Hue University Journal of Science: Natural Science; ISSN 1859–1388

Vol. 127, No. 1A, 2018, P. 101–109; DOI: 10.26459/hueuni-jns.v127i1A.4746

A VARIANT OF THE RSA CRYPTOSYSTEM ON THE ENDOMORPHISM RING $End(\mathbb{Z}_n \times \mathbb{Z}_{n^k})$

Tran Dinh Long[1*], Le Thi Kim Nga[2]

[1] Department of Mathematics, University of Sciences, Hue University, 77 Nguyen Hue St., Hue, Vietnam
[2] Faculty of Information Technology, Ho Chi Minh City University of Education

Abstract. Based on the arithmetic of the endomorphisms ring End($\mathbb{Z}_p \times \mathbb{Z}_{p^k}$), the paper constructs an exponent type encryption and decryption cryptosystem. Although involving more operations in the encryption and decryption phases than those of the original RSA one, the cryptosystem has some advantages in avoiding lattice and chosen plaintext attacks compared to the original RSA cryptosystem.

Keywords: RSA cryptosystem, endomorphism ring, lattice, attack

1 Introduction

Constructed for the first time on the ring $\mathbb{Z}_n$ by Rivest, Shamir and Adleman in 1978 [1], RSA is a famous cryptosystem and has been widely used in various applications. Together with cryptanalysing on RSA, constructing variants of the RSA cryptosystem on platforms other than $\mathbb{Z}_n$ are the problems concerned by many authors. By convention, a cryptosystem is called an RSA variant if its encryption and decryption are an exponent type. The RSA variants on the quotient rings of Euclidean rings, such as the Gaussian integer ring or rings of polynomials having coefficients on finite fields [2], and the RSA variants on finite groups such as elliptic curve groups [3], or groups of non-singular matrices whose elements are on the finite fields [4], are examples of the RSA variants.

A way of constructing a new platform is considering the ring $End(G)$, where G is a given group. However, the arithmetic on that ring should be easy to handle so that we can perform operations on it. The ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ was first considered by Bergman [5] in 1974 and the isomorphism between this ring and the ring of 2×2 matrices was pointed out by Climent et.al [6] in 2011. With a similar method as in [6], Liu and Liu later established the isomorphism between the ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$ and a ring of 2×2 matrices whose elements in the first row and second row are in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^m}$, respectively [7]. The arithmetic of the endomorphism ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$, therefore, is easy to handle.

The aim of this paper is to construct an RSA cryptosystem on the subset $End(\mathbb{Z}_n \times \mathbb{Z}_{n^k})$, where n is the product of two distinct primes p and q. Section 2 presents some preliminaries of

* *Corresponding: trandinhlong1963@yahoo.com.vn*

Submitted: 10–4–2018; Revised: 8–7–2018; Accepted: 12–7–2018

the ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$ considered in [7], which are necessary for our work in the next section. In Section 3, our main results are constructing the platform for our RSA cryptosystem, establishing the equality $M^{ed} = M$ and finally proposing the cryptosystem together with an illustrated example. A comparison of some attacks to the original RSA cryptosystem will be mentioned in Section 4. This shows the disadvantages, as well as advantages, of our proposed cryptosystem.

2 Arithmetic of the ring-endomorphism $End(\mathbb{Z}_n \times \mathbb{Z}_{n^k})$

This section recalls some properties of the ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$, which are considered in [7], where p is a prime and k is a whole positive number. We emphasize that $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$ is a noncommutative ring with the usual componentwise addition and composition of endomorphisms.

Proposition 2.1 (Lemma 2.2 in [7]) *Let*

$$E_{p,p^k} = \left\{ \begin{pmatrix} a & b \\ p^{k-1}c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, 0 \le a, b, c < p, 0 \le d < p^k \right\}.$$

The set E_{p,p^k} is a ring where the addition is defined by

$$\begin{pmatrix} a_1 & b_1 \\ p^{k-1}c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ p^{k-1}c_2 & d_2 \end{pmatrix} = \begin{pmatrix} (a_1 + a_2) \bmod p & (b_1 + b_2) \bmod p \\ p^{k-1}(c_1 + c_2) \bmod p^k & (d_1 + d_2) \bmod p^k \end{pmatrix}$$

and the multiplication is defined by

$$\begin{pmatrix} a_1 & b_1 \\ p^{k-1}c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ p^{k-1}c_2 & d_2 \end{pmatrix} = \begin{pmatrix} (a_1 . a_2) \bmod p & (a_1 b_2 + b_1 d_2) \bmod p \\ p^{k-1}(c_1 a_2 + c_2 d_1) \bmod p^k & (p^{m-1} c_1 b_2 + d_1 d_2) \bmod p^k \end{pmatrix}.$$

The isomorphism between $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$ and E_{p,p^k}, then, pointed out by the following proposition.

Proposition 2.2 (Theorem 2.3 in [7]) *Define the map φ as follows*

$$\varphi : End(\mathbb{Z}_p \times \mathbb{Z}_{p^k}) \longrightarrow E_{p,p^k}$$

$$\alpha \longmapsto \varphi(\alpha) = \begin{pmatrix} a & b \\ p^{k-1}c & d \end{pmatrix}$$

where $\alpha(1,0) = (a, p^{k-1}c), \alpha(0,1) = (b, d)$ and $a, b, c, d \in \mathbb{Z}, 0 \le a, b, c < p, 0 \le d < p^k$. Then, φ is a ring isomorphism from $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$ to E_{p,p^k}.

Regarding the proposition above, the operations in $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$ are now easy to handle. Before mentioning the invertible elements in $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$, note that the element $d \in \mathbb{Z}, 0 \leq d < p^k$ can be expressed in the form

$$d = p^{k-1}u_{k-1} + p^{k-2}u_{k-2} + \cdots + pu_1 + u_0$$

where $u_{m-1}, u_{m-2}, \ldots, u_1, u_0 \in \mathbb{Z}, 0 \leq u_{k-1}, u_{k-2}, \ldots, u_1, u_0 < p$.

Proposition 2.3 (Theorem 3.6 in [7]) *Suppose that*

$$M = \begin{pmatrix} a & b \\ p^{k-1}c & d \end{pmatrix} = \begin{pmatrix} a & b \\ p^{k-1}c & p^{k-1}u_{k-1} + p^{k-2}u_{k-2} + \cdots + pu_1 + u_0 \end{pmatrix} \in E_{p,p^k}$$

where $a, b, c, u_{k-1}, u_{k-2}, \ldots, u_1, u_0 \in \mathbb{Z}, 0 \leq a, b, c, u_{k-1}, u_{k-2}, \ldots, u_1, u_0 < p$. *Then, M is invertible if and only if* $a \neq 0$ *and* $u_0 \neq 0$.

Since E_{p,p^m} is a ring, the set E^*_{p,p^m} of all invertible elements in E_{p,p^k} is a multiplicative group. The order of that group can be computed as follows:

Corrolary 2.1 (Corrolary 3.7 in [7]) The order of the group E^*_{p,p^k} is $\left|E^*_{p,p^k}\right| = (p-1)^2 p^{k+1}$.

3 The proposed cryptosystem

3.1 Constructing the platform

Suppose that p and q are two prime numbers, $n = pq$, and $k \geq 2$ is a whole number. We denote

$$E_{n,n^k} = \left\{ \begin{pmatrix} a & b \\ n^{k-1}c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, 0 \leq a, b, c < n, 0 \leq d < n^k \right\}.$$

For $x = \begin{pmatrix} a_1 & b_1 \\ n^{k-1}c_1 & d_1 \end{pmatrix} \in E_{n,n^k}$ and $y = \begin{pmatrix} a_2 & b_2 \\ n^{k-1}c_2 & d_2 \end{pmatrix} \in E_{n,n^k}$, we also define

$$x.y = \begin{pmatrix} (a_1.a_2) \bmod n & (a_1b_2 + b_1d_2) \bmod n \\ n^{k-1}(c_1a_2 + c_2d_1) \bmod n^k & (n^{k-1}c_1b_2 + d_1d_2) \bmod n^k \end{pmatrix}.$$

It is easy to check that the multiplication defined above is an associative binary operation on E_{n,n^k}.

In the case of group-platform, the equality $M^{ed} = M$ can be obtained using the Lagrange theorem. However, E_{n,n^k} is not a multiplicative group since there are many non-invertible elements on it. With the aim of reducing to multiplicative group of invertible elements in E_{n,n^k}, we define the map

$$\mu: E_{n,n^k} \longrightarrow E_{p,p^k}$$

$$\begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix} \mapsto \begin{pmatrix} a_p & b_p \\ p^{k-1}c_p & d_p \end{pmatrix}$$

where $a_p, b_p, c_p, d_p \in \mathbb{Z}, 0 \leq a_p, b_p, c_p < p, 0 \leq d_p < p^k, a \equiv a_p (\text{mod } p), b \equiv b_p (\text{mod } p), q^{k-1}c \equiv c_p (\text{mod } p)$

and $d \equiv d_p (\text{mod} p^k)$.

We also define the map

$$\eta: E_{n,n^k} \longrightarrow E_{q,q^k}$$

$$\begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix} \mapsto \begin{pmatrix} a_q & b_q \\ q^{k-1}c_q & d_q \end{pmatrix}$$

where $a_q, b_q, c_q, d_q \in \mathbb{Z}, 0 \leq a_q, b_q, c_q < q, 0 \leq d_q < q^k, a \equiv a_q (\text{mod } q), b \equiv b_q (\text{mod } q), p^{k-1}c \equiv c_q (\text{mod } q)$

and $d \equiv d_q (\text{mod} q^k)$.

It is easily seen that μ and η are well defined.

Proposition 3.1 μ and η are multiplicative monoid – homomorphisms.

Proof. For $= \begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix}, y = \begin{pmatrix} a' & b' \\ p^{k-1}q^{k-1}c' & d' \end{pmatrix} \in E_{n,n^k}$, we have

$$\mu(x) = \begin{pmatrix} a_p & b_p \\ p^{k-1}c_p & d_p \end{pmatrix},$$

$$\mu(y) = \begin{pmatrix} a'_p & b'_p \\ p^{k-1}c'_p & d'_p \end{pmatrix}$$

and

$$xy = \begin{pmatrix} aa' mod\ n & ab' + bd' mod\ n \\ p^{k-1}q^{k-1}(ca' + dc')\ mod\ n^k & p^{k-1}q^{k-1}cb' + dd' mod\ n^k \end{pmatrix},$$

where

$$a_p, b_p, c_p, d_p, a'_p, b'_p, c'_p, d'_p \in \mathbb{Z}, 0 \leq a_p, b_p, c_p, a'_p, b'_p, c'_p < p, 0 \leq d_p, d'_p < p^k, \quad (1)$$

and

$$a_p \equiv a(mod\ p), b_p \equiv b(mod\ p), c_p \equiv q^{k-1}c(mod\ p), d_p \equiv d(mod\ p^k), \quad (2)$$

$$a'_p \equiv a'(mod\ p), b'_p \equiv b'(mod\ p), c'_p \equiv q^{k-1}c'(mod\ p), d'_p \equiv d'(mod\ p^k). \quad (3)$$

From (1)–(3), we obtain

$$a_p a'_p \equiv aa'(mod\ p), a_p b'_p + b_p d'_p \equiv ab' + bd'(mod\ p), \quad (4)$$

$$c_p a'_p + d_p c'_p \equiv q^{k-1} ca' + dq^{k-1} c'(mod\ p), \quad (5)$$

and

$$c_p b'_p \equiv q^{k-1} cb'(mod\ p).$$

(6) and (5) imply that

$$p^{k-1}(c_p a'_p + d_p c'_p) \equiv p^{k-1}(q^{k-1} ca' + dq^{k-1} c')(mod\ p^k), \quad (6)$$

It is deduced from (6) that

$$p^{k-1} c_p b'_p \equiv p^{k-1} q^{k-1} cb'(mod\ p^k). \quad (7)$$

Combining (3) and (8) gives

$$p^{k-1} c_p b'_p + d_p d'_p \equiv p^{k-1} q^{k-1} cb' + dd'(mod\ p^k). \quad (8)$$

(4), (7) and (9) lead to the equality $\mu(xy) = \mu(x)\mu(y)$. Hence, μ is a homomorphism.

The same conclusion can be withdrawn for η.

Proposition 3.2 The map $\lambda: E_{n,n^k} \longrightarrow E_{p,p^k} \times E_{q,q^k}$

$$M \mapsto \lambda(M) = (\mu(M), \eta(M)$$

is an injection.

Proof.

Suppose that $x = \begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix}, y = \begin{pmatrix} a' & b' \\ p^{k-1}q^{k-1}c' & d' \end{pmatrix} \in E_{n,n^k}$ such that $\lambda(x) = \lambda(y)$.

By the definition of μ and η, we have

$$\mu(x) = \begin{pmatrix} a_p & b_p \\ p^{k-1}c_p & d_p \end{pmatrix}, \mu(y) = \begin{pmatrix} a'_p & b'_p \\ p^{k-1}c'_p & d'_p \end{pmatrix}$$

and

$$\eta(x) = \begin{pmatrix} a_q & b_q \\ q^{k-1}c_q & d_q \end{pmatrix}, \eta(y) = \begin{pmatrix} a'_q & b'_q \\ q^{k-1}c'_q & d'_q \end{pmatrix}$$

where

$$a_p, b_p, c_p, d_p, a'_p, b'_p, c'_p, d'_p \in \mathbb{Z}, 0 \le a_p, b_p, c_p, a'_p, b'_p, c'_p < p, 0 \le d_p, d'_p < p^k,$$

$$a_q, b_q, c_q, d_q, a'_q, b'_q, c'_q, d'_q \in \mathbb{Z}, 0 \le a_q, b_q, c_q, a'_q, b'_q, c'_q < q, 0 \le d_q, d'_q < q^k,$$

$$a_p \equiv a(mod\ p), b_p \equiv b(mod\ p), c_p \equiv q^{k-1}c(mod\ p), d_p \equiv d(mod\ p^k),$$

$$a'_p \equiv a'(mod\ p), b'_p \equiv b'(mod\ p), c'_p \equiv q^{k-1}c'(mod\ p), d'_p \equiv d'(mod\ p^k),$$

$$a_q \equiv a(mod\ q), b_q \equiv b(mod\ q), c_q \equiv p^{k-1}c(mod\ q), d_q \equiv d(mod\ q^k),$$

$$a'_q \equiv a'(mod\ q), b'_q \equiv b'(mod\ q), c'_q \equiv p^{k-1}c'(mod\ q), d'_q \equiv d'(mod\ q^k).$$

Since $\lambda(x) = \lambda(y)$, we have $\mu(x) = \mu(y)$ and $\eta(x) = \eta(y)$. This leads to

$$a_p = a'_p, b_p = b'_p, p^{k-1}c_p = p^{k-1}c'_p, d_p = d'_p,$$

and

$$a_q = a'_q, b_q = b'_q, q^{k-1}c_q = q^{k-1}c'_q, d_q = d'_q.$$

Since $a_p = a'_p$ and $a_q = a'_q$, we obtain $a = a'$. By the similar argument, $b = b'$.

Since $\begin{cases} p^{k-1}c_p = p^{k-1}c'_p(mod\ p^k) \\ q^{k-1}c_q = q^{k-1}c'_q(mod\ q^k) \end{cases}$, then $\begin{cases} c_p \equiv c'_p(mod\ p) \\ c_q \equiv c'_q(mod\ q) \end{cases}$. Hence, $c = c'$.

Since $\begin{cases} d_p = d'_p(mod\ p^k) \\ d_q = d'_q(mod\ q^k) \end{cases}$, then $d = d'$.

Therefore, $x = y$. This implies that λ is an injection. □

The equality $M^T = M$ plays a critical role in an RSA-cryptosystem. We will show this equality for a suitable integer T on a subset $S$of E_{n,n^k}. For this, we define

$$S = \left\{M \in E_{n,n^k} : \mu(M) \in E^*_{p,p^k}, \eta(M) \in E^*_{q,q^k}\right\}.$$

Note that $S \neq \emptyset$, for example, with $M = \begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix} \in E_{n,n^k}$ where $\gcd(a,n) = \gcd(d,n) = 1$, then $M \in S$ according to Proposition 2.3.

Proposition 3.3 If T is a whole number satisfying $T \equiv 1(\mathrm{mod}(p-1)^2p^{k+1})$ and $T \equiv 1(\mathrm{mod}(q-1)^2q^{k+1})$, then

$$M^T = M$$

for all

$$M \in S.$$

Proof.

Since $\mu(M)$ is an element of E^*_{p,p^k} which is a multiplicative group with the order of $(p-1)^2p^{k+1}$, the Lagrange theorem implies that $\mu(M)^T = \mu(M)$.

A similar argument shows that $\eta(M)^T = \eta(M)$.

Because λ is a homomorphism, we have $\lambda(M^T) = \lambda(M)^T$. This leads to

$$\lambda(M^T) = (\mu(M)^T, \eta(M)^T) = \big(\mu(M), \eta(M)\big) = \lambda(M).$$

Therefore, $M^T = M$ since λ is an injection.

3.2 The proposed cryptosystem

Key creation

- Choose distinct primes p, q and a positive integer m. Compute $n = pq$ and $L = \text{lcm}((p-1)^2 p^{k+1}, (q-1)^2 q^{k+1})$.
- Choose encryption exponent e with $\gcd(e, L) = 1$.
- Compute decryption exponent d satisfying $ed \equiv 1 (\text{mod } L)$.
- Publish n, m and e as a public key. Keep d as a private key.

Encryption

- Choose $a, d \in \mathbb{Z}, 1 \leq a < n, 1 \leq d < n^k$ such that $\gcd(a, n) = \gcd(d, n) = 1$.
- A plaintext $M = \begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix} \in S$ is encrypted by computing $C = M^e$, where $b, c \in \mathbb{Z}, 0 \leq b, c < n$.

Decryption

- A cipher text C is then decrypted by computing $C^d = M$.

To illustrate how the cryptosystem works, we consider the following example.

3.3 Example

For setting up the cryptosystem, we choose $p = 3, q = 5$ and $k = 3$. Then $n = pq = 15$ and

$$L = \text{lcm}((p-1)^2 p^{k+1}, (q-1)^2 q^{k+1}) = lcm(324, 10000) = 810000.$$

The value $e = 991$ satisfies the condition $\gcd(L, e) = 1$, d is the inverse for e in $\mathbb{Z}_L$ and it is easy to compute d: $d = 250111$.

Now, assume that Alice would like to send the message $m = 3$ to Bob. Then, Alice will choose the values a, c, d satisfying $\gcd(a, n) = \gcd(d, n) = 1$ to form the matrix $M = \begin{pmatrix} a & m \\ p^{k-1}q^{k-1}c & d \end{pmatrix}$.

If Alice chooses $a = 13$, $c = 7$ and $d = 8$, then $M = \begin{pmatrix} 13 & 3 \\ 1575 & 8 \end{pmatrix}$. Alice sends the cipher matrix $C = M^e = \begin{pmatrix} 7 & 12 \\ 2925 & 1142 \end{pmatrix}$ to Bob. Receiving C from Alice, Bob computes $C^d = \begin{pmatrix} 13 & 3 \\ 1575 & 8 \end{pmatrix}$ and recovers the message $m = 3$ at the 1st row and 2nd row of the result matrix.

If Alice chooses $a = 7, c = 7$ and $d = 4$, then = $\begin{pmatrix} 7 & 3 \\ 1575 & 4 \end{pmatrix}$, and the cipher text matrix is $C = M^e = \begin{pmatrix} 13 & 9 \\ 225 & 1354 \end{pmatrix}$.

The example shows that with the same message $m = 3$, the cipher matrix can have various forms depending on the chosen values of a, c and d. It also shows that two messages $m_1 = m = 3$ and $m_2 = c = 7$ can be wrapped in the matrix M.

4 Discussion

The encryption and decryption phases in our cryptosystem involve matrix multiplication, therefore our scheme involves more operations than that of the original RSA cryptosystem. We can overcome this disadvantage by including many real messages to the plaintext matrix $M = \begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix}$. Since d can be expressed in the form $d = d_0 + d_1 n + \cdots + d_{k-1}n^{k-1}$ where $d_i \in \mathbb{Z}, 0 \le d_i < n$, the plaintext M now contains k+1 messages $b, c, d_1, d_2, \ldots, d_{k-1}$.

Compared to the cryptosystem considered in [4], in which a plaintext is also a matrix, the sender must check the non-singularity of the plaintext matrix. In our scheme, the sender does not face the similar problem but has to choose a, d satisfying $\gcd(a, n) = \gcd(d, n) = 1$. These conditions do not leak any information of p and q.

For real messages b and c, we can choose various values a and d to form the plaintext $M = \begin{pmatrix} a & b \\ p^{k-1}q^{k-1}c & d \end{pmatrix}$. It leads to the cipher text $C = M^e$ that can have many different values. This makes our cryptosystem avoid chosen-plaintext attacks or plaintext checking attack.

The two-dimension lattice is an effective tool for attacking in the original RSA cryptosystem having a small secret exponent [8]. This type of attacking can be applied to our cryptosystem as follows. Because p and q are balanced to avoid factoring modulus attack, then $\varphi(n) = n + u$; where $u = 1 - p - q = O(\sqrt{n})$. This leads to $L = \text{lcm}((p-1)^2 p^{k+1}, (q-1)^2 q^{k+1}) = p^{k+1}q^{k+1} lcm((p-1)^2, (q-1)^2) < n^{k+2}\varphi(n)$. The equation $ed \equiv 1 (\text{mod } L)$ implies that there exists an integer $h = O(d)$ such that $ed = 1 + hL < hn^{k+2}\varphi(n) = hn^{k+2}(n + u)$. Hence, $ed - hn^{m+3} < n^{k+2}ku$. Denote $l = ed - hn^{k+3}$, then $l = O(dn^{k+2}\sqrt{n})$. Consider the two-dimensional lattice H in $\mathbb{R}^2$ spanned by two vectors $v_1 = (e, n^{k+2}\sqrt{n})$ and $v_2 = (n^{k+3}, 0)$. H contains the

vector $t = de_1 - he_2 = (ed - kn^{k+3}, dn^{k+2}\sqrt{n})$ whose norm is $\|t\| \approx dn^{k+2}\sqrt{n}$. Since $vol(H)^{\frac{1}{2}} = \sqrt{n^{2k+5}\sqrt{n}} = n^{\frac{4k+11}{4}}$, t could be the shortest vector in H being a reasonable guess if $dn^{k+2}\sqrt{n} < n^{\frac{4k+11}{4}}$ or $d < n^{\frac{1}{4}}$. In this case, we can apply the Gaussian algorithm to H for finding t and then recover the private key d. In the original RSA, the range of d is from 1 to $(p-1)(q-1)-1$, in which the range $1 < d < n^{\frac{1}{4}}$ is regarded as a weak key case for the two-dimension lattice attack. Thus, the probability to succeed the two-dimension lattice attack in the original RSA is $\frac{n^{\frac{1}{4}}}{(p-1)(q-1)} \approx \frac{1}{n^{\frac{3}{4}}}$. In our scheme, the range of d is from 1 to $L = \text{lcm}((p-1)^2p^{k+1}, (q-1)^2q^{k+1}) > n^{k+1}$, and therefore, the probability to succeed two-dimension lattice attack is $\frac{n^{\frac{1}{4}}}{L} < \frac{n^{\frac{1}{4}}}{n^{k+1}} = \frac{1}{n^{k+\frac{3}{4}}}$.

5 Conclusion

A new variant of RSA on the platform $\text{End}(\mathbb{Z}_n \times \mathbb{Z}_{n^k})$ has been proposed. Some disadvantages, as well as advantages of the cryptosystem in comparison to the original RSA, are also considered. We will mention the implementation of the cryptosystem in another paper. As for future work, we plan to consider the arithmetic of the ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^k})$ and to establish a variant of RSA on this platform.

References

1. R. L. Rivest, A. Shamir, and L. M. Adleman (1978), A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM 21*, no. 2, 120–126.
2. El-Kassar A.N., R. Haraty and Y. Awad (2004), Modified RSA in the Domains of Gaussian Integers and Polynomials over Finite Fields,*Proc. Intl. Conf. Computer Science*, *Software Engineering*, *Information technology*, *e-Business and Applications (CSITeA'04)*. Cairo, Egypt.
3. N. Demytko (1994), A new elliptic curve based analogue of RSA, *Advances in Cryptology-EUROCRYPT'93*, *LNCS 765*, 40–49.
4. V. Varadharajan and R. Odoni (1985), Extension of RSA cryptosystem to matrix rings, *Cryptologia*, Volume 9, Number 2.
5. Bergman G.M., Examples in PI ring theory (1974), *Israel J. Math.* 18, 257–277.
6. J.J. Climent, P.R. Navarro and L.Tortosa (2011), On the arithmetic of the endomorphismsring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, *AAECC*.
7. X. Liu and H. Liu (2016), On the arithmetic of the endomorphism ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^m})$, *arXiv*:1605.00805.
8. Phong Q. Nguyen (2008), Public Key Cryptanalysis, *Recent Trends in Cryptography*, *Contemporary Mathematics series*, AMS-RSME.