情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

그룹 서명 기법에서 수정된 Linear Encryption을 기반으로 하는 지역 연결성에 대한 연구*

강 전 일,[1†] 김 기 태,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

Study of Local Linkability based on Modified Linear Encryption in Group Signature Schemes*

Jeonil Kang,[1†] Kitae Kim,[1] DaeHun Nyang,[1] KyungHee Lee[2‡]
[1]INHA University, [2]The University of Suwon

요 약

그룹 서명 기법은 서명자의 익명성을 제공하기 위해서 만들어졌지만, 연산 및 공간(서명 길이) 효율성이 높지 않을 뿐만 아니라 복잡한 구성, 제한된 사용자 관리 등으로 인하여 실제 응용 가능성은 많지 않았다. 강전일, 황정연 등은 이러한 이유에서 그룹 서명 기법을 실제로 이용하기 더 쉽도록 지역 연결성을 도입하는 연구를 진행하였다. 이 논문에서는 기존의 연구에서 수행하지 못했던 지역 연결성에 대한 구체적인 성질을 파악하고, 지역 연결성을 갖는 특별한 사용자(개체)에 대한 보안성의 형식적인 증명을 시도하였다.

ABSTRACT

Group signature schemes were made for serving anonymities of signers, but the group signature schemes have been seldomly adapted to the real-world applications because of their low computation and space (i.e. signature length) efficiency, complicated construction, limited user management, and so on. Kang, Hwang, etc. performed the study about the local linkability that is for helping group signature schemes to be adapted more easily to the real world. In this paper, we investigate the nature of local linkability, which did not deal with well in the previous studies, in detail and perform the formal proof for the security of special entities who hold the local linkability.

Keywords: group signature, local linkability, linear encryption

I. 서 론

그룹 서명(group signature) 기법은 서명자의 익명성을 제공하는 서명 디지털 서명 기법 중에 하나이다[1]. 그룹 서명의 개념이 소개된 이후로 20여 년 동안 꾸준히 연구가 진행 되었으며 몇 차례의 기술의 큰 전환을 거치며 효율성 측면에서 장족의 발전을 이루었다. 그러나 현재 그룹 서명 기법은 다른 많은 암호학적 구성요소(cryptography primitive)와 마찬가지로, 실제로 우리의 환경에 적절히 사용되지는 못하고 있다. 그럼에도 불구하고 그룹 서명 기법을 이용하기 위한 연구는 현재까지도 꾸준히 이루어지고 있으며, 앞으로의 연구 필요성에도 이론은 없을 것이다.

접수일(2012년 4월 16일), 수정일(2012년 8월 1일), 게재확정일(2012년 8월 20일)
* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었습니다 (2012-0002146).
† 주저자, dreamx@isrl.kr
‡ 교신저자, khlee@suwon.ac.kr

그룹 서명 기법의 이용에 관련된 많은 연구들은 주로 응용환경을 찾아서 기존의 그룹 서명 기법을 거의 그대로 적용하는 방식이 많다. Lin 등은 2007년에 VLR(verifier-local revocation) 그룹 서명 기법을 VANET(vehicle ad-hoc network)에 적용하여 차량들이 메시지를 보낼 때 익명으로 서명된 메시지를 보내는 프로토콜을 제안하였다[2]. Wu 등은 2010년에 일괄 검증(batch verification) 그룹 서명 기법을 차량 대 차량(vehicle-to-vehicle, V2V) 통신에 적용하는 방법을 제안하였다[3]. Balasch 등은 2010년에 그룹 서명 기법을 이용하여 이용자의 익명성을 제공하면서 도로 이용에 따른 과금 시스템을 제안하였다[4]. Ren 등은 2010년에 그룹 서명 기법을 메시 네트워크에 적용하여, 익명 사용자가 라우터 등과 통신할 수 있는 시스템에 대해서 연구하였다[5]. 이러한 기법들에서 그룹 서명 기법은 원래 그룹 서명 기법을 거의 변형하지 않을 뿐만 아니라, 겹선형 접합(bilinear pairing)을 이용하는 Boneh 등의 짧은 그룹 서명 기법[6]과 Boneh와 Shacham이 2004년 제안하였던 그룹 서명 기법[7] 같은 기법을 주로 사용한다.

하지만 그룹 서명 기법을 실제로 응용하여 사용하였을 때, 발생할 수 있는 잠재적인 문제들은 기존의 연구들이 실제로 사용 가능할까 하는 의문을 남긴다. 누가 신뢰할 수 있는 제3자(trusted third party, TTP)가 되고 서비스 제공자의 권한을 정하는 기초적인 문제부터, 잘못된 행위를 하는 사용자 퇴출이나, 특정 사용자 추적에 이르는 다양한 문제들은 그룹 서명 기법 자체만 가지고는 잘 해결되지 않는다. 추적 가능 서명(traceable signature) 기법[8]은 그룹 서명이 갖는 비실용성을 극복하고자 하는 한 시도라고 볼 수 있을 것이다.

강전일 등과 황정연 등은 이와 비슷한 맥락에서 Boneh 등의 짧은 그룹 서명 기법[6]에 지역 연결성(local linkability)이라는 개념을 도입함으로써, 그룹 서명 기법을 조금 더 유연성 있게 사용하고자 했다[9,10]. 지역 연결성이란 '시간과 공간적인 지역'에서 '익명 취소 관리자에 의해서 제어되는 연결성'을 의미한다고 볼 수 있다. 강전일 등은 자신들의 논문[9]에서 지역 연결성의 개념을 도입하면서 이를 지원하기 위한 두 가지 추가적인 방법을 제안하였지만, 지역 연결성을 갖는 서비스 제공자에 대한 보안성 분석은 결여되어 있다. 황정연 등은 겹선형 접합의 두 덧셈 그룹을 다르게 사용함으로써, 효율성을 높이는 시도를 하였다[10]. 이 두 연구에 있어서 저자들은 지역 연결성이 갖는 특성과 개념에 대해서는 구체적으로 설명하고 있지 않으며, 기법마다 조금씩 다르게 보이는 '제어되는 연결성'을 가지고 있어 그 개념이 혼란스럽다. 이 논문에서는 지역 연결성에 대한 구체적 개념 정립 이외에 다음과 같은 내용을 연구 하였다.

〔표 1〕 논문에서 사용되는 기호

기호 이름	예시	설명
겹선 대문자	$\mathbb{A}$	집합 $\mathbb{A}$ (그룹 또는 체)
왼쪽 화살표	$a \leftarrow b$	값 b를 값 a에 할당
오른쪽 화살표	$f : \mathbb{A} \rightarrow \mathbb{B}$	어떠한 함수 또는 매핑 f는 집합 $\mathbb{A}$에 속한 원소의 입력으로부터 집합 $\mathbb{B}$에 속한 출력을 가짐
물결 표시	$\mathbb{A} \sim B$	집합 $\mathbb{A}$이 어떤 구조체 B위에 존재함
원소 속함	$a \in \mathbb{B}$	집합 $\mathbb{B}$에 원소 a가 속함
양꺾괄호	$\mathbb{B} = \langle a \rangle$	a는 집합 $\mathbb{B}$의 모든 원소를 생성함
소문자 기호	a, δ	숫자 변수(값)
대문자 기호	A, Δ	덧셈 순환군 위의 한 점(값)
괄호가 있는 대소문자 기호의 연속	$a()$, $A()$	맵핑 또는 함수

지역 연결성이 필요한 이유와 더불어 지역 연결성의 개념에 대해서 설명한다. 그러한 개념에 근거하여 지역 연결성이 갖는 특성에 대해서 구체적으로 설명한다.

지역 연결성을 갖는 특수 사용자의 관점에서의 보안성(익명성)에 대한 형식적 증명(formal proof)을 시도한다.

이 논문은 II장에서 이 연구를 이해하는 데 필요한 내용에 대해서 기술하였다. 겹선형 접합과 관련된 DH 문제와 $O(1)$ 그룹 서명 기법, 그리고 LE(Linear Encryption) 기법에 대한 내용을 포함한다. III장에서 강전일 등과 황정연 등에 의해서 기술되었던 내용[9,10]을 바탕으로 지역 연결성을 갖는 그룹 서명 기법에 대해서 정리하고, 구체적인 성질에 대해서 기술하였다. IV장에서 이러한 지역 연결성이 갖는 보안성의 형식적 증명에 대해서 서술하고, 이와 관련된 문제점에 대해서 설명한다. V장은 결론으로 이 논문을 마무리 한다.

II. 일러두기

2.1. 사용 기호

이 논문에서는 대부분의 경우에 있어서, 광범위하

게 사용되는 수학 표기를 따르고 있다. 특별하게는 〔표 1〕 같은 일관된 형태의 기술을 가지고 있다. 각각 소문자 및 대문자 기호로 이루어진 변수의 경우 해당 부분에서 다시 설명한다.

2.2. 겹선형 접합(bilinear pairing)과 DH 문제

겹선형 접합(bilinear pairing) $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_T$는 두 덧셈 순환군(additive cyclic group) $\mathbb{G}_1$과 $\mathbb{G}_2$ 위의 각각 한 원소로부터 한 곱셈 순환군(multiplicative cyclic group) $\mathbb{G}_T$의 한 원소를 구하는 맵(map)이다. 일반적으로 덧셈 순환군은 타원 곡선 위에서 정의되고, 곱셈 순환군은 유한한 정수 위에서 정의된다. 일반적으로 $\mathbb{G}_2$의 (x,y)좌표는 $\mathbb{G}_1$의 (x,y) 좌표를 정의하는 유한체(finite field) $\mathbb{F}$를 이용한 확장 필드(extension field)에서 정의된다. ($\mathbb{G}_1 \sim E(\mathbb{F}_q)$, $\mathbb{G}_2 \sim E(\mathbb{F}_{q^k})$)

- 겹선형성(bilinearity): 모든 $P\in\mathbb{G}_1$, $Q\in\mathbb{G}_2$와 $(a,b)\in\mathbb{Z}^2$에 대해서, $e(aP,bQ)=e(P,Q)^{ab}$이다.
- 비퇴보성(non-degeneracy): 만약 $\mathbb{G}_1=\langle P\rangle$, $\mathbb{G}_2=\langle Q\rangle$이고, 모든 $X\in\mathbb{G}_1$, $Y\in\mathbb{G}_2$에 대해서 $e(P,Y)\neq 1_{\mathbb{G}_T}$, $e(X,Q)\neq 1_{\mathbb{G}_T}$이다. ($1_{\mathbb{G}_T}$는 $\mathbb{G}_T$의 항등원이다.)
- 계산의 용이성(computable): 모든 $P\in\mathbb{G}_1$, $Q\in\mathbb{G}_2$에 대해서, $e(P,Q)$는 쉽게 계산될 수 있다.

겹선형성으로부터 다음과 같은 $\mathbb{G}_1$위의 두 점 $R_1=aP$, $R_2=bP$를 가정함으로써 다음과 같은 성질을 얻을 수 있다. 여기서 P는 $\mathbb{G}_1$의 기준점(base point)이다.

$$\begin{aligned} &e(R_1+R_2,Q)=e(aP+bP,Q)\\ &=e((a+b)P,Q)=e(P,Q)^{a+b}\\ &=e(P,Q)^a\cdot e(P,Q)^b=e(aP,Q)\cdot e(bP,Q)\\ &=e(R_1,Q)\cdot e(R_2,Q)\end{aligned} \quad (1)$$

같은 이유에서 $\mathbb{G}_2$위의 두 점 R_3과 R_4에 대해서도 다음과 같이 동일한 성질을 갖는다.

$$e(P,R_3+R_4)=e(P,R_3)\cdot e(P,R_4) \quad (2)$$

비퇴보성은 그룹 $\mathbb{G}_1$과 $\mathbb{G}_2$위의 임의의 두 점에 대한 연산 결과가 그룹 $\mathbb{G}_T$의 항등원이 되면 안 된다는 것이다. 그룹 위의 모든 점은 기준점의 반복으로 표현될 수 있고 —예를 들면, $X=aP$, $Y=bQ$— 겹선형성의 성질 때문에 모든 겹선형 접합의 연산 결과는 $e(P,Q)$의 제곱으로 표현된다. 만약, $e(P,Q)$이 그룹 $\mathbb{G}_T$의 항등원으로 표현되면 겹선형 접합이 그룹 $\mathbb{G}_1$과 $\mathbb{G}_2$의 DLP(Discrete Logarithm Problem)와 관련된 그룹 동형 $\mathrm{Dlog}_P(X):\mathbb{G}_1\rightarrow\mathbb{Z}/n\mathbb{Z}$와 $\mathrm{Dlog}_Q(Y):\mathbb{G}_2\rightarrow\mathbb{Z}/n\mathbb{Z}$에 대해 어떠한 정보도 줄 수 없기 때문에 연산은 퇴보(degeneracy)하게 된다. (여기서, $\mathbb{G}_1$의 항등원 O_1와 $\mathbb{G}_2$의 항등원 O_2에 대해서, $nP=O_1$, $nQ=O_2$이다.) 이는 겹선형 접합이 덧셈 순환군 $\mathbb{G}_1$이나 $\mathbb{G}_2$에서의 DLP를 곱셈 순환군 $\mathbb{G}_T$의 문제로 변환하기 위해서 고안되었음을 생각하면 겹선형 접합이 가져야만 하는 당연한 속성이다.

겹선형 접합과 관련하여 암호학적 안전성은 DDH(Decisional Diffie-Hellman) 문제와 크게 연관되어 있다. 만약 $\mathbb{G}_1=\mathbb{G}_2$라면, $\mathbb{G}_1$(또는 $\mathbb{G}_2$)에서의 DDH는 어렵지 않다. $\mathbb{G}_1$에서의 DDH 문제가 (P,xP,yP,zP)와 같이 주어졌다면, $e(P,zP)=e(xP,yP)$인지 확인함으로써, $z=xy$인지 검증할 수 있다. 이러한 그룹 $\mathbb{G}_1$을 GDH(Gap DH) 그룹이라고 한다. GDH 그룹은 CDH(Computational DH) 문제는 어렵지만, DDH 문제는 쉬운 그룹을 의미한다. 일반적으로, 겹선형 접합과 관련된 DDH 문제의 어려움은 $\mathbb{G}_1$과 $\mathbb{G}_2$ 사이의 그룹 동형(group isomorphism)을 계산하는 효율적 알고리즘의 존재 유무에 따라 결정된다. 두 그룹 사이의 그룹 동형을 $\psi_1:\mathbb{G}_2\rightarrow\mathbb{G}_1$와 $\psi_2:\mathbb{G}_1\rightarrow\mathbb{G}_2$라고 할 때, 그룹 동형을 계산하는 효율적 알고리즘의 존재 유무는 세 가지가 나뉠 수 있으며[1] DDH가 어려워지는 그룹은 이에 따라 달라진다. 예를 들어, ψ_1이 있고, ψ_2가 없으면, $\mathbb{G}_1$에서의 DDH 문제는 어려워지지만, $\mathbb{G}_2$에서의 DDH 문제는 어렵지 않다. 이 경우 $\mathbb{G}_1$에서의 DDH 문제 (P,xP,yP,zP)에 대해서 $e(P,zP)$와 $e(xP,yP)$의 연산 자체가 성립되지 않지만, $\mathbb{G}_2$에서의 DDH 문제 (Q,xQ,yQ,zQ)에 대해서는 $e(\psi_1(Q),zQ)=e(\psi_1(xQ),yQ)$를 확인함으로써 $z=xy$인지 검증할 수 있다. 이러한 그룹 동형의 존재와 DDH 문제의 어려움 사이의 연관 관계는 〔표 2〕에서 확인할 수 있다.

1) ψ_1이 비효율적이고 ψ_2가 효율적인 경우는, ψ_1와 ψ_2를 바꿔서 사용하는 경우에 ψ_1이 효율적이고 ψ_2가 비효율적인 경우와 동일하다.

〔표 2〕 그룹 동형과 DDH 문제의 연관 관계
(* = GDH 그룹)

그룹 동형을 계산하는 효율적 알고리즘의 존재 유무		DDH 문제의 어려움		비고
$\psi_1 : \mathbb{G}_2 \rightarrow \mathbb{G}_1$	$\psi_2 : \mathbb{G}_1 \rightarrow \mathbb{G}_2$	$\mathbb{G}_1$	$\mathbb{G}_2$	
○	○	쉬움*	쉬움*	
○	×	어려움	쉬움*	XDH
×	×	어려움	어려움	SXDH

XDH(eXternal DH)[11]나 SXDH(Symmetric eXternal DH)[12] 가정은 겹선형 접합과 관련된 그룹에서의 DDH 문제를 명시적으로 제한하는 가정이다. XDH 가정은 $\mathbb{G}_1$에서의 DDH 문제가 어렵다는 것이다. 이는 곧, 그룹 동형 $\psi_2 : \mathbb{G}_1 \rightarrow \mathbb{G}_2$이 존재하지 않는다고 명시적으로 선언한 것과 동일하다. SXDH 가정은 여기에 더 나아가 $\mathbb{G}_1$과 $\mathbb{G}_2$에서의 DDH 문제가 어렵다는 것이고, 그룹 동형 ψ_1과 ψ_2이 모두 존재하지 않는다는 것을 명시적으로 선언한 것이다. 당연하게도 이러한 가정은 모두 그에 적합한 순환군 $\mathbb{G}_1$와 $\mathbb{G}_2$을 사용해야만 성립될 수 있다.

한편, 표준 모델(standard model)에서, DLP 또는 DH 문제군(problem family)을 기반으로 하여 만들어진 암호화(encryption) 기법들의 경우, 제한된 자원을 가진 공격자(computationally -bounded adversary)에 대해서 IND-CPA (Indistinguishability under Chosen Plaintext Attack, SS(semantic security)와 동일) 또는 IND-CCA (Indistinguishability under Chosen Ciphertext Attack) 안전하기 위해서 일반적으로는 DDH 문제가 어려워야 한다. 예를 들어, ElGamal 암호화 기법은 DDH 문제가 어려울 때, IND-CPA 안전하지만, 그렇지 않고 CDH 문제만 어렵다면, 단지 OW-CPA (One-wayness under CPA) 안전할 뿐이다.

따라서 XDH나 SXDH 가정은 겹선형 접합을 사용하는 암호화 기법이 IND-CPA 안전성을 보장하기 위해서 해당 암호화 기법에 사용해야 하는 덧셈 그룹 $\mathbb{G}_1$과 $\mathbb{G}_2$의 종류를 제한하는 방법이라고 볼 수 있다. 익히 알려진 것처럼, 표준 모델에서 IND-CPA 안전한 암호화 기법은 해시 함수를 이용하여 ROM (Random Oracle Model)에서 IND-CCA2(IND under adaptive CCA) 안전한 암호화 기법으로 만들 수 있다[13].

2.3. $O(1)$ 그룹 서명 기법

Chaum이 최초로 제안한 그룹 서명(group signature) 기법은 그룹에 속한 정직한 서명자의 익명성을 보장하는 서명 기법이다[1]. 그룹 서명에는 그룹에 속한 사용자들 이외에, 그룹과 사용자들의 익명성을 관리하는 멤버십 관리자(membership manager, 또는 issuer)와 익명취소 관리자(revocation manager, 또는 opener)가 존재한다. 그룹 서명 기법은 때때로 멤버십 관리자와 익명취소 관리자를 신뢰할 수 있는 그룹 관리자(group manager) 하나로 가정하기도 한다[14]. 멤버십 관리자와 익명취소 관리자를 신뢰할 할 수 없는 조금 더 일반적인 환경에서의 그룹 서명 기법에서 다음과 같은 구성을 갖는다[15].

- $(gpk, gik, gok) \leftarrow$ GKeyGen() : 그룹 공개키 gpk, 멤버십 인증서 발행키 gik, 그룹 익명 철폐키 gok를 생성한다.
- $gsk[i] \leftarrow$ Join/Iss$(gpk, gik, [i])$: 멤버십 관리자는 i번째 그룹 구성원의 그룹 서명키(=멤버십 인증서) $gsk[i]$를 생성한다.
- $\sigma \leftarrow$ GSign$(gpk, gsk[i], m)$: 사용자는 그룹 서명키 $gsk[i]$를 이용하여 메시지 m의 그룹 서명 σ를 생성한다.
- $0/1 \leftarrow$ GVerify(gpk, m, σ) : 그룹 서명 σ의 유효성을 확인한다. 이는 그룹 공개키 gpk를 알고 있는 누구나 가능하다.
- $(A, \pi) \leftarrow$ Open(gpk, gok, m, σ) : 익명취소 관리자는 그룹 익명 철폐키 gok를 이용하여 유효한 서명 σ로부터 사용자의 식별자 A의 계산 과정이 올바르다는 증거 π를 구한다.
- $0/1 \leftarrow$ Judge(gpk, m, σ, A, π) : 철폐 증거 π에 대한 유효성을 확인한다.

그룹 서명 기법에 따라 Open의 결과가 바로 서명자의 식별자 A인 경우가 있다. 이런 그룹 서명 기법을 '$O(1)$ 그룹 서명 기법'이라고 한다. 예를 들어, Boneh, Ateniese, Delerablée, Makita 등이 각각 제안하였던 그룹 서명 기법들[6,16,17,18] 등이 여기에 속한다. 반면, 어떠한 그룹 서명 기법에서는 Open의 결과로 얻은 정보를 이용하여 그룹 구성원에 관련한 데이터베이스를 검색한 뒤에야 서명자를 특정할 수 있는 경우도 있다. —여기서 n은 그룹에 속한 그룹의 구성원의 수를 의미한다.— 이러한 그룹 서명 기법을 '$O(n)$ 그룹 서명 기법'이라고 하며, Boyen과 Waters

가 제안하였던 그룹 서명 기법들[19, 20] 등이 이에 속한다.

이 논문에서 주로 관심 있는 $O(1)$ 그룹 서명 기법은 정형화된 단계들을 거쳐 그룹 서명이 구성되는 것이 일반적이다[21]. 발행자는 Join/Issue 단계에서 사용자에게 사용자 고유의 식별자 A를 할당한다. 이때 식별자 A는 발행자가 사용자에게 무작위로 선택하여 할당하는 고유한 수 x의 서명인 경우가 많다. 그룹 서명키가 때때로 멤버십 인증서(membership certificate)라고 불리는 이유이기도 하다. 최종적으로 무작위수 x와 식별자 A 이외에 몇 개의 추가적인 정보가 그룹 서명키가 된다. 서명자는 이 그룹 서명키를 이용하여 서명을 생성한다. 여기서 그룹 서명은 사용자의 식별자의 암호문을 포함하는 그룹 서명키의 NIZK(Non-Interactive Zero-Knowledge proof)가 된다. 또한, 서명자의 식별자를 구함으로써 서명자의 익명성을 철폐하는 Open 절차는 식별자의 암호문을 복호화하는 절차와 동일하다. 이러한 구성을 가진 $O(1)$ 그룹 서명 기법은 당연하게도 식별자를 암호화하기 위해서 사용하는 암호화 기법이 그룹 서명의 익명성(anonymity)에 직접적으로 영향을 주게 된다. 따라서 식별자의 암호화에는 더 강력한 공격자에게 안전한 암호화 기법이 사용될 필요가 있다.

많은 $O(1)$ 그룹 서명 기법들은 그룹 서명키의 발급에 사용되는 그룹 공개키와 사용자의 식별자를 암호화하기 위해서 사용되는 그룹 공개키 사이에 별다른 연관성을 가지고 있지 않다. 이를 이용하면, 전체 그룹에서 부분 그룹을 만들어 사용할 수 있다. 그룹의 일원은 동일한 그룹 서명키를 이용하여 서로 다른 부분 그룹을 위한 그룹 서명 기법을 생성할 수 있다. 이는 복수의 익명취소 관리자가 동시에 존재할 수 있다는 의미와 같다. 이와 관련된 자세한 내용은 III 장에서 다루기로 한다.

2.4. Linear Encryption 기법

그룹 서명 기법의 지나치게 긴 서명의 길이는 오랜 시간 동안 문제점으로 지적되어 왔다. 초기 그룹 서명 기법의 경우, 서명의 길이는 그룹 크기에 비례했었다. 이러한 초기의 그룹 서명 기법은 사용자의 공개키를 등록하여 사용함으로써, 서명 권한의 철폐(revocation)를 쉽게 구현할 수 있었지만, 그룹에 속한 사용자들이 매우 많은 경우 서명 자체가 비효율적일 수밖에 없다. 예를 들어, Camenisch가 1997년 제안하였던 그룹 서명 기법[22]이 여기에 속한다. 반면, 사용자들에게 그룹 서명키를 발급하는 방식의 경우 그룹의 크기와 상관없이 일정한 길이를 서명으로 갖지만, 서명 권한의 철폐 절차가 복잡한 단점이 있다. 1990년대 후반에 만들어진 대부분의 그룹 서명 기법이 여기에 속한다. 그럼에도 불구하고 이러한 인증서 발급 방식의 그룹 서명 기법도 서명의 길이는 수 KByte에 이른다. 예를 들어, Camenisch와 Stadler가 1997년에 제안하였던 그룹 서명 기법[21]의 경우 약 1.4-KByte이며, Camenisch와 Michels가 2000년에 제안하였던 그룹 서명 기법[23]의 경우 약 1-KByte 정도이다. 또한 Ateniese 등이 동년 제안하였던 그룹 서명 기법[16]의 경우 2.5~10-KByte 정도이다. 이렇게 긴 그룹 서명의 길이는 그룹 서명의 실용화에 큰 걸림돌이 되었다 해도 과언이 아니었다.

겹선형 접합은 그룹 서명의 길이를 획기적으로 줄이는 역할을 했다. 겹선형 접합을 이용하는 대표적인 그룹 서명 기법인 Boneh 등의 짧은 그룹 서명 기법[6]의 경우 서명의 길이는 200-Byte 정도에 이른다. 이 논문에서 저자들은 $\mathbb{G}_1$의 원소 표기가 (170+1)-bit에 가능한 타원 곡선을 가정하여 이러한 결과를 도출하였다. 이는 2012년 현재 널리 사용되고 있는 2,048-bit의 RSA 서명보다 더 짧은 것으로 서명 자체의 길이로만 보면 충분히 실용성이 있다고 할 수 있다. 일반적으로 겹선형 접합을 이용하는 암호 기법에서는 암호문이나 서명의 길이를 짧게 하기 위하여 대부분의 연산을 $\mathbb{G}_1$에서 수행하는 경향이 있다. $\mathbb{G}_1$이 짧게 표시되기 위해서는, 삽입차수(embedding degree) k가 클 필요가 있는데, $\mathbb{G}_1$이 갖추어야 하는 최소한의 암호학적 강도와 $\mathbb{G}_T$가 가져야 하는 최소한의 길이로 인하여, k가 6을 넘기 힘들다. ($\mathbb{G}_1 \sim E(\mathbb{F}_q)$, $\mathbb{G}_2 \sim E(\mathbb{F}_{q^k})$, $\mathbb{G}_T \sim \mathbb{F}_{q^k}$이고, $|E(\mathbb{F}_q)| \approx q$, $|\mathbb{F}_{q^k}| \approx q^k$이다. 일반적으로 $q \geq 2^{160}$이고 $q^k \approx 2^{1024}$이므로, $k \approx 6$이다.)

한편, 앞서 설명한 것처럼, 겹선형 접합에서 사용하는 덧셈 순환군 $\mathbb{G}_1$에서의 DDH 문제는 쉬울 수도 어려울 수도 있다. 예를 들어, 초특이(supersingualr) 곡선 위에 정의된 모든 부분 그룹(subgroup)에서의 DDH 문제는 쉽다[24]. 반면, MNT 곡선[25] 위에 정의된 그룹에서의 DDH 문제는 어려울지도 모른다. 이러한 모호성을 제거하기 위해서, XDH나 SXDH와 같은 가정은 겹선형 접합을 이용한 암호 기법을 설계함에 있어서 많은 이득과 편리함을 제공한다. 하지만 이러한 이득과 편리함은 현실 세계에 해당 암호 기법

을 구현함에 있어서는 더 많은 제약 사항으로 바뀌게 된다. 또한 현실 세계에서 해당 암호 기법이 사용되기 위해서는 당연히 XDH나 SXDH와 같은 가정에 관해서 더 깊이 있는 고찰이 선행되어야만 할 것이다.

덧셈 순환군 $\mathbb{G}_1$이 갖는 DDH 문제의 모호성을 제거하기 위한 또 다른 방법은 덧셈 순환군 $\mathbb{G}_1$에서의 DDH 문제가 쉽다고 단순히 인정하는 것이다. 즉, 그룹 동형 $\psi_2 : \mathbb{G}_1 \rightarrow \mathbb{G}_2$이 효율적이라고 가정하는 것이다. 타원 곡선에 따라 DDH 문제가 어려워질지도 모르지만, 암호 기법을 설계함에 있어서 이러한 기대를 하지 않겠다는 것으로, 보안을 바라보는 보수적인 접근 방법이라고 할 수 있다. 그러나 이러한 접근 방법은 $O(1)$ 그룹 서명 기법을 설계할 때, 필연적으로 DDH 문제가 쉬운 그룹에서라고 할지라도 IND-CPA 또는 IND-CCA 안전한 암호화 기법을 필요로 하게 된다. LE 기법은 이러한 필요를 만족시키기 위한 한 가지 방법이라고 볼 수 있다.

어떠한 덧셈 순환군 $\mathbb{G} = \langle H \rangle$가 있을 때, LE 기법은 (LE.KeyGen, LE.Enc, LE.Dec)로 이루어지며 다음과 같은 구성을 갖는다. 여기서, $nH = O$이다. 메시지 M과 암호문 $C = (C_1, C_2, C_3)$는 그룹 $\mathbb{G}$위에 점들로써 표현된다.

- LE.KeyGen$() \rightarrow (pk, sk)$:
  $(\xi_1, \xi_2) \leftarrow_R \{\mathbb{Z}/n\mathbb{Z}\}^2$, $U \leftarrow (\xi_1)^{-1} H$, $V \leftarrow (\xi_2)^{-1} H$,
  $pk \leftarrow (U, V, H)$, $sk \leftarrow (\xi_1, \xi_2)$
- LE.Enc$(pk, M) \rightarrow C$:
  $(\alpha, \beta) \leftarrow_R \{\mathbb{Z}/n\mathbb{Z}\}^2$, $C_1 \leftarrow \alpha U$, $C_2 \leftarrow \beta V$,
  $C_3 \leftarrow M + (\alpha + \beta) H$, $C \leftarrow (C_1, C_2, C_3)$
- LE.Dec$(pk, sk, C) \rightarrow M$:
  $M \leftarrow C_3 - (\xi_1 C_1 + \xi_2 C_2)$

LE 기법은 ElGamal 암호화 기법과 다르게, 공격자가 그룹 연산(여기에서는 덧셈 연산)만을 이용한 일반적 알고리즘(generic algorithm)을 이용해서는 다항 시간 안에 메시지를 구별해낼 확률이 매우 낮다[6]. 즉, LE 기법은 GGM(Generic Group Model)에서 IND-CPA 안전하다.

III. 지역 연결성을 갖는 그룹 서명 기법

3.1 사용자 퇴출 절차의 어려움

그룹 서명 기법에서 가장 우려하는 역기능은 사용자가 자신에게 주어진 익명성을 남용 또는 악용하는 것이다. 그런 이유에서 그룹 서명 기법은 특정한 사용자가 익명성과 관련하여 잘못된 행위를 하는 경우, 서명으로부터 서명자의 식별자를 알아낼 수 있는 방법을 제공한다. '$O(1)$ 그룹 서명'이라면, 그룹 서명 안에 포함되어 있는 식별자의 암호문을 복호하여, 간단하게 서명자의 식별자를 알아낼 수 있다. 이렇게 알아낸 식별자는 잘못된 행위를 하는 사용자를 처리하는데 이용될 수 있다. 최종적으로 어떤 사용자들은 더 이상 그룹의 일원으로 있을 수 없게 되었을 때, 그룹에서 퇴출시키기 위한 사용자 퇴출(revocation) 과정이 필요하다. 이는 그룹 서명 기법에 있어서 유일한 예외(exception) 처리 과정이다.

Ateniese 등은 그들의 논문에서 사용자 퇴출에 대한 몇 가지 방법론에 대해서 기술하였다[26]. 상대적으로 효율적인 퇴출 절차를 가졌다는 그들의 기법을 포함하여, 많은 그룹 서명 기법에서 퇴출 절차는 전체적으로 큰 자원을 소모한다. 일반적으로 그룹 서명 기법의 사용자 퇴출 절차는 1) 그룹 서명키를 전부 재발급하거나, 2) CRL(Certificate Revocation List)을 발급하여 모든 서명에 대해서 하나하나 검사하게 하는 것으로 나뉠 수 있다. 그룹 서명키를 재발급 하는 방법은 1-1) 기존의 그룹 서명키를 모두 폐기하고 재발급 받는 방식과 1-2) 기존의 그룹 서명키를 업데이트 하는 방식으로 다시 나뉠 수 있다. 그룹 서명키를 모두 재발급하거나 업데이트하기 위해서는 정상적인 사용자들이 모두 참여해야만 한다. 상식적으로 이러한 과정은 모든 사용자의 순차적인 멤버십 재발급이나 업데이트로 인하여 어떠한 사용자가 생성한 그룹 서명들은 상대적으로 익명성이 낮아질 수 있는 문제를 고려하지 않다하더라도, 결코 빈번하게 일어나게 할 만한 것이 아님을 쉽게 납득할 수 있을 것이다. CRL을 발급하여 모든 서명에 대해서 검사하는 방식은 모든 그룹의 일원이 참여하여 무언가를 할 필요는 없지만 이 또한 쉬운 문제가 아니다. 정상적인 사용자는 제한 없이 그룹 서명을 생성할 수 있고, 그룹에 몇 명의 사용자가 많을 수도 있다. 그룹 서명이 갖는 익명성으로 인하여 CRL과의 비교에는 공개키 연산이 필요로 하기 때문에 퇴출된 사용자가 많으면 많을수록 CRL의 검색에 많은 연산이 필요하게 되며, 결과적으로 그룹 서명의 확인에 필요한 연산량이 CRL의 크기에 비례하여 증가하게 된다. 따라서 CRL 기반의 퇴출 절차라고 하더라도 긴 주기를 가지고 전체 그룹 서명키를 업데이트함으로써 CRL의 크기를 일정 수준이

하로 유지해야만 한다.

이렇게 부담이 되는 사용자 퇴출 절차는 그룹 서명 기법의 사용에 있어서 최소화해야 할 것이다. 하지만 그룹 서명 기법이 사용되는 분야마다 사용자 퇴출을 위한 정책은 서로 다를 수 있으므로 이를 서명 기법 차원에서 제한하는 것은 결코 바람직하지 않을 것이다. 따라서 그룹 서명 기법은 그 기법의 종류에 따라서 서명의 생성과 확인 이외에도 사용자 퇴출 절차와 관련하여 특정한 분야에서는 너무 많은 연산 때문에 적용이 불가능한 기법이 될 수밖에 없다. 예를 들어, Boneh 등의 짧은 그룹 서명 기법[6]의 경우 사용자 퇴출은 오로지 전체 그룹 서명키의 업데이트를 통해서만 가능한데, 이때 그룹의 크기가 매우 큰 경우 급하게 특정 사용자를 퇴출하는 것은 매우 큰 자원을 요구하게 된다. 앞서 설명한 것과 같이 사용자 퇴출 절차가 긴 주기에 한 번씩 발생하는 경우, 어떠한 잘못된 행위를 하는 사용자는 자신이 퇴출되기 전까지 시스템에 해가 되는 행위를 무제한으로 행할 수 있는 권한을 얻게 되는 것과 다르지 않다. 이러한 이유에서 그룹 서명 기법이 실제로 실생활에 응용되어 사용되기 위해서는, 사용자 퇴출 절차와 관련하여 잘못된 행위를 하는 사용자에 대한 관리 방법 등이 충분히 고려되어야만 한다.

이 논문에서는 이러한 문제에 대한 효율적인 해결 방법으로 지역 연결성을 갖는 그룹 서명 기법에 대해서 논의하고자 한다. 이 논문에서의 지역 연결성의 필요성에 대한 논의는 강전일 등이 2009년 처음 제시하였던 그룹 서명 기법에서의 지역 연결성의 필요 이유[9]와는 다르다는 점에 유의할 필요가 있다.

3.2 지역 연결성의 개념

강전일 등은 2009년, Boneh 등의 짧은 그룹 서명 기법[6]을 실생활에 사용하기 힘든 이유에 대해서 설명하면서, 이를 위해 짧은 그룹 서명을 수정하는 방법에 대해서 연구하였다[9]. 그들은 GM이 서비스 제공자가 되면 안 되며, 그러한 이유에서 필연적으로 GM의 권한이 분할될 필요가 있다고 결론 내렸다. 강전일 등은 권한 분할의 한 방법으로써 지역 연결성이라는 개념을 제시하였다. 그들은 그들의 논문에서 지역 연결성에 대해, '익명 취소 관리자가 갖는 전역 연결성에 비해서 서비스 제공자가 갖는 연결성'이라고 정의하고 있다. 서비스 제공자는 익명 취소 관리자와 다르게 주어진 그룹 서명들로부터 익명 사용자의 식별자를 알아낼 수 없고, 단지 연결성만을 갖는다. 그들은 그 논문에서 익명 취소 관리자에게 두 서명을 보내 두 서명을 동일한 익명 사용자가 생성했는지 물어보는 단순한 방법 이외에, 익명 사용자의 실제 서명을 전송하지 않으면서, 연결성을 확보하는 두 가지 방법을 소개하였다. 한편, 2010년 황정연 등은 2009년 강전일 등이 소개하였던 지역 연결성을 제공하는 방법 중에 서비스 제공자에게 트랩도어를 발급하는 기법을 보다 효율적으로 개선하는 방법을 소개하였다[10]. 그들은 이 논문에서 연결성이란 서명 값들이 한 서명키로부터 생성되었음을 의미한다고 정의 하였으며, 지역 연결성은 연결키라는 특별한 키가 주어진 경우에만 확인할 수 있는 연결성이라고 말하고 있으며, 그러므로 '제어 가능하다'고 언급하고 있다. 물론, 이는 지역 연결성을 제공하는 여러 방법 중 트랩도어를 이용하는 방법에 대한 것이다.

위 두 논문에서 밝힌 지역 연결성에 대한 정의 또는 성질은 그 구체적인 기술의 부족으로 인하여 직관적으로 이해하기 힘든 측면이 있다. 연결성을 '두 서명이 같은 서명키로부터 생성된 것임을 확인할 수 있는 능력'이라고만 정의할 경우, 서비스 제공자가 얻는 연결성(지역 연결성)과 익명 취소 관리자가 가진 연결성(전역 연결성)이 과연 다른 것인가 하는 의구심이 들 수밖에 없을 것이다. 서비스 제공자는 익명 취소 관리자에게 제한 없이 질의를 보낼 수 있다면 '연결성'에 대해서는 익명 취소 관리자와 별반 다르지 않은 정보를 얻어낼 수 있으며, 이는 지역 연결성과 전역 연결성이 본질적으로는 동일한 성질을 가짐을 의미한다.

그러나 익명 취소 관리자와 서비스 제공자가 얻는 '연결성'은 동일할 수도 있지만, 보다 일반적인 관점에 있어서는 동일한 것으로 보기 힘들다. 강전일 등이 자신들의 논문[9]에서 서비스 제공자의 권한을 제한하는 방법에 대해서 언급하고 있는 것으로 보아, 위와 같은 서비스 제공자가 익명 취소 관리자에게 제한 없는 질의를 보내는 것을 고려하고 있지는 않은 것으로 보인다. 또한, 황정연 등이 자신들의 논문[10]에서 새롭게 사용하였던 '제어 가능한 지역 연결성'이라는 말은 익명 취소 관리자가 서비스 제공자에게 연결키를 할당하거나 철회할 수 있다는 의미로 볼 수 있을 것이다. 따라서 '지역 연결성'은 익명 취소 관리자가 자신의 관리를 담보로 서비스 제공자에게 양도 해주는 어떠한 권한으로 볼 수 있을 것이며, 오로지 익명 취소 관리자의 동의가 있을 때에만 얻을 수 있는 것으로 보인다. 익명 취소 관리자가 제한 없이 서비스 제공자로부터의

질의에 응답하는 경우가 특수한 경우라는 것에는 이견이 없을 것이다.

지역 연결성이 익명 취소 관리자에 의해서 제어되었을 때, 서비스 제공자와 익명 취소 관리자가 얻을 수 있는 연결성에는 자연스럽게 차이가 발생한다. 익명 취소 관리자는 주어진 그룹 서명으로부터 사용자의 식별자를 얻어낼 수 있다. 이러한 사용자의 식별자를 이용하여 익명 취소 관리자는 어떠한 경우에서도 그 그룹 서명이 유효하다면 모든 그룹 서명을 '연결'할 수 있다. 이를 '전역 연결성(global linkability)'이라고 할 수 있을 것이다. 한편, 서비스 제공자는 익명 취소 관리자가 허용해주는 그룹 서명에 대해서만 연결성을 얻을 수 있다. 강전일 등은 바로 이러한 연결성을 '지역 연결성'이라고 보았다[9].

이러한 정의는 그들이 제안하였던 두 기법들에서는 경우에 따라서 확보할 수 없는 성질로 보인다. 서비스 제공자가 두 그룹 서명을 익명 취소 관리자에게 직접 보내는 방식에 있어서 익명 취소 관리자는 특정한 서비스 제공자와 시간, 사용자들, 그리고 서명의 내용에 따라서 연결성을 제한할 수 있다. 그러나 강전일 등이 제안하였던 두 기법들에서 익명 취소 관리자는 특정한 서비스 제공자와 시간에 대해서만 연결성을 제한할 수 있을 뿐이다. 이 또한 트랩도어를 이용하는 기법에서는 명시적인 것이 아니며, 서비스 제공자에게 할당된 그룹 공개키와 이에 따른 연결키의 할당에 의해서 암묵적으로 제한되는 것이다. 강전일 등이 그들의 논문[9]에서 제안하였던 두 기법들 간에도 시스템을 어떻게 구성하고 신뢰하느냐의 선택의 문제가 존재하는 것이다.

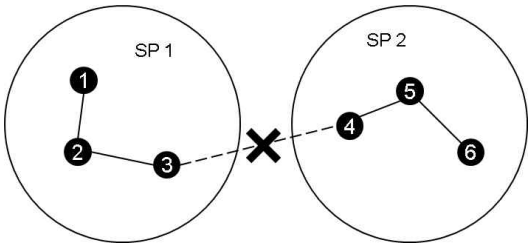
따라서 강전일 등과 황정연 등이 주로 고려하였던 지역 연결성에서 '지역'은 시간과 공간적으로만 구별되는 개념에 가깝다. 즉, 그들의 관점에 있어서 '지역'이란, '서비스 제공자'를 염두에 둔 개념이라는 것이다. 이러한 지역의 개념으로 볼 때, 서비스 제공자가 '현재 자신들에게 할당된 그룹 공개키에 유효한 연결키'를 알고 있다면 '지역 연결성'을 갖는다고 볼 수 있다. 이는 황정연 등이 그들의 논문에서 밝힌 바와 일치한다[10].

3.3. 지역 연결 관리자와 지역 연결성의 성질

이 논문에서는 앞과 같은 지역 연결성에 대한 고찰을 바탕으로, 익명 취소 관리자로부터 '시간과 공간적으로 제한되는 지역' 개념 아래서의 '지역 연결성'을 위임받은 지역 연결 관리자로써의 서비스 제공자를 가정한다. 우리는 이 논문에서 익명 취소 관리자로부터 완화된 연결성(즉, 지역 연결성)을 위임받은 관리자를 '지역 연결 관리자'라고 부른다. 지역 연결 관리자는 하나의 그룹에 여럿 존재할 수 있다. 앞서 설명한 것과 같이, $O(1)$ 그룹 서명 기법에서는 사용자 식별자를 암호화하기 위한 공개키가 부분 그룹마다 서로 다를 수 있으므로, 익명취소 관리자가 여럿 존재할 수 있다. 이는 곧 지역 연결 관리자가 하나의 시스템에 여럿 존재할 수 있음을 의미한다.

지역 연결 관리자의 존재는 서비스의 제공과 정상적이지 않은 사용자 퇴출에 보다 유연성 있게 접근할 수 있게 해준다. 익명 서비스를 제공하기 위한 다음과 같은 시나리오를 생각해보자. 서비스 제공자가 직접 GM이 되어 사용자에게 그룹 서명 기법을 사용하도록 하는 것은 아무런 의미 없는 행위이므로, GM은 일반적으로 서비스 제공자의 외부에 존재해야 한다. 또한 하나의 GM에 하나의 서비스 제공자가 존재하는 것보다 하나의 GM에 여러 서비스 제공자가 존재하는 경우가 더욱 현실적이다. 서비스 제공자는 잘못된 행위를 하는 사용자를 제지하기 위해서는 GM의 도움을 받을 수 있다. 모든 그룹 서명에 대해서 GM에게 잘못된 행위를 했던 사용자가 생성한 것인지 물어보는 것은 바람직하지 않다. 따라서 서비스 제공자는 자신에게 해가 되었던 행동과 연관된 그룹 서명들을 모아 GM에게 주어 사용자 퇴출 절차를 밟도록 하는 것 이외에 딱히 할 수 있는 일이 없다. 앞서 설명한 것과 마찬가지로 사용자 퇴출 절차는 그룹 전체에 큰 부담이 되므로 일정한 주기를 가지고 실행되어야할 필요가 있는데, 이때, 서비스 제공자는 정상적이지 않은 사용자들이 퇴출 될 때까지 그 사용자들을 제지할 방법이 없다.

이 경우 GM은 서비스 제공자에게 익명취소 권한을 양도함으로써, 문제를 보다 유연하게 가져갈 수 있을 것이다. 서비스 제공자마다 식별자의 암호화를 위한 공개키를 다르게 사용함으로써, 서비스 제공자가 GM으로부터 양도받은 익명취소 권한은 자신에게 제출된 그룹 서명에 한하여 동작하게 된다. 이 때 서비스 제공자가 그룹 서명으로부터 얻을 수 있는 것은 사용자의 고유 식별자에 해당한다. 서비스 제공자는 이러한 사용자의 고유 식별자를 이용하여 서비스를 제공하거나 정상적이지 않은 사용자에 대해서 퇴출 절차를 거치지 않고 서비스를 제한할 수 있다. 이 과정에서 서비스 제공자가 얻게 되는 사용자의 식별자가 곧바로



〔그림 1〕 복수의 서비스 제공자(지역 연결 관리자)와 지역 연결성. 서비스 제공자끼리 공모한다고 해도 그룹 서명 ❸과 ❹사이에 연결성을 확신할 수 없다.

사용자의 실명을 의미하지는 않기 때문에 큰 문제는 없어 보인다. 그러나 각각의 서비스 제공자들이 얻게 되는 사용자의 식별자는 모든 서비스 제공자에게 있어서 동일하며, 서비스 제공자들이 공모할 경우, 사실상 그룹 서명 기법이 갖는 익명성은 오로지 사용자의 실명과 식별자 사이의 연결성으로 좁혀지게 되는 결과를 가져온다. 지역 연결 관리자는 이런 경우에 있어서 사용자들이 지역적으로 완전하게 분리된 익명성을 갖도록 도와준다. 즉, 지역 연결 관리자의 권한을 가진 서비스 제공자들이 공모한다고 해도 지역 간 사용자들의 연결성을 추정할 수는 없다. 〔그림 1〕은 지역 연결성에 이러한 성질에 대해서 간략히 보여준다.

3.4. 수정된 LE 기법을 이용한 지역 연결성의 확보

황정연 등이 강전일 등의 논문[9]에 소개되었던 트랩도어를 이용하여 지역 연결성을 제공하는 방법을 효율적으로 개선한 기법[10]은 Boneh 등의 짧은 그룹 서명 기법[6]이나 Makita 등이 제안한 기법[18]과 같이 LE 기법을 사용하는 모든 그룹 서명에 사용될 수 있다. 이 논문에서는 편의를 위하여 황정연 등이 개선한 지역 연결성을 제공하는 그룹 서명 기법에서 얻을 수 있는 수정된 LE 기법을 MLE(Modified Linear Encrypotion) 기법이라고 부르도록 한다. 비록 강전일 등과 황정연 등은 그들의 논문에서 그룹 서명의 추가된 함수의 형태로 그들의 기법을 제안하였지만, 이 논문에서는 형식적인 증명을 위하여 암호화 부분만을 먼저 따로 떼어 암호화 기법으로 생각하기로 한다. 기술적으로는 황정연 등의 논문[10]과 동일하지만, 기법의 기술(記述)에 있어서의 통일성을 위해서 해당 논문과는 다른 기호를 사용한다.

MLE 기법은 다음과 같은 {MLE.KeyGen, MLE.Enc, MLE.Dec, MLE.GetLabel}로 구성된다. MLE.Enc는 LE.Enc와 동일하며, MLE. Dec는 LE.Dec와 동일하여 생략한다. 앞선 LE 기법과 다르게, $\mathbb{G}_1=\mathbb{G}=\langle H\rangle$이고 $nH=O$이다. 여기서 추가적으로 $\mathbb{G}_2=\langle F\rangle$, 메시지 M은 $\mathbb{G}_1$ 위의 한 점이라고 할 때, MLE.KeyGen과 MLE. GetLabel은 다음과 같다.

- MLE.KeyGen()$\rightarrow(pk,sk,lk)$:
  $(\xi_1,\xi_2)\leftarrow_R\{\mathbb{Z}/n\mathbb{Z}\}^2$, $U\leftarrow(\xi_1)^{-1}H$,
  $V\leftarrow(\xi_2)^{-1}H$, $\ell\leftarrow\xi_1/\xi_2$, $L\leftarrow-\xi_2F$
  $pk\leftarrow(U,V,H)$, $sk\leftarrow(\xi_1,\xi_2)$, $lk\leftarrow(\ell,F,L)$,
- MLE.GetLabel$(pk,lk,C)\rightarrow B$:
  $B\leftarrow e(C_3,F)\cdot e(\ell C_1+C_2,L)$

MLE.GetLabel의 결과로 출력되는 B는 $e(M,F)$와 같다. 즉, 메시지 M이 동일하다면, 서로 다른 암호문들이 주어졌다고 하더라도 MLE. GetLabel은 항상 동일한 값을 구해낼 수 있다. 왜냐하면,

$$\begin{aligned}B&=e(C_3,F)\cdot e(\ell C_1+C_2,L)\\&=e(M+(\alpha+\beta)H,F)\cdot e(\ell\alpha U+\beta V,L)\\&=e(M,F)e((\alpha+\beta)H,F)\\&\quad\cdot e((\xi_1/\xi_2)\alpha(\xi_1)^{-1}H+\beta(\xi_2)^{-1}H,-\xi_2F)\\&=e(M,F)e(H,F)^{\alpha+\beta}\cdot e(H,F)^{-(\alpha+\beta)}\\&=e(M,F)\end{aligned}\tag{3}$$

와 같은 관계가 성립하기 때문이다.

이제 이 기법을 LE 기법이 사용되는 그룹 서명에 사용하는 경우에 대해서 생각해보자. MLE 기법이 사용되는 그룹 서명에서는 시스템의 참여자들은 다음과 〔표 3〕 같은 권한과 정보를 갖게 된다.

MLE 기법의 암호화와 복호화 절차는 LE 기법과 동일하기 때문에 MLE 기법이 그룹 서명에 사용된다고 하더라도, 사용자들은 기존의 서명 기법과 동일하게 사용할 수 있다. 단지, 익명취소 관리자에게 연결

〔표 3〕 수정된 LE를 사용하는 그룹 서명에서의 참여자와 그 역할

	보유 비밀	역할
멤버십 관리자	멤버십 인증서 발행키	Join/Iss()을 통해 사용자에게 그룹 서명키 발행
익명취소 관리자	그룹 익명 철폐키	Open()을 통해 그룹 서명의 식별자와 증거 생성
지역 연결 관리자(서비스 제공자)	연결키	GetLabel()을 통해 서명자의 지역 연결 레이블 생성
사용자	그룹 서명키	GSign()을 통해 그룹 서명의 생성

키 lk를 양도받은 지역 연결 관리자는 동일한 그룹 공개키를 사용한 모든 그룹 서명(이 포함하는 사용자 식별자 A의 암호문)으로부터 레이블 B를 계산해낼 수 있다. 따라서 레이블 B를 가진 그룹 서명들을 모음으로써 지역 연결성을 확보할 수 있다. 그러나 일반적으로 지역 연결 관리자는 어떠한 그룹 서명으로부터 얻어낸 레이블 B로부터 사용자의 식별자 A를 알아낼 수는 없다.

모든 지역 연결 관리자는 서로 다른 연결키 lk를 가질 수 있다. 예를 들어, 어느 지역 연결 관리자가 보유한 연결키 $lk_1=(\ell,F_1,L_2)$라고 했을 때, 다른 어떤 지역 연결 관리자는 $lk_2=(\ell,F_2,L_2)$를 보유할 수 있다. 이 때, $F_1\neq F_2$라면, 두 지역 연결 관리자가 사용자 식별자가 A인 동일한 사용자가 생성한 두 그룹 서명 σ_1과 σ_2로부터 얻는 레이블은 $B_1=e(A,F_1)$과 $B_2=e(A,F_2)$으로 서로 다르다. A에 대한 지식 없이는 지역 연결 관리자들은 이 둘을 연결시킬 수 없다.

이러한 성질은 지역 연결 관리자가 없이, 단지 서로 다른 그룹 공개키를 지역 마다 사용하고 서로 다른 그룹 익명 철폐키를 보유한 익명 철회 관리자가 다수 있는 경우에 비하여 더 높은 보안성을 제공한다. 두 그룹 서명 σ_1과 σ_2가 서로 다른 익명 철회 관리자에게 주어졌을 때, 멤버십 관리자는 결국 혼자이므로 Open의 결과는 항상 동일한 A가 나오게 된다. 이 경우 익명 철회 관리자들이 공모하면 지역 간 연결성을 만들 수 있다.

3.5. 프라이버시 관점에서의 지역 연결성

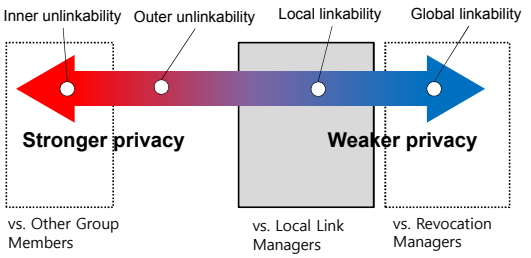
그룹 서명 기법에 있어서 사용자의 프라이버시와 관련하여, Bellare 등은 완전 익명성(full-anonymity)을 어떠한 공격자도 GM의 비밀키 없이는 서명자의 식별자를 알아낼 수 없는 것으로 정의하였다[14]. 여기에서는 사용자의 그룹 서명키를 알아낸 공격자도 포함된다. 이러한 완전 익명성은 그동안 많은 그룹 서명에서 고려되었던 익명성(anonymity)과는 다소 차이를 보이는 데, 자신의 서명을 자신이 누가 만들어냈는지 알 필요는 없기 때문에 서명자의 그룹 서명키를 공격자에게 줄 필요가 없었다.

한편, 비연결성(unlinkability)은 여러 서명이 있을 때 이를 보고 동일한 서명자가 생성한 두 서명을 연결 지을 수 없다는 것이다. 어떠한 수단으로 인하여 그룹 서명의 익명성이 깨어졌을 때, 다른 그룹 서명들로 문제가 확대되는 것을 막아줄 수 있다. 일반적으로 비연결성을 말할 때, 공격자를 그룹 일원이 아니라고 가정하지만 —외부자 비연결성(outer unlinkability)—, 실제적으로는 그룹 일원일 수도 있기 때문에 —내부자 비연결성(inner unlinkability), 이는 그룹 일원의 공모 가능성을 포함한다— 비연결성을 공식화하는 것은 쉽지 않다. 또한 비연결성의 합리적인 정의는 익명성을 배경에 깔고 생각해보아야 할 것처럼 보이기 때문에, Bellare 등은 익명성과 비연결성은 전혀 다른 요구 사항처럼 보이지만, 실질적으로는 같은 성질의 것이라고 결론 내렸다[14]. 이들의 결론에 따르면 '완전 익명성'은 '비연결성'과 '익명성'을 포함한 개념으로 볼 수도 있다.

한편, BSZ05 모델[15]에서는 GM의 권한이 멤버십 관리자와 익명 취소 관리자에게 나누어지기 때문에 비연결성과 익명성은 동일하지 않다. 전역 연결성을 갖는 익명 취소 관리자라고 할지라도 자신이 얻은 정보(사용자의 식별자)만으로는 실제 사용자(이름, 전화번호, 주민등록번호 등)를 특정할 수 없기 때문에 여전히 일부 익명성(프라이버시)은 존재한다. 즉, 일반 그룹 일원은 익명 취소 관리자에게 있어서 GM보다 더 강한 프라이버시를 갖게 된다.

단순하게 생각한다면 그룹 서명 기법이 제공해야만 하는 비연결성이 비해 지역 연결성은 프라이버시를 완화한 것처럼 보인다. 그러나 지역 연결성은 일반적인 그룹의 일원에게는 주어지지 않는 능력일 뿐만 아니라, 지역 연결 관리자끼리의 공모 가능성 또한 고려하고 있다. 거꾸로 생각해보면, '지역' 연결성은 전역 연결성에서 프라이버시를 강화한 개념으로 볼 수 있을 것이다. 이러한 관점에서 지역 연결성은 그룹 서명 기법에서 사용하고 있는 2단계 구조(익명 취소 관리자 - 일반 그룹 일원)에, 중간에 하나의 단계(익명 취소 관리자 - 지역 연결 관리자 - 일반 그룹 일원)를 추가함으로써 고려해야만 하는 프라이버시 요구 사항에 지나지 않는다. 그룹 서명 기법에서 비연결성과 관련된 프라이버시 요구는 외부자 비연결성과 내부자 비열결성의 논란에서 볼 수 있듯이 일반 그룹 일원이 특정한 대상에게 갖는 프라이버시로 바라보아야 할 것이다. 다시 말하자면, 일반 그룹 일원은 지역 연결 관리자에게 있어서 익명 취소 관리자보다 더 강한 프라이버시를 갖는다. [그림 2]는 프라이버시 관점에서 바라본 지역 연결성과 그 외의 다른 연결성 및 비 연결성에 대해서 간략히 보여준다.

하지만, 이와 같은 관점과는 반대로, 현실 세계에서는 GM보다 익명 취소 관리자가 더 많고, 익명 취소



〔그림 2〕 그룹 일원이 갖는 프라이버시. 그룹 일원은 지역 관리자에게 익명 취소 관리자보다 더 강한 프라이버시를 갖는다.

관리자보다 지역 연결 관리자가 더 많은 경우가 더욱 상상하기 쉽기 때문에, 지역 연결 관리자는 시스템의 전체적인 프라이버시를 약화시킨다고 보는 것이 조금 더 직관적이다. 그러나 이러한 직관적 결론을 내리기 위해서는 현실 세계를 더 많이 고려해야만 한다.

예를 들어, 어떠한 시스템에서 서비스 제공자들에게 익명 취소 관리자들의 권한을 부여하는 경우를 생각해보자. 서비스 제공자들에게 지역 연결 관리자의 권한을 부여했을 때보다 일반 그룹 일원의 프라이버시는 더 낮아졌고, 오히려 지역 연결 관리자들이 존재하는 경우가 프라이버시가 더 높다. 이 두 경우에 대해서 서비스 제공자가 부여받은 권한의 차이는 매우 커 비교 자체가 불합리할 수 있다는 점을 차치하고서라도, 지역 연결성을 가진 지역 연결 관리자가 있느냐 없느냐 보다는 시스템을 어떻게 구성하느냐가 일반 그룹 일원의 프라이버시에 영향을 미친다고 볼 수 있는 것이다.

앞서 설명했다시피, 지역 연결성과 지역 연결 관리자는 현실 세계에서 그룹 서명 기법의 사용을 유연하게 하기 위해서 고안된 것이다. 일반 그룹 일원의 프라이버시가 시스템 구성에 더 큰 영향을 받는다고 보면, 지역 연결성을 사용하지 않고 원래의 그룹 서명 기법에서 고려된 시스템 참가자만을 고려하여 시스템을 구성하는 것보다 지역 연결성을 이용하는 것이 일반 그룹 일원에게 더 높은 프라이버시를 제공할 수도 있다.

지역 연결성은 그 자체로 다른 기능을 수행하는 것이기 때문에, 그러한 기능이 존재하지 않는 시스템과 직접적인 비교는 올바르지 않을 수 있다. 즉, 지역 연결성만을 따로 떼어 이 성질이 시스템의 프라이버시를 완화하거나 약하게 한다고 또는 반대로 강화한다고 쉽게 결론 내릴 수 없다.

IV. 지역 연결 관리자를 위한 MLE 기법의 보안성 분석

4.1. 지역 연결 관리자의 보안성

지역 연결 관리자는 그룹의 특별한 일원 중 하나이다. 따라서 LE 기법 대신 MLE 기법을 사용한다고 하더라도, 그룹의 일반적 사용자들 사이에서는 같은 수준의 보안성을 갖는다. 여기에서는 지역 연결 관리자에게 그룹 서명이 갖는 보안성에 대해서만 이야기한다. 그룹 서명 기법의 익명성과 관련된 형식적 증명은 BMW03 모델[14]이나 BSZ05 모델[15]을 따르는 것이 일반적이나, 이 논문에서 대상으로 하고 있는 LE 기법의 익명성은 이 두 모델로써 증명되지 못한다. Boneh 등은 BMW03 모델에서 고안된 완전 익명성(Full-anonymity)을 따르지 않고, CPA 완전 익명성(CPA-full-anonymity)이라는 완전 익명성보다 완화된 익명성에 대한 증명을 시도하였다[6]. 완전 익명성의 경우 선택적 암호문 공격(CCA)에 대한 안전성을 증명해야 하지만, 선택적 평문 공격(CPA)에 대한 안전성만을 증명한 것이다. 또한, 그 증명에서도 그룹 서명 기법의 핵심이 되는 LE 기법의 안전성은 표준 모델이 아닌 GGM 아래에서 IND-CPA 안전함이 증명한 것이다.

지역 연결 관리자가 일반 사용자보다 더 많이 갖게 되는 정보는 오로지 $\ell = \xi_1/\xi_2$ 뿐이다. 황전연 등의 연구[10]에서 알 수 있다시피, F와 L은 $\mathbb{G}_1$과 $\mathbb{G}_2$이 서로 다른 겹선형 접합을 위해 추가된 정보로 그 자체가 DLP이다. 또한 (ℓ, F, L)로부터 ξ_1이나 ξ_2에 대한 정보를 얻어내는 것은 DLP를 해결하는 것과 동일하다는 사실은 표준 모델에서 쉽게 증명된다. 하지만 $\ell = \xi_1/\xi_2$이 공격자에게 주는 정보는 매우 크다고 할 수 있다. 단순하게 생각해서, 그룹 익명 철폐키 $gok = (\xi_1, \xi_2)$를 전사적 탐색 공격으로 찾아내기 위해서는 $O(q^2)$만큼의 시간이 걸린다. 하지만, $\ell = \xi_1/\xi_2$이 주어졌을 때, 공격자는 단지 $O(q)$만큼의 시간으로 (ξ_1, ξ_2)를 찾아낼 수 있다. $O(q^2)$와 $O(q)$ 모두 다항 시간에 해결할 수 없는 시간인 것은 동일하지만, 그 차이는 매우 크다. 따라서 지역 연결 관리자는 일반 사용자보다 더 많은 정보를 가지고 있음은 분명해 보인다. 표준 모델에서 LE 기법이 일반 사용자들에게 있어서 OW-CPA 안전한 것은 더 이상의 논란의 여지가 없다. 그렇다면 MLE 기법이 지역 연결 관리자에게도 OW-CPA 안

전한지 확인해볼 필요가 있을 것이다.

〔**정의 1**〕 SCDH(Square Computational Diffie-Hellman) 문제: 큰 소수인 그룹 오더(order) q와 생성자 P를 갖는 어떠한 덧셈 순환군 $\mathbb{G}$가 있을 때, SCDH 문제는 주어진 $Q\in\mathbb{G}$로부터 어떠한 $x\in\mathbb{Z}/q\mathbb{Z}$에 대해서 $Q=xP$와 $R=x^2P$을 동시에 만족하는 $R\in\mathbb{G}$를 찾는 문제이다.

〔**가정 1**〕 SCDH 가정: 모든 확률 기반의 다항식(Probabilistic Polynomial-Time, PPT) 알고리즘 $\mathscr{P}$에 대해서 SCDH 문제를 해결할 확률은 무시할 만하다.

$$\Pr[\mathscr{P}(P,Q)=x^2P|Q=xP]\le\mu(q) \tag{4}$$

여기서 $\mu(q)$는 입력 q에 대해서 무시해도 좋을 정도로 낮은(negligible) 확률을 나타내는 확률 함수이다.

SCDH 문제는 CDH 문제와 동일하다. 이 문제들의 동등성은 잘 알려져 있고, 쉽게 확인해볼 수 있으므로 자세한 내용은 생략한다. CDH 가정을 이 논문에서 바로 사용하지 않는 것은 다음의 증명에서 SCDH 가정을 바로 적용할 수 있기 때문이다.

〔**정리 1**〕 $(\xi_1,\xi_2)\in_R\{\mathbb{Z}/q\mathbb{Z}\}^2$와 $\mathbb{G}=\langle H\rangle$에 대해서, $\xi_1U=H$와 $\xi_2V=H$라고 하자. SCDH 가정이 옳다면, 주어진 $C=(\alpha U,\beta V,M+(\alpha+\beta)H)$와 $\ell=\xi_1/\xi_2$로부터, 어떠한 확률 기반의 다항식 알고리즘 $\mathscr{A}$이 M을 구할 확률은 무시할 만하다.

$$\Pr\left[\mathscr{A}\begin{pmatrix}(\xi_1)^{-1}U,(\xi_2)^{-1}V,H,\xi_1/\xi_2,\\ \alpha(\xi_1)^{-1}H,\beta(\xi_2)^{-1}H,\\ M+(\alpha+\beta)H\end{pmatrix}=M\right]\le\mu(q) \tag{5-1}$$

〔**증명**〕 증명을 위해서 (정리 1)의 역을 선언한다. 즉, 어떠한 확률 기반의 다항식 알고리즘 $\mathscr{A}$는 무시하지 못할 확률을 가지고 M을 구할 수 있다고 가정한다.

$$\Pr\left[\mathscr{A}\begin{pmatrix}(\xi_1)^{-1}U,(\xi_2)^{-1}V,H,\xi_1/\xi_2,\\ \alpha(\xi_1)^{-1}H,\beta(\xi_2)^{-1}H,\\ M+(\alpha+\beta)H\end{pmatrix}=M\right]>\mu(q) \tag{5-2}$$

이러한 알고리즘 $\mathscr{A}$가 존재한다면, 다음과 같이 SCDH 문제 (P,Q)를 해결하는 알고리즘 $\mathscr{B}$를 생각해 볼 수 있다.

SCDH 문제 (P,Q)를 해결하는 알고리즘 $\mathscr{B}$:

1) 알고리즘 $\mathscr{B}$는 $(\alpha,\beta,\ell)\in_R\{\mathbb{Z}/q\mathbb{Z}\}^3$와 $C_3\in_R\mathbb{G}$를 무작위로 선택한다.
2) 알고리즘 $\mathscr{B}$는 $U=P$, $V=\ell P$, $H=Q$, $C_1=\alpha H$, $C_2=\beta H$를 계산한다.
3) 알고리즘 $\mathscr{B}$는 $\mathscr{A}(U,V,H,\ell,C_1,C_2,C_3)$를 실행한다.
4) 알고리즘 $\mathscr{A}$는 $\mu(q)$보다 큰 확률로 어떠한 M을 반환할 것이다.
5) 알고리즘 $\mathscr{B}$는 $R=(\alpha+\beta/\ell)^{-1}\cdot(C_3-M)$으로 계산하고 이를 답으로 내놓는다.

$Q=xP$라고 가정했을 때, $C_1=\alpha H=\alpha xP$이고, $C_2=\beta H=bxP$이다. $\tilde{\alpha}=\alpha x$, $\tilde{\beta}=\beta x/\ell$이라고 놓으면, $C_1=\tilde{\alpha}U$, $C_2=\tilde{\beta}V$이다. 앞서 C_3는 무작위로 선택되었지만, 이는 어떠한 알지 못하는 메시지 M에 대해서 $M+(\tilde{\alpha}+\tilde{\beta})H$와 동일해야 한다. 따라서 (C_3-M)은 $(\tilde{\alpha}+\tilde{\beta})H$와 같다. 위 4) 단계에서 알고리즘 $\mathscr{A}$가 돌려주는 M으로부터 알고리즘 $\mathscr{B}$는 $(\tilde{\alpha}+\tilde{\beta})H$를 구할 수 있다.

$$\begin{aligned}C_3-M&=(\tilde{\alpha}+\tilde{\beta})H=\left(\alpha x+\frac{bx}{\ell}\right)Q\\&=\left(\alpha+\frac{\beta}{\ell}\right)xQ=\left(\alpha+\frac{\beta}{\ell}\right)x^2P\end{aligned} \tag{6}$$

이 때, SCDH 문제 (P,Q)의 답에 해당하는 $R=x^2P$ 이외의 값들에 대해서 알고리즘 $\mathscr{B}$는 자신이 선택했으므로 알고 있다. 따라서 알고리즘 $\mathscr{B}$는 R을 $R=(\alpha+\beta/\ell)^{-1}(C_3-M)$와 같이 구할 수 있다.

$$\begin{aligned}R&=\left(\alpha+\frac{\beta}{\ell}\right)^{-1}(C_3-M)\\&=\left(\alpha+\frac{\beta}{\ell}\right)^{-1}\left(\alpha+\frac{\beta}{\ell}\right)x^2P=x^2P\end{aligned} \tag{7}$$

따라서,

$$\Pr[\mathscr{B}(P,Q)=x^2P|Q=xP]\ge\Pr\left[\mathscr{A}\begin{pmatrix}(\xi_1)^{-1}U,(\xi_2)^{-1}V,H,\xi_1/\xi_2,\\ \alpha(\xi_1)^{-1}H,\beta(\xi_2)^{-1}H,\\ M+(\alpha+\beta)H\end{pmatrix}=M\right] \tag{8}$$

이다. 그런데, 위의 식 (8)의 우측은 식 (5-2)와 같고 ((정리 1)의 역), 좌측은 식 (4)와 같아야 하므로

$$\mu(q)\ge\Pr[\mathscr{B}(P,Q)=x^2P|Q=xP]>\mu(q) \tag{9}$$

이다. 하지만, 이는 $\mu(q) > \mu(q)$를 이끄는 모순이다. 따라서 〔정리 1〕의 역이 거짓이므로, 〔정리 1〕이 옳음이 증명된다. □

〔정리 1〕로부터, MLE 기법이 지역 연결키 lk를 가지고 있는 공격자에게 평문이 노출되지 않음을 알 수 있다. 즉, MLE 기법은 지역 연결키 lk를 가지고 있는 공격자에 대하여 OW-CPA 안전하다. 더 나아가 〔정리 1〕을 바탕으로, 지역 연결키 lk를 가지고 있는 지역 연결 관리자가 그룹 서명에 갖는 보안성을 분석할 수 있다.

〔정리 2〕 SCDH 가정이 옳다면, 그룹 공개키 gpk와 연결키 $lk=(\ell=\xi_1/\xi_2, F, L=-\xi_2 F)$를 가진 어떠한 확률 기반의 다항 시간 공격자 $\mathscr{A}$는 주어진 LE 기반의 그룹 서명 σ으로부터 사용자의 식별자 A를 구할 확률은 무시할 만하다.

$$\Pr[\mathscr{A}(gpk, lk, m, \sigma) = A] \le \mu(q) \tag{10}$$

〔증명의 대략〕 그룹 서명과 관련된 랜덤 오라클을 이용한 증명은 대체로 정형화 되어 있으므로 이 논문에서는 자세한 기술에 대해서는 생략하고, 간략히 그 전략에 대해서만 기술한다.

이제 그룹 서명 σ으로부터 식별자 A를 무시하지 못할 확률로 구해낼 수 있는 어떠한 확률 기반의 다항 시간 알고리즘 $\mathscr{A}$을 생각해보자. 이 알고리즘이 무시하지 못할 확률로 식별자 A를 구해낼 수 있을 때, 이를 이용하여 SCDH 문제 (P, Q)를 해결할 수 있음을 보일 수 있다면, 그러한 알고리즘 $\mathscr{A}$는 존재할 수 없음을 증명할 수 있을 것이다. LE 기법을 사용하는 그룹 서명 σ에서 사용자 식별자 A랑 관련된 정보를 가진 것은 오로지 A의 암호문밖에 없으므로, 〔정리 2〕의 증명과정과 〔정리 1〕의 증명과정은 별반 다르지 않다. 하지만 SCDH 문제 (P, Q)를 이용하여 유효한 그룹 서명 σ를 만들어 알고리즘 $\mathscr{A}$에게 입력으로 주는 것은 정상적인 방법으로는 쉽지 않다. 왜냐하면 실제 지식을 바탕으로 만들어낸 영지식 증명(zero-knowledge proof)에 의한 서명이 아니므로, 서명의 확인 값(checksum)이 실제로는 올바르지 않게 된다. 표준모델에서는 알고리즘 $\mathscr{A}$가 실제로 올바르지 않은 서명을 받았으므로, 연산 자체를 거부할 것이다. 따라서 〔정리 2〕의 증명을 위해서는 프로그래밍 가능한(programmable) 랜덤 오라클이 필요하다. 랜덤 오라클에서 조작된 서명의 확인 값을 알고리즘 $\mathscr{A}$가 알아낼 확률은 무시할 만하므로, 알고리즘 $\mathscr{A}$는 여전히 무시하지 못할 확률로 식별자 A를 구해낼 수 있다. 이는 모순을 이끌고, 따라서 〔정리 2〕가 올바름을 확인할 수 있다. □

이상과 같은 증명에 의하면, 지역 연결 관리자는 MLE 기법을 이용한 그룹 서명 기법으로부터 사용자의 식별자를 알아낼 수 없다. 하지만 지역 연결 관리자는 자신이 선택한 두 식별자 A_0, A_1를 이용하여 그룹 서명이 생성 되었을 때, 이를 구별해낼 수 있다. 왜냐하면 자신이 선택한 두 식별자로부터 $e(A_0, F)$와 $e(A_1, F)$를 모두 계산해낼 수 있고, 서명으로부터 $e(A_b, F)$를 계산해내어 비교할 수 있기 때문이다.

4.2. 사용자 식별자 공개 유무에 따른 보안성

지역 연결 관리자에 대한 안전성의 증명과 관련하여 더 고려해야만 하는 것은 사용자 식별자의 공개 유무와 관계가 있다. 대부분의 $O(1)$ 그룹 서명 기법들은 사용자 식별자의 공개에 별다른 언급이 없다. 하지만 $O(n)$ 그룹 서명 기법에서는 사용자의 식별자 또는 그에 준하는 정보를 공개해야만 Open을 수행할 수 있다. 이렇게 놓고 생각해보면 그룹 서명 기법에서 사용자의 식별자를 공개하는 것이 더 바람직해 보인다. 하지만 Boneh와 Shacham이 제안하였던 VLR 그룹 서명 기법[7]의 경우 특정한 사용자의 식별자가 공개되면, 서명으로부터 그 사용자가 서명했는지 확인하는 것이 가능하다. 즉, 사용자의 식별자가 공개되면 사용자의 익명성은 존재하지 않게 된다.

이 논문의 OW-CPA 테스트에서는 지역 연결 관리자는 기본적인 모든 사용자의 식별자를 알지 못한다고 가정해야 한다. 만약 지역 연결 관리자가 모든 사용자의 식별자를 알고 있다면, 모든 사용자 식별자로부터 레이블 값을 생성하고 주어진 서명으로부터 레이블을 계산하여 서로 비교해 봄으로써, 서명에 어떠한 사용자의 식별자가 사용되었는지 알아낼 수 있다. 즉, 모든 사용자의 식별자를 알고 있는 지역 연결 관리자에게는 MLE 기법을 사용하는 그룹 서명 기법은 OW-CPA 안전하지 않다.

이렇게 지역 연결자의 입장에서 MLE 기법이 사용된 그룹 서명 기법이 갖는 암호학적으로 증명된 보안성과 현실에서의 보안성이 일치하지 않는 상황이 벌어질 수도 있는 이유는 사용자의 식별자가 일반 메시지와 성질이 다르기 때문이다. 사용자의 식별자는 그룹

의 크기에 따라서 다항 시간에 처리할 수 있는 정보인데 반해서, 일반 메시지는 다항 시간에 처리할 수 없는 정보이다. 이러한 고찰은 기존의 공개키 암호문에서 정형화되어 사용되고 있는 '보안 목적과 공격자의 능력'에 대한 증명 방법을 그룹 서명 기법에 그대로 적용하는 것이 올바른가에 대한 의문을 낳는다.

하지만 이러한 의미를 강전일 등과 황정연 등의 논문[9,10]에서 변형되어 사용하는 해당 그룹 서명 기법이 본래의 그룹 서명 기법과 비교하여 보안적 측면에서 문제가 있다고 받아들이는 것은 바람직하지 않다. 일반적으로 그룹 서명 기법에서 익명취소 관리자에게 그룹 서명 기법이 어떠한 보안성도 갖고 있지 않다고 해서 그룹 서명 기법이 보안에 문제가 있다고 말하지 않는다. 지역 연결 관리자는 익명취소 관리자에게 일정한 권한을 양도받은 특별 관리자 중에 하나임에 주의해야 한다. 또한 동적 그룹 서명 기법 모델[15]에서 멤버십 관리자와 익명취소 관리자의 신뢰성에 따라 성취가 불가능한 보안 요구 사항이 존재한다는 사실에 주목할 필요가 있다.

따라서 강전일 등과 황정연 등의 제안[9,10]과 같이 지역 연결성을 갖는 그룹 서명 기법에서는 정상적인 사용자의 식별자는 반드시 비밀로 남아 있어야 한다. 그렇지 않고 사용자의 식별자를 공개해야만 하는 경우라면, 지역 연결성은 확보하기 힘들다.

V. 결론

이 논문에서는 수정된 LE 기법을 이용하여 지역 연결성을 갖도록 한 그룹 서명 기법에 대해서 연구하였다. 기존의 연구[9,10]에서는 미흡했던 지역 연결성의 성질 및 프라이버시 요구 사항에 대해서 고찰하고, 새롭게 도입되는 특수 관리자인 지역 연결자가 갖는 보안성에 대해서 분석하였다. 지역 연결성은 사용자의 식별자가 공개되지 않은 환경에서 일반 사용자들은 지역 연결 관리자에게 OW-CPA한 익명성을 갖게 된다.

지역 연결성에 대해서 더 잘 알게 되었다고, 실제로 지역 연결성을 더 이용하기 쉬워진 것은 아니다. 원래 추상적인 응용 환경을 위해서 만들어진 그룹 서명 기법처럼 추적 가능 서명 또한 추상적인 응용 환경에서의 문제점을 지적하고 만들어졌다. 마찬가지로 지역 연결성 또한 이러한 응용 환경을 위해서 만들어졌다고 볼 수 있다. 많은 암호학적 구성요소들이 현실 세계에서의 적합한 응용 환경을 찾지 못하는 것처럼 지역 연결성을 갖는 그룹 서명 기법 또한 마찬가지일지 모른다. 그렇다하더라도 지역 연결성을 갖는 그룹 서명 기법이 사용될 가능성을 열어놓고 적합한 환경을 찾고 필요에 따라 기법을 수정하여 사용할 수 있도록 노력하는 것이 앞으로 우리가 해결해야할 과제일 것이다.

참고문헌

[1] D. Chaum and E. van Heyst, "Group signatures," EUROCRYPT '91, LNCS 547. pp. 257-265, 1991.

[2] X. Lin, X. Sun, P-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," IEEE Transactions on Vehicular Technology, Vol. 56, No. 6. pp. 3442-3456, Nov. 2007.

[3] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," IEEE Transactions on Vehicular Technology, Vol. 59, No. 2, pp. 559-573, Feb. 2010.

[4] J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," Proceedings of the 19th USENIX Security Symposium, pp. 203-215, pp. 63-78. Aug. 2010.

[5] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks," IEEE Transactions on Distributed Systems, Vol. 21, No. 2, pp. 203-215, Feb. 2010.

[6] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," CRYPTO '04, LNCS 3152, pp. 41-55, 2004.

[7] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proceedings of the 11th ACM conference on Computer and Communications Security, pp. 168-177, Nov. 2004.

〔8〕 A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," EUROCRYPT '04, LNCS 3027, pp. 571-589, 2004.
〔9〕 강전일, 양대헌, 이석준, 이경희, "실생활 응용을 위한 짧은 그룹 서명 기법(BBS04)에 대한 연구", 정보보호학회논문지, 19(5), pp. 3-15, 2009년 10월.
〔10〕 황정연, 이석준, 정병호, 양대헌, "지역 연결성을 제공하는 효율적인 그룹 서명 기법", 대한전자공학회 하계종합학술대회발표집, pp. 863-865, 2010년 6월.
〔11〕 J. Camenisch, S. Hohenberger, and A. Lysyanskaya. "Compact E-cash," EUROCRYPT '05, LNCS 3494, pp. 302-321, 2005.
〔12〕 G. Ateniese, J. Camenisch, and B. de Medeiros. "Untraceable RFID Tags Via Insubvertible Encryption," Proceedings of the 12th ACM conference on Computer and Communications Security, pp. 92-101, Nov. 2005.
〔13〕 M. Naor and M. Yung, "Universal One-Way Hash Functions and Their Cryptographic Applications," Proceedings of the 21st Annual ACM Symposium on Theory of Computing, pp. 33-43. May 1989.
〔14〕 M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and A Construction Based on General Assumptions," EUROCRYPT '03, LNCS 2656, pp. 614-629, 2003.
〔15〕 M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The case of Dynamic Groups," CT-RSA '05, LNCS 3376, pp. 136-153, 2005.
〔16〕 G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-resistant Group Signature Scheme," CRYPTO '00, LNCS 1880, pp. 255-270, 2000.
〔17〕 C. Delerablée and D. Pointcheval, "Dynamic Fully Anonymous Short Group Signatures," VIETCRYPT '06, LNCS 4341, pp. 193-210, 2006.
〔18〕 T. Makita, Y. Manabe, and T. Okamoto, "Short Group Signatures with Efficient Flexible Join," Proceedings of the 2006 Symposium on Cryptography and Information Security, Jan. 2006.
〔19〕 X. Boyen and B. Waters, "Compact Group Signatures Without Random Oracles," EUROCRYPT '06, LNCS 4004, pp. 427-444, 2006.
〔20〕 X. Boyen and B. Waters, "Full-Domain Subgroup Hiding and Constant-Size Group Signatures," Public Key Cryptography (PKC) '07, LNCS 4450. pp. 1-15. 2007.
〔21〕 J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups (Extended abstract)," CRYPTO '97, LNCS 1294, pp. 410-424, 1997.
〔22〕 Jan Camenisch, "Efficient and Generalized Group Signatures," EUROCRYPT '97, LNCS 1233, pp. 465-479, 1997.
〔23〕 J. Camenisch and M. Michels, "A Group Signature Scheme with Improved Efficiency (Extended Abstract)," ASIACRYPT '98, LNCS 1514, pp. 160-174, 2000.
〔24〕 S.D Galbraith and V. Rotger, "Easy decision-Diffie-Hellman groups," Cryptology ePrint Archive, Report 2004/070, 2004.
〔25〕 A. Miyaji, M. Nakabayashi, and S. Takano. "New Explicit Conditions of Elliptic Curve Traces for FR-reduction," IEICE Transactions on Fundamentals, Vol. E84-A, No. 5, pp. 1234-1243, 2001.
〔26〕 G. Ateniese, D. Song, and G. Tsudik, "Quasi-Efficient Revocation of Group Signatures." Financial Cryptography (FC) '02, LNCS 2357, pp. 183-197, 2002

〈著者紹介〉

강 전 일 (Jeonil Kang) 학생회원
2003년 2월: 인하대학교 컴퓨터 공학과 졸업
2006년 2월: 인하대학교 정보통신대학원 석사
2006년 3월~현재: 인하대학교 정보공학과 박사 과정
〈관심분야〉 RFID 보안, 생체 인식 보안, 무선 센서 네트워크 보안, 무선 인터넷 보안, 웹 인증 보안, 암호 프로토콜

김 기 태 (Kitae Kim) 정회원
1997년 2월: 건양대학교 수학과 졸업
2000년 2월: 인하대학교 수학과 석사
2009년 8월: 인하대학교 수학과 박사
2009년 9월~2010년 8월: 인하대학교 정보통신대학원 박사 후 연구원
2010년 9월~현재: 인하대학교 수학과 강의교수
〈관심분야〉 전자서명, 암호분석, 대수적 정수론

양 대 헌 (DaeHun Nyang) 정회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터정보공학부 부교수
〈관심분야〉 암호 이론, 암호 프로토콜, 인증 프로토콜, 무선 인터넷 보안

이 경 희 (Kyunghee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 전기공학과 조교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 패턴인식