1998 International Computer Symposium
Workshop on Algorithms
December 17-19, 1998, N.C.K.U., Tainan, Taiwan, R.O.C.

An Enhanced ElGamal Scheme with Respect to the Tiersma Attack

Jonathan Jen-Rong Chen
National Defense Management College, Taipei, Taiwan, R.O.C
E-Mail: jonathan@im.ndmc.edu.tw

Yuanchi Liu
Ta-Hwa Institute of Technology, Hsin-Chu, R.O.C.

Abstract

To enhance ElGamal's protection based on a discrete logarithm problem, He & Kiesler propose a protection based on discrete logarithm and factorization problems. Although Tiersma suggests that as long as the discrete logarithm problem can be solved, the He & Kiesler scheme can also be crypt-analyzed. This paper is to strengthen the He & Kielser scheme. In addition to the He & Kiesler advantage, Tiersma's attack can be stopped. Given the solution of discrete logarithm, Tiersma focuses on obtaining the square of the private key and forging the digital signature of the user under attack to detour the factorization problem. In order to counteract this attack, an additional parameter is needed to result in a failure to find the private key. In our scheme, an attacker can hardly detour factorization problem. Thus, in addition to the He & Kiesler advantage, our method can be used to counteract the Tiersma attack.

I. Introduction

To enhance ElGamal's protection based on discrete logarithm problem [1], He & Kiesler [2] broach a protection based on discrete logarithm and factorization problems. Although Tiersma [3] suggests that if the discrete logarithm problem can be dismantled, the

He & Kiesler scheme can also be cryptanalyzed and exposed to attacks. This paper is to enhance the He & Kielser scheme. In addition to providing He & Kiesler advantage, Tiersma's attack can be stopped.

The layout of this paper is as follows. Section II introduces ElGamal's signature scheme. Section III is our scheme. Section IV analyzes and discusses the security of our scheme. In Section V, we conclude the paper and provide the research direction for the future.

II. ElGamal's Signature Scheme

Let p be a strong prime number and g a primitive element over *GF(p)*. A user in network u_i selects a number $x(1 < x < \phi(p))$ as his/her private key. The public key satisfies the following equation

$$y \equiv g^x (\bmod p)$$

The procedure for the user u_i to attach the digital signature to message m is as follows.

(I) Selecting a number $k(1 < k < \phi(p))$ which is relatively prime to $\phi(p)$ and finding r and s satisfying the following equations.

$$r \equiv g^k (\bmod p) \qquad (1)$$

$$m \equiv xr + ks (\bmod \phi(p)) \qquad (2)$$

sign(m) = (r, s) is the .digital signature attached to the message m by u_i.

III. Our Scheme

Let p be a strong prime number and g a primitive element over *GF(p)*. $\phi(p)$ has two big prime factors p_1 and q_1 [2].

A user in network u_i selects a number $x_1(1 < x_1 < \phi(p))$ as his/her private key and then find x and y satisfying the following equations.

$$x \equiv x_1^3 (\bmod \phi(p)) \qquad (3)$$

$$y \equiv g^{x^3} (\bmod p) \qquad (4)$$

where y is the public key of the user u_i.

The user u_i can put a digital signature on the message m as follows:

Selecting a number $f_1 (1 < f_1 < \phi(p))$ and a number $t_1 (1 < t_1 < \phi(p), t_1 \neq f_1)$ which is relatively prime to $\phi(p)$. $t, f, k, r, R, s,$ and c are generated from t_1, f_1 on the basis of the following equations.

$$t \equiv t_1^3 (\bmod \phi(p)) \qquad (5)$$

$$f \equiv f_1^3 (\bmod \phi(p)) \qquad (6)$$

$$k \equiv t^3 (\bmod \phi(p)) \qquad (7)$$

$$r \equiv g^k (\bmod p) \qquad (8)$$

$$R \equiv g^{f^3} (\bmod p) \qquad (9)$$

$$mf \equiv x(r + R) + ts (\bmod \phi(p)) \qquad (10)$$

$$c \equiv x_1 t_1 f_1 (\bmod \phi(p)) \qquad (11)$$

sign(m) = (r, R, s, c) denotes the u_i's digital signature of the message m.

We can verify the validity of the equation

$$R^{m^3} \overset{?}{\equiv} y^{(r+R)^3} g^{3ms(r+R)c^3} r^{s^3} (\bmod p) \qquad (12)$$

The digital signature is correct if Eq.(12) is valid. If not, flaws can be expected.

IV. Analyses and Discussion

In this section, three theorems are proposed to deal with the cases if an attacker is going to attack our scheme, he/she has to solve discrete logarithm and factorization problems. However, we have pointed out that Tiersma's attack is improper to our scheme. In addition, this paper provides discussion about the use of parameters in verifying digital signature.

Theorem 1: Eq.(12) is true

Proof:

To have cubic on both sides of Eq.(10), we obtain six equations as follows.

$$m^3 f^3 \equiv x^3 (r + R)^3 + 3x^2 (r + R)^2 ts + 3x(r + R) t^2 s^2 + t^3 s^3 (\bmod \phi(p))$$

$$m^3 f^3 \equiv x^3 (r + R)^3 + 3x(r + R) ts[x(r + R) + ts] + t^3 s^3 (\bmod \phi(p))$$

According to Eq.(10), we have

$$m^3 f^3 \equiv x^3 (r+R)^3 + 3sm(r+R)xft + t^3 s^3 (\bmod \phi(p))$$

According to Eqs.(3), (5)-(7), (11), we have

$$m^3 f^3 \equiv x^3 (r+R)^3 + 3sm(r+R)c^3 + ks^3 (\bmod \phi(p))$$

$$g^{m^3 f^3} \equiv g^{x^3 (r+R)^3} g^{3sm(r+R)c^3} g^{ks^3} (\bmod p)$$

According to Eqs.(4), (8), (9),

$$R^{m^3} \equiv y^{(r+R)^3} g^{3ms(r+R)c^3} r^{s^3} (\bmod p)$$

Theorem 1 is proven, E.O.Q.

Theorem 2

The Tiersma attack on the He & Kiesler method is no longer valid to our scheme.

Proof:

Let the digital signature intercepted by an attacker be sign(m) = (r, R, s, c) and m be relatively prime to $\phi(p)$. The attacker is capable of solving the discrete logarithm problem. According to Eqs.(4), (8), and (9), the attacker can find x^3, k, and f^3. From Eq.(10), the attacker can obtain the following equations.

$$s \equiv t^{-1}[mf - x(r+R)](\bmod \phi(p)) \qquad (13)$$

$$sc^3 \equiv xf[mf - x(r+R)](\bmod \phi(p)) \qquad (14)$$

From Eq.(14), the attacker fails to find x because he has no knowledge of f, xf. Thus, unless the attacker can solve factorization problem, he/she can hardly find x. Consequently, the attacker cannot forge the digital signature and associated message m' as Tiersma claimed. Thus, our theorem can be proved. E.O.Q.

Theorem 2 tells us that an attacker can hardly undermine our scheme if he/she can only solve the discrete logarithm problem. Theorem 1 shows that Eq.(12) is correct. As long as the attacker can forge some parameters and make Eq.(12) valid, can the attacker win? Theorem 3 provides the answer.

Theorem 3

According to Eq.(12), only when an attacker has to solve discrete logarithm and factorization problems, can he/she win in forging digital signature.

Proof:

If an attacker tries to look for the forged digital signature $\mathrm{sign}(m_1)=(r_1,R_1,s_1,c_1)$ and attempts make Eq(12) valid, we classify five cases as follows.

Case 1.

Selecting m_1,r_1,R_1,s_1 at random and looking for the correspondent c_1. The attacker transfers Eq.(12) into the following equation

$$g^{3(r_1+R_1)m_1s_1c_1^3} \equiv R_1^{m_1^3}/[y^{(r_1+R_1)^3}r_1^{s_1^3}] \pmod p \qquad (15)$$

The attacker can find c_1^3 by solving discrete logarithm and obtain c_1 by working out factorization problem.

Case 2.

Selecting m_1,r_1,R_1,c_1 at random and looking for correspondent s_1.

The attacker has to transfer Eq.(12) into Eq.(16).

$$g^{3(r_1+R_1)m_1s_1c_1^3}r_1^{s_1^3} \equiv R_1^{m_1^3}/[y^{(r_1+R_1)^3}] \pmod p \qquad (16)$$

As long as we are going to find s_1 making Eq.(16) valid, no literature can propose any easier method than to solve discrete logarithm and factorization problems.

Case 3

Selecting m_1,r_1,c_1,s_1 and trying to work out R_1. The attacker transfers Eq.(12) into Eq.(17)

$$R_1^{m_1^3}/[y^{(r_1+R_1)^3}g^{3(r_1+R_1)m_1s_1c_1^3}] \equiv r_1^{s_1^3} \pmod p \qquad (17)$$

No literature has proposed a better approach to solving discrete logarithm and factorization problems to work out R_1.

Case 4

Choosing m_1, R_1, c_1, s_1 at random and finding correspondent r_1.

The attacker transfers Eq.(12) into Eq.(18)

$$y^{(r_1+k_1)^3} g^{3(r_1+R_1)m_1 s_1 c_1^3} r_1^{s_1^3} \equiv R_1^{m_1^3} (\bmod p) \tag{18}$$

No literature has proposed a better approach to solving discrete logarithm and factorization problems to work out r_1.

Case 5

Choosing r_1, R_1, c_1, s_1 and finding correspondent m_1.

The attacker transfers Eq.(12) into Eq.(19).

$$R_1^{m_1^3} / g^{3(r_1+R_1)m_1 s_1 c_1^3} \equiv y^{(r_1+R_1)^3} r_1^{s_1^3} (\bmod p) \tag{19}$$

No literature has proposed a better approach to solving discrete logarithm and factorization problems to work out m_1.

In order to avoid being attacked, ElGamal suggests not using the same r in Eq.(1) to find the private key. For the same reason, in digital signature, the values of (r_a, R_a) and (r_b, R_b) should satisfy the four conditions as follows.

$r_a \not\equiv R_a (\bmod p)$

$r_b \not\equiv R_b (\bmod p)$

$r_a \not\equiv r_b (\bmod p)$

$R_a \not\equiv R_b (\bmod p)$

Then, the Tiersma attack cannot win.

V. Conclusion and direction for future research

Given the solution of discrete logarithm, Tiersma focuses on obtaining the square of the private key (i.e., x, please see p.47 of reference 3) and then forging the digital signature of the user under attack to detour the factorization problem. In order to counteract this attack, we need an additional parameter f_1 to result in a failure to find the private key (x, see Eqs.(3) & (14)). With our scheme, an attacker can hardly detour the factorization problem. Thus, in addition to the He & Kiesler advantage, our method can be used to counteract the Tiersma attack.

If a time stamp scheme can be linked with the method presented in this paper, we can stop replay attack. To be sure, a hashing function plus the ElGamal theory can strengthen our scheme. In addition, the study of methods for reducing the parameter numbers of digital signatures and the applications of our approach to multi-signature, secret sharing, and group-oriented digital signature are worthy of future research.

References

[1] ElGamal, T., "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete logarithm," IEEE Transactions on Information Theory, Vol.31, No.4, pp.469-472, 1985.

[2] HE. J.. and KIESLER, T.: Enhancing the secruity of ElGamal's signature scheme," IEE proc., E., 1994, 141, (4), pp.249-252.

[3] Tiersma, H.J. : Enhancing the secruity of ElGamal signature scheme: technical note, IEE Proc., E., 1997, 144, (1), pp.47-48.