Issue 3 volume 1,February 2013
ISSN 2249-9954

AN EFFICIENT PKC BASED ON RPRIME CRYPTOSYSTEM

SUSHMA PRADHAN, B. K. SHARMA

Abstract. An variant of RSA called RPrime RSA [4] proposed by Ceaser. Its decryption speed is 27 times faster than the standard RSA and 8 times faster than the QC RSA [10]. However due to the large encryption exponent, the encryption process becomes slower than the standard RSA. In this paper, we eradicate this problem by improving the design of RPrime RSA. Our PKC is semantically secure also.

1. Introduction

Since the mid-1970's, when public-key cryptography was first developed, the RSA Cryptosystem [11] has become the most popular cryptosystem in the world. Based on the believed difficulty of computing e^{th} roots modulo N, where N is the product of two large unknown primes, it is widely believed to be secure for large enough N . Since RSA can also be broken by factoring N, the security of RSA is often based on the integer factorization problem, which is and continues to be a well-studied problem. Currently, it is suggested that the bit length of N should be at least 1024 for RSA to be considered secure. Using the best known factoring algorithms, the expected workload of factoring a 1024-bit modulus is 280 which is currently believed to be infeasible. One of the reasons that RSA is so popular is its simplicity. Both encryption and decryption require only one modular exponentiation. To improve the efficiency of standard RSA scheme, many variants have been proposed. Boneh and Shacham [3] proposed a variant of RSA and gave a nice survey of all four variants (Batch RSA, MPrime RSA, MPower RSA, Rebalanced RSA). The result given by Boneh and Shacham [3] was further extended by Ceaser [4] and who proposed a fast variant of RSA scheme. He called it RPrime RSA. It is in fact, a combination of MPrime RSA [6] and Rebalanced RSA [3]. The theoretical speed up of RPrime RSA is about 4.8 times faster than the QC-RSA [10] for the moduli of 1024 bits and it is 27 times faster than standard RSA for 2048 bit moduli. Although, RPrime-RSA speed up the efficiency of decryption process, but due to the large encryption exponent e, the encryption speed becomes very slow. In this paper we extend the result given by Ceasar [4] to improve the efficiency of encryption process. In addition, our proposed cryptosystem is semantically secure where as RPrime is not semantically secure.

Next, Semantic Security is the notion of security which means that a cryptosystem should not reveal any useful information about the plaintext. That is, in a semantically secure encryption system, a cryptosystem is indistinguishable from a random string. The indistinguishability of encryptions, was first introduced by Goldwasser and Micali [7]. Under this notion of security, a semantically secure encryption system is said to be broken if the cryptanalyst can find two messages m_0 and m_1, such that it can distinguish between their cryptosystem.

2000 *Mathematics Subject Classification.* 94A60.
Key words and phrases. Public Key Cryptosystem, Semantic Security, QC-RSA, Equivalent- RSA Scheme, RPrime-RSA.

The rest of this paper is organized as follows. In next section , we first describe the RPrime RSA method which is the combination of (MPrime and Rebalanced RSA). In section 3, we introduce our proposed scheme and in section 4, we discuss the efficiency and security with comparison to the RPrime RSA.

2. RPrime-RSA:

In the above para we have mentioned that Ceaser [4] introduced an efficient variant of RSA by combining MPrime- RSA [6] and Rebalanced RSA [3]. He called this RPrime-RSA. In this scheme, Rebalanced RSA(modified for k primes) was used for key generation together with the decryption algorithm of MPrime RSA. Some other possibilities of combinations are also analyzed by him and concluded that RPrime is the better than all other combinations. The Key generation, Encryption and Decryption process of RPrime RSA is as follows:

2.1. **Key generation:** The key algorithm receives as parameter, the integer k, indicating the number of primes to be used. The key pairs(public and private) are generated according to the following steps:

(1) Chooses an integer $s \leq \lceil log\, n/k \rceil$.
(2) Generates k distinct random primes of $\lceil log\, n/k \rceil$ bits $p_1, p_2, p_3, ..., p_k$ with gcd $(p_1 - 1, p_2 - 1, ..., p_k - 1) = 2$ and calculate $n = p_1, p_2, p_3, ..., p_k$.
(3) Generate k random numbers of s bits $d_{p_1}, d_{p_2}, ...d_{p_k}$, such that gcd $(d_{p_i}, p_{i-1}) = 1$ $\forall i = 1, 2, 3, ...k$ and $d_{p_1} \equiv d_{p_2} \equiv ..... \equiv d_{p_k}\ mod\, 2$.
(4) Finds d such that $d \equiv d_{p_1}\ mod\,(p_1 - 1), d_{p_2}\ mod\,(p_2 - 1), ...d_{p_k}\ mod\,(p_k - 1)$.
(5) Calculate e such that $e \equiv d^{-1}\ mod\,(n)$.

The public keys for the receiver R are (e, n) and the private keys are $(p_1, p_2, p_3, ...p_k, d_{p_1}$, d_{p_2} , ..., $d_{p_k})$.

2.2. **Encryption:** The encryption process for the RPrime RSA is same as that for the standard RSA. To encrypt any plaintext M sender S computes $C = M^e\ mod\, n$, sends the ciphertext C to the receiver R.

2.3. **Decryption:** To decrypt the ciphertext C, the receiver R first calculate $M_i = C^{d_i}\ mod\, p_i$ for each $i = 1, 2, 3, ..., k$. Thus, R computes the plaintext $M(= C^d\ (mod\, n))$ with the help of above congruence equations via CRT. The use of CRT takes negligible time with comparison to k exponent because of the choice of primes.

3. Proposed Cryptosystem

Now we propose a cryptosystem to improving the encryption speed of RPrime RSA [4]. The key generation, encryption,and decryption algorithms are as follows:

3.1. **Key Generation:** To generate key the receiver R takes an integer $s \leq \lceil log\, n/k \rceil$ and executes the following steps:

(1) Generates k distinct random primes of $\lceil log\, n/k \rceil$ bits $p_1, p_2, p_3, ..., p_k$ with gcd $(p_1 - 1, p_2 - 1, ..., p_k - 1) = 2$ and calculate $n = p_1, p_2, p_3, ..., p_k$.
(2) Generate k random numbers of s bits $d_{p_1}, d_{p_2}, ...d_{p_k}$, such that gcd $(d_{p_i}, p_{i-1}) = 1$ $\forall\, i = 1, 2, 3, ...k$ and $d_{p_1} \equiv d_{p_2} \equiv ..... \equiv d_{p_k}\ mod\, 2$.
(3) Finds d such that $d \equiv d_{p_1} mod(p_1 - 1), d_{p_2} mod(p_2 - 1), ...d_{p_k}\ mod\,(p_k - 1)$.
(4) Calculate e such that $e \equiv d^{-1}\ mod\,(n)$.

Public key$=< n, e >$; **Private key**$=< p_1, p_2, p_3, ...p_k, d_{p_1}, d_{p_2}, ..., d_{p_k} >$.

3.2. **Encryption:** To encrypt any message $M \in Z_n$ where $Z_n = \{0, 1, ...n-1\}$, sender S chooses a random integer $l \in Z_n^*$ where Z_n^* is the multiplicative group under modulo n i.e set if all invertible elements under multiplication modulo n and computes
$C_1 = l^e \ (mod\, n)$
$C_2 = M\, l^{-1} \ (mod\, n)$
sends the ciphertext $(C_1,\ C_2)$ to the receiver R.

3.3. **Decryption:** To Decrypt the given message R use the secret key $p_1, p_2, ...p_k, d_{p_1}, d_{p_2}, ...d_{p_k}$ as below: R first computes $lp_1 = C_1^{d_{p_1}} mod p_1, ..., l_{p_k} = C_1^{d_{p_k}} : mod p_k$ and then he computes l from the above congruence equations via Chinese Remainder Theorem. Finally computes $M = C_2\, l \ mod\, n$.

3.4. **Example:**

(1) S chooses distinct random prime integers p_1=11, p_2=17, p_3=19, p_4=23 with gcd(10, 16, 18, 22)=2. Thus, $n = 11.17.19.23 = 81719$.

(2) Select $d_{p_1} = 3$; $d_{p_2} = 5$; $d_{p_3} = 7$; $d_{p_4} = 13$ such that gcd$(d_{p_i}, p_i - 1)$=1 $\forall$ $i = (1, 2, 3, 4)$ and $3\, mod\, 2 \equiv 5\, mod\, 2 \equiv 7\, mod\, 2 \equiv 13\, mod\, 2$.

(3) Find the value of d by computing $d \equiv 1\, mod\, 5;\ 2\, mod\, 8;\ 3\, mod\, 9;\ 6\, mod\, 11$ by using CRT we get $d = 6613$.

(4) Finally, compute $e = d^{-1}\ mod\, n = 27517$

Public key=$< 81719, 27517 >$; **Private**=$< 11, 17, 19, 23, 3, 5, 7, 13 >$.

Suppose sender S wants to encrypt the message $M = 11$, then first the sender S choose the random integer $l(5 \in Z_n^*)$ and compute $C_1 = l^e\, mod\, n = 5052$ and $C_2 = M\, l^{-1}\, mod\, n = 16346$. Hence the ciphertext (5052, 16346) is obtained.

To decrypt the given message the receiver R uses the secret key and first compute $lp_1 = C_1^{d_{p_1}}\ mod p_1, ..., l_{p_k} = C_1^{d_{p_k}}\ mod\ p_k$, i.e ; $lp_1 = 5052^3\ mod\ 11 = 5\ mod\ 11$, $lp_2 = 5052^5\, mod\, 17 = 5\, mod\, 11$, $lp_3 = 5052^7\, mod\, 19 = 5\, mod\, 11$, $lp_4 = 5052^{13}\, mod\, 11 = 5\, mod\, 23$ and then R get $l = 5$ via CRT. Finally, Receiver R recover the plaintext by computing $M = C_2\, l\ mod\, n = 11$

4. Security and Efficiency Analysis:

4.1. **Fast Computation:** In the RPrime-RSA scheme [3], the encryption exponent e is taken very large, hence the efficiency of encryption process of the RPrime-RSA cryptosystem becomes very slow. In our proposed scheme, since the pairs like $(l^e mod\, n, l^{-1} mod\, n)$ can be computed well in advance, therefore the encryption process requires only one multiplication modulo n, where as in the RPrime-RSA one exponentiation to the power e modulo n is required. In this way, we can say that our the encryption process is very fast with comparison to RPrime- RSA. Next, RPrime RSA is not semantically secure whereas our proposed cryptosystem is semantically secure.

4.2. **Semantic Secure:** The proposed cryptosystem is semantically secure against chosen plaintext attack is as follows. In order to determine any information about the plaintext M from the ciphertext (C_1, C_2), the attacker needs to have some information about $l^{-1}(mod\, n)$, where l is randomly chosen element in Z_n^*. The only way to ascertain any

information about the value of $l^{-1}(mod\, n)$ is to first compute l. It is not possible without knowing the secret key d. Since to determine the value of $l^{-1} mod\, n$, it is necessary to have complete information about l , as l is randomly chosen. Thus our scheme is semantically secure.

4.3. **Another efficiency factor:** Our scheme do not require any constraint on the size of the public key e. The security of our proposed scheme as well as that of Rebalanced RSA, depends on the security offered by the exponent d and on the size of the used primes(as MPrime RSA). We know that such private exponent d is large enough to become ineffective for the attacks of the small private exponents [2]. The attack on the small public exponents is not the problem, due to the size of the public exponent e which is generated by the generation algorithm. M.Jason Hinek [5] made an analysis of the partial key exposure attack on the MPrime RSA and verified that for three and four primes the attack becomes ineffective. Thus it would be same for our scheme also because primes are larger than four. This improves efficiency of our scheme

References

[1] M. Bellare, P. Rogaway, "Optimal Asymmetric Encryption How to Encrypt with RSA", in Advances in Cryptology - Proceedings of EUROCRYPT 94, vol. 950 LNCS, pp. 92-111, Springer- Verlag 1995.
[2] D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem", Notices of the American Mathematical Society, vol.46(2): pp:203213,1999.
[3] D. Boneh, H. Shacham, "Fast variant of RSA", RSA laboratories, 2002.
[4] Cesar Alison Monticro Paixao, "An efficient variant of the RSA cryptosystem", Cryptology ePrint Archive, pp. 159, 2003.
[5] M. J. Hinek,"New partial key exposure attacks on RSA revisited", Technical Report CACR 2004-2, Centre for Applied Cryptographic Research, University of Waterloo, 2004.
[6] Collins T, Hopkin D, Langford S. and Sabin M., Public key cryptographic apparatus and method. US patent ♯5, 848,159, 1997.
[7] S. Goldwasser, S. Micali, "Probabilistic encryption", Journal of Computer and System Sciences, Vol. 28, pp. 270-299, 1984.
[8] Hossein Ghodosi, "An efficeint public key cryptosystem secure against chosen ciphertext attack ", 2007
[9] D. Pointcheval, "New PKC based on the dependent RSA problem", LNCS EUROCRYPT'99, Vol. 1592, pp. 239-254, Springer Verlag, 1999.
[10] J. Quisquater, Couvruur, "Fast decyhpering algorithm for RSA public key cryptosystem", Electronics Letters, Vol. 01, pp. 905-907, 1982.
[11] R.L. Rivest, A. Shamir, L. Adlemann, "A method for obtaining digital signature and public key cryptosystem", Communication of the ACM, vol. 2, pp.120-126, 1978.
[12] M. Wiener, "Cryptanalysis of short RSA secret exponent", IEEE Trans. Inform. Theory, Vol. 36, pp. 553-55, 1990.

School of Studies in Mathematics, Pt.Ravishankar Shukla University Raipur - 492010 (C.G.), India