通信情報保護學會論文誌
第 7 卷 第 2 號, 1997. 6

# 그룹 식별 정보를 이용한 그룹 서명 방식의 암호 분석

박 상 준*, 원 동 호**

# Cryptanalysis of ID-based Group Signature

Sang Joon Park*, Dong Ho Won**

## 요 약

Chaum과 Heyst는 부인 방지 서명에 근거한 그룹 서명 방식을 제안하였다. 그러나 부인 방지 서명은 서명 검증시 서명자의 도움이 요구되므로 정당한 수신자 조차도 서명을 검증할 수 없을 뿐 아니라, 서명자의 신분을 확인하고자 할 경우에도 그룹 소속원 전체의 협조가 있어야만 소속원의 신분을 확인할 수 있는 불편함이 있다. 박성준등은 서명자의 도움 없이 자체 검증이 가능하며 신분 확인시에도 소속원의 도움 없이 신뢰 센터가 소속원의 신분 확인이 가능한 그룹 식별 정보를 이용한 그룹 서명 방식을 제안하였다. 본 논문에서는 박성준등이 제안한 그룹 서명 방식의 신분 확인 과정의 문제점을 밝히고, 사용자 결탁시 새로운 그룹 서명키를 계산할 수 있을 뿐 아니라 신뢰 센터의 비밀키가 노출될 수 있음을 보이고자 한다.

## Abstract

Chaum and Heyst first proposed group signature which is based on the undeniable signature. So, a receiver of the signature can't verify a group signature without cooperation of the signer and, in case of dispute later on, he can't reveal the identity of the signer without help of the group members. Park et. al. proposed an id-based group signature with self-authentication, in which the receiver of the signature reveals the identity of the signer without help of the group members. However, the proposed scheme has two problem :

1) the receiver can't identify the signer, since every keys of the group members hold the identification procedure.
2) By collusion of the group members, new secret key for a group signature can be computed and the secret key of the trusted center can be revealed.

---

. 한국전자통신연구원
.. 성균관대학교 정보공학과

## 1. 서 론

그룹 서명에 대한 개념은 Chaum과 Heyst에 의하여 처음 제안되었으며, 다음과 같은 3가지 요구 조건을 갖는다[1].

- 그룹에 속하는 사용자만이 서명을 할 수 있다.
- 서명의 수신자는 그룹에 속한 소속원이 생성한 서명을 그룹의 정당한 서명으로 검증 가능하며, 그룹의 어떤 사용자가 서명을 생성하였는지 확인할 수 없다.
- 분쟁이 발생할 경우, 서명자의 신원을 확인할 수 있어야 한다.

Chaum과 Heyst는 논문 [1]에서 모두 4가지의 그룹 서명을 제안하였다. 4가지의 서명 기법중 하나는 일반적인 공개키 암호 알고리즘에 적용 가능한 방법이고, 나머지 3개는 부인 방지 서명(undeniable signature)을 이용하였다. 그러나 부인 방지 서명(undeniable signature)은 서명 검증시 서명자의 도움이 요구되므로 정당한 수신자조차도 서명을 검증할 수 없으며, 서명을 생성한 소속원의 신분을 확인하고자 할 경우에도 그룹에 속한 전체 소속원의 협조가 요구된다. 따라서, 서명 검증시와 신분 확인시 통신량과 계산 복잡도가 매우 높다. 일반적인 공개키 암호 알고리즘을 이용하는 방법은 수시로 변화하는 각 사용자의 공개키들을 신뢰 센터(trusted center)가 관리해야 할 뿐 아니라, 이미 사용된 공개키들도 분쟁 해결을 위하여 신뢰 센터가 계속적으로 보관하여야 한다.

1995년 박성준등은 Chaum과 Heyst가 제안한 그룹 서명 기법의 비효율성을 개선하기 위하여 합성수 n에서의 고차 잉여류 문제에 안전성을 둔 새로운 그룹 서명 방식을 제안하였다[8]. 제안된 그룹 서명 방식에서는 수신자에 의한 서명의 자체 검증이 가능하고, 그룹 소속원의 협조 없이 센터에 의하여 서명자의 신분을 확인할 수 있다.

본 논문에서는 기 제안된 그룹 서명 방식의[8] 신분 확인 과정에 의하여 서명자의 신분을 확인하는 것이 불가능함을 밝히고, 사용자 결탁시 새로운 그룹 서명키를 계산할 수 있을 뿐 아니라 신뢰 센터의 비밀키가 노출될 수 있음을 보이고자 한다.

본 논문은 모두 4개 절로 구성된다. 2절에서는 박성준등이 제안한 그룹 식별 정보를 이용한 그룹 서명 방식의 특성과 서명 방식을 소개하고, 3절에서는 제안된 방식의 신분 확인 과정의 문제점과 사용자 결탁에 의한 암호 해독 가능성을 기술하였으며, 4절은 결론부이다.

## 2. 그룹 식별 정보를 이용한 그룹 서명 방식

1995년 박성준등은 역설적인 개인 식별 방식에 기반을 둔 서명 방식을 제안하였다[5]. 제안된 서명 방식은 합성수 $n$의 인수 분해 문제의 어려움과 법 $n$ 상에서의 고차 잉여류근을 구하는 문제의 어려움에 안전성의 근거를 두고 있다[5][8]. 역설적인 개인 식별 방식에 근거한 서명 방식은 또한 기 제안된 박성준의 고차 잉여류를 이용한 공개키 암호시스템의 개념에 근거한다[5][10]. 신뢰 센터가 사용자의 비밀키를 생성하는 과정에서 고차 잉여류를 이용한 공개키 암호시스템의 복호화 과정이 요구된다. 본 절에서 소개하는 그룹 서명 방식은 역설적인 개인 식별 방식에 근거한 서명 방식을 그룹 서명 방식에 응용한 것이다. 합성수 n 상에서의 고차 잉여류 문제를 이용한 그룹 서명 방식은 두 가지가 제안되었으나 본 절에서는 설명의 편의성을 위하여 보다 간단한 형태를 갖는 그룹 서명 방식만을 소개하고자 한다. 먼저 제안된 그룹 서명 방식은 Chaum과 Heyst의 그룹 서명에 대한 요구 사항외에도

다음과 같은 특성을 갖는다.

① 그룹 식별 정보에 기반을 둔 서명 방식을 사용한다[6].
② 서명 검증 및 서명에 의한 신분 확인 과정이 비대화형으로 수행된다.
③ 그룹의 공개키 사이즈가 고정된다.
④ 센터만이 서명자를 확인할 수 있다.
⑤ 그룹 소속원의 수가 제한되지 않는다.
⑥ 센터라도 소속원의 서명문을 만들 수 없다.

신뢰 센터는 먼저 큰자리 소수 $p,q$ 를 랜덤하게 생성하여 RSA 합성수 $n=pq$ 를 구성한다. 이때, 특별히 소수 $p,q$는 다음과 같은 형태를 갖는다.

$$p = 2\gamma^s f p' + 1,\ q = 2f q' + 1$$

센터는 시스템의 안전성을 위하여 $p'$, $q'$, $f$ 를 큰자리 소수로 선택하며, $\gamma$는 센터에 의한 키 생성의 효율성을 위하여 작은 소수로 선택한다. $\gamma$ 와 s 는 안전성과 효율성을 고려하여 $\gamma$는 257인 소수로 하고 s는 16으로 한다[5]. 만일, 센터가 $\gamma$의 값을 큰 값으로 선정할 경우 제안된 그룹 서명 방식에서 사용자의 비밀키 생성이 어려워진다. 이제, $h_1$을 법 $p$상의 원시원소라 하고 $h_2$를 법 $q$상의 원시원소라 하자. 이때, $b = h_1^{2p'\gamma^s} \cdot h_2^{2q'} \bmod n$ 이라 하면, $b$는 법 $n$상에서 위수(order)가 $f$인 원소가 된다. $w \cdot \gamma^s = 1 \bmod f$ , $v = h_1^{2p'} \cdot h_2^{29'w} \bmod n$ 라고 하면 $b = v^{\gamma^s} \bmod n$ 이므로 다음의 정의1에 의하여 $b$는 법 $n$상에서 $(\gamma^s)^{th}$ 잉여류가 된다.

**정의 1**[5] 양의 정수 $\gamma$, $n$이 주어졌을 때, 정수 $\gcd(z, n) = 1$인 $z$에 대하여 $z = x^{\gamma} \bmod n$을 만족하는 $x$가 존재할 때, $z$를 법 $n$에 대하여 $(\gamma)^{th}$ - 잉여류 ($\gamma^{th}$ - *nonresidue*)라 한다. 만일, $z = x^{\gamma} \bmod n$ 을 만족하는 $x$가 존재하지 않으면 $z$를 법 $n$에 대하여 $\gamma^{th}$ - 비잉여류 ( $\gamma^{th}$ -*nonresidue*)라고 한다.

**정리 1**[5] $p'$, $q'$, $f$, $\gamma$는 소수이고 $n$을 다음과 같은 소수 $p$, $q$로 구성된 RSA 합성수라 하자.

$$p = 2\gamma^s f p' + 1\ ,\ q = 2f q' + 1$$

임의의 $\gcd(z, n) = 1$이고 $y = h_1^{t_1\gamma^s + e} \cdot h_2^{t_2} \bmod n$ $(0 \le e \le \gamma^s)$이면, 적당한 $u$에 대해서 $z = y^i u^{\gamma^s} \bmod n$ 이 되는 $0 \le i \le \gamma^s$ 가 유일하게 존재한다. 이때, $i$를 $(n, \gamma^s, y)$에 대한 $z$의 잉여류 지수(*class-index*)라고 정의한다.

$b = v^{\gamma^s} \bmod n$ 라 하면, $b^s = (v^s)^{\gamma^s} \bmod n$ 이므로 $(\gamma^s)^{th}$ - 잉여류이면 임의의 $s$에 대하여 $b^s$ 또한 $(\gamma^s)^{th}$ - 잉여류가 된다. $x = y^i \cdot u^{\gamma^s} \bmod n$ 이면 $x \cdot b^s = y^i \cdot (u \cdot v^s)^{\gamma^s} \bmod n$ 이므로 $x$의 잉여류 지수와 $x \cdot b^s$ 의 잉여류 지수는 동일하다. 즉, 그룹의 그룹 식별 정보를 $ID_G$라 할 경우 $ID_G$의 잉여류 지수와 $ID_G \cdot b^s$의 잉여류 지수는 같게 된다. 이러한 성질을 이용하여 센터는 식별 정보 $ID_G$를 갖는 그룹 소속원의 비밀키를 다음과 같이 생성한다.

① 센터는 그룹 G의 식별 정보 $ID_G$에 대응되는 잉여류 지수 $i$를 먼저 계산한다. ( $ID_G = y^i \cdot u\, G^{\gamma^s} \bmod n$)
② 사용자 A는 자신만의 비밀키 정보 $0 < s_A < f$를 생성하고 $b^{s_A} \bmod n$을 센터에게 비밀리에 전달한다.
③ 센터는 A가 그룹 G의 소속원임을 확인한 뒤 $ID_G \cdot y^{-i} \cdot b^{s_A} = x_A^{-\gamma^s} \bmod n$을 만족하는 $x_A$를 계산하여 소속원 $A$에게 비밀리에 전달한다.
④ 소속원 $A$는 $(s_A, x_A)$를 자신의 비밀키로서 관리한다.

⑤ 시스템내의 모든 사용자에게 공통되는 센터의 공개 정보는 $n, y, b, i, \gamma^s$이며 비밀 정보는 $p', q', p, q$이다.

위와같은 과정에서 센터가 그룹 $G$의 식별 정보 $ID_G$의 잉여류 지수와 $ID_G \cdot y^{-i} \cdot b^{s_A} \bmod n$의 $(\gamma^s)^{th} - \sqrt{x_A}$를 계산하는 방법은 고차 잉여류를 이용한 공개키 암호시스템에 관련된 논문 [5]에 상세히 기술되어 있다. 제안된 키 생성 과정에서 센터는 $b^{s_A}$로 부터 사용자 $A$의 비밀키 $s_A$를 계산하는 문제는 이산대수 문제이므로 센터는 $s_A$를 알 수 없다. 박성준등은 본 논문에서 소개된 그룹 서명외에 $y$의 지수승 값 $i$를 사용자 $A$가 선택할 수 있도록하는 그룹 서명 방식도 함께 제안하였다[5][8][7]. 생성된 키 정보를 이용하여 사용자 $A$가 평문 $m$에 대한 서명문을 생성하는 과정은 다음과 같다.

① $0 < r_1 < f, 0 < r_2 < n$ 인 랜덤수 $r_1$, $r_2$를 생성하여 $X = b^{r_1} \cdot r_2^{\gamma^s} \bmod n$ 을 계산한다.
② 해쉬 함수 $h(\cdot)$에 의한 해쉬값 $e=h(X, m)$을 계산한다.
③ 다음과 같은 $c_1$, $c_2$를 계산한다.

$$c_1 = r_1 + s_A \cdot e \bmod f,\ c_2 = r_2 \cdot x_A^e \bmod n$$

④ $(X, m, c_1, c_2)$를 수신자에게 전달한다.

서명문$(X, m, c_1, c_2)$를 수신한 수신자는 서명자의 도움 없이 다음과 같은 과정을 통하여 자체 검증 가능하다.

① 메시지 $m$ 해쉬값 $e = h(X, m)$을 계산한다.
② 다음의 수식이 만족되는지 확인한다.

$$(ID_G \cdot y^{-i})^e \cdot b^{c_1} \cdot c_2^{\gamma^s} \stackrel{?}{=} X \bmod n$$

수신자는 검증 과정에서 서명문이 그룹의 서명문임을 확인 가능할 뿐 서명자의 신원을 확인할 수 없다. 본 검증 방법은 부인 방지 서명을 이용하는 그룹 서명과 달리 서명자의 협조 없이도 수신자에 의하여 검증되므로 서명 검증이 매우 효율적이다. 제안된 방법이 그룹 서명의 요구 조건을 만족시키기 위해서는 서명문으로부터 서명자의 신원을 확인할 수 있어야 한다. 박성준등이 제안한 신원 확인 과정은 다음과 같은 과정으로 센터에 의하여 수행된다[5][7].

① 서명문 $(X, m, c_1, c_2)$이 그룹 $G$의 그룹 서명이 됨을 확인한다.
② 그룹 $G$에 속하는 소속원들의 사용자 키들이 $(x_1, b^{s_1}), \cdots; (x_k, b^{s_k})$이라 할 때, 각 키들에 대하여 다음과 같은 $R1_i, R2_i$를 계산한다.

$$R2_i = c_2 \cdot x_i^{-e} \bmod n$$
$$R1_i = X \cdot R2_i^{\gamma^s} \bmod n$$

③ $R1_1, \cdots, R1_k$에서 $b^{c_1} = b^{s_i \cdot e} \cdot R1_i \bmod n$ 이 되는 $i$를 찾아 서명자로서 판정한다.

서명문 $(X, m, c_1, c_2)$의 서명자 $A$의 키 $(x_A, b^{s_A})$는 위의 관계식을 만족시킨다. 제안된 신분 확인 과정은 그룹 $G$에 소속하는 소속원들의 도움 없이 센터가 보유한 서명자의 비밀키 정보에 의하여 수행 가능하다. 따라서, 부인 방지 서명을 이용하는 그룹 서명 방법 보다 신분 확인 과정에 있어서도 매우 효율적임을 알 수 있다.

## 3. 암호 분석

### 3.1 신원 확인 과정 분석

신분 확인 과정에서 서명문을 생성한 서명자 $A$의 비밀키 정보는 센터의 검증 수식을 만

족시킨다. 그러나, 서명자 $A$의 키 뿐 아니라 그룹 $G$에 속하는 임의의 사용자들이 갖는 모든 키들이 센터의 신분 확인 과정에 의한 검증 수식을 만족시킨다는 문제점을 갖는다. 그룹 $G$에 속하는 사용자 B의 키 정보를 $(x_B, s_B)$라 하자. 이 경우, 사용자 $A$의 키 정보와 B의 키 정보는 다음과 같은 관계식을 갖는다.

$$(ID_G \cdot y^{-i}) = b^{-s_A} \cdot x_A^{-\gamma^s} = b^{-s_B} \cdot x_B^{-\gamma} \bmod n$$

이제 사용자 B의 키 $(x_B, b^{s_B})$ 또한 센터의 신분 확인 과정을 통과한다는 사실을 다음의 관계식으로 알 수 있다.

$$b^{s_A} = \frac{b^{s_B} \cdot x_B^{\gamma^s}}{x_A^{\gamma^s}}$$

$$R2 = c_2 \cdot x_B^{-e} = r_2 \cdot (x_A / x_B)^e \bmod n$$

$$R1 = X \cdot R2^{-\gamma^s} = b^{r_1} \cdot (x_B / x_A)^{e \cdot \gamma^s} \bmod n$$

$$R1 \cdot b^{s_B \cdot e} = b^{r_1} \cdot \left( \frac{b^{s_B} \cdot x_B^{\gamma^s}}{x_A^{\gamma^s}} \right)^e = b^{r_1 + s_A \cdot e} = b^{c_1} \bmod n$$

그러므로 센터가 수행하는 신분 확인 과정은 그룹 $G$에 속하는 모든 소속원의 키들이 만족시키므로 센터는 서명문의 진정한 서명자를 확인하는 것이 불가능하다. 따라서, 제안된 방식은 그룹 서명 방식의 기본 요구 사항을 충족시키지 못한다.

## 3.2 그룹 서명키의 위조

그룹 $G$에 속하는 사용자 $A$와 $B$가 결탁할 경우 A, B는 다음과 같은 방법으로 새로운 그룹 서명용 키를 계산할 수 있다.

$$s_C = ks_A - (k-1)s_B \bmod f, \; x_C = \frac{x_A^k}{x_B^{k-1}} \bmod n$$

$k$는 2 보다 크거나 같은 임의의 정수이다. 다음은 $(s_C, x_C)$가 그룹 G의 서명 키가 됨을 보여준다.

$$b^{-s_C} \cdot x_C^{-\gamma^s} = \frac{(b^{-s_A} \cdot x_A^{\gamma^s})^k}{(b^{-s_B} \cdot x_B^{-\gamma^s})^{k-1}}$$

$$= \frac{(ID_G \cdot y^{-i})^k}{(ID_G \cdot y^{-i})^{k-1}}$$

$$= ID_G \cdot y^{-i} \bmod n$$

따라서, 사용자 A, B는 신뢰 센터의 도움없이도 무수히 많은 새로운 그룹 서명 키를 생성할 수 있다.

## 3.3 인수 분해

RSA 합성수를 갖는 암호시스템의 안전성에 관련된 잉여류 문제로서 가장 잘 알려져 있는 문제는 2차 잉여류(quadratic residue)에 관한 문제이다. RSA 합성수 $n = pq$을 구성하는소수들은 홀수이므로 $p-1, q-1$은 항상 짝수가 된다. 이때, 임의의 x가 2차 잉여류라고 하면 x의 2차 잉여근(quadratic root)을 구하는 문제는 합성수 n을 인수 분해하는 문제와 동치가 된다. Rabin 공개키 암호는 이러한 2차 잉여근을 구하는 문제를 이용한 암호이다[3]. Zheng-Matsumoto-Imai는 2차 이상의 $\gamma^h$-잉여류 개념을 이용하는 확률론적 공개키 암호시스템을 제안하였으나[4] $\gamma$의 값이 커질 경우 암호문을 복호하기 어렵기 때문에 $\gamma$의 값을 크게할 수는 없다. 따라서, 암호화시 평문에 대한 암호문의 비트 확장율이 커질수밖에 없는 문제점을 갖는다. 박성준등은 이러한 문제점을 해결하기 위하여 $\gamma$의 값은 작게하는 대신 $(\gamma^s)^h$-잉여류 개념을 도입하여 s에 따라 $\gamma^s$값을 크게함으로서 암호문에서의 비트 확장율을 크게 줄일 수 있었다[5][10].

2 절에서 소개된 그룹 서명 방식에서는 $(\gamma^s)^h$-잉여류 개념을 이용한 박성준등의 공개키 암호시스템의 복호화 과정을 이용하여 각 사용자의 비밀키를 생성한다. 그러나, 같은 그룹 식별 정

보에 대응되는 여러 사용자의 비밀키 계산을 위하여 $\gamma^{th}$- 잉여류근을 생성하는 과정은 사용자 결탁에 의하여 센터의 비밀 정보 $p, q$를 해독할 수 있다. 먼저 그룹 서명 방식에서 사용하는 RSA $n$ 상에서의 $\gamma^{th}$- 잉여류 문제와 $n$을 인수 분해하는 문제와의 관련성을 다음의 정리를 통하여 살펴보자.

**정리 2** $\gamma, f, p', q'$은 서로 다른 소수이고, $p, q$를 다음과 같은 소수라 하자.

$$p = 2 \cdot \gamma^s f p' + 1, q = 2 \cdot f \cdot q' + 1$$

그러면, 다음의 두 가지 사실이 성립한다.

① 임의의 x가 법 q 상에서 $\gamma^{th}$- 잉여류이면 x는 단 하나의 $\gamma^{th}$- 잉여근을 갖는다.

② 임의의 x가 법 p 상에서 $\gamma^{th}$- 잉여류이면 x 는 $\gamma$개의 $\gamma^{th}$- 잉여근을 갖는다. $h_2$를 법 p상에서 원시원소라하고 $a = h_2^j \bmod p$를 x의 $\gamma^{th}$- 잉여근이라 하면 $\gamma^{th}$- 잉여근들은 다음과 같다($0 \le j < 2 \cdot \gamma^{s-1} \cdot f \cdot p'$).

$$x = a_i^{\gamma}, a_i = h_2^{j+i \cdot 2 \cdot \gamma^{s-1} \cdot f \cdot p'} \ (i = 0, 1, \cdots, \gamma\text{-}1)$$

**증명**

① $a_1, a_2$를 x의 서로 다른 $\gamma^{th}$- 잉여근이라 하자. $\gcd(\gamma, q\text{-}1) = 1$이므로, $\gamma \cdot d = 1 \bmod q\text{-}1$인 $d$가 존재한다. Fermat의 소정리 (little theorem)에 의하여, $a_1^{\gamma \cdot d} = a_1, a_2^{\gamma \cdot d} = a_2 \bmod q$이다. 따라서, $a_1 = x^d \bmod q, a_2 = x^d \bmod q$이 되므로 $a_1 = a_2$이다. 이것은 가정에 모순이다.

② 임의의 $x = a^{\gamma} \bmod p$라 하면 $x = h_2^{j \cdot \gamma} \bmod p$를 만족하는 $0 \le j < 2 \cdot \gamma^{s-1} \cdot f \cdot p'$인 $j$가 단 하나 존재한다. $h_2$는 법 $p$상에서 원시원소이므로 $i = 0, 1, \cdots, \gamma\text{-}1$인 $i$에 대하여 $a_i = h_2^{i \cdot 2 \cdot \gamma^{s-1} \cdot f \cdot p' + j}$는 $x = a_i^{\gamma} \bmod p$를 만족한다. 또한 $h_2$가 원시원소이므로 $\gamma$개의 잉여류 근들 $a_0, a_1, \cdots, a_{\gamma-1}$은 모두 서로 다르다.

**따름정리1** $n = pq$라하고 $p, q, \gamma, f, p', q'$는 앞의 정리에서 정의한 것과 같은 형태이다. 임의의 서로 다른 원소 $x, y$가 $\gcd(x, n) = \gcd(y, n) = 1$이고 $x^{\gamma} = y^{\gamma} \bmod n$을 만족하면, $\gcd(x - y, n) = q$이 된다.

**증명** $x^{\gamma} = y^{\gamma} \bmod n$이므로 $x^{\gamma} = y^{\gamma} \bmod p, x^{\gamma} = y^{\gamma} \bmod q$를 만족한다. 앞의 정리 2에 의하여 $x = y \bmod q$이다. 또한 가정에 의하여 $x \not\equiv y \bmod n$라고 하였으므로 $x \not\equiv y \bmod p$이다. 따라서, $\gcd(x - y, n) = q$이다.

따름정리에서는 법 $n$상에서 서로 다른 $\gamma^{th}$- 잉여류를 구할 수 있다면 합성수 n의 소인수를 구할 수 있음을 보인다. 이제 위와같은 정리를 이용하여 본 고에서 소개된 그룹 서명 방식을 해독할 수 있음을 보이고자 한다. 그룹 $G$에 속하는 사용자 $A$와 $B$의 비밀키 $s_A$와 $s_B$는 다음과 같이 표현된다.

$$s_A = u_1 \cdot \gamma + t_1, s_B = u_2 \cdot \gamma + t_2$$

이때, 센터가 선정한 $\gamma$의 값은 매우 작은 값이므로 $t_1$과 $t_2$가 같게 될 가능성이 매우 높다. 만일 $t_1 = t_2$가 되는 사용자 $A, B$가 결탁할 경우 다음과 같은 관계식을 만들 수 있다

$$ID_G = b^{-s_A} \cdot x_A^{-\gamma^s} = b^{-s_B} \cdot x_B^{-\gamma^s} \bmod n$$
$$(b^{u_1} \cdot x_A^{\gamma s-1})^{\gamma} = (b^{u_2} \cdot x_B^{\gamma s-1})^{\gamma} \bmod n$$

$X = b^{u_1} \cdot x_A^{\gamma s-1} \bmod n$, $Y = b^{u_2} \cdot x_B^{\gamma s-1} \bmod n$라 하면, $X^{\gamma} = Y^{\gamma} \bmod n$이다. 만일, $X \not\equiv Y$이면 앞의 따름 정리에 의하여 $\gcd(X - Y, n) = q$가 된

다. 실제로 $X, Y$는 대부분의 경우 서로 다른 값을 갖게 된다. 따라서, $s_A \bmod \gamma = s_B \bmod \gamma$를 만족하는 사용자 $A, B$가 결탁할 경우 센터의 비밀 정보 $p, q$는 해독된다. 또한, 그룹 $G$에 속하는 사용자들의 키 $s_i$ 에서 $s_i \bmod \gamma$의 값들이 모두 서로 다른 값을 갖는다 하더라도, 이러한 값들의 적당한 조합을 통하여 $X^\gamma = Y^\gamma \bmod n$을 만족하는 $X, Y$를 구할 수 있다. 예를들어, $s_1 \bmod \gamma = i_1$, $s_2 \bmod \gamma = i_2$, $s_3 \bmod \gamma = i_3$, $s_4 \bmod \gamma = i_4$이고 이러한 값들이 모두 다르다고 하자. 그러나 이러한 값들이 $i_1 + i_2 = i_3 + i_4$ 이 된다면 $X^\gamma = Y^\gamma \bmod n$을 만족하는 $X, Y$를 구할 수 있다. 이러한 방법은 같은 그룹에 속하는 소속원들의 결탁뿐 아니라, 서로 다른 그룹에 속하는 소속원들 사이의 결탁에 의해서도 해독 가능하다.

## 4. 결 론

본 고에서는 박성준등이 제안한 그룹 서명 방식이 갖는 두 가지 문제점을 분석하였다. 하나는 제안된 그룹 서명 방식이 그룹 서명의 기본 요구 사항인 서명자의 신원 확인이 불가능하다는 사실이며, 또 다른 문제점은 사용자 결탁에 의하여 센터의 도움없이도 새로운 그룹 서명키를 생성할 수 있으며 센터의 비밀 정보가 해독될 수 있다는 사실이다. 최근 Chen과 Pedersen은 신뢰 센터가 그룹 멤버들의 도움없이 서명자의 신원을 확인할 수 있는 그룹 서명 방식을 제안하였으나[2] 그룹 서명 계산량이 전체 그룹 멤버의 수에 비례하여 증가하기 때문에 그룹 멤버의 수가 많을 경우 현실적으로 실현이 불가능하다. 따라서, 그룹 서명 생성과 서명자 신원 확인이 효율적인 그룹 서명 방식이 존재하는가 하는 문제는 아직 해결되지 않은 문제로 남아있다.

## 참 고 문 헌


[1] D. Chaum and E.van Heyst, 'Group Signature', EUROCRYPT' 91, pp.256-265, 1991

[2] L. Chen and T. P. Pedersen, 'New Group Signature Scheme', Eurocrypt' 94, pp.163-173, 1994.

[3] M. O. Rabin, 'Digitalized signatures and public-key functions as intractable as factorization', *Tech. Rep. MIT/LCS/TR-212*, MIT, Cambridge, Mass., 1979.

[4] Y. Zheng, T. Matsumoto, and H. Imai, 'Residuosity Problem and its Applications to Cryptography', Trans. IEICE, vol.E71, No.8, pp.759-767, 1988

[5] S. J. Park, 분산통신망을 위한 확률론적 암호 알고리즘 및 정보보호 프로토콜에 관한 연구 , 성균관 대학교, 정보공학과, 박사학위논문, 1995

[6] 박성준, 원동호, '고차 잉여류 문제와 이산대수 문제에 기반을 둔 역설적인 id-based 암호시스템', 한국통신정보보호학회 논문지 제4권 제2호, pp.113-118, 1994.12

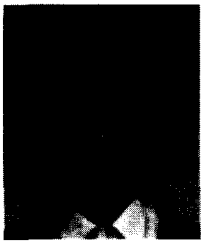
[7] 박성준, 김승주, 원동호, '효율적인 그룹 서명 방식', 한국정보과학회 가을학술발표회 논문집, pp.633-636, 1994.10.

[8] 박성준, 김지연, 원동호, 'Identity-based 그룹 서명', 한국전자공학회 하계종합학술발표회 논문집, pp.219-221, 1995. 6.

[9] S. J. Park, I. S. Lee, and D. H. Won, 'Practical Group Signature', Proc. of JW-ISC' 95, pp.127-133, Jan., 1995

[10] S. J. Park, B. Y. Lee, and D. H. Won, 'A Generalized Public Key Residue Cryptosystem and Its Applications', IEEE GLOBECOM' 95, Singapore, pp.1179-1182, 1995. 11.

## □ 著者紹介



**박 상 준(朴 商 竣, Sangjoon Park)**

1984년 2월 한양대학교 자연과학대학 수학과(이학사)
1986년 2월 한양대학교 대학원 수학과(이학석사)
1986년 1월 ~ 현재 한국전자통신연구소 선임연구원
1995년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정

**원 동 호(元 東 豪, Dong Ho Won)**

1976년 2월 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 성균관대학교 대학원 졸업(공학석사)
1988년 2월 성균관대학교 대학원 전자공학과(공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경 특공대 객원 연구원
1982년 3월 ~ 현재 성균관대학교 공과대학 정보공학과 교수
1991년 ~ 현재 한국통신정보보호학회 편집이사
1996년 4월 ~ 현재 정보화추진위원회 자문위원

※ 주관심분야 : 암호이론, 정보이론