ID기반 그룹서명에서의 안전한 개인 서명키 생성기법에 관한 연구1)

김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[kimsh, imylee]@sch.ac.kr

A Study on Creating a Secure Private Signature Key in ID-based Group Signature

Su-Hyun Kim, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

1984년 A.Shamir에 의해 처음 소개된 ID 기반 공개키 암호시스템은 ID나 메일, 주소, 소속 등 유일하게 특정할 수 있는 것을 사용자의 공개키로 사용함으로써 송신자의 공개키에 대한 정당성 확인 과정을 필요 없게 하는 방식으로 전자서명에 적용되어 다양한 방식으로 제안되었다. 하지만 ID 기반 그룹 서명에서는 그룹 관리자만이 사용자의 서명키를 생성하기 때문에 그룹 내 사용자로 위장이 가능한 문제점을 가지고 있다. 본 논문에서는 ID기반 서명에서의 문제점인 키 위탁 문제를 해결할 수 있고, 그룹 관리자만이 부담하고 있는 그룹 구성원들의 개인 서명키 생성 및 사용자 식별 연산을 소그룹 관리자를 이용하여 연산량을 분산시킬 수 있는 그룹 서명 방식을 제안한다.

1. 서론

1984년 A. Shamir은 공개키 암호방식의 단점인 공개키와 개체의 관계 정당성에 대한 확인과정에서 발생하는 큰 부하를 해결하기 위해 ID를 이용한 암호화 방법을 제안하였다[1]. 즉, 개체를 유일하게 특정할 수 있는 ID나 메일, 주소, 소속 등을 공개키로 사용함으로써 다른 사용자들이 공개키를 직접 그 사용자의 ID로부터 생성가능한 방법이다.

ID를 이용한 그룹 서명 방식은 ElGamal 형태의 디지털 서명 방식에 근거한 그룹 서명과는 달리 Ohta-Okamoto 서명 방식과 같은 사용자 개인의 ID에 근거한 서명방식을 사용하여 그룹 서명을 만들게 된다. 따라서, 그룹 서명은 그룹에 속한 그룹 소속원들의 ID 정보에 의하여 검증된다. 위와 같이 ID 기반 암호시스템을 그룹 서명에 적용한다면 그룹 소속원들이 다른 소속원의 공개키를 직접 그 소속원의 신원정보로부터 생성할 수 있으며, 기존 공개키 시스템과 달리 공개키와 사용자를 묶어주는 인증서가 필요하지 않다[2]. 이처럼 ID 기반 암호 시스템은 시스템의 전체적인 복잡도를 낮추며, 공개키 프레임워크의 확립 및 관리와 관련된 비용절감의 효과가 있다[3].

하지만 ID 기반 암호 시스템의 가장 큰 문제점으로 키 위탁문제가 발생 할 수 있다. 각 사용자의 개인 서명키가 그룹 관리자의 마스터 키에 의해 생성되기 때문에 그룹 관리자는 어떤 메시지든 복호화가 가능하며, 또한 어떤 사용자로도 위장이 가능하게 된다. 암호화의 경우 프라이버시를 제한해도 되는 경우에 한해 때때로 유용하게 사용될 수 있지만 서명의 경우 부인방지의 특성을 제공할 수 없게 된다. 이와 같이 키 위탁 문제를 해결할 수 있는 효율적인 ID 기반 암호화 및 서명 알고리즘을 설계하는 연구가 필요하다. 이에 따라 본 연구에서는 키 위탁 문제를 해결하기 위해 사용자가 생성한 난수를 이용하여 그룹 관리자가 추측할 수 없는 계산 값으로 개인 서명키를 생성하는 방법을 제안하였다. 본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 기술들을 소개하고, 3장에서는 그룹 서명이 갖추어야 할 기본적인 보안 요구사항에 대하여 알아보고, 4장에서는 제안 방식에 대하여 설명한다. 5장에서는 제안 방식의 안전성을 분석한고, 마지막으로 6장에서는 결론 및 향후 연구 방향으로 마치도록 한다.

2. 관련연구

본 장에서는 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 기술들을 소개한다.

2.1 그룹 서명

그룹 서명 기법의 개념은 D. Chaum과 van Heyst에 의해 최초로 제안되었다[4]. 그룹 서명 기법은 그룹 소속원의 익명을 보장하며 그룹의 소속인임을 확인하는 방식

※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0022607)

으로 그룹의 가입된 멤버만이 서명을 할 수 있다. 서명자가 누구인지 확인이 필요한 경우, 그룹 관리자는 서명을 개봉하여 서명자를 찾아 낼 수 있다. 이러한 특징들 때문에 그룹 서명 기법은 다양한 분야에서 인증 및 조건부 프라이버시, 부인방지 기능을 제공하는데 적합하다.

일반적으로 그룹 서명 기법은 SETUP, JOIN, SIGN, VERIFY, OPEN과 같은 과정으로 구성되어 있다.

・초기구성(SETUP)

그룹 관리자가 그룹 멤버들이 사용할 그룹 개인키와 그룹 공개키, 그룹 비밀키를 생성하는 과정이다.

・멤버가입(JOIN)

그룹 멤버들이 그룹에 가입하는 과정으로 가입이 완료된 사용자는 그룹 관리자로부터 그룹 서명을 생성할 수 있는 그룹 서명키를 얻게 된다.

・서명(SIGN)

그룹 관리자로부터 얻은 서명키를 이용하여 그룹 서명을 생성한다.

・검증(VERIFY)

그룹 공개키를 이용하여 수신자로부터 제공받은 서명이 정당한 그룹 멤버에 의해 서명된 것인지 확인한다.

・개봉(OPEN)

서명자가 누구인지 확인이 필요한 경우, 그룹 관리자는 그룹 비밀키로 서명을 개봉하여 서명자를 찾아내는 과정이다.

3. 보안 요구 사항

본 제안 방식은 ID기반의 그룹 서명에서 안전한 서명키를 생성하는 기법으로 그룹 관리자와 그룹 멤버 간의 개인 서명키 생성 과정에서 제 3자의 불법적인 공격에 안전해야 한다. 또한 그룹서명이 일반적으로 요구하는 다음의 성질을 만족해야 한다.

・anonymity : 그룹의 서명자는 검증 시 그룹 관리자를 제외한 누구에게도 신원이 노출되지 않아야 한다.

・exculpability : 그룹 멤버가 다른 그룹 멤버의 서명을 대신하여 생성할 수 없어야 한다.

・traceability : 그룹 관리자 비밀키에 의해 서명으로부터 서명의 신원추적이 가능해야 한다.

・framing : 그룹 멤버들의 결탁에 의해 임의의 멤버의 서명을 생성할 수 없어야 한다.

・unlinkability : 각기 다른 메시지와 서명 쌍이 주어져도 동일한 그룹 소속원에 의한 서명인지 알 수 없어야 한다.

4. 제안방식

본 장에서는 ID기반 서명에서의 문제점인 키 위탁 문제를 해결할 수 있고, 그룹 관리자 (GA : Group Authority)만이 부담하고 있는 그룹 구성원들의 개인 서명키 생성 및 사용자 식별 연산을 소그룹 관리자 (SGA : Small Group Authority)를 이용하여 연산량을 분산시킬 수 있는 그룹 서명 방식을 제안한다. ID를 이용한 그룹서명 방식에서는 ID에 근거한 서명 방식인 Ohta-Okamoto 방식과 Stadler의 검증 방식을 기반으로 만들어진다[5][6].

4.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템 계수를 사용하여 프로토콜을 설계한다.

・ $*$: 참여 객체 (GA : 그룹 관리자, SGA : 소그룹 관리자, i : i 번째 그룹 구성원)
・ K_G : 그룹 구성원 식별자 리스트
・ K_S : 그룹 구성원 비밀키 리스트
・ ID_* : $*$의 식별자
・ S_* : $*$의 개인 서명키
・ p : 소수 ≥ 512bit
・ q : 소수 ≥ 160bit ($q \mid p-1$)
・ d_* : $*$의 비밀정보
・ e_* : $*$의 공개정보
・ ID_*^{x*} : $*$번째 가입자의 비밀키
・ k_*, a_*, x_* : $*$가 생성한 임의의 난수
・ r,c : 개인 서명값
・ A,B : 그룹 서명값
・ *H()* : 일방향 해쉬 함수

4.2 그룹 가입 및 소그룹 관리자 권한 부여 단계

그룹 가입은 그룹 관리자가 관할하며, 그룹에 등록하여 소그룹으로 배정하기 위해서는 다음과 같은 과정을 거친다. 그룹 관리자는 소그룹 크기를 m으로 가정하였을 경우 mn+1번 째 사용자에게 소그룹 관리자 권한을 부여하게 된다.

소그룹 관리자 권한을 부여받은 사용자는 추후에 가입될 m명의 사용자에 대해 개인 서명키 생성 및 그룹 서명에 대해 사용자 식별을 할 수 있는 권한을 가지게 된다.

Step 1: 그룹에 등록하고자 하는 사용자는 자신의 식별정보를 GA에게 제공한다.

ID_i

Step 2: 그룹 관리자는 사용자의 식별정보를 확인 후에 K_G에 차례대로 저장하고, mn+1번 째에 해당하는 사용자에게는 소그룹 관리자의 권한을 부여하게 된다.

그룹 관리자는 사용자의 식별정보를 다음과 같이 등록한다.

$K_G=\{ID_1, ID_2, ID_3, \cdots, ID_k\}$

4.3 개인 서명키 분배 단계

본 단계에서는 키 위탁 문제 해결을 위해 그룹 관리자

자체에서의 개인 서명키 생성을 제한함으로써 키 위탁 문제를 해결하였다. 사용자의 개인 서명키 요청 시 사용자가 생성한 난수를 이용하여 그룹 관리자가 추측할 수 없는 계산 값을 사용하게 된다.

소그룹 관리자는 그룹 관리자와 개인 서명키를 생성하게 되고, 그 외 사용자의 경우 소그룹 관리자와 함께 개인 서명키를 생성 하게 된다. 각 사용자는 그룹에 등록하여 개인 서명키를 분배받기 위해서 아래와 같은 과정을 거친다.

Step 1: 그룹 관리자와 소그룹 관리자는 시스템을 구성하기 위해 아래와 같이 각 정보를 구성한다.

- $n=p \cdot q$, $e \cdot d=1 (\mathrm{mod}\ \varnothing(n))$
- 공개 정보 : n, e
- 비밀 정보 : p, q, d
- 그룹 공개키 : ID_{GA}
- 그룹 서명키 : $y=g^{IDGA}$

Step 2: 그룹에 가입하고자 하는 구성원은 최초 등록 요청 메시지를 자신의 식별자를 이용하여 그룹 관리자에게 전송하게 된다. 그룹 관리자는 구성원의 소그룹 관리자 자격요건을 판단 후, 소그룹 관리자일 경우 개인 서명키 생성 과정에 참여하게 된다. 개인 서명키를 생성하기 위해서 사용자는 랜덤 수 x를 선택하여 그룹 관리자의 공개정보를 이용하여 아래와 같이 계산 후 그룹 관리자에게 전송한다.

$(IDi^{xi})^{e_{GA}}$

Step 3: 그룹 관리자는 사용자로부터 받은 값을 아래와 같이 계산하여, 구성원 식별자에 대응하는 비밀키 리스트를 저장한다. 그룹 구성원의 비밀키 리스트는 소그룹 관리자 간에 서로 공유하게 된다.

$((IDi^{xi})^{e_{GA}})^{d_{GA}} = IDi^{xi}$

$K_S=\{ID_1^{x1}, ID_2^{x2} \cdot \cdot \cdot ID_k^{xk}\}$

Step 4: 그룹 구성원의 비밀키를 받은 그룹 관리자는 그룹 공개키의 해쉬값과 같이 연산하여 i번째 구성원의 개인 서명키를 생성하게 된다. 서명키를 생성한 그룹 관리자는 자신이 연산한 값을 구성원에게 보내줌으로써 구성원 또한 그룹 관리자가 생성한 개인 서명키와 동일한 서명키를 생성하게 된다.

$t=h(ID_{GA})$

$Si=t^{d_{GA}} \cdot IDi^{xi}$

Step 5: 그룹 관리자가 서명키 생성 요청을 받을 시, 요청 사용자가 소그룹 관리자가 아닐 경우 가입 요청자에 가장 근접한 소그룹 관리자에게 가입 요청자의 식별자를 전송해 주게 된다. 식별자를 전달 받은 소그룹 관리자는 위와 같은 과정을 거쳐 사용자로부터 전달받은 값을 이용해 그룹 관리자와 마찬가지로 사용자의 서명키 생성에 참여하게 된다.

4.4 그룹 서명 및 검증 단계

서명자 i는 자신의 비밀키 Si를 사용하여 일반적인 형태의 ID 기반 디지털 서명 (r,c)를 계산한다. 이때, ID에 근거한 서명 방식인 Ohta-Okamoto 프로토콜을 기반으로 생성하며, 검증 시에 Stadler 방식을 기반으로 증명한다.

Step1 : 서명자는 다음과 같은 과정으로 일반 서명과 그룹 서명 과정을 수행한다.

- 그룹 구성원이 속해 있는 소그룹 관리자의 공개정보 e와 난수 k를 이용하여, 다음과 같은 디지털 서명 (r,c)를 생성한다.

  $r = k_i^{e1} \ (\mathrm{mod}\ n),\quad c = S_i^{h(M,r)} \cdot k \ (\mathrm{mod}\ n)$

- 서명 c를 그룹 서명키 y로 그룹 서명을 한다.

  $A = g^a \ (\mathrm{mod}\ n),\quad B = c \cdot y^a \ (\mathrm{mod}\ n)$

- 서명 수신자에게 (M,r,c,A,B)를 전송한다.

Step 2: 메시지를 받은 수신자는 그룹 공개키 ID_G를 사용하여 그룹 서명을 다음과 같이 검증한다.

$c' = B / A^{IDG}$

$c \stackrel{?}{=} c'$

4.5 신분 확인 과정

서명 수신자와 그룹 서명자 간의 메시지 M에 대한 분쟁이 발생하는 경우 소그룹 관리자는 서명 수신자가 가지고 있는 그룹 서명으로부터 서명자의 신원을 확인 할 수 있다. 소그룹 관리자의 비밀정보로 소그룹 내 서명자의 개인 서명키를 생성하였기 때문에 검증 시에 소그룹 관리자의 공개정보를 필요로 하게 된다.

신분 확인 과정은 서명 수신자로부터 받은 (r,c)를 통해 다음 수식을 만족한다면 이 서명에 해당하는 ID_i^{xi}를 찾아 비밀키 리스트와 식별자 리스트를 비교하여 찾을 수 있다.

- $c^{ei} \stackrel{?}{=} t \cdot ID_i^{xi \cdot ei \cdot h(M,r)} \cdot r \ (\mathrm{mod}\ n)$

5. 제안방식 분석

본 장에서는 개인 서명키 생성 과정에서 발생할 수 있는 제 3자의 불법적인 공격인 중간자 공격 및 도청 공격에 대해 다음과 같이 안전성 분석을 한다[7].

5.1 중간자 공격 (Man-In-The-Middle Attack)

공격자가 그룹 관리자와 그룹 구성원 사이에서 DH 키 교환의 문제점인 중간자 공격을 시도할 수 있다. 공격자는 가입을 원하는 사용자의 서명키 생성 요청 메시지의 공개

값 ID_i를 저장하고 ID_i'를 생성하여 그룹 관리자에게 전송하고, 그룹 관리자의 응답 메시지의 DH 공개값 역시 저장 및 생성하여 그룹 구성원에게 전송함으로써 각 구성원들과의 비밀 통신 세션을 생성할 수 있다. 그러나 제안 기법은 구성원들과 그룹 관리자 사이에서 교환되는 DH 공개값이 상호인증을 통해 이루어지기 때문에 공격자는 중간자 공격을 수행할 수 없다.

5.2 도청 공격 (Eavesdropping Attack)

공격자는 그룹 관리자와 그룹 구성원 간에 전송되는 메시지를 도청하고, 서명키를 계산하여 신분을 위장하려고 시도할 수 있다. 하지만, 제안 기법은 안전하게 서명키를 전송하기 위해서 서명키 자체를 통신로 상에 노출 시키지 않고 DH 키 교환 방식을 이용하여 각자 계산하게 된다. 이 과정에서 교환되는 메시지는 DH 파라미터 g^c에서 c를 알 수 없다는 DLP(Discrete Logarithm Problem) 성질을 가진다. 따라서 공격자는 도청 공격을 통해 획득한 메시지로 서명키를 생성할 수 없고, 서명키로 생성된 서명자의 메시지를 통해 식별자를 추출해 낼 수 없게 된다.

6. 결론 및 향후 연구 방향

본 논문에서는 기존의 ID기반 그룹서명 방식들의 문제점을 분석하고, 그룹 관리자의 연산 부담을 개선한 그룹 서명 방식을 제안하였다. 기존 ID기반 서명 방식에서는 그룹 관리자가 생성하는 개인 서명키를 사용함으로써 그룹 관리자가 어떤 메시지든 복호화 가능 할 뿐만 아니라, 어떤 사용자로도 위장이 가능한 문제를 볼 수 있었다. 이러한 키 위탁 문제를 해결하기 위해 본 논문에서는 개인 서명키 생성 시 사용자가 생성한 난수를 이용하여 그룹 관리자가 추측할 수 없는 계산 값을 생성하는 방법을 사용하였다. 이처럼 그룹 관리자 자체에서의 개인 서명키 생성을 제한함으로써 키 위탁 문제를 해결 할 수 있다.

본 논문에서 제안한 개인 서명키 생성 방식은 기존 그룹서명에서의 개인 서명키 생성방식 보다 연산량이 많다는 단점이 있지만, 그룹 내에 일정한 구성원으로 이루어진 소그룹을 생성함으로써 그룹 관리자가 부담하던 연산을 분산 시킬 수 있다. n명의 그룹 구성원을 가지는 그룹 관리자의 경우 개인 서명키 생성과 신분 검증 과정에서 n번의 연산을 그룹 관리자만이 부담하게 된다. 하지만 본 논문에서 제안하는 소그룹 관리자를 사용함으로써 기존 그룹관리자에게 집중되었던 연산을 1/n만큼 분산시켜 보다 효율적인 그룹 서명 방식을 제안하고 있다. 또한 서명키 생성 과정에서 매번 다른 DH 파라미터들을 생성함으로써 보다 안전한 개인 서명키 교환이 가능하다는 장점을 갖고 있다.

하지만 그룹 구성원의 탈퇴 시 남은 그룹 구성원들의 그룹 공개키 및 그룹 서명키의 변경은 불가피하므로 이에 따른 많은 연산을 해결 할 수 있는 방법에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] A. Shamir, “Identity-based cryptosystems and signature schemes,” Proc. of Crypto’84, LNCS 196, pp. 47-53, 1984.

[2] 박상준, 김승주, 원동호, "ID를 이용한 그룹 서명과 안전성", 한국정보보호학회논문지, Volume 8. Issue 3, pp.27~27 ,1998

[3] 김광조, 김진, 여운동, “ID 기반 암호시스템,” 2005 tech-issue energing s&t report, KISTI, 한국과학기술정보연구원, 2005.

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

[5] K. Ohta and T. Okamoto, "Practical Extension of Fiat-Shamir scheme", emEletron. Lett., 1988, bf 24, (15), pp.955-956.

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

[7] J. Cha and J. H. Cheon. "An Identity-Based Signature from Gap Diffie-Hellman Groups", PCK 2003, LNCS 2567, pp.18-30, 2003.