# Cryptanalysis of Modification to Self-Certified Group-Oriented Cryptosystem Without A Combiner

Willy Susilo[1] and Hiroaki Kikuchi[2]
*(Corresponding author: Willy Susilo)*

Centre for Information Security Research School of Information Technology and Computer Science[1]
University of Wollongong Wollongong 2522, Australia (Email: wsusilo@uow.edu.au)
Department of Electrical Engineering School of Information Technology and Electronics[2]
Tokai University, Japan (Email: kikn@ep.u-tokai.ac.jp)

*(Received Dec. 18, 2005; revised and accepted Dec. 31, 2005)*

## Abstract

In a $(t, n)$ group-oriented cryptosystem collaboration of at least $t$ participants is required to perform a designated cryptographic operation. This type of cryptographic operation is very important to support an ad-hoc type network, such as the one that is built using Bluetooth or ad-hoc wireless LAN, since the existence of a combiner is not required to decrypt an encrypted message. In the earlier paper, it was shown that a group-oriented encryption scheme, as proposed by Saeednia and Ghodosi, can be subjected to a conspiracy attack in which two participants collude to decrypt an encrypted message. Recently, it was shown that the modified scheme is subjected to a conspiracy attack of at least three group members with probability 0.608. In this paper, we show a stronger result that shows *any* conspiracy of at least three group members can collude and decrypt an encrypted message.

*Keywords: Conspiracy attack, cryptography, group-Oriented Cryptosystem*

## 1 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 $n$ participants can perform the designated cryptographic operation.

Saeednia and Ghodosi [5] proposed a threshold encryption system that allows a group of $t$ participants to collaboratively decrypt an encrypted message. An attractive feature of the system was that public keys of users were publicly verifiable.

We showed [6] that the scheme was vulnerable to a conspiracy attack by two colluders.

In 2001, Ghodosi and Saeednia [3] proposed a modified scheme that was resistant against this attack.

Very recently, Lee and Liao [4] showed that a conspiracy attack by three users can successfully decrypt an encrypted message with a probability 0.608.

In this paper, we strengthen the result of Lee and Liao [4] by showing that the modified scheme is *vulnerable* to *any* conspiracy attack by three or more users.

The paper is organized as follows. In the next section, we briefly recall the scheme proposed in [3]. In Section 3, we describe a conspiracy attack against the scheme and Section 4 concludes the paper.

## 2 A Self-Certified Group-Oriented Cryptosystem Without a Combiner

For completeness, in this section, we briefly review the scheme proposed in [3]. The scheme is as follows.

**Model:**
There is a group $U_1, U_2, \cdots, U_n$ of $n$ participants and a trusted authority (TA).

**Setup Phase:**
TA 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 $r = p'q' \ mod \ N$.
- A one way hash function $h$ that outputs integers less than $p'$ and $q'$.

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

**Key Generation:**
A group member $U_i$ chooses his secret key $x_i$, computes its shadow $z_i = \alpha^{x_i} \ mod \ N$, and sends $z_i$ to TA. He then uses a zero-knowledge protocol to convince the TA that he knows the secret key. TA chooses a random value $r_i$ and sends it to $U_i$ and also generates $U_i$'s public key as,

$$y_i = (z_i^{-1} - ID_i)^{ID_i^{-1}} \ mod \ N,$$

where $ID_i = h(I_i)$ and $ID_i$ is the $U_i$'s identity ($I_i$ can be some information such as his name, address, etc).

**Encryption:**
If Alice wants to encrypt a message $m$ $(0 \leq m \leq N)$ for the group, such that any $t$ out of $n$ receivers can retrieve and decrypt her message, then she will perform the following steps.

1) Randomly choose an integer $k$ and compute $c = \alpha^{-k} \ mod \ N$.

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

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$

in $GF(F)$, where $a_0 = \alpha^{h(m)} \ mod \ N$.

3) Compute for $i = 1, \cdots, n$,

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

and send $(t, c, d_i, e_i)$ to $U_i$.

**Decryption:**
To decrypt a cryptogram, $t$ group members must collaborate. If $U_1, \cdots U_t$ want to decrypt ciphertext $c$, first $U_i, i = 1, \cdots t$, 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

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

# 3 Conspiracy Attack

We show a conspiracy attack in which a group of at least three participants can decrypt an encrypted message.

Let $U_1, U_2$ and $U_3$ be the colluding members and denote their secret keys by $X_1, X_2$ and $X_3$, respectively. Without loss of generality, let $X_1 < X_2 < X_3$, and $X_2 = X_1 + R_2$ and $X_3 = X_1 + R_3$.

The three colluding members $U_1, U_2$ and $U_3$ receive the encrypted messages,

$$\begin{aligned} e_1 &= m\alpha^{-X_1 h(m)} \pmod N, \\ e_2 &= m\alpha^{-(X_1+R_2)h(m)} \pmod N, \\ e_3 &= m\alpha^{-(X_1+R_3)h(m)} \pmod N, \end{aligned}$$

and compute,

$$\begin{aligned} \eta_1 &= \frac{e_2}{e_1} = \alpha^{-R_2 h(m)} \pmod N, \\ \eta_2 &= \frac{e_3}{e_1} = \alpha^{-R_3 h(m)} \pmod N. \end{aligned}$$

We consider three cases:
**Case 1:** $gcd(R_2, R_3) = 1$**:**
Colluders use the extended Euclid algorithm to compute $a_2, a_3 \in Z$ such that,

$$a_2 R_2 + a_3 R_3 = 1,$$

and find $g^{-h(m)} \pmod N$ as,

$$\begin{aligned} \rho &= \eta_1^{a_2} \eta_2^{a_3} \pmod N \\ &= \alpha^{-(a_2 R_2 + a_3 R_3)h(m)} \pmod N \\ &= \alpha^{-h(m)} \pmod N. \end{aligned}$$

Finally they decrypt the message as,

$$\frac{e_1}{\rho^{X_1}} \pmod N = \frac{m\alpha^{-X_1 h(m)}}{\alpha^{-X_1 h(m)}} \pmod N.$$

**Case 2:** $gcd(R_2, R_3) = \delta, \delta \neq 1$ ***and*** $\delta$ ***is small:***
The colluders first compute $\delta = gcd(R_2, R_3)$ and set $\tilde{R}_2 = \frac{R_2}{\delta}$ and $\tilde{R}_3 = \frac{R_3}{\delta}$. Next, they use the extended Euclid algorithm to compute $a_2, a_3 \in Z$ such that,

$$a_2 \tilde{R}_2 + a_3 \tilde{R}_3 = 1,$$

and compute,

$$\begin{aligned} \rho &= \eta_1^{a_2} \eta_2^{a_3} \pmod N, \\ &= \alpha^{-(a_2 R_2 + a_3 R_3)h(m)} \pmod N, \\ &= \alpha^{-\delta(a_2 \tilde{R}_2 + a_3 \tilde{R}_3)h(m)} \pmod N, \\ &= \alpha^{-\delta h(m)} \pmod N. \end{aligned}$$

Finally $U_1$ computes,

$$\begin{aligned} \zeta &= \frac{e_1^\delta}{\rho^{X_1}} \pmod N, \\ &= \frac{m^\delta \alpha^{-X_1 \delta h(m)}}{\alpha^{-X_1 \delta h(m)}} \pmod N, \\ &= m^\delta \pmod N, \end{aligned}$$

and the problem is to find $m$, given $\zeta = m^\delta \pmod N$ and $\delta$. This is the well-known RSA problem which, if $\delta < N^{0.292}$, is known to have an efficient algorithm [1,

2, 7]). We note that TA does *not* know the secret keys of participants and there is no way for the TA to enforce this condition.

*Case 3:* $gcd(R_2, R_3) = \delta, \delta \neq 1$ and $\delta$ is large:

If $\delta$ is large, we will extend the attack, as shown below, such that as the number of colluders increases their success chance will also increase.

Let $A(e_1, e_2, e_3)$ denote a procedure that takes three ciphertexts $e_1, e_2$ and $e_3$ from three colluders $P_1, P_2$ and $P_3$ respectively, use the methods described in Cases 1 and 2, and either outputs the message $m$, or `Fail`. The extended attack repeatedly uses $A(e_1, e_2, e_3)$ for subsets of three colluders until $m$ is found. The attack is summarised in the following algorithm.

**Algorithm 3.1:**
Conspiracy Attack $(U_0, U_1, \cdots, U_b, b \geq 3)$

$V_0 \leftarrow \{U_0, U_1, U_2\}, i \leftarrow 1, j \leftarrow 1, k \leftarrow 2, l \leftarrow 3.$

Apply $A(e_j; e_k; e_l)$ :

**while** $m$ is not found

**do**
- $V_i \leftarrow V_{i-1} \cup \{U_{i+2}\}$
- **for all** $W \subset V_i, W \leftarrow \{U_j, U_k, U_l\}, j \neq k \neq l$ :
- **if** $A(e_j, e_k, e_l) \neq m$
  - **then** *choose another* $W$
  - *else stop*
- $i \leftarrow i + 1$

The attack starts with three colluders and if $m$ cannot be found add colluders one by one until the message is found.

Let us estimate how certain the conspiracy attack would succeed. According to the Direichlet's result, the probability that given two integers chosen at random are relatively prime is

$$Pr_0 = 6/\pi^2 = 0.608.$$

So, Case 1 happens with very high probability. Since the secret key $x_i$ is picked independently by each group member, it is hard to avoid two keys from being relatively prime. Even if the first match fails, the probability of success increases as many members colluded. Given $b$ colluders, by noticing there are $\binom{b}{2}$ pairs, the probability of Case 1 is

$$1 - (1 - Pr_0)^{(b^2-b)/2}.$$

As shown in the well-known birthday problem, the attack succeeds if we have the number of colluders given by

$$b = \sqrt{(\pi^w/6)} = 1.283,$$

with probability 50%.

More precisely, we should consider probability of Case 2. Let $Pr_2$ be the probability that the greatest common divisor of two uniformly chosen integers is less than $N^{0.292}$, i.e,

$$Pr_2 = Pr[\delta = gcd(R1, R2), 1 < R1, R2 < N | \delta < N^{0.292}].$$

Instead of identifying $Pr_2$, we estimate the expected value of $\delta$. If two integers $R_1$ and $R_2$ are even, the probability is $1/4$ and the *gcd* is 2. Hence, the expected value of *gcd* is

$$\begin{aligned} E[\delta] &= Sum_{i=2,3,5,7,..,\delta} \left( \frac{1}{i^2} * i \right) \\ &< Sum_{i=2,3,4,..,\delta} \left( \frac{1}{i^2} * i \right) \\ &= H_\delta - 1 \end{aligned}$$

where $H_\delta$ is a harmonic number. If we consider the threshold value of $\delta$ is up to 11, the expected $\delta$ is $55991/27720 = 2.02$, which implies that the *gcd* does *not* increases. Therefore, we conclude that combining Cases 1 and 2 gives significant probability of attack.

# 4 Conclusion

We have shown that the modified scheme proposed in [3] can be subjected to conspiracy attack by at least three group members and hence is insecure.

This result strengthen the attack in [4] that showed a conspiracy of at least three participants can successfully decrypt an encrypted message with a probability 0.608. In contrast to [4], we show that if at least three participants conspire, then they will certainly be able to decrypt an encrypted message.

# References


[1] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key $d$ less than $n^{0.292}$," *Advances in Cryptology - Eurocrypt '99*, LNCS 1592, pp. 1-11, Springer-Verlag, 1999.

[2] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," *Journal of Cryptology*, vol. 10, pp. 233-260, 1997.

[3] H. Ghodosi and S. Saeednia, "Modification to self-certified group-oriented cryptosystem without combiner," *Electronics Letters, 18th January 2001*, vol. 37, no. 2, pp. 86-87, 2001.

[4] W. B. Lee and K. C. Liao, "Improved Self-Certified Group-Oriented Cryptosystem without a Combiner," *The Journal of Systems and Software*, (to appear), 2005 .

[5] S. Saeednia and H. Ghodosi, "A self-ceritified group-oriented cryptosystem without a combiner," *Information Security and Privacy, ACISP '99*, LNCS 1587, pp. 192-201, Springer-Verlag, 1999.

[6] W. Susilo and R. Safavi-Naini, "Remark on self-certified group-oriented cryptosystem without a combiner," *Electronics Letters, 2nd September 1999*, vol. 35 no. 18, pp. 1539-1540, 1999.
[7] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, IT-36, no. 3, pp. 553-558, 1990.

**Willy Susilo** received a Ph.D. in Computer Science from University of Wollongong, Australia. He is currently an Associate Professor at the School of Information Technology and Computer Science of the University of Wollongong. He is the coordinator of Network Security Research Laboratory at the University of Wollongong. His research interests include cryptography, information security, computer security and network security. His main contribution is in the area of digital signature schemes, in particular fail-stop signature schemes and short signature schemes. He has served as a program committee member in a number of international conferences. He is a member of the IACR. He has published numerous publications in the area of digital signature schemes and encryption schemes.

**Hiroaki Kikuchi** was born in Japan. He received B. E. , M. E. and PhD. degrees from Meiji University in 1988, 1990 and 1994. After he worked in Fujitsu Laboratories Ltd. from 1990 through 1993, he joined Tokai university in 1994. He is currently an Associate Professor in Department of Information Media Technology, School of Information Technology and Electronics, Tokai University. He was a visiting researcher of school of computer science, Carnegie Mellon university in 1997. His main research interests are fuzzy logic, cryptographical protocol, and network security. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan (IEICE), the Information Processing Society of Japan (IPSJ), the Japan Society for Fuzzy Theory and Systems (SOFT), IEEE and ACM.