A SOLUTION TO IMPROVING ENCRYPTION EFFICIENCY OF DTRU CRYPTOSYSTEM

Cao Minh Thang, Nguyen Binh
Posts and Telecommunications Institute of Technology, Ha Noi, Vietnam

Abstract: DTRU, a new variant of NTRU public - key cryptosystem, has some advantages in comparison with original NTRU at the same security levels. However, in DTRU, the cipher-text is at least three time longer than the plain-text i.e., message-expansion factor of DTRU is higher than that of other well-known public-key cryptosystems. By modifying encryption procedure, in this paper, we propose a new variant of DTRU, called M-DTRU, that has not only smaller message-expansion factor but also larger message-security than original cryptosystem.

Keywords: cryptography, cryptosystem, binary, truncated polynomial rings, message-expansion factor, message-security, NTRU, DTRU.

I. INTRODUCTION

NTRU [2], proposed by J. Hoffstein, J. Pipher and J.H. Silverman in 1996, is a probabilistic public key cryptosystem runs on a N - *th* degree truncated polynomial ring $R = Z[x]/(x^N - 1)$. NTRU is known as one of the fastest public-key encryption schemes and is standardized in 2008 by IEEE in standard P.1363.1. Because of the speed of the NTRU and its low memory use, it can be used in applications such as mobile devices and smart-cards. In April 2011, NTRU was accepted as a X9.98 Standard, for use in the financial services industry. For those reasons, NTRU is attractive cryptosystem to use in constrained environments such as embedded systems.

Beside standard NTRU, there are some interesting variants of NTRU proposed over the last two decades in [3], [4], [5], [6], [7], [8] and [9]. Recently, by exploiting two special class of binary truncated polynomial ring, a newest variants of NTRU, called DTRU [1] was introduced with the same complexity and security but smaller keys in comparison with original NTRU.

However, as in NTRU, the message-expansion factor in DTRU is a disadvantage of this cryptosystem. Depending on two integers S and L, with the proposed constrain of $L > 3S$, the message-expansion factor of DTRU is larger than 3, a rather large value in comparison with other well-known public key cryptosystems. This issue impacts much on the encrypting performance and prevent applying DTRU in practical uses.

By observing the structure of encrypting function in DTRU, we realize that the random polynomial ϕ, which is used for blinding the plain-text m, can be exploited to store the extra plain-text while still ensuring the security purpose.

For convenience, the brief introduction about DTRU is provided in section II. In section III, we give a simple but important lemma for recovering from ϕ product $\phi \times (x^S + 1)$ in $R_L[x]$ thereby propose a modification of DTRU, called M-DTRU, that has not only smaller message-expansion factor but also larger message-security. The conclusion and future works are mentioned in section IV.

II. DTRU CRYPTOYSTEM

DTRU is a new variant of NTRU cryptosystem that operates on dual polynomial rings with some advantages in comparison with standard NTRU. The trap-doors of DTRU is a polynomial which is invertible in two different polynomial rings.

Corresponding author: Cao Minh Thang
Email: thangcm@ptit.edu.vn
Manuscript received: 23/7/2016, revised: 30/8/2016, accepted: 03/9/2016

A. Definition and notation

Definition 1: The set of integers n such that $x^n + 1 = (1 + x).T$ where $T = \sum_{i=0}^{N-1} x^i$ is irreducible polynomial in GF(2) is denote as N_{2C}

Definition 2: The set of $n = 2^k$ where k is a arbitrary positive integer is denote as N_{2^k}

B. Key generation

Bob chooses two arbitrary positive integers $S, L \in Z^+ \mid L > S, \gcd(S, L) = 1$ and use two rings $R_S[x]$ and $R_L[x]$ to construct DTRU.

Bob chooses an arbitrary polynomial $f \in R_S[x]$ invertible in both $R_S[x]$ and $R_L[x]$ and computes two polynomials $F_S \in R_S[x]$ and $F_L \in R_L[x]$ such that

$$F_L * f = 1 \bmod (x^L + 1)$$

and $F_S * f = 1 \mod (x^S + 1)$

Bob chooses a non-zero $g \in R_S[x]$ and computes $L - bit$ public key

$$h = g * F_L * (x^S + 1). \quad (1)$$

Bob keeps (f, F_s) (f, F_S) as two private keys (F_L can be discarded) and sends S, L and h to Alice

C. Encryption

To encrypt $S - bit$ plain-text message m, Alice selects a non-zero arbitrary $\phi \in R_S[x]$ and computes

$$e = \phi * h + m \quad (2)$$

and send $L - bit$ cipher-text message e to Bob.

D. Decryption

When receiving e, Bob computes

$$a = f * e \bmod (x^L + 1) \quad (3)$$

and then recovers

$$m = F_S * a \bmod (x^S + 1). \quad (4)$$

E. Decryption criteria

The requirement for correct decryption in DTRU is that $a = \phi * g * (x^S + 1) + f * m$ does not change under modulo $x^L + 1$ therefore we must ensure

Table I. Underlying algebraic structures of equivalent parameters of NTRU and DTRU

Parameters	NTRU	DTRU
N, p, q	$N, p, q \in Z^+ \mid q >> p, \gcd(p, q) = 1$	$S, L \in Z^+ \mid \gcd(S, L) = 1$
$\mathcal{L}_f$	$\mathcal{L}(d_f, d_f - 1)$	$I_S[x]$
$\mathcal{L}_g$	$\mathcal{L}(d_g, d_g)$	$R_S[x]$
$\mathcal{L}_\phi$	$\mathcal{L}(d, d)$	$R_S[x]$
$\mathcal{L}_m$	$m \in R \mid m_i \in [-(p-1)/2, (p-1)/2]$	$m \in R_S[x] \mid \deg m \le S - 1$
F_p	$F_p * f = 1 \pmod p$	$F_S * f = 1 \pmod{x^S + 1}$
F_q	$F_q * f = 1 \pmod q$	$F_L * f = 1 \pmod{x^L + 1}$

Table II. Theoretical performance and security of DTRU in comparison with NTRU where $S \in N_{2C}$ *and* $L \in N_{2^k}$

	DTRU	**NTRU**
Public Key (bits)	L	$M = N.\log_2 q$
Private Key (bits)	$2S$	$2N.\log_2 p$
Cipher-text block (bits)	L	$N.\log_2 q$
Plain-text block (bits)	$S-1$	$N.\log_2 p$
Encryption (bit operations)	$O((\log_2 L)^2)$	$O((\log_2 M)^2)$
Decryption (bit operations)	$O((\log_2 L)^2)$	$O((\log_2 M)^2)$
Message expansion (e (bits) – to – m (bits))	$L/(S-1)-to-1$	$\log_p q - to - 1$
Decryption criteria	$L > 3S-1$	$\lvert f*m + p\phi * g\rvert_\infty < q$
Message-security, Key-security	2^{S-2}, 2^{S-2}	$\frac{1}{d!}\sqrt{\frac{N!}{(N-2d)!}}$, $\frac{1}{d_g!}\sqrt{\frac{N!}{(N-2d_g)!}}$

Table III. Comparison in moderate security mode of NTRU

Moderate security	**NTRU**	**DTRU**
Basic parameters	$(N,p,q) = (107,3,64)$	$(S,L) = (53,256)$
Message security	$2^{26.5}$	2^{51}
Key security	2^{50}	2^{51}
Public key (bits)	642	256
Private key (bits)	340	106
Message-expansion factor	3.78	4.92

Table IV. Comparison in high security mode of NTRU

High security	**NTRU**	**DTRU**
Basic parameters	$(N,p,q) = (167,3,128)$	$(S,L) = (83,256)$
Message security	$2^{77.5}$	2^{81}
Key security	$2^{82.9}$	2^{81}
Public key (bits)	1169	256
Private key (bits)	530	166
Message-expansion factor	4.23	3.16

Table V. Comparison in highest security mode of NTRU

Highest security	NTRU	DTRU
Basic parameters	$(N, p, q) = (502, 3, 256)$	$(S, L) = (293, 1024)$
Message security	2^{170}	2^{291}
Key security	2^{285}	2^{291}
Public key (bits)	4024	1024
Private key (bits)	1595	586
Message-expansion factor	5.05	3.51

$$\deg\phi + \deg g + S < L$$

Since $\deg\phi, \deg g, \deg f, \deg m < S$, by choosing

$$L > 3S \qquad (5)$$

we can make sure that decryption is always success.

F. DTRU in comparison with NTRU

The comparison underlying algebraic structures of DTRU in comparison with NTRU are described in Table I.

Table II shows the theoretical performance of DTRU in comparison with NTRU. It is clear that DTRU is as fast as NTRU.

The comparison in three proposed security cases of NTRU and DTRU in [2] is given in table III, table IV and table V.

The theoretical results show that, at nearly the same security levels, DTRU always uses much smaller keys. At the security levels equivalent to high and highest security cases of NTRU, the massage expansion factor of DTRU is smaller than that of NTRU.

III. M-DTRU, PROPOSED VARIANT OF DTRU

In this section, we point out that the polynomial ϕ can be exploited to store the extra plain-text and propose a variant of DTRU, named M-DTRU, with lower message-expansion factor and higher message-security in comparison with DTRU summarized above

A. Definition and notation

Definition 3: The Hamming weight of arbitrary polynomial $f \in R_n[x]$ is denoted as $w(f)$

Definition 4: A polynomial $f \in R_n[x]$ is invertible if there exists $g \in R_n[x]$ satisfying $g * f = 1 \ (\mathrm{mod}(x^n + 1))$

Definition 5: The set of polynomials having odd Hamming weight in $R_n[x]$ is denoted as $I\ [x]$

It is clear that $\left|I_n[x]\right| = 2^{n-1}$

Definition 6: In $R_n[x]$, the ratio of number of invertible element over the total number of polynomials in ring is denoted as K_n

Since invertible polynomials always have odd Hamming weight, by Definition 5, we can see that $\max(K_n) = \left|I_n[x]\right| / \left|R_n[x]\right| = 1/2$

For easy comparison between NTRU and DTRU we reuse some notations in NTRU including parameters $f, g, \varphi, m, h, e, a$ and four sets $\mathcal{L}_f$, $\mathcal{L}_g$,

$\mathcal{L}_\phi$, $\mathcal{L}_m$ as well as truncated ring $R = Z[x]/x^N - 1$. We use $*$ to denote the polynomial multiplication in $R_N[x]$

Because DTRU runs on two binary truncated polynomial rings, $R_L[x]$ is larger than $R_S[x]$, we denote two inverse of private key f in those rings as F_L and F_S, respectively.

B. A supplement lemma

In this sub-section we proof a lemma allowing M-DTRU to decrypt the ϕ polynomial from cipher-text successfully.

Lemma 3.1: With two positive integers S and L where $L \geq 2S$, suppose that f is a polynomial of $\deg f \leq S-1$ in polynomial ring $R_L[x]$.

if $g = \sum_{i=0}^{L-1} g_i x^i = f*(x^S+1)$ then $f = \sum_{i=0}^{S-1} g_i x^i$

Proof: Since $\deg f \leq S-1$ then

$$f = \sum_{i=0}^{S-1} f_i x^i \mid f_i \in GF(2)$$

therefore we have

$$g = \sum_{i=0}^{S-1} f_i x^i + x^S * \sum_{i=0}^{S-1} f_i x^i = \sum_{i=0}^{S-1} f_i x^i + \sum_{i=0}^{S-1} f_i x^{(i+S) \bmod L}.$$

Since $i+S < L$, By replacing $i = j - S$, we have

$$\sum_{i=0}^{S-1} f_i x^{(i+S) \bmod L} = \sum_{j=S}^{2S-1} f_j x^{j+S} = \sum_{i=S}^{2S-1} f_i x^{i+S} \text{ and}$$

$$g = \sum_{i=0}^{S-1} f_i x^i + \sum_{i=S}^{2S-1} f_i x^{i+S}$$

thereby $f_i = g_i \mid i \in [0, S-1]$ or $f = \sum_{i=0}^{S-1} g_i x^i$. □

C. Key generation

Firstly, Bob chooses two positive integers $S, L \in Z^+ \mid L > S, \gcd(S, L) = 1$ and use two rings $R_S[x]$ and $R_L[x]$ to construct DTRU.

Bob chooses an arbitrary polynomial $f \in R_S[x]$ invertible in both $R_S[x]$ and $R_L[x]$ and computes two polynomials $F_S \in R_S[x]$ and $F_L \in R_L[x]$ such that

$$F_L * f = 1 \bmod (x^L + 1) \text{ and } F_S * f = 1 \bmod (x^S + 1)$$

Bob chooses an arbitrary $g \in R_S[x]$ which is invertible in $R_L[x]$ and computes its inverse $G_L \in R_L[x]$ such that $G_L * g = 1 \bmod (x^L + 1)$.

Finally, Bob computes $L-bit$ public key

$$h = g * F_L * (x^S + 1). \quad (6)$$

Bob keeps (f, F_S, G_L) as two three keys (F_L can be discarded) and sends S, L and h to Alice.

D. Encryption

To encrypt $2S-bit$ plain-text ℓ, Alice divides it into $S-bit$ message m and $S-bit$ ϕ where $\ell = m.x^{S-1} + \phi$ and computes

$$e = \phi * h + m \quad (7)$$

and send $L-bit$ cipher-text message e to Bob.

E. Decryption

When receiving e, Bob computes

$$a = f * e \bmod (x^L + 1) \quad (8)$$

and then obtains $S-bit$

$$m = F_S * a \bmod (x^S + 1). \quad (9)$$

After that, Bob computes

$$d = f * G_L * (e + m) \bmod (x^L + 1) \quad (10)$$

and then, by Lemma 3.1, gets $S - bit$

$$\phi = \sum_{i=0}^{S-1} d_i x^i \quad (11)$$

Finally, Bob recovers $2S - bit$ plain-text

$$\ell = m.x^{S-1} + \phi \ .$$

F. Proof of Decryption

By replacing (7) into (8) we have

$$a = f * e \bmod (x^L + 1) = f * (\phi * h + m) \bmod (x^L + 1)$$
$$a = (f * \phi * g * F_L * (x^S + 1) + k * m) \bmod (x^L + 1)$$
$$a = (\phi * g * (x^S + 1) + f * m) \bmod (x^L + 1)$$

Therefore,

$$F_S * a \bmod (x^S + 1) = F_S * f * m \bmod (x^S + 1) = m \bmod (x^S + 1)$$

or $m = F_S * a \bmod (x^S + 1)$

In addition, since $m + e = \phi * h \bmod (x^L + 1)$ we have

$$d = f * G_L * (e + m) \bmod (x^L + 1) = f * G_L * (\phi * h) \bmod (x^L + 1)$$
$$= f * G_L * \phi * (g * F_L * (x^S + 1)) \bmod (x^L + 1)$$
$$= \phi * (x^S + 1) \bmod (x^L + 1).$$

and, by Lemma 3.1, we get $\phi = \sum_{i=0}^{S-1} d_i x^i$

thereby we can recover $2S - bit$ plain-text $\ell = m.x^{S-1} + \phi$. □

G. Theoretical message-security of M-DTRU

Since the size of plain-text message in M-DTRU is now double longer than that of DTRU, the message-security value of M-DTRU is thus two times larger and is 2^{S-1} while the DTRU's one is 2^{S-2}.

H. Decryption criterion

The requirement for correct decryption in M-DTRU is the same as in DTRU and is

$$L > 3S \quad (12)$$

I. Examples

Bob chooses $S = 5, L = 16$ and uses $R_5[x]$ and $R_{16}[x]$ to construct cryptosystem.

Key generation:

Bob chooses $f = x^3 + x^2 + 1$ and computes its two inverses

$F_S = x^4 + x + 1$ and

$$F_L = x^{15} + x^{13} + x^{10} + x^9 + x^8 + x^6 + x^3 + x^2 + x$$

Bob chooses $g = x^4 + x^3 + 1$ and computes its inverse in $R_{16}[x]$

$$G_L = x^{15} + x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^4 + 1$$

Finally, Bob computes public key

$$h = x^{15} + x^{14} + x^{12} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x^2$$

and sends *S, L* and *h* to Alice.

Encryption:

In order to encrypt $10 - bit$ message $\ell = (0010111100)$, or $\ell = x^7 + x^5 + x^4 + x^3 + x^2$ in polynomial form, Alice divides it into

$5 - bit$ m = (00101) and $5 - bit$ ϕ = (11100) or $m = x^2 + 1$ and $\phi = x^4 + x^3 + x^2$ in polynomial form

After that, by using (7), Alice computes

$$e = (x^4 + x^3 + x^2) * (x^{15} + x^{14} + x^{12} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x^2) + (x^2 + 1) \bmod (x^{16} + 1)$$
$$= (x^{15} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^4 + x^3 + x^2 + 1) \bmod (x^{16} + 1)$$

and sends $16 - bit$ cipher-text e to Bob.

Decryption:

When receiving e from Alice, by using (8), Bob computes

$$a = (x^3 + x^2 + 1) * (x^{15} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^4 + x^3 + x^2 + 1) \bmod (x^{16} + 1)$$
$$= (x^{13} + x^{10} + x^9 + x^7 + x^6 + x^3 + x^2 + x) \bmod (x^{16} + 1)$$

and by (9) obtains

$$m = (x^3 + x^2 + 1) * (x^{13} + x^{10} + x^9 + x^7 + x^6 + x^3 + x^2 + x) \bmod (x^5 + 1)$$
$$= (x^2 + 1) \bmod (x^5 + 1).$$

In the next step, by (10), Bob computes

$$d = (x^9 + x^8 + x^7 + x^4 + x^3 + x^2) \bmod (x^{15} + 1)$$
$$= (x^4 + x^3 + x^2) * (x^5 + 1) \bmod (x^{15} + 1)$$

and, by Lemma 3.1, get $\phi = x^4 + x^3 + x^2$

Finally, Bob reconstructs 10 – *bit*

$$\ell = m * x^5 + \phi = (x^2 + 1) * x^5 + (x^4 + x^3 + x^2)$$
$$= x^7 + x^5 + x^4 + x^3 + x^2$$

or $\ell = (0010111100)$ in binary form.

J. Comparison with DTRU

By making use of ϕ, M-DTRU can encrypt maximally $2S$ bit plain-text message at once therefore the message-expansion of M-DTRU is twice smaller than that of DTRU. Consequently, the message-security value is increased by factor of 2 in comparison with DTRU.

However, the drawback of M-DTRU is that it uses 03 private keys f, F_S, G_L with totally $2S + L$ while this value of DTRU is only $2S$.

The theoretical performance and security of M-DTRU and DTRU are compared in Table VI.

The comparison in three proposed security cases of NTRU, DTRU in [1] and M-DTRU is given in table VII, table VIII and table IX

At nearly the same security levels, M-DTRU always has much smaller message-expansion factor and larger message-security than NTRU and DTRU does. Especially, in table IX, the message-expansion factor of DTRU is only 1.75, nearly three time smaller equivalent value of NTRU (5.05).

At all three security levels, the total size of private keys in M-DTRU is nearly the same as that of NTRU but larger than DTRU's one.

IV. CONCLUSION

By exploiting the random polynomial in encrypting procedure, the M-DTRU scheme obtains lower message-expansion factor and higher message-security in comparison with original DTRU. This variant also provides another choice for constructing DTRU. However, similar to DTRU, this proposal needed more cryptanalysis under various attacks to ensure about its security.

ACKNOWLEDGEMENT

This research was supported by Information and Communication Institute of Technology (CDIT), a subsidiary research institute of Posts and Telecommunications Institute of Technology (PTIT).

Table VI. Theoretical performance and security of M-DTRU modification in comparison with DTRU

	DTRU	M-DTRU
Public Key (bits)	L	L
Private Key (bits)	$2S$	$2S + L$
Cipher-text block (bits)	L	L
Plain-text block (bits)	$S - 1$	$2S$
Encryption (bit operations)	$O((\log_2 L)^2)$	$O((\log_2 L)^2)$
Decryption (bit operations)	$O((\log_2 L)^2)$	$O((\log_2 L)^2)$

	DTRU	M-DTRU
Message-expansion factor	$L/(S-1)-to-1$	$L/2S-to-1$
Decryption criteria	$L>3S-1$	$L>3S-1$
Message-security	2^{S-2}	2^{S-1}
Key-security	2^{S-2}	2^{S-2}

Table VII. Comparison in moderate security mode of NTRU and DTRU

Moderate security	NTRU	DTRU	M-DTRU
Basic parameters	$(N,p,q)=(107,3,64)$	$(S,L)=(53,256)$	$(S,L)=(53,256)$
Message security	$2^{26.5}$	2^{51}	2^{52}
Key security	2^{50}	2^{51}	2^{51}
Public key (bits)	642	256	256
Private key (bits)	340	106	309
Message-expansion factor	3.78	4.92	2.42

Table VIII. Comparison in high security mode of NTRU and DTRU

High security	NTRU	DTRU	M-DTRU
Basic parameters	$(N,p,q)=(167,3,128)$	$(S,L)=(83,256)$	$(S,L)=(83,256)$
Message security	$2^{77.5}$	2^{81}	2^{82}
Key security	$2^{82.9}$	2^{81}	2^{81}
Public key (bits)	1169	256	256
Private key (bits)	530	166	422
Message-expansion factor	4.23	3.16	1.54

Table IX. Comparison in highest security mode of NTRU and DTRU

Highest security	NTRU	DTRU	M-DTRU
Basic parameters	$(N,p,q)=(502,3,256)$	$(S,L)=(293,1024)$	$(S,L)=(293,1024)$
Message security	2^{170}	2^{291}	2^{292}
Key security	2^{285}	2^{291}	2^{291}
Public key (bits)	4024	1024	1024
Private key (bits)	1595	586	1610
Message-expansion factor	5.05	3.51	1.75

REFERENCES

[1] Cao Minh Thang, Nguyen Binh (2015). "DTRU, a new NTRU-like cryptosystem based-on dual truncated polynomial rings". Journal of Science and Technology, Vietnam Academy of of science and technology, Set 53 – Number 2C, 2015. ISSN 0866 708X, pp 103-118.

[2] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. NTRU: Alice ring-based public key cryptosystem. Lecture Notes in Computer Science Volume 1423, pp 267-288, Springer Verlag 1998.

[3] William D. Banks, Igor E. Shparlinski. A Variant of NTRU with Non-invertible Polynomials. Lecture Notes in Computer Science Volume 2551, 2002, pp 62-70.

[4] Gaborit, P., Ohler, J., Sole, P.: CTRU, a Polynomial Analogue of NTRU, INRIA. Rapport de recherche, N.4621 (November 2002), (ISSN 0249-6399).

[5] Michael Coglianese, Bok-Min Goi. MaTRU: A New NTRU-Based Cryptosystem. Lecture Notes in Computer Science Volume 3797, 2005, pp 232-243.

[6] Malekian, E. Zakerolhosseini. OTRU: A non-associative and high speed public key cryptosystem. A.Computer Architecture and Digital Systems (CADS), 2010 15th CSI International Symposium on, Tehran, pp 83 – 90, ISBN: 978-1-4244-6267-4.

[7] Yanbin Pan, Yingpu Deng. A General NTRU-Like Framework for Constructing Lattice-Based Public-Key Cryptosystems. Lecture Notes in Computer Science Volume 7115, 2012, pp 109-120.

[8] Katherine Jarvis, Monica Nevins. ETRU: NTRU over the Eisenstein integers. Springer Date: 13 Jul 2013.

[9] Yanbin Pan, Yingpu Deng, Yupeng Jiang, Ziran Tu. A New Lattice-Based Public-Key Cryptosystem Mixed with a Knapsack. Lecture Notes in Computer Science Volume 7092, 2011, pp 126-137.

Cao Minh Thang

MSc. He is working at the Posts and Telecommunications Institute of Technology (PTIT). His research interests include networking, electronics, cryptography.

Nguyen Binh

He is a professor in Electronics and Telecommunications Engineering at the Posts and Telecommunications Institute of Technology (PTIT) of Vietnam. His research interests include electronics, telecommuni-cations, cryptography.