A Server Assisted Authentication Protocol for Detecting Error Vectors

Cheng-Chi Lee‡ Min-Shiang Hwang† I-En Liao‡
Department of Management Information System, National Chung Hsing University†
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw
Department of Computer Science, National Chung Hsing University‡
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Abstract

This articel presents a server assisted authentication protocol for RSA signature and two cryptanalysis of the protocol. An improved protocol is also proposed for extending the previous server assisted authentication protocol for RSA signature to detect the one-round active attack.
Keywords: Server assisted, cryptanalysis, RSA, cryptography.

I Introduction

The RSA scheme is one of the most popular digital signature algorithms [2, 10]. The security of this scheme is based on solving the factoring problem. We briefly introduce the RSA signature scheme as follows. Suppose a modulus goes $n = p \times q$, where p and q are two large primes. On the other hand, e and d denote a signer's public key and private key, respectively, such that $e \times d \bmod \phi(n) \equiv 1$, where $\phi(n) = (p-1)(q-1)$. The RSA signature of a message M is $S = M^d \bmod n$. The signature verification is performed by checking the equation $M = S^e \bmod n$.

To reach a high security standard, d, n, and M are usually set to be 512 bits or 1024 bits. It is a heavy load of computation for a client (e.g. terminal, personal computer, or smart card). To make things easier, Matsumoto et al. proposed a variety of protocols to speed up secret computations by making good use of the computing power of auxiliary devices in small pieces of computing equipment, such as a smart card [9]. For example, a smart card facing the task of calculating an RSA signature ($M^d \bmod n$) requires the computational assistance from a powerful server. Since then, several studies have been proposed to address this problem [3, 5, 6, 7, 8]. Anderson tried a one-round active attack on Matsumoto et al.'s protocol [1] and showed that this attack could disclose the private key d of the client by way of the server. However, Hwang pointed out Anderson's attack can be easily detected by the client (cardholder) and proposed another attack on Matsumotot et al.'s protocol [4].

In this article, we shall not only propose a revised version of Matsumoto et al.'s protocol, but also propose a detecting method against Anderson's and Hwang's attacks. We show that their attacking method also can be easily detected by the client.

II Review of Matsumoto et al.'s Protocol

In this section, we shall briefly review Matsumoto et al.'s protocol [9], and Anderson's cryptanalysis [1] and Hwang's cryptanalysis of Matsumoto et al.'s protocol [4].

2.1 Matsumoto et al.'s Protocol

Assume that a client wants to obtain a digital signature $S = M^d \bmod n$, where M is a message, d is the client's private RSA key, and n is the client's public modulus.

1. The client randomly breaks down d as follows.

$$d = \sum_{i=0}^{k} d_i w_i \bmod \phi(n), \tag{1}$$

   where $\phi(n)$ is the Euler quotient function, $D = [d_0, d_1, d_2, \ldots, d_k]$ denotes a set of integer vectors where $1 \leq d_i < n$, and $W = [w_0, w_1, w_2, \ldots, w_k]$ is a set of binary weight vectors.

2. The client sends M, D, and n to the server.

3. After receiving (M, D, n), the server computes the following integer vectors $Z = [z_0, z_1, z_2, \ldots, z_k]$, and sends them to the client.

$$z_i = M^{d_i} \bmod n, for i = 1, ..., k. \tag{2}$$

4. After receiving Z, the client can derive the signature S from the following equation.

$$S = \prod_{w_i=1}^{k} z_i. \tag{3}$$

2.2 Anderson's Cryptanalysis

In this cryptanalysis [1], Anderson pointed out that Matsumoto et al.'s protocol could in fact not withstand the one-round active attack and that the server would disclose the private key d of the client. The cryptanalysis can be briefly described as follows. Instead of Equation (2), the server sends $z_i = p_i r$ to the client, where r is a random number and p_is are random primes chosen so that their product is less than n. Thus, when the server receives S, he/she can disclose the private key d by repeatedly dividing it by r until the result is $\prod_{w_i=1} p_i$, which is no longer divisible by r, thus obtaining w_i and hence d.

2.3 Hwang's Cryptanalysis

Although Anderson proposed a one-round attack on Matsumoto et al.'s protocol, his attacking method can be easily detected by the client [4]. Therefore, Hwang proposed another attack as follows. Instead of Equation (2), the server sends $z_i = p_i r_i$ to the client, where r_is are a set of random numbers and p_is are unique primes so that they satisfy two conditions: one is that their product must be less than n, and the other is that all r_is can not be divided by p_js. When the server receives S, he/she can disclose the private key d by adding together those d_i for which $S \bmod p_i = 0$. Since $S \bmod p_i = 0$, it implies that $w_i = 1$. Therefore, the server can easily disclose the d by adding those d_i.

III Improved Protocol

In this section, we shall propose an improved server assisted authentication protocol for detecting error vectors to overcome the cryptanalysis in the above section. The improved protocol is similar to Matsumoto et al.'s protocol. The first step of Matsumoto et al.'s protocol is modified as follows.

1. The client randomly breaks down d as follows.

$$d = \sum_{i=0}^{k} d_i w_i \bmod \phi(n), \tag{4}$$

   where $\phi(n)$ is the Euler quotient function, $D = [d_0, d_1, d_2, \ldots, d_k] = [2^0, 2^1, 2^2, \ldots, 2^k]$ is a set of integer vectors where $1 \leq d_i < n$, and $W = [w_0, w_1, w_2, \ldots, w_k]$ is a set of binary weight vectors.

We give an example for Step 1. Any value d can be broken using Equation (4). Assume that d is equal to 53. Then, $D = [1, 2, 4, 8, 16, 32]$ and $W = [1, 0, 1, 0, 1, 1]$.

To overcome both of Anderson's and Hwang's attacks, we propose a detecting method to detect the returned error vectors z_i based on our improved protocol.

Detecting Method:

When the client receives Z from the server, the client checks if $z_{i+1} = {z_i}^2$ for Z. If all the results are correct, the client can derive the signature S. Otherwise, the client asks the server to re-compute z_i and return it.

IV Discussions and Conclusions

According to our detecting method, both of Anderson's and Hwang's attacks can be detected by the client. Then, the client can require that the server re-compute the vectors and send them back. Hence, Anderson's and Hwang's attacks can do no harm to our proposed protocol. However, some might have doubts as to the efficiency of our protocol. For example, in our protocol, the client must generate the integer vectors $D = [2^0, 2^1, 2^2, \ldots, 2^k]$, which at first glance seems like a difficult task.

In fact, the work is very easy to do because all we have to do here is only multiply the previous number by 2 successively. Others might think that it is a big burden for the client to compute the exponential ${z_i}^2$ in our detecting method. The truth is that the work is also very easy to do because it is nothing more than multiplication.

In this article, we have shown that Matsumoto et al.'s protocol cannot withstand the one-round active attack according to Anderson's and Hwang's Cryptanalysis. To strengthen this weakness, a revised protocol, which is a slight modification of Matsumoto et al.'s protocol, is proposed. Furthermore, the revised protocol can detect error vectors sent from the server. The protocol can also speed up secret computations using the computing power of auxiliary devices the same way Matsumoto et al.'s protocol does.

ACKNOWLEDGEMENTS

Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-004.

References

[1] R. J. Anderson, "Attack on server assisted authentication protocols," *IEE Electronics Letters*, vol. 28, p. 1473, July 1992.

[2] Chin-Chen Chang and Min-Shiang Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[3] G. Horng, "An active attack on protocols for server-aided RSA signature computation," *Information Processing Letters*, vol. 65, pp. 71–73, 1998.

[4] Min-Shiang Hwang, "Improved attack on server assisted authentication protocols," *Journal of Chaoyang*, vol. 4, pp. 93–100, Oct. 1999.

[5] Shin-Jia Hwang and Chin-Chen Chang, "A new efficient server-aided RSA secret computation protocol against active attacks," *IEICE Trans. on Fundamentals*, vol. E83-A, pp. 567–570, Mar. 2000.

[6] Shin-Jia Hwang, Chin-Chen Chang, and Wei-Pang Yang, "Some active attacks on fast server-aided RSA secret computation protocol for modular exponentiation," in *Proceedings of Cryptography: Policy and Algorithem Conference*, pp. 3–5, July 1995.

[7] Chi-Sung Laih and Fu-Kuan Tu, "Remarks on parameter selection for server-aided secret RSA computation schemes," in *Proceedings of International Workshops on Parallel Processing*, pp. 167–172, 1999.

[8] Chu-Hsing Lin and Chin-Chen Chang, "A server-aided computation protocol for RSA enciphering algorithm," in *National Computer Symposium'93, R.O.C.*, pp. 547–552, Dec. 1993.

[9] Tsutomu Matsumoto, Koki Kato, and Hideki Imai, "Speeding up secret computations with insecure auxiliary devices," in *Advances in Cryptology, CRYPTO'88*, pp. 497–506, Lecture Notes in Computer Science, Vol. 403, Aug. 1988.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.