On DRSA Public Key Cryptosystem

Sahadeo Padhye
School of Studies in Mathematics, Pandit Ravishankar Shukla University, India

Abstract: *The standard RSA cryptosystem is not semantically secure. Pointcheviel proposed a variant of RSA cryptosystem with the property of semantic security by introducing a new problem known as DRSA problem. He called it DRSA scheme. In this paper, we underlined a shortcoming of that scheme and proposed an alternative DRSA public key cryptosystem.*

Keywords: *Public key cryptosystem, RSA, DRSA, semantically secure.*

Received May 26, 2005; accepted August 1, 2005

1. Introduction

The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published "New Direction in Cryptography" [5]. This paper introduced the revolutionary concept of public key cryptosystem and also provided a new and ingenious method for key exchange, its security depends on the intractability on the discrete logarithm problem. In such a system, each user secretly obtains a crypto cell (E, D) and then publishes the encryptor E in a public file. The user keeps secret the details of his corresponding decryption procedure D. Clearly, the central requirement of such a system is that it is prohibitively difficult to figure out the decryptor D = E^{-1} from a knowledge of E, but D and E are easy to compute. In 1978, Ravist, Shamir and Adleman discovered the first practical, the most popular public key system, and a signature scheme known as RSA [13] using the idea of Diffie-Hellman key exchange protocol. The security of RSA scheme was based on factoring the product of two large prime numbers, which is a hard mathematical problem.

The efficiency and security are two important goals for any cryptosystem. To get the details about the all kinds of attacks and security notions, we refer the reader to the paper by Bellare *et al.* [2]. In 1984, Goldwasser and Micalli [8] defined a security notion, that an encryption scheme should satisfy, namely semantic security. This notion means that the ciphertext does not leak any useful information about the plaintext. The encryption scheme proposed by ElGamal [7] based on the Diffie-Hellman [5] problem was semantically secure. Its semantic security was related to the decisional Deffie-Hellmann problem [5]. However, because of the computational load, this scheme never became very popular. The speed of the standard RSA cryptosystem is very slow [page-469, 12] and several attacks [6] on RSA cryptosystem were identified. Hence, to increase the security and/or efficiency of the standard RSA cryptosystem other variants of RSA were developed. The standard RSA cryptosystem was not semantically secure. Although, its variants such as [1, 4, 10] were semantically secure against the chosen plaintext attack and chosen ciphertext attack but not all of them were more efficient than the ElGamal [7] encryption scheme. Pointcheviel [11] proposed a new DRSA (Dependent-RSA) problem and introduced an efficient RSA version of ElGamal encryption with some security properties, namely semantically security against chosen-plaintext attacks. The scheme given by Pointcheviel was 6 times faster than the ElGamal encryption scheme. Here, we demonstrate a shortcoming of DRSA. Further, we suggest a new scheme to overcome such shortcoming.

2. DRSA Problem

DRSA problem means "dependent RSA problem". To get the details about the DRSA problem, any one can refer to the papers [3, 9, 11]. Certain definition and results are given below.

Definition 2.1: *Computational Dependent-RSA (C-DRSA (n, e)).*
To determine the value of $(k + 1)^e \bmod n$ for given $k^e \bmod n$ where k is randomly chosen element in Z_n^* is known as C-DRSA problem. The success probability of an adversary A is denoted by Succ (A) and defined by:

$$\begin{aligned}\text{Succ}(A) = \Pr\ [&A\,(k^e \bmod n)\\ &= (k+1)^e \bmod n \mid k \leftarrow Z_n^*\ ]\end{aligned}$$

The decisional version of this problem defined by Decision Dependent RSA problem (D-DRSA).

Definition 2.2: The Decisional Dependent-RSA (D-DRSA (n, e)).
Distinguish the two distributions:

$$R_{and} = \{(\alpha, \gamma) = (k^e \bmod n\ ,\ r^e \bmod n\ ) \mid k, r \leftarrow Z_n^*\}$$

DRSA = $\{(\alpha, \gamma) = (k^e \bmod n, (k + 1)^e \bmod n) \mid k \leftarrow Z_n^*\}$.

The advantage of a distinguisher A denoted by Adv (A) and defined by:

Adv (A) = $|\Pr_{\text{Rand}} [A (\alpha, \gamma) = 1] - \Pr_{\text{DRSA}} [A (\alpha, \gamma) = 1] |$

Definition 2.3: Extraction Dependent-RSA (E-DRSA). A problem to determine the value k for given k^e mod n and $(k + 1)^e$ mod n is known as Extraction Dependent RSA (E-DRSA) problem.

In briefly, to determine the value of $(k + 1)^e$ mod n for given k^e mod n is known as computational DRSA problem and to distinguish the distribution (k^e mod n, $(k + 1)^e$ mod n) and (k^e mod n, C^e mod n)| k , c Z_n^*} is known as decisional DRSA problem. It can be easily proved that the extraction of e^{th} root is easier to solve than the computational dependent RSA problem and extraction dependent RSA problem together.

Theorem 2.1: Breaking the RSA problem is computationally equivalent to the breaking the C-DRSA and E-DRSA problem together both [11].

In the light of extraction dependent RSA problem and the theorem 2.1, we state the following theorem:

Theorem 2.2: There exists a reduction from the RSA problem to the computational dependent RSA problem in O ($|n|^2$, $e \times |e|^2$) time [11].

3. DRSA Scheme

This scheme was given by Pointcheviel [11] and it is based on the computational C-DRSA and decisional D-DRSA problem. The protocol for DRSA system is as follows:

3.1. Key Generation

The key generation for DRSA scheme is the same as that for the standard RSA scheme. To generate keys for DRSA scheme, the receiver (Bob) chooses two large primes p and q and computes $n = pq$. Bob then determines an integer e less than and relatively prime to n and computes an integer d such that ed 1 mod Φ (n). The public key for the Bob is (e, n) and the secret key is d, respectively. The prime p and q are also kept secret.

3.2. Encryption

To encrypt any plaintext M $\in Z_n$, sender (Alice) first randomly selects an integer $k \in Z_n^*$ and sends the complete ciphertext (C_1, C_2) to the Bob where:

$C_1 = k^e \bmod n$
$C_2 = M (k + 1)^e \bmod n$

3.3. Decryption

To decrypt the ciphertext (C_1, C_2), Bob first computes $C_1^d \bmod n = k$ and then he obtains the original plaintext by computing $M = C_2 / (k + 1)^d \bmod n$.

4. Improved DRSA Scheme

In the DRSA scheme, for the decryption process receiver has to compute $(k + 1)^{-1}$ mod n for given $k \in Z_n^*$. It is possible only if $k \in Z_n^*$ implies $k + 1 \in Z_n^*$. This is not necessarily always being true. If the sender accidentally chooses k such that $k + 1$ is not invertible then the receiver cannot get the required plaintext using the decryption process proposed by Pointcheviel [11]. To deal with this situation we are giving two suggestions for the DRSA scheme. First, either sender (Alice) advised to choose k such that k, $k + 1 \in Z_n^*$ and uses the same protocol as given by Pointcheviel. Second, alternatively user (sender and receiver) proceed as follow.

4.1. Encryption

To encrypt any plaintext, M $\in Z_n$ sender (Alice) first randomly selects an integer $k \in Z_n^*$ and computes:

$C_1 = (k + 1)^e \bmod n$
$C_2 = M k^e \bmod n$

Then she sends the complete ciphertext (C_1, C_2) to the receiver (Bob).

4.2. Decryption

After having the ciphertext (C_1, C_2), Bob computes the original plaintext M as follows:

$k = (C_1^d \bmod n) - 1$
$M = C_2 / k^e \bmod n$

A simple example in support of our comments:

Let $p = 5$ and $q = 11$, $n = 55$, $\phi(n) = 40$, $e = 3$, $d = 15$.

Z_n^* = {1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 21, 23, 24, 26, 27, 28, 29, 31, 32, 34, 36, 37, 38, 39, 41, 42, 43, 46, 47, 48, 49, 51, 52, 53, 54}.

Here we see that for k = 4, 9, 10, 14, 19, 21, 24, 29, 32, 34, 39, 43, 49, $(k + 1) \notin Z_n^*$.

5. Conclusion

Above, we have highlighted the shortcoming of the DRSA scheme. We remove it by proposing a condition for choosing the random element k and further consequently a new way for encryption as well as decryption process.

Acknowledgement

This work is supported by CSIR (JRF) Scheme-2002, India. Author is also thankful to Prof. Sharma B. K. for his kind suggestion.

References

[1] Bellare M. and Rogaway P., "Optimal Asymmetric Encrytion: How to Encrypt with RSA," *in Proceedings of Eurocrypt'94*, LNCS 950, Springer Verlag, pp. 92-111, 1995.

[2] Bellare M., Desai A., Pointcheval D. and Rogaway P., "Relation Among Notions of Security for Public Key Encryption Schemes," *in Proceedings of Cryto'98*, LNCS 1462, Springer Verlag, pp. 26-45, 1998.

[3] Coppersmith D., Franklin M., Patarin J., and Reiter M., "Low Exponent RSA with Related Messages," *in Proceedings of Eurocrypt'96*, LNCS 1070, Springer Verlag, pp. 1-9, 1996.

[4] Cramer R. and Shoup V., "A Practical Public Key Cryptosystem Provably Secure Against Chosen Ciphertext Attack," *in Proceedings of Crypto'98*, LNCS 1462, Springer Verlag, pp. 13-25, 1998.

[5] Diffie W. and Hellmann M., "New Direction in Cryptography," *IEEE Transaction on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[6] Don B., "Twenty Year Attacks on RSA Cryptosystem," *Notice of American Mathematical Society*, pp. 203-213, 1999.

[7] ElGamal T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transaction on Information Theory*, vol. C.IT-31, no. 4, pp. 469-472, July 1985.

[8] Goldwasser S. and Micali M., "Probabilistic Encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270-299, 1984.

[9] Hasted J. "Solving Simultaneous Modular Equations of Low Degree," *SIAM Journal of Computing*, vol. 17, pp. 336-341, 1988.

[10] Okamoto T. and Uchiyama S, "A New Public Key Cryptosystem as Secure as Factoring," *in Proceedings of Eurocrypt'98*, LNCS 1403, Springer Verlag, pp. 308-318, 1998.

[11] Pointcheval D., "New Public Key Cryptosystem Based on the Dependent-RSA Problem," *in Proceedings of Eurocrypt'99*, LNCS 1592, Springer Verlag, Berlin Hoidelberg, pp. 239-254, 1999.

[12] Schneier B., *Applied Cryptography*, John Wiley & Sons, 1996.

[13] Rivest R. L., Shamir A., and Adlemann L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystem," *Communication of the ACM*, vol. 1, no. 2, pp. 120-126, 1978.

Sahadeo Padhye received his BSc and MSc degree in mathematics form Pandit Ravishankar Shukla University, India in 1999 and 2001, respectively. The Council of Scientific and Industrial Research (CSIR), India has granted him Junior Research Fellowship (2002-2004). He then joined School of Studies in Mathematics, Pandit Ravishankar Shukla University, India for his research work. He is a member of Cryptology Research Society of India (CRSI). Currently, he is working as a senior research fellow of CSIR, India at the same university in the field of public key cryptography.