IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

Improving Rebalanced RSA Against Chosen Ciphertext Attacks

Ch J.L. Padmaja[1*], V.S. Bhagavan[2], B. Srinivas[3]

[1]Research Scholar, Department of Mathematics, KLEF, Vaddeswaram, India
[2]Department of Mathematics, KLEF, Vaddeswaram, India
[3]Department of Technical Education, Amaravathi, India

[*]*Corresponding Author: padmajachivukula@gmail.com,*

Available online at: www.ijcseonline.org

Accepted: 29/Sept./2018, Published: 30/Sept./2018

***Abstract*—**RSA cryptosystem is the most widely used public key cryptosystem. There have been many variants to the original RSA proposed in the literature and Rebalanced RSA is one of such modified RSA cryptosystems. This paper provides new designs of Rebalanced RSA which are semantically secure against chosen ciphertext attack as well as adaptive chosen ciphertext attack. The proposed schemes are proved to be more efficient than other schemes like DRSA, Rebalanced RSA and standard RSA.

***Keywords*—**Ciphertext, Decryption, Encryption, Rebalanced RSA

I. INTRODUCTION

Public key cryptosystems (PKC) are of paramount importance in today's secure communications due to their dual key nature. The mathematical tools used in the algebraic structure of the PKC's provide a substantial security but at the same time they attract the attention of intruders trying to break those systems. RSA [1] is one of the most popular PKC's that are being used worldwide [2]. Its security lies in the problem of integer factorization. As it is not yet feasible to factorize a large composite number into its prime factors, RSA remains safe when large modulus is used [3].

Semantic Security just implies that a ciphertext should not reveal any valuable data about the plaintext. That is, in a semantically secure encryption framework, it is impossible to differentiate ciphertext from a random or arbitrary string. According to Goldwasser and Micali [4], a semantically secure encryption framework is said to be broken if an adversary can discover two messages m_0 *and* m_1 such that it can differentiate between their ciphertexts.

In chosen ciphertext attack (CCA), an adversary or cryptanalyst has access to decryption oracle, observes the ciphertext and tries to find out the corresponding plaintext. The objective of the cryptanalyst is to find the decryption key or encrypt the target ciphertext. If he fails to do so, then the system is deemed to be secure against chosen ciphertext attack. If the cryptanalyst fails to guess any partial information about the plaintext corresponding to the target ciphertext, then that system is said to be secure against adaptive chosen ciphertext attack (ACCA). To make the system immune against ACCA, there should appear no mathematical relationship between the plaintext and the ciphertext.

It is difficult to trust that a deterministic symmetric or public key cryptosystem can be semantically secure since one can process the encryption of every single conceivable message, and compare with the target ciphertext. The RSA cryptosystem is prone to this type of attack whereas OAEP and ElGamal are semantically secure [5].

Due to the slow execution nature of RSA with larger moduli, several faster variants were proposed in the literature [6]. Rebalanced RSA [7] was one of them which targets at fast decryption to enable it to be used even in smaller machines like cell phones [8].

As RSA and its faster variants are not semantically secure [9], two new schemes are proposed in this paper duly modifying the encryption and decryption procedures of Rebalanced RSA, which are secure against the CCA and ACCA. Proper hash function is utilized during encryption to hide s^{e+1}.

The Section II of this paper presents a new Scheme-I which is safe against chosen ciphertext attacks using a hash function. The Section III contains the presentation of a new Scheme-II using two hash functions which is a modification of the Scheme-I. The performance of the two schemes is

discussed in Section IV and Section V gives the conclusion of this research paper.

II. SCHEME-I

This scheme is based on ERSA-1 [9] that proposes the use of a hash function while encrypting the plaintext message which eventually makes the system semantically secure. Key generation for this scheme is similar to the Rebalanced RSA [7].

Key Generation

1. Generate two keys; public key $< N,\ e >$ and private key $< d_p, d_q, p, q >$ where, N is product of two distinct random primes p and q i.e., $N = p.q$ with each prime of bit length $(n/2)$ bits such that gcd $(p-1, q-1) = 2$.
2. Select two random integers d_p and d_q such that gcd $(d_p, p-1) = 1$, gcd$(d_q, q-1) = 1$ and $d_p = d_q \mod 2$.
3. Calculate d such that $d \equiv d_p \bmod p-1$ and $d \equiv d_q \bmod q-1$
4. Obtain e using $e = d^{-1} \bmod \phi(n)$

Encryption

To encrypt any message $M \in Z_N = \{0,\ 1,\ .....N-\ 1\}$, Sender chooses a random integer S such that $s \in Z_N{}^*$ which is a multiplicative group under modulo N and let h be a proper hash function. Sender computes,

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

$$C_2 = M.\ \mathrm{h}(s^{e+1}) \mod N \quad (2)$$

$$C_3 = h(M \parallel s) \quad (3)$$

where $M \parallel s$ denotes the concatenation of M and S.

The Sender then communicates the cryptogram (C_1, C_2, C_3) to the Receiver.

Decryption

Receiver computes,

$$s_p = C_1{}^{dp} \bmod p \quad (4)$$

$$s_q = C_1{}^{dq} \bmod q \quad (5)$$

and computes S.

$$M = C_2 / \mathrm{h}(s^{e+1}) \bmod N \quad (6)$$

Outputs M only if $C_3 = h(M \parallel s)$ is verified, otherwise outputs " ?"

III. SCHEME-II

This scheme is based on ERSA-2 [9] that proposes the use of two hash functions while encrypting the plaintext message which eventually makes the system semantically secure against CCA and ACCA.

Key Generation

The key generation is same as Scheme-I.

Encryption

To encrypt any message $M \in Z_N = \{0,\ 1,\ .....N-\ 1\}$, Sender chooses a random integer S such that $s \in Z_N{}^*$ which is a multiplicative group under modulo N and $h_1 : Z_N \to \{0,1\}^{s_1}$ and $h_2 : \{0,1\}^{s_1} \times Z_N \to \{0,1\}^{s_2}$ be two hash functions which output $s_1 -$ bit and $s_2 -$ bit numbers respectively. Sender computes,

$$C_1 = s^e \mod N \quad (7)$$

$$C_2 = \mathrm{M}.h_1(s^{e+1}) \bmod N \quad (8)$$

$$C_3 = h_2(M \parallel s) \quad (9)$$

and sends the cryptogram (C_1, C_2, C_3) to the Receiver.

Decryption

Receiver computes,

$$s_p = C_1{}^{dp} \bmod p \quad (10)$$

$$s_q = C_1{}^{dq} \bmod q \quad (11)$$

and computes S.

$$M = C_2 / h_1(s^{e+1}) \bmod N \quad (12)$$

Outputs the message M if $C_3 = h_2(M \parallel s)$, otherwise outputs "?"

IV. PERFORMANCE OF PROPOSED SCHEMES

Chosen Ciphertext Attack: Security of Scheme-I and Scheme-II in terms of security against chosen ciphertext attacks can be demonstrated as in the case of Pointcheval [10], since ERSA-1 and ERSA-2 are similar to DRSA-1 and DRSA-2 [10]. However, a considerable difference is that the proposed schemes are constructed over a problem that is proved equivalent to the RSA problem [9] and not used any conjecture or unproven assertions. If a message is encrypted multiple times using these schemes, every time different ciphertexts are computed since "s" is a random integer chosen and hence the values are different. If an intruder has access to decryption oracle and obtains the different ciphertexts, he/she cannot get a hint of plaintext.

Adaptive Chosen Ciphertext Attack: The Scheme-I and II gain semantic security against ACCA, in the circumstances where it is practically equivalent to the RSA problem. Attaching a tag to the set of ciphertexts makes the schemes secure against ACCA. Again, the security of these proposes schemes against ACCA can be demonstrated as in the case of DRSA [5]. Even smaller exponents can be used to obtain improved efficiency, however, public key exponent greater than 2^{67} is advised [10].

Efficiency: According to Pointcheval [10], DRSA is the most efficient scheme in this field. Since ERSA schemes are constructed similar to DRSA, the security of the proposed schemes can be compared with DRSA. In case of DRSA, there are two exponentiations carried both in encryption and decryption, i.e. $s^e \bmod N$ and $(s+1)^e \bmod N$. In the proposed schemes, both Sender and Receiver need to compute $s^e \bmod N$ and $s^{e+1} \bmod N$, i.e. the former is exponentiation and the latter is just one multiplication ($s^{e+1} = s^e \times s$).

These proposed schemes use the key generation similar to that of Rebalanced RSA, but use distinct encryption and decryption methods. With the use of the hash functions in encryption, these schemes offer semantic security while the Rebalanced RSA does not give any such security. Rebalanced RSA needs exponentiations done to the message M whereas the proposed schemes need exponentiations to a randomized parameter s rather than the message M itself. These computations, s^e and s^{e+1} can be done well in advance prior to the communication of information. So, the proposed schemes offer less computational time or greater speed online.

When compared to the classical RSA scheme, here the Sender performs one exponentiation to public key and the receiver needs to perform one exponentiation with small secret keys with one or two extra multiplications and/or computing hash functions. The proposed schemes are faster since they deal with exponentiations of randomly chosen integers which can be computed prior to the communication. Moreover, they do not exhibit any relationship between the plaintext and ciphertext.

DRSA [10] scheme is already faster compared to OAEP [11] in both encryption and decryption. Thus, the proposed schemes are also much faster than the standard OAEP encryption scheme.

V. CONCLUSION

RSA cryptosystem is an asymmetric key cryptosystem[12]. Given the trapdoor non-invertibility nature of the keys, RSA cryptosystem has become the most popular and widely used cryptosystem. Several modifications have been proposed to the original RSA cryptosystem to make it perform better in all the spheres of the encryption algorithm [13]. All of the Going in that way, this paper proposes some schemes which are semantically secure.

New designs are proposed in this paper introducing hash functions during the encryption process of the messages. Thus, the paper successfully presented two new schemes based on Rebalanced RSA and ERSA. When comparing the security and comparison analysis with DRSA, Rebalanced RSA and the standard RSA, these new methods are proved to make the system safe against chosen cipher text and adaptive chosen cipher text attacks. The proposed schemes are semantically secure against chosen ciphertext attacks and adaptive chosen ciphertext attacks in the standard model. In this way, it can be said that the proposed schemes are computationally less expensive in comparison to the DRSA scheme. Hence the proposed schemes are more efficient than that of DRSA, Rebalanced RSA and the standard RSA schemes.

REFERENCES

[1] 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.
[2] Ch. Padmaja, "Number theory: Backbone of RSA cryptography", Global Journal of Pure and Applied Mathematics, Vol.11, No.5, pp.3495-3500, 2015.
[3] Ch. Padmaja, B. Srinivas, and V.S. Bhagavan, "A Systematic Mapping Study of the Published Research on Cryptanalytic Attacks on RSA", International Journal of Pure and Applied Mathematics, Vol.119, No. 11, pp.283-291, 2018.
[4] S. Goldwasser and S. Micali, " Probabilistic Encryption", Journal of Computer and System Sciences, Vol.28, pp.270–299, 1984.
[5] S. Pradhan, "A Study of Public Key Cryptosystems Based on Factorization", Ph.D. thesis, Pt. Ravishankar Shukla University, Raipur, India, 2013.

[6] Ch. Padmaja, B. Srinivas, and V.S. Bhagavan, "On the Usage of Aryabhatta Remainder Theorem for Improved Performance of Rprime RSA", Journal of Theoretical and Applied Information Technology, Vol.96, No.9,pp.2505-2518, 2018.
[7] M.J.Wiener, " Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, Vol.36, No.3, pp.553-558, 1990.
[8] Ch. Padmaja, V.S. Bhagavan, and B. Srinivas, "Enhancing the performance of Rebalanced RSA", Journal of Computer and Mathematical Sciences, (In Press), 2018.
[9] H. Ghodosi, " An efficient public key cryptosystem secure against chosen ciphertext attack", Information system security, Lecture Notes in Computer Science, Vol. 4332, pp.303-314, 2007.
[10] D. Pointcheval, " New Public Key Cryptosystems Based on the Dependent–RSA Problems", In Proceedings of Eurocrypt'99, Lecture Notes in Computer Science, Vol.1592, pp.239-254, 1999.
[11] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption-How to Encrypt with RSA", Advances in Cryptology - Proceedings of Eurocrypt'94, Lecture Notes in Computer Science, Vol. 950, pp.92–111, 1994.
[12] S.Dubey,R.Jhaggar, R.Verma, and D. Gaur, "Encryption and Decryption of Data by Genetic Algorithm", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, No.3, pp.42-46.
[13] V. Kapoor, "Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number", International Journal of Scientific Research in Network Security and Communication, Vol.1, No.2, pp.35-38.

Authors Profile

Dr. V.S. Bhagavan is a Professor in Mathematics, KL University, Andhra Pradesh, India. He completed his Ph.D in Mathematics from Benarus Hindu University, India. His focus areas of research interest are Special functions, Cryptography and Lie groups. His research is acknowledged in several reputed international journals (SCI, Scopus, WOS). He has presented several papers at national and international conferences. He is a lifetime member in AP Mathematical Society.

Dr. B. Srinivas is Head of the Department, Department of Technical Education, Andhra Pradesh, India. He has done post graduation in Mathematics from Osmania University, Hyderabad, India. He completed his Ph.D in Mathematics from Motilal Nehru National Institute of Technology, Allahabad, India. His research is acknowledged in several international journals. He has presented several research papers at national and international level conferences. He is a lifetime member in Cryptology Research Society of India, Kolkata.

Mrs. Ch. JL Padmaja is a Lecturer in Mathematics in Government Polytechnic, Guntur, Andhra Pradesh, India. She has done post graduation in Mathematics from Dr. B.R.Ambedkar Open University, Hyderabad, India. She completed her M. Phil. in Applied Mathematics from Annamalai University, Tamil Nadu. She is presently pursuing Ph.D in Cryptography from KL University, Guntur, India. Her research is acknowledged in Scopus indexed international journals. She has presented papers at an international conference in Chennai, India. She is a lifetime member in Cryptology Research Society of India, Kolkata.

