Cryptanalysis of the Batch Verifying Multiple DSA-type Digital Signatures
1

Min-Shiang Hwang, Cheng-Chi Lee,
and Eric Jui-Lin Lu

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

Abstract

To reduce the signature verification time, Harn proposed an efficient batch verifying multiple DSA-type digital signatures instead of verifying each individual digital signature separately. However, there is a weakness in his scheme. In this article, we present our attack to against his scheme.

Keywords: Cryptography, digital signature, DSA.

1 Introduction

In digital signature, a sender signed a document using his/her private key and a receiver can verify this signature by the sender's public key. When the sender signed t documents for the receiver, the sender need to generate t signatures and the receiver need to verify these signatures in t times. This is inefficient to verify those signatures for the receiver. In 1994, Naccache et al. [Naccache, 1994] proposed an efficient scheme to batch verify multiple DSA digital signatures. The multiple DSA digital signatures are batch verified by

[1]This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-053.

the receiver which requires only one times. However, this scheme is insecure [Lim 1994]. In 1995, Harn proposed a DSA-type secure interactive batch verification protocol [Harn, 1995]. In 1998, Harn proposed two types of efficient non-interactive batch verification protocol: DSA-type and RSA-type multiple digital signatures [Harn, 1998, Harn, 1998]. However, the batch verifying multiple RSA-type digital signatures [Harn, 1998] is insecure [Hwang, 2000].

The batch verifying multiple DSA-type digital signatures [Harn, 1998] can against Lim and Lee's attack [Lim 1994]. This scheme is based on the DSA-type digital signature [Harn, 1994]. The main advantage of this scheme is that it reduces signature verification time. It is more efficient than verify each individual signature separately. However, there is a weakness in his scheme. In this article, we will show that an attacker can easily forge individual signatures and make the batch verification valid.

2 Rieview

In this section, we review the Harn's DSA-type digital signature [Harn, 1994] and batch verifying multiple DSA-type digital signature [Harn, 1998].

DSA-type Digital Signature:

The parameters of DSA-type digital signature are composed by public information p, q, g, a public key y and a secret key x, where p is a large prime, q is a factor of $(p-1)$, g is generated from GF(p), x is a random number less than q, and y is computed by $y = g^x \bmod p$.

Assume that Alice wants to send message M and its digital signature (r, s) to Bob. The sender, Alice, need to generate the digital signature (r, s) as follows. First, Alice generates a random number, k, less than q. Next, Alice computes r and s as follows.

$$r = (g^k \bmod p) \bmod q, \quad (1)$$

$$s = rk - Mx \bmod q. \quad (2)$$

Whenever Bob receives (M, r, s) from Alice, he verifies the correctness of the signature on the message M by checking whether the equation $r = (g^{sr^{-1}} y^{Mr^{-1}} \bmod p) \bmod q$ holds.

Multiple DSA-type Digital Signature:
Assume that Alice wants to send $M_1, M_2, \cdots, M_t$ and its digital signatures $(r_1, s_1), (r_2, s_2), \cdots, (r_t, s_t)$ to Bob. All digital signatures satisfy the following equation:

$$r_i = (g^{s_i r_i^{-1}} y^{M_i r_i^{-1}} \bmod p) \bmod q, \quad i = 1, 2, \cdots, t. \quad (3)$$

Whenever Bob receives these multiple signatures from Alice, Bob verifies the correctness of these multiple signatures on messages $M_1, M_2, \cdots, M_t$ by checking the following equation:

$$\prod_{i=1}^{t} r_i = (g^{\sum_{i=1}^{t} s_i r_i^{-1}} y^{\sum_{i=1}^{t} M_i r_i^{-1}} \bmod p) \bmod q. \quad (4)$$

By verifying the above equation, Bob can verify the multiple signatures of messages $M_1, M_2, \cdots, M_t$ are signed by Alice. Harn's scheme is efficient to batch verifying multiple DSA-type digital signatures. However, there is a weakness in his scheme. We show that the weakness in next section.

3 The Weakness of Harn's Scheme

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

We assume that the signer, Alice, sends messages and its forged signatures to the receiver Bob. Let $s'_i = s_i + a_i r_i \bmod q, i = 1, 2, \cdots, t$, where a_i is an integer such that $\sum_{i=1}^{t} a_i = 0$. Alice sends the forged pairs (M_i, r_i, s'_i), $i = 1, 2, \cdots, t$, to Bob. Since these multiple signatures satisfy the verification in Equation 4, Bob is convinced that these message are signed by the dishonest user, Alice.

For example, Alice forges three signatures $(r_1, s'_1), (r_2, s'_2), (r_3, s'_3)$ of messages M_1, M_2, M_3, respectively. Here, $s'_1 = s_1 + 2r_1 \bmod q$, $s'_2 = s_2 + 3r_2 \bmod q$, $s'_3 = s_3 - 5r_3 \bmod q$, and $s_i = r_i k_i - M_i x \bmod q, r_i = (g^{k_i} \bmod p) \bmod q, i = 1, 2, 3$. Then Alice sends $(M_1, r_1, s'_1), (M_2, r_2, s'_2)$, and (M_3, r_3, s'_3) to Bob. Bob can verify the correctness of the signature on the message M_1, M_2, and M_3 by checking the following equation:

$$\begin{aligned}
r_1 r_2 r_3 &= (g^{s'_1 r_1^{-1} + s'_2 r_2^{-1} + s'_3 r_3^{-1}} y^{M_1 r_1^{-1} + M_2 r_2^{-1} + M_3 r_3^{-1}} \bmod p) \bmod q. \\
&= (g^{(s_1 + 2r_1) r_1^{-1} + (s_2 + 3r_2) r_2^{-1} + (s_3 - 5r_3) r_3^{-1}} y^{M_1 r_1^{-1} + M_2 r_2^{-1} + M_3 r_3^{-1}} \bmod p) \bmod q. \\
&= (g^{s_1 r_1^{-1} + s_2 r_2^{-1} + s_3 r_3^{-1}} y^{M_1 r_1^{-1} + M_2 r_2^{-1} + M_3 r_3^{-1}} \bmod p) \bmod q. \qquad (5)
\end{aligned}$$

Since the above equation holds, Bob believes that the signatures (r_1, s'_1), (r_2, s'_2), and (r_3, s'_3) are valid signatures of messages M_1, M_2, and M_3, respectively. However, Alice can deny she had signed these messages to Bob, because $r_i \neq (g^{s'_i r_i^{-1}} y^{M_i r_i^{-1}} \bmod p) \bmod q$, $i = 1, 2, 3$.

Although the DSA-type digital signature is a secure scheme to produce individual signature [Harn, 1994], the batch verifying multiple DSA-type digital signatures [Harn, 1998] is insecure.

4 Conclusion

Harn proposed an efficient batch verifying multiple DSA-type digital signatures instead of verifying each individual digital signature separately. However, we presented a weakness of his scheme in this letter. We have shown that a signer can easily forge his/her signatures and the receiver cannot discover that the signatures are illegal in Harn's scheme.

References

[Diffie, 1976] Diffie, W. and M. Hellman (1976). New direction in cryptography. *IEEE Transactions On Information Theory*, **22**(6), 472–492.

[Harn, 1995] L. Harn, "DSA type secure interactive batch verification protocol," *Electronics Letters*, vol. 31, no. 4, pp. 257–258, 1995.

[Harn, 1998] L. Harn, "Batch verifying multiple DSA-type digital signatures," *Electronics Letters*, vol. 34, no. 9, pp. 870–871, 1998.

[Harn, 1998] L. Harn, "Batch verifying multiple RSA digital signatures," *Electronics Letters*, vol. 34, no. 12, pp. 1219–1220, 1998.

[Harn, 1994] L. Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electronics Letters*, vol. 30, no. 24, pp. 2025–2026, 1994.

[Hwang, 2000] M. S. Hwang, I. C. Lin, and K. F. Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.

[Lim 1994] C. H. Lim and P. J. Lee, "Security of interactive DSA batch verification," *Electronics Letters*, vol. 30, no. 19, pp. 1592–1593, 1994.

[Naccache, 1994] D. Naccache, D. Mraihi, D. Rapheali, and S. Vaudenay, "Can DSA be improved: Complexity trade-offs with the digital signature standard," in *Proceedings of Eurocrypt'94*, pp. 85–94, Lecture Notes in Computer Science, 1994.