# A Bergman ring based cryptosystem analogue of RSA

Long D. T.,Thu D. T., and Thuc D. N.

***Abstract*—Based on results of J.J.Climent, Pedro R. Navarro and Leandro Tortosa about Bergman ring, the paper constructs an exponent type encryption and decryption cryptosystem analogue of RSA. Althought involving many operations than original RSA in encryption and decryption processes, the cryptosystem has some advantages compare to known RSA variants.**

***Keywords*—RSA cryptosystem, Bergman ring, monoid.**

## I. Introduction

SINCE RSA was first introduced in 1978, there have been many works related to it. Besides cryptanalysing on RSA, there have been many developed variants of RSA. For RSA variants on platform $\mathbf{Z}_n$, some extra algorithms are added to speed up the decryption or encryption process. Batch RSA [9], and Multi Prime RSA [3] are examples for this. MultiPower RSA cryptosystem [12] was built on $\mathbf{Z}_n$ where the modulus $n$ having the form $n = p^k q$ with $k \in \mathbf{Z}, k \geq 2$ and $p, q$ are distinct primes. This RSA variants was then combined with DRSA to increase the encryption verification performance [5], [6].

Constructing RSA variants on new platforms other than $\mathbf{Z}_n$ is also a problem concerned by many authors. RSA variants on quotient rings of Euclidean rings such as Gaussian integer ring or rings of polynomials having coefficients on finite fields [10], RSA variant on finite groups such as elliptic curve groups [7] or groups of non-singular matrices whose elements on finite fields [13] are examples for this type of RSA variants. We construct in this paper a RSA variant on a monoid whose multiplicative operation is defined similarly to that on Bergman ring.

Bergman ring was introduced by Bergman [1], J.J. Climent, Pedro R. Navarro and Leandro Tortosa in [2] pointed out the isomorphism between Bergman ring End($\mathbf{Z_p} \times \mathbf{Z_{p^2}}$) and ring of $2 \times 2$ matrices with operations slightly different from usual matrix operation. This allows us to perform operations on elements of Bergman ring as doing on matrices. With two distinct primes $p$ and $q$, based on operations on Bergman ring $E_p$ and $E_q$ we define a monoid $E_n$ where $n = pq$ and construct a cryptosystem analogue of RSA on a subset of $E_n$. We recall details on Bergman ring in Section 2. Section 3 reserves for the constructing our Bergman ring based cryptosystem and discussing on that cryptosystem.

## II. Bergman ring

Bergman [1] established the End($\mathbf{Z}_p \times \mathbf{Z}_{p^2}$) is a semilocal ring with $p^5$ elements, where $p$ is a prime. J.J. Climent, Pedro R. Navarro and Leandro Tortosa [2] identified the elements of End($\mathbf{Z}_p \times \mathbf{Z}_{p^2}$) as matrices of size $2 \times 2$, whose elements in the first row belong to $\mathbf{Z}_p$ and elements in the second row belong to $\mathbf{Z}_{p^2}$. Now we recall briefly some properties of End($\mathbf{Z}_p \times \mathbf{Z}_{p^2}$) which are necessary for our purpose, for more details we refer the reader to [2].

**Theorem 1.**(J. Climent et al. [2]) The set

$$E_p = \left\{ \begin{bmatrix} a & b \\ pc & d \end{bmatrix} : a, b, c, d \in \mathbf{Z}, 0 \leq a, b, c < p, 0 \leq d < p^2 \right\}$$

is a noncommutative unitary ring with addition and multiplication given as follows.

If

$$x = \begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix}, y = \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} \in E_p \text{ then}$$

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

and

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

respectively.

J. Climent et al. in [2] pointed out that there is an isomorphism ring an ring isomorphism between the Bergman ring End($\mathbf{Z_p} \times \mathbf{Z_{p^2}}$) and $E_p$. Therefore, each element in End($\mathbf{Z_p} \times \mathbf{Z_{p^2}}$) can be regarded as a $2 \times 2$ matrix of the form

$$\begin{bmatrix} a & b \\ pc & d \end{bmatrix} (a, b, c, d \in \mathbf{Z}, 0 \leq a, b, c < p, 0 \leq d < p^2)$$

or

$$\begin{bmatrix} a & b \\ pc & pu + v \end{bmatrix} (a, b, c, u, v \in \mathbf{Z}, 0 \leq a, b, c, u, v < p).$$

Because the multiplicative group of invertible matrices is involved in our scheme, we need the following theorem.

**Theorem 2.**(J. Climent et al. [2])*Assume that* $M = \begin{bmatrix} a & b \\ pc & pu + v \end{bmatrix} \in E_p$ *with* $a, b, c, u, v \in \mathbf{Z}, 0 \leq a, b, c, u, v < p$. *Then* $M$ *is invertible if and only if* $a \neq 0$ *and* $v \neq 0$.

The above theorem allows us to calculate the number of invertible elements in $E_p$ as follows.

**Theorem 3.**(J. Climent et al. [2])The number of invertible elements in $E_p$ is $p^3(p-1)^2$.

## III. Our proposed cryptosystem analogue of RSA

Let $p, q$ be two distinct primes and $n = pq$. In this section, we construct a monoid $E_n$ and establish the equation $M^{ed} = M$ for all $M \in X$, where $X$ is a subset of $E_n$.

This work was supported by the HCMC-DOST project "RSA-cryptosystem and cryptanalysis".

978-1-4799-2845-3/13/$31.00 ©2013 IEEE

*A. Constructing the monoid $E_n$*

Now we denote

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

For $x = \begin{bmatrix} a_1 & b_1 \\ nc_1 & d_1 \end{bmatrix}, y = \begin{bmatrix} a_2 & b_2 \\ nc_2 & d_2 \end{bmatrix} \in E_n$ we define

$$x.y = \begin{bmatrix} (a_1a_2) \bmod n & (a_1b_2 + b_1d_2) \bmod n \\ n(c_1a_2 + d_1c_2) \bmod n^2 & (nc_1b_2 + d_1d_2) \bmod n^2 \end{bmatrix}.$$

It is easy to check that the defined multiplication is associative binary operation on $E_n$.
We define the map

$$\mu : E_n \to E_p$$
$$\begin{bmatrix} a & b \\ pqc & d \end{bmatrix} \mapsto \begin{bmatrix} a_p & b_p \\ pc_p & d_p \end{bmatrix}$$

where

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

and

$$a_p \equiv a(\bmod p), b_p \equiv b(\bmod p), c_p \equiv qc(\bmod p),$$
$$d_p \equiv d(\bmod p^2).$$

We also define the map

$$\eta : E_n \to E_q$$
$$\begin{bmatrix} a & b \\ pqc & d \end{bmatrix} \mapsto \begin{bmatrix} a_q & b_q \\ qc_q & d_q \end{bmatrix}$$

where

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

and

$$a_q \equiv a(\bmod q), b_q \equiv b(\bmod q), c_q \equiv pc(\bmod q),$$
$$d_q \equiv d(\bmod q^2).$$

It is easily seen that $\mu$ and $\eta$ are well defined.

**Proposition 1.** *$\mu$ and $\eta$ are monoid - homomorphisms.*

*Proof.* For $x = \begin{bmatrix} a & b \\ pqc & d \end{bmatrix}, y = \begin{bmatrix} a' & b' \\ pqc' & d' \end{bmatrix} \in E_n$ we have

$$\mu(x) = \begin{bmatrix} a_p & b_p \\ pc_p & d_p \end{bmatrix}, \mu(y) = \begin{bmatrix} a'_p & b'_p \\ pc'_p & d'_p \end{bmatrix},$$

and

$$xy = \begin{bmatrix} aa'(\bmod n) & (ab' + bd')(\bmod n) \\ pq(ca' + dc')(\bmod n^2) & (ncb' + dd')(\bmod n^2) \end{bmatrix},$$

where

$$a_p, b_p, c_p, d_p, a'_p, b'_p, c'_p, d'_p \in \mathbf{Z}, \quad (1)$$
$$0 \le a_p, b_p, c_p, a'_p, b'_p, c'_p < p, 0 \le d_p, d'_p < p^2, \quad (2)$$
$$a_p \equiv a(\bmod p), b_p \equiv b(\bmod p), \quad (3)$$
$$c_p \equiv qc(\bmod p), d_p \equiv d(\bmod p^2), \quad (4)$$
$$a'_p \equiv a'(\bmod p), b'_p \equiv b'(\bmod p), \quad (5)$$
$$c'_p \equiv qc'(\bmod p), d'_p \equiv d(\bmod p^2), \quad (6)$$

Since (1)-(6) we have

$$a_pa'_p \equiv aa'(\bmod p), \quad (7)$$
$$a_pb'_p + b_pd'_p \equiv ab' + bd'(\bmod p), \quad (8)$$
$$c_pa'_p + d_pc'_p \equiv q(ca' + dc')(\bmod p), \quad (9)$$

and

$$c_pb'_p \equiv qcb'(\bmod p). \quad (10)$$

It follows from (8) that

$$p(c_pa'_p + d_pc'_p) \equiv pq(ca' + dc')(\bmod p^2) \quad (11)$$

and from (9) that

$$pc_pb'_p \equiv pqcb'(\bmod p^2). \quad (12)$$

Combine (11), (12) and $d_pd'_p \equiv dd'(\bmod p^2)$ implies

$$c_pb'_p + d_pd'_p \equiv ncb' + dd'(\bmod p^2). \quad (13)$$

(7), (8), (9) and (13) deduces the equation $\mu(xy) = \mu(x)\mu(y)$. Hence, $\mu$ is a homomorphism. The same conclusion can be drawn for $\eta$.■

**Proposition 2.** *The map* $\lambda : E_n \to E_p \times E_q$
$$M \mapsto \lambda(M) = (\mu(M), \eta(M))$$
*is an injection.*

*Proof.* The proof is based on the following:
If $k, l \in \mathbf{Z}, \gcd(k, l) = 1, 0 \le x, y < kl, x \equiv y(\bmod k)$ and $x \equiv y(\bmod l)$ then $x = y$.
Now, suppose that $M = \begin{bmatrix} a & b \\ pqc & d \end{bmatrix}, N = \begin{bmatrix} a' & b' \\ pqc' & d' \end{bmatrix} \in E_n$ such that $\lambda(M) = \lambda(N)$.
By definition of $\mu$ and $\eta$ we have

$$\mu(M) = \begin{bmatrix} a_p & b_p \\ pc_p & d_p \end{bmatrix}, \mu(N) = \begin{bmatrix} a'_p & b'_p \\ pc'_p & d'_p \end{bmatrix},$$

$$\eta(M) = \begin{bmatrix} a_q & b_q \\ qc_q & d_q \end{bmatrix}, \eta(N) = \begin{bmatrix} a'_q & b'_q \\ qc'_q & d'_q \end{bmatrix},$$

where
$a_p, b_p, c_p, d_p, a'_p, b'_p, c'_p, d'_p \in \mathbf{Z}$,
$0 \le a_p, b_p, c_p, a'_p, b'_p, c'_p < p, 0 \le d_p, d'_p < p^2$,
$a_q, b_q, c_q, a'_q, b'_q, c'_q \in \mathbf{Z}_q, d_q, d'_q \in \mathbf{Z}_{q^2}$,
$a_p \equiv a(\bmod p), b_p \equiv b(\bmod p)$,
$c_p \equiv qc(\bmod p), d_p \equiv d(\bmod p^2)$,
$a_q \equiv a(\bmod q), b_q \equiv b(\bmod q)$,
$c_q \equiv pc(\bmod q), d_q \equiv d(\bmod q^2)$,
$a'_p \equiv a'(\bmod p), b'_p \equiv b'(\bmod p)$,
$c'_p \equiv qc'(\bmod p), d'_p \equiv d'(\bmod p^2)$,
and
$a'_q \equiv a'(\bmod q), b'_q \equiv b'(\bmod q)$,
$c'_q \equiv pc'(\bmod q), d'_q \equiv d'(\bmod q^2)$.

Since $\lambda(M) = \lambda(N)$, then $\mu(M) = \mu(N)$ and $\eta(M) = \eta(N)$. It follows that

$$\begin{bmatrix} a_p & b_p \\ pc_p & d_p \end{bmatrix} = \begin{bmatrix} a'_p & b'_p \\ pc'_p & d'_p \end{bmatrix} \text{ and } \begin{bmatrix} a_q & b_q \\ qc_q & d_q \end{bmatrix} = \begin{bmatrix} a'_q & b'_q \\ qc'_q & d'_q \end{bmatrix}.$$

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

Since $\begin{cases} pc_p \equiv pc'_p (\mathrm{mod}\, p^2) \\ qc_q \equiv qc'_q (\mathrm{mod}\, q^2) \end{cases}$, then $\begin{cases} c_p \equiv c'_p (\mathrm{mod}\, p) \\ c_q \equiv c'_q (\mathrm{mod}\, q) \end{cases}$.
Thus, $c = c'$.

Since $\begin{cases} d_p \equiv d'_p (\mathrm{mod}\, p^2) \\ d_q \equiv d'_q (\mathrm{mod}\, q^2) \end{cases}$, then $\begin{cases} d \equiv d' (\mathrm{mod}\, p^2) \\ d \equiv d' (\mathrm{mod}\, q^2) \end{cases}$. Hence, $d = d'$.■

Denote by $E_p^*$ and $E_q^*$ the sets of invertible elements in $E_p$ and $E_q$, respectively. According to Theorem 3, the numbers of elements in $E_p^*$ and $E_q^*$ are $p^3(p-1)^2$ and $q^3(q-1)^2$, respectively. Analogous to the equation $m^{ed} = m$ in the original RSA cryptosystem, we have the following.

**Proposition 3.** *If $M \in E_n$ such that $\mu(M) \in E_p^*$ and $\eta(M) \in E_q^*$ then $M^{ed} = M$, where $e, d$ are integers satisfying $ed \equiv 1 (mod\, L)$ with $L = lcm(p^3(p-1)^2, q^3(q-1)^2)$.*

*Proof.* It follows from $\mu$ and $\eta$ are monoid homomorphisms that $\mu(M^{ed}) = (\mu(M))^{ed}$ and $\eta(M^{ed}) = (\eta(M))^{ed}$.
Since $\mu(M)$ is a element of $E_p^*$, which is a group of order $p^3(p-1)^2$, then $(\mu(M))^{ed} = \mu(M)$. In the same manner we obtain $(\eta(M))^{ed} = \eta(M)$. Thus,

$$\begin{aligned} \lambda(M^{ed}) &= (\mu(M^{ed}), \eta(M^{ed})) = ((\mu(M))^{ed}, (\eta(M))^{ed}) \\ &= (\mu(M), \eta(M)) = \lambda(M). \end{aligned}$$

Since $\lambda$ is a injection according to proposition 2, then $M^{ed} = M$. ■

With $M \in E_n$, the following proposition gives the condition which ensures $\mu(M) \in E_p^*$ and $\eta(M) \in E_q^*$.

**Proposition 4.** *Let $M = \begin{bmatrix} a & b \\ nc & nu+v \end{bmatrix} \in E_n$, then $\mu(M) \in E_p^*$ and $\eta(M) \in E_q^*$ iff $gcd(a, n) = 1$ and $gcd(v, n) = 1$.*

*Proof.* According to Theorem 2, we have

$\mu(M) \in E_p^*$ if and only if $\gcd(a, p) = \gcd(v, p) = 1$
and
$\eta(M) \in E_q^*$ if and only if $\gcd(a, q) = \gcd(v, q) = 1$.
Therefore, $\mu(M) \in E_p^*$ and $\eta(M) \in E_q^*$ if only if $\gcd(a, p) = \gcd(a, q) = 1$ and $\gcd(v, p) = \gcd(v, q) = 1$. The last conditions mean $\gcd(a, n) = 1$ and $\gcd(v, n) = 1$.■

We are now in a position to introduce our cryptosystem.

### B. The proposed cryptosystem

*Key creation.*

-Choose two distinct primes $p, q$. Calculate $n = pq$.
-Compute $L = \mathrm{lcm}(p^3(p-1)^2, q^3(q-1)^2)$.
-Choose an integer $e$ sarisfying $\gcd(L, e) = 1 (0 < e < L)$.
-Compute $d \equiv e^{-1} (\mathrm{mod}\, L)$.
-Publish $n$ and $e$ as public key, keep $d$ as private key.

*Encryption.*

-Plaintexts are elements $m \in \mathbf{Z}_n$.
-Choose randomly $a, c, u, v \in \mathbf{Z}_n$ such that $\gcd(a, n) = 1$ and $\gcd(v, n) = 1$.
-$m$ in then encrypted by calculating $C = M^e$ where $M = \begin{bmatrix} a & m \\ nc & nu+v \end{bmatrix} \in E_n$.

*Decryption.*

-$m$ is decrypted by computing $C^d$, $m$ is the element at the position $(1, 2)$ of $C^d$.

**Example.** Choose $p = 7, q = 11$, then $n = pq = 77$. Next we compute
$s = p^3(p-1)^2 = 12348, t = q^3(q-1)^2 = 133100, L = \mathrm{lcm}(s, t) = 410879700$.
Choose $e = 87211199$ satisfying $1 < e < L$ and $\mathrm{lcd}(e, L) = 1$, then $d = e^{-1} (\mathrm{mod}\, L) = 1069799$.
For encrypting the plaintext $m = 12$, we choose $a, c, u, v \in \mathbf{Z}_{77}$ such that $\gcd(a, 77) = \gcd(v, 77) = 1$ and compute $C = M^e$ where $M = \begin{bmatrix} a & m \\ nc & nu+v \end{bmatrix}$. Choose $a = 2, c = 3, u = 5, v = 1$ then $M = \begin{bmatrix} 2 & 12 \\ 231 & 386 \end{bmatrix}$. Hence, $C = M^e = M^{87211199} = \begin{bmatrix} 39 & 71 \\ 2849 & 3389 \end{bmatrix}$ is the correspondent ciphertext.
To recover $m$ from $M$, we calculate $C^d = C^{1069799} = \begin{bmatrix} 2 & 12 \\ 231 & 386 \end{bmatrix}$ and the value $m = 12$ at position (1,2) in the resulting matrix is the plaintext.

### C. Discussion

Because $L = \mathrm{lcm}(p^3(p-1)^2, q^3(q-1)^2)$ is much larger than $(p-1)(q-1)$, the encryption and decryption processes in our scheme are involved many operations than those in the original RSA scheme. To compensate for this, we have the following.

In our scheme, the real plaintext $m$ is contained only at position $(1, 2)$ in matrix $M = \begin{bmatrix} a & m \\ nc & nu+v \end{bmatrix}$. However, $c$ and $u$ can hide real plaintext and therefore the length of plaintext can be strengthen.
Compare to the cryptosystem considered in [13], in which each plaintext is also a matrix, the sender must verify the nonsingularity of matrix plaintext. In our proposed cryptosystem, the sender does not face to problem of verifying non-singularity of matrix plaintext $M$. The condition $\gcd(a, n) = \gcd(v, n) = 1$ ensures that and does not leak out any information of $p$ and $q$.

For a plaintext $m$, we can choose various values for $a$ and $v$, this leads to the matrix $M = \begin{bmatrix} a & m \\ nc & nu+v \end{bmatrix} \in E_n$ and then $C = M^e$ can have many different values. This makes our cryptosystem avoid chosen-plaintext attacks or plaintext-checking attacks.

Lattice reduction algorithms are effecitive tools in cryptanalysis on RSA [4], [8], [11]. As in the original RSA cryptosystem, lattice attack can be applied to our proposed cryptosystem in the case the public key $e$ and the private key $d$ are not balance. For this, we apply the reasonable argument in [11] as follows. Because $p$ and $q$ are balance to avoid factoring $n$ attack, then $\varphi(n) = n + u$ where $u := 1 - p - q = O(\sqrt{n})$. Estimate $L = \mathrm{lcm}(p^3(p-1)^2, q^3(q-1)^2) = p^3q^3\mathrm{lcm}((p-1)^2, (q-1)^2) < n^4\varphi(n)$. The equation $ed \equiv 1 (\mathrm{mod}\, L)$ implies that there exists an integer $k = O(d)$ such that $ed = 1 + kL < kn^4(n+u)$, hence $ed - kn^5 < n^4ku$. Denote $l = ed - kn^5$ then $l = O(dn^4\sqrt{n})$. Consider the 2-rank lattice in $\mathbf{R}^2$ spanned by two vector $v_1 = (e, n^4\sqrt{n})$ and $v_2 = (n^5, 0)$. $H$ contains vector $t = de_1 - ke_2 = (ed - kn^5, dn^4\sqrt{n})$ whose norm is $\|t\| \approx dn^4\sqrt{n}$, while $\mathrm{vol}(H)^{\frac{1}{2}} = \sqrt{n^9\sqrt{n}} = n^{\frac{19}{4}}$. Thus, $t$

could be a shortest vector in $H$ being a reasonable guess if $dn^4\sqrt{n} < n^{\frac{19}{4}}$ or $d < n^{\frac{1}{4}}$. We can apply Gaussian algorithm to $H$ for finding $t$ and then recover the public 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 weak key case for lattice attack, hence the probability for succeed lattice attack in 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 $L = \text{lcm}(p^3(p-1)^2, q^3(q-1)^2) > n^3$ and the probability for success lattice attack is $\frac{n^{\frac{1}{4}}}{L} < \frac{n^{\frac{1}{4}}}{n^3} = \frac{1}{n^{\frac{11}{4}}}$.

We finish this section by following remark. A bad choice values of $a, c, u$ and $v$ can lead to a trivial system. For example, if we choose $a = v = 1, c = u = 0$, then $M = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$. It is easily seen that $M^k = \begin{bmatrix} 1 & km \\ 0 & 1 \end{bmatrix}$ for all $k \in \mathbf{N}^*$. The equation $M^{ed} = \begin{bmatrix} 1 & edm \\ 0 & 1 \end{bmatrix}$ gives us a trivial encryption and decryption as follows: a plaintext $m \in \mathbf{Z}_n$ is encrypted to ciphertext $c = em$ and $c$ is in turn decrypted to $dc = edm = m(\text{mod}\, n)$.

## IV. Conclusion

Althought having some advantages, the main drawback of our cryptosystem is involving many operations in calculating power of a matrix. To avoid this, we can choose suitable values for $a, c, u, v$ so that we can establish formula for the element at position $(1, 2)$ in matrix $M^k$, computing ciphertext now is only doing on plaintext $m$. Thus, we reduce a lot of operations. This is an open problem arising from our scheme.

## References


[1] Bergman, G.M, *Examples in PI ring theory*, Israel J. Math. 18, 257-277 (1974).

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

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

[4] Christophe Coupe, Phong Nguyen, and Jacques Stern, *The effectiveness of lattice attacks against low-exponent RSA*, Public Key Cryptography '99.

[5] Garg D. and Verma S.: Improvement over Public key Cryptographic Algorithm, *Advance Computing Conference, 2009, IACC 2009, IEEE International Conference*, March 2009, pp. 734-739.

[6] Garg D. and Verma S.: Improvement in RSA Cryptosystem, *Journal of Advances in Information Technology*, Vol. 2, No. 3, August 2011.

[7] N. Demytko, *A new elliptic curve based analogue of RSA*, Advances in Cryptology-EUROCRYPT'93, LNCS 765, pp. 40-49, 1994.

[8] C. Dwork, *Lattices and Their Application to Cryptography*, Lecture Notes, Stanford University, 1998.

[9] A. Fiat: Batch RSA, *Advances in Cryptology*, Crypto'89, Vol. 435, 1989, pp. 175-185.

[10] El-Kassar A.N., R. Haraty and Y. Awad, *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.

[11] Phong Q. Nguyen, *Public key cryptanalysis*, Recent Trends in Cryptography, Contemporary Mathematics series, AMS-RSME, 2008.

[12] T. Takagi: Fast RSA - Type Cryptosystem Modulo $p^k q$, *Crypto'98*, 1462 of LNCS, 1998, pp. 318-326.

[13] V. Varadharajan and R. Odoni, *Extension of RSA cryptosystem to matrix rings*, Cryptologia, Volume 9, Number 2, 1985.