Remark on Self-Certified Group-Oriented Cryptosystem Without a Combiner

Indexing terms: Group-Oriented Cryptosystem

In a (t, n) group-oriented cryptosystem collaboration of at least t participants is required to perform the designated cryptographic operation. In this paper, we show that a recently proposed group-oriented encryption scheme by Saeednia and Ghodosi is insecure and allows two participants to collude and decrypt an encrypted message.

Introduction: In a *threshold cryptosystem* the cryptographic power of the transmitter, or the receiver, is distributed among a group of n participants such that any t out of n participant can perform the designated cryptographic operation. Recently Saeednia et.al [1] proposed a threshold cryptosystem that allows a group of t participant to collaboratively decrypt an encrypted message.

Recently Saeednia et.al. [1] proposed a threshold encryption system that does not require a combiner and allows each group member to decrypt an encrypted message once at least t group members partcipate in the decryption process. An attractive feature of the system is that public keys of users are publicly certifiable. In this paper, we show that the proposed scheme does not resist against conspiracy attack by two group members.

A Self-Certified Group-Oriented Cryptosystem without a Combiner: In this section we briefly review the scheme proposed in [1].

Model

There exists a trusted authority who sets up the system. There are n group members, $(U_1, U_2, \cdots, U_n)$.

Setup Phase

The trusted authority sets up the system and chooses the following parameters.

- An integer N which is the product of two distinct safe primes p and q ($p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also prime integers).

- A prime $F > N$.

- A base $\alpha \neq 1$ of order $r = p'q' \bmod N$.

- A one way hash function h, that outputs integers less than the minimum value of p' and q'.

The authority makes (α, h, F, N) public, keeps r secret and discards p and q.

Key Generation

A group member chooses his secret key x and computes his shadow $z = \alpha^x \ mod \ N$. Next, he sends the shadow value to the authority. After the authority is convinced that the user knows the secret key, he generates the user's public key as

$$y = (z^{-1} - ID)^{ID^{-1}} \ mod \ N$$

where $ID = h(I)$, and I corresponds to the user's identity (such as his name, address, etc).

Encryption

Suppose Alice wants to encrypt a message m for the group. She will do the following steps:

1. Randomly chooses k and computes $c = (\alpha^{-k} \ mod \ N)$.

2. Form a polynomial of degree $t-1$ in $GF(F)$, such that $g(0) = \alpha^{h(m)} \ mod \ N$.

3. Computes for $i = 1, \cdots, n$ (where n denotes the number of users in the group)

$$
\begin{aligned}
w_i &= y_i^{ID_i} + ID_i \ mod \ N \\
s_i &= w_i^k \ mod \ N \\
d_i &= g(s_i) \\
e_i &= mw_i^{h(m)} \ mod \ N
\end{aligned}
$$

and sends (t, c, d_i, e_i) to each member U_i in the group.

Decryption

To decrypt a cryptogram, a group of at least t group members, must collaborate. Without loss of generality assume $U_1, \cdots U_t$ want to decrypt a message. Firstly, $U_i, i = 1, \cdots t$ calculates

$$s_i = c^{x_i} \ mod \ N$$

and broadcasts the pair (d_i, s_i). After t such pairs are broadcasted, each U_i can recover $v = \alpha^{h(m)} \ mod \ N$ and compute the plaintext message as

$$m = v^{x_i} e_i \ mod \ N$$

Conspiracy Attack: In this section, we show that a conspiracy of two members in the group can decrypt an encrypted message without the need for collaboration of the other members.

Suppose, a member U_1 who has chosen a secret key x_1 wants to join the group. He will be interrogated by the trusted authority and once successful, will obtain his public key as

$$y_1 = (\alpha^{-x_1} - ID_1)^{ID_1^{-1}} \ mod \ N$$

Next, another member U_2 conspires with U_1 and chooses her secret key as $x_2 = 2x_1$. She will also be interrogated by the trusted authority and once is able to convince him of the knowledge of the relevant secret key, obtains her public key as

$$y_2 = (\alpha^{-x_2} - ID_2)^{ID_2^{-1}} \ mod \ N$$

Now when an encrypted message is broadcasted, U_1 and U_2 will do the following. First they calculate,

$$e_1 = m\alpha^{-x_1 h(m)} \ mod \ N$$

and

$$e_2 = m\alpha^{-x_2 h(m)} \ mod \ N$$

which is equal to

$$e_2 = m\alpha^{-2x_1 h(m)} \ mod \ N$$

Next they can collaboratively obtain the plaintext by first calculating γ as follows (all operations are in $mod \ N$).

$$\begin{aligned}
\gamma & = \frac{e_2}{e_1} \\
& = \frac{m\alpha^{-2x_1 h(m)}}{m\alpha^{-x_1 h(m)}} \quad (1) \\
& = \alpha^{-x_1 h(m)}
\end{aligned}$$

And finally they will obtain the plaintext m as

$$\begin{aligned}
m & = \frac{e_1}{\gamma} \\
& = \frac{m\alpha^{-x_1 h(m)}}{\alpha^{-x_1 h(m)}} \quad (2)
\end{aligned}$$

Note that the step in equation 1 or 2 may fail. If the step fails, it means that

$$gcd(m\alpha^{-x_1 h(m)}, N) \neq 1$$

(in equation 1) or

$$gcd(\alpha^{-x_1 h(m)}, N) \neq 1$$

(in equation 2). In this case they are able to obtain a non-trivial factor of N, given by

$$p = gcd(m\alpha^{-x_1 h(m)}, N)$$

or

$$p = gcd(\alpha^{-x_1 h(m)}, N)$$

Hence, without the help of any other group member the two conspirators can either obtain the plaintext, or break the whole system (by factorising N). This means that the scheme does not provide the claimed level of security.

Conclusion: We have shown that the scheme proposed in [1] does not resist a conspiracy attack by two group members and hence is insecure.

Willy Susilo and Rei Safavi-Naini
Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, AUSTRALIA

References

[1] Shahrokh Saeednia and Hossein Ghodosi. A self-ceritified group-oriented cryptosystem without a combiner. *ACISP 99, Lecture Notes in Computer Science 1587*, pages 192–201, 1999.