EasyChair Preprint

№ 5314

An Ameliorated "Strengthened He-Kiesler Digital Signature"

Lee Ching-Min, Chiou Shin-Yan, Chen Jonathan Jen-Rong and Hu Ya-Ping

April 11, 2021

An ameliorated "Strengthened He-Kiesler Digital Signature"

Ching-Min Lee[1], Shin-Yan Chiou[2], Jonathan Jen-Rong Chen[3], Ya-Ping Hu[4]
Department of Electrical Engineering, Chang Gung University, Taiwan[1,2]
No.259, Wenhua 1st Rd., Guishan Dist., Taoyuan City 33302, Taiwan (R.O.C.)
Department of Information Management, Vanung University of Science and Technology, Taiwan[3]
No.1, Wanneng Rd., Zhongli Dist., Taoyuan City 32061, Taiwan (R.O.C.)
Department of Accounting and Information Systems, Asia University, Taiwan[4]
E-Mail: lcm.paul@msa.hinet.net[1]
E-Mail: ansel@mail.cgu.edu.tw[2]
E-Mail: jonathan@mail.vnu.edu.tw[3]
E-Mail: yapinghu@asia.edu.tw[4]

Abstract

The advancement of information technology, cryptanalysis technology is also changing with each passing day. He & Kiesler[4] studied the squaring of the cipher on the discrete logarithm exponent, forcing the attacker to simultaneously crack the complexity of the double hypothesis before they could challenge their system. However, Harn[6], Lee & Hwang[10] have repeatedly disproved their views by using the complexity of solving a single hypothesis without having to solve the complexity of a double hypothesis at the same time. Shao[16] tried to create another double-complexity signature strategy similar to He & Kiesler, but was denied by Li & Xiao[5]. We point that Chen etc. tried to strengthen He and Kiesler on the basis of the Laih & Kuo[1] assumptions is failed.

Key words：Discrete logarithm, Dual-complexities, Factorization, Digital signature

1. Introduction

The introduction of digital signature technology overcomes the technical bottleneck of signature and stamping required for traditional business activities. In the past forty years or so, some scholars on signature technology have used the complexity of the factorization hypothesis [9][13] or the complexity of the discrete logarithm hypothesis [15][12] as a starting point, and have made different thinking aspects. the study. With the advancement of information technology, the technology required to crack passwords also changes with each passing day. Brickell and McCurley[3] first considered the study of the complexity of combining factorization and the single hypothesis of discrete logarithms to establish the complexity of the double hypothesis, and their method has two defects: first, the signer and the verifier need Two-way identification (Interactive Indentification) is not conducive to the fight for timeliness, and is easy to cause network traffic; the modulus of factorization is too long, and the calculation is time-consuming.

He and Kiesler[4] squared the cipher on the discrete logarithm exponent, in an attempt to force the attacker to simultaneously crack the complexity of the double hypothesis in order to challenge their system. However, Harn[6], Lee & Hwang[10] were recently overturned by the complexity of solving a single hypothesis instead of the complexity of a dual hypothesis at the same time. Shao [16] tried to create another dual-complexity signature strategy similar to He and Kiesler's method, but it was rejected by Li and Xiao [5].

Harn[7] builds a strategy of dual hypothesis complexity based on individual users having their own modulus, which was later modified by Lee & Hwang [10], but its method is different from the original ElGamal theory. Laih & Kuo[1] adopted the Naccache[2] model to construct a system with double hypothesis complexity, and users have the amount $O(t)$ of both public and secret keys, which is the burden of the messenger and the system center.

This paper intends to strengthen the method of He and Kiesler based on the hypothesis of Laih & Kuo.[1] The paper sequence is as follows: the literature discussion is presented in the second part, our method is introduced in the third part, the fourth part is a security analysis, and the conclusion is discussed at the end.

2. Literature Discussion

2.1 The method of He & Kiesler[4] selects a large prime number p that satisfies the following formula for the center of the system.

$$p = 4p_1q_1 + 1 \text{……..……(1)}$$

p_1, q_1 both are large prime numbers.

Make $n = p_1 \cdot q_1$…… …(2)

Then system center select a number q as a primitive root (a primitive element g over GF(p)) and the modulo p whose order is n, $\{p, n, g\}$ which is the public key of the system center and $\{p_1, q_1\}$ is its secret key.

User A (hereinafter referred to as A) selects a

number $x \in Z_n^*$ as its secret key, and calculates:

$$g^{x_i^4} \equiv y_i (mod\ \ p) \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Register$\{y_i\}$with the system center as its public key, and $\{x_i\}$ as the A's private key.

A signed a digital signature on message m, the calculation steps are:

Step 1: Choose a number $d \in Z_n^*$ and to calculate:

$$r \equiv g^{d^4} \left(\mathrm{mod}\, p\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Step 2: Calculation:

$$m \equiv x^2 r + d^2 s \left(\mathrm{mod}\, n\right) \ldots\ldots\ldots\ldots\ldots (5)$$

Step 3: Calculation:

$$b \equiv dx \left(\mathrm{mod}\, n\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Step 4: Send the signature $sig(m) = (r, s, b)$to recipient B (hereinafter referred to as B), after B receives the relevant message, verify:

$$g^{m^2} \equiv y^{r^2} r^{s^2} g^{2rsb^2} \left(\mathrm{mod}\, p\right) \ldots\ldots\ldots (7)$$

If formula (7) is established, accept the message m, otherwise, reject it.

2.2 Harn [4] organizes formula (5) into:

$$mx^2 \equiv x^4 r + x^2 d^2 s \left(\mathrm{mod}\, n\right)$$

$$\equiv \left(x^2\right)^2 r + b^2 s \left(\mathrm{mod}\, n\right) \ldots\ldots\ldots\ldots (8)$$

In equation (8), if the attacker N (hereinafter referred to as N) can crack the complexity of the factorization hypothesis, then the secret key of A can be calculated.

2.3 Lee & Hwang[8] believe that N only need to collect two known signatures $(m_1, r_1, s_1, b_1)$and (m_2, r_2, s_2, b_2), and formula (5) can be sorted into:

$$\left(m_1 - x^2 r_1\right)^2 \equiv d_1^4 s_1^2 \left(\mathrm{mod}\, n\right) \ldots\ldots\ldots\ldots (9)$$

$$\left(m_2 - x^2 r_2\right)^2 \equiv d_2^4 s_2^2 \left(\mathrm{mod}\, n\right) \ldots\ldots\ldots\ldots (10)$$

If N can solve the complexity of the discrete logarithm hypothesis, and sort out equations (9) and (10), we can know that equations (5) x^2 , d_1^2 and. d_2^2 Therefore, N can carry out a forgery attack.

3. Our Scheme

We continue the parameters and definitions of He & Kiesler in the previous section, and then let $\alpha = 4$ [5], then:

$$p = 4p_1 q_1 + 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (11)$$

This method uses He & Kiesler calculation steps 1 to 3, that is, equations (2)-(6) are all extended, and the modified calculation steps are:

Step 4: A select a number $K_1, K_2, S_1 \in Z_m^*$ and calculate:

$$g^{K_1^4} \equiv r_1 (mod\ \ p) \ldots\ldots\ldots\ldots\ldots\ldots (12)$$

$$g^{K_2^4} \equiv r_2 (mod\ \ p) \ldots\ldots\ldots\ldots\ldots (13)$$

$$\mathrm{t} \equiv x_i^2 r_1 + K_1^2 \cdot S_1^2 (mod\ \ p) \ldots (14)$$

$$\mathrm{m} \equiv t^2 \cdot r_2 + K_2^2 \cdot S_2 (mod\ \ p) \ldots (15)$$

Step 5: Calculation:

$$g^{x_i K_1 S_1} \equiv A_1 (mod\ \ p) \ldots\ldots\ldots (16)$$

Select a number K_3 , and calculate:

$$g^{K_3} \equiv r_3 (mod\ \ p) \ldots\ldots\ldots\ldots\ldots (17)$$

Step 6: Calculate:

$$\mathrm{m} \equiv (x_i K_1 S_1) r_3 + K_3 S_3 (mod\ \ p) \ldots (18)$$

$$g^{t^2} \equiv T (mod\ \ p) \ldots\ldots\ldots\ldots\ldots (19)$$

$$g^{x_i K_1 S_1 K_3} \equiv r_4 (mod\ \ p) \ldots\ldots (20)$$

Step 7:Send $\{m,\ r_1, r_2, r_3, r_4, S_1, S_2, T, A_1\}$ to B. After B receives the relevant message, verify:

$$g^m \equiv A_1^{r_3} \cdot r_3^{S_3}\ \ (mod\ \ p) \ldots\ldots\ldots\ldots (21)$$

$$A_1^m \equiv \left(\frac{T}{y_i^{r_1^2} r_1^{S_1^4}}\right)^{r_1^{-1} r_3} \cdot r_4^{S_3}\ \ (mod\ \ p)\ \ldots (22)$$

If formula (21,22) is established, accept the message m, otherwise, reject it.

4. Security analysis

The weakness of the He & Kiesler methods is that the attacker only needs to solve the complexity of the factorization hypothesis, use the b value of equation (6), and then skillfully integrate it into equation (5), so that the attacker does not need to face the discrete logarithm hypothesis. Complexity, and get the secret golden key of the attacked; In addition, for an attacker who can crack the complexity of the discrete logarithm hypothesis, the clues provided by equation (4) can be resolved without factorization of equation (6) If it is difficult to calculate formula (5), the forgery attack can be carried out.

5. Conclusion

In order to solve the aforementioned deficiencies, Chen et al. used the techniques of formulas (12) ~ (15), combined with the assumptions of Laih & Kuo, and strengthened the methods of He & Kiesler. The verification calculation required for this digital signature is four modular exponential operations, which is one more than the original ElGamal method; the transmission volume of the digital signature is four, which is two more than the original ElGamal method. How to reduce the number of digital signatures The amount of verification and calculation and overcoming its weaknesses will be the direction of future research.

References

[1] C. –S. Laih and W. -C. Kuo, "New signature schemes based on factoring and discrete Logarithms," IEICE Trans. Fundamentals, Vol.E80-A, No.1, pp.46-53, 1997.

[2] D. Naccache, "Can O. S. S. be repaired? Proposal for a new practical signature scheme,"

Advances in Cryptology-EUROCRTPT'93, pp.233-239, 1994.
[3] E. F. Brickell and K. S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring," Journal of Cryptology, Vol.5, No.1, pp.29-40, 1992.
[4] J. He and T. Kiesler, "Enhancing the security of ElGamal's signature scheme," IEE Proc.-Comput. Digit. Tech., Vol.141, No.4, pp.249-252, 1994.
[5] J. Li and G. Xiao, "Remarks on new signature scheme based on two hard problems," Electronics Letters, Vol.34, No.25, p.2401,1998.
[6] L. Harn, "Comment: Enhancing the security of ElGamal's signature scheme," IEE Proc.-Comput. Digit. Tech., Vol.142, No.5, p.376, 1995.
[7] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," IEE Proc.-Comput. Digit. Tech., Vol.141, No.3, pp.193-195, 1994.
[8] L. Harn, "Reply: Comment-Public-key cryptosystem design based on factoring and discrete logarithms," IEE Proc.-Comput. Digit. Tech., Vol.143, No.1, p.96, 1995.
[9] M. O. Rabin, " Digitaliged signatures and public-key functions as intractable as factorigation," Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. 1979.
[10] N. -Y. Lee and T. Hwang, "Modified Harn signature scheme based on factoring and discrete logarithms," IEE Proc.-Comput. Digit. Tech., Vol.143, No.3, pp.196-198, 1996.
[11] N. -Y. Lee and T. Hwang, "The security of He and Kiesler's signature schemes," IEE Proc.-Comput. Digit. Tech., Vol.142, No.5, pp.370-372, 1995.
[12] NIST FIPS PUB XX, Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 1993.
[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.
[14] T. ElGamal, "A public key cryptosystem and a signature scheme based on the discrete logarithm," IEEE Transactions on Information Theroy, Vol.31, pp.469-472, 1985.
[15] Z. Shao, "Signature schemes based on factoring and discrete logarithms," IEE Proc.-Comput. Digit. Tech., Vol.145, No.1, pp.33-36, 1998.