf{S}$ in the field of 2048-bit size for [15] is $1280 \cdot 2^{22} + 16 \cdot 2^{22}$ AND operations. Similarly, the cost for $5 \cdot 509 \log 509\mathbf{M}$ in the field of 11-bit size is less than 2^{21}. In conclusion, due to the low size (11-bit) of the ring, the proposed scheme has better signature generation and verification performance comparing with the similar schemes in terms of the arithmetic complexity. □

3.2. Security analysis

In Theorem 3.9, we give the security analysis of Algorithm 1 by dividing it into two parts: the encryption and signature algorithms.

Theorem 3.9 *The proposed scheme is resistant against modifying attacks on Nyberg Rueppel type algorithms and lattice-based algorithms.*

Proof The proof has two main sections: considering as an encryption algorithm and considering as a signature algorithm.

Considering as an encryption algorithm. In the proposed NR-NTRU-DSA, instead of sending only a summary of the message, the encrypted form of the message is sent, compared to the verification by classical signature methods. Therefore, when an attacker catches the output of the algorithm $\big((c,(s,t))$ pair$\big)$, it has the ciphertext (output of c). In this case, the attacker can perform some attacks by treating the proposed signature algorithm as only the encryption algorithm. Key recovery, a problem on the NTRU encryption system, is based on finding f and g polynomials that satisfy $f \circledast h \equiv g \pmod q$ while the public key h is known. The security of the NTRU encryption system depends on the hardness of obtaining the shortest (close one) vector in the corresponding lattice, which is a difficult problem in the lattice of appropriate sizes. Also, there are

well-known attacks in the literature that can be used against NTRU-based encryption systems, such as brute force, lattice-based and man-in-the-middle attacks.

- **Brute force attack.** An attacker to the NR-NTRU digital signature algorithm can perform one of the most basic brute force attack. The attacker makes an effort to access the key by trying the possibilities in the whole search space. In our scheme, an attacker can do this to detect the secret key by testing all possible $f \in p\mathcal{R}(3/2)$ elements to see if the polynomial $f \circledast h \pmod q$ has small inputs or by testing all possible $g \in \mathcal{R}(p/2)$ elements to see if the polynomial $g \circledast h^{-1} \pmod q$ has small inputs. In a similar manner, the attacker can get the message m by testing all possible $r \in \mathcal{T}(d,d)$ elements and checking whether the $c - r \circledast l \pmod q$ polynomial has small inputs. Thus, in practice, considering that $p = 3$, the security is measured by the number of elements of the set $\mathcal{T}(d,d)$.

- **Lattice-based attacks.** The security of the message is related with finding the closest vector whereas the security of obtaining keys is on the shortest vector problem. NTRU can be attacked by algorithms that find short vectors in a lattice, so the parameters should be large enough to make finding short vectors impossible. In theory, there are so many algorithms such as sieving to reveal the smallest vector, however this is not applicable for the large sizes in a reasonable time. Lenstra-Lenstra-Lovasz's (LLL) algorithm [28], also mathematically called the shortest vector finding problem, finds relatively small vectors in polynomial time with various improvements made by Schnorr [38], but needs a long time. Morever, it has also been noted that the encryption algorithms proposed in [9, 16] and the signature algorithms proposed in [20] can be selected to be resistant to various lattice attacks. As a result, since the proposed NR-NTRU-DSA is a combination of encryption and signature algorithms, it is also resistant to the lattice-based forgery and key recovery attacks.

- **Man-in-the-middle attack.** The security of NTRU-based encryption algorithms was studied in detail in [45] and [21]. In this attack, the square root of the security levels of the brute force attack is taken because the search set is halved by splitting the key [4, 16]. In this case, the security of the key and the message can be computed as follows:

$$\sqrt{\#\mathcal{T}(d,d)} = \frac{1}{d!}\sqrt{\frac{N!}{(N-2d)!}} \tag{3.3}$$

Considering as a signature algorithm.

- **Forgery and key recovery attacks.** A well-known attack on the signature algorithms in the literature is the forgery attack. Studies have been carried out on whether the signature algorithms with a similar structure of the proposed one are resistant to these lattice-based attacks. If an attacker wants to perform a forgery attack on the signature scheme, as expressed in [20, 37], it must solve the problem of finding the approximate closest vector in the corresponding lattice. Finding the approximate nearest vector in the corresponding lattice arises as a problem: It cannot be obtained in polynomial time by choosing inappropriate lattice dimensions. At the same time, as with NTRU-based encryption algorithms, a key recovery is also an attack that can be performed for signature algorithms. In [20], the analysis was performed against this attack based on the lattice basis, and the provided bit security levels were calculated. In light of these reasons, the proposed signature algorithm will also be resistant to these attacks.

- **Transcript attack.** Each document to be signed and signature pair $(c,(s,t))$ can reveal important information about the secret encryption key f in any signature scheme. When considering lattice-based signature schemes, the difference between the document and the signature pair will be a random point in the corresponding lattice fundamental domain. Therefore, a point is found in the lattice associated with taking the difference of each document and signature pair, and with enough points, the corresponding fundamental domain can be determined. This causes the corresponding lattice to be known, thus revealing the secret keys. Since 2001, efforts have been made to improve signature algorithms against this attack. In [13], it has been shown that the NSS algorithm [17] is not resistant to the transcript attack. In [16] a "semibased" NTRU digital signature algorithm which is so called NTRUSign was proposed. Then, in [11, 32] it is shown how to avoid transcript attack using Gauss distribution and its derivatives. For NTRU-based signature algorithms to gain resistance to the transcript attack, it was aimed to select the polynomials using uniform distributions, thus providing resistance to this attack. In [20], it is proved that the transcript of signatures, generated by using the signature algorithm, contains no additional information for someone having the public authentication key. In [10], some improvements were made to transcript attack-resistant signature schemes. NTRU-based signature algorithms have now been made resistant to transcript attack [11, 12, 18, 20, 32, 37]. As a result, the proposed NR-NTRU-DSA will be resistant to transcript attack, since it is designed by combining the following algorithms [20, 37].

- **Congruence and homomorphism attack.** NR signature scheme over finite fields of prime order is not resistant to the forgery attacks: congruence equation (CE) and homomorphism attacks (HA) in [30]. The NR-NTRU-DSA resists such attacks since this scheme is resistant to CE attack due to the redundancy and using hashing for the encrypted message, and the HA is not applicable due to not having a homomorphism.

□

4. Conclusions and future works

In this paper, we proposed Nyberg-Rueppel type of NTRU DSA by adjusting the signature scheme suggested by Nyberg and Rueppel to the NTRU-based signature algorithm. It was carried out by combining an NTRU-based encryption and NTRU-based signature algorithm. Then, we compared the computational cost of our Nyberg-Rueppel type signature scheme with the others in terms of the arithmetic complexity. We also examined the security of the proposed scheme in detail considering attacks on Nyberg-Rueppel type algorithms and lattice-based algorithms. As future work, with the recommendation of the reviewers, we will study on constructing a new signature scheme based on NTRU. Then, we will focus on building a new signature scheme with message recovery property.

Acknowledgments

This study was partially supported by the Scientific and Technical Research Council of Turkey (TÜBİTAK) under Grant No. 118E312. The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions in putting the present study into its final form and providing nice ideas for future works.

References

[1] Abe M, Okamoto T. A signature scheme with message recovery as secure as discrete logarithm. Advances in Cryptology - Asiacrypt 1999; LNCS 1716: 378-389.

[2] Accredited Standards Committee X9. Lattice-based polynomial public key establishment algorithm for the financial services industry. 2010.

[3] Ajtai M, Dwork C. A public key cryptosystem with worst-case/average-case equivalence. ECCC 1996; TR96-065.

[4] Akleylek S, Çevik N. MaTRU-KE revisited: CCA2-secure key establishment protocol based on MaTRU. International Journal of Communication Systems 2020; 33 (7): e4326.

[5] Ashraf M, Kırlar BB. Message transmission for GH-public key cryptosystem. Journal of Computational and Applied Mathematics 2014; 259: 578-585.

[6] Buchmann J, May A, Vollmer U. Perspectives for cryptographic long-term security. Communications of the ACM 2006; 49: 50-55.

[7] Chen, Q et al. NTRU:A submission to the NIST post-quantum standardization effort. NIST PQC Project, 2019.

[8] Coglianese M, Goi BM. MaTRU a new NTRU-based cryptosystem. In Proceedings of INDOCRYPT 2005; LNCS 3797: 232-243.

[9] Dai W, Whyte W, Zhang Z. Optimizing polynomial convolution for NTRUEncrypt. IACR eprint Archive 2018; 229.

[10] Das D, Hoffstein J, Pipher J, Whyte W, Zhang Z. Modular lattice signatures, revisited. Designs, Codes and Cryptography 2019; 88 (3): 1-28.

[11] Ducas L, Nguyen PQ. Learning a zonotope and more: cryptanalysis of NTRUSign countermeasures. Advances in Cryptology - Asiacrypt 2012: LNCS 7658: 433-450.

[12] Ducas L, Durmus A, Lepoint T, Lyubashevsky V. Lattice signatures and bimodal gaussians. Advances in Cryptology - CRYPTO 2013; LNCS 8042: 40-56.

[13] Gentry C, Szydlo M. Cryptanalysis of the revised NTRU signature scheme. Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2002; 299-320.

[14] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems. Advances in Cryptology - CRYPT0 1997; LNCS 1294: 112-131.

[15] Gong G, Harn L, Wu H. The GH public-key cryptosystem. Selected Areas in Cryptography - SAC 2001; LNCS 2259: 284-300.

[16] Hoffstein J, Pipher J, Silverman JH. NTRU: A ring-based public key cryptosystem. Algorithmic Number Theory (ANTS) 1998; LNCS 1423: 267-288.

[17] Hoffstein J, Pipher J, Silverman JH. NSS: An NTRU lattice-based signature scheme. International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2001; LNCS 2045: 211-228.

[18] Hoffstein J, Pipher J, Silverman JH. NTRUSign: digital signatures using the NTRU lattice. Topics in Cryptology - CT-RSA 2003; LNCS 2612: 122-140.

[19] Hoffstein J, Pipher J, Silverman JH. An Introduction to Mathematical Cryptography, New York: Springer, 2008.

[20] Hoffstein J, Pipher J, Schanck JM, Silverman JH, Whyte W. Transcript secure signatures based on modular lattices. IACR eprint Archive 2014; 457.

[21] Howgrave-Graham N. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. Advances in Cryptology CRYPTO 2007: LNCS 4622: 150-169.

[22] IEEE Std 1363.1-2008. IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. 2008.

[23] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security 2001; 1 (1): 36-63.

[24] Karabsi AH, Atani RE. ILTRU: An NTRU-like public key cryptosystem over ideal lattices. IACR eprint Archive 2015; 549.

[25] Kırlar BB. Efficient message transmission via twisted Edwards curves. Mathematica Slovaca 2020; 70 (6): 1511-1520.

[26] Koblitz N. Elliptic curves cryptosystems. Mathematics of Computation 1987; 48: 203-209.

[27] Lenstra AK, Verheul ER. An overview of the XTR public key system. In Alster K, Urbanowicz J, Williams HC (editors). Public-Key Cryptography and Computational Number Theory 2001. Warsaw, Poland: Walter de Gruyter, 2001; 151-181.

[28] Lenstra AK, Lenstra HW, Lovász L. Factoring polynomials with rational coefficients. Mathematische Annalen 1982; 261 (4): 515-534.

[29] Malekian E, Zakerolhosseini A, Mashatani A. QTRU: a lattice attack resistant version of NTRU. IACR eprint Archive 2009; 386.

[30] Miyaji A. Weakness in message recovery signature schemes based on discrete logarithm problems 1. IEICE Japan Technical Reports, ISEC95-7, 1995.

[31] Nevins M, Karimianpour C, Miri A. NTRU over rings beyond $\mathbb{Z}$. Designs, Codes and Cryptography 2010; 56: 65-78.

[32] Nguyen PQ, Regev O. Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. Journal of Cryptology 2009; 22 (2): 139-160.

[33] NIST. Post-Quantum Cryptography Project 2017.

[34] Nyberg K, Rueppel RA. A new signature scheme based on the DSA giving message recovery. Proceedings of the 1st ACM Conference on Computer and Communications Security 1993; 58-61.

[35] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm problem. Designs, Codes and Cryptography 1996; 7 (1-2): 61-81.

[36] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystem. Communications of the ACM 1978; 21: 120-126.

[37] Schanck J. Practical lattice cryptosystems: NTRUEncrypt and NTRUMLS. M.Sc. Thesis. University of Waterloo, Canada, 2015.

[38] Schnorr CP. Fast LLL-type lattice reduction. Information and Computation 2006; 204: 1-25.

[39] Shor P. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994; 124-134.

[40] Silverman JH. Almost inverses and fast NTRU key creation. NTRU Cryptosystems. Technical Note # **014**, 1999.

[41] Singh S, Padhye S. Generalisations of NTRU cryptosystem. Security and Communication Networks 2016; 9: 6315-6334.

[42] Steinfeld R. NTRU cryptosystem: recent developments and emerging mathematical problems in finite polynomial rings. Niederreiter H, Ostafe A, Panario D, Winterhof A (editors). Algebraic Curve and Finite Fields: Cryptography and Other Applications 2014. Berlin, Germany: De Gruyter, 2014; 179-212.

[43] Yashoda T, Dahan X, Sakurai K. Characterizing NTRU-variants using group ring evaluating their lattice security. IACR eprint Archive 2015; 1170.

[44] Yeun CY. Digital signature with message recovery and authenticated encryption (signcryption) a comparison. IMA - Cryptography and Coding 1999; LNCS 1746: 307-312.

[45] Wang H, Ma Z, Ma CG. An efficient quantum meet-in-the-middle attack against NTRU-2005. Chinese Science Bulletin 2013; 58 (28-29): 3514-3518.