情報保護學會論文誌
第14券 第1號, 2004. 2

그룹서명을 이용하여 익명성이 보장되는 디지털 권한 전달 시스템

주 학 수,[a)†] 김 대 엽,[b)‡] 이 동 훈[c)]

한국정보보호진흥원,[a)] 삼성 종합기술원,[b)] 고려대학교 CIST[c)]

An Anonymous Rights Trading System using group signature schemes

Hak-Soo Ju,[a)†] Dae-Youb Kim,[b)‡] Dong Hoon Lee[c)]

KISA,[a)] SAIT,[b)] CIST[c)]

요 약

전자상거래가 일상생활에서 급격히 확산되고 있다. 그 중 하나의 분야가 티켓, 쿠폰, 라이센스 등과 같은 권한(rights)을 발행·전달해주는 디지털 권한·전달 시스템이다. 현재까지 제안된 디지털 권한 전달 시스템은 크게 디지털 권한을 계좌의 형태로 관리하는 계좌 기반 방식(온라인 방식)과 디지털 권한을 스마트카드에 저장하여 전달하는 스마트카드 기반 방식(오프라인 방식)으로 분류할 수 있다. 최근 NTT는 스마트카드 기반 권한 전달 시스템에서 권한의 복사방지를 할 수 있는 기능을 제공하는 FlexToken 시스템을 제안하였다.[1,2] 이들의 방식에서는 사용자들의 익명성을 보장하기 위해 Petersen과 Horster의 방식[3]을 사용할 것을 제안하였다. 그러나, Petersen과 Horster의 방식은 사용자들이 불연계성(unlinkablity)을 만족하는 서명을 생성하기 위해 매번 다른(one-time) 공개키와 개인키 쌍(pseudonym public key/secret key)을 생성하여 등록해야 하는 문제점이 있다. 이러한 문제점을 해결하기 위해, 본 논문에서는 그룹서명을 사용하여 익명성이 보장되는 디지털 권한·전달 시스템을 제안하고자 한다. 이 논문은 디지털 권한·전달 시스템에 스마트카드기반 그룹서명을 처음 적용하였다는 점에서 의의가 있다.

ABSTRACT

E-Commerce is suddenly spreading in a daily life. A rights trading system is a system that circulates digital-tickets such as plane tickets, software license, coupon. There are two main approaches so far : account-based and smart-card based systems. The NTT proposed FlexToken, a new smart card based copy prevention scheme for digital rights.[1,2] They proposed using pseudonymous self certified keys of Petersen and Horster[3] in order to ensure anonymity of users. However, Petersen and Horster 's scheme should register a pseudonymous key pair at TTP (One-time) every time so that users create the signature which is satisfied with unlinkability property. In this paper, we propose a new anonymous rights trading system using group signature. This paper has a meaning having applied to digital rights trading system an efficient smart card based group signature.

Keywords: *Digital Rights, Group Signature, Anonymity, Unlinkability*

Ⅰ. 서 론

현재 인터넷에서의 전자상거래는 가장 화제가 되는 부분이다. 상품을 주문하고 이벤트를 예약하고 은행계좌를 관리하는 등 모든 부분이 인터넷을 통해 이루어지고 있다. 이 때 상품이나 서비스를 살 수 있는 권리를 디지털 형태로 표현하여 전달해주는 시스템을 디지털 권한(혹은 티켓이라 함) 전달 시스템이라고 한다.

접수일: 2003년 7월 19일; 채택일: 2004년 1월 8일
† 주저자, hsju@kisa.or.kr
‡ 교신저자, daeyoub.kim@samsung.com

현재까지 제안된 디지털 권한(티켓) 전달 시스템은 크게 디지털 권한을 계좌의 형태로 관리하는 계좌 기반 방식(온라인 방식)[4]과 디지털 권한을 스마트카드에 저장하여 전달하는 스마트카드 기반 방식(오프라인 방식)[1]으로 분류할 수 있다. 대부분의 온라인 방식은 디지털 권한(티켓) 정보가 계좌(accounts)의 형태로 각 서비스 제공자(service provider)에 의해 관리된다. 따라서, 악의 있는 사용자들로부터 디지털 권한(rights)을 보호할 수 있지만 악의 있는 서비스 제공자 및 관리자에 의해 쉽게 변경 혹은 삭제될 수 있는 위험이 있다. 또한, 사용자들이 권한(rights)에 해당되는 컨텐츠를 이용하기 위해서는 먼저 해당 컨텐츠에 대한 권한(rights)을 받기 위해 온라인으로 매번 접속해야하는 불편함이 있다.

스마트카드 기반 방식의 경우, 온라인 방식의 문제점을 해결할 수 있었지만 스마트카드의 메모리 크기, CPU의 조건, 성능 등 제약된 환경적 제약으로 인하여 특정 응용환경에 따라, 매번 서비스 제공자에 따라 다른 스마트카드를 발급 받아야 하는 문제점이 있다. 현재 많은 디지털 권한(티켓)·전달 시스템들이 구축되었지만 대부분 특정부분의 어플리케이션만을 제공하고 있을 뿐 모든 티켓을 통합하여 제공할 수 있는 권한(티켓)·전달 시스템이 제안되지는 않았었다.[5~7]

최근 NTT는 모든 티켓들을 통합하여 하나의 스마트카드로 제공할 수 있는 디지털 권한(티켓) 전달 시스템 FlexToken 시스템을 제안하였다.[1] 그들은 사용자의 익명성을 제공하기 위해 Petersen과 Horster의 방식[3]을 사용하였다. Petersen과 Horster의 방식은 사용자들이 불연계성(unlinkablity)을 만족하는 서명을 생성하기 위해 매번 다른(one-time) 공개키, 개인키 쌍(pseudonym public key/secret key)을 생성하여 등록하여야 하는 문제점이 있다.

pseudonym을 사용하지 않으면서 익명성 및 불연계성을 제공하는 방법으로는 그룹서명이 있다. 본 논문에서는 그룹서명을 이용하여 익명성을 보장하는 새로운 디지털 권한·전달 시스템을 제안하고자 한다.

본 논문의 전체 구성은 다음과 같다. 2절에서는 디지털 권한·전달 시스템에 대한 기본구조 및 NTT의 FlexToken[1]방식에 대해 알아본다. 3절에서는 디지털 권한·전달 시스템에 익명성을 제공하기 위한 방법으로 NTT의 FlexToken방식에서 제시한 Petersen과 Horster의 방식에 대해 설명한다. 4절에서는 새롭게 제안하는 방법으로, 그룹서명을 이용하여 익명성을 보장할 수 있는 방법에 대해 설명한다. 5절은 기존에 제시된 방법들과 새롭게 제시한 방법과의 비교를 한다.

II. 기본개념

2.1 용어 정리

디지털 권한(Rights)이란 상품이나 서비스에 대한 권한을 주장할 수 있는 권리에 대한 디지털 표현이다.[2] 디지털 권한을 수식으로 표현하면

$$m = Sign_I(I, P, U) \quad (1)$$

로 정의할 수 있다. 여기서 I는 권한(티켓)을 생성하여 발행하는 발행자, U는 권한(티켓)에 대한 소유자를 말하며, P는 U에 대한 발행자 I의 약속(promise)을 나타낸다. P는 컨텐츠 구매 시 더해질 수 있는 마일리지 점수, 할인혜택, 할인비율, 비행기 티켓의 좌석 번호 등과 같은 발행자가 사용자에게 약속하는 내용이 될 수 있다. 디지털 권한(rights)의 전체적인 권한흐름 및 전체 프로토콜은 다음과 같이 구성된다.

- 발행(Issue) 프로토콜: 발행자가 디지털 권한을 생성하여 사용자에게 생성한 권한의 소유권을 주는 프로토콜이다.
- 전달(Transfer) 프로토콜: 사용자가 자신이 갖고 있는 권한에 대한 소유권을 다른 사용자에게 전달하는 프로토콜이다.
- 상환(Redemption) 프로토콜: 권한에 대한 소유권을 갖고 있는 사용자가 권한을 서비스 제공자(service provider)에게 반납하고 그에 대한 서비스/컨텐츠를 제공받는 프로토콜이다. 상환하는 방식에 따라, 라이센스 혹은 여권처럼 소유권이 사용자에게 계속남아 있게 하는 제시(presentation) 프로토콜과, 비행기 티켓, 게임 티켓, 전화 카드

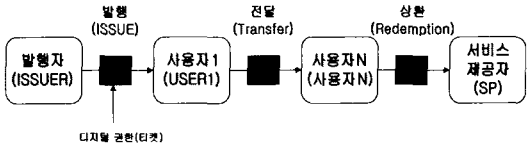


그림 1. 디지털 권한(티켓)의 흐름도

처럼 다 사용되었을 경우 그에 대한 소유권이 소멸되는 소비(consumption) 프로토콜로 분류할 수 있다.

이러한 디지털 권한(티켓) 전달 시스템의 안전성 및 편리성을 보장하기 위한 요구조건은 다음과 같다.[2]

- ㅇ 다양한 형태의 권한(Various types of rights): 특정 화폐를 다루는 전자화폐시스템과 달리 다양한 형태의 권한(rights)을 다루어야 한다.
- ㅇ 다양한 발행자(Different issuers): 중앙은행과 같은 특정 발행자가 발행하는 화폐를 다루는 전자화폐 시스템과 달리, 시스템은 많은 발행자들이 발행하는 디지털 권한(rights)을 다루어야만 한다.
- ㅇ 위조방지(Preventing forgery): 발행자만이 유효한 디지털 권한을 발행할 수 있다.
- ㅇ 변경방지(Preventing alteration): 디지털 권한은 권한 소유자가 다시 결정되는 전달(transfer) 프로토콜을 제외한 다른 프로토콜에서는 변경되어서는 안된다.
- ㅇ 이중사용방지(Preventing duplicate-redemption): 디지털 권한은 이중 상환되어서는 안 된다.
- ㅇ 부인봉쇄(Non-repudiation): 발행자가 발행을 부인하고, 권한이 발급된 후 권한 소유자가 권한의 전달 혹은 상환한 내역을 부인할 수 없다.
- ㅇ 프라이버시 보장(Ensuring privacy): 권한에 대한 현재 그리고 이전의 소유권자가 그 이후의 권한자에게 숨겨져야 한다.

이외에도 실제적인 구현 측면에서 가변성(scalability), 효율성(efficienty), 간결성(simplicity) 등의 요구조건이 있지만, 이 논문에서는 이를 다루지 않는다[더 자세한 요구조건은 [2]을 참조].

2.2. NTT의 FlexToken 시스템[1]

이 절에서는 스마트카드를 사용하여 앞 절에서 언급된 디지털 권한들의 요구조건들을 만족하면서, 발급된 권한에 대한 복사방지를 제공하는 NTT의 디지털 권한 전달 시스템 FlexToken에 대해 간략히 설명하고자 한다.

디지털 권한을 하나의 전자화폐로 생각하여 Mondex, VISA 등과 같은 전자화폐 시스템을 변형하여 권한·전달 시스템으로 설계할 수 있지만, 이 경우 다음과 같은 문제점들이 존재하게 된다.

첫째, 디지털 권한은 화폐와 달리 다양한 형태의 권리가 존재한다. 따라서 다양한 권한을 발급 받을려면 사용자는 권한에 따라 각각 다른 스마트카드를 발급받아야 한다. 다양한 권한의 형태를 모두 하나의 스마트카드에 저장하여 이 문제를 해결할 수 있으나 스마트카드의 메모리 및 CPU의 제약 때문에 비효율적이다.

둘째, 전자화폐는 스마트카드 발행자가 미리 선택한 발행자가 발급한 화폐의 형태만을 다루지만 디지털 권한에 대한 발행자는 권한에 따라 각각 다른 발행자가 존재하게 된다.

이러한 문제들을 해결하기 위해 FlexToken시스템은 디지털 권한을 두 개의 다른 정보인 권한 명세서(rights definition)와 토큰(token)정보로 분할한다. 권한 명세서는 권리에 대한 내용 및 조건을 나타내고, 토큰정보는 권한에 대한 소유자의 유일성을 보장해 준다. 토큰은 스마트카드와 같은 물리적 보안장치에 저장되어 있는 정보로, 권한 명세서가 토큰에 의해 검증이 될 때에만 디지털 권한은 유효하게 된다.

참석자는 권한을 발행해주는 발행자(I: Issuer), 스마트카드의 물리적 보안능력을 보장해주는 보증자(G: Guarantor), 사용자들(U: $User_1$, $User_2$,..., $User_N$), 서비스 제공자(Service Provider 혹은 Collector)들이 있으며, 참석자들은 각각 공개키와 개인키 쌍 (pk_X, sk_X)을 갖고 있다고 가정한다(단, $X \in \{I, G, U, C\}$를 말함). 전체 프로토콜은 발행 프로토콜, 전달 프로토콜, 상환 프로토콜로 구성되어 있으며, 상세 프로토콜은 다음과 같다.

ㅇ 기호

- $H(\cdot)$: SHA1, MD5등과 같은 해쉬함수를 말한다.
- $Sign_{sk_X}(m)$: 메시지 m에 대한 개인키 sk_X의 서명을 나타낸다.
- $Ver_{pk_X}(m, sig)$: 공개키 pk_X에 대한 메시지 m에 대한 서명 $Sign$의 검증함수를 말한다.
- 권한 명세서 m: 상품이나 서비스에 대한 권한을 주장할 수 있는 권리에 대한 디지털 표현이며 $m = Sign_{sk_I}(I, P, U)$으로 정의되고, XML이 주로 사용된다.
- 토큰 T: (t_1, t_2)의 2개의 정보로 구성되며, t_1은 권한 명세서 m에 대한 해쉬값이고, t_2는 디지털 권

한의 발행자를 나타내는 발행자의 해쉬값을 말한다. 토큰 $T=(H(m), H(pk_I))$를 자신의 스마트카드에 갖고 있는 사용자가 m과 발행자 I에 대응되는 디지털 권한의 소유자로 간주된다.

- 챌린지 c: (c_1, c_2)의 두 개의 값으로 구성되며, c_1은 수신자의 해쉬값이고, c_2는 수신자가 생성하는 세션마다 새롭게 생성되는 일련번호 s로 송신자가 토큰을 재사용하는 것을 방지하기 위해 사용된다.
- 응답값 r: (r_1, r_2)의 두 개의 값으로 구성되며, r_1은 수신자의 챌린지 값에 대한 서명값이며, r_2는 수신자의 공개키 정보이다. 이 정보는 토큰 정보가 수신되었다는 것을 나타내며, 수신자의 부인봉쇄를 막기 위한 정보로 사용된다.
- (g_1, g_2): 스마트 카드에 저장되어 있는 공개키에 대한 신뢰할 수 있는 제3자인 보증자(G: guarantor)의 인증정보로, g_1은 스마트카드의 공개키에 대한 보증자의 서명값 $Sign_{sk_G}$를 나타내고 g_2는 보증자의 공개키 pk_G를 의미한다.

○ 발행(Issue) 프로토콜

단계 1: a_1정보는 발행자가 신뢰하는 스마트카드 보증자의 리스트 $\{H(pk_{G_1}), H(pk_{G_2}), \ldots, H(pk_{G_n})\}$이며, $Sign_{sk_I}(a_1)$과 pk_I 정보에 의해 변경되지 않는다. 발행자 I는 m, a_1, $Sign_{sk_I}(a_1)$, pk_I를 사용자 U에게 전달하면, 사용자 U는 $Sign_{sk_I}(a_1)$를 검증한 뒤, 검증이 성립하면 챌린지 $c_U=(H(pk_U), s)$를 생성하여 발행자에게 전달한다. 챌린지에 사용된 s는 세션마다 새롭게 생성되는 일련번호로 송신자가 토큰을 재사용하는 것을 방지하기 위해 사용된다.

단계 2: I는 챌린지 c_U를 검증한 뒤, 검증이 성립하면 토큰정보 $(H(m), H(pk_I))$와 사용자로부터 온 챌린지 $(H(pk_U), s)$, 그에 대한 서명값 $Sign_{sk_I}(H(m), H(pk_I), H(pk_U), s)$을 생성하여 pk_I와 함께 사용자에게 보낸다.

단계 3: 사용자는 수신된 $H(pk_U)$와 s의 값이 챌린지 c_U와 같은지를 검증하여 챌린지의 유효성을 검증한다. 또한, $H(pk_I)$를 계산하여 송신된 $H(pk_I)$ 값과 같은지를 검증하고, 서명 $Sign_{sk_I}$를 검증함으로써 디지털 권한을 발행해주는 발행자 I를 검증하게 된다.

단계 4: 모든 검증이 성공하면 사용자는 일련번호들의 집합 S_U로부터 일련번호 s를 삭제한 뒤 토큰 $T=(H(m), H(pk_I))$를 저장하게 된다. 그리고 나서 그에 대한 응답값 $R_U=(r_1, r_2)=(Sign_{sk_U}(c_U), pk_U)$를 생성하여 I에게 보낸다.

단계 5: I는 R_U에 포함되어 있는 서명 $Sign_{sk_U}(c_U)$를 검증하여 응답값이 이 거래에 해당된다는 것과 r_2의 사용자가 생성한 값이라는 것을 확인하게 된다. 또한, $r_2=H(pk_U)$가 c_U의 $H(pk_U)$와 같은지를 검증하여 r_2의 생성자가 챌린지 c_1의 생성자와 같다는 것을 확인하게 된다.

위의 챌린지-응답 프로토콜을 통해, 사용자는 권한 정의 m에 대응되는 유일한 소유정보 토큰 T를 발급 받아 안전한 스마트 카드 안에 저장하면 발행 프로토콜은 종료된다.

○ 전달(Transfer) 프로토콜

디지털 권한 전달 프로토콜은 I가 발행한 디지털 권한 m을 U_1이 U_2에게 전달하는 프로토콜로써, 발행 프로토콜 방식과 유사하게 챌린지-응답 프로토콜로 진행된다. 세부 프로토콜은 다음과 같다.

단계 1: 사용자 U_1은 디지털 권한명세서 m과 스마트카드 보증자의 리스트 및 그에 대한 서명값 a_1, $Sign_{sk_I}(a_1)$, pk_I, 그리고 스마트카드에 대한 보증자의 인증정보 $(g_1, g_2)=(Sign_{sk_G}(pk_{U_1}), pk_G)$를 사용자 U_2에게 전달한다.

단계 2: 사용자 U_2는 서명값들을 검증한 뒤, 검증이 성립하면 챌린지 $c_{U_2}=(c_1, c_2)=(H(pk_{U_2}), s)$를 생성하여 U_1에게 전달한다.

단계 3: U_1은 저장되어 있는 토큰 T를 삭제하고 발행 프로토콜과 유사한 이유로, $H(m)$, $H(pk_I)$, c_1, c_2, $Sign_{sk_{U_1}}(H(m)||H(pk_I)||c_1||c_2)$, pk_{U_1}을 생성하여 U_2에게 전달한다.

단계 4: U_2는 c_1과 c_2가 자신이 보낸 챌린지 c와 같은지 검증하여 챌린지의 유효성을 검증한 뒤, $Sign_{sk_{U_1}}$을 확인하여 보내준 정보가 사용자 U_1이 생성하였다

는 것을 검증한다. 또한, $g_1 = Sign_{sk_G}(pk_{U_1})$을 검증하여 보증자 g_2가 사용자 U_1의 스마트카드 물리적 보안능력을 보장하고 있다는 것을 검증하게 된다. 그리고 $H(g_2)$가 a_1에 있는지를 검증하여 보증자가 I가 선택한 보증자의 리스트에 있는 정당한 보증자인지를 확인하고, $H(pk_I)$를 계산하여 전달된 값과 비교함으로써 토큰 발행자의 유효성을 검증하게 된다. 검증이 성립하면, 세션번호 s를 S_{U_2}로부터 삭제한 뒤 토큰 T를 저장하고 나서, 그에 대한 응답값 $R_{U_2} = (Sign_{sk_{U_1}}(c_{U_2}), pk_{U_2})$을 생성하여 U_1에게 보낸다.

단계 5: U_1은 발행 프로토콜에서와 유사하게 R_{U_2}를 검증한 뒤, $H(m)$, $H(pk_I)$, c_1, c_2, pk_{U_1}, $Sign_{sk_{U_1}}(H(m)\|H(pk_I)\|c_1\|c_2)$의 복사본을 삭제한다.

○ 상환(Redemption) 프로토콜

사용자와 서비스제공자(Service Provider) 사이의 상환 프로토콜은 사용자들 사이의 거래 프로토콜과 유사하다. 단, 챌린지 c가 소비(comsumption) 프로토콜인지 혹은 제시(presentation) 프로토콜인지를 분류하기 위해 음수와 양수로 각각을 구분해서 처리한다. 예를 들어, 소비 프로토콜을 하기 위해서 챌린지 값을 양수로 정한다면 제시 프로토콜에서는 음수 값으로 챌린지를 선택한다. 응답 프로토콜까지 프로토콜이 성공하면, 상품 혹은 서비스(Goods/Service)가 서비스제공자(혹은 컬렉터)로부터 사용자에게 전달되는 것으로 종료된다. 서비스와 그에 대한 지불체계가 이루어져야 하지만 이 범위는 이 논문의 영역을 벗어나기 때문에 다루지 않는다.[1]

제안된 방식은 토큰의 재사용방지, 도청 등의 공격에 안전하게 하기 위해 챌린지-응답 프로토콜을 기반으로 설계되었다. 그리고 디지털 권한의 위변조를 방지하기 위해 물리적 보안능력이 보장되는 스마트카드와 전자서명, 해쉬함수의 안전성에 의존하고 있다.

그러나, 권한(rights)의 송신자가 권한을 수신자에게 전달할 때 송신자의 서명 값이 검증되어야 하기 때문에, 수신자는 송신자의 공개키를 알고 있게 된다. 소유자들의 공개키들이 알려지게 되기 때문에 익명성이 보장되지 않는다. Flextoken방식에서는 사용자의 공개키와 카드소유자를 연결(link)시키지 않도록 함으로써, 프라이버시를 향상시키는 방법으로 Petersen과 Horster의 방식[3]을 사용할 것을 제안하였다.

Ⅲ. Petersen and Horster의 방식[3]을 사용한 익명성을 보장하는 디지털 권한 · 전달 시스템

Petersen과 Horster의 방식을 간략히 설명하면 다음과 같다. 먼저 사용자는 익명(pseudonym)에 해당하는 (sk^*, pk^*)을 생성하여 TTP에 제공하면, TTP가 서명을 함으로써 익명(pseudonym)에 해당되는 인증을 받게 된다. 이 방식은 TTP만이 사용자의 ID정보와 익명(pseudonym)정보를 연결시킬 수 있음으로 해서 사용자의 익명성을 제어할 수 있는 방식이다.

이 방식을 권한 · 전달 시스템에 적용한다면, Flex-Token의 전체 프로토콜에서 사용되는 공개키/개인키 쌍 (sk, pk)을 익명(pseudonym)에 해당하는 (sk^*, pk^*)로 변환하면 된다. 이 방법은 공개키 정보가 노출되지 않아, 사용자의 익명성을 제공해 줄 수 있지만, 같은 익명(pseudonym), (sk^*, pk^*)을 두 번 이상 사용하게 되면 사용자의 정보들이 연결(linkable)되어 추적되는 문제점이 있다. 따라서, 불연계성(unlinkablility)을 만족하면서 사용자의 익명성을 보장하기 위해서는 사용자는 매번 다른 익명(pseudonym)정보를 생성해서 TTP에 등록하여야 한다.

Ⅳ. 그룹서명을 사용하여 익명성을 보장하는 디지털 권한 · 전달 시스템

익명성 및 불연계성(unlinkability)을 제공하는 다른 방법으로는 그룹서명이 있다. 이 절에서는 그룹서명을 이용하여 익명성을 보장하는 새로운 디지털 권한 · 전달 시스템을 제안하고자 한다.

4.1 그룹서명

그룹서명은 1992년 Chaum과 van Heijst[8]에 의해 처음 제안된 개념으로 그룹에 속한 구성원이 그룹을 대표하여 서명하는 기법을 말한다. 그룹서명기법에서 그룹 구성원에게 서명 권한을 부여하는 것은 그룹관리자에 의해 이루어지며 각 구성원이 발행하는 서명에 대해서는 익명성이 보장된다. 이 때 서명된 문서는 그룹의 공개키에 의하여 서명이 검증되며 분쟁이 발생하는 경우에는 그룹관리자만이 구성원의 신분을 밝혀낼 수 있는 기법이다. 효율적인 그룹서명을 위해, 그룹서명의 길이와 그룹의 공개키가

그룹의 크기와 구성원의 변동과 독립적으로 운영할 수 있도록 설계된 다양한 그룹서명들이 제시되었다.[9-12] 안전성 측면에서 그룹에 속한 소속원들이 공모하여 새로운 인증서를 만들어 서명을 생성할 수 있는 공모공격에 강인한 기법들도 제시되었다.[13] 그러나, 이들 방식들은 서명생성 및 공모공격에 강인하기 위해 많은 계산량이 필요하다는 문제를 여전히 갖고 있다. 최근 이러한 문제들을 해결하기 위해 스마트카드를 이용하여 그룹서명을 생성하는 방법이 제시되었다.[14] 본 논문에서는 이 기법을 기반으로 오프라인 디지털 권한(티켓) 전달 시스템을 설계하고자 한다.

〈정의1 : 그룹서명〉

그룹서명이란 다음의 성질을 만족하는 전자서명을 말한다.

① Correctness: 그룹소속원이 생성한 서명은 항상 유효하다.
② Unforgeability: 그룹소속원만이 그룹을 위해 서명을 생성할 수 있다.
③ Anonymity: 그룹매니저를 제외한 누구도 그룹 서명으로부터 서명자가 누구인지를 알 수 없어야 한다.
④ Unlinkability: 두 개의 다른 유효한 서명이 같은 동일한 그룹 소속원에 의해 서명되었다는 것을 결정하는 것이 불가능해야 한다.
⑤ Exculpability: 그룹맴버 혹은 그룹매니저는 다른 그룹 소속원을 대신하여 서명할 수 없어야 한다.
⑥ Traceability: 그룹매니저는 항상 서명으로부터 서명자의 익명성을 개봉할 수 있다.
⑦ Coalition-Resistance: 그룹소속원들의 공모는 그룹매니저로 하여금 공모한 소속원들 중 적어도 한명을 추적할 수 없도록 하는 서명을 생성할 수 없어야 한다.

〈스마트카드 기반 그룹서명 방식[14]〉

[14]에서 제안하고 있는 방식은 스마트카드와 그룹이 공유하는 개인키를 사용하는 것으로 구성된다. 먼저 개인키와 공개키 쌍 (sk_G , pk_G) 이 있는 전자서명 스킴 SA와 개인키와 공개키 쌍 (D_{Aut} , E_{Aut}) 이 있는 확률론적 암호시스템 EA를 가정한다. 그룹매니저는 개인키 D_{Aut}를 자신만의 비밀로 유지하고

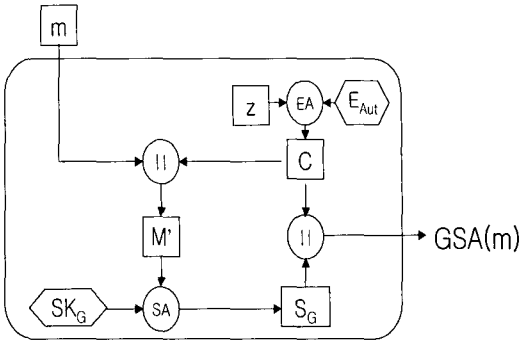


그림 2. 스마트카드 기반 그룹서명 방식

개인키 sk_G는 그룹소속원들과 공유하게 되며, 그에 대한 공개키들 pk_G와 E_{Aut}는 공개한다.

사용자가 그룹멤버가 되고 싶다면 그룹매니저로부터 먼저 스마트카드를 발급 받는다. 그리고 그룹매니저로부터 식별자 z와 모든 그룹멤버들에게 공유되어 있는 공유된 개인키 sk_G를 얻어야 한다. 사용자의 스마트카드는 암호시스템과 전자서명을 사용할 수 있는 모든 파라미터에 대한 접근권한을 갖고 있어야만 한다. 단, 그룹 매니저만이 식별자 z와 그룹 멤버의 Id의 연결을 기억하고 있다.

사용자가 메시지에 그룹멤버로서 서명하고자 할 때 자신의 스마트카드를 사용한다. 먼저 식별자 z 는 그룹 매니저의 공개키 E_{Aut}로 암호화된다. 그리고 나서 메시지 m은 암호화된 값 C와 연접되고 연접된 값은 공유된 개인키 sk_G로 전자서명 알고리즘 SA를 사용하여 서명하게 된다. 전체 그룹서명을 할 수 있는 스마트카드의 구조는 다음과 같다.

- EA: 안전한 확률론적 공개키 암호시스템 (개인키 : D_{Aut}, 공개키 : E_{Aut})
- SA: 공유된 개인키 sk_G로 서명될 전자서명 알고리즘
- z: 사용자 식별정보
- ||: Concatenation
- GSA(m): 메시지 m에 대한 그룹서명

4.2 제안방식

제시하고자 하는 방법의 기본적인 생각은 스마트카드를 발행해주는 보증자 $G_1, G_2, \ldots, G_n$을 그룹매니저들로 생각하고, 사용자들을 그룹에 속한 소속원으로 생각하는 것이다. 이 방식에서는 pk_{G_i}를 각

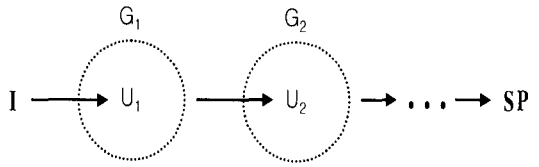


그림 3. 그룹서명에 이용하여 새롭게 제안하는 모델

그룹들의 공개키로 생각하고 각 사용자들의 스마트카드에는 그룹서명 시 사용하기 위한 공유 개인키 정보인 sk_{G_i}들이 저장되어 있다는 것을 가정한다. sk_{G_i}는 그룹에 속한 사용자들이 공유해야 한다.

전체적인 권한 전달 모델은 그림과 같다.

사용자들은 자신이 어떠한 그룹에 소속되었는지를 전달할 뿐, 자신의 공개키 정보를 전달하지는 않는다.

○ 발행(Issue) 프로토콜

이 프로토콜은 발행자 I가 비밀키 sk_{G_i}를 저장하고 있는 스마트카드 사용자 U에게 디지털 권한을 발급해주는 프로토콜로, 기본 방법은 FlexToken의 방식처럼 챌린지-응답프로토콜을 기반으로 한다.

단계 1: 발행자 I는 m, a_1, $Sign_{sk_I}(a_1)$, pk_I를 사용자 U에게 전달한다. a_1은 발행자가 신뢰하는 스마트카드 보증자 그룹공개키들의 리스트 $\{H(pk_{G_1}), H(pk_{G_2}), \ldots, H(pk_{G_n})\}$이며, 이는 $Sign_{sk_I}(a_1)$정보에 의해 변경되지 않는다.

단계 2: 사용자 U는 $Sign_{sk_I}(a_1)$ 대한 발행자의 서명을 검증하고 자신의 개인키 sk_{G_i}에 해당하는 공개키 pk_{G_i}의 해쉬값 $H(pk_{G_i})$를 계산하여, 계산 결과값이 a_1의 리스트에 있는지를 검증한다. 검증이 성립하면 $H(pk_{G_i})$와 일련번호 $s \in S_U$를 생성하여 만든 챌린지 c_U: $(c_1, c_2) = (H(pk_{G_i}), s)$를 발행자 I에게 전송한다.

단계 3: 발행자 I는 $E_I = (e_1, e_2, e_3, e_4, e_5, e_6)$를 생성하여 사용자 U에게 전달한다. 단, $e_1 = H(m)$, $e_2 = H(pk_I)$, $e_3 = c_1$, $e_4 = c_2$, $e_5 = S_{sk_I}(e_1 \| e_2 \| e_3 \| e_4)$, $e_6 = pk_I$. I는 트랜잭션이 끊어지는 경우를 대비하여, E_I의 백업 복사본을 응답(Receipt)이 올 때까지 저장하고 있다.

단계 4: 사용자는 U는 E_I를 다음과 같이 검증한다.

① $e_4 \in S_U$

② $e_3 = H(pk_{G_i})$

③ $Ver_{e_6}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1$

④ $e_2 = H(e_6)$

①,②는 챌린지의 유효성을 검증하는 것을 의미하고, ③은 E_I가 I에 의해 생성되었다는 것을 보증한다. ④는 I가 m을 발행하였다는 것을 보장한다. 검증이 성공하면, U는 S_U로부터 일련번호 e_4를 삭제하고 토큰 $T = (t_1, t_2) = (e_1, e_2) = (H(m), H(pk_I))$를 저장한다. 응답값에 해당하는 $R_U = (r_1, r_2) = (GSig_{sk_{G_i}}(c_U), pk_{G_i})$를 생성하여 발행자 I에게 전달한다. 여기서, 그룹서명 $GSig_{sk_{G_i}}(c_U)$은 4.1절의 스마트카드 기반 그룹서명에 기반하고 있기 때문에 다음과 같이 구성되어 있다.

$$GSig_{sk_{G_i}}(c_U) = Sign_{sk_{G_i}}(c_U \| E_{pk_{G_i}}(z)) \| E_{pk_{G_i}}(z)$$

단, z는 사용자의 식별자를 의미하며 pk_{G_i}는 그룹 매니저 즉 스마트카드 보증자의 공개키를 말한다.

단계 5: 발행자 I는 그룹서명 $GSig_{sk_{G_i}}(c_U)$를 검증함수 $GVer_{pk_{G_i}}(r_1)$를 사용하여 검증 확인함으로써 트랜잭션이 올바르게 진행되었다는 것을 확인한다. 또한, $H(r_2)$와 $H(pk_{G_i})$가 같은지를 검증함으로써, r_2의 생성자가 그룹 G_i에 속한다는 것을 검증한다. 검증이 성공하면 I는 E_I의 백업 복사본을 삭제하게 된다.

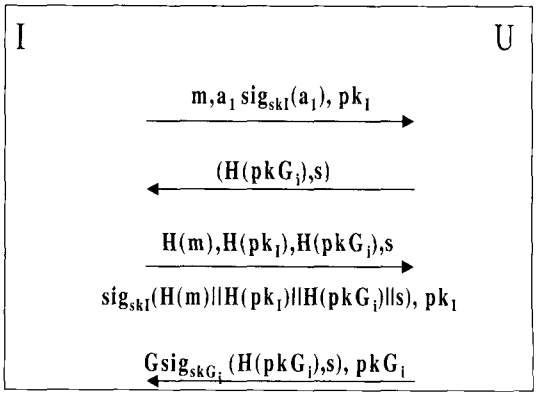


그림 4. 발행프로토콜

○ 전달(Transfer) 프로토콜

이 프로토콜에서는 개인키 sk_{G_i}가 들어있는 스마트카드를 갖고 있는 사용자 U_1이 sk_{G_j}가 탑재된 스마트카드를 갖고 있는 사용자 U_2에게 디지털 권한을 전달하는 프로토콜이다. 단, $i, j \in \{1, \ldots, n\}$.

단계 1: 사용자 U_1은 디지털 권한명세서 m과 스마트카드 보증자의 그룹 공개키 리스트 및 그에 대한 서명값 a_1, $Sign_{sk_I}(a_1)$, pk_I을 사용자 U_2에게 전달한다.

단계 2: 사용자 U_2는 서명값을 검증한 뒤, 검증이 성립하면 챌린지 $c_{U_2} = (c_1, c_2) = (H(pk_{G_j}), s)$를 생성하여 U_1에게 전달한다.

단계 3: U_1은 토큰에 해당하는 T를 삭제하고 그에 대응되는 $E_{u_1} = (e_1, e_2, e_3, e_4, e_5, e_6)$를 생성하여 사용자 U_2에게 전달한다. 단, $e_1 = H(m)$, $e_2 = H(pk_I)$, $e_3 = c_1, e_4 = c_2, e_5 = GSig_{sk_{U_1}}(e_1 \| e_2 \| e_3 \| e_4), e_6 = pk_{G_i}$. 또한, 발행프로토콜과 유사하게 E_{U_1}의 백업복사본을 응답값 R_{U_2}가 올때까지 저장한다.

단계 4: 사용자 U_2는 E_{U_1}을 검증한 뒤 검증이 성공하면, S_{U_2}로부터 e_4를 삭제한 뒤, 토큰 $T = (H(m), H(pk_I))$를 저장한다. E_{U_1}의 검증과정은 다음과 같다.

① $e_3 = H(pk_{G_j})$

② $e_4 \in S_{U_2}$

③ $GVer_{pk_G}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1$

④ $Ver_{pk_I}(m) = 1$

⑤ $e_2 = H(pk_I)$

①,②는 챌린지의 유효성을 검증하는 것을 의미하고 ③은 E_I가 사용자 U_1에 의해 올바르게 생성되었다는 것을 보장하며, ④ 와 ⑤는 정당한 I가 m을 발행하였다는 것을 보장한다. 위의 검증식들이 성공하면, 사용자 U_2는 $R_{U_2} = (GSig_{sk_{U_2}}(c), pk_{G_j})$를 생성하여 U_1에게 전달한다.

단계 5: U_1은 R_{U_2}를 검증한 뒤 검증결과에 이상이 없으면, 같은 방식으로 E_{U_1}의 백업복사본을 삭제한다.

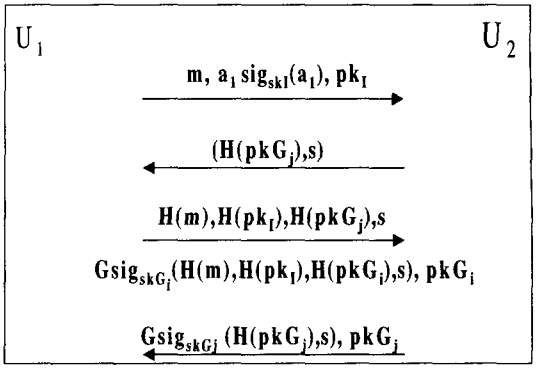


그림 5. 전달 프로토콜

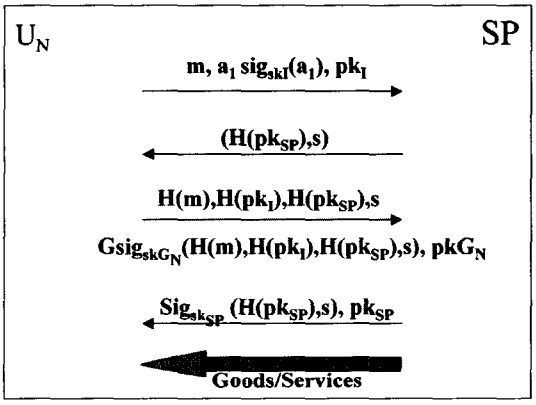


그림 6. 상환 프로토콜

○ 상환(Redemption) 프로토콜

사용자와 서비스 제공자 SP 사이의 상환 프로토콜은 사용자들 사이의 전달 프로토콜과 유사하다. NTT의 Flextoken방식처럼, 단지 차이는 챌린지 c가 소비(comsumption) 프로토콜인지 혹은 제시(presentation) 프로토콜인지를 분류하기 위해 음수 혹은 양수로 구분해서 처리한다는 점과 사용자 U_2 대신 서비스 제공자 SP가 참여한다는 사실만 다르다. 전달 프로토콜과 유사하게 진행되어, 서비스 제공자의 응답(receipt)과정까지 성공하면, 상품 혹은 서비스(Goods/Service)가 서비스 제공자로부터 사용자에게 전달되는 것으로 종료된다.

V. 안전성

- **변조 방지(Preventing Alteration)**: 디지털 권한의 변조를 방지하기 위해서는 권한에 대한 정

의 m과 토큰에 저장된 $H(m)$이 변조되는 것을 방지하여야 한다. m의 변조는 토큰에 저장된 m의 해쉬값 때문에 안전하다. $H(m)$이 저장된 토큰의 변조는 물리적 보안장치인 스마트카드에 저장되기 때문에 안전하며, E_I로 전달되는 $H(m)$에 대한 변조의 어려움은 그룹서명의 안전성에 의존하고 있다.

- **위조 방지(Preventing Forgery)**: 디지털 권한을 위조하기 위해서는 토큰에 저장된 발행자 정보와 참석자의 공개키 정보를 포함하고 있는 토큰을 생성하여야 한다. 앞에서 언급하였듯이 토큰의 변경은 그룹서명의 안전성에 의존하고, 공격자가 발행자 정보를 위조하여 발행자 인척하는 공격은 발행자의 서명에 대한 검증과 해쉬함수에 의해 방지된다.
- **재사용 방지(Preventing Reproduction)**: E_I를 재 사용하는 것은 챌린지 값에 의해 방지된다. 공격자가 E_I를 다시 사용하려고 한다면 일련번호에 해당하는 s 값이 이미 삭제되었기 때문에 그에 대한 검증과정에서 검증이 실패한다.
  디지털 권한을 받았으면서 받지 않았다고 주장하여 다시 보내달라고 재발급을 요청하는 경우는 E_I의 백업 복사본에 의해 방지된다. 만약 수신자가 E_I를 받지 않았다고 주장하면 수신자는 E_I의 백업복사본을 보내야한다.
- **익명성 보장(Ensuring Privacy)**: 제안된 방식은 그룹서명을 사용하여 사용자의 공개키 정보가 노출되지 않게 하고, 연계되지 않도록 함으로써 익명성과 불연계성(unlinkablility)을 만족한다. 권한을 전달시 사용자들은 자신이 어떠한 그룹에 소속되었는지에 대한 정보를 전달한다. 또한, SP가 이중거래를 발견한 경우, 그룹매니저들과 협동하여 사용자 식별정보인 z를 알아낼 수 있으므로 익명성 제어도 할 수 있다.

Ⅵ. 제안된 방식과 기존에 제시된 방법들의 비교

이 절에서는 기존에 제시된 디지털 권한·전달 시스템들과 본 논문에서 제시된 방식을 비교한다.

Matsuyama와 Fujimura[4]는 온라인 방식의 디지털 권한·전달 시스템을 제안하였다. 이 방식은 권한을 전달받은 사용자가 자신이 권한에 대한 유일한 소유자라는 것을 주장하고, 권한을 다른 사용자에게 전달하기 위해 온라인으로 TTP에 접속해야 한다.

디지털 권한의 특정 형태인 티켓방식도 제안되었다.[5] 그러나, 이 방식은 티켓 형태만을 지원하고 있을 뿐 다양한 권한 발행자들이 발행하는 권한들을 다루지 않는다. 또한 그룹서명을 사용한 오프라인 전자화폐 시스템 설계 기법[15]과 유사하게 설계되어, 그룹서명을 사용하여 익명성, 분할성, 양도성 등을 만족하지만, 서명생성 및 공모공격에 대해 안전하게 설계하기 위해 많은 계산량을 요구하고 있다.

최근 스마트카드에 기반한 NTT의 FlexToken[1] 방식은 특정부분의 어플리케이션만을 제공하지 않고 모든 권한(티켓)을 하나의 스마트카드로 통합하여 제공할 수 있는 권한(티켓)·전달 시스템을 제안하였다. 그러나, 이 방식에서는 사용자의 익명성을 제공하기 위해 Petersen과 Horster의 Pseudonym방식을 사용할 수 있다는 것을 언급하였다. Petersen과 Horster의 방식은 불연계성을 유지하기 위해 매번 다른 익명(pseudonym)정보를 생성하여야 한다.

본 논문에서는 이러한 불편함을 해결하면서 익명성을 제공하기 위해 그룹서명을 이용하는 방법을 제안하였다. 기존의 그룹서명기법은 서명 생성 및 검증에 signature of knowledge라는 증명을 수행하기 때문에 비효율적이다. 예를 들어, 기존에 제시된 가장 효율적이라 할 수 있는 그룹서명 방식은 Camenish와 Stadler가 제안한 그룹서명방식[9]이라 할 수 있다. 그러나, 이 논문에서 권장되는 시스템 파라메터가 $e_1=5, e_2=3, f_1=1$이고 f_2가 세제곱근을 계산하기 어렵도록 선택되는 경우, 그룹서명 및 검증에 드는 연산은 모듈러스 길이 n이 600비트일 때, 약 20번의 지수승이 소요되는 것으로 알려져 있다.[9] 반면 스마트 카드 기반 그룹서명의 경우, 그룹서명값은 한번의 전자서명 연산과 한번의 공개키 암호연산만을 요구하고 있기 때문에 2번의 지수연산만이 사용된다.[14]

이에 Camenish와 Stader의 그룹서명 방식을 기반으로 하여 설계된 익명성이 보장되는 디지털 티켓방식[5]에서는 그룹서명에 대응되는 티켓 전달(지불) 시 연산량을 생각하면 20번의 지수승 연산 이상[1]이 사용된다. 반면 제안된 방식은 권한(티켓) 전달 시 2번의 그룹서명이 사용되어 4번의 지수연산이 사용되기 때문에 훨씬 더 적은 연산이 드는 방식이라 할 수 있다.

1) 이중 사용방지 및 사후 추적(tracing)을 위해 i, $\tilde{g}$, $\tilde{z}$, $\tilde{h}_i$, $\tilde{V}_4$, $\tilde{V}_5$정보가 그룹서명에 추가되기 때문

표 1. 제안된 방식과 기존의 방식들과의 비교

구분	[4]	NTT의 FlexToken[1]	[5]	제안방식
다양한 형태의 권한	○	○	×	○
다양한 발행자	○	○	×	○
익명성	×	○ (Pseudonym)	○ (그룹서명)	○ (그룹서명)
효율성	○	○	× (20지수승 이상)	○ (4지수승 이상)
기반 방식	온라인	오프라인 (스마트카드 기반)	오프라인	오프라인 (스마트카드 기반)

이들 전체 방식들을 비교하면 표 1과 같다.

Ⅵ. 결 론

NTT의 FlexToken방식이 익명성을 제공하는 방법으로 one-time pseudonym방식을 제안하였지만 이 방식은 불연계성을 유지하기 위해 매번 다른 익명정보를 생성하여 등록하여야 하는 문제점을 갖고 있었다.

이러한 불편함을 해결하면서 효율성을 보장하는 디지털 권한 시스템을 설계하기 위해 본 논문에서는 스마트카드 기반의 그룹서명을 이용한 방법을 제안하였다. 이 방식은 기존에 제안된 디지털 권한의 특정 형태인 티켓시스템에 비해 효율적이며 NTT의 FlexToken 방식에 비해 익명성이 보장된다는 점에서 큰 장점을 갖고 있다.

참 고 문 헌

[1] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura, "Copy Prevention Scheme for Right Trading Infrastructure," the 4th Smart Card Research and Advanced Application Conference, 2000. 9.

[2] K. Fujimura and D. Eastlake, "Requirements and Design for Voucher Trading System (VTS)," 2003. 3. ftp://ftp.rfc-editor.org/in-notes/rfc3506.txt/.

[3] H. Petersen and P. Horster, "Self-certified Keys-concepts and applications," In Proceedings of the 3rd Conference on Communication and Multimedia Security, 1997.

[4] K. Matsuyama and K. Fujimura, "Distributed digtal ticket management for rights trading system," In Proceedings of the 1st ACM Conference on Electronic Commerce, 1999.

[5] T. Nakanishi, N. Haruna and Y. Sugiyama, "Unlinkable electronic coupon protocol with anonymity control," Proceedings of Information Security Workshop'99, volume 1729 of Lecture Notes in Computer Science, Berlin, pp. 37-46, Springer Verlag, 1999.

[6] E-Stamp Cooperation, "E-Stamp", http://www.e-stamp.com/.

[7] Gold & Silver Reserve, Inc., "e-gold", http://www.e-gold.com/.

[8] D. Chaum and E. van Heyst, "Group Signatures," In advances in Cryptology -Eurocrypt'91, volume 547 of Lecture Notes in Computer Science, pp. 257-265, Springer Verlag, 1991.

[9] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," In advances in Cryptology- Crypto'97, volume 1296 of Lecture Notes in Computer Science, pp. 410-424, Springer Verlag, 1997.

[10] G. Ateniese and G. Tsudik, "Group signatures a la carte," In ACM Symposium on Discrete Algorithms, 1999.

[11] J. Camenisch, "Efficient and generalized group signature," In advances in Cryptology-Eurocrypt'97, volume 1233 of Lecture Notes in Computer Science, pp. 465-479, Springer Verlag, 1997.

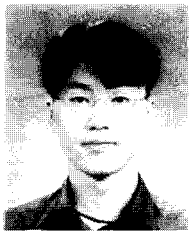
[12] J. Camenish and M. Michels, "A group signature scheme based on an RSA-variant," Tech. Rep. RS-98-27. BRICS. Dept of Comp. Sci., 1998.

[13] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme," In advances in Cryptology-Crypto'00, volume 1880 of Lecture Notes in Computer Science, pp. 255-270, Springer Verlag, 2000.

[14] S. Canard and M. Girault, "Implementing Group Signature Schemes With Smart Cards," Proceedings of the 5th Smart Card Research and Advanced Application Conference, USENIX 2002. 12.

[15] J. Traore, "Group Signatures and Their Relevance to Privacy-Protecting Offline Electronic Cash Systems," ACISP'99, volume 1587 of Lecture Notes in Computer Science, pp. 228-243, Springer-Verlag, 1999.

〈著者紹介〉



주 학 수 (Hak-Soo Ju) 정회원
1997년 8월: 고려대학교 수학과 졸업
1999년 8월: 고려대학교 수학과 이학석사(대수학 전공)
2001년 8월: 고려대학교 수학과 박사과정 수료
2001년 9월~현재: 한국정보보호진흥원 연구원
〈관심분야〉 암호학, 공개키암호, 응용보안프로토콜

김 대 엽 (Dae-Youb Kim) 종신회원
1994년 2월: 고려대학교 수학과 졸업
1996년 8월: 고려대학교 수학과 석사(대수학 전공)
2000년 2월: 고려대학교 수학과 박사(대수학 전공)
1997년 8월~2001년 3월: (주)텔리맨, 위성통신 연구소, CAS팀 선임연구원
2001년 4월~2002년 7월: 삼성 시큐아이닷컴(주) 정보보호 연구소 PKI실 차장
2002년 9월~현재: 삼성 종합기술원, i-Networking Lab. 전문연구원
〈관심분야〉 CAS, DRM, PKI/WPKI, Smart Card, 응용 보안프로토콜

이 동 훈 (Dong Hoon Lee) 정회원
1984년: 고려대학교 경제학과 졸업
1987년: Oklahoma Univ. 전산학과 석사
1992년: Oklahoma Univ. 전산학과 박사
1993년~2000: 고려대학교 전산학과 교수
2000년~현재: 고려대학교 정보보호 대학원 교수
〈관심분야〉 암호이론, 정보보호 프로토콜, 계산이론