Enhancing The Performance Of RSA-Type Cryptosystems

Ch. JL Padmaja, V.S.Bhagavan, B.Srinivas, P.L.R. Kameswari

Abstract: Many RSA variants have been proposed to improve the efficiency of the standard RSA cryptosystem. Out of all such RSA-type cryptosystems, Rebalanced RSA has been constructed for effective transactions with smaller machines. In this scheme, decryption is made faster by choosing "d", the secret key first in key generation instead of choosing the public key "e" as in the case of RSA leaving the computational burden on encryption side. This chapter introduces two new schemes to further enhance the efficiency of Rebalanced RSA.

Index Terms: Complexity, Cryptosystem, Decryption, Encryption, Factorization, Lattice, Rebalanced RSA.

1. INTRODUCTION

Researchers' attention has been drawn to information security, along with the growth of interconnected computers. Users expect their information to be protected in its originality from unauthorized access and alteration. There have been some secure mechanisms that are otherwise known as cryptosystems to meet the growing demand for data security [1],[2],[3]. RSA [4] is the most widely used public key cryptosystem across the world. Owing to the infeasibility of factoring a composite into two prime numbers, this cryptosystem is being in practice specifically in secure business transactions. RSA system is a bit slower than other public key cryptosystems [5], [6], [7] because of the key length taken to build the system. Many variants have been proposed duly enhancing the decryption speed of RSA system [8], [9]. In some communication systems, one cannot expect both ends of communication to be suitable enough to carry out the encryption and decryption using RSA or RSA-type cryptosystems. Small devices like cellphones cannot afford such calculations. Hence, Rebalanced RSA [10], [11], [12] was designed in such a way that smaller devices can run decryption effectively putting the entire burden on the encryption side [13],[14],[15] in the resources like servers. In this paper, an attempt is made to enhance the performance of Rebalanced RSA in enciphering stage but not compromising the decryption workload.

2 PROPOSED SCHEME

The Rebalanced RSA was improved to design Rebalanced RSA CRT Schemes [16]. The RRCS was further extended as ERRCS [17] for improvement in decryption speed. In Rebalanced RSA-CRT Scheme A^+ [16], the modulus was taken with two primes [18], [19]. In this proposed scheme, the modulus is proposed with taking multiple primes. The key generation along with encryption and decryption phases is as follows.

- *Ch. JL Padmaja, Department of Mathematics, KL Education Foundation, Vaddeswaram, Andhra Pradesh, India. E-mail: padmajachivukula@gmail.com*
- *V.S.Bhagavan, . Department of Mathematics, KL Education Foundation, Vaddeswaram, Andhra Pradesh, India*
- *B.Srinivas, Department of Technical Education, Vijayawada, Andhra Pradesh, India*
- *P.L.R. Kameswari, Sri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh, India.*

Let n be the number of bits in the modulus N, n_ε be the number of bits in the public key e, n_δ be the number of bits in private key exponents d_{pi}. The key generation algorithm for the proposed scheme takes $(n, n_\varepsilon, n_\delta)$ as input, with $n_\varepsilon > n/i$ for i primes. It outputs a valid public key (e, N) and the corresponding private key $(d_{p1}, d_{p2}, \ldots.. p_1, p_2 \ldots..)$.

Key Generation

1.Select a random prime (n/i)-bit prime p_1 and a random (n_δ)-bit odd integer d_{p1} such that $\gcd(dp_1, p_1 - 1)=1$.

2.Select $k_{p1\alpha}$, random $(n_\varepsilon - n/i)$- bit integer, compute (e, d_{p1}) satisfying

$ed_{p1} = k_{p1\alpha}k_{p1\beta}(p_1 - 1) + 1$, where $k_{p1\alpha}(p_1 - 1) < e < 2k_{p1\alpha}(p_1 - 1)$ and $d_{p1} < k_{p1\beta} < 2d_{p1}$

3. Select $k_{p2\alpha}$, a random (n_δ)-bit integer such that $\gcd(k_{p2\alpha}, e) = 1$

4.Compute

(d_{p2}, Q) satisfying $ed_{p2} = k_{p2\alpha}Q + 1$, *where* $k_{p2\alpha} < d_{p2} < 2k_{p2\alpha}$ and Q $e < Q < 2e$

5.Factor Q as $Q = k_{p2\beta}(p_2 - 1)$ where $k_{p2\beta}$ is an $(n_e - n/i)$-bit number and p_2 is prime. If p_2 is not prime, go to step3.

6.Repeat steps 2 to 5 to calculate the primes $p_3 \ldots\ldots p_i$ and the private exponents $d_{p3}, \ldots., d_{pi}$

7. Calculate $N = p_1.p_2 \ldots. p_i$

8.Public key is $< N, e >$ and private key is $< d_{p1}, d_{p2} \ldots, p_1, p_2 \ldots >$

Encryption

To encrypt any message $M \in Z_N = \{0, 1, \ldots.. N - 1\}$,

Sender chooses a random integer s such that $s,(s+1) \in Z_N^*$ which is multiplicative group under moduloN and computes:

$$C_1 = (s+1)^e \mod N. \quad (1)$$

$$C_2 = M.s^{-1} \mod N. \quad (2)$$

and sends the cryptogram (C_1, C_2) to the receiver.

Decryption

Receiver first computes the set of equations:

$$s_{pi} = C_1^{dpi} \mod p_i. \quad (3)$$

Computes $(s+1)$ and hence s from the above and computes

$$M = C_2.s \bmod N. \quad (4)$$

2.1 Precision of key generation

When N is calculated with 3 primes, the key equations of the proposed schemes are:

$$ed_{p1} = k_{p1\alpha}k_{p1\beta}(p_1 - 1) + 1. \quad (5)$$

$$ed_{p2} = k_{p2\alpha}k_{p2\beta}(p_2 - 1) + 1. \quad (6)$$

$$ed_{p3} = k_{p3\alpha}k_{p3\beta}(p_3 - 1) + 1. \quad (7)$$

Multiplying the equations (5), (6), (7),

$$(ed_{p1} - 1)(ed_{p2} - 1)(ed_{p3} - 1) = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}(p_1 - 1)(p_2 - 1)(p_3 - 1). \quad (8)$$

$$e(e^2 d_{p1}d_{p2}d_{p3} - ed_{p1}d_{p2} - ed_{p2}d_{p3} - ed_{p3}d_{p1} + d_{p1} + d_{p2} + d_{p3}) = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}\phi(N) + 1. \quad (9)$$

(or)

$$ed' = k'\phi(N) + 1. \quad (10)$$

where

$$d' = (e^2 d_{p1}d_{p2}d_{p3} - ed_{p1}d_{p2} - ed_{p2}d_{p3} - ed_{p3}d_{p1} + d_{p1} + d_{p2} + d_{p3})$$

$$k' = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$$

Hence, the keys of this scheme generate a valid pair of public key and private key.

2.2 Performance of proposed scheme

The performance of the proposed scheme is analysed below in terms of its security and speed. Factorization attacks applicable to the RSA and its variants also pose a threat to this scheme. Probabilistic factorization attacks look at using known private key d or knowing multiple of the totient function $\phi(N)$. Deterministic algorithms are GNFS and SNFS. These can be effectively countenanced by taking large modulus size like 2048 and 4096 for GNFS and large prime numbers for SNFS. As of now, modulus of size 768 bit is cracked using GNFS[20]. The estimated number of primes safe to face the factorization problem for 1024, 2048 and 4096 moduli are 3, 3 and 4 respectively [21]. The complexity of factoring the modulus decreases with increase in the number of primes as limited to the above mentioned. All other attacks decreases in strength with increased number of primes, but factorization becomes a threat with multiple primes greater than the constraint numbers. As far as the low public exponent attack[21] is concerned, this scheme is intended for those instances where it uses a public key exponent $e > N^{0.5}$. Hence the security against low public key attack is assured in this scheme. Private exponents are taken with the restriction as $n \geq 160$ bits for a modulus of size 1024. Hence, low private exponent attack does not arise in this scheme. As the scheme proposes a more number of parameters for key generation algorithm as against the original Rebalanced[10] and similar to the variant by Sun[16], attacks due to improper selection of parameters arise using lattice methods.

Multiplying the equations (5), (6) and 7),

$$\begin{aligned} &e^3 d_{p1}d_{p2}d_{p3} - e^2[d_{p1}d_{p2}(k_{p3\alpha}k_{p3\beta} - 1) + d_{p1}d_{p3}(k_{p2\alpha}k_{p2\beta} - 1) \\ &+ d_{p2}d_{p3}(k_{p1\alpha}k_{p1\beta} - 1)] \\ &+e[d_{p1}(k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p2\alpha}k_{p2\beta} + 1) + d_{p2}(k_{p1\alpha}k_{p1\beta}k_{p3\alpha}k_{p3\beta} \\ &- k_{p3\alpha}k_{p3\beta} - k_{p1\alpha}k_{p1\beta} + 1) + d_{p3}(k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta} - k_{p2\alpha}k_{p2\beta} - k_{p1\alpha}k_{p1\beta} + 1)] \\ &- k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}(N-1) - k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta} - k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} \\ &- k_{p3\alpha}k_{p3\beta}k_{p1\alpha}k_{p1\beta} + k_{p1\alpha}k_{p1\beta} + k_{p2\alpha}k_{p2\beta} + k_{p3\alpha}k_{p3\beta} - 1 = 0. \end{aligned} \quad (11)$$

$$\begin{aligned} &e^3 d_{p1}d_{p2}d_{p3} - e^2[d_{p1}d_{p2}(k_{p3\alpha}k_{p3\beta} - 1) + d_{p1}d_{p3}(k_{p2\alpha}k_{p2\beta} - 1) \\ &+ d_{p2}d_{p3}(k_{p1\alpha}k_{p1\beta} - 1)] \\ &+e[d_{p1}(k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p2\alpha}k_{p2\beta} + 1) + d_{p2}(k_{p1\alpha}k_{p1\beta}k_{p3\alpha}k_{p3\beta} \\ &- k_{p3\alpha}k_{p3\beta} - k_{p1\alpha}k_{p1\beta} + 1) + d_{p3}(k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta} - k_{p2\alpha}k_{p2\beta} - k_{p1\alpha}k_{p1\beta} + 1)] \\ &- k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}(N-1) + k_m + k_0 = 0. \end{aligned} \quad (12)$$

Here, $d_{p1}, d_{p2}, d_{p3}, k_{p1\alpha}, k_{p1\beta}, k_{p2\alpha}, k_{p2\beta}, k_{p3\alpha}, k_{p3\beta}$ are unknown variables whereas k_m can be found with exhaustive searching. This equation is solved using lattice basis reduction techniques by Coppersmith [22] in case there are relatively small unknown variables. For this, this equation can be considered in 4 ways: i) multivariate (four) linear modular equation (mod e^3) ii) trivariate linear modular equation (mod e^2) iii) bivariate linear modular equation (mod e) and iv) multivariate (four) with (mod N).

Case (i)

The polynomial equation with four variables mod e^3 is

$$f(x; y; z; w) \bmod e^3 = e^2x + ey - (N-1)z + w + k_m. \quad (13)$$

where,

$$x = d_{p1}d_{p2}(k_{p3\alpha}k_{p3\beta} - 1) + d_{p1}d_{p3}(k_{p2\alpha}k_{p2\beta} - 1) + d_{p2}d_{p3}(k_{p1\alpha}k_{p1\beta} - 1)$$

$$y = d_{p1}(k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p2\alpha}k_{p2\beta} + 1) + d_{p2}(k_{p1\alpha}k_{p1\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p1\alpha}k_{p1\beta} + 1) + d_{p3}(k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta} - k_{p2\alpha}k_{p2\beta} - k_{p1\alpha}k_{p1\beta} + 1)$$

$$z = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$$

$$w = k_0$$

The roots can be defined as x_0, y_0, z_0, w_0 for each of the polynomials if $|x_0| < X,\ |y_0| < Y,\ |z_0| < Z, |w_0| < W$ and $XYZW < e^3$ for some bounds $X,\ Y,\ Z\ and\ W$

The upper bounds are:

$$X = 2^{3n_\delta + n_\varepsilon - n/3}$$

$$Y = 2^{3n_\delta + 2n_\varepsilon - 2n/3}$$

$$Z = 2^{3n_\delta + 3n_\varepsilon - n}$$

$$W = 2^{2n_\delta + 2n_\varepsilon - 2n/3 - m}$$

Using the above bounds, solving the equation (13) for $XYZW < e^3$,

$$11n_\delta + 5n_\varepsilon < (8/3)n + m. \quad (14)$$

Since $n_k = n_\varepsilon + n_\delta - n/3$, equation (14) can be written as:

$$n_k < (6n_\varepsilon - n + m)/11. \quad (15)$$

Using this, $k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$ and k_0 are found and when substituted in equation (12), new equation with $d_{p1}d_{p2}d_{p3}$ is formed. If $k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$ can be factored, the values of each k can be obtained but with high complexity of factorization.

Case (ii)

The equation (12) modulo mod e^2, the following equation is obtained:

$$f(x; y; z) \bmod e^2 = ex + (N-1)y + z + k_m. \quad (16)$$

where,

$$x = d_{p1}(k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p2\alpha}k_{p2\beta} + 1) + d_{p2}(k_{p1\alpha}k_{p1\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p1\alpha}k_{p1\beta} + 1) + d_{p3}(k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta} - k_{p2\alpha}k_{p2\beta} - k_{p1\alpha}k_{p1\beta} + 1)$$

$$y = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$$

$$z = k_0$$

The equation (16) can be solved for the upper bounds X, Y and Z such that

$$|x_0| < X,\ |y_0| < Y,\ |z_0| < Z.$$

X, Y and Z are as follows:

$$X = 2^{3n_\delta + 2n_\varepsilon - 2n/3}$$

$$Y = 2^{3n_\delta + 3n_\varepsilon - n}$$

$$Z = 2^{2n_\delta + 2n_\varepsilon - 2n/3 - m}$$

Using the above bounds, solving the equation (12) for $XYZ < e^2$,

$$8n_\delta + 5n_\varepsilon < (7/3)n + m. \quad (17)$$

Since $n_k = n_\varepsilon + n_\delta - n/3$, equation (4.3.17) can be taken as:

$$n_k < (9n_\varepsilon - n + 3m)/24. \quad (18)$$

If n_k is chosen using this inequality, $k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$ can be obtained but no other variables of equation (12) are obtained.

Case iii)

The following polynomial is obtained by using equation (12) with modulo e

$$f(x; y) \bmod e = (N-1)x + y + k_m. \quad (19)$$

where,

$$x = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$$

$$y = k_0$$

The roots are x_0 and y_0 which can be solved for $X \geq x_0$ and $Y \geq y_0$, X and Y are the upper bounds which can be written as:

$$X = 2^{3n_\delta + 3n_\varepsilon - n}$$

$$Y = 2^{2n_\delta + 2n_\varepsilon - 2n/3 - m}$$

Using the above bounds, solving the equation (12) for $XY < e$,

$$5n_\delta + 4n_\varepsilon < (5/3)n + m. \quad (20)$$

Since $n_k = n_\varepsilon + n_\delta - n/3$, equation (20) can be taken as

$$n_k < (n_\varepsilon + m)/5. \quad (21)$$

Again, if n_k is chosen so as to satisfy this inequality, no other variables of equation (12) are obtained except $k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta}$.

Case (iv)

The equation (12) with modulo N gives the following polynomial:

$$f(x; y; z; w) \bmod N = e^3x + e^2y + ez + w + k_m. \quad (22)$$

The roots of this polynomial can be taken as x_0, y_0, z_0, w_0, where

$$x = d_{p1}d_{p2}d_{p3}$$

$$y = d_{p1}d_{p2}(k_{p3\alpha}k_{p3\beta} - 1) + d_{p1}d_{p3}(k_{p2\alpha}k_{p2\beta} - 1) + d_{p2}d_{p3}(k_{p1\alpha}k_{p1\beta} - 1)$$

$$z = d_{p1}(k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p2\alpha}k_{p2\beta} + 1) + d_{p2}(k_{p1\alpha}k_{p1\beta}k_{p3\alpha}k_{p3\beta} - k_{p3\alpha}k_{p3\beta} - k_{p1\alpha}k_{p1\beta} + 1) + d_{p3}(k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta} - k_{p2\alpha}k_{p2\beta} - k_{p1\alpha}k_{p1\beta} + 1)$$

$$w = k_{p1\alpha}k_{p1\beta}k_{p2\alpha}k_{p2\beta}k_{p3\alpha}k_{p3\beta} + k_0$$

The roots can be defined as x_0, y_0, z_0, w_0 for each of the polynomials if $|x_0| < X,\ |y_0| < Y,\ |z_0| < Z, |w_0| < W$ and $XYZW < N$ for some upper bounds $X,\ Y,\ Z\ and\ W$.

The upper bounds are:

$X = 2^{3n_\delta}$

$Y = 2^{3n_\delta + n_\varepsilon - n/3}$

$Z = 2^{3n_\delta + 2n_\varepsilon - 2n/3}$

$W = 2^{3n_\delta + 3n_\varepsilon - n}$

Using the above bounds, solving the equation (12) for $XYZW < \mathrm{N}$,

$$12n_\delta + 6n_\varepsilon < 3n. \qquad (23)$$

Since $n_k = n_\varepsilon + n_\delta - n/3$, equation (23) can be re-written as:

$$n_k < (6n_\varepsilon - n)/12. \qquad (24)$$

Again, if n_k is chosen so as to satisfy this inequality, $d_{p1} d_{p2} d_{p3}$ can be obtained and each value can be derived using factorization but with high complexity.

In summary, for the proposed scheme considered to be secure from improper selection of parameters, if the following conditions are satisfied while generating the keys.

1. $n_k > (6n_\varepsilon - n + m)/11$
2. $n_k > (9n_\varepsilon - n + 3m)/24$
3. $n_k > (n_\varepsilon + m)/5$
4. $n_k > (6n_\varepsilon - n)/12$
5. $n_\delta > 2m$
6. $n_\delta + n_\varepsilon = n_i + n/3$

2.3 Comparison with Rebalanced RSA CRT Scheme A+

The Rebalanced RSA CRT Scheme A by [16] was designed in a way such that the public exponent is chosen before the selection of prime numbers. Though it is flexible to adjust the selection of public exponent and private exponent according to the need, the key generation is a very time consuming job. Later, the Rebalanced RSA CRT Scheme A+ [16], worked towards faster key generation, but it was very slow in encryption. The Scheme A+ [16] is proved 1.7 times faster than the original Rebalanced RSA CRT[10]. In this Proposed Scheme, the key generation is constructed based on the Rebalanced RSA CRT Scheme A+ [16] but using multiple primes. To improve the encryption speed, instead of calculating a modular exponentiation to a large private key, a random integer is selected. To minimize the overhead of exponentiation part, this scheme provides a chance of computing the random integer calculation $(s+1)^e \bmod N$ in advance. At the same time, decryption is also improved by using ART instead of CRT. During encryption of the Proposed Scheme, there is one inversion and one multiplication. Computation of $(s+1)^e$ is ignored for complexity since it can be carried offline.

So,

$$En(C) = 20(2n^2 + 2n) + (2n^2 + 2n) \approx 42n^2$$

During decryption, three small decryption exponents are used in the Proposed Scheme. Let n_d be the bit length of the private exponents and n_p be the bit length of the modulus. Since the decryption exponent is taken smaller in Rebalanced RSA and also in the proposed scheme, let n_d =280 bits and n_p is the size of the modulus, i.e. n. Since the decryption involves three decryption calculations with smaller parameters and one multiplication,

$$Dec(C) = 3 \times (n_d + n_d/2) {n_p}^2 + O(n^2).$$

$$= 3 \times (n/i + n/2i) {n_p}^2 + O(n^2)$$

$$= (280/6)n^2 + O(n^2)$$

$$= 48n^2.$$

TABLE 1

COMPLEXITY OF SCHEME A+ AND PROPOSED SCHEME

Scheme	Encryption Complexity	Decryption Complexity
Scheme A+	n^3	$(3/4)n^3$
Proposed Scheme	$42n^2$	$48n^2$

Thus the proposed scheme is proved to be faster in terms of encryption and decryption when compared with the scheme, Rebalanced RSA CRT Scheme A+[16].The Rebalanced RSA CRT Scheme A+ variant algorithm takes 2 primes, while it is improved with multiple primes in the Proposed Scheme. As per [21], all the possible attacks go weak with increased number of primes. But factorization remains a threat if there are more and more multiple primes. Hence, it is recommended to use not more than 3 or 4 primes for 2048 and 4096 moduli respectively

2.4 COMPARISON WITH ERRCS

In ERRCS, Verma and Garg[17] extended the Rebalanced RSA scheme B [16] with multiple primes to improve the decryption speed. Flexibility is provided in choosing the public exponent according to the need of fast encryption or slow encryption. The Proposed Scheme is also similar to ERRCS where encryption is modified using some small parameters limiting to only one exponentiation and inverse calculation modulo N. Further, decryption is also improved limiting to the calculation of the small parameter modulo small Chinese remainder theorem (CRT) exponents of the private key and one multiplication modulo N. Aryabhatta theorem (ART) [23] is used in place of Chinese remainder theorem to solve the congruences of s_{pi} to get the value of S.The encryption complexity of the proposed scheme is nearly 4 times faster than ERRCS[17] and decryption complexity is nearly 3 times faster than ERRCS.

TABLE 2

COMPLEXITY OF ERRCS AND PROPOSED SCHEME

Scheme	Encryption Complexity	Decryption Complexity
ERRCS	$170n^2$	$140n^2$
Proposed Scheme	$42n^2$	$48n^2$

3 CONCLUSION

Rebalanced RSA is a better option for a setting where decryption is done on smaller devices and encryption is done on the end of a high server, for example smart phones etc [24], [25]. Since decryption is made simpler, the encryption phase bears more burden in this system making the process slower. This paper deals with a new scheme to improve the encryption speed of the Rebalanced RSA. This scheme is a modified approach of Rebalanced RSA-CRT Scheme A+[16]. This scheme proposes using multiple primes for key generation. As the key generation involves a number of parameters, the conditions for correct selection of parameters using lattice methods are drawn. Further, a randomized parameter is introduced having a goal of reduction in encryption time. This scheme is proved to offer a better encryption speed when compared to Rebalanced RSA-CRT Scheme A+ [16] and ERRCS[17].

REFERENCES

[1] G. Swain, "High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis", Security and Communication Networks, 2018

[2] G. Swain, G, "Digital image steganography using eight-directional PVD against RS analysis and PDH analysis", Advances in Multimedia, 2018

[3] G. Swain, "A data hiding technique by mixing MFPVD and LSB substitution in a pixel", Information Technology and Control, vol. 47, No.4, pp. 714-727, 2018

[4] R. Rivest, A. Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM , vol. 21, No. 2 ,pp. 120-126, 1978

[5] E.Suresh Babu, C. Naga Raju, M. H. M. Krishna Prasad, "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks", International Journal of Network Security, vol. 18, No. 2, pp.291-303, 2016

[6] B. Suneela, EV Krishna Rao, and KC Sri Kavya, "Design and implementation of MF-MB cancellation detection in transmission of physical layer network", Journal of Theoretical and Applied Information Technology, vol. 91, No. 1, pp. 202-209., 2016

[7] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges", Multimedia Tools and Applications, vol. 75, No. 21, pp.13541-13556., 2016

[8] D. Boneh and H. Shacham,"Fast Variants of RSA", CryptoBytes vo.,5., No. 1, pp.1-9, 2002

[9] VR Rentapalli, B. Sowjanya, B.T.P. Madhav, B. Madhavi, B. & K. Bhavani, "A novel transmission technique for interference management and mitigation in 3GPP LTE-advanced", Journal of Theoretical and Applied Information Technology, vol. 87, No. 1, pp. 47-53, 2016

[10] M.J. Wiener, "Cryptanalysis of short RSA secret exponents",IEEE Transactions on Information Theory, vol. 36, No. 3, pp. 553-558, 1990

[11] E S. Razia, and M.R. Narasingarao, "A neuro computing frame work for thyroid disease diagnosis using machine learning techniques",Journal of Theoretical and Applied Information Technology, vol. 95, No. 9, pp.1996-2005, 2017

[12] S. Razia, and M.R. Narasingarao. And P. Bojja, "Development and analysis of support vector machine techniques for early prediction of breast cancer and thyroid", Journal of Advanced Research in Dynamical and Control Systems, vol. 9, No. 9, pp. 869-878, 2017

[13] J. Amudhavel, P. Kathavate, LSS Reddy, and A. BhuvaneswariAadharshini, "Assessment on authentication mechanisms in distributed system: A case study. Journal of Advanced Research in Dynamical and Control Systems, vol. 9, No. 12, pp. 1437-1448, 2017

[14] B. T. P Madhav., MVK Reddy, MV Rao, CM. Krishna, PC Raj, and G. Jaya, "Quad band filtenna using split ring resonators to notch unwanted frequencies in medical application bands", Journal of Theoretical and Applied Information Technology, vol. 95, No.9, pp. 2070-2077, 2017

[15] V. Subba Reddy, M. Siva Ganga Prasad, and BTP Madhav, "Triple band notch tree structured fractal antenna for uwb applications', Journal of Advanced Research in Dynamical and Control Systems, vol.9, No. 14, pp.1755-1763, 2017.

[16] H-M. Sun, M-E. Wu, M.J. Hinek, C-T. Yang, and V.S. Tseng," Trading decryption for speeding encryption in Rebalanced-RSA", The Journal of Systems and Software, vol. 82,pp.1503-1512, 2009

[17] S. Verma, and D. Garg , "Improvement in RSA Cryptosystems", Journal of Advances in Information Technology, vol. 2, No. 3, pp.146-151, 2011

[18] V. Allam, and BTP Madhav, "A frequency reconfigurable antenna with bluetooth, wi-fi and WLAN notch band characteristics", International Journal of Engineering and Technology, vol. 7, No. 2, pp.127-130, 2018

[19] B.S. Alladi, and S. Prasad, " Big data life cycle: Security issues, challenges, threat and security model", International Journal of Engineering and Technology, vol. 7, No. 3, pp.100-103, 2018

[20] T. Kleinjung, K. Aoki, J.Franke, A.K. Lenstra, E. Thome, J.W. Bos, P. Gaudry, A. Kruppa, PL Montgomery, D. Osvik, H. teRiele, A. Timofeev, and P. Zimmermann, " Factorization of a 768-bit RSA modulus", Advances in Cryptology, Lecture Notes in Computer Science, vol.6223, pp. 333–350, 2010

[21] M.J. Hinek, " Low Public Exponent Partial Key and Low Private Exponent Attacks on Multi-prime RSA", Master's thesis, Dept. of Combinatories and Optimization, University of Waterloo, Canada, 2002

[22] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter, “Low-exponent RSA with related messages”, Lecture Notes in Computer Science, vol. 1070, pp.1–9, 1996
[23] Ch. Padmaja, V.S. Bhagavan, and B. Srinivas, “On using Aryabhatta Remainder Theorem to Decrypt a Message with RPrime and Rebalanced RSA”, International Journal of Engineering & Technology, vol. 7, No.2.7, pp.758-762, 2018
[24] T. Sajana and M.R. Narasingarao, “A comparative study on imbalanced malaria disease diagnosis using machine learning techniques”, Journal of Advanced Research in Dynamical and Control Systems, vol. 10, pp. 552-51, 2018
[25] T. Sajana and M.R. Narasingarao, “Classification of imbalanced malaria disease using naïve bayesian algorithm”, International Journal of Engineering and Technology, vol.7, pp. 786-790, 2018