Available online at www.sciencedirect.com

SCIENCE DIRECT®

The Journal of Systems and Software 79 (2006) 502–506

The Journal of Systems and Software

www.elsevier.com/locate/jss

Improved self-certified group-oriented cryptosystem without a combiner

Wei-Bin Lee *, Kuan-Chieh Liao

Department of Information Engineering and Computer Science, Feng Chia University, 100, Wenhwa Road, Seatwen, Taichung 407, Taiwan, ROC

Received 30 May 2004; received in revised form 8 March 2005; accepted 12 April 2005
Available online 1 June 2005

Abstract

In 2001, Ghodosi and Saeednia proposed a self-certified group-oriented cryptosystem without a combiner to prevent the Susilo et al.'s attack. However, in this paper we will show that their scheme is still insecure and probably suffers from the conspired attack. To remedy the weakness, an enhanced version is proposed while providing the new functionality to confirm the source of the encrypted message.

Keywords: Group-oriented cryptosystem; Self-certified; Public key cryptosystem

1. Introduction

A group-oriented cryptosystem is one of the society-oriented cryptographic systems, which allows group participants to perform a cryptographic operation respectively. A (t,n) group-oriented cryptosystem is constructed by a sender who composes the subgroup $P = \{U_1, U_2, \ldots, U_n\}$ of all users as the intended receivers in the system. In this cryptosystem, an encrypted message is split into n shares, and the sender distributes those separated shares to each member of the group P. At least t or more participants of the group P are required to decrypt the encrypted message with their own shares. Two important issues of such cryptosystems' implementation are:

(1) The sender needs to collect those authenticated public keys of the intended receivers.
(2) The combiner needs a secure channel to collect the partial results from collaborating participants.

In 1999, Saeednia and Ghodosi discussed these two relevant problems in implementation of such systems and then proposed a (t,n) group-oriented cryptosystem (Saeednia and Ghodosi, 1999) that works with self-certified public keys. Therefore, the public keys of the users are publicly certifiable. In addition, the threshold encryption system does not require a combiner and allows each group member to perform the decryption procedure once at least t group members participate.

However, Susilo and Safavi-Naini (1999) show that any two members in the group can decrypt an encrypted message conspiratorially without other members' collaboration. After that, Ghodosi and Saeednia proposed a new version (Ghodosi and Saeednia, 2001) to prevent the Susilo et al. 's attack. Unfortunately, the modified scheme is still insecure and suffers from the conspired attack.

In this paper, we will show that three malicious members have high probability 0.608 to decrypt an encrypted message without working together with other $t-3$ members. In addition, a remedy is proposed not only

[*] Corresponding author. Tel.: +886 4 24517250x3751; fax: +886 4 24516101.

E-mail addresses: wblee@fcu.edu.tw (W.-B. Lee), p9112062@knight.fcu.edu.tw (K.-C. Liao).

0164-1212/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2005.04.007

prevents such conspire attack in an efficient way, but also allows the group of receivers to assure that the encrypted message coming from the one alleged. Thus, the new scheme is further functionally superior to the Ghodosi and Saeednia's modified scheme.

2. Review

First, we take a brief review of the Ghodosi and Saeednia's modified protocol (Ghodosi and Saeednia, 2001) and make our comment comprehensibly.

2.1. Preparation phase

Without loss of generality, let $P = \{U_1, U_2, \ldots, U_t\}$ be the intended group setting up by a trusted authority. And the following parameters are also chosen by the trusted authority.

N the product of two large distinct primes p and q such that $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also prime integers,

F a prime, where $F > N$,

g a generator of order $r = p'q'$,

$h(\cdot)$ a one way hash function that outputs integers less than the minimum value of p' and q'.

The authority makes N, F, g, $h(\cdot)$ public while keeping r secret.

2.2. Key generation phase

(1) Each group member chooses his secret key x_i, computes

$$z = g^{x_i} \bmod N,$$

and gives the value z to the authority.

(2) The trusted authority chooses a random number r_i and gives it to U_i.

(3) The secret value of the user U_i is $X_i = x_i + r_i$ and his shadow is

$$Z_i = z \cdot g^{r_i} = g^{x_i + r_i} = g^{X_i} \bmod N. \quad (1)$$

(4) After the authority is convinced that the user knows the secret key, he generates the user's public key as

$$y_i = (Z_i^{-1} - ID_i)^{ID_i^{-1}} \bmod N, \quad (2)$$

where $ID_i = h(I_i)$, and I_i is the U_i's identity such as his name, network address, …, etc.

2.3. Encryption phase

Suppose a sender wants to send a message $0 \leqq m \leqq N$ to the group $P = \{U_1, U_2, \ldots, U_n\}$ such that the cooperation of any t members of the group is sufficient to retrieve the message. Afterwards, the sender proceeds as follows:

(1) Choose a random number k and compute $c = g^{-k} \bmod N$.

(2) Construct a polynomial $f(x) = a_0 + a_1 x + a_2\, x^2 + \cdots + a_{t-1} x^{t-1}$ in $GF(F)$, such that $f(0) = a_0 = g^{h(m)} \bmod N$.

(3) Compute

$$w_i = y_i^{ID_i} + ID_i \bmod N,$$
$$s_i = w_i^k \bmod N,$$
$$d_i = f(s_i), \quad \text{and}$$
$$e_i = m w_i^{h(m)} \bmod N, \quad \text{for } i = 1, 2, \ldots, n.$$

(4) Send (t, c, d_i, e_i) to each member U_i in the group.

2.4. Decryption phase

Any t members of the group must collaborate in order to retrieve the message. Without loss of generality, it can be assumed $U_1, U_2, \ldots$, and U_t want to decrypt the message. They calculate

$$s_i = c^{X_i} \bmod N, \quad \text{for } i = 1, 2, \ldots, t,$$

and broadcast the pair (d_i, s_i) to each other. Then the t members can cooperate together to obtain $v = g^{h(m)} \bmod N$.

According to the secret parameter v, all the members can further derive the message individually as

$$m = v^{X_i} e_i \bmod N.$$

Note that, the decryption phase can be divided into two parts. First, the collaboration of at least t participants is required to reconstruct the secret parameter v. Second, according to v, each member then decrypts message individually without the help of a combiner. However, in the following, we will show that a conspiracy of three members in the group is possible to obtain the secret parameter v and then the message is revealed directly without working together with other $t - 3$ group members.

3. Conspired attack

Without loss of generality, assume that U_1, U_2, and U_3 in the group desire a complicit usurpation of the plaintext. They can firstly inherit e_1, e_2, and, e_3 from the encrypted broadcasting message, where

$$\begin{aligned} e_1 &= m w_1^{h(m)} \\ &= m(y_1^{ID_1} + ID_1)^{h(m)} \\ &= m(((Z_1^{-1} - ID_1)^{ID_1^{-1}})^{ID_1} + ID_1)^{h(m)}, \text{ according to Eq. (2)} \\ &= m(Z_1^{-1} - ID_1 + ID_1)^{h(m)} \\ &= m Z_1^{-h(m)} \\ &= m g^{-X_1 h(m)} \bmod N, \text{ according to Eq. (1),} \end{aligned}$$

$e_2 = mg^{-X_2 h(m)} \bmod N$, and

$e_3 = mg^{-X_3 h(m)} \bmod N$.

After that, they can collaboratively calculate γ_1 and γ_2 as follows:

$$\gamma_1 = \frac{e_1}{e_2} = \frac{mg^{-X_1 h(m)}}{mg^{-X_2 h(m)}} = g^{-(X_1 - X_2)h(m)} = (g^{h(m)})^{(X_2 - X_1)} \bmod N,$$

and

$$\gamma_2 = \frac{e_1}{e_3} = \frac{mg^{-X_1 h(m)}}{mg^{-X_3 h(m)}} = g^{-(X_1 - X_3)h(m)} = (g^{h(m)})^{(X_3 - X_1)} \bmod N.$$

With the knowledge of the secret X_1, X_2, and X_3, the plaintext m can be revealed if $(X_2 - X_1)$ and $(X_3 - X_1)$ are relatively prime.

(1) Find integers a and b such that
$a(X_2 - X_1) + b(X_3 - X_1) = 1$.

(2) Compute

$$\begin{aligned} v &= g^{h(m)} \bmod N \\ &= (g^{h(m)})^{a(X_2 - X_1) + b(X_3 - X_1)} \bmod N \\ &= ((g^{h(m)})^{(X_2 - X_1)})^a \cdot ((g^{h(m)})^{(X_3 - X_1)}) \bmod N \\ &= (\gamma_1)^a \cdot (\gamma_2)^b \bmod N. \end{aligned}$$

(3) Obtain the plaintext m as

$$m = v^{X_i} e_i \bmod N.$$

From the above, the critical point is the existence of a and b; that is, the success of the conspired attack is only determined by whether $(X_2 - X_1)$ and $(X_3 - X_1)$ are relative prime or not.

Since that x_i is the secret key chosen randomly by U_i, and r_i is the random number chosen by authority. Therefore, $X_i = x_i + r_i$ is also a random number. It implies that $(X_2 - X_1)$ and $(X_3 - X_1)$ are both random numbers. Because the probability of two random numbers being relative prime is 0.608 (Knuth, 1981), the probability is obviously too high.

Hence, a conspiracy of these three group members may decrypt an encrypted message without working together with other $t - 3$ members, and the high probability is unacceptable.

4. Proposed method

In the following, a modification of the Ghodosi and Saeednia's scheme is proposed to eliminate the weakness of the conspiracy attack and provide the origin authentication. The modification is just applied to the encryption and decryption phase under the same scenario.

4.1. Modified encryption phase

The sender will do as follows for the recipient group $P = \{U_1, U_2, \ldots, U_n\}$.

(1) Choose a random number k_1 and compute
$K = g^{k_1} \bmod N$, and
$\sigma = k_1 K + x_s$,
where x_s is the sender's private key, and $y_s = g^{x_s} \bmod N$ is the corresponding public key.

(2) Construct a polynomial $f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$ in $GF(F)$.

(3) Choose a random number k_2 and compute

$$\begin{aligned} &c = g^{-k_2} \bmod N, \\ &w_i = y_i^{ID_i} + ID_i \bmod N, \\ &s_i = w_i^{k_2} \bmod N, \\ &d_i = f(s_i), \quad \text{and} \\ &e_i = m \cdot h(w_i^{-\sigma})^{-1} \bmod N. \end{aligned} \tag{3}$$

(4) Send (t, c, d_i, e_i) to each member U_i in the group P.

4.2. Modified decryption phase

Any t members of the group must collaborate in order to retrieve the message. Without loss of generality, assume $U_1, U_2, \ldots,$ and U_t want to decrypt the message. They calculate

$$s_i = c^{X_i} \bmod N, \quad (i = 1, 2, \ldots, t)$$

and broadcast the pair (d_i, s_i) to each other.

Then t members can cooperate together to recover $f(x)$ according to the value pairs and further obtain K if all the pairs are correct.

The correctness of s_i can be proved as

$$\begin{aligned} s_i &= w_i^{k_2} \bmod N, \\ &= (y_i^{ID_i} + ID_i)^{k_2} \bmod N \\ &= (((Z_i^{-1} - ID_i)^{ID_i^{-1}})^{ID_i} + ID_i)^{k_2} \bmod N, \text{ according to Eq. (2)} \\ &= (Z_i^{-1} - ID_i + ID_i)^{k_2} \bmod N \\ &= Z_i^{-k_2} \bmod N \\ &= (g^{X_i})^{-k_2} \bmod N, \text{ according to Eq. (1)} \\ &= (g^{-k_2})^{X_i} \bmod N \\ &= c^{X_i} \bmod N. \end{aligned}$$

Based on K, the message m can be derived as

$$m = h((K^K \cdot y_s)^{X_i}) \cdot e_i \bmod N, \quad \text{and} \tag{4}$$

the correctness is shown as follows.

According to Eq. (3), we have

$$\begin{aligned} m &= h(w_i^{-\sigma}) \cdot e_i \bmod N \\ &= h((y_i^{ID_i} + ID_i)^{-\sigma}) \cdot e_i \bmod N \\ &= h((((Z_i^{-1} - ID_i)^{ID_i^{-1}})^{ID_i} + ID_i)^{-\sigma}) \\ &\quad \cdot e_i \bmod N, \text{ according to Eq. (2)} \\ &= h(((Z_i^{-1} - ID_i) + ID_i)^{-\sigma}) \cdot e_i \bmod N \\ &= h((Z_i^{-1})^{-\sigma}) \cdot e_i \bmod N \\ &= h((g^{-X_i})^{-\sigma}) \cdot e_i \bmod N, \text{ according to Eq. (1)} \end{aligned}$$

$$\begin{aligned}&= h((g^{\sigma})^{X_i}) \cdot e_i \bmod N\\ &= h((g^{k_1K} + x_s)^{X_i}) \cdot e_i \bmod N\\ &= h((g^{k_1K} \cdot g^{x_s})^{X_i}) \cdot e_i \bmod N\\ &= h((K^K \cdot y_s)^{X_i}) \cdot e_i \bmod N.\end{aligned}$$

Thus, Eq. (4) can decrypt the ciphertext correctly if all the involved keys are genuine.

5. Discussion

The trusted authority has no knowledge of the secret value of any user, because the key generation phase is tally the same as the original design. Accordingly, the focus is shifted to the encryption and decryption phase, so two major concerns exist in the proposed scheme.

(1) Collaboration of at least t participants is required to perform the designated cryptographic operation.

Assume that a group of legal members $(U_1, U_2, \ldots, U_u)$, where $1 \leqq u \leqq t-1$, conspires, and desires to derive the encrypted message. Under this assumption, the conspiracy can derive $(d_1, d_2, \ldots, d_u)$ from the broadcasting message, and obtain $(s_1, s_2, \ldots, s_u)$ by calculating $s_i = c^{X_i} \bmod N$, $(i = 1, 2, \ldots, u)$. Then, the conspiracy may intend to solve the $(t-1)$ degree polynomial $f(x)$ and derive the key point of the decryption process K. But, fortunately, $f(x)$ can be recovered only if greater then t out of n shares (d_i, s_i), where $1 \leqq i \leqq n$, are available. Thus, the message m is still unrevealed.

Furthermore, it is also impossible to do that by solving the following u equations

$$\begin{aligned}e_1 &= m \cdot h((K^K \cdot y_s)^{X_1})^{-1} \bmod N,\\ e_2 &= m \cdot h((K^K \cdot y_s)^{X_2})^{-1} \bmod N,\\ &\vdots\\ e_u &= m \cdot h((K^K \cdot y_s)^{X_u})^{-1} \bmod N.\end{aligned}$$

Because the decryption key is hashed, the mathematical relation cannot be found and predicted, hence it leaves no way to solve K. Thus the scheme can resist the conspiracy attack.

(2) The source of the encrypted message can be assured.

Assume that a forger intends to impersonate the sender to encrypt the message m^* the critical issue is to compute e_i to satisfy Eq. (4) so that

$$m^* = e_i \cdot h((K^K \cdot y_s)^{X_i})^{-1} \bmod N, \quad \text{where } 1 \leqq i \leqq n.$$

It is easy to understand that anyone can embed K into a $(t-1)$ degree polynomial, but the question is now whether $(K^K \cdot y_s)^{X_i} \bmod N$ can only be determined by the sender, where $1 \leqq i \leqq n$.

Since

$$\begin{aligned}(K^K \cdot y_s)^{X_i} &= (g^{k_1K} \cdot g^{x_s})^{X_i} \bmod N\\ &= (g^{k_1K + x_s})^{X_i} \bmod N\\ &= (g^{X_i})^{k_1K + x_s} \bmod N\\ &= w_i^{k_1K + x_s} \bmod N, \text{ according to Eq. (1).}\end{aligned}$$

Accordingly, it is obvious that $(K^K \cdot y_s)^{X_i} \bmod N$, where $1 \leqq i \leqq n$, cannot be derived without the knowledge of the sender's private key x_s or user U_i's secret value X_i. Besides, it is clear that the calculation of x_s and X_i form the equations

$$\begin{aligned}&y_s = g^{x_s} \bmod N, \text{ and}\\ &Z_i = g^{X_i} \bmod N,\end{aligned}$$

are as difficult as solving the discrete logarithm problem. Thus, it implies that impersonate the sender to encrypt the message can be prevented while the sender's private key x_s and U_i's secret value X_i are still secure.

6. Conclusion

In this paper, we have shown that at least three group members in the Ghodosi and Saeednia's scheme can conspire successfully with an unacceptable high probability 0.608. Hence, an improved approach is proposed which eliminate the vulnerable mathematical relation in the Ghodosi and Saeednia's modified scheme. Therefore, the security of our system is no longer assessed by an amount of the probability but shifting to the computational complexity. In addition, our threshold encryption scheme also providing a new functionality which allows the group of receivers to assure that the message is from the alleged one.

References

Ghodosi, H., Saeednia, S., 2001. Modification to self-certified group-oriented cryptosystem without combiner. Electronics Letters 37 (2), 1453–1454.

Knuth, D., 1981. The Art of Computer Programming: vol. 2 Seminumerical Algorithms, second ed. Addison-Wesley, Chapter 4.5.2, Theorem D, pp. 324.

Saeednia, S., Ghodosi, H., 1999. A self-certified group-oriented cryptosystem without a combiner. ACISP99, Lecture Notes in Computer Science 1587, 192–201.

Susilo, W., Safavi-Naini, R., 1999. Remark on self-certified group-oriented cryptosystem without combiner. Electronics Letters 35 (18), 1539–1540.

Wei-Bin Lee received his B.S. degree from the Department of Information and Computer Engineering, Chung-Yuan Christian University, Chungli, Taiwan, in 1991 and his M.S. degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi, Taiwan in 1993. He received his Ph.D. degree in 1997 from National Chung Cheng University. Since 1999, he has been with the Department of Information Engineering at Feng Chia University, where he is currently an associate professor. His research interests currently include cryptography, information security management, steganography, and network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.

Kuan-Chieh Liao received his B.S. degree from the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, in 2001, and his M.S. degree in Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, in 2002. He is currently pursuing his Ph.D. degree in Department of Information Engineering and Computer Science, Feng Chia University. His research interests currently include cryptography, steganography, and network security.