A Collusion Attack on Ghodosi and Saeednia's Scheme

(對 Ghodosi 和 Saeednia 系統之共謀攻擊分析)

Chien-Yuan Chen
Department of Information Engineering,
I-Shou University, Kaohsiung County,
Taiwan, 840 R.O.C
E-mail: cychen@isu.edu.tw

Chih-Cheng Hsueh
Department of Information Engineering,
I-Shou University, Kaohsiung County,
Taiwan, 840 R.O.C
E-mail: jdjdtw@giga.net.tw

中文摘要

在這篇論文中，我們提出一種共謀的攻擊方式，來攻擊 Ghodosi 和 Saeednia 所改良的不須結合者的自我認證的團體密碼系統[1]。根據我們的分析，若八個人以上共謀，則至少有 0.9239 的機率可以求得訊息 m。

關鍵字: 自我驗證公開金匙，密碼學

Abstract

In this paper, we present the collusion attack on the improved self-certified group-oriented cryptosystem without combiner such that the message can be discoved with high probability.

Keyword: self-certified public key, cryptography

1. Introduction

In 1999, a self-certified group-oriented cryptosystem without combiner was introduced by Saeednia and Ghodosi [2]. However, Susilo and Safavi presented an attack on it in 1999 [4]. Thus, Ghodosi and Saeednia presented an improved self-certified group-oriented cryptosystem without combiner in 2001 [1]. But, in this paper, we find that the improved scheme will suffer from the collusion attack with high probability.

The remainder of this paper is organized as follows. Section 2, we give a brief review of Ghodosi and Saeednia's scheme. Next, we describe our collusion attack on Ghodosi and Saeednia's scheme in Section 3. Section 4 draws the conclusions from our attack.

2. Review of Ghodosi and Saeednia's scheme

In this section, we briefly review the improved self-certified group-oriented cryptosystem without combiner. In that scheme, there is a trusted authority (TA) to setup the system parameters. First, TA chooses two primes p and q such that $p-1=2p'$ and $q-1=2q'$, where p' and q' are primes. Then, TA computes $N=pq$ and selects a base $g \neq 1$ of order $r = p'q' \bmod N$. Further, TA chooses a prime $F>N$ and a one-way function $h(\cdot)$ such that the hash values are less than $\min(p', q')$. Then, TA publishes g, $h(\cdot)$, F and N. Let $U=\{U_1, U_2, \ldots, U_L\}$ be a group of L members. Each U_i can obtain his self-certified public key from TA by performing following protocol.

Step 1: U_i chooses his initial secret key x_i to compute $z_i' = g^{x_i} \bmod N$. Then, U_i sends z_i' to TA.

Step 2: TA chooses a random value r_i and sends it to U_i.

Step 3: U_i computes his new secret value $X_i=x_i+r_i$ and $z_i = z_i' \times g^{r_i} = g^{x_i+r_i} = g^{X_i} \bmod N$. Then, U_i sends z_i to TA.

Step 4: TA generates U_i's public key $y_i = (z_i^{-1} - ID_i)^{ID_i^{-1}} \bmod N$ and sends it to U_i.

Step 5: U_i can verify y_i by $z_i(y_i^{ID_i} + ID_i) = 1 \bmod N$.

Therefore, the public key and secret key of U_i are y_i and X_i, respectively.

Encryption and Decryption:

Assume that the sender wants to send a message m to the group P, where P contains n members of U, say $\{U_1, U_2, \ldots, U_n\}$. According to [1], in the group P, any t of n members can cooperate to obtain the message m by performing following encryption and decryption processes. First, the sender chooses a random integer k and computes $c = (g^{-1})^k \bmod N$. Then, the sender randomly generates a polynomial $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{t-1} x^{t-1}$ in GF(F), where $g(0) = b_0 = g^{h(m)} \bmod N$. Finally, the sender computes $w_i = y_i^{ID_i} + ID_i \bmod N$, $s_i = w_i^k \bmod N$, $d_i = g(s_i)$, $e_i = m w_i^{h(m)} \bmod N$ and sends (t, c, d_i, e_i) to U_i, where i=1 to n. Note that the above e_i can be computed by

$$e_i = m g^{-X_i h(m)} \bmod N. \qquad (1)$$

If t members want to get the message m, each member U_i must compute $s_i = c^{X_i} \bmod N$ and broadcasts his pair (d_i, s_i). When U_i receives t pairs, U_i can recover $v = g^{h(m)} \bmod N$ and get the message $m = v^{X_i} e_i \bmod N$.

3. Our Attack

In this section, we present a collusion attack on Ghodosi and Saeednia's scheme. Assume that k members conspire to discover the message m, where k is even member and less than t. Let the k members be $\{U_1, U_2, \ldots, U_k\}$. At first, they reveal their secret keys $\{X_1, X_2, \ldots, X_k\}$ and their received ciphertexts $\{e_1, e_2, \ldots, e_k\}$ to each other. Then, any two members U_i and U_j jointly remove the hash value from their ciphertexts e_i and e_j by computing

$$t_{ij} = \frac{e_i^{a_j}}{e_j^{a_i}} \bmod N, \qquad (2)$$

where $a_i=X_i/\gcd(X_i, X_j)$ and $a_j=X_j/\gcd(X_i, X_j)$. From Equation (1), we have

$$t_{ij} = \frac{(m g^{-X_i h(m)})^{a_j}}{(m g^{-X_j h(m)})^{a_i}} = m^{a_j - a_i} \bmod N.$$

Therefore, U_1 and U_2 can get $t_{12} = m^{a_2 - a_1} \bmod N$. Similarly, U_3 and U_4 can get $t_{34} = m^{a_4 - a_3} \bmod N$. If gcd($a_2$-$a_1$, a_4-a_3)=1, there exist two integer s_{12} and s_{34} such that $s_{12}(a_2-a_1)+s_{34}(a_4-a_3)=1$. Then, we can discover m by computing $m = t_{12}^{s_{12}} + t_{34}^{s_{34}} \bmod N$. Furthermore, consider k/2 pairs $\{(U_1, U_2), (U_3, U_4), \ldots, (U_{k-1}, U_k)\}$. If gcd($a_2$-$a_1$, a_4-a_3, …, a_k-a_{k-1})=1, we can discover the message m.

Next, we discuss the odds of our collusion attack. Because the secret keys X_i and X_j are randomly selected by the members and TA, the value a_j-a_i can be viewed as a random number. According to [4], the probability that $k/2$ randomly selected integers is coprime is $W_{k/2} \approx [\zeta(k/2)]^{-1}$, where $\zeta(k/2)$ is Riemann's zeta function. By this theorem, if k=8, we have $W_4 \approx 90/\pi^4$ =0.9239. Thus, the k members conspire to discover message m with high probability when $k \geq 8$.

4. Conclusion

In this paper, we analyze the improved scheme [1] from the collusion attack. We show that the odds of discovering the message m are at least 0.9239 when at least 8 members collude.

ACKNOWLEDGMENTS

This research was partially supported by the National Science Council (NSC), the Republic of China, under the contact NSC-89-2745-P-214-004.

References

[1] Ghodosi, H. and Saeednia, S.: "Modification to self-certified group-oriented cryptosystem without a comber", Electron. Lett., 37, pp. 86-87, 2001.

[2] Saeednia, S. and Ghodosi, H.: "A self-certified group-oriented cryptosystem without a comber", Proc. Australasian Conference on Information Security and Privacy (ACISP'99), pp. 192-201, 1999.

[3] Schroeder, M. R.: Number theory in science and communication, 2nd edition, Springer-Verlag Berlin Heidelberg New York Tokyo, 1984.

[4] Susilo, W., and Safavi-Naini, R.: "Remark on self-certified group-oriented cryptosystem without a comber", Electron. Lett., 35, pp. 1539-1540, 1999.