© 2000 *Institute of Mathematics and Informatics, Vilnius*

Cryptanalysis of the Batch Verifying Multiple RSA Digital Signatures *

Min-Shiang HWANG, Iuon-Chung LIN

Department of Information Management Chaoyang University of Technology
168, Gifeng E.Rd., Wufeng, Taichung Country, Taiwan 413, R.O.C.
e-mail: mshwang@cyut.edu.tw

Kuo-Feng HWANG

Department of Computer Science and Information Engineering
National Chung Cheng University, Chaiyi, Taiwan, R.O.C.

Received: January 2000

Abstract. Recently, Harn proposed an efficient scheme that can batch verification multiple RSA digital signatures. His scheme can reduce signature verification time. However, there is a weakness in his scheme. In this study, we present two methods to against his scheme.

Key words: cryptography, digital signature, RSA.

1. Introduction

Recently, Harn (1998) proposed an efficient scheme to batch verify RSA signatures. In Harn's scheme, multiple signatures can be signed by the same private key and these same multiple signatures can be verified simultaneously, instead of a scheme in which the signer must verify signatures repeatedly. Multiple RSA digital signatures are verified using batch verifying which requires computation of only one exponential operation. The main advantage of this scheme is that it reduces signature verification time. It is more efficient than separate veriffied signatures. However, there are some weaknesses in this scheme. If the batch verification fails, we cannot find out where the signature fault is located and we must verify all individual signatures separately. In addition, we show that the signer can easily forge individual signatures.

In this article, we provide two methods to demonstrate that the signer can forge individual signatures and make the batch verification valid. In other words, the receiver verifies that all individual signatures are valid signatures, but cannot repudiate a false signature.

*This research was partially supported by the NSC89-2213-E-324-001.

2. Review

We review the RSA cryptosystem (Rivest *et al.*, 1978) as follows. The RSA cryptosystem has to select p, q that are two large primes and obtains the modulus $n = p \times q$. Next, let $e \times d \bmod (p-1)(q-1) = 1$, we denote e as the public key, d as the private key. Assume that Alice wants to send message M and its signature to the receiver Bob, Alice uses the RSA digital signature algorithm to sign the message M. The RSA signature of message M is $S = h(M)^d \bmod n$, where $h(\cdot)$ is a public one-way hash function. Then, Alice sends (M, S) to Bob. Whenever, Bob receives (M, S) from Alice, he proves the correctness of the signature on the message M by checking $h(M) = S^e \bmod n$.

Now, assume that Alice wants send $M_1, M_2, \ldots, M_t$, and its' signatures to Bob. The multiple signatures $S_1, S_2, \ldots, S_t$ of messages $M_1, M_2, \ldots, M_t$ are signed using the same private key belonging to Alice. The $\left(\prod_{i=1}^{t} S_i\right)$ is a product of the individual signatures. In Harn's scheme, a new algorithm is given, based on the RSA cryptosystem. We can easily and efficiently to prove the correctness of those multiple signatures by checking the following equation:

$$\begin{aligned}\left(\prod_{i=1}^{t} S_i\right)^e &= \left(\prod_{i=1}^{t} \left[h(M_i)\right]^d\right)^e \bmod n \\ &= \left(\left[\prod_{i=1}^{t} h(M_i)\right]^d\right)^e \bmod n \\ &= \prod_{i=1}^{t} h(M_i) \bmod n. \end{aligned} \qquad (1)$$

If the multiple signatures satisfy the above equation, the receiver can prove that the multiple signatures are valid signatures of messages $M_1, M_2, \ldots, M_t$. Harn's scheme is efficient to batch verify multiple RSA digital signatures. However, there is a weakness in his scheme. In next section, we present two methods to subvert his scheme.

3. Cryptanalysis

In this section, we provide two methods to show that the signer, Alice, can forge individual signatures and make a false batch verification valid.

In the first method, we assume that the signer, Alice, sends messages and the signatures to the receiver Bob. Let $S'_i = h(M_{f(i)})^d$, where S'_i is a forged signature of S_i and $f(\cdot)$ is a one to one and onto function, $f(i) = j,\ i = 1, 2, \ldots, t,\ j = 1, 2, \ldots, t$. Alice sends the forged pairs $(M_i, S'_i),\ i = 1, 2, \ldots, t$, to Bob. Since $\left(\prod_{i=1}^{t} S'_i\right)^e = \prod_{i=1}^{t} h(M_{f(i)}) \bmod n$, Bob is convinced that the messages are signed by Alice.

For example, Alice, a dishonest user, want send three messages with signatures, $(M_1, S'_1),\ (M_2, S'_2),\ (M_3, S'_3)$, to the receiver Bob. Alice can forge individual signature that $S'_1 = h(M_2)^d \bmod n$, $S'_2 = h(M_3)^d \bmod n$, and $S'_3 = h(M_1)^d \bmod n$. The dishonest user, Alice, sends (M_1, S'_1), (M_2, S'_2), (M_3, S'_3) to the receiver Bob. Bob proves the correctness of the multiplicative signatures on messages M_1, M_2, M_3 by checking the following equation:

$$\begin{aligned}(S_1' \times S_2' \times S_3')^e &= \big[h(M_2)^d \times h(M_3)^d \times h(M_1)^d\big]^e \operatorname{mod} n\\ &= \Big(\big[h(M_2) \times h(M_3) \times h(M_1)\big]^d\Big)^e \operatorname{mod} n\\ &= h(M_1) \times h(M_2) \times h(M_3) \operatorname{mod} n. \end{aligned} \tag{2}$$

Sinec the above equation holds, Bob convinces that the messages were signed by Alice. In fact, Alice can deny she had sent these messages to Bob, because $h(M_i) \neq (S_i')^e \operatorname{mod} n$.

In the second method, we assume that Alice sends (S_1', M_1), $(S_2', M_2), \ldots, (S_t', M_t)$ to Bob and lets $S_i' = a_i \times S_i,\ i = 1, 2, \ldots, t$, where $\prod_{i=1}^t a_i = 1$. Since $\big(\prod_{i=1}^t S_i'\big)^e = \big(\prod_{i=1}^t h(M_i) \operatorname{mod} n\big)$, Bob is convinced that these messages were signed by Alice.

For example, Alice, a dishonest user, forges three signatures S_1', S_2', S_3' and lets $S_1' = \frac{1}{4}S_1$, $S_2' = 8S_2$, $S_3' = \frac{1}{2}S_3$. Here S_1, S_2 and S_3 are a signature of M_1, M_2 and M_3, respectively. In other words, $S_i = h(M_i)^d \operatorname{mod} n,\ i = 1, 2, 3$. Next, Alice sends (S_1', M_1), (S_2', M_2), and (S_3', M_3) to Bob. Bob proves the correctness of the multiplicative signatures on messages M_1, M_2, M_3 by checking the following equation:

$$\begin{aligned}(S_1' \times S_2' \times S_3')^e &= \left(\frac{1}{4}S_1 \times 8S_2 \times \frac{1}{2}S_3\right)^e \operatorname{mod} n\\ &= (S_1 \times S_2 \times S_3)^e \operatorname{mod} n\\ &= \big[h(M_1)^d \times h(M_2)^d \times h(M_3)^d\big]^e \operatorname{mod} n\\ &= \big(\big[h(M_1) \times h(M_2) \times h(M_3)\big]^d\big)^e \operatorname{mod} n\\ &= h(M_1) \times h(M_2) \times h(M_3) \operatorname{mod} n. \end{aligned} \tag{3}$$

Since the above equation holds, Bob believes that the signatures S_1', S_2' and S_3' are valid signatures of messages M_1, M_2, M_3. In fact, Alice can deny she had sent these messages to Bob, because $h(M_i) \neq (S_i')^e \operatorname{mod} n$.

4. Conclusions

We have proposed two methods to attack Harn's batch multiple RSA digital signatures verification method. We have shown that a signer can easily forge signatures and that the receiver cannot discover that the signatures are illegal in Harn's scheme.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-324-001.

References

Harn, L. (1998). Batch verifying multiple RSA digital signatures. *Electronics Letters*, **32**(12), 1219–1220.

Rivest, R.L., A. Shamir, and L. Adelman (1978). A method for obtainning digital signatures and public key cryptosystem. *Commun. ACM*, **21**(2), 120–126.

M.-S. Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

I.-C. Lin received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998. He is currently pursuing his master degree in Information Management from Chaoyang University of Technology. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

K.-F. Hwang received the B.S. in Construction Engineering from National Lien-Ho College of Technology and Commerce, Taiwan, Republic of China, in 1991; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 1999; He is currently pursuing his Ph.D. degree in Department of Computer Science and Information Engineering, at Nation Chung Cheng University. His research interests include cryptography, image processing, and information management.

Grupės skaitmeninių parašų, užšifruotų RSA metodu, kriptoanalizė

Min-Shiang HWANG, Iuon-Chung LIN, Kuo-Feng HWANG

Neseniai Harn'as pasiūlė efektyvią grupės skaitmeninių parašų, užšifruotų RSA metodu, patikrinimo algoritmą, kuris sumažina šių parašų patikrinimo laiką. Tačiau šis algoritmas turi trūkumą. Straipsnyje parodyta, kaip galima suklastoti parašus, o paršų gavėjas šios klastotės išaiškinti negalės.