Copyright ⓒ2016 KSII

RSA-type Algebra Structures

Long D. Tran[1], Thu D. Tran[2], Deokjai Choi[3] and Thuc D. Nguyen[2]
[1]Hue University of Science
77 Nguyen Hue, Hue, Vietnam
[email: trandinhlong1963@yahoo.com.vn]
[2] University of Science
227 Nguyen Van Cu, District 5, HCMC, Vietnam
[email: tdthu@fit.hcmus.edu.vn, ndthuc@fit.hcmus.edu.vn]
[3] School of Electrical and Computer Engineering, Chonnam National University
77 Yongbong-ro, Buk-gu, Gwangju 500-757, Korea
[e-mail: dchoi@jnu.ac.kr]
*Corresponding author: Deokjai Choi

Received April 23, 2015; revised July 17, 2015; revised January 16, 2016; accepted April 7, 2016; published June 30, 2016

Abstract

RSA is a public key cryptosystem that is currently the most popularly used in information security. Development of RSA variants has attracted many researchers since its introduction in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman. In this paper, we propose an algebraic structure for RSA and show that the proposed structure covers all known RSA variants. The usefulness of the proposed structure is then proved by showing that, following the structure we can construct a RSA variant based on the Bergman ring. We compare the original RSA and its variants from the point of view of factoring the modulus to determine why the original RSA is widely used than its variants.

Keywords: Cryptography, RSA cryptosystem, semigroup, ring.

This work was supported by the Funding VNU-HCMC, Vietnam (B2012-18-02TĐ, Design and Implementation of FPGA-cryptography IP Cores). This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2012R1A1A2007014)

http://dx.doi.org/10.3837/tiis.2016.06.021 **ISSN : 1976-7277**

1. Introduction

The RSA cryptosystem, named after its inventors Ron Rivest, Adi Shamir, and Len Adleman, was introduced in 1978 and has been widely used for ensuring the privacy and authenticity of digital data. Since then, there has been concentration on two trends considering the RSA cryptosystem: (i) point out vulnerabilities of the cryptosystem, and (ii) develop its variants. Although there have been many variants of the RSA, cryptanalysis on those has not attracted many researchers as compared to the original RSA. We recall some remarkable results in cryptanalysing on low private exponent RSA in Section 2 after recalling the original RSA cryptosystem. In Section 3, we give an answer for the question why RSA variants are built on platform other than $\mathbb{Z}_n$. Section IV devotes for an algebraic structure of RSA, we also show in this Section all known RSA cryptosystems having this algebraic structure. The usefulness of the structure is then made clear in Section V, where we recall the construction of Bergman ring based RSA. A slight comparison between known RSAs in Section 4 can help answer the question why the original RSA is preferred over its variants.

2. RSA and cryptanalysis on the RSA cryptosystem

2.1. The original RSA cryptosystem

For the convenience of the reader, we briefly describe the original RSA cryptosystem in the form of a theorem. The proof of this theorem and its working can be found in [1].

Theorem 2.1 *Given p and q as two distinct primes. Let $n = pq$, $\varphi(n) = (p-1)(q-1)$, and e, d be two integers such that $ed \equiv 1\big(\bmod \varphi(n)\big)$. Then, for all $m \in \mathbb{Z}_n$, we have $m^{ed} \equiv m \pmod n$.*

This theorem ensures the encryption and decryption phases in the RSA cryptosystem as follows: a plaintext $m \in \mathbb{Z}_n$ is encrypted by computing $m^e \equiv c(\bmod n)$ and c is in turn decrypted by calculating $c^d \equiv m(\bmod n)$.

2.2. Attacks on RSA

Although there has been no polynomial time algorithm for factoring an integer n into product of primes so far, there have been many attacks on the original RSA scheme. By considering the continued fraction expansion of $\frac{e}{n}$, Wiener showed in [2] that one can recover d for the case when $d < \frac{1}{3} n^{\frac{1}{4}}$. A better result was considered by Boneh and Durfee [3] for the case when $d < n^{0.292}$. In such a case, by solving the small inverse problem, d can be recovered. Lattice reduced algorithms, such as Gaussian or LLL algorithms can also be applied to recover d in some cases of low exponent private key [4]. However, so far, no devastating attack has ever been found.

A common attack on RSA is factoring the modulus n. Knowing $n = pq$, an attacker can calculate $\varphi(n) = (p-1)(q-1)$ and then find the private key $d = e^{-1}(\mathrm{mod}\ \varphi(n))$. Factoring modulus n in the case p, q being weak primes was considered by A. Nitaj and T. Rachidi [5]. Currently, the fastest algorithm for the factoring a whole number n is the General Number Field Sieve algorithm [6], which has a complexity of $exp\left(\left(\sqrt[3]{\frac{64}{9}} + O(1)\right)(\ln n)^{\frac{1}{3}}(\ln \ln n)^{\frac{2}{3}}\right)$.

3. RSA variants

If n is a positive integer and $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where $p_1, p_2, \dots, p_k$ are distinct prime numbers and $r_i \in \mathbb{Z}$ $(i = 1,2,\dots,k)$, then we denote $\mathrm{rad}(n) = p_1 p_2 \dots p_k$. Apparently, the original RSA scheme still holds when $n = \mathrm{rad}(n)$[7]. We first prove that $n = \mathrm{rad}(n)$ is the only form of n under that an RSA encryption scheme can be applied to all messages belonging to $\mathbb{Z}_n$.

Proposition 3.1 *Suppose that there exists a natural number* $k \neq 1$ *such that the map*

$$F: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$x \longmapsto x^k$$

is a bijection. Then, $n = \mathrm{rad}(n)$.

Proof.

Suppose that $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$where $p_1, p_2, \dots, p_k$ are distinct prime numbers and assume the contrary that $n \neq \mathrm{rad}(n)$, then at least one of $r_1, r_2, \dots, r_k$ is larger than 1. Without loss of generality, we can assume $r_1 > 1$. Considering $x = p_1^{r_1 - 1} p_2^{r_2} \dots p_k^{r_k} \in \mathbb{Z}_n$, it is obvious that $x \neq 0$. Since $k \geq 2$, then $k(r_1 - 1) > r_1$. It follows that $F(x) = x^k = 0$, which contradicts the bijection of F.

Proposition 3.1 explains the reason for the two trends in developing RSA variants. For the first trend, the RSA cryptosystems are developed on the ring $\mathbb{Z}_n$. For RSA cryptosystems where the modulus n is the product of distinct primes, some additional algorithms are applied to speed up the decryption or encryption process in the cryptosystem. The Batch RSA [8], Multi Prime RSA [7], DRSA [9] are examples of such cryptosystems. For RSA cryptosystems where the modulus n is not a product of distinct primes, the space of plaintexts must be reduced to a subset of $\mathbb{Z}_n$ instead of the entire $\mathbb{Z}_n$. For example, in the MultiPower RSA cryptosystem [10], the modulus n

has the form $n = p^k q$ with $k \in \mathbb{Z}, k \geq 2$, where p, q are distinct primes and the space of plaintexts is the reduced residue group modulo n. This RSA variant was then combined with DRSA to increase the encryption verification performance [11-12]. Attacking to these RSA variants has been concerned by many authors, we refer the reader to [13-14] for cryptanalysing on MultiPower RSA.

In the second trend, platforms other than $\mathbb{Z}_n$ should be chosen for plaintexts. So far, there have been many variants of RSA constructed in this manner: In 1985, Varadharajan and Odoni constructed an extension of RSA to matrix rings [15]; In 1993, Demytko, proposed an elliptic curve-based RSA variant at EUROCRYPT [16]; In 2004, El-Kassar, Hatary, and Awad developed a modified RSA in the domains of Gaussian integers and polynomials over finite fields [17]. The critical equality $m^{ed} = m$ in those cryptosystems was obtained using different methods depending on the platforms. Here, we concentrate on an abstract model by proposing a semigroup platform together with conditions that ensure equality and then show that the model will cover all mentioned RSA cryptosystems.

From now on, if $*$ is a binary operation on a set X, k is a positive integer, and $x \in X$, then we denote $\underbrace{x * x * \ldots * x}_{k\ times}$ by $(*_k)x$.

4. Generic RSA scheme

4.1 A generic model for RSA

Let Y be a nonempty set and * be a binary operation on Y such that $(Y,*)$ is a semigroup, and suppose that $X \subset Y$ is a set of plaintexts. The equation $m^{ed} = m$ for all $m \in X$ is a basic equation in RSA cryptosystems. We propose some conditions for establishing this equation as follows.

Proposition 4.1 Let Y, U, V be multiplicative semigroups, X be a nonempty subset of Y, and $\mu: Y \longrightarrow U, \eta: Y \longrightarrow V$ be two homomorphisms. Suppose that

(i) There exist groups $U_1 \subset U, U_2 \subset U$ and $V_1 \subset V, V_2 \subset V$ such that $\mu(X) \subset (U_1 \cup U_2)$ and $\eta(X) \subset (V_1 \cup V_2)$.

(ii) The map $\theta: Y \longrightarrow U \times V$ defined by $\theta(x) = (\mu(x), \eta(x))$ is an injective.

Let $N_i = |U_i|, M_i = |V_i| (i = 1,2)$, $L = \operatorname{lcm}(N_1, N_2, M_1, M_2)$, and e, d be two chosen integers such that $\gcd(e, L) = 1$ and $ed \equiv 1 (\operatorname{mod} L)$. Then, we have $x^{ed} = x$ for all $x \in X$.

Proof. Assume that $x \in X$.

For $x \in X$, since $\mu(X) \subset (U_1 \cup U_2)$ and U_1, U_2 are groups, then $(\mu(x))^i = \mu(x)$ for all integers i satisfying $i \equiv 1(\operatorname{mod} \operatorname{lcm}(N_1, N_2))$. This implies that $(\mu(x))^{ed} = \mu(x)$. As μ is a homomorphism, $\mu(x^{ed}) = (\mu(x))^{ed} = \mu(x)$.

Similarly, we have $(\eta(x))^{ed} = \eta(x)$.

Since $\mu(x^{ed}) = \mu(x)$ and $\eta(x^{ed}) = \eta(x)$, then $\theta(x^{ed}) = \theta(x)$. Therefore, $x^{ed} = x$ as θ is an injective.■

Using the symbols and hypothesis as in the above theorem, we propose a generic model for an RSA cryptosystem as follows.

The generic RSA cryptosystem

Key creation

- Choose e satisfying $1 < e < L$ and $\gcd(e, L) = 1$.

- Find $d = e^{-1}(\operatorname{mod} L)$.

- Publish e as public key and keep d as private key.

Encryption

- A plaintext $m \in X$ is encrypted by calculating $c = m^e$.

Decryption

- Ciphertext c is then decrypted by calculating $c^d = m$.

From now on, if Y is a ring and $x \in Y$, we write $\langle x \rangle$ for the ideal of Y generated by x and write $Y/\langle x \rangle$ for the quotient ring of Y by $\langle x \rangle$. Next, we show that our proposed model can cover all known RSA variants.

4.2 The original RSA

Consider the ring $Y = \mathbb{Z}_n$, where $n = pq$ is the product of two distinct primes p, q and $X = Y$. Since the ring isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$, the projectors μ, η from Y to $U = \mathbb{Z}_p$ and $V = \mathbb{Z}_q$ satisfy the hypothesis in Proposition 4.1. Therefore, the equation $m^{ed} = m$ holds for all $m \in X = \mathbb{Z}_n$, where e, d are integers that satisfy $ed \equiv 1(\operatorname{mod} L)$. In this case, we choose

$U_1 = \{0\}, U_2 = \mathbb{Z}_p \backslash \{0\}, V_1 = \{0\}, V_2 = \mathbb{Z}_q \backslash \{0\},$

then

$N_1 = |U_1| = 1, N_2 = |U_2| = p - 1,$

$M_1 = |V_1| = 1, M_2 = |V_2| = q - 1,$

$L = lcm(p - 1, q - 1).$

We achieve the original RSA cryptosystem.

4.3 The RSA on the quotient rings of polynomials

The ring of polynomials $\mathbb{Z}_p[x]$ is considered in this instance, where p is a prime number. Similar to the original RSA, let $g(x), h(x) \in \mathbb{Z}_p[x]$ be irreducible polynomials having degree r, s and $f(x) = g(x).h(x)$. Consequently, the number of invertible elements in $\mathbb{Z}_p[x]/\langle g(x)\rangle, \mathbb{Z}_p[x]/\langle h(x)\rangle$ and $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is $p^r - 1, p^s - 1$ and $L = (p^r - 1)(\,p^s - 1)$, respectively. Therefore, $m(x)^{ed} = m(x)$ holds for all $m(x) \in \mathbb{Z}_p[x]/\langle f(x)\rangle$, where e, d are integers chosen such that $\gcd(e, L) = 1$ and $ed \equiv 1(\mathrm{mod}\ L)$. The equation $m(x)^{ed} = m(x)$ ensures the encryption $c(x) = (m(x))^e$ and decryption $(c(x))^d = m(x)$. The RSA on the quotient rings of polynomials can be regarded as an instance of the proposed model mentioned in Section 4.1 where

$Y = X = \mathbb{Z}_p[x]/\langle f(x)\rangle,$

$U = \mathbb{Z}_p[x]/\langle g(x)\rangle, V = \mathbb{Z}_p[x]/\langle h(x)\rangle,$

$U_1 = \{0\}, U_2 = U\backslash U_1, V_1 = \{0\}, V_2 = V\backslash V_1.$

$N_1 = |U_1| = 1, N_2 = |U_2| = p^r - 1,$

$M_1 = |V_1| = 1, M_2 = |V_2| = p^s - 1,$

and μ, η are projectors from $\mathbb{Z}_p[x]/\langle f(x)\rangle$ onto $\mathbb{Z}_p[x]/\langle g(x)\rangle, \mathbb{Z}_p[x]/\langle h(x)\rangle$ respectively.

4.4 The RSA on the quotient ring of Gaussian integers

The Gaussian ring is defined by $\mathbb{Z}[i] = \{a + bi: a, b \in \mathbb{Z}\}$ with common addition and multiplication. The norm on $\mathbb{Z}[i]$ is given by $\delta(a + bi) = a^2 + b^2$. Euclidean division is valid on $\mathbb{Z}[i]$; hence, $\mathbb{Z}[i]$ is an Euclidean ring. All units in $\mathbb{Z}[i]$ are $1, -1, i, -i$. Euclidean division gives rise to the concept of primes in $\mathbb{Z}[i]$. A number $x \in \mathbb{Z}[i]$ is prime in $\mathbb{Z}[i]$ if and only if x is a unit multiplied by one of the following:

(i) $1 + i,$

(ii) a prime number $p \in \mathbb{Z}$, where $p \equiv 3(\mathrm{mod}\ 4)$, or

(iii) $u + vi \in \mathbb{Z}[i]$, where $q = u^2 + v^2$ is a prime in $\mathbb{Z}$ with $q \equiv 1(\mathrm{mod}\ 4)$.

A prime $x \in \mathbb{Z}[i]$ is called type α, type p, or type π corresponding to cases (i), (ii), and (iii), respectively.

The Euler's Phi function $\Phi\colon \mathbb{Z}[i]\backslash\{0\} \longrightarrow \mathbb{N}$ is a function in which for all $x \in \mathbb{Z}[i]\backslash\{0\}$, $\Phi(\mathrm{x})$ is the number of invertible elements in the quotient ring $\mathbb{Z}[i]/\langle x\rangle$. Then, for prime element $x \in \mathbb{Z}[i]$, we have $\Phi(\mathrm{x}) = \delta(\mathrm{x})$ [18].

Let β, γ be two prime elements in $\mathbb{Z}[i]$ and $\eta = \beta.\gamma$, then $\Phi(\eta) = \Phi(\beta).\Phi(\gamma)$. The equation $m^{ed} = m$ holds for all $m \in \mathbb{Z}[i]/\langle\eta\rangle$, where e, d are integers chosen such that $\gcd\big(e, \Phi(\eta)\big) = 1$ and $ed \equiv 1(\mathrm{mod}\ \Phi(\eta))$. This ensures the encryption $c = m^e$ and decryption $c^d = m$ for all plaintext $m \in \mathbb{Z}[i]/\langle\eta\rangle$.

The RSA on the quotient ring of Gaussian integers can be regarded as an instance of the proposed model described in Section 4.1 where

$$Y = X = \mathbb{Z}[i]/\langle\eta\rangle, U = \mathbb{Z}[i]/\langle\beta\rangle, V = \mathbb{Z}[i]/\langle\gamma\rangle,$$

$$U_1 = \{0\}, U_2 = U\backslash U_1, V_1 = \{0\}, V_2 = V\backslash V_1,$$

$$N_1 = |U_1| = 1, N_2 = |U_2| = \Phi(\beta),$$

$$M_1 = |V_1| = 1, M_2 = |V_2| = \Phi(\gamma),$$

$$L = \mathrm{lcm}(\Phi(\beta).\Phi(\gamma),$$

and μ, η are projectors from $Y = \mathbb{Z}[i]/\langle\eta\rangle$ to $U = \mathbb{Z}[i]/\langle\beta\rangle$ and $V = \mathbb{Z}[i]/\langle\gamma\rangle$, respectively.

4.5 The RSA on the ring of matrices

Let p, q be two prime numbers, $n = pq$, and l be a positive integer. Let $M_l(p), M_l(q)$, and $M_l(n)$ denote the multiplicative groups of all non-singular $l \times l$ matrices having elements in $\mathbb{Z}_{p,}\mathbb{Z}_q$, and $\mathbb{Z}_n$, respectively. The orders $N_{p,}N_q$, and N_n of these groups can be shown by

$$N_p = \left(p^l - 1\right)\left(p^l - p\right) \dots \left(p^l - p^{l-1}\right), \tag{1}$$

$$N_q = \left(q^l - 1\right)\left(q^l - q\right) \dots \left(q^l - q^{l-1}\right), \tag{2}$$

and

$$N_n = N_p N_q, \tag{3}$$

respectively.

Choose two positive integers e, d satisfying $\gcd(e, N_n) = 1$ and $ed \equiv 1(\mathrm{mod}\ N_n)$. The Lagrange theorem in group theorem implies that $m^{N_n} = I_n$, where I_n denotes the unit matrix in $M_l(n)$; hence, $m^{ed} = m$ for all $m \in M_l(n)$. This ensures the encryption $c = m^e$ and decryption $c^d = m$ for all plaintext $m \in M_l(n)$. Since $M_l(n) \cong M_l(p) \times M_l(q)$, the RSA variant on the ring of matrices is an instance of the model described in Section 3.1 where

$Y = X = M_l(n), U = M_l(p), V = M_l(q),$

$U_1 = \{I_p\}, U_2 = M_l(p), V_1 = \{I_q\}, V_2 = M_l(q),$

$N_1 = |U_1| = 1, N_2 = |U_2| = N_p,$

$M_1 = |V_1| = 1, M_2 = |V_2| = N_q,$

and $\mu, \eta$are projectors from $M_l(n)$ to $M_l(p)$ and $M_l(q)$, respectively.

4.6 The RSA on the elliptic curve group

Let $p > 3$ be a prime, and let a, b be integers chosen such that $4a^3 + 27b^2 \not\equiv 0(\mathrm{mod}\, p)$. The elliptic curve group modulo p, denoted by $E_p(a, b)$, is a set of all pairs $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfying $y^2 = x^3 + ax + b$ on $\mathbb{Z}_p$, together with an element denoted ∞. The operation $+$ on $E_p(a, b)$ is defined such that ∞ is the identity element and for two points $P(x_1, y_1), Q(x_2, y_2) \in E_p(a, b)$, the result $R(x_3, y_3) = P + Q$ is determined as follows:

-If $Q = \infty$, then $P + Q = Q + P = P$.

-If $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q = \infty$.

-Otherwise, $\begin{cases} x_3 = \lambda^2 - x_1 - x_1, \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases}$ where

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } x_1 \neq x_2, \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2 \text{ and } y_1 \neq -y_2. \end{cases}$$

A complementary elliptic curve group, denoted by $\overline{E_p(a, b)}$, is a set of all pairs $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfying $y^2 = x^3 + ax + b$, together with an element denoted ∞; however, y is of the form $y = u\sqrt{v}$, where $u, v \in \mathbb{Z}_p$ and v is a fixed quadratic non-residue. The operation $+$ on $\overline{E_p(a, b)}$ is identically defined to that on $E_p(a, b)$. The orders of $E_p(a, b)$ and $\overline{E_p(a, b)}$ are denoted by $|E_p(a, b)|$ and $|\overline{E_p(a, b)}|$, respectively. These numbers can be found by some polynomial time algorithms, for example, the algorithm considered in [19].

For RSA on the elliptic group, we choose two distinct primes p, q and let $n = pq$. Select two integers a, b such that $\gcd(4a^3 + 27b^2, n) = 1$. Denote $N_1 = |E_p(a, b)|$, $N_2 = |\overline{E_p(a, b)}|, M_1 = |E_q(a, b)|, M_2 = |\overline{E_q(a, b)}|$, and $L = N_1 N_2 M_1 M_2$.

Choose two integers e, d such that $ed \equiv 1(\bmod L)$, then the equation $(+_{ed})(x, y) = (x, y)$ holds for all $x \in \mathbb{Z}_n$ and $y = \sqrt{x^3 + ax + b}$. This equation ensures the encryption and decryption as in the original RSA.

We can apply the proposed model to this instance of RSA. Indeed, suppose that v_p and v_q are generators of multiplicative groups $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$, respectively. Then, $\overline{E_p(a, b)} = \{u\sqrt{v_p} : u \in \mathbb{Z}_p\}$ and $\overline{E_q(a, b)} = \{u\sqrt{v_q} : u \in \mathbb{Z}_q\}$ are complementary elliptic groups of $E_p(a, b)$ and $E_q(a, b)$, respectively. Denote by $w_1, w_2,$ and w_3 elements in $\mathbb{Z}_n$ such that

$$w_1 \equiv 1(\bmod p), w_1 \equiv v_q(\bmod q),$$

$$w_2 \equiv v_p(\bmod p), w_1 \equiv 1(\bmod q),$$

and

$$w_3 \equiv v_p(\bmod p), w_1 \equiv v_q(\bmod q).$$

Then, for each $x \in \mathbb{Z}_n$, one and only one of the following cases occurs:

$$x^3 + ax + b = t^2,$$

$$x^3 + ax + b = t^2 w_1,$$

$$x^3 + ax + b = t^2 w_2,$$

$$x^3 + ax + b = t^2 w_3.$$

Therefore, if we define

$$E_n^{11} = \{(x, y): x \in \mathbb{Z}_n, y \in \mathbb{Z}_n: x^3 + ax + b = y^2\},$$

$$E_n^{12} = \{(x, y): x \in \mathbb{Z}_n, y = t\sqrt{w_1}, x^3 + ax + b = y^2\},$$

$$E_n^{21} = \{(x, y): x \in \mathbb{Z}_n, y = t\sqrt{w_2}, x^3 + ax + b = y^2\},$$

$$E_n^{22} = \{(x, y): x \in \mathbb{Z}_n, y = t\sqrt{w_3}, x^3 + ax + b = y^2\},$$

then for each $x \in \mathbb{Z}_n$, there exists exactly one of the above sets containing an element with the first coordinate x.

It is well known that we can define a operation $+$ on $E_n(a, b) = E_n^{11}$ and$E_n(a, b) \cong E_p(a, b) \times E_q(a, b)$. Therefore, two projectors $\mu: E_n^{11} \to E_p(a, b)$ and $\eta: E_n^{11} \to E_q(a, b)$ are homomorphisms. Proposition 3.2 ensures that $(+_{ed})(x, y) = (x, y)$ for all $(x, y) \in E_n^{11}$, where e, d are integers satisfying $ed \equiv 1(\bmod L_{11})$ with $L_{11} = \text{lcm}(N_1, M_1)$.

Similar to the operation $+$ on $E_n(a,b) = E_n^{11}$, we can define a binary operations $+$ on E_n^{12}, E_n^{21}, and E_n^{22} such that these sets become groups and

$$E_n^{12} \cong E_p(a,b) \times \overline{E_q(a,b)},$$

$$E_n^{21} \cong \overline{E_p(a,b)} \times E_q(a,b),$$

$$E_n^{22} \cong \overline{E_p(a,b)} \times \overline{E_q(a,b)}.$$

Proposition 4.1 ensures the equation $(+_{ed})(x,y) = (x,y)$ for all $(x,y) \in E_n^{ij}(i,j = 1,2)$ if e,d satisfy $ed \equiv 1(\text{mod } L_{ij})$ with $L_{ij} = lcm(N_i, M_j)$. In other words, the proposed model is applied to each group $E_n^{ij}(i,j = 1,2)$ separately.

Because the operators $+$ on $E_n^{ij}(i,j = 1,2)$ are defined in a similar way, the first coordinates x_k in the equation $(x_k, y_k) = (+_k)(x,y)$ are the same, and they do not depend on i,j, where $(x,y) \in E_n^{ij}$. Demytko [16] gave a formula for x_k by setting $x_i = \frac{X_i}{Z_i}, y = \frac{Y_i}{Z_i}$ in homogenous coordinates:

$$X_{2i} = (X_i^2 - aZ_i^2)^2 - 8bX_iZ_i^3(\text{mod } n), \quad (4)$$

$$Z_{2i} = 4Z_i\left(X_i^3 + aX_iZ_i^2 + bZ_i^3\right)(\text{mod } n), \quad (5)$$

$$X_{2i+1} = 4bZZ_i^2Z_{i+1}^2 + 2Z(aZ_iZ_{i+1} + X_iX_{i+1})(X_iZ_{i+1} + X_{i+1}Z_i) - X(X_iZ_{i+1} - X_{i+1}Z_i)^2 \ (\text{mod } n), \quad (6)$$

$$Z_{2i+1} = Z(X_iZ_{i+1} - X_{i+1}Z_i)^2(\text{mod } n), \quad (7)$$

$$x_i = \frac{X_i}{Z_i}. \quad (8)$$

4.7 Comparison

Since there are many time polynomial algorithms (e.g., Berlekamp [20], Ben-Or [21], and Cantor–Zassenhaus [22]) for factoring a polynomial $f(x) \in \mathbb{Z}_p[x]$ into the product of irreducible polynomials, the RSA cryptosystem on the quotient ring of polynomials can be easily broken using these algorithms.

We compare the security among RSAs by evaluating the complexity of the brute-force algorithm for factoring the modulus n. For simplicity, we assume that the length of each plaintext is 1024 bits.

Table 1 shows the lengths of modulus as well as the number of operations involved in encryption processes in original RSA and those in its variants, where e is the public key.

Table 1. Lengths of modulus and number of operations involved in RSAs cryptosystem

	Length of the modulus	Least number of operations
Original RSA	1024	$log_2 e$
RSA on the quotient ring of Gauss integers	512	$6log_2 e$
RSA on the group of matrix	256	$12log_2 e$
RSAon the elliptic curve group	1024	$5log_2 e$
Bergman ring based RSA	256	$12log_2 e$

For the original RSA cryptosystem, because a plaintext $m \in \mathbb{Z}_n$ has a length of 1024 bits, the modulus n must have the same length as m. Therefore, the algorithm for factoring n is applied for a 1024-bit number n.

For the RSA cryptosystem on the quotient ring of Gaussian integers, a plaintext $m = a + bi$ has a length of 1024 bits, and therefore, both a and b have a length of 512 bits. Thus, the length of the value $\delta(m) = a^2 + b^2$ does not exceed 1025 bits. Because $m \in \mathbb{Z}[i]/\langle\eta\rangle$, $\delta(\eta)$ must have a length less than 1025 bits. Hence, the length of modulus η is 512 bits. Factoring a 512-bit number η may be simpler than the case for the original RSA.

For the RSA on the ring of matrix, one can determine p, q by factoring n. Hence, we calculate N_p, N_q by (1), (2), respectively, and then N_n by (3). Then, the private key d can be calculated from these values. Suppose that $l \geq 2,$ then a plaintext $m \in M_l(n)$ is a matrix having at least four elements. Because m has a length of 1024 bits, each of its four elements must be 256 bits. Since each element belongs to $\mathbb{Z}_n$, n must be 256 bits. Factoring n in this case is simpler than that in the original RSA.

In both the original RSA and the RSA on the elliptic curve group, each plaintext element $x \in \mathbb{Z}_n$has the same bit length as modulus n. However, the encryption and decryption in RSA on the elliptic curve group requires more operations than those in the original RSA. In the original RSA, encrypting $c \equiv m^e (\text{mod}\, n)$ requires $2\log_2 e$ multiplications using a fast power algorithm. The numbers of operations in (4), (5), (6), and (7) are 11, 12, 21, and 5, respectively. Therefore, for the RSA on the elliptic curve group, the number of operations for encrypting a plaintext x to cipher text s using the equation $(+_e)(x, y) = (s, t)$ requires at least $5\log_2 e$ multiplications.

In our cryptosystem mentioned in the next Section, a plaintext m is a matrix having four elements. Because m has a length of 1024 bits, each of its four elements must be 256 bits. Since each element belongs to $\mathbb{Z}_n$, n must be 256 bits. Factoring n in this case is simpler than that in the original RSA.

The above argument shows that, for the same length of the modulus, the lengths of plaintexts and cipher texts in original RSA cryptosystems are shorter than those in its variants. This partially explains why the original RSA cryptosystem is more widely used compared to other RSA variants.

5. A new variant of RSA: probability RSA

Based on the proposed scheme, we developed a Bergman ring based cryptosystem analogue of RSA. We briefly describe this cryptosystem as follows.

Bergman [23] established that $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a semilocal ring with p^5 elements, where p is a prime. Climent et al. [24] identified the elements of this ring as 2×2 matrices that form the ring

$$E_p = \left\{\begin{pmatrix} a & b \\ pc & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, 0 \le a, b, c < p, 0 \le d < p^2\right\}.$$

The multiplication and addition operations on this ring are defined as follows:

if $x = \begin{pmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{pmatrix}$ and $y = \begin{pmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{pmatrix}$, then

$$x + y = \begin{pmatrix} (a_1 + a_2)(\mathrm{mod}\, p) & (b_1 + b_2)(\mathrm{mod}\, p) \\ p(c_1 + c_2)(\mathrm{mod}\, p^2) & (d_1 + d_2)(\mathrm{mod}\, p^2) \end{pmatrix},$$

and

$$x.y = \begin{pmatrix} (a_1 a_2)(\mathrm{mod}\, p) & (a_1 b_2 + b_1 d_2)(\mathrm{mod}\, p) \\ p(c_1 a_2 + d_1 c_2)(\mathrm{mod}\, p^2) & (pc_1 b_2 + d_1 d_2)(\mathrm{mod}\, p^2) \end{pmatrix}.$$

Now, let p, q be two distinct primes and $n = pq$. We denote

$$E_n = \left\{\begin{pmatrix} a & b \\ pc & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, 0 \le a, b, c < n, 0 \le d < n^2\right\}.$$

It is easy to verify that the multiplication defined by

$$\begin{pmatrix} a_1 & b_1 \\ nc_1 & d_1 \end{pmatrix} . \begin{pmatrix} a_2 & b_2 \\ nc_2 & d_2 \end{pmatrix} = \begin{pmatrix} (a_1 a_2)(\mathrm{mod}\, n) & (a_1 b_2 + b_1 d_2)(\mathrm{mod}\, n) \\ n(c_1 a_2 + d_1 c_2)(\mathrm{mod}\, n^2) & (nc_1 b_2 + d_1 d_2)(\mathrm{mod}\, n^2) \end{pmatrix}$$

is a binary operation on E_n.

We define the maps $\mu: E_n \to E_p$ and $\eta: E_n \to E_q$ as follows.

For $x = \begin{pmatrix} a & b \\ pqc & d \end{pmatrix} \in E_n$, $\mu(x) = \begin{pmatrix} a_p & b_p \\ pc_p & d_p \end{pmatrix}$ and $\eta(x) = \begin{pmatrix} a_q & b_q \\ qc_q & d_q \end{pmatrix}$,

where

$a_p, b_p, c_p, d_p \in \mathbb{Z}, 0 \le a_p, b_p, c_p < p, 0 \le d_p < p^2,$

$a_p \equiv a(\mathrm{mod}\, p), b_p \equiv b(\mathrm{mod}\, p), c_p \equiv qc(\mathrm{mod}\, p),$

$a_q, b_q, c_q, d_q \in \mathbb{Z}, 0 \le a_q, b_q, c_q < q, 0 \le d_q < q^2,$

$a_q \equiv a(\mathrm{mod}\, q), b_q \equiv b(\mathrm{mod}\, q), c_q \equiv pc(\mathrm{mod}\, p),$

and

$d_p \equiv d(\mathrm{mod}\, p^2), d_q \equiv d(\mathrm{mod}\, q^2).$

Then, we can prove the following propositions.

Proposition 5.1 *μ and η are homomorphisms and the map $\theta: E_n \to E_p \times E_q$ defined by $\theta(x) = (\mu(x), \eta(x))$ is an injective.*

We denote by E_p^* and E_q^* the set of all invertible elements in E_p and E_q, respectively. Further, E_p^* and E_q^* are multiplicative groups with orders $p^3(p-1)^2$ and $q^3(q-1)^2$, respectively [24]. Applying the model proposed in Section 3.1 where

$Y = E_n, U = E_p, V = E_q,$

$X = \{x \in Y : \mu(x) \in \mathrm{E}_\mathrm{p}^* \text{ and } \eta(x) \in \mathrm{E}_\mathrm{q}^*\},$

and

$U_1 = U_2 = \mathrm{E}_\mathrm{p}^*, \mathrm{V}_1 = \mathrm{V}_2 = \mathrm{E}_\mathrm{q}^*,$

the equality $m^{ed} = m$ holds for all $m \in X$ if e, d satisfy $ed \equiv 1(\mathrm{mod}\, L)$ with $L = \mathrm{lcm}(p^3(p-1)^2, q^3(q-1)^2)$. Therefore, we can construct the cryptosystem analogue of RSA. The details and the cryptanalysis of this cryptosystem were discussed in [25].

6. Conclusions

The equality $m^{ed} = m$ plays an important role in a RSA cryptosystem, it ensures encryption and decryption phases in the cryptosystem. The paper has proposed a algebraic structure, or a scheme, for constructing a RSA cryptosystem by proposing conditions which ensure that equality on a semigroup. Applying this scheme, the equalities in known RSAs are then established by uni-scheme, despite of the RSA platforms being quotient rings or groups. The usefulness of the proposed scheme is proved when constructing Bergman ring based RSA, which follows the proposed scheme and has some advantages compared to the original RSA. One may ask whether the proposed scheme will be applied for a future RSA variant. The answer is yes if that RSA variant built on a commutative group; we will look more closely at the answer in another article.

References

[1] R.L.Rivest, A.Shamir, and L.M.Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM 21 (1978)*, no 2, 120-126.
Article (CrossRef Link)

[2] M.Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, 36:553-558, 1990. Article (CrossRef Link)

[3] D. Boneh and G. Durfee, Cryptanalysis of RSA with private key d less than $n^{0.292}$, Eurocrypt'99. Article (CrossRef Link)

[4] C.Coupe, P.Nguyen, and J.Stern, "The effectiveness of lattice attacks against low-exponent RSA," *Public Key Cryptography* '99. Article (CrossRef Link)

[5] A. Nitaj and T. Rachidi, "Factoring RSA moduli with weak prime Factors, Codes," in *Proc. of Cryptology and Information Security Conference*, *C2SI 2015*, LNCS 9084, pp. 361-374, 2015. Article (CrossRef Link)

[6] A.K. Lenstra and J.H.W.Lenstra, "The development of the number field sieve," *Lecture Notes in Mathematics*, vol. 1554, Springer-Verlag, Berlin, 1993. Article (CrossRef Link)

[7] T. Collins, D. Hopkins, S. Langford, and M. Sabin, "Public Key Cryptographic Apparatus and Method," *US Patent 5*, 848, 159. Jan.1997.

[8] A. Fiat, "Batch RSA," *Advances in Cryptology*, Crypto'89, Vol. 435, pp. 175-185, 1989.
Article (CrossRef Link)

[9] D. Pointcheval, "New public key cryptosystem based on the dependent RSA problem," *Eurocrypt'99 LNCS Springer-Verlag*, vol. 1592, pp. 239-254, 1999. Article (CrossRef Link)

[10] T. Takagi, "Fast RSA - Type Cryptosystem Modulo $p^k q$," *Crypto'98, 1462 of LNCS*, 1998, pp. 318-326, 1998. Article (CrossRef Link)

[11] Garg D. and Verma S., "Improvement over Public key Cryptographic Algorithm," in *Proc. of Advance Computing Conference, 2009, IACC 2009, IEEE International Conference*, March 2009, pp. 734-739. Article (CrossRef Link)

[12] Garg D. and Verma S., "Improvement in RSA Cryptosystem," *Journal of Advances in Information Technology*, vol. 2, no. 3, August 2011. Article (CrossRef Link)

[13] M.F. Esgin, M.S. Kiraz, and O. Uzunkol, "A new partial key exposure attack on MultiPower RSA," in *Proc. of 6th International Conference on Algebraic Information* (CAI 2015).
Article (CrossRef Link)

[14] A. Nitaj and T. Rachidi, "New attacks on RSA with moduli $n = p^k q$," C2SI 2015, LNCS 9084, pp. 352-360, 2015. Article (CrossRef Link)

[15] Varadharajan V. and Odoni R., "Extension of RSA cryptosystems to matrix rings," Cryptologia, 9:2, 140-153, 1985. Article (CrossRef Link)

[16] N. Demytko, "A new elliptic curve based analogue of RSA," EUROCRYPT'93, LNCS 765 40-49 (1993). Article (CrossRef Link)

[17] El-Kassar, A.N., R. Hatary and Y. Awad, "Modified RSA in the domains of Gaussian integers and polynomials over finite fields," in *Proc. of Intl. Conf. Computer Science, Software Engineering, Information Technology, e-Business and Applications* (CSITeA'04), Cairo, Egypt.

[18] James.T. Cross, "The Euler Φ-function in the Gaussian integers," *The American Mathematical Monthly*, vol. 90, no. 8, pp. 518-528, Oct., 1983. Article (CrossRef Link)

[19] R.Schoof, Elliptic curves over finite fields and the computation of square roots mod *p*,Mathematics of Computation, vol. 44, no. 170, pp 483-494. Article (CrossRef Link)

[20] Lindsay N. Childs, "A concrete introduction to higher algebra," *Third Edition, Springer Science + Business Media LLC*, pp. 543-552, 2009. Article (CrossRef Link)

[21] M. Ben-Or, "Probabilistic algorithms in finite fields," in *Proc. of 22nd Annual Symposium on Foundations of Computer Science*, 394-398, 1981. Article (CrossRef Link)

[22] Victor Shoup, "A computational introduction to number theory and algebra," *Cambridge University Press*, pp.530-538, 2008.

[23] Bergman G.M., Examples in PI ring theory, Israel J. Math. 18, 257-277, 1974.
Article (CrossRef Link)

[24] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa, "On the arithmetic of the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$," *AAECC*, 2011. Article (CrossRef Link)

[25] Long T.D., Thu D.T. and Thuc D.N., "A Bergman ring based cryptosystem analogue of RSA," *ICITCS 2013 eBook*, Macau, Dec., 2013, pp. 377-380. Article (CrossRef Link)

Dr. TRAN Dinh Long is lecturer at Hue University. His research focus on Cryptography and Applied Mathematics.

Dan-Thu Tran is Dean of the Faculty of Information Technology, University of Science, Vietnam National University – Ho Chi Minh city, Vietnam. His research focus on Combinatorics, Algebra and Cryptography. He obtained his Ph.D. in computer science from National Polytechnical Institute of Toulouse, France in 2001.

Deokjai Choi, Ph. D is a professor of School of Electronics and Computer Engineering, Chonnam National University, Korea. He got PhD degree in Computer Science and Telecommunication Program, University of Missouri-Kansas City, USA in 1995. His research interests are context awareness, sensor network, future Internet, SDN.

Dr. NGUYEN Dinh Thuc is professor at School of Information Technology, University of Science, Vietnam National University of Ho Chi Minh City. His research focus on Applied Cryptography, Information Security and Database Security.