Digital Signature Scheme Based on Two Hard Problems

Shimin Wei

Department of Computer Science and Technique, Huaibei Coal Normal College, Huaibei 235000, P. R. China

Summary
In 1998, Shao Proposed two digital signature schemes based on factoring and discrete logarithms. At the same year, Li and Xiao showed that Shao's schemes are insecure are not based on any hard problem. This paper modifies Shao's schemes. Two new schemes whose security is based on both factorization and discrete logarithms are proposed.

Key words:
Cryptography; Digital signature; Factoring; Discrete logarithms; Security

1. Introduction

In 1994, Harn [1], He and Kiesler [2] proposed digital signature schemes based on two hard problems—the factoring problem and the discrete logarithms problem. Since then, many digital signature schemes based on these two hard problems were proposed [3-7]. Unfortunately, most of them have shown to be insecure. For example, in 1998, Li and Xiao [8] showed that Shao's schemes are insecure are not based on any hard problem. This paper modifies Shao's schemes. Two new schemes whose security is based on both factorization and discrete logarithms are proposed.

2. Shao's Scheme and Its Security

Let p be a big prime $p = 4p_1q_1 + 1$, where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, and p_1, p_2, q_1, q_2 are all large primes. These parameters must be kept secret from every user, thus they will be discarded once p is produced. Let g be an element with order p_1q_1 of the finite field GF(p). Any user A has a secret key $x(1 < x < p_1q_1/2)$ and a corresponding public key $y = g^{x^2+x^{-2}} \bmod p$.

Shao's scheme 1: To sign a message m, User A does the following
1) Randomly chooses an integer t, $1 < t < p_1q_1/2$, and calculates

$$r = g^{t^2+t^{-2}} \bmod p;$$

2) Computing integer s and odd k such that

$$xs + x^{-1}r = mt + kt^{-1} \bmod p_1q_1 \qquad (1)$$

$$x^{-1}s + xr = mt^{-1} + kt \bmod p_1q_1 \qquad (2)$$

3) Sends $sig(m) = (k, r, s)$ as the signature of m.

To verify that (k, r, s) is a valid signature of m, one simply checks the identity

$$y^{s^2+r^2} = r^{m^2+k^2} g^{4(mk-sr)} \bmod p.$$

Shao's scheme 2: To sign a message m, User A does the following
1) Randomly chooses an integer t, $1 < t < p_1q_1/2$, and calculates

$$r = g^{t^2+t^{-2}} \bmod p;$$

2) Computing integer s and odd k such that

$$xs + x^{-1}r = m^2t + mkt^{-1} \bmod p_1q_1$$

$$x^{-1}s + xr = m^2t^{-1} + mkt \bmod p_1q_1$$

3) Sends $sig(m) = (k, r, s)$ as the signature of m.

To verify that (k, r, s) is a valid signature of m, one simply checks the identity

$$y^{s^2+r^2} = r^{m^4+m^2k^2} g^{4(m^3k-sr)} \bmod p.$$

In 1998, Li and Xiao [8] found a simple attack. Let (k, r, s) be a signature obtained by the attacker of a known message m. From Equation (1) and (2)

$$(x + x^{-1})(t + t^{-1})^{-1} = (m + k)(s + r)^{-1} \bmod p_1q_1$$

$$(x - x^{-1})(t - t^{-1})^{-1} = (m - k)(s - r)^{-1} \bmod p_1q_1.$$

Suppose that the attacker forge signature (k', r, s') for any message m' satisfying Equation (1) and (2). Then

$$(x + x^{-1})(t + t^{-1})^{-1} = (m' + k')(s' + r)^{-1} \bmod p_1q_1,$$

$$(x - x^{-1})(t - t^{-1})^{-1} = (m' - k')(s' - r)^{-1} \bmod p_1q_1$$

From above four equations

$$(m' + k')(s' + r)^{-1} = (m + k)(s + r)^{-1} \bmod p_1q_1$$

$$(m' - k')(s' - r)^{-1} = (m - k)(s - r)^{-1} \bmod p_1q_1$$

By solving above two equations we have

$$s' = s + (m' - m)(s^2 - r^2)(ms - kr)^{-1} \bmod p_1q_1$$

$$k' = k + (m' - m)(sk - mr)(ms - kr)^{-1} \bmod p_1q_1.$$

For Shao's scheme 2 we have the same attack.

3. Modified Signature Scheme

Let p be a big prime $p = 4p_1q_1 + 1$, where

Manuscript received December 5, 2007
Manuscript revised December 20, 2007

$p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, and p_1, p_2, q_1, q_2 are all large primes. These parameters must be kept secret from every user, thus they will be discarded once p is produced. Let g be an element with order $p_1 q_1$ of the finite field GF(*p*). Any user A has a secret key $x (1 < x < p_1 q_1 / 2)$ and a corresponding public key $y = g^{x^2 - x^{-2}} (\mathrm{mod}\, p)$.

Modified scheme 1: To sign a message *m*, User A does the following

1) Randomly chooses an integer *t* and odd number *k* ($1 < t, k < p_1 q_1 / 2$), and calculates

$$u = g^{t^2 - t^{-2}} (\mathrm{mod}\, p) \quad \text{and} \quad v = u^{k^2}$$

2) Computing *s* and *r* such that

$$xs + x^{-1} r = umt + vkt^{-1} \bmod p_1 q_1 \tag{3}$$

$$x^{-1} s + xr = umt^{-1} + vkt \bmod p_1 q_1 \tag{4}$$

3) Sends $sig(m) = (u, v, r, s)$ as the signature of *m*.

To verify that (*u*, *v*, *r*, *s*) is a valid signature of *m*, one simply checks the identity

$$u^{u^2 m^2} = v^{v^2} y^{s^2 - r^2} \bmod p .$$

Theorem 1 If the signer follows the above protocol, the recipient always accepts the signature.

Proof: From Equation (3) and (4)

$$x^2 s^2 + x^{-2} r^2 + 2sr = u^2 m^2 t^2 + v^2 k^2 t^{-2} + 2mk \bmod p_1 q_1$$

$$x^{-2} s^2 + x^2 r^2 + 2sr = u^2 m^2 t^{-2} + v^2 k^2 t^2 + 2mk \bmod p_1 q_1$$

So that

$$(x^2 - x^{-2})(s^2 - r^2) = (t^2 - t^{-2})(u^2 m^2 - v^2 k^2) \bmod p_1 q_1$$

hence

$$g^{(x^2 - x^{-2})(s^2 - r^2)} = g^{(t^2 - t^{-2})(u^2 m^2 - v^2 k^2)} \bmod p$$

so

$$y^{s^2 - r^2} = u^{u^2 m^2 - v^2 k^2} \bmod p$$

Thus

$$u^{u^2 m^2} = v^{v^2} y^{s^2 - r^2} \bmod p$$

Modified scheme 2: To sign a message m, User A does the following

1) Randomly chooses an integer *t* and odd number *k* ($1 < t, k < p_1 q_1 / 2$), and calculates $u = g^{t^2 - t^{-2}} (\mathrm{mod}\, p)$ and $v = u^{k^2}$

2) Computing *s* and *r* such that

$$xs + x^{-1} r = um^2 t + vmkt^{-1} \bmod p_1 q_1 ,$$

$$x^{-1} s + xr = um^2 t^{-1} + vmkt \bmod p_1 q_1$$

3) Sends $sig(m) = (u, v, r, s)$ as the signature of m

To verify that (*u*, *v*, *r*, *s*) is a valid signature of *m*, one simply checks the identity

$$u^{u^2 m^4} = v^{v^2 m^2} y^{s^2 - r^2} \bmod p .$$

Similar to the proof of Theorem 1, we can prove that if the signer follows the above protocol, the recipient always accepts the signature.

4. The security of Modified Scheme

We only discuss the security of Modified Scheme 1. The discussion of the security of Modified Scheme 2 is similar. In the following discussion, we use the fact that the problem of solving quadratic equation $x^2 = k \bmod p_1 q_1$ are equivalent to solving the problem of factoring $p_1 q_1$ [9].

1) To recover x from public key $y = g^{x^2 - x^{-2}} \bmod p$ it is necessary to compute both the discrete logarithm of y modulo p (obtain $x^2 - x^{-2} = a \bmod p - 1$), and solve the equation $x^2 - x^{-2} = a \bmod p - 1$ to obtain x he must be face with another difficult problem: factoring *p*-1.

2) To recover x from Equation (3) and (4) it is necessary to compute both the discrete logarithm of v (obtain k^2) and *u* (obtain $t^2 - t^{-2} = b \bmod p$) modulo *p*, and to factor *p*-1 for computing the square root of k^2 modulo *p*-1 (obtain *k*) and solving the equation

$$t^2 - t^{-2} = b \bmod p - 1 \text{(obtain } t\text{)}.$$

3) Even if the attacker has the ability to compute the discrete logarithms modulo a large prime number *p*, he can recover $x^2 - x^{-2}, k^2, t^2 - t^{-2}$ from a signature (u, v, r, s) of a known message m and public key *y*. To forge the signature of for any message m', the attacker must finds r', s' such that

$$x^2 s'^2 + x^{-2} r'^2 + 2s'r' = u^2 m'^2 t^2 + v^2 k^2 t^{-2} + 2uvm'k \bmod p_1 q_1 \tag{5}$$

$$x^{-2} s'^2 + x^2 r'^2 + 2s'r' = u^2 m'^2 t^{-2} + v^2 k^2 t^2 + 2uvm'k \bmod p_1 q_1 \tag{6}$$

From Equation (5) and (6)

$$(x^2 - x^{-2})(s'^2 - r'^2) = (t^2 - t^{-2})(u^2 m'^2 - v^2 k^2) \bmod p_1 q_1$$

hence

$$s'^2 - r'^2 = (x^2 - x^{-2})^{-1} (t^2 - t^{-2})(u^2 m'^2 - v^2 k^2) \bmod p_1 q_1$$

Even if the attacker has the ability to compute s'^2 and r'^2, and substituting them in Equation (5) and (6), but he can’t solve s' and r', since s', r' and k are unknown, and the corresponding coefficient of Equation (5) and (6) are in proportion.

4) Suppose that attacker have a signature (u, v, r, s) of a known message *m*, From Equation (3) and (4)

$$(x + x^{-1})(t + t^{-1})^{-1} = (um + vk)(s + r)^{-1} ,$$

$$(x - x^{-1})(t - t^{-1})^{-1} = (um - vk)(s - r)^{-1} .$$

Suppose that attacker forge signature (u, v, r', s') for message m' satisfying Equation (3) and (4). Then

$$(x + x^{-1})(t + t^{-1})^{-1} = (um' + vk)(s' + r')^{-1} ,$$

$$(x - x^{-1})(t - t^{-1})^{-1} = (um' - vk)(s' - r')^{-1} .$$

From above four equation

$$(um' + vk)(s' + r')^{-1} = (um + vk)(s + r)^{-1} ,$$

$$(um' - vk)(s' - r')^{-1} = (um - vk)(s - r)^{-1} .$$

Since s', r' and k are unknown, we cannot solve s' an r' in above two equation. These show that Modified scheme 1 can protect from Li-Xiao attack.

3.1 Simulation Experiment

5. Conclusion

Two modified Shao signature schemes is proposed, the security of which is based on both factorization problem and discrete logarithms problem.

Acknowledgment

This work was supported in part by the Natural Science Foundation of China under Grant 60573026 and 60773121, the Key Project of Chinese Ministry of Education under Grant 205074, and the Academic and Technical leading scholars Research Project of the Education Department of Anhui Province in China under Grant 2005hbz24, and the Natural Science Foundation of Anhui Province in China under Grant 070412052.

References

[1] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," IEE Proc.-Computers and Digital Techniques, 141(3), 1994:193-195

[2] J. He and T. Kiesler, "Enhancing the security of ElGamal's signature scheme", IEE Proc.-Computers and Digital Techniques, 141(4), 1994:249-252

[3] N. Y. Lee and T. Hwang, "Modified Harn signature scheme based on factoring and discrete logarithms," IEE Proc.-Computers and Digital Techniques, Vol. 143, No. 3, 1996, pp. 196-198

[4] C. S. Laih, , and W. C. Kuo, "New signature schemes based on factoring and discrete logarithms," IEICE Trans. Fund, E80-A(1), 1997:46-53

[5] Z. Shao, "Signature schemes based on factoring and discrete logarithms", IEE Proc.-Computers and Digital Techniques, 145(1), 1998:33-36

[6] W. H. He, "Digital signature scheme based on factoring and discrete logarithms," Electron. Letters, 37(4), 2001:220-222

[7] S. Wei, "New signature scheme based on factoring and discrete logarithms", Progress on Cryptography: 25 years of Cryptography in China, Massachusetts: Cluwer Academic Publishers, 2004, pp. 107-112

[8] J. Li and G. Xiao, "Remarks on new signature scheme based on two hard problems," Electron. Letters, 34(25), 1998: 2401-2402

[9] R. C. Peralta, "A simple and fast probabilistic algorithm for computing square roots modulo a prime number," IEEE Trans. on Information Theory, 32, 1986: 846-847

Shimin Wei received the B. S. degree in Mathematics from the Huaibei Coal Normal College, Huaibei, Anhui, China, in 1986, the M. S. Degree in Mathematics from the Northwest University, Xi'an, Shaanxi, China, in 1993, and the Ph. Degree in Cryptography from the Xidian University, Xi'an, Shaanxi, China, in 2001. From April 2001 to July 2003, he was a postdoctoral with the Department of Department of Computer Science and Technique, Peking University, Beijing, China.

He was a Lecturer from June 1993 to November 1994, was a associate professor from December 1994 to November 1996, has been a professor since December 1996, with the Department of Mathematics and the Department of Computer Science & Technique, Huaibei Coal Normal College, Huaibei, Anhui, China. Since October 2003, he has been the header with the Department of Computer Science & Technique, Huaibei Coal Normal College. His research interests include Applied Mathematics, Cryptography and Coding, Information and Network Security.