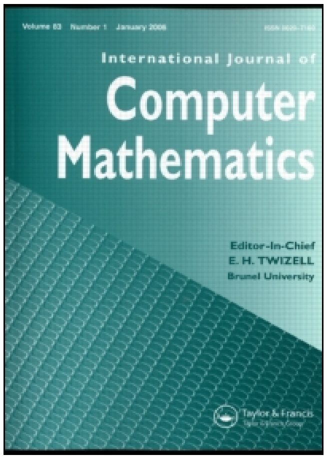

International Journal of Computer Mathematics
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713455451

A new digital signature scheme based on factoring and discrete logarithms

Shiang-Feng Tzeng [a]; Cheng-Ying Yang [b]; Min-Shiang Hwang [c]
[a] Department of Computer Science and Information Engineering, National Central University, Taoyan, Taiwan, R.O.C.
[b] Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology, Taichung County, Taiwan, R.O.C.
[c] Department of Management Information System, National Chung Hsing University, Taichung, Taiwan, R.O.C.

Online Publication Date: 01 January 2004
To cite this Article: Tzeng, Shiang-Feng, Yang, Cheng-Ying and Hwang, Min-Shiang (2004) 'A new digital signature scheme based on factoring and discrete logarithms', International Journal of Computer Mathematics, 81:1, 9 - 14
To link to this article: DOI: 10.1080/00207160310001614954
URL: http://dx.doi.org/10.1080/00207160310001614954

International Journal of Computer Mathematics
Vol. 81, No. 1, January 2004, pp. 9–14

Taylor & Francis
Taylor & Francis Group

A NEW DIGITAL SIGNATURE SCHEME BASED ON FACTORING AND DISCRETE LOGARITHMS

SHIANG-FENG TZENG[a], CHENG-YING YANG[b] and MIN-SHIANG HWANG[c,*]

[a]*Department of Computer Science and Information Engineering, National Central University, No. 300, Jung-da Road, Jung-li City, Taoyan, Taiwan 320, R.O.C.;* [b]*Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology, 168 Gifeng E. Road, Wufeng, Taichung County, Taiwan 413, R.O.C.;* [c]*Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.*

(Received 1 March 2003)

This article proposes a new digital signature scheme based on the difficulty of simultaneously factoring a composite number and computing discrete logarithms. In the proposed scheme, each user uses common arithmetic moduli and only owns one private key and one public key. Furthermore, some possible limitations have been analyzed, but none of them can successfully over-rule the proposed scheme.

Keywords: Cryptography; Discrete logarithms; Digital signature; Factoring

C.R. Categories: E.3.

1 INTRODUCTION

Diffie and Hellman [1] were the first to propose the concept of the public-key cryptosystem in 1996. However, several public-key cryptosystems have since been discussed [2–4]. The security of these proposed cryptosystems are based on the following cryptographic assumptions: factoring (FAC) a large composite number [4–7] and solving the discrete logarithm (DL) problem [2, 8–10]. Although these cryptosystems are based on the above cryptographic assumptions that appear secure today, they are very likely to be over-ruled in the future. As soon as some cryptanalyst develops an efficient algorithm to factor the composite number or to compute DL, which could very likely be right around the corner, these cryptosystems will go insecure.

In 1994, Harn [11] first developed a digital signature scheme based on multiple cryptographic assumptions, *i.e.* a mixture of FAC and DL, to enhance the security of the digital signature. Since then many such digital signature schemes have been proposed [12–15]. Unfortunately, all those proposed schemes have proved to be insecure against forgery. In 1996, Lee and Hwang [14] pointed out that Harn's digital signature scheme [11] would not be secure if the DL problem could be solved.

[*] Corresponding author. E-mail: mshwang@mail.nchu.edu.tw

ISSN 0020-7160 print; ISSN 1029-0265 online © 2004 Taylor & Francis Ltd
DOI: 10.1080/00207160310001614954

He and Kiesler's digital signature scheme [12] has also been shown to be insecure [16]. For example, if one has the ability to solve DL [16], then she/he will be able to forge the signature. Also, if one can solve the FAC problem, she/he can obtain the signer's private key.

Recently, Li and Xiao [17] have shown that Shao's digital signature schemes [15] are vulnerable to signature forgery. In addition, Lee [18] has also shown that if the FAC problem can be solved, Shao's digital signature schemes [15] can be broken. Not long ago, He [13, 19] proposed a digital signature scheme based on the difficulty of simultaneously FAC a composite number and computing DLs. He's scheme has three significant advantages.

1. The security of He's scheme is based on the difficulty of simultaneously solving the FAC and the DL problems with arithmetic moduli of almost the same size.
2. Each user has common arithmetic moduli.
3. Each user only owns one private key and one public key.

However, as Sun [20] had pointed out, He's scheme [13] is still not secure against forgery if the DL problem can be solved. To overcome the above limitations a new digital signature is proposed in this paper.

In the next section, we introduce our new digital signature scheme. In Section 3, we analyze the security and performance of the new digital signature scheme and finally, the conclusions are given in Section 4.

2 THE PROPOSED DIGITAL SIGNATURE SCHEME

In this section, a new digital signature scheme based on FAC and DL is proposed. The scheme can be divided into three phases: initialization, digital signature generation and digital signature verification.

2.1 Initialization

There exists a trusted center whose tasks are to initialize the system and to manage the public directory. First, the trusted center selects the following parameters.

- P: a large prime $P = 4p_1 \cdot q_1 + 1$, where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, and p_1, q_1, p_2, q_2 are all primes.
- R: the product of p_1 and q_1, $i.e.$ $R = (P - 1)/4 = p_1 \cdot q_1$.
- g: a primitive element with order $p_1 \cdot q_1$.
- $h(\cdot)$: a one-way hash function, $e.g.$ MD5 or SHA-1.

The parameters P and g are used by all users, and p_1, q_1, p_2 and q_2 are all discarded. Each user owns a private key $x \in Z_R$ such that $gcd(x^2, R) = 1$ and the corresponding public key y which is certified by the certificate authority as

$$y = g^{x^2+x^{-2}} \bmod P. \tag{1}$$

2.2 Digital Signature Generation

To sign a message M, the signee carries out the following steps.

1. Randomly select an integer t_1 and compute k as

$$k = t_1 x \bmod R. \tag{2}$$

2. Compute

$$t_2 = kx \bmod R, \tag{3}$$

$$r = g^{t_1^2+t_2^2} \bmod P. \tag{4}$$

3. Calculate s_1 and s_2 under the conditions

$$s_1 = h(r, M)t_1 + x \bmod R, \tag{5}$$

$$s_2 = h(r, M)t_2 - x^{-1} \bmod R. \tag{6}$$

Then (r, s_1, s_2) is a signature of M. The signee then sends (r, s_1, s_2) to the verifier.

2.3 Digital Signature Verification

On receiving the digital signature (r, s_1, s_2) the verifier can confirm the validity of the digital signature by the following equation

$$g^{s_1^2+s_2^2} = r^{h^2(r,M)} y \bmod P. \tag{7}$$

If it holds, then (r, s_1, s_2) is a valid signature of M.

THEOREM 2.1 *If the signee follows the above digital signature protocol, the verifier always accepts the digital signature.*

Proof Squaring Eqs (5) and (6)

$$s_1^2 = h^2(r, M)t_1^2 + 2h(r, M)t_1x + x^2 \bmod R,$$
$$s_2^2 = h^2(r, M)t_2^2 - 2h(r, M)t_2x^{-1} + x^{-2} \bmod R.$$

Summing the above 2 equations

$$s_1^2 + s_2^2 = h^2(r, M)(t_1^2 + t_2^2) + 2h(r, M)(t_1x - t_2x^{-1}) + (x^2 + x^{-2}) \bmod R.$$

According to Eqs (2) and (3)

$$s_1^2 + s_2^2 = h^2(r, M)(t_1^2 + t_2^2) + (x^2 + x^{-2}) \bmod R.$$

Therefore we have

$$g^{s_1^2+s_2^2} = g^{h^2(r,M)(t_1^2+t_2^2)+(x^2+x^{-2})} \bmod P$$

or

$$g^{s_1^2+s_2^2} = r^{h^2(r,M)} y \bmod P.$$

The above equation is equivalent to Eq. (7). With the knowledge of the signee's public key y and the signature (r, s_1, s_2) of M, the verifier can authenticate the message M because the verifier can be convinced that the message was really signed by the signee. Else, the signature (r, s_1, s_2) is invalid.

3 SECURITY AND PERFORMANCE ANALYSIS

The security of the proposed scheme is based on the cryptographic assumptions of intractability of FAC and DLs. In this section, we analyze some possible limitations of our digital signature scheme.

Limitation 1: An adversary attempts to derive the private key from the corresponding public key for any user.

Analysis of limitation 1: For the adversary, to recover a private key x from Eq. (1) is polynomially equivalent to figuring out both FAC and DL simultaneously. She/he also has to solve the DL problem to obtain $(x^2 + x^{-2}) \bmod R$; at the same time, she/he also has to solve the FAC problem to obtain a private key x from $(x^2 + x^{-2}) \bmod R$.

Limitation 2: An adversary attempts to derive the private key from a valid signature (r, s_1, s_2) of message M.

Analysis of limitation 2: To obtain a private key x or to compute a private key x for x^{-1} from Eqs (5) and (6), the adversary has to know t_1 or t_2. Given P, g, r, s_1 or P, g, r, s_2 to obtain t_1 or t_2 from Eq. (4) is non-feasible under FAC and DL assumptions.

Limitation 3: An adversary attempts to forge a valid signature (r, s_1, s_2) for message M. In this case, the adversary has to find a three-tuple (r, s_1, s_2) to satisfy Eq. (7).

Analysis of limitation 3:

1. The adversary randomly chooses r and s_1. She/he then has to solve the problem of finding s_2 from α where

$$\begin{aligned}\alpha &\equiv r^{h(r,M)^2} y g^{-s_1^2} \bmod P,\\ &\equiv g^{s_2^2} \bmod P.\end{aligned}$$

   This is equivalent to solving both the FAC and the DL at the same time.

2. The adversary randomly chooses r and s_2. She/he has to solve the problem of obtaining s_1 from β where

$$\begin{aligned}\beta &\equiv r^{h(r,M)^2} y g^{-s_2^2} \bmod P,\\ &\equiv g^{s_1^2} \bmod P.\end{aligned}$$

   This is as difficult as solving FAC and DL simultaneously.

3. The adversary randomly chooses s_1 and s_2. She/he has to solve the problem of deriving r from γ where

$$\begin{aligned}\gamma &\equiv g^{s_1^2+s_2^2} y^{-1} \bmod P,\\ &\equiv r^{h(r,M)^2} \bmod P.\end{aligned}$$

   This is as hard as distinguishing between the FAC, DL and one-way hash function assumptions.

4. The adversary randomly chooses a three-tuple (r, s_1, s_2). This is also as difficult as solving the FAC, DL and one-way hash functions simultaneously.

Therefore, we conclude that the task of forging the message is more difficult than solving the problems of FAC and DLs simultaneously.

Next, we analyze the computational cost of the proposed scheme. In the performance evaluation T_{exp} represents the time for a modular exponentiation computation, T_{inv} is the time for a modular inverse computation, and T_h is the time for computing a one-way hash function $h(\cdot)$.

We ignore the time for performing modular multiplication and addition. Then, the total computational complexities of the signee and the verifier are $T_{\text{exp}} + T_{\text{inv}} + T_h$ and $2T_{\text{exp}} + T_h$, respectively.

4 CONCLUSION

A new digital signature scheme has been proposed in this paper. The security of the proposed scheme is equivalent to solving both the FAC problem and the DL problem. Some possible limitations have also been considered. The advantages of the proposed scheme are the following three characteristics: (i) the sizes of the arithmetic moduli for FAC and DLs are almost the same; (ii) each user uses common arithmetic moduli; and (iii) each user only owns one private key and one public key.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

References

[1] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theor.*, IT-22 (Nov.) (1976) 644–654.

[2] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theor.*, IT-31 (July) (1985) 469–472.

[3] M. O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, *Technical Report, MIT/LCS/TR212, MIT Lab.*, Computer Science Cambridge, MA, USA, January (1979).

[4] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM*, 21 (Feb.) (1978) 120–126.

[5] Chin-Chen Chang and Min-Shiang Hwang, Parallel computation of the generating keys for RSA cryptosystems, *IEE Elec. Lett.*, 32 (15) (1996) 1365–1366.

[6] S. Wesley Changchien and Min-Shiang Hwang, A batch verifying and detecting multiple RSA digital signatures, *Int. J. Comput. Num. Anal. Appl.*, accepted (Feb. 18, 2002) and to appear.

[7] Min-Shiang Hwang, Iuon-Chung Lin, and Kuo-Feng Hwang, Cryptanalysis of the batch verifying multiple RSA digital signatures, *Informatica*, 11 (1) (2000) 15–19.

[8] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, An ElGamal-like cryptosystem for enciphering large messages, *IEEE Trans. Know. Data Eng.*, 14 (2) (2002) 445–446.

[9] Min-Shiang Hwang, Cheng-Chi Lee, and Eric Jui-Lin Lu, Cryptanalysis of the batch verifying multiple DSA-type digital signatures, *Pakistan J. Appl. Sci.*, 1 (3) (2001) 287–288.

[10] Yuan-Liang Tang, Min-Shiang Hwang, and Yan-Chi Lai, Cryptanalysis of a blind signature scheme based on ElGamal signature, *to appear in Int. J. Pure Appl. Math.* (2002).

[11] L. Harn, Public-key cryptosystem design based on factoring and discrete logarithms, *IEE Proc. Comp. Digital Tech.*, 141 (3) (1994) 193–195.

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

[13] W. H. He, Digital signature scheme based on factoring and discrete logarithms, *Elec. Lett.*, 37 (4) (2001) 220–222.

[14] N. Y. Lee and T. Hwang, Modified Harn signature scheme based on factorising and discrete logarithms, *IEE Proc. Comp. Digital Tech.*, 143 (3) (1996) 196–198.

[15] Z. Shao, Enhancing the security of ElGamal's signature scheme, *IEE Proc. Comp. Digital Tech.*, 145 (1) (1998) 33–36.

[16] H. J. Tiersma, Enhancing the security of ElGamal's signature scheme, *IEE Proc. Comp. Digital Tech.*, 144 (1) (1997) 47–48.

[17] Jihong Li and Guozhen Xiao, Remarks on new signature scheme based on two hard problems, *Elec. Lett.*, 34 (25) (1998) 2401.

[18] N. Y. Lee, Security of Shao's signature scheme based on factoring and discrete logarithms, *IEE Proc. Comp. Digital Tech.*, 146 (2) (1999) 119–121.

[19] Min-Shiang Hwang, Chao-Chen Yang, and Shiang-Feng Tzeng, Improved digital signature scheme based on factoring and discrete logarithms, *J. Disc.. Math. Sci. Crypt.*, accepted (April 12, 2002) and (to appear).

[20] Hung Min Sun, Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms, in *Proceedings of the National Computer Symposium*, Taipei, Taiwan, December (2001) pp. F043–F045.