通信情報保護學會論文誌
第 8 卷 第 3 號, 1998. 9

ID를 이용한 그룹 서명과 안전성

박 상준*, 김 승주*, 원 동호*

On the Security of ID-based Group Signature

Sang-Joon Park*, Seung-Joo Kim*, Dong-Ho Won**

요 약

Chaum과 Heyst가 그룹 소속원에 대한 익명성을 보장하는 그룹 서명 방식을 처음 제안한 이래 많은 종류의 그룹 서명 방식이 제안되었다. 그러나, 제안된 방식들의 대부분은 이산 대수에 근거한 ElGamal 형태의 디지털 서명 방식에 근거하고 있다. Ohta-Okamoto 방식과 Guillou-Quisquater 방식과 같은 ID-based 서명 방식에 근거한 그룹 서명 방식이 최근 제안되었으나[1], Mao는 제안된 방식이 그룹 서명으로 부터 서명자의 신분을 보호하지 못한다는 사실을 밝혀내었다. 본 논문에서는 Mao의 분석 방법을 피할 수 있는 방법을 제안하고 제안 방식의 안전성을 분석하였다. 본 논문에서 제안하는 방식은 기 제안된 방식과 마찬가지로 Stadler의 검증 가능 암호 기법(verifiable encryption)과 Schoenmakers 프로토콜을 사용한다.

Abstract

The most group signatures are based on the ElGamal-type signature scheme. Last year, we proposed the first ID-based group signature. However, Mao had a cryptanalysis of the scheme that the receiver (or any user) can identify the signer from the group signature. In this paper, we introduce our ID-based group signature and Mao's cryptanalysis, and propose an improved scheme that Mao's method can't be applied.

1. 서 론

그룹 서명에 대한 개념은 Chaum과 Heyst에 의하여 처음 제안되었으며, 다음과 같은 3가지 요구 조건을 갖는다[2].

• 그룹에 속하는 사용자만이 서명을 할 수

* 한국전자통신연구원
** 성균관대학교 정보공학과

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 모두 4가지의 그룹 서명을 제안하였다[2]. 4가지의 서명 기법중 하나는 일반 공개키 암호 알고리즘을 이용하는 방법이고, 나머지 3개는 부인 방지 서명(undeniable signature) 기법을 이용하였다[1]. 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. 일반 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 하므로 신뢰센터의 부담이 너무 크다.

1994년 Chen과 Petersen은 Schoenmakers의 프로토콜을 사용하여 Chaum과 Heyst의 그룹 서명 방식을 개선하였다[3]. 그들은 또한 그룹 소속원들 전체가 아니라 일부 그룹 소속원의 도움만으로 그룹 서명자의 신원을 밝힐 수 있는 방법을 함께 제안하였다. 1997년 Petersen은 임의의 서명 방식을 그룹 서명 방식으로 만들 수 있음을 보였다[12]. 이러한 그룹 서명 방식들은 이산 대수에 근거한 ElGamal 형태의 서명 방식을 사용한다.

1995년 박성준 등은 Chaum과 Heyst가 제안한 그룹 서명 기법의 비효율성을 개선하기 위하여 합성수 n에서의 고차 잉여류 문제에 안전성을 둔 새로운 그룹 서명 방식을 제안하였다[8][16]. 제안 방식은 수신자에 의한 서명의 자체 검증이 가능하고, 그룹 소속원의 협조 없이 센터에 의하여 서명자의 신원 확인이 가능하다. 또한 그룹의 ID 정보를 이용하는 등 효율성면에서 많은 장점을 가지고 있다. 그러나 제안된 방식은 실제로 그룹 관리자가 서명자의 신분을 확인하는 것이 불가능하고 사용자 결탁시 새로운 그룹 서명키를 계산할 수 있을 뿐 아니라 신뢰 센터의 비밀키가 노출될 가능성이 있는 등 안전하지 못한 것으로 판명되었다[15].

ID를 이용한 그룹 서명 방식은[11] 이제까지 제안된 ElGamal 형태의 디지털 서명 방식에[7] 근거한 그룹 서명과는 달리, Ohta-Okamoto[10]와 Guillou-Quisquater[6] 서명 방식과 같은 사용자 개인의 ID에 근거한 서명 방식(ID-based Digital Signature)을 사용하여 그룹 서명을 만드는 그룹 서명 방식을 말한다. 따라서, 그룹 서명은 그룹에 속한 그룹 소속원들의 ID 정보에 의하여 검증된다. 본 방식에서는 Stadler의 검증 가능 암호 기법(verifiable encryption)을[14] 이용한다. 서명자의 일반 서명문을 그룹 관리자의 공개키로 ElGamal 암호화하여 그룹 서명문을 생성하며, 그룹의 관리자(Group Authority)가 서명자의 신원을 확인할 수 있음을 서명 수신자에게 증명한다. 이때, 서명자의 신원을 숨기기 위하여 Schoenmakers 프로토콜을 이용한다[3]. 그룹 관리자에 의한 서명자의 신원 확인은 그룹 서명만으로 가능하기 때문에 부인 방지 서명을 이용하는 Chaum과 Heyst의 방법 보다 효율적이다.

그러나 기 제안된 ID를 이용한 서명 방식에서 서명 생성의 효율성을 위하여 선정된 파라메터들로 인하여 그룹 관리자의 도움없이 임의의 검증자가 그룹 서명으로 부터 서명자의 신원을 확인할 수 있음을 Mao가 지적하였다[9].

본 논문에서는 Mao의 분석 결과를 소개하

고, 안전성을 개선한 ID를 이용한 그룹 서명 방식을 제안하고자 한다.

본 논문은 모두 6개 절로 구성된다. 2절에서는 제안되는 방식에서 요구되는 ID를 이용한 서명 방식, Schoenmakers 프로토콜, Stadler의 검증 가능 암호(verifiable encryption) 기법들을 소개하였으며, 3절에서는 기 제안된 ID를 이용한 그룹 서명 방식을 기술하였다. 4절에서는 기 제안된 그룹 서명 방식의 안전성과 Mao의 암호 분석 결과를 소개하고, 5절에서는 Mao의 분석 방법을 피할 수 있는 개선된 ID를 이용한 그룹 서명 방식을 제안한다.

6절은 결론부이다.

2. 준비 단계

본 절에서는 ID-based 그룹 서명 방식에서 사용하는 ID를 이용한 서명 방식[10][6], Schoenmakers 프로토콜[3], Stadler의 검증 가능 암호 기법에[14] 대하여 소개하고자 한다. ID를 이용한 서명 방식의 대표적인 예로는 Ohta-Okamoto 방식과 Guillou-Quisquater 방식이 있으나 본 논문에서는 Ohta-Okamoto 방식만을 다룬다.

2.1 Ohta-Okamoto 서명방식

센터는 RSA 모듈라 n과 사용자의 개인식별 정보 ID에 대응되는 비밀키 s_A를 다음과 같이 계산한다.

- $n=pq$이고 p, q는 RSA 강한 소수(strong prime)이다.
- $e \cdot d = 1 \bmod \phi(n) = (p-1)(q-1)$
- 사용자 A의 ID정보 ID_A에 대응되는 비밀키 $s_A = ID_A^d \pmod n$
- 센터의 비밀 정보 : p, q, d
- 센터의 공개 정보 : n, e

임의의 메시지 m에 대한 사용자 A의 서명 및 검증 과정은 다음과 같다.

- 서명 과정
  - 난수 k를 생성하여 $r=k^e \pmod n$을 계산한다.
  - 메시지 m과 r의 해쉬값 $h(m, r)$을 계산한다.
  - 서명 $c = s_A^{h(m, r)} \cdot k \pmod n$을 계산
  - (r, c)를 메시지 m의 서명으로 서명 수신자에게 보낸다.
- 검증 과정
  - 메시지 m과 r의 해쉬값 $h(m, r)$을 계산한다.
  - 관계식 $c^e \stackrel{?}{=} ID_A^{h(m, r)} \cdot r \pmod n$을 확인한다.

2.2 Schoenmakers 프로토콜

본 절에서는 그룹 서명 방식에서 자주 사용되는 Schoenmakers 프로토콜에 대하여 소개하고자 한다[3]. Schoenmakers 프로토콜은 여러개의 witness중 하나의 witness에 대응되는 비밀정보를 가지고 있음을 증명하는 프로토콜이다. 그룹 서명에서는 그룹에 속한 소속원들의 공개키를 witness로 하고 그룹에 속한 특정 서명자는 자신의 공개키에 대응되는 비밀키를 가지고 그룹의 공개키들 중 하나에 대응되는 비밀키를 가지고 있음을 증명하는 방식으로 자신의 신분을 감추는 동시에 그룹의 서명을 생성하는데 이용한다.

p, q는 소수이고 $q|p-1$라고 하자. 또한, g의 위수를 q라고 하고 $h_i = g^{x_i} \pmod p$ $(i=1, 2, \cdots, l)$라 하자. $(g, h_1, h_2, \cdots, h_l)$는 서명자와 검증자 모두에게 공개된 정보이고 증명자는 x_1만을 안다고 하자. 이제 증명자가 l개의 $h_1, h_2, \cdots, h_l$에서 $h_i = g^{x_w}$이 되는 w를 적어도 하나를 알고 있다는 것을 다음과 같이 증명할 수 있다.

1. 증명자 : 난수 $0<w_i, d_i<q$ $(i=1, 2, \cdots, l, j=2, \cdots, l)$를 생성하고 $a_i(i=1, 2, \cdots, l)$를 다음과 같이 생성한다.

$$a_1=g^{w_1} \pmod p,\ a_i=g^{w_i}\cdot h_i^{-d_i} \pmod p \quad (i\geq 2)$$

2. 검증자 : 난수 $0<c<q$를 생성하여 증명자에게 보낸다.
3. 증명자 : $d_1=c-\sum_{i=2}^{l} d_i \pmod q$을 계산한 후 다음과 같이 $r_i(i=1, 2, \cdots, l)$을 계산하고 $(d_1, \cdots, d_l, r_1, \cdots, r_l)$을 검증자에게 보낸다.

$$r_1=w_1+x_1d_1,\ r_i=w_i(i\geq 2)$$

4. 검증자 : $c=\sum_{i=1}^{l} d_i \pmod q$와 $g^r=a_i\cdot h_i^d \pmod p (i=1, \cdots, l)$을 확인한다.

2.3 Stadler의 검증 가능 암호

Stadler는 키 위탁 시스템과 분쟁시 사용자의 신원 확인이 가능한 전자 화폐 등에 적용하기 위하여 검증 가능 암호(verifiable encryption)를 제안하였다[14].

검증 가능 암호는 증명자, 검증자외에 암호문을 복구할 수 있는 제3의 위탁기관이 있다. 증명자는 임의의 메시지를 암호화시키고 암호문에 대한 평문을 제3의 위탁기관이 풀수 있음을 증명하기 위하여 메시지를 위탁기관의 공개키로 다시 암호화하여 검증자에게 제공한다. 이때 증명자는 두개의 암호문이 같은 평문에 대한 암호문임을 증명함으로서 위탁기관이 암호문으로 부터 평문을 복구할 수 있음을 검증자에게 증명한다. Stadler는 두가지 검증 가능 암호를 제안하였는 데 이산 로그에 대한 검증 가능 암호(verifiable encryption of discrete logarithm)와 e-제곱근에 대한 검증 가능 암호(verifiable encryption of e-제곱근)를 제안하였다. 본 논문에서는 ID-based 그룹 서명에서 사용되는 e-제곱근의 검증 가능 암호 기법을 소개하고자 한다.

먼저 n을 RSA 합성수라 하고 $g\in Z_n^*$는 큰 위수를 갖는 생성원이라 하자. 중개자는 자신의 비밀키 z를 생성하여 공개 $y=g^z \pmod n$을 계산한다. 증명자는 위탁기관의 공개키 y로 메시지 m을 ElGamal 암호화시킨 암호문(A, B)을 다음과 같이 계산한다.

$$A=g^{\alpha} \pmod n,\ B=m\cdot y^{\alpha} \pmod n$$

이 경우 위탁기관은 암호문 (A, B)로 부터 평문 m을 다음과 같이 구할 수 있다.

$$m=B/A^z \pmod n$$

증명자는 메시지 m의 암호문 $C=m^e \pmod n$을 계산하고 암호문 C를검증자에게 준다. 이제 검증자는 (A, B)가 암호문 C의 e-제곱근에 대한 ElGamal 암호라는 사실을 다음과 같은 프로토콜에 의하여증명할 수 있다.

1. 증명자 : $w\in\{0, 1, \cdots, \lceil 2^l n^{1+\varepsilon}\rceil\}$를 생성하고 t_S, t_y를 다음과 같이 계산하여 검증자에게 (t_S, t_y)를 전송한다.

$$t_S=g^w \pmod p,\ t_y=y^{\alpha w} \pmod p$$

2. 검증자 : $c\in\{0, \cdots, 2^l-1\}$를 생성하여 증명자에게 보낸다.
3. 증명자 : $r=w-c\cdot\alpha$를 계산하고 r을 검증자에게 전송한다.
4. 검증자 : t_S, t_y가 다음의 관계식을 만족하는지 확인한다.

$$t_S \stackrel{?}{=} g^r A^c \pmod n$$
$$t_y \stackrel{?}{=} y^r (B^e/C)^c \pmod n$$

5. 위와같은 과정을 K회 반복 시행한다.

해쉬 함수를 이용하면 위의 대화형 상호 프로토콜을 비대화형 프로토콜로 변환시킬 수 있다. 이때, 검증자가 선택하는 난수 c는 해쉬 함수에 의하여 다음과 같이 계산된다.

$$c = h(M||A||B||t_g||t_y)$$

제안 방법의 안전성을 위하여 n, l, ε은 다음과 같은 조건을 갖는다.

$$n > 2^{750},\ l > 80,\ \varepsilon \approx \frac{1}{5}$$

3. ID 정보를 이용한 그룹 서명

본 절에서는 기 제안된 ID를 이용한 그룹 서명 방식[11]의 구성 요소와 키 생성 과정, 그룹 서명 생성 및 검증 과정, 서명자 신분 확인 과정등을 기술하고자 한다. ID를 이용한 그룹 서명 방식은 검증자가 그룹 소속원의 ID를 이용하여 그룹 서명을 검증하며, ID에 근거한 서명 방식인 Ohta-Okamoto 방식과 Guillou-Quisquater 서명 방식을 기반으로 하여 만들어진다. 본 방식은 신뢰 센터(TC:Trusted Center), 그룹 관리자(GA:Group Authority), 어떤 특정 그룹에 속한 서명자, 서명 수신자로 구성된다. 신뢰 센터는 시스템내의 시큐리티 변수를 결정하고 시스템과 사용자의 키를 생성하며, 그룹 관리자는 자신이 관리하는 그룹에서 발행한 그룹 서명에 대하여 분쟁이 발생할 경우 그룹 서명으로 부터 서명자의 신원을 확인하는 역할을 수행한다.

서명자는 먼저 자신의 서명용 비밀키를 사용하여 Ohta-Okamoto 방식에 의하여 서명 c를 생성한다. 서명자는 c를 그룹 관리자의 공개키로 ElGamal 암호화 시켜 얻은 암호문 (A, B)를 서명 수신자에게 보낸다. 따라서, 서명 수신자는 분쟁 발생시 암호문 (A, B)를 그룹 관리자에게 제출하고, 그룹 관리자는 (A, B)로 부터 본래의 Ohta-Okamoto 방식의 서명 c을 얻을 수 있다. 이때, 서명자는 수신자에게 (A, B)가 자신의 서명 c의 암호문이라는 것을 증명하여야 하며 이 증명 과정에서 자신의 신분을 감추기 위하여 Schoenmakers 프로토콜을 사용한다.

3.1 키 생성 과정

시스템을 구성하기 위해서는 우선 신뢰 센터가 시스템 구성에 필요한 각종 시큐리티 변수와 시스템내의 각 사용자에 대한 키를 생성하여야 한다.

- 신뢰 센터에 의한 키 생성
  - $n = p_1 \cdot p_2$, $q|(p_1 - 1)$, $q|(p_2 - 1)$ p_1, p_2, q는 모두 소수이고 q의 비트 사이즈는 160 비트이다($|q| = 160$).
  - $g \in Z_n$는 위수 q를 갖는다.
  - $e \cdot d = 1 \pmod{\phi(n)}$이고 e는 160 비트 사이즈를 갖는다.
  - 사용자 i의 개인 식별 정보 id_i에 대응되는 서명용 비밀키 $s_i = id_i^d \pmod{n}$을 계산한다.
  - 공개 정보 : n, e, q
  - 비밀 정보 : p_1, p_2, d
- 그룹 관리자의 키 생성
  - 비밀키 $x \in Z_n^*$를 랜덤하게 생성한다.
  - 공개키 $y = g^x \pmod{n}$을 계산하여 공개한다.

소수 p_1, p_2가 충분히 클 경우, 그룹 관리자의 공개키 y로 부터 비밀키 x를 구하는 것은 이산 로그 문제이므로 p_1, p_2를 알고 있는 신뢰 센터 조차도 그룹 관리자의 비밀키 x를 알 수 없다.

3.2 그룹 서명 생성 및 검증 과정

서명자 i는 자신의 비밀키 s_i를 사용하여 일반적인 형태의 ID-based 디지털 서명 c를 계산한다. 이때, Stadler의 e-제곱근 검증 가능 암호 기법을 사용하여 그룹 관리자가 자신의 신원을 확인할 수 있음을 증명한다. 또한 Schoenmakers 프로토콜을 사용하여 그룹 서명이 그룹 소속원중의 한명이 만든 서명임을 증명한다.

$G=\{id_1, \cdots, id_k\}$를 그룹 소속원 개인 식별 정보들의 집합이고 $h(\cdot)$는 안전한 해쉬 함수이다. 그룹 소속원 id_i이 그룹 서명을 생성하고 서명 수신자가 검증하는 과정은 Stadler의 검증가능 암호와 Schoenmakers 프로토콜을 이용하여 다음과 같이 구성된다.

1. 서명자 : 다음과 같은 과정으로 일반 서명과 암호화 과정을 수행한다.
   - 난수 $r \in Z_n^*$을 생성하여, 다음과 같은 Ohta-Okamoto 방식에 의하여 디지탈 서명 (R, c)를 생성한다.

$$R=r^e \pmod n,\ c=s_i^{h(m,R)} \cdot r \pmod n$$

   - 서명 c를 그룹 관리자의 공개키 y로 암호화 한다.

$$A=g^\alpha \pmod n, B=c \cdot y^\alpha \pmod n \ (\alpha \in Z_q \text{는 난수})$$

   - $C_i = id_i^{h(m,R)} \cdot R \pmod n \ (i=1, \cdots, k)$
   - $w_1, \cdots, w_k, d_2, \cdots, d_k \in Z_q$를 랜덤하게 선택하여 t_{g_i}, t_{y_i}를 다음과 같이 계산한다.

$$t_{g_1}=g^{w_1} \pmod n,\ t_{g_i}=g^{w_i} \cdot A^{d_i} \pmod n$$
$$t_{y_1}=y^{w_1} \pmod n,\ t_{y_i}=y^{w_i} \cdot (B^e/C_i)^{d_i} \pmod n$$

   - $(t_{g_1}, \cdots, t_{g_k}, t_{y_1}, \cdots, t_{y_k})$를 서명 수신자에게 전송한다.
2. 수신자 : $d_0 \in Z_q$를 랜덤하게 선택하여 서명자에게 전송한다.
3. 서명자 : 그룹 서명$(m, R, A, B, d_1, \cdots, d_k, r_1, \cdots, r_k)$을 계산하여 수신자에게 전송한다.
   - $d_1=d_0-\sum_{i=2}^{k} d_i \pmod q$을 계산한다.
   - $r_1=w_1-d_1 \cdot \alpha \pmod q$, $r_i=w_i (2 \le i \le k)$을 계산한다.
4. 수신자 : 수신자는 그룹 소속원의 개인 식별 정보 id_i를 사용하여 그룹 서명을 다음과 같이 검증한다.
   - $C_i=id_i^{h(m,R)} \cdot R \pmod n$를 계산한다.
   - $d_0=\sum_{i=1}^{k} d_i \pmod q$을 확인한다.
   - $i = 1, 2, \cdots, k$에 대하여 t_{g_i}, t_{y_i}이 다음의 관계식을 만족하는지 확인한다.

$$t_{g_i} \stackrel{?}{=} g^{r_i} \cdot A^{d_i},\ t_{y_i} \stackrel{?}{=} y^{r_i} \cdot (B^e/C_i)^{d_i}$$

해쉬 함수를 사용하여 서명 수신자가 선택하는 난수 d_0를 다음과 같이서명자가 결정할 경우 제안된 그룹 서명 방식은 비대화형 그룹 서명 방식으로 변환될 수 있다.

$$d_0=h(t_{g_1}, \cdots, t_{g_k}, t_{y_1}, \cdots, t_{y_k}, A, B, h(m, R))$$

3.3 신분 확인 과정

서명 수신자와 그룹 사이에 메시지 m의 그룹 서명에 대한 분쟁이 발생하는 경우 그룹 관리자는 서명 수신자가 가지고 있는 그룹 서명으로 부터 서명자의 신원을 확인할 수 있다.

또한, Chaum-Heyst 방식에서는 서명자의 신원을 확인하기 위해서 그룹 소속원 전체의 도움이 필요하나, 본 방식은 신원 확인 과정에서 그룹 소속원의 도움이 필요없다. 신원을 확인하는 방법은 일반 서명의 ElGamal 암호문 (A, B)을 자신의 비밀키 x를 사용하여 복호화한 후, 그룹 G에 속하는 모든 ID 정보로 서명을 검증하여 검증이 되는 개인 식별 정보를

갖는 사용자를 구한다. 자세한 검증 과정은 다음과 같다.

- (A, B)를 복호화 하여 일반 서명문 $c=B/A^x \pmod n$를 구한다.
- $c' \stackrel{?}{=} id_i^{h(m,\ R)} \cdot R \pmod n$을 만족하는 id_i를 찾는다.

왜냐하면 $c=s_1^{h(m,\ R)} \cdot r \pmod n$이므로 $c'=C_1$이 되나 $i=2, \cdots, k$에 대해서는 $c' \neq C_i \pmod n$이므로, 위의 과정을 통해서 서명자 id_1을 결정할 수 있다.

4. 암호 분석

서명자 id_1은 메시지 m에 대하여 다른 서명자의 서명을 위조할 수 없다. 서명자 id_j의 서명을 위조하기 위해서는 $C_j=id_j^{h(m,\ R)} \cdot R \pmod n$의 e-제곱근를 계산하여야 한다. 그러나, RSA 합성수 n의 소인수 p_1과 p_2를 알지 못하기 때문에 C_j의 e-제곱근를 계산하는 것은 계산상 불가능하다. 또한, 서명 수신자와 그룹 관리자는 서명자의 비밀키 s_1을 알지 못하며 계산할 수도 없기 때문에 서명자 id_1의 그룹 서명을 만들 수 없다.

신뢰 센터와 서명 수신자는 그룹 관리자의 비밀키 x를 알지 못하며, x를 계산하는 것은 이산 로그 문제가 되기 때문에 p_1, p_2가 충분히 클 경우 신뢰 센터 조차도 x를 계산할 수 없다. 따라서, 암호문 (A, B)를 복호화하여 c를 구할 수 없다.

그러나, Mao는 앞절에서 제안한 방법과는 다른 방법을 사용하여 그룹 관리자의 비밀키 없이 서명자의 신원을 확인할 수 있음을 지적하였다. 서명자가 생성하는 정보중에서 t_{y_1}와 $t_{y_i}(i=2, \cdots, k)$의 분포는 서로 다르다. $S=\{g^i \pmod n \mid 0 \le i < q\}$라 하면 집합 S의 원소의 개수는 q-1이며, t_{y_1}의 집합 S에 속한다. 그러나, $t_{y_i}(2 \le i \le k)$는 집합 Z_n에 랜덤하게 분포한다. n의 비트 사이즈를 756이라 하고, q의 비트 사이즈를 160이라 하면 임의의 원소 $v \in Z_n$가 집합 S에 속할 확률은 2^{-596}이다. 이 경우, 집합 S에 속하는 원소는 q를 위수로 가지나, S에 속하지 않는 원소는 q를 위수로 갖지 않는다. 따라서, 임의의 원소 $v \in Z_n$가 q를 위수로 가질 확률은 거의 없다. 결과적으로, t_{y_1}의 위수는 q가 되지만, $t_{y_i}(0 \le i \le k)$는 q를 위수로 갖지 않으며, 서명 수신자는 그룹 관리자의 키 x를 모르고서도 그룹 서명자의 신원을 확인할 수 있다.

$$(t_{y_1})^q = 1 \pmod p,\ (t_{y_i})^q \neq 1 \pmod n \quad (i \neq 1)$$

5. 개선 방안

Mao의 분석은 제안된 그룹 서명 방식이 계산의 효율성을 위하여 p_1-1과 p_2-1의 공통 소인수 q를 위수로 갖는 g를 사용하는 경우 t_{y_1}과 $t_{y_i}(i \ge 2)$의 위수가 서로 다르다는 사실을 이용한다. 이러한 문제점은 p_1-1과 p_2-1의 공통 인수 q를 없애고 Z_n^*상에서 최대 위수 $\lambda(n)=(p_1-1, p_2-1)$를 갖는 생성원 g를 사용하여 해결할 수 있다. 그러나 이경우 160 비트 사이즈 공통 인수 q를 사용할 때 보다 지수들의 크기가 증가하기 때문에 계산 복잡도가 커진다. 또한, 위수 $\lambda(n)$은 신뢰 센터의 비밀 정보이므로 서명자가 $\lambda(n)$을 알지 못하기 때문에 $\lambda(n)$에 대한 잉여류 계산을 할 수 없다. 따라서, $\lambda(n)$의 잉여류 연산을 정수상의 연산으로 바꾸어야 한다.

먼저 신뢰 기관은 소수 p_1, p_2를 생성하여 합성수 $n=p_1 \cdot p_2$을 만든다. 생성원 g는 Z_n^*에서 최대 위수 $\lambda(n)=lcm(p_1-1, p_2-1)$을 갖는 생성원 g를 선택한다. e, id_i, s_i, x, y는 기존에 제안된 방식과 동일하다. 안전성을 위하여 n의 비트 사이즈는 756 보다 크거나 같다($|n| \ge$

756).

개선된 ID를 이용한 그룹 서명 프로토콜

1. 서명자 : 다음의 과정을 수행한다.
   - 난수 $r \in Z_n^*$을 생성하여, 다음과 같은 Ohta-Okamoto 서명 (R, c)를 생성한다.

$$R = r^e \pmod n,\ c = s_1^{h(m,R)} \cdot r \pmod n$$

   - 서명 c를 그룹 관리자의 공개키 y로 암호화 한다.

$$A = g^\alpha \pmod n,\ B = c \cdot y^\alpha \pmod n\ (\alpha는\ 0 < \alpha < 2^h인\ 난수)$$

   - $C_i = id_i^{h(m,R)} \cdot R \pmod n\ (i = 1, \cdots, k)$
   - $|d_i| < 2^h (i = 2, \cdots, k)$이고 $|\sum_{i=2}^{k} d_i| < 2^h$이 되는 난수 d_i들과 $0 < w_1, \cdots, w_k < 2^{l_2}$인 r_i들을 선택한다(단, $l_2 > l_0 + l_1 + 64$).
   - t_{g_i}, t_{y_i}를 다음과 같이 계산한다.

$$t_{g_1} = g^{w_1} \pmod n,\ t_{g_i} = g^{w_i} \cdot A^{d_i} \pmod n$$
$$t_{y_1} = y^{rw_1} \pmod n,\ t_{y_i} = y^{rw_i} \cdot (B^r/C_i)^{d_i}\ n \pmod n\ (2 \le i \le k)$$

   - $(t_{g_1}, \cdots, t_{g_k}, t_{y_1}, \cdots, t_{y_k})$를 서명 수신자에게 전송한다.
2. 수신자 : $|d_0| < 2^{h-64}$인 난수 d_0를 선택하여 서명자에게 전송한다.
3. 서명자 : 그룹 서명$(m, R, A, B, d_1, \cdots, d_k, r_1, \cdots, r_k)$을 계산하여 수신자에게 전송한다.
   - $d_1 = d_0 - \sum_{i=2}^{k} d_i$을 계산하고 $|d_1| < 2^h$이면 프로토콜을 계속 수행하고, 아니면 프로토콜을 중지하고 처음부터 다시 시작한다.
   - $r_1 = w_1 - d_1 \cdot \alpha$, $r_i = w_i (2 \le i \le k)$에서 r_1이 $0 < r_1 < 2^{l_2}$이면 프로토콜을 계속 수행하고, 아니면 프로토콜을 중지하고 처음 부터 다시 시작한다.
4. 수신자 : 수신자는 그룹 소속원의 개인 식별 정보 G를 사용하여 그룹 서명을 다음과 같이 검증한다.
   - $C_i = id_i^{h(m,R)} \cdot R \pmod n$를 계산한다.
   - $d_0 \stackrel{?}{=} \sum_{i=2}^{k} d_i$이 되는지 확인한다.
   - $i = 1, 2, \cdots, k$에 대하여 t_{g_i}와 t_{y_i}이 다음의 관계식을 만족하는지 확인한다.

$$t_{g_i} \stackrel{?}{=} g^{r_i} \cdot A^{d_i},\ t_{y_i} \stackrel{?}{=} y^{r_i} \cdot (B^e/C_i)^{d_i}$$

그룹 관리자가 서명자의 신원을 확인하는 방법은 기 제안된 방법과 동일하다[11]. 제안된 방법에서는 g의 위수를 서명자가 알지 못하기 때문에 위수 $\lambda(n)$상의 잉여류 연산을 하지 않고 정수상의 연산을 한다. 이러한 정수 연산 과정에서 사용자의 신원을 숨기기 위해서는 난수 $d_1, \cdots, d_k, r_1, \cdots, r_k$이 서로 구별되는 분포 특성을 가져서는 안된다.

- 난수 $d_1, d_2, \cdots, d_k$들의 분포 범위
  - $|d_0| < 2^{l_1 - 64}$이고 $|\sum_{i=2}^{k} d_i| < 2^{l_2}$이므로 $|d_0 - \sum_{i=2}^{k} d_i| < 2^{l_2} + 2^{l_1 - 64}$이다.
  - 그러나 $|d_0 - \sum_{i=2}^{k} d_i| > 2^{l_1}$이 되는 경우에는 프로토콜이 중단되므로 d_1의 값이 수신자에게 제공되지 않는다. 또한, $|d_0| < 2^{l_1 - 64}$이기 때문에 부등식 $|d_0 - \sum_{i=2}^{k} d_i| > 2^{l_1}$이 성립할 확률은 $\frac{1}{2^{64}}$ 보다 작으므로 거의 발생하지 않을 것이다.
  - 따라서, 수신자가 받는 d_1은 항상 $|d_1| < 2^{l_1}$이 되는 랜덤한 수로서, 수신자는 d_1 값의 분포와 $d_2, \cdots, d_k$ 값의 분포를 구분할 수 없다.
- 난수 $r_1, r_2, \cdots, r_k$들의 분포 범위
  - $|d_1| < 2^{l_1}$이고 $0 < \alpha < 2^{l_0}$이므로 $|d_1 \cdot \alpha| < 2^{l_0 + l_1}$이다.

- $0<w_1<2^{l_0}$이므로 $2^{l_1}-2^{l_0+l_1}<r_1=w_1-d_1\cdot\alpha<2^{l_0}+2^{l_0+l_1}$이다.
- 그러나, 서명자는 $0<r_1<2^{l_0}$인 경우에만 프로토콜을 계속 수행하고, 아니면 프로토콜을 중지하므로 서명 수신자가 받는 r_1은 항상 $0<r_1<2^{l_0}$이다.
- 따라서, r_1과 r_2, …, r_k들이 분포하는 범위는 구별할 수 없다.
- 또한, $l_2>l_0+l_1+64$이기 때문에 r_1이 부등식 $0<r_1<2^{l_0}$을 만족하지 않을 확률은 $\frac{1}{2^{64}}$보다 작다.

• $l_0=160$, $l_1=256$, $l_2=512$라고 하면 제안된 시스템에서 충분한 안전성을 제공할 수 있다.

본 방식에서 t_{y_1}과 $t_{y_i}(i\geq 2)$의 위수는 $\lambda(n)$의 약수이며, $\lambda(n)$이 비밀 정보이기 때문에 서명자와 수신자는 알 수 없다. 또한 $\lambda(n)$을 알고 있는 신뢰 센터라 할지라도 n의 소인수 p_1, p_2가 충분히 클 경우 비밀키 x를 구하는 것은 p_1(또는 p_2)상의 이산 로그를 계산하는 것이기 때문에 x를 계산할 수 없다.

각 t_{y_i}들은 모두 다음의 수식을 만족한다.

$$t_{y_1}^{\lambda(n)}=1 \pmod n,\ t_{y_i}^{\lambda(n)}=1 \pmod n (i=2, \cdots, k)$$

기존의 방식에서는 t_{y_1}의 위수가 $\lambda(n)$ 보다 작은 q로 고정되나 새로운 방식에서는 w_1 값에 따라 위수가 $\lambda(n)$의 약수중 하나로 가변된다. $t_{y_i}(i\geq 2)$의 위수 또한 $\lambda(n)$의 약수중 하나로 가변되기 때문에 t_{y_1}과 $t_{y_i}(i=2, \cdots, k)$를 구분하는 것은 불가능하다. 따라서, Mao의 분석 방법을 적용할 수 없다.

6. 결 론

본 논문에서는 기 제안된 ID를 이용한 그룹 서명 방식의[11] 문제점을 분석하고 안전성을 개선한 그룹 서명 방식을 제안하였다. 기 제안 방식에서는 서명 생성과 검증 과정에서의 효율성을 위하여 합성수 n의 소인수 p_1, p_2에서 p_1-1, p_2-1의 공통 소인수 q를 위수로 갖는 생성원을 사용하였다. 그러나 Mao가 지적하였듯이 q를 위수로 갖는 생성원의 사용은 그룹 관리자의 도움없이도 검증자가 서명자의 신원을 확인할 수 있다. 이러한 문제점을 해결하기 위하여 Z_n^*상에서 최대 위수 $\lambda(n)=\mathrm{lcm}(p_1-1, p_2-1)$을 갖는 생성원을 사용하는 방법을 제안하였다. 기존 방법에서는 q를 공개 정보로 사용하였으나, 새로운 방법에서는 $\lambda(n)$가 신뢰 센터의 비밀 정보이기 때문에 서명자는 $\lambda(n)$에서의 잉여류 연산 대신 정수 연산을 수행한다. 정수 연산은 잉여류 연산과 달리 연산의 결과값의 크기가 증가거나 감소할 수 있기 때문에 이러한 특성으로 서명자의 신원을 확인할 수 없도록 하기 위하여 서명자가 선택하는 난수의 선택 조건을 추가하였다.

참고문헌

[1] D. Chaum and H. van Antwerpen, 'Undeniable Signatures', Advances in Cryptology - CRYPTO'89, Springer, 1990, pp.212-216.

[2] D. Chaum and E. Heyst, 'Group signatures', Advances in Cryptology - EUROCRYPT'91, LNCS 547, Springer, 1992, pp.257-265.

[3] L. Chen and T. Pedersen, 'New group signature schemes', Advances in Cryptology - EUROCRYPT'94, LNCS 950, Springer, 1995, pp.163-173.

[4] T. ElGamal, 'A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms', em IEEE Trans. on Information Theory, Vol. IT-31, No. 4, 1985, pp.469-472.

[5] Y. Frankel, Y. Tsiounis and M. Yung, 'em Indirect Disclosure Proofs : Achieving Efficient Fair Off-Line E-cash', Advances in Cryptology - ASIACRYPT' 96, LNCS 1163, Springer, 1996, pp.286-300.

[6] L. C. Guillou and J.-J. Quisquater, 'A paradoxical identity-based signature scheme resulting from zero-knowledge', Advances in Cryptology - CRYPTO' 88, LNCS 403, Springer-Verlag, 1990, pp.216-231.

[7] L. Harn and Y. Xu, 'Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm', em Electronics Letters, Vol. 30, No. 24, Nov 1994, pp.2025-2026.

[8] KIM, S. J., PARK, S. J., and WON, D. H., 'Convertible group signatures', Advances in Cryptology - ASIACRYPT' 96, LNCS 1163, Springer, 1996, pp.311-321.

[9] W. Mao, 'Cryptanalysis of ID-based Group Signature', em private communication, Feb 1998.

[10] K. Ohta and T. Okamoto, 'Practical extension of Fiat-Shamir scheme', em Eletron. Lett., 1988, bf 24, (15), pp. 955-956

[11] Sangjoon Park, Seungjoo Kim and Dongho Won, 'ID-based group signature', em Electron. Lett., 1997, bf 33, (19), pp.1616-1617.

[12] H. Petersen, 'How to convert any digital signature scheme into a group signature scheme', The Proceedings of Security Protocols Workshop' 97 (to appear).

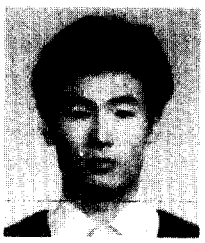
[13] L. R. Rivest, lqlq Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystemrqrq, em Cryptologia, 1978, Vol.2, No. 1,pp. 62-65

[14] M. Stadler, 'Publicly verifiable secret sharing', Advances in Cryptology - EUROCRYPT' 96, LNCS 1070, Springer, 1996, pp.190-199.

[15] 박상준, 원동호, '그룹 식별 정보를 이용한 그룹 서명 방식의 암호 분석', 통신정보보호학회 논문지, 제7권 제2호, 1997년 6월.

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

□ 著者紹介



박 상 준

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

※ 주관심분야 : 암호이론, 인증 및 서명

김 승 주

1994년 2월 성균관대학교 정보공학과(학사)
1996년 2월 성균관대학교 대학원 정보공학과(공학석사)
1996년 3월 - 현재 성균관대학교 대학원 전기·전자 및 컴퓨터공학부 박사과정

원 동 호

1976년 2월 성균관대학교 전자공학과 졸업 (공학사)
1978년 2월 성균관대학교 대학원 전자공학과 졸업 (공학석사)
1988년 2월 성균관대학교 대학원 전자공학과 졸업 (공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경공대 객원연구원
1982년 3월 - 현재 성균관대학교 공과대학 정보공학과 교수
1991년 - 현재 한국통신정보보호학회 편집이사

※ 주관심분야 : 암호이론, 정보이론