Comments on Wei's Digital Signature Scheme Based on Two Hard Problems

H. F. Lin[1], C. Y. Gun[2, 3], C. Y. Chen[2]

[1]Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan,

[2]Department of Communications Engineering, Feng Chia University, Taichung 40724, Taiwan, R.O.C.

[3]Department of Mechanical Engineering, Nan Kai University of Technology, Nan-tou 54210, Taiwan, R.O.C

Summary
In 1998, Shao proposed two digital signature schemes and claimed that the security of which is based on the difficulties of computing both integer factorization and discrete logarithm. However, at the same year, Li and Xiao demonstrated that Shao's schemes are insecure are not based on any hard problem. Recently, Wei proposed two "Digital Signature Schemes Based on Two Hard Problems" to improve Shao's schemes, and showed that it can resist Li and Xiao's attack. We show that neither scheme is as secure as the author claim. One can forge a valid signature of an arbitrary message by using Pollard and Schnorr's method without solving the discrete logarithm problem or the factorization hard problem.

Key words:
digital signature, factorization problem, discrete logarithm problem, two hard problems

1. Introduction

The concept of public-key cryptography was invented by Diffie and Hellman [1] in 1976. Since then, several public-key cryptographic algorithms based on single computationally hard problem, such as factorization or discrete logarithm problem, have been proposed [2, 3]. Although, these algorithms appear secure today, it is very likely that a clever cryptanalyst will discover some efficient ways to solve one hard problem in the future. In 1988, McCurley [4] proposed a key distribution system based on double hard problems, *i.e.*, on both integer factorization and discrete logarithm problems. Since then, several cryptographic systems have been proposed that try to base their security on solving two or more hard problems simultaneously in order to enhance the security [5-11].

In 1998, Shao [12] also proposed two dual-algorithm digital signature schemes with optimized computational and memory requirements. However, Li and Xiao [13] revealed that the two schemes were insecure. If one valid signature is known, one can forge a valid signature for a randomly chosen message.

In 2007, Wei [14] presented two improvements of Shao's signature schemes and showed that the new schemes can resist Li and Xiao's attack [13]. Hence, the security of which were claimed to be based on the difficulties of computing integer factorization and discrete logarithm problems.

In this paper, we show that Wei's schemes [14] were still insecure without solving either factoring problem or discrete logarithm problem, one can forge a valid signature of an arbitrary message by using Pollard and Schnorr's method [15].

The rest of this paper is organized as follows. In sections 2, we will briefly review Wei's modified signature schemes. Security analysis of Wei's modified scheme is given in section 3. Finally, the conclusion is given in section 4.

2.A brief review of Wei's modified signature schemes

A trusted key centre is assumed to select the following system parameters [16]:

(i) Let $p = 4p_1q_1 + 1$ be a big prime, where $p_1 = 2p_2 + 1, q_1 = 2q_2 + 1,$ and p_1, p_2, q_1 ,q_2 are all large primes;

(ii) Let g be an element with order p_1q_1 of the finite field GF(p). Any user A has a random secret key x $(1 < x < p_1q_1/2)$ and publishes the corresponding public key

$$y = g^{x^2 - x^{-2}} \pmod{p}.$$

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

1) Randomly chooses an integer t and odd k $(1 < t, k < p_1q_1/2)$, and calculates

Manuscript received February 5, 2009
Manuscript revised February 20, 2009

$u = g^{t^2 - t^{-2}} \pmod{p}$ and $v = u^{k^2} \pmod{p}$.

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

$$\begin{cases} xs + x^{-1}r \equiv umt + vkt^{-1} \mod (p_1 q_1) & (1) \\ x^{-1}s + xr \equiv umt^{-1} + vkt \mod (p_1 q_1) & (2) \end{cases}$$

3) Sends *sig*(*m*) = (*u*, *v*, *r*, *s*) as the signature of *m*.
4) The verifier to check that (*u*, *v*, *r*, *s*) is a valid signature of *m* by inspecting the identity

$$u^{(u^2 m^2)} \equiv ?\ v^{v^2} \cdot y^{s^2 - r^2} \mod p.$$

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

$u = g^{t^2 - t^{-2}} \pmod{p}$ and $v = u^{k^2} \pmod{p}$.

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

$$\begin{cases} xs + x^{-1}r \equiv um^2 t + vmkt^{-1} \mod (p_1 q_1) & (3) \\ x^{-1}s + xr \equiv um^2 t^{-1} + vmkt \mod (p_1 q_1) & (4) \end{cases}$$

3) Sends *sig*(*m*) = (*u*, *v*, *r*, *s*) as the signature of *m*.
4) The verifier to check that (*u*, *v*, *r*, *s*) is a valid signature of *m* by inspecting the identity

$$u^{u^2 m^4} \equiv ?\ v^{v^2 m^2} \cdot y^{(s^2 - r^2)} \mod p.$$

3.Cryptanalysis of Wei's signature schemes

Both schemes in [14] were claimed to be secure if one cannot simultaneously solve both cryptographic assumptions, factoring and discrete logarithms. We want to show that his claim is invalid.

3.1 Cryptanalysis on the Wei's modified scheme 1

For any message m, the attacker substitutes $u = y^2, v = y^3$ on the verification identity

$$u^{(u^2 m^2)} \equiv v^{v^2} \cdot y^{s^2 - r^2} \mod p.$$

He obtains

$$(y^2)^{u^2 m^2} \equiv (y^3)^{v^2} \cdot y^{s^2 - r^2} \mod p$$

or $2u^2 m^2 - 3v^2 \equiv s^2 - r^2 \mod p_1 q_1$

Since the condition $\gcd(2u^2 m^2 - 3v^2, p_1 q_1) = 1$ is satisfied with non-negligible probability, we then by using the method of Pollard and Schnorr [15] can solve out (r, s) from $s^2 - r^2 \equiv 2u^2 m^2 - 3v^2 \mod p_1 q_1 \cdots (*)$. Otherwise, one can repeat to adjust the values of *u* and *v* until $\gcd(2u^2 m^2 - 3v^2, p_1 q_1) = 1$ such that the condition $(*)$ holds, so that one can forge a valid signature (u, v, r, s) of an arbitrary message m without solving the discrete logarithm problem or the factorization hard problem.

3.2 Cryptanalysis on the Wei's modified scheme

Similar to the forge signature of the modified scheme 1, we can forge a valid signature from the modified scheme 2.

For any message m, the attacker substitutes $u = y^2, v = y^3$ on the verification identity

$$u^{(u^2 m^4)} \equiv v^{v^2 m^2} \cdot y^{s^2 - r^2} \mod p.$$

He obtains

$$(y^2)^{u^2 m^4} \equiv (y^3)^{v^2 m^2} \cdot y^{s^2 - r^2} \mod p$$

or $2u^2 m^4 - 3v^2 m^2 = s^2 - r^2 \mod p_1 q_1$.

Since the condition $\gcd(2u^2 m^4 - 3v^2 m^2, p_1 q_1) = 1$ is satisfied with non-negligible probability, we then by using the method of Pollard and Schnorr [15] can solve out (r, s) from $s^2 - r^2 \equiv 2u^2 m^4 - 3v^2 m^2 \mod p_1 q_1 \cdots (**)$. Otherwise, one can repeat to adjust the values of *u* and *v* until $\gcd(2u^2 m^4 - 3v^2 m^2, p_1 q_1) = 1$ such that the condition $(**)$ holds, so that one can forge a valid signature (u, v, r, s) of an arbitrary message m without solving the discrete logarithm problem or the factorization hard problem.

4. Conclusions

We have shown that the security of Wei's digital signature schemes [14] are insecure under the special assumptions of u and v. One can forge a valid signature of an arbitrary message by using Pollard and Schnorr method [15]. Notice that neither discrete logarithm nor factoring problem is needed to solve, as claimed in [14].

References

[1]. W. Diffie and M. Hellman, "*New Directions in Cryptography,*" IEEE Transactions on Information Theory 1976, vol. IT-22, pp. 644-654.

[2]. T. ElGamal, "*A public key cryptosystem and a signature scheme based on discrete logarithms,*" IEEE Transactions on Information Theory, Vol. IT-31, 1985, pp. 469-472.

[3]. R. L. Rivest, A. Shamir, and L. M. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems,*" Communications of the ACM, Vol. 21, 1978, pp. 120-126.

[4]. K. McCurley, "*A key distribution system equivalent to factoring,*" Journal Cryptology, Vol. 1, 1988, pp. 95-106.

[5]. E. F. Brickell and K. S. McCurley, "*An interactive identification scheme based on discrete logarithms and factoring,*" Journal of Cryptology, Vol. 5, 1992, pp. 29-39.

[6]. L. Harn, "*Public-key cryptosystems design based on factoring and discrete logarithms,*" IEE Proceedings of Computer Digital Techniques, Vol. 141, 1994, pp. 193-195.

[7]. J. He and T. Kiesler, "*Enhancing the security of Elgamal's signature scheme,*" in IEE Proceedings of Digital Techniques, Vol. 141, 1994, pp. 249-252.

[8]. N. Lee and T. Hwang, "*Modified Harn signature scheme based on factorizing and discrete logarithms,*" in IEE Proceedings of Computer Digital Techniques, Vol. 143, 1996, pp. 196-198.

[9]. C. Laih and W. C. Kuo, "*New signature schemes based on factoring and discrete logarithms,*" IEICE Transactions on Fundamentals, Vol. E80-A, 1997, pp. 46-53.

[10]. Z. Shao, "*Signature schemes based on factoring and discrete logarithms,*" in IEE Proceedings on Digital Techniques, Vol. 149, 1998, pp. 33-36.

[11]. S. Y. Chiou, "*The design and analysis of digital signatures based on factoring and discrete logarithm problems,*" Ph.D. Thesis, Dept. of Electrical Engineering, National Cheng Kung University, Taiwan, 2004.

[12] Z. Shao, "*Signature schemes based on factoring and discrete logarithms,*"Computers and Digital Techniques, IEE Proceedings, Jan. 1998, vol. 145, issue 1, pp. 33 –36.

[13] J. Li and G. Xiao, "*Remarks on new signature scheme based on two hard problems,*" Electronics Letters, 10 Dec. 1998, Volume: 34 (25), pp. 2401-2402

[14] S. Wei "*Digital Signature Scheme Based on Two Hard Problems,*" IJCSNS International Journal of Computer Science and Network Security, December 2007, vol.7 No.12.

[15] J. Pollard and C. Schnorr, "*An Efficient Solution of the Congruence* $x^2 + ky^2 = m \bmod n$," IEEE Trans. on Information Theory, 1987, vol. IT-33 , pp. 17-28.

H. F. Lin was born in Taipei, Taiwan. He received his B.S. degree in Mathematics form Fu Jen Catholic University in 1970 and M.S. degree in Mathematics from the National Tsing Hua University in 1974. Currently, he is an Associate Professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His major areas of interest are computer cryptography, computer arithmetic, and algorithms.

C. Y. Gun was born in Taiwan, She received her B.S. degree in Mathematics form National Normal University in 1979 and M.S. degree in Statistics from the University of Texas at Austin (USA) in 1993, Currently, She is a Ph.D student in the Department of Communications Engineering, Feng Chia University, Taichung, Taiwan. She is also a lecture in the Department of Mechanical Engineering, Nan- Kai University of Technology, Nan-tou, Taiwan**.**

C. Y. Chen was born in Taiwan in 1951. He received the B.S. degree and the M.S. degree in Mathematics from Tamkang University in 1974 and National Central University in 1976, respectively, and the Ph.D. degree in Computer Sciences from National Tsing Hua University in 1995. He is currently a Professor in the Department of Communications Engineering, Feng Chia University, Taichung, Taiwan. His main research interests include database design, algorithm design and analysis, coding theory, and computer cryptography.