Comment

Signature scheme based on discrete logarithm without using one-way hash-function

Chan Yeob Yeun, Chris J. Mitchell and Siaw Lynn Ng

Information Security Group

Royal Holloway, University of London

Egham, Surrey TW20 0EX, UK

Email : {c.yeun,c.mitchell,phah033}@rhbnc.ac.uk

Abstract

We show that the signature scheme proposed by Shao [1] is subject to homomorphism attacks, despite a claim in [1] to the contrary.

1 Introduction

ElGamal [2] and DSS [3] signature schemes are subject to homomorphism attacks. ElGamal signatures work as follows. Let p be a large prime such that $p-1$ has a large prime factor, and let g be a primitive element modulo p. Suppose user A has private key x $(1 < x < p-1)$ and public key $y = g^x \bmod p$. To sign message m, A randomly chooses

an integer k, $1 < k < p-1$, computes $r = g^k \bmod p$, $s = (m - xr)k^{-1} \bmod (p-1)$ and (r, s) is the signature.

He and Kiesler [4] describe the following 'homomorphism attack'. Suppose that, for three distinct signatures, the respective random values k satisfy $k_3 = k_1 + k_2$. An observer can deduce this by noting that $r_3 = r_1 r_2$. This immediately yields the private key from

$$x = (m_1 s_2 s_3 + m_2 s_1 s_3 - m_3 s_1 s_2) \times (r_1 s_2 s_3 + r_2 s_1 s_3 - r_1 r_2 s_1 s_2)^{-1}.$$

Shao [1] describes an ElGamal variant claimed to be immune to this attack. However, we show that this is not the case.

2 Shao's Scheme

We first describe Shao's scheme. The globally known system parameters are a large prime modulus p, a prime divisor q of $p-1$, and an integer g of order q. User A has two secret keys x_1, x_2 $(1 < x_i < p)$, and two public keys:

$$y_1 = g^{x_1} \bmod p, \quad y_2 = g^{x_2} \bmod p.$$

To sign message m, A randomly chooses two integers k_1 and k_2, $1 < k_1, k_2 < q$, computes $r^* = g^{k_1} + m g^{k_2} \bmod p$, $r = r^* \bmod q$, $s_1 = (k_1 - r - m)x_1^{-1} \bmod q$, $s_2 = (k_2 - r - m)x_2^{-1} \bmod q$, and (r, s_1, s_2) is the signature.

3 The Attack

An observer can compute $g^{k_1} \bmod p$ and $g^{k_2} \bmod p$ from message m and its signature (r, s_1, s_2), since

$$g^{k_i} \equiv g^{x_i s_i + r + m} \equiv y_i^{s_i} g^{r+m} \pmod p, \; i = 1, 2.$$

Suppose three pairs of random values: (k_1, k_2), (k_1', k_2'), (k_1'', k_2'') were used to generate the signatures (r, s_1, s_2), (r', s_1', s_2'), (r'', s_1'', s_2'') on messages m, m', m'' respectively. If $k_1 = k_1' + k_1''$, then this relation can be recognised by an observer, since

$$g^{k_1} \equiv g^{k_1'} g^{k_1''} \pmod{p}.$$

This gives three linear equations in x_1, k_1, k_1', k_1'':

$$x_1 s_1' \equiv k_1' - r' - m' \pmod{q},$$

$$x_1 s_1'' \equiv k_1'' - r'' - m'' \pmod{q},$$

and

$$x_1 s_1 \equiv k_1 - r - m \pmod{q}.$$

From these equations, and since $k_1 = k_1' + k_1''$, one can easily obtain the first half of the private key from:

$$x_1 = \{(r' + r'' - r) + (m' + m'' - m)\} \times (s_1 - s_1' - s_1'')^{-1} \bmod p.$$

Similarly, if $k_2 = k_2' + k_2''$, the second part of the private key is given by:

$$x_2 = \{(r' + r'' - r) + (m' + m'' - m)\} \times (s_2 - s_2' - s_2'')^{-1} \bmod p.$$

4 Conclusion

Contrary to Shao's claim, we have shown that Shao's scheme is vulnerable to homomorphism attacks. The main justification in [1] for the use of Shao's scheme is its resistance to homomorphism and substitution attacks. Substitution attacks can be avoided by the use of a one-way hash-function, and so there appears to be no reason to use Shao's scheme.

Although the ElGamal scheme and its variants (e.g. DSS) are subject to homomorphism attacks, such an attack being successful appears to be no more likely than finding a discrete logarithm, as long as the random integer used to construct the signature is chosen at random.

References

[1] Z. Shao. "Signature scheme based on discrete logarithm without using one-way hash-function". *Electronics Letters*, 34(11):1079–1080, 1998.

[2] T. ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". *IEEE Transactions on Information Theory*, 31:469–472, 1976.

[3] "The digital signature standard proposed by NIST". *Communications of the ACM*, 35(7):36–40, 1992.

[4] J. He and T. Kiesler. "Enhancing the security of ElGamal's signature scheme". *IEE Proc. Digit. Tech.*, 141(4):249–252, 1994.