Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms
（基於分解因數與離散對數之數位簽章方法之安全性分析）

Hung-Min Sun (孫宏民)
Department of Computer Science and Information Engineering
National Cheng Kung University Tainan, Taiwan 70101
Email: hmsun@mail.ncku.edu.tw

ABSTRACT

Recently, He proposed a new digital signature scheme based on the difficulties of simultaneously solving the factoring problem and the discrete logarithms problem. In this paper, we show that He's digital signature scheme is insecure against forgery if the discrete logarithms problem is solved.

Keywords: Cryptography, Digital Signature, Factoring, Discrete Logarithms

中文摘要

最近，植基於同時解因數分解與離散對數之問題，何提出一個新的數位簽章演算法。在本論文中，我們證明了假如離散對數的問題解決了，何的數位簽章演算法是不安全的。

關鍵字: 密碼學、數位簽章、因數分解、離散對數

1. Introduction

Since Harn [1] presented the first digital signature scheme based on two hard problems – the factoring problem [2] and the discrete logarithms problem [3], several digital signature schemes, based on the difficulties of simultaneously solving these two hard problems, have been proposed [4,5,8]. All these schemes were designed to provide the advantage that once one hard problem is solved, these schemes are still secure against forgery. Unfortunately, most of them have been shown to be insecure against forgery. For example, Harn's scheme [1] was shown to be insecure [4] if the discrete logarithms problem is solved; He and Kiesler's scheme [5] was shown to be insecure [6-7]; and Shao's schemes [8] were shown to be not sufficiently secure [9-10]. Recently, He [11] proposed a new digital signature scheme based on the difficulties of simultaneously solving the factoring and discrete logarithms problems. In this paper, we show that He's digital signature scheme is still insecure against forgery if the discrete logarithms problem is solved.

2. Review of He's digital signature scheme

In this section, we briefly review He's digital signature scheme as follows:

Initialisation: The trusted center of the system selects a large prime *P* satisfying *P* = 4 $p_1 \cdot q_1$ +1, where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are all primes. Let *R* =(*P*-1)/4= $p_1 \cdot q_1$. The trusted center selects an element *g* with order *R* in Z_P. The system parameters *P* and *g* are made public, while p_1, p_2, q_1, q_2 are all discarded. Each user in the system selects a private key $x \in Z_R$ such that gcd($(x+x^{-1})^2$, *R*)=1, where $x \cdot x^{-1}$ =1 (mod *R*), and the corresponding public key is

$$y = g^{(x+x^{-1})^2} \pmod{P}.$$

Digital signature generation: In order to generate a digital signature on a message *m*, the signer first select a random integer $t \in Z_R$ such that gcd($(t+t^{-1})^2$, *R*)=1. Then he computes $r_1 = g^{(t+t^{-1})^2}$ (mod *P*) and $r_2 = g^{(t+t^{-1})^{-2}}$ (mod *P*). Finally, he computes *s* which satisfies the following congruence:

$(x+x^{-1}) = \mathrm{s}\cdot(t+t^{-1})+f(r_1, r_2, m)\cdot(t+t^{-1})^{-1}$ (mod *R*), ……………………………..….Eq.(1)
where *f* is a one-way hash function.

Thus, (r_1, r_2, *s*) is a valid digital signature on the message *m*.

Digital signature verification: Upon receiving a digital signature (r_1 , r_2 , *s*) associated with *m* with respect to the signer, anyone can verify the validity of the digital signature by checking whether the following congruence holds or not:

$$y = r_1^{s^2}\cdot r_2^{f^2(r_1,r_2,m)}\cdot g^{2s\cdot f(r_1,r_2,m)} \pmod{P} \quad\text{……………………………….Eq.(2)}$$

If this congruence holds, then (r_1, r_2, *s*) is a valid digital signature on the message *m*.
Here we call Eq.(2) the signature verification equation. In the following, we show that Eq.(2) holds if Eq.(1) holds.

Because $(x+x^{-1}) = \mathrm{s}\cdot(t+t^{-1})+f(r_1, r_2, m)\cdot(t+t^{-1})^{-1}$ (mod *R*), it is obvious that

$$y = g^{(x+x^{-1})^2} \pmod{P}$$
$$= g^{s^2\cdot(t+t^{-1})^2+2\cdot s\cdot f(r_1,r_2,m)+f^2(r_1,r_2,m)\cdot(t+t^{-1})^{-2}} \pmod{P}$$
$$=[g^{(t+t^{-1})^2}]^{s^2}\cdot g^{2\cdot s\cdot f(r_1,r_2,m)}\cdot [g^{(t+t^{-1})^{-2}}]^{f^2(r_1,r_2,m)} \pmod{P}$$
$$= r_1^{s^2}\cdot r_2^{f^2(r_1,r_2,m)}\cdot g^{2s\cdot f(r_1,r_2,m)} \pmod{P}.$$

3. Cryptanalysis of He's scheme

We assume that an attacker knows a previous valid digital signature (r_1, r_2, *s*) on a message *m* with respect to the signer. Assuming that the discrete logarithms problem is solved, the attacker can easily obtain $(t+t^{-1})^{-2}$ (mod *R*) by solving the discrete logarithm: $\log_g r_2$ in Z_P. Thus, the attacker can forge another valid digital signature ($r_1, r_2, \tilde{s}$) on an arbitrary message $\tilde{m}$ with respect to the signer by assigning $\tilde{s}$ $=[f(r_1, r_2, m)- f(r_1, r_2, \tilde{m})]\cdot(t+t^{-1})^{-2} + s$ (mod *R*).

Theorem 1. The triple ($r_1, r_2, \tilde{s}$) satisfies: $y = r_1^{\tilde{s}^2}\cdot r_2^{f^2(r_1,r_2,\tilde{m})}\cdot g^{2\tilde{s}\cdot f(r_1,r_2,\tilde{m})}$ (mod *P*).

Proof: Because (r_1, r_2, *s*) is a valid digital signature, the equation Eq.(1) holds.
That is, $(x+x^{-1}) = \mathrm{s}\cdot(t+t^{-1})+f(r_1, r_2, m)\cdot(t+t^{-1})^{-1}$ (mod *R*).
Because $\tilde{s}$ $=(f(r_1, r_2, m)- f(r_1, r_2, \tilde{m}))^{-1}\cdot(t+t^{-1})^{-2} + s$ (mod *R*), it is clear that

$$\tilde{s}\cdot(t+t^{-1})+f(r_1, r_2, \tilde{m})\cdot(t+t^{-1})^{-1} \pmod{R}$$
$$= \{[f(r_1, r_2, m)- f(r_1, r_2, \tilde{m})]\cdot(t+t^{-1})^{-2} + s\}\cdot(t+t^{-1})+f(r_1, r_2, \tilde{m})\cdot(t+t^{-1})^{-1} \pmod{R}$$
$$= [f(r_1, r_2, m)- f(r_1, r_2, \tilde{m})]\cdot(t+t^{-1})^{-1}+ s\cdot(t+t^{-1})+ f(r_1, r_2, \tilde{m})\cdot(t+t^{-1})^{-1} \pmod{R}$$
$$= f(r_1, r_2, m)\cdot(t+t^{-1})^{-1} - f(r_1, r_2, \tilde{m})\cdot(t+t^{-1})^{-1}+ s\cdot(t+t^{-1})+ f(r_1, r_2, \tilde{m})\cdot(t+t^{-1})^{-1} \pmod{R}$$
$$= f(r_1, r_2, m)\cdot(t+t^{-1})^{-1} + s\cdot(t+t^{-1}) \pmod{R}\text{, by Eq.(1),}$$
$$= (x+x^{-1}) \pmod{R}.$$

That is, $(x+x^{-1}) = \tilde{s}\cdot(t+t^{-1})+f(r_1, r_2, \tilde{m})\cdot(t+t^{-1})^{-1}$ (mod *R*).
Hence, the signature verification equation

$$y = r_1^{\tilde{s}^2}\cdot r_2^{f^2(r_1,r_2,\tilde{m})}\cdot g^{2\tilde{s}\cdot f(r_1,r_2,\tilde{m})} \pmod{P}$$

holds.

4. Conclusions

In this paper, we have shown that He’ s digital signature scheme, based on the factoring and discrete logarithms problems simultaneously, is not secure against forgery if the discrete logarithms problem is solved.

Acknowledgments

This work was supported in part by the National Science Council, Taiwan, under contract NSC-90-2213-E-006-111.

REFERENCES

[1] HARN, L.: 'Public-key cryptosystem design based on factoring and discrete logarithms', *IEE Proc. Comput. Digit. Tech.*, 1994, **141**, (3), pp. 193-195

[2] RIVEST, R., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signature and public-key cryptosystem', *Commun. ACM*, 1978, **21**, (2), pp. 120-126

[3] ELGAMAL, T.: 'A public key cryptosystem and signature scheme based on discrete logarithms', *IEEE Tran. Information Theory*, 1985, **IT-31**, (4), pp. 469-472

[4] LEE, N. Y., and HWANG, T.: 'Modified Harn signature scheme based on factorizing and discrete logarithms', *IEE Proc. Comput. Digit. Tech.*, 1996, **143**, (3), pp. 196-198

[5] HE, J., and KIESLER, T.: 'Enhancing the security of ElGamal's signature scheme', *IEE Proc. Comput. Digit. Tech.*, 1994, **141**, (4), pp. 249-252

[6] HARN, L.: 'Comment: Enhancing the security of ElGamal's signature scheme', *IEE Proc. Comput. Digit. Tech.*, 1995, **142**, (5), pp. 376

[7] LEE, N. Y., and HWANG, T.: 'The security of He and Kiesler's signature schemes', *IEE Proc. Comput. Digit. Tech.*, 1995, **142**, (5), pp. 370-372

[8] SHAO, Z.: 'Signature schemes based on factoring and discrete logarithms', *IEE Proc. Comput. Digit. Tech.*, 1998, **145**, (1), pp. 33-36

[9] LI, J., and XIAO, G.: 'Remarks on new signature scheme based on two hard problems', *Electron. Lett.*, 1998, **34**, (25), pp. 2401

[10] LEE, N. Y.: 'Security of Shao's signature schemes based on factoring and discrete logarithms', *IEE Proc. Comput. Digit. Tech.*, 1999, **146**, (2), pp. 119-121

[11] HE, W. H.: 'Digital signature scheme based on factoring and discrete logarithms', *Electron. Lett.*, 2001, **37**, (4), pp. 220-222