# On the Security of A Group Signature Scheme

Jianhong Zhang[1,2] and Wei Zou[1]

[1] Institute of Computer Science & Technology, Peking University, Beijing,100871 China
jhzhang@ncut.edu.cn
[2] College of Sciences, North China University of Technology, Beijing 100041, China
zouwei@icst.pku.edu.cn

**Abstract.** As a special digital signature, a group signature scheme allows a group member to sign message on behalf of the group in an anonymous and unlinkability way, In case of a dispute, the group manager can reveal the actual identity of signer. Anonymity and unlinkability are basic properties of group signature, which distinguish other signature scheme. Recently, based on the work of Camenisch and Lysyanskaya, which is known to be the most efficient scheme so far, E.Y.Choi *et.al* propose an efficient group signature scheme with member revocation at TrustBus 2005. Unfortunately, in this work we show that the scheme has linkability, Namely, any one can distinguish whether two different group signatures are produced by the same signer, and that the revocation manager cannot trace the actual identity of a signer by a group signature. Finally, we give the corresponding attack to the scheme.

## 1 Introduction

Digital signatures are rapidly becoming ubiquitous in many aspects of *electronic* life. They are used to obtain security services such as authentication, data integrity and non-repudiation. Group signatures, first introduced by Chaum and van Heyst in[14]. In such a scheme each group member of a given group is allowed to sign messages on behalf of the group in an anonymous and unlinkable way. A receiver only needs the unique group public key to check the validity of a group signature. In case of a dispute, group manager can reveal the identify the identity of the signer, while other group members neither can identify the identity of the signer nor determine whether multiple signature are produced by the same group member. Various researches in group signature schemes have been investigated to propose an efficient one of which the length of signature and the size of the group public key are independent of the size of the group. Anonymity and unlinkability are two important properties of group signatures, which are distinguished from other signature schemes. Because of the anonymity and unlinkability of group signature, these properties can hide the group internal structure for a verifier, while they can assure group manager to reveal the signer's identities. Hence, group signature is widely used in electronic cash,electronic voting, electronic bid and so on.

The rest of this paper is organized as follows, In Section 2, we recall the related work of group signature, in Section 3, we introduce the informal definitions of a secure group signature scheme and the security requirements. Section 4 reviews the proposed group signature scheme[3](for short CKL scheme) by E.Y.Choi, H.J.Kim and D.H.Lee . Then, our security analysis is presented in Section 5, Finally, we conclude this paper in section 6.

## 2 Related Work

Following the first schemes constructed in [14], a number of new group signature schemes and improvements have been proposed [15, 9, 10, 2, 3, 18, 8,17, 14, 12, 7]. In [15], Chen and Pedersen constructed the first scheme, which allows new members to join the group dynamically, and suggested to use group signatures in e-bidding. Camenisch and Stadler proposed the first group signature scheme that can be used for large groups, since in their scheme the group public key and signatures have lengths independent of the group size [9]. Based on the strong RSA assumption [16], Camenisch and Michels presented an efficient group signature scheme in [10, 11]. Later, Kim et al. extended their scheme to support efficient member revocation [18]. Ateniese and Tsudik pointed out some obstacles that stand in the way of real world applications of group signatures, such as coalition attacks and member deletion [2]. At present, there have been several papers which focused on the problem of member deletion [3,8,4,18]. Ateniese et al. presented a provably secure group signature scheme in [1]. in 2003, Ateniese and de Medeiros[5] proposed another group scheme, which is not as efficient as ACJT2000 scheme. However, it aims at one big advantage over other schemes:no party is required to know any trapdoor secret. So different groups can share the same cryptographic domain without compromising security. it is new research branch of group signature.

At present, these group signature schemes available are mainly classified into two types, a public-key registration type, and a certificate-based type. In the former type, [5, 6] are constructed by using only known-order groups. However, in their schemes, both a group public key and the signature size depend on the number of group members. It yields a serious problem for large groups. In the latter type, [9, 8, 1, 4,16, 7, 3, 2] give a membership certificate to group embers, and the group signature is based on the zero-knowledge proof of knowledge(SPK) of membership certificate. Therefore, neither a group public key nor signature size depends on the number of group members. In these previous certificate-based type group signature schemes, the membership certificate has used an RSA signature over an unknown-order group, and, thus, the size of group signature becomes huge.

Though many group signature schemes[1-5,7-15,17] were proposed and researched by many specialists. because these special properties: anonymity and unlinkability, the construction of group signature is intricate. Some schemes

among group signature schemes available are *insecure*. Attack on the group signature schemes is mainly divided into unforgeability attack and unlinkability attack . the unforgeability of signature is a basic property which all secure signature schemes should satisfy. as for group signature, unlinkability problem is an important problem of group signature. Because of this property, group signature is widely used in electronic commerce such as e-bid. In the following security analysis, we mainly aim at unlinkability of the scheme to attack.

The member revocation of group signature is a more complicated problem. One intuitive way to revoke member is via Certificate Revocation List (CRL), but the way exists the following problem: (1) How can a group manager "identity" a revoked member? (2) Can the anonymity and unlinkability of **past signatures** of a revoked member be preserved? Another tactic to revoke member is to change the group public key, the group manager simply issues a new set of membership certificate to all remaining members while the rest are automatically excluded. While the way is an acceptable solution only for small and stable groups. At present, there isn't an efficient way to solve membership deletion. In 2001, Kim, Lim and Lee proposed the first group signature scheme with a member deletion procedure[18]. Their extension is very efficient in both communication and computation aspects, while the scheme is *linkable*. Bresson and Stern also provided a group scheme with member deletion [8]. However, the size of signature depends on the number of member deletion. Recently, Camenisch *et.al* [12] proposed a new revocation method which is an improvement over previous works since the verification phase requires a constant work.

In 2005, E.Y.Choi[3] *et al* presents an efficient group signature scheme with member revocation based on the work of Camenisch and Lysyanskaya [12]. They claim that the scheme realizes the full features of unforgeability, exculpability,anonymity, traceability, unlinkability, and revocability. And the signature size and computation amount of signature generation and verification are reduced. Unfortunately, in this paper, we present security analysis of the scheme and show that the scheme is is linkable, any one can determine whether two different group signatures are produced by the same signer. Because of its linkability, it weakens the anonymity of the scheme. At the same time, we also show that the revocation cannot trace the actual identity of a signature by a signature.

## 3 Definition

A secure group signature scheme involves a group manager, a set of group members, and a set of verifiers. The group manager (for short, GM) is responsible for admitting/revoking group members, and for opening group signatures to reveal the true signers. When a potential user registers with GM, he/she becomes a group member and then can sign messages on behalf of the group. A verifier checks the validity of a group signature by using the unique group public key. The computational capability of each entity is modeled by a probabilistic

polynomial-time Turing machine. We now review the definitions of secure group signature schemes and their security requirements as follows. For more formal definitions on this subject, please refer to [7].

**Definition 1.** *A secure group signature scheme is comprised of the following procedures [9, 2, 3, 14, 16]:*

• SETUP: On input of a security parameter , this probabilistic algorithm outputs the initial group public key and the secret key for the group manager.

• JOIN: An interactive protocol between the group manager and a user that results in the user becoming a new group member. The user's output is a group-signing key.

• SIGN: A probabilistic algorithm that on input a group public key, a group signing key, and a message m outputs a group signature on m.

• VERIFY: An algorithm for establishing the validity of an alleged group signature of a message with respect to a group public key.

• OPEN: An algorithm that, given a message, a valid group signature on it, a group public key and the corresponding group manger's secret key, determines the identity of the signer.

• REVOKE: An algorithm that on input a group member's certificate, a group public key and the corresponding group manger's secret key, outputs a revocation token that revokes the group member's signing ability.

**Definition 2.** *A secure group signature scheme is secure if it satisfies all the following security requirements [1,2, 3, 14, 16]:*

• Correctness: Signatures produced by a group member using SIGN procedure must be accepted by VERIFY procedure.

•Unforgeability: Only group members are able to sign messages on behalf of the group.

• Anonimity: Given a valid group signature for some message, identifying the actual signer is computationally hard for everyone but the group manager.

• Unlinkability: Deciding whether two different valid signatures were generated by the same group member is computationally hard for everyone but the group manager.

• Excupability: Even if the group manager and some of the group members collude, they cannot sign on behalf of non-involved group members.

• Traceability: The group manager can always open a valid group signature using OPEN procedure and then identify the actual signer.

• Coalition-resistance: A colluding subset of group members cannot generate a valid group signature that cannot be traced by the group manager.

• Revocability: The group manager can revoke a group member so that this group member cannot produce a valid group signature any more after being revoked.

## 4 Review of the CKL Group Signature Scheme

In the following, we briefly describe the CKL group signature scheme which was proposed by E.Y.Choi, H.J.Kim and D.H.Lee, please interested reader refer to [3] for more detail. in the paper, the symbol "SPK" denotes knowledge proof signature.

[**Setup Phase**]

**(1)** The membership manager chooses a group $G =< g >$ and two random element $z, h \in G$ with the same order($\approx 2^{l_g}$) such that modified strong RSA and DDH assumptions hold, then publishes them. Computing discrete logarithm in $G$ to the base $g, h$ or $z$ must be infeasible. Only the membership manager can easily compute these roots and the order of $G$ is keep secretly.
**(2)** The membership manager randomly chooses two large primes $p_1, p_2$ which satisfies $p_1 = 2p_2 + 1, q_1 = 2q_2 + 1$ where $p_2, p_2$ are also primes. Finally, the membership manager keeps $p_1$ and $p_2$ secret and publishes $n = p_1 q_1$.
**(3)** Select and publish a large prime $p$, $\alpha$ is a generator $Z_p^*$. Choose $t \in Z_p^*$ at random and keep $t$ secretly. Compute $PK = \alpha^t \bmod p$ and publish $PK$.
**(4)** Choose a public key $e_N$ and a secret key $d_N$ such that $e_N d_N = 1 \pmod{\phi(n)}$ where $n$ is RSA-modulus and publish $e_N$.
**(5)** Generate a signature key pair $(sk_M, vk_M)$: $sk_M$ is the secret siging key and $vk_M$ is the public verification key, and publish $vk_M$.
**(6)** Set the hash function $H : \{0,1\}^* \longrightarrow \{0,1\}^k$, $H_0 : \{0,1\}^* \longrightarrow \{0,1\}^k$,$H_1 : \{0,1\}^* \longrightarrow \{0,1\}^k$ and security parameters $l, l_1, l_2, l_g$ and $\epsilon$, then select a secure signature algorithm $\Sigma = (K, S, V)$.
**(7)** Publish a counter $c$ in order to indicate a membership exchanger event and increase a counter $c$ in the event of membership changes.
**(8)** To revoke a member , the revocation manager chooses a secret key $x_R$ randomly in $1, \cdots, 2^{l_g} - 1$ and publish $y_R = g^{x_R}$.

[**Join Phase**]

If Alice wants to be a new group member, she can obtain the membership key $(x_I, y_I)$, where $y_I \in G$ and $y_I^{x_I} = z$, and shares a symmetric key with the membership manager through join process. At the same time, the membership

manager regenerates group public property key $U_M$ and renewal property key $U_N$ using $y_I$ and generates Alice's secret property key $U_I$. Before generating a signature, current members check whether the group renewal property key has been updated or not. Let $C = \{I_1, I_2, \cdots, I_{m-1}\}$ be the set of current group members, and $I_m$ be a new member, Alice. Before Alice joins the group, the group public property key has been $U_M = y_{I_1} \cdots y_{I_{m-1}} y'$ with a random number $y' \in_R G$ and a counter $c$.

Alice executes as follows:

**(1)** Generate a signature key pair $(sk_{I_m}, vk_{I_m})$.
**(2)** Randomly choose a prime $\hat{x}_{I_m} \in_R \{2^{\tilde{l}-1}, \cdots, 2^{\tilde{l}}-1\}$ and $x_{I_m} \in_R \{2^{l_1}, \cdots, 2^{l_1} + 2^{l_2} - 1\}$ such that $x_{I_m}\hat{x}_{I_m} \neq 1(mod 8)$ and $x_{I_m} \neq \hat{x}_{I_m}(mod 8)$.
**(3)** Compute $\tilde{x_{I_m}} = x_{I_m}\hat{x}_{I_m}$ and $\tilde{z} = z^{\hat{x}_{Im}}$, and commit to $\hat{x}_{I_m}$ and $\tilde{z}$.
**(4)** Randomly choose $t_m \in Z_p^*$, and compute $SK_m = \alpha^{t_m} mod p$ and the shared key $K_m = (PK)^{t_m} mod p$ (Assume $K_m$ differs from other group member's $t_i$'s $1 \leq i \leq m-1$).
**(5)** Generate siganture $s = S_{sk_m}(SK_m)$ and compute $H_0(c||K_m)$. Then she sends identity, $SK_m, s, H_0 c||K_m, \tilde{x}_{I_m}, \tilde{z}$ and their commitments to the membership manager.
**(6)** Execute the interactive protocols corresponding to $W = SPK\{(\tau, \varrho)|z^{\tilde{x}_{Im}} = \tilde{z}^{\tau} \bigwedge \tilde{z} = z^{\varrho} \bigwedge \tau \in \{2^{l_1} - 2^{\epsilon(l_2+k)+1}, \cdots, 2^{l_1} + 2^{\epsilon(l_2+k)+1}\}\}(\tilde{z})$ with the membership manager.

The membership manager executes the following operations:

**(1)** Check $s$ to verify the received value $SK_m$ and compute the share key $K_m = (SK_m)^t mod p$ to $H_0(c||K_m)$. If they hold, the membership manager accepts that $K_m$ is actually shared with Alice and increases the counter $c$ into $c'$.
**(2)** Generate signature $s' = S_{sk_M}(SK_m)$, and compute $H_1(c'||K_m)$.
**(3)** Generate Alice's public $y_{I_m} = \tilde{z}^{1/\tilde{x}_{Im}}$ and compute a new group public property key $U_M = y_{I_1} \cdots y_{I_m} y''$, where $y'' \in_R G$.
**(4)** Compute the new group's renewal property key $U_N = (y_{I_m} y''/y')^{d_N}$.
**(5)** Generate the member $I_m$'s secret property key $U_{I_m} = (y_{I_1} y_{I_2} \cdots y_{I_{m-1}} y'')^{d_N}$.
**(6)** Encrypt $U_{I_m}$ and $y_{I_m}$ with the shared symmetric key $K_m$, encrypt $U_N$ with the group members' symmetric keys, and publish $\varepsilon_{K_i}(U_N)$, $1 \leq i \leq m-1$, where $\varepsilon(\cdot)$ is symmetric encryption algorithm.
**(7)** Send $\varepsilon_{K_m}(U_{I_m}, y_{I_m}), s'$ and $H_1(c'||K_m)$ to Alice and publish $c', U_M$.

Then Alice does the followings:

**(1)** Check $s', c'$ and $H_1(c'||K_m)$ to verify the shared symmetric key. If successful, Alice accepts that $K_m$ is shared with the membership manager. Then decrypt the received message $\varepsilon_{K_m}(U_{I_m}, y_{I_m})$.
**(2)** The pair $(x_{I_m}, y_{I_m})$ is the membership key of Alice, she can verify her public key $y_{I_m}$ and secret property key $U_{I_m}$ by checking $y_{I_m}^{x_{Im}} = z$ and $(U_{I_m})^{e_N} y_{I_m} = U_M$ respectively.

For other valid group members $I_i$ $(1 \leq i \leq m-1)$ except the new member $I_m$ decrypt the encrypted messages with the shared symmetric key $K_i (i \leq i \leq m-1)$ and change their secret property key $U_{I_i} = (y_{I_1} \cdots y_{I_{i-1}} y_{I_{i+1}} \cdots y_{I_{m-1}} y')^{d_N}$ into $U'_{I_i} = U_{I_i} \cdot U_N$, where

$$U'_{I_i} = U_{I_i} \cdot U_N = (y_{I_1} \cdots y_{I_{i-1}} y_{I_{i+1}} \cdots y_{I_{m-1}} y_{I_m} y'')^{d_n}$$

Each group member can check new value $U'_{I_i}$ by computing $U_M = (U'_{I_i})^{e_N} y_{I_i}$.

[**Delete Phase**]

To delete a group member $I_j$ , the membership manager eliminates public key $y_{I_j}$ from the group public property $U_M$ and changes a random number. The remaining group members change their secret property keys to generate a valid signature. Let the current group public property key be $U_M = y_{I_1} \cdots y_{I_m} y'$ where $y' \in_R G$ and a counter $c$. The membership manager performs **Delete** as follows:

**(1)** Compute $U_M = U_M \cdot \frac{y''}{y_{I_j} y'}$ where $y'' \in_R G$,i.e., $U_M = y_{I_1} \cdots y_{I_{j-1}} y_{I_{j+1}} \cdots y_{I_m} y''$ .
**(2)** compute $U_N = (y''/(y_{I_j} y'))^{d_N}$ and increase the counter $c$ into $c'$.
**(3)** Encrypt $U_N$ with the group members' symmetric keys and publishes $U_M, c'$ and $\varepsilon_{K_i}(U_N)$, $1 \leq i (i \neq j) \leq m$.

Each valid group member $I_i 1 \leq i (i \neq j) \leq m$ decrypts the encrypted messages with the shared symmetric key $K_i$ $1 \leq i (i \neq j) \leq m$. Then each group member $I_i$ can change his secret property key $U_i$ into $U'_{I_i} = U_{I_i} \cdot U_N$.

[**Signing Phase**]

To sign a message $m$, a group member executes as follows:

**(1)** Choose two random integers $w_1, w_2 \in_R \{0,1\}^{l_g}$ and compute $a = g^{w_1}$, $b = y_I y_R^{w_1}$, $d = g^{x_I} h^{x_I w_1}$,$\alpha = U_I g^{w_1} h^{w_2}$ and $\beta = y_R^{w_1} h^{w_2 e_N}$.
**(2)** Choose $r_1 \in_R \{0,1\}^{\epsilon(l_2+k)}, r_2 \in_R \{0,1\}^{\epsilon(l_g+l_1+k)}$ and $r_3 \in_R \{0,1\}^{\epsilon(l_g+k)}$
**(3)** Compute $t_1 = b^{r_1}(1/y_R)^{r_2}$, $t_2 = a^{r_1}(1/g)^{r_2}, t_3 = g^{r_3}$, $t_4 = g^{r_1} h^{r_2}, t_5 = y_R^{r_3} h^{r_3 e_N}$ and compute $c = H(g||h||y_R||z||a||b||d||\beta||t_1||t_2||t_3||t_4||t_5||m)$
**(4)** Compute $s_1 = r_1 - c(x_I - 2^{l_1})$(in Z), $s_2 = r_2 - c w_1 x_I$ (in Z), $s_3 = r_3 - c w_1$ (in Z) and $s_4 = r_3 - c w_2$ (in Z).
**(5)** Finally, the group signature on the message $m$ is $(c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta)$

[**Verification Phase**]

Given a signature $(c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta)$, the verifier checks as follows:

**(1)** Check the signature $(c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta) \in \{0,1\}^k \times \{-2^{l_2+k}, \cdots, 2^{\epsilon(l_2+k)}\}$
$\times \{-2^{l_g+l_1+k}, \cdots, 2^{\epsilon(l_g+l_1+k)}\} \times \{-2^{l_g+k}, \cdots, 2^{\epsilon(l_g+k)}\} \times \{-2^{l_g+k}, \cdots, 2^{\epsilon(l_g+k)}\} \times G^5$
.

**(2)** Check the equation $c = H(g||h||y_R||z||a||b||d||\beta||z^c b^{s_1 - c2^{l_1}} / y_R^{s_2} || a^{s_1 - c2^{l_1}} / g^{s_2} || a^c g^{s_3} ||$

$$d^c g^{s_1 - c2^{l_1}} h^{s_2} || \beta^c y_R^{s_3} h^{s_4 e_N} || m)$$

**(3)** Finally, the verifier checks if $U_M(\frac{a}{\alpha})^{e_N}\beta = b$ holds.

(**Note that** the author thinks that the verifier should checked $U_M a^{e_N}\beta = b\alpha^{e_N}$ not $U_M(\frac{a}{\alpha})^{e_N}\beta = b$, since the verifier cannot know the order of group $G =< g >$, thus he cannot obtain the inverse of an element of $G =< g >$, while $\alpha$ is the element of $G$ )

[**Revocation Phase**]

To reveal the actual identity of a signer of a given signature $\delta = (c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta)$ of the message $m$, the revocation manager first checks its correctness, then computes $y_I' = b/a^{x_R}$, at the same time,he issues a signature of knowledge

$$P = SPK\{(\rho) : y_R = g^\rho \wedge b/y_I' = a^\rho\}(y_I' || \delta || m)$$

and reveals $arg = y_I' || P$, then the membership manager looks up $y_I'$ in the group-member list and find the corresponding $y_I$.

## 5 Security Analysis of the CKL Scheme

E.Y.Choi et al have claimed that their group scheme satisfies the above all security requirements and give security proof to guarantee all security properties. The anonymity and the unlinkability of group signature are basic properties to distinguish from other signature schemes. We show that the scheme doesn't satisfy unlinkability and the revocation manager cannot trace the actual identity of a signer by analyzing security of the CKL scheme.

### 5.1 Linkability

In the following, we show that the scheme has linkability, Namely, any one can determine whether two different group signatures are produced by the same signer, the detail attack is as follows.

Let $(c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta)$ and $(c', s_1', s_2', s_3', s_4', a', b', d', \alpha', \beta')$ be two valid group signatures. To decide whether they are produced by the same group member, Supposed that a verifier can compute the following relation.

$$\gamma = \frac{\alpha}{a} = \frac{U_I g^{w_1} h^{w_2}}{g^{w_1}} = U_I h^{w_2}, \gamma' = \frac{\alpha'}{a'} = \frac{U_I g^{w_1'} h^{w_2'}}{g^{w_1'}} = U_I h^{w_2'} \quad (1)$$

$$\mu = \frac{b}{\beta} = \frac{y_I y_R^{w_1}}{y_R^{w_1} h^{w_2 e_N}} = \frac{y_I}{h^{w_2 e_N}}, \mu' = \frac{b'}{\beta'} = \frac{y_I y_R^{w_1'}}{y_R^{w_1'} h^{w_2' e_N}} = \frac{y_I}{h^{w_2' e_N}}. \quad (2)$$

$$\theta_1 = (\gamma)^{e_N}\mu = U_I y_I \tag{3}$$

$$\theta_2 = (\gamma')^{e_N}\mu' = U_I y_I \tag{4}$$

if the equation (3) and equation (4) are equal, then it means that the two group signatures are produced by the same signer, otherwise, they are produced by the different group member. Because the order of $g$ isn't been known, we cannot obtain the inverse of an integer, then we adopt a equivalence transform

**Theorem 1.** *If two different group signatures* $(c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta)$ *and* $(c', s_1', s_2', s_3', s_4', a', b', d', \alpha', \beta')$ *satisfy the following equation*

$$b\beta'(\alpha a')^{e_N} = b'\beta(\alpha' a)^{e_N}$$

*, then two group signatures must be produced by the same signer.*

*Proof.* According to the above signing phase, we know that they satisfy

$$a = g^{w_1}, b = y_I y_R^{w_1}, \alpha = U_I g^{w_1} h^{w_2}, \beta = y_R^{w_1} h^{w_2 e_N}$$

and

$$a' = g^{w_1'}, b = y_I y_R^{w_1'}, \alpha = U_I g^{w_1'} h^{w_2'}, \beta = y_R^{w_1'} h^{w_2' e_N}$$

According to the equation (1),(2),(3) and (4), we can conclude the following relation

$$\begin{aligned}
(\gamma)^{e_N}\mu = (\gamma')^{e_N}\mu' &\Longleftrightarrow \mu \times (\gamma)^{e_N} = \mu' \times (\gamma')^{e_N} \\
&\Longleftrightarrow \frac{b}{\beta} \times (\frac{\alpha}{a})^{e_N} = \frac{b'}{\beta'} \times (\frac{\alpha'}{a'})^{e_N} \\
&\Longleftrightarrow \frac{b\alpha^{e_N}}{\beta a^{e_N}} = \frac{b'\alpha'^{e_N}}{\beta' a'^{e_N}} \\
&\Longleftrightarrow b\beta'(\alpha a')^{e_N} = b'\beta(\alpha' a)^{e_N}
\end{aligned} \tag{5}$$

Hence, given two different group signatures $(c, s_1, s_2, s_3, s_4, a, b, d, \alpha, \beta)$ and $(c', s_1', s_2', s_3', s_4', a', b', d', \alpha', \beta')$, if the two signature satisfy the equation (5), it means that the two group signature are produced by the same group member. According the above state, the scheme has linkability.

Unlinkability is the basic property of group signature. this property makes group signature widely be used in electronic commerce such as e-cash. The reason of producing the above attack is to use the same random number in $a$ and $\alpha$.But to make that the verifier can verify that $U_M(\frac{a}{\alpha})^{e_N}\beta = b$ holds, he must use the same random number, thus this is an intrinsical error of the scheme.

### 5.2 Non-Traceability

According the **System Setup** of the CKL scheme, we know that the order of the group $G =< g >$ is secret except the membership manager. The revocation manager cannot know the order of group $< g >$, then he cannot compute the

inverse of an element of group $< g >$; thus given a signature he cannot reveal the actual identity of a signer by computing $y_I' = b/a^{x_R}$, since he cannot obtain the inverse of $a^{x_R}$ without the order of $g$ except that the membership manager and the revocation manager collaborate. However, usually, the membership manager and the revocation manager are independent. Thus if a dispute, the revocation manager cannot trace an actual identity of a signer by a signature. To overcome non-traceability, the membership manager and the revocation manager must be the same one or the revocation manager also know the order of group $< g >$.

## 6 Conclusion

In this paper, we presented security analysis of E.Y.Choi *et al* group signature scheme. By successfully attack on the scheme, we demonstrated that their scheme is insecure. More specifically, we shows that the scheme is linkable,namely any one can distinguish whether two different group signatures are produced by the same signer. At the same time, we also show the revocation manager cannot trace the actual identity of a signer by a signature.Because of special properties: anonymity and unlinkability, to how design a secure and more efficient group signature scheme is still an open problem.

## References


1. G.Ateniese, J.Camenisch, M.Joye, and G.Tsudik,(2000) A Pracical and provably secure coalition-resistant group signature. In Advances in Cryptography-CRYPTO'00, LNCS 1880, pp 255-270, Springer-Verlag .
2. G.Ateniese and G.Tsudik.(1999) Some open issues and new direction in group signatures. In Financial Cryptography(FC'99), LNCS 1648, pp 196-211.Springer-Verlag.
3. Eun Young Choi, Hyun-Jeong Kim and Dong Hoon Lee,(2004) Efficient Member Revocation in Group Signature Scheme, TrustBus 2005 Springer-verlag, LNCS 3592 pp 195-205
4. G.Ateniese, D.Song, and G.Tsudik.(2002) Quasi-efficient revocation of group signatures.In Financial Cryptography (FC'02),LNCS 2357. Springer-verlag,Primary version available at Http:// eprint.iacr.org/2001/101.
5. G.Ateniese and B.de medeiros.(2003) Efficient group signature without trapdoors. In Asiacrypt , Springer-verlag, 2003, http://eprint.iacr.org/2002/173
6. M.Bellare, and S.Miner.(1999) A forward-secure digital signature scheme. In Advances in Cryptography-CRYPTO'99, LNCS 1666, pp 431-448. Springer-Verlag,
7. M.Bellare, D. Micciancio, and B. Warinschi.( 2003) Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. In: Advances in Cryptology - EUROCRYPT03, LNCS 2656, pp. 614- 629. Springer-Verlag.
8. E. Bresson and J. Stern.(2001) Efficient revocation in group signatures. In: Public Key Cryptography (PKC01), LNCS 1992, pages 190-206. Springer-Verlag.
9. J. Camenisch and M. Stadler.( 1997) Efficient group signature schemes for large groups. In: Advances in Cryptology - CRYPTO97, LNCS 1294, pages 410-424. Springer-Verlag .

10. J. Camenisch and M. Michels. (1998) A group signature scheme with improved efficiency. In: Advances in Cryptology - ASIACRYPT98, LNCS 1514, pages 160-174. Springer- Verlag.
11. J. Camenisch and M. Michels. (1998)A group signature scheme based on an RSA-variant. Technical Report RS-98-27, BRICS, University of Aarhus, November .
12. J. Camenisch and A.Lysyanskaya. (2002)Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Advances in Cryptology - CRYPTO 2002, LNCS 2442, pages 61-76. Springer-Verlag .
13. S. Canard and J. Traore. (2003)On fair e-cash systems based on group signature schemes. In: Information Security and Privacy (ACISP 2003), LNCS 2727, pp. 237-248. Berlin: Springer-Verlag.
14. D. Chaum and E. van Heyst.(1992) Group signatures. In: Advances in Cryptology - EUROCRYPT 91, LNCS 950, pages 257-265. Springer-Verlag.
15. L. Chen and T. P. Pedersen.(1995)New group signature schemes. In: Advances in Cryptology - EUROCRYT94, LNCS 950, pages 171-181. Springer-Verlag .
16. E. Fujisaki and T. Okamoto.(1997) Statistical zero-knowledge protocols to prove modular polynomial relations. In: Advances in Cryptology - CRYPTO97, LNCS 1294, pages 16-30. Springer-Verlag, 1997.
17. A.Kiayias and M.Yung. (2003)Extracting group signature from traitor tracing schemes. In Advances in Cryptology-EUROCRYPTO 2003, LNCS 2656, pp 630-648, Springer-Verlag,
18. H.J.Kim, J.I.Lim,and D.H.Lee. (2001) Efficient and secure member deletion in group signature schemes. In information security and crytology(ICISC2000), LNCS 2015, pp 150-161, Springer-Verlag,2001.