Improved Digital Signature Scheme Based on Factoring and Discrete Logarithms*

Min-Shiang Hwang　　Chao-Chen Yang　　Shiang-Feng Tzeng

Department of Information Management
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

November 28, 2001

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-053.

Improved Digital Signature Scheme Based on Factoring and Discrete Logarithms

Abstract

Recently, He proposed a new digital signature scheme based on factoring and discrete logarithms. In this article, we propose an improvement of He's digital signature scheme. Our scheme is secure and efficient.

Index Terms: cryptography, digital signature.

1 Introduction

Recently, He [2] proposed a new digital signature scheme which was based on two well-known assumptions: the difficult of factoring and discrete logarithms. The security of He's scheme is based on the difficulty of simultaneously solving the factoring (FAC) a composite number [6, 7] and computing the discrete logarithms (DL) [1, 3, 4, 5]. To increase efficiency, we propose an improvement of He's digital signature scheme in this article.

2 Review of He's Scheme

There are three phases in He's scheme: initialization, digital signature generation, and verification [2].

(i) Initialization Phase:

First, the trusted center of the system selects p_1, p_2, q_1, q_2, P, R, and g such that $P = 4p_1q_1 + 1$, $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, $R = p_1q_1$, and g is with order p_1p_2 in Z_P. The following parameters p_1, q_1, p_2, q_2, and P are all primes. P, R, and g are made public. p_1, q_1, p_2, and q_2 are all discarded. Next, each user in the system selects a private key x in Z_R such that $\gcd((x+x^{-1})^2, R) = 1$. The corresponding public key y is computed as follows.

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

(ii) Digital Signature Generation Phase:

To generate a signature for a message m, the signer performs the following steps:

1. Randomly select an integer t in Z_R such that $\gcd((t+t^{-1})^2, R) = 1$. Then, compute

$$r_1 = g^{(t+t^{-1})^2} \bmod P, \tag{2}$$

$$r_2 = g^{(t+t^{-1})^{-2}} \bmod P, \tag{3}$$

   where r_1 and r_2 have the same order R.

2. Find s such that

$$(x+x^{-1}) = s(t+t^{-1}) + f(r_1, r_2, m)(t+t^{-1})^{-1} \bmod R, \tag{4}$$

   where f is a one-way hash function.

The pair (r_1, r_2, s) is a signature for the message m. The signer can send the signature (r_1, r_2, s) associated with the message m to a verifier.

(iii) Digital Signature Verification Phase:

Upon receiving the signature (r_1, r_2, s) associated with the message m, the verifier validates the signature by checking the following congruent equality:

$$y = r_1^{s^2} r_2^{f^2(r_1,r_2,m)} g^{2sf(r_1,r_2,m)} \bmod P. \tag{5}$$

If the equality holds, (r_1, r_2, s) is a valid signature.

3 Improved Digital Signature Scheme

Our improved digital signature scheme is the same as He's scheme except that the following two items are modified.

1. In Initialization Phase, each user in the system selects a private key X in Z_R such that $\gcd(X^2, R) = 1$. The corresponding public key y in Equation (1) is replaced by

$$y = g^{X^2} \bmod P. \tag{6}$$

2. In Digital Signature Generation Phase, the signer selects an integer T in Z_R such that $\gcd(T^2, R) = 1$. The parameters r_1 and r_2 in Equations (2) and (3) are replaced by

$$r_1 = g^{T^2} \bmod P \tag{7}$$

and

$$r_2 = g^{T^{-2}} \bmod P, \tag{8}$$

respectively. Equation (4) is also replaced by

$$X = sT + f(r_1, r_2, m)T^{-1} \bmod R. \tag{9}$$

Upon receiving the signature (r_1, r_2, s) which is generated by the above improved scheme, the verifier validates the signature using Equation (5). We show that (r_1, r_2, s) is a valid signature if the equality in Equation (5) holds.

$$\begin{aligned} y &= g^{X^2} \bmod P \\ &= g^{(sT+f(r_1,r_2,m)T^{-1})^2} \bmod P \\ &= g^{s^2T^2} g^{f^2(r_1,r_2,m)T^{-2}} g^{2sf(r_1,r_2,m)} \bmod P \\ &= r_1^{s^2} r_2^{f^2(r_1,r_2,m)} g^{2sf(r_1,r_2,m)} \bmod P. \end{aligned} \tag{10}$$

4 Security Analysis

Our improved scheme is the same as He's scheme except that we replace $(x + x^{-1})$ and $(t + t^{-1})$ with X and T, respectively. The security analysis of our improved scheme is similar to that of He's scheme. We similarly analyze some possible ways in which an adversary may attempt attacks on the proposed scheme.

An adversary attempts to derive the private key from the public key for any user. In this attack, the adversary must solve the DL problem [1, 3, 4, 5] from Equation (6) to obtain $X^2 \bmod R$. In addition, the adversary need to solve the FAC a composite number problem [6, 7] to derive X from $X^2 \bmod R$.

An adversary attempts to derive the private key from a valid signature (r_1, r_2, s) for a given message m. In this attack, the adversary must know T and then to derive X from Equation (9). However, given y, g, and r_1 or r_2, deriving T from Equation (7) or Equation (8) is also under the FAC and the DL problems.

An adversary attempts to forge a valid signature (r_1, r_2, s) for a given message m without knowing the private key and any valid signature for the signer. In this attack, the adversary attempts to find the solution of three variables r_1, r_2 and d satisfying Equation (10). First, the adversary sets two variables to find the solution of the other variable from Equation (10). It is also under the FAC and the DL problems that given y, g, m, r_1 and r_2 to find s such that Equation (10) is hold.

5 Conclusions

We have proposed an improved digital signature scheme and showed that the security of our improved scheme is equivalent to that of He's scheme. In addition, we replace $(x + x^{-1})$ and $(t + t^{-1})$ in He's scheme with X and T, respectively. The performance of our improved scheme is better than that of

He's scheme. In Initialization Phase, our improved scheme less one addition operation and one modular inverse operation for generating the public key y. In Digital Signature Generation Phase, our improved scheme less two addition operations and two modular inverse operations for generating r_1, r_2, and s.

References

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

[2] W. H. He, "Digital signature scheme based on factoring and discrete logarithms," *Electronics Letters*, vol. 37, no. 4, pp. 220–222, 2001.

[3] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *accepted and to appear in IEEE Transactions on Knowledge and Data Engineering.*

[4] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *to appear in IEEE Transactions on Knowledge and Data Engineering.*

[5] Min-Shiang Hwang, Cheng-Chi Lee, and Eric Jui-Lin Lu, "Cryptanalysis of the batch verifying multiple DSA-type digital signatures," *Pakistan Journal of Applied Sciences*, vol. 1, no. 3, pp. 287–288, 2001.

[6] Min-Shiang Hwang, Iuon-Chung Lin, and Kuo-Feng Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.