Improved PKC Provably Secure against Chosen Cipher text Attack

Sushma Pradhan[1] and Birendra Kumar Sharma[2]
[1]School of Studies in Mathematics, Pt. Ravi Shankar Shukla University, Raipur, Chhattisgarh
sushpradhan@gmail.com

[2]School of Studies in Mathematics, Pt. Ravi Shankar Shukla University, Raipur, Chhattisgarh
Sharmabk07@gmail.com

ABSTRACT

A new public key cryptosystem is presented which is based on Equivalent-RSA that is provably secure against adaptive chosen cipher text attack (as defined by Rackoff [22]).

KEYWORDS
RSA Cryptosystem; Semantic security; Chosen cipher text attack; Adaptive chosen cipher text attack; Mprime RSA; D-RSA; Equivalent RSA problem.

1. INTRODUCTION

Public key cryptosystems, in the sense of Diffee-Hellman [11], provide public access to the encryption key while the decryption key is kept secret by the recipient of the cipher text. The algebraic structure in the form of modern mathematical tools provides considerable security in a public key cryptosystem, but such system is not beyond the reach of attacker. The classical version of most popular public key cryptosystem RSA [23] is neither semantically secures nor is it secure against adaptive chosen chipper text attack.

Chosen Ciphertext Security- To assist the security of a public key cryptosystem against the Chosen Cipher text Attack (CCA), the assumption is that the cryptanalyst also has access to the decryption oracle. The cryptanalyst can select any cipher text, and observe the corresponding plaintext. The cryptanalyst aims to find out the secret key or encrypt a "target" ciphertext. A cryptosystem is said to be secure against CCA if the cryptanalyst fails in this attack.

Natural extension of CCA is, however the adaptive chosen ciphertext attack. It is defined by Rackoff and Simon [22]. A cryptosystem is said to be secure against the Adaptive Chosen Ciphertext Attack (ACCA) if the cryptanalyst fails even to obtain any partial information about the plaintext relevant to the "target" ciphertext.

One way of immunizing a cryptosystem against ACCA is that the encryption algorithm should destroy the mathematical relationship between the plaintext and its ciphertext. Moreover, the decryption algorithm must be designed in such way such that it does not output the result, if the result does not satisfy a predetermined structure. This way, every ciphertext does not become a good/acceptable input to the decryption oracle. In other words, finding an acceptable ciphertext implies that the message is known to the adversary (this is known as the Plaintext-Awareness [1]). However, if the adversary knows the message, he learns nothing from deciphering the ciphertext (i.e., the chosen ciphertext attack makes no sense).Since, definition of ACCA, several designs of pkc are introduced with claim to be secure from ACCA. This paper reviews most of

DOI : 10.5121/ijcsa.2013.3102

them and uses most recent encryption scheme given by Hossein Ghodosi [18], in order to propose encryption scheme secure from ACC and ACCA both having more e_ectively as compare to others.

To achieve our goal we organize this paper as follows. In section 2, we first give a brief review of previous works. We then review the results achieved by Pointcheval [13], since the proposed scheme follows a similar structure. In section 3, we explain the Equivalent RSA (ERSA) [18]. In section 4, we describe the MPrime RSA method. In section 5, we show how to construct secure systems according to basic scheme of ERSA scheme. Finally, in section 6 and 7, we conclude with the security and the efficiency performance of the proposed schemes.

2. RELATED WORK

Naor and Yung [20] have constructed a public key cryptosystem secured against CCA. Later, Dolev Dwork and Naor [12], and Rackoff and Simon [22] have which constructed cryptosystems was secured against ACCA. Although these schemes were provably secure but these were very inefficient and therefore found impractical

Next, attempt to design an efficient public-key cryptosystem secure against CCA was made by Damgard [10]. In this work two constructions, one based on any deterministic public key system and the other based on the ElGamal public key system, have been presented. However, there is no proof of security in this system (in fact, the work ends with an open problem; asking the reader to prove or disprove the assumption made in the paper). This scheme is secure against the "lunch-time" at-tack, but is not secure against ACCA [25, 26].

Zheng and Seberry [26] presented three methods for immunizing public key cryptosystems against ACCA. In [19], Lim and Lee have shown that, in some cryptosystems, Zheng-Sebberys method fails under known plaintext attacks. They then presented two schemes that are claimed to be secure against ACCA. However, both schemes were subsequently broken by Frankel and Yung [15].

Bellare and Rogaway [1] presented the OAEP concept, which is heuristically secure under the random oracle model (a hash function plays the role of random oracle).

Cramer and Shoup [9] who pointed out that, although the security under the random oracle model is valuable, it is not reliable. They presented a new public key cryptosystem, which is secure against ACCA under standard intractability assumptions. Their work was the best design of a public key cryptosystems secure against ACCA. However, Pointcheval [13] argued that Cramer and Shoups scheme [9] requires more than four exponentiations for an encryption, and presented a new scheme based on the dependent-RSA problem. Informally, the dependent-RSA problem of [13] states that "given m^e in an RSA system, find $(m+1)^e$ ". Their conjecture is that, this problem is hard. In order to achieve semantic security, they have defined another problem called the Decisional Dependent-RSA problem. These problems states that, for a randomly chosen r, two pairs (m^e, r) and $(m^e, (m+1)^e)$ are indistinguishable. Their conjecture is that this problem is intractable when e is greater than 260. Based on these conjectures, they have then presented the following schemes:

2.1 The DRSA-1 Encryption Scheme

This is a strengthened version of the DRSA encryption scheme for attaining security against ACCA. Let l be a security parameter, and $h: Z_n \times Z_n \to \{0,1\}^l$ be a hash function. The ciphertext of a message m is a triple (A, B, H), such that: $A = k^e; B = m \times (k+1)^e$ and H = h(m, k). Here, k is a random value. To decrypt the ciphertext, the receiver computes: $k = A^d (\mathrm{mod}\, n)$ and $m = B/(k+1)^e (\mathrm{mod}\, n)$ and then checks for equality H = h (m, k). If the equality is satisfied, then m is accepted to be the message; otherwise, the ciphertext is rejected. This scheme is to be secure against ACCA, since the probability of generating an acceptable ciphertext, without knowing the message, is negligible.

2.2 The DRSA-2 Encryption Scheme

This is similar to DRSA-1, but the resulting scheme is equivalent to the computational problem rather than to the decisional one. Let k_1 be the size of the plaintext, k_2 a security parameter, let $h_1: Z_n \to \{0,1\}^{k_1}$ and $h_2: \{0,1\}^{k_1} \times Z_n \to \{0,1\}^{k_2}$ be two hash functions. The ciphertext of a message m is a triple (A, B, H), such that:
$A = k^e; B = m \times h_1((k+1)^e \bmod n)$ and $H = h_2(m,k)$. To decrypt the ciphertext, the receiver computes:
$k = A^d (\mathrm{mod}\, n)$ and $m = B / h_1((k+1)^e \bmod n)$ and then checks for equality $H = h_2(m,k)$.
They have shown that this scheme is also non-malleable, and thus secure against ACCA.

3. ERSA Encryption Scheme

Hossein Ghodosi [18] designed public key cryptosystems which was secure against chosen ciphertext attacks. The main advantage of given schemes is that he employ a problem equivalent to the well-studied RSA problem, and thus their scheme do not rely on conjectures or unproven claims. Therefore, the resulting schemes are as secure as the RSA system. The Scheme is as follows:

Key Generation

An RSA system with public parameters n, e, where n is the RSA modulus and e is the encryption key. Let d be the encryption key and h be the proper hash function.

Encryption

To encrypt a message $0 \le m < n$, select $k \in Z_n^*$ and compute $a = k^e (\mathrm{mod}\, n)$ and $b = h(k^e + 1) \times m (\mathrm{mod}\, n)$ the ciphertext is (a, b).

Decryption

The recipient of the ciphertext (a, b) first computes $k = a^d (\mathrm{mod}\, n)$, and then retrieves the message, using $m = \dfrac{b}{h(k^e+1)} (\mathrm{mod}\, n)$.

It is not difficult to show that a ciphertext in ERSA system looks like a randomly chosen pair, since the first entry is a ciphertext of a random value in the original RSA and thus is indistinguishable from a random value. The second entry is the multiplication of the message, m, in the output of a hash function, and therefore is random. Note that in a random pair, one cannot find any logical relationship between two entries. While in ERSA system, there is a strong relationship between two entries of a ciphertext. This relationship, however, cannot be utilized in order to distinguish a ciphertext from a random pair, except one can solve the RSA problem. That is, shown by the following theorem.

Theorem1. If RSA problem is intractable, then a ciphertext in the ERSA system is indistinguishable from a random pair.

3.1 ERSA-1 Encryption Scheme

In order to achieve security against ACCA, a common technique is to attach a tag to the ciphertext.

Initialization: Consider an RSA system with public parameters (n, e) and the secret key d. Let h be a proper hash function.

Encryption

To encrypt a message $0 \le m < n$, select $k \in Z_n^*$, and compute, $a = k^e, b = h(k^e + 1) \times m$ and $c = h(m // k)$ where m//k denotes the concatenation of m and k. The ciphertext is (a, b, c).

Decryption

For this scheme we assume that the encryption algorithm is an oracle that works in the following way.

1) It computes $k = a^d \pmod n$, and then retrieves the message m, using $b = h(k^e + 1)$.
2) It outputs the message m if c = h(m//k).

As it can be seen, any modification to the second entry of the ciphertext implies some modification of the third entry; otherwise the encryption oracle will detect the modification. However, the third entry is a hash function. Because of the one-wayness property of the underlying hash function, it is intractable to know the output without knowledge of the input. But the input to this hash function is a concatenation of m and k. Hence, generating a good/acceptable ciphertext implies knowledge of the message. That is, the plaintext awareness property, which is equivalent to non-malleability, is achieved.

Theorem2. The ERSA-1 encryption scheme is semantically secure against ACCA.

3.2 ERSA-2 Encryption Scheme

Initialization

Consider an RSA system with public parameters (n; e). Let l be the size of the plaintext and $h_1(.), h_2(.)$ be two hash functions, such that $h_1 : Z_n \to \{0,1\}$.

Encryption

To encrypt a message $0 \le m < n$, the sender choose $k \in Z_n^*$

and computes $a = k^e (\mathrm{mod}\, n), b = m \times h_1((k^e + 1) \mathrm{mod}\, n)$ and $c = h_2(m // k)$. The ciphertext then is a triple (a, b, c).

Decryption

The recipient of the ciphertext first computes,

$k = a^d (\mathrm{mod}\, n)$ And $m = b = h_1((k^e + 1) \mathrm{mod}\, n)$

If $c = h_2(m // k)$ then it outputs the message m; otherwise, it outputs?

Theorem3. The ERSA-2 encryption scheme is semantically secure against adaptive chosen ciphertext attack.

4. Mprime RSA-(Multi-prime RSA)

Mprime RSA was introduced by Collins [7], who modified the RSA modulus so that it consists of k primes $N = p_{1,} p_{2,} \ldots\ldots p_k$ instead of the traditional two prime's p and q. The key generation, encryption and decryption algorithms are as follows:

Key generation

The key generation 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) Compute k distinct primes $p_1, p_2, \ldots p_k$, each one $\left\lceil \frac{\log n}{k} \right\rceil$ bits in length and $N = \prod_{i_1}^{b} p_i$.

(2) Compute e and d such that $d = e^i \mathrm{mod}(N)$, where $\gcd(e, \phi(N)) = 1$, $\phi(N) = \prod_{i=1}^{b} (p_i - 1)$.

(3) For $1 \le i \le k$, compute $d_i = d \,\mathrm{mod}(p_i - 1)$.

Encryption

Given a public key N, e_i and a message $m \in Z_n$, encrypts M exactly as in the original RSA, thus $c = M^e \,\mathrm{mod}\, N$.

Decryption

To decrypt a ciphertext C, first calculate $M_i = C^{d_i} \,\mathrm{mod}\, p_i$ for each i, $1 \le i \le k$.

Next, apply the CRT to the Mi's to get $M = C^d \,\mathrm{mod}\, N$.

5. Proposed Schemes Secure Against CCA and ACCA

Now we propose a new scheme which is secure against the ACC and ACCA in order to achieve in distinguish ability of a ciphertext with a random pair, we employ a proper hash function to hide K^{e+1} as follows:

5.1 Scheme 1

This scheme is similar to ERSA basic scheme, but it utilizes a hash function and also the key generation is similar to MPrime RSA. The scheme works as follows:

Key Generation

Let the key will be generated by using the key generation of Multiprime RSA scheme:

The key generation 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) Compute k distinct primes $p_1, p_2, \ldots p_k$ each one $\left\lceil \frac{\log n}{k} \right\rceil$ bits in length and $N = \prod_{i_1}^{b} p_i$

(2) Compute e and d such that $d = e^i \bmod(N)$, where $\gcd(e, \phi(N)) = 1$, $\phi(N) = \prod_{i=1}^{b}(p_i - 1)$.

(3) For $1 \le i \le k$, compute $d_i = d \bmod(p_i - 1)$.

Encryption

To encrypt a message $0 \le m < n$, Let L be a security parameter, $h : Z_n \times Z_n \to \{0,1\}^l$ be a hash function and select $k \in Z_n^*$ and compute $C_a = k^e (\bmod n)$ and $C_b = h(k^e + 1) \times m (\bmod n)$ the ciphertext is (C_a, C_b).

Decryption

The recipient of the ciphertetx (C_a, C_b) first computes $k = a^d (\bmod n)$, and then retrieves the message, using $m = \frac{C_b}{h(k^e + 1)} (\bmod n)$.

5.2 Scheme2

Key Generation

The key generation is same as scheme 1.

Encryption

To encrypt a message $0 \le m < n$, select $k \in Z_n^*$, and compute, $C_a = k^e, C_b = h(k^e + 1) \times m$ and $C_c = h(m // k)$ where m//k denotes the concatenation of m and k. The ciphertext is (C_a, C_b, C_c).

Decryption

For this scheme we assume that the encryption algorithm is an oracle that works in the following way.

1) It computes $k = C_a^{\,d} (\bmod n)$, and then retrieves the message m, using $C_b = h(k^e + 1)$.
2) It outputs the message m if c = h (m//k).

5.3 Scheme3

Key Generation

The key generation is same as scheme 1.

Encryption

To encrypt a message $0 \le m < n$, the sender choose $k \in Z_n^*$

And computes $c_a = k^e (\mathrm{mod}\, n), C_b = m \times h_1((k^e + 1) \mathrm{mod}\, n)$ and $C_c = h_2(m // k)$. The ciphertext then is a triple (C_a, C_b, C_c).

Decryption

The recipient of the ciphertext first computes,

$k = C_a^{\,d} (\mathrm{mod}\, n)$ And $m = C_b = h_1((k^e + 1) \mathrm{mod}\, n)$

If $C_c = h_2(m // k)$ then it outputs the message m; otherwise, it outputs?

6. Security of the Proposed Scheme

(1) Semantic Secure- Security of ERSA, ERSA-1, and ERSA-2 encryption schemes (from the point of view of semantical security and security against chosen ciphertext attacks) can be demonstrated in the way of Pointchevals work [13], since these schemes are similar to DRSA, DRSA-1, and DRSA-2. In our basic scheme, the ciphertext (ke;m_ ke+1) does not help an opponent to learn any useful information about the message. That is, dividing the second entry by the first entry and/or computing the greatest common divisors of these two items gives absolutely no useful information to the opponent.

(2) Partial Key Exposure Attack- We know that such private exponent d is large enough to become ineffective for the attacks of the small private exponents [3]. The attack on the small public exponents is also not a problem, due to the size of the public exponent e which is generated by the generation algorithm. M.Jason Hinek [16] made an analysis of the partial key exposure attack on the MPrime RSA and verified that for three and four primes the attack becomes inffective. Thus it would be same in our scheme also.

(3) Random Oracle Model- If we consider the security in the random oracle model, the scheme-1 reaches the security against adaptive chosen-ciphertext attacks with an same our efficiency.

(4) ***ACC-Attack-*** However, the most interesting scheme is the Scheme-2 cryptosystem that reaches semantic security both against adaptive chosen-ciphertext attacks, in a situation where it is practically equivalent to the RSA problem. Indeed, a smaller exponent, such as e = 65537 (or even 3), can be used, hence an improved efficiency is obtained with N = 1024, this scheme is already faster than OAEP, for both encryption and decryption. This scheme can gain higher rates, and become much faster than the original RSA encryption scheme.

7. Efficiency Performance

- Pointcheval [13] has claimed that his scheme is the most efficient scheme to date in this field. Here, if we compare the efficiency of our schemes with his work, thus we find that both schemes

have similar structures therefore it is easy to compare their efficiency. In [13], the sender and the receiver each needs to perform two exponentiations. This is due to calculation of k^e and $(k+1)^e$ which must be done by both, the sender and the receiver. In our scheme, although the sender and the receiver compute k^e and $(k+1)^e$, the calculation of $(k+1)^e$ needs just one multiplication $i.e.(k+1)^e = k^e \times k.$

- Another efficiency factor in our schemes is that our schemes do not require any constraint on the size of the public-key e. However, in order to achieve reasonable level of security in [13], it has been conjectured that the chosen e must be larger than 260.

- Altogether, the efficiency of our scheme is comparable to the classical RSA system. The sender needs to perform one exponentiation (to the size of the public key), and the receiver also needs to perform one exponentiation (to the size of the secret key) with one or two extra multiplications and/or computing hash functions.

8. Conclusion

We have presented three new schemes with security proofs. The proposed cryptosystem is semantically secure against \chosen ciphertext attacks in the standard model, relative to a new difficult problem (the inversion problem is equivalent to RSA in many cases), with an encryption rate 6 times faster than El-Gamal (with similar security levels: RSA-1024 bits vs. El-Gamal-512 bits). In this way, we conclude that the proposed scheme is computationally less expensive with comparison to the ERSA scheme. Hence our proposed scheme is more efficient than that of the ERSA scheme.

REFERENCES

[1] M. Bellare, P. Rogaway, (1994) “Optimal Asymmetric Encryption How to Encrypt with RSA,”, Advances in Cryptology EUROCRYPT 94 , Vol. 950, LNCS, pp. 92-111.

[2] D. Bleichenbacher, (1998) “Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS-1 “, Advances in Cryptology CRYPTO 98 , Vol. 1462 LNCS, pp. 1-12.

[3] D. Boneh, (1999) “Twenty Years of Attacks on the RSA Cryptosystem”, Notices of the American Mathematical Society, Vol.46 (2), pp203-213.

[4] D.Boneh, G. Durfee and Y. Frankel, (1998) “Exposing an RSA private key given a small fraction of its bits”. Advances in cryptology- ASIACRYPT' 98, Vol. 1514, LNCS, pp 25-34.

[5] R. Canetti, O. Goldreich, and S. Halevi, (1998) “The Random Oracle Model, Revisited”, 30th Symposium on the Theory of Computing (STOC).
.

[6] Cesar Alison Monticro Paixao, (2003) “An efficient variant of the RSA cryptosystem”, Cryptology ePrint Archive, pp. 159.

[7] T. Collins , D. Hopkin , Langford S. and Sabin M.,(1997) “Public key cryptographic apparatus and method”. US patent 5.

[8] J. Coron, D. Naccache, Y. Desmedt, A. Odlyzko, J.P. Stern, (2006) “Index Calculation Attacks on RSA Signature and Encryption Designee ", Codes and Cryptography, Vol. 38, pp. 41-53.

[9] R. Cramer and V. Shoup, (1998) “A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack ", Advances in Cryptology CRYPTO 98, vol. 1462, LNCS, pp13-25.

[10] I. Damgard, (1992) “Towards Practical Public Key Systems Secure Against Chosen Ciphertext attacks ", Advances in Cryptology CRYPTO 91, Vol. 576, LNCS, pp 445-456, .

[11] W. Diffie and M. Hellman, (1976) “New Directions in Cryptography", IEEE Trans On Inform Theory, vol. IT-22, pp. 644-654.

[12] D. Dolev, C. Dwork, and M. Naor, (1991) “Non-Malleable Cryptography", 23rd Annual Symposium on the Theory of Computing (STOC), pp 542-552.

[13] D. Pointcheval, (1999) "New Public Key Cryptosystems Based on the Dependent-RSA Problem ", Advances in Cryptology EUROCRYPT 99, Vol. 1592, LNCS, pp 239-254.

[14] T. ElGamal, (1985) “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms ", IEEE Trans. on Inform. Theory, Vol. IT-31, pp 469-472.

[15] Y. Frankel and M. Yung, (1995) “Cryptanalysis of the Immunized LL Public Key Systems ", Advances in Cryptology CRYPTO 95, Vol. 963 , LNCS, pp 287-296.

[16] M. J. Hinek, (2004) ”New partial key exposure attacks on RSA revisited", Technical Report CACR 2004-2, Centre for Applied Cryptographic Research, University of Waterloo.

[17] S. Goldwasser, S. Micali, (1984) “Probabilistic Encryption ", Journal of Computer and System Sciences, Vol. 28, pp 270-299.

[18] Hossein Ghodosi, (2007) “An efficeint public key cryptosystem secure against chosen ciphertext attack ",Information system security, Vol-4332 (LNCS), pp 303-314.

[19] C. Lim , P. Lee, (1994) “Another Method for Attaining Security Against Adaptively Chosen Ciphertext Attacks", Advances in Cryptology CRYPTO 93, Vol. 773 , LNCS , pp. 420-434.
.
[20] M. Naor, M.Yung, (1990) “Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks”, 22nd Annual ACM Symp. on Theory of Computing, pp. 427-437.

[21] T. Okamoto and D. Pointcheval, (2001) “RSA-REACT: An Alternative to RSA-OAEP", Proceedings of Second NESSIE Workshop, Egham, UK.

[22] C. Racko_, D. Simon, (1992) “Noninteractive Zero-knowledge Proof of Knowledge and Chosen Ciphertext Attack ", Advances in Cryptology CRYPTO 91 , vol. 576, LNCS, pp. 433-444.

[23] R. Rivest, A. Shamir, L. Adleman, (1978) “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, pp. 120 -126.

[24] V. Shoup, R. Gennaro, (1998) “Securing Threshold Cryptosystems against Chosen Ciphertext Attack, in Advances in Cryptology - Proceedings of EUROCRYPT98 (K. Nyberg, ed.), Vol. 1403 of Lecture Notes in Computer Science, pp. 116.

[25] Y. Tsiounis, M. Yung, (1998) “On the Security of ElGamal based Encryption”, Proceedings of the First International Workshop on Practice and Theory in Public Key cryptography (PKC 98), Vol. 1431, LNCS, pp. 117-134.

[26] Y. Zheng , J. Seberry, (1993) “Practical Approaches to Attaining Security against Adaptive Chosen Ciphertext Attacks”, Advances in Cryptology CRYPTO 92, Vol. 740 , LNCS, pp292-304.

Authors

Sushma Pradhan received the B.Sc, M.Sc and M.Phill degree in Mathematics Pt. Ravi Shankar Shukla University, Raipur, Chattigarh, India in 2002, 2004 and 2007. She joined School of Studies in Mathematics, Pt. Ravi Shankar Shukla University, and Raipur, India for her Research work. She is a life time member of Cryptology Research Society of India (CRSI). Her area of interest is Public Key Cryptography and Integer factorization Problem.

Birendra Kumar Sharma Professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.