ETRI

전자통신동향분석 제 23권 제 4호 2008년 8월

익명 인증 기술과 동향

The Technology and Trend of Anonymous Authentication

21세기를 대비하는 정보보호 특집

이윤경 (Y.K. Lee)	지식정보보호연구팀 선임연구원
한승완 (S.W. Han)	지식정보보호연구팀 선임연구원
이석준 (S.J. Lee)	지식정보보호연구팀 선임연구원
정병호 (B.H. Chung)	지식정보보호연구팀 책임연구원
양대헌 (D.H. Nyang)	인하대학교 교수
권태경 (T.K. Kwon)	세종대학교 교수

목 차

인터넷 이용이 활성화 되면서 각종 웹 서버에서의 개인정보 과다 수집 및 노출이 큰 이슈가 되고 있다. 인터넷이 우리 생활에 주는 편리함을 그대로 누리면서 개인정보를 보호할 수 있는 방안으로 익명 인증 기술이 있을 수 있다. 익명 인증은 익명성을 제공하는 디지털 서명을 이용한 인증 방법이다. 익명성을 제공하는 디지털 서명 방법은 전자화폐와 전자투표 시스템 등의 응용을 위해서 주로 연구되어 왔으나, 최근에는 인터넷 환경에서 개인정보 보호를 위한 익명 인증 방법의 하나로써 연구되고 있다. 본 고에서는 익명성을 제공하는 전자서명 방법에 관하여 소개하고, 이들 전자서명 방법 중 익명 인증을 위해서 가장 많은 연구가 되고 있는 그룹 서명 방법의 최근 연구동향에 관하여 기술하고자 한다.

Ⅰ. 서론

인터넷은 우리 생활에 없어서는 안될 필수 요소가 되고 있다. 그러나 인터넷 서비스 및 전자상거래 이용시 서비스 제공자들은 불필요하거나 지나치게 과도한 사용자의 개인정보를 요구하여 개인의 프라이버시를 침해하고 있으며, 또한 정보관리의 부주의로 인하여 대형 개인정보 유출사고가 빈번하게 발생하고 있다. 또한 인터넷 이용자들의 의식 변화로 개인정보 보호에 대한 인식이 커지고 있는 실정이다. 이러한 상황에서 중요한 개인 정보들은 제 3의 믿을 만한 기관에 안전하게 저장하고, 서비스 제공자에게는 꼭 필요한 정보만을 제공하는 방안을 생각할 수 있다. 그러나, 실명을 사용하는 현 인터넷 체계에서 이런 방법을 이용한 개인정보보호에는 한계가 있으며, 이를 해결하기 위한 방안으로 익명 인증 방법이 논의되고 있다.

익명 인증은 1985년 David Chaum이 제안한 익명 신용장(anonymous credential) 시스템에서 기인한 전자서명을 이용한 인증 방법이다. 초기의 익명 신용장은 전자화폐 혹은 전자투표 등의 응용을 위해 주로 연구되었고, 대부분이 이론적인 연구에 그쳤으나, 최근에는 실용성이 강조되면서 실생활에 적용할 수 있는 수준까지 발전하였으며, 프라이버시 보호를 위한 익명 인증의 한 방법으로 연구가 활발히 진행되고 있다.

본 고의 Ⅱ장에서는 익명 디지털 신용장의 의미에 대하여 알아보고, 익명성을 제공하는 디지털 서명 방식인 Blind Signature, Group Signature, Ring Signature, Traceable Signature 등에 대하여 Ⅲ장에서 기술하고자 한다. 또한 Ⅳ장에서 인터넷 서비스 이용시 개인신원 확인용으로 가장 적절한 디지털 서명 방식인 Group Signature의 연구 동향에 관하여 기술하고자 한다.

Ⅱ. 익명 디지털 신용장

신용장 시스템(credential system)이란 사용자가 기관들로부터 신용장(credentials)을 획득할 수 있고, 이들 신용장을 가지고 있음을 알릴 수 있는 시스템을 말한다. 또한 동일한 사용자가 하는 행동들이, 동일한 사용자에 의해 이루어지는 행동임을 다른 사람들이 모를 때 익명 신용장 시스템(anonymous credential system)이라고 한다[1].

익명 디지털 신용장(anonymous digital credential)의 메인 아이디어는 암호 토큰(cryptographic token)을 받은 사용자가 익명으로, 그리고 공공기관 및 사적인 기관과 그 사용자에 대한 연관관계를 밝히지 않고, 자신의 신분 및 자신에 대한 정보들을 증명할 수 있도록 하는 것이다. 따라서 익명 디지털 신용장은 프라이버시와 익명성(anonymity)과 관련되어 있다. 이러한 신용장(credential)과 유사한 것을 실생활(paper world)에서 찾는다면 여권, 운전 면허증, 화폐 등이 있을 수 있다. 또 다른 예로 신용 카드, 의료보험 카드, 영화티켓, 대중교통 이용 티켓, 클럽 등의 멤버십 카드 등이 있다. 신용장은 신용장에 적힌 정보가 확실하다는 것을 확인할 수 있는 기관에서 발행되고, 요구가 있을 때 이용자들(entity)을 확인하기 위해서 제공될 수 있다.

신용장의 프라이버시 관점에서의 특성을 좀 더 확실히 하기 위해서, 두 가지 종류의 신용장(화폐와 신용카드)에 대하여 살펴보자. 이 두 가지는 의심의 여지 없이 지불과정을 수행하는 데 적절한 정보를 제공한다. 그러나 노출되는 정보의 양과 질이 다르다. 화폐는 그것을 물리적 특성에 의해서 위조를 방지한다. 그리고 아주 적은 정보만이 노출된다; 동전들의 타고난 가치에 대한 특성과 동전이 주조된 연도, 그리고 추가적으로, 은행은 법적인 문제가 있을 때 추적할 수 있도록 하기 위해서 유일한 시리얼 넘버를 기록해 둔다. 반면에 신용카드를 사용할 경우, 신용카드의 주요 목적은 돈과 비슷하지만 신용카드 소유자에 대한 더욱 상세한 기록들을 포함하게 된다. 돈이 가진 프라이버시 측면의 중요한 장점은 돈의 사용자가 익명으로 남아 있을 수 있다는 것이다.

1. Anonymous Digital Credential and Pseudonyms

David Chaum이 제안한 원래의 익명 신용장 시스템[2]은 때때로 pseudonym system으로 언급되기도 한다. 이는 각 기관마다 다른 pseudonym을 사용하여 신용장을 발급받고, 그 기관에서만 사용하기 때문에 동일한 사용자가 다른 기관에서 사용하는 신용장이나 pseudonym을 자신의 기관에서 사용하는 신용장이나 pseudonym과 연결 지을(linked) 수 없기 때문이다. Pseudonym은 익명성(anonymity)에 대한 아주 유용한 확장이다. Pseudonym은 사용자들이 각 기관마다 다른 이름을 선택할 수 있게 해준다. 각 기관들은 pseudonym을 통하여 사용자를 사용자 계정과 연결 지을 수 있지만, 기관들은 자신의 고객들의 실제 신분을 알 수는 없다. 그러나 익명 신용장을 사용함으로써 pseudonym으로 연결된 사용자와 기관의 관계를 확실히 할 수 있고, 다른 기관에 그 관계를 증명할 수 있다.

2. History of Anonymous Digital Credentials

익명 신용장 시스템은 Chaum이 제안하였듯이 익명 지불 또는 추적 불가능성(untraceable)의 개념과 연관되어 있다. 이 연구에서, Chaum은 새로운 암호학적 토대인 Blind Signature 프로토콜을 제안하였다. 이 서명에서, 서명자(signer)는 자신이 서명하는 메시지에 대해서 모르고, 또한 그 서명을 받는 수령자(recipient)가 그 메시지를 획득했는지도 모른다. Blind Signature는 익명지불, 전자 투표, 그리고 credential 같은 프라이버시 보호가 중요한 응용에 적용될 수 있다. 익명 신용장 시스템에 대한 초기 아이디어는 Blind Signature에서 왔지만, 익명 신용장 시스템은 하나의 pseudonym에서 또 다른 pseudonym으로 변환하는 신용장(credential)을 전송해 주는 제3의 기관(trusted party)에 의존한다. Chaum이 제안한 Blind Signature는 RSA 서명 기반이었다. 이산대수 문제에 근거한 Blind Signature 구조는 익명 신용장 시스템을 구축하는 데 사용될 수 있다.

Stefan Brands는 디지털 신용장을 신용장에 기반한 자신의 비밀키 인증서(secret key certificate)로 확장함으로써 디지털 신용장을 일반화 하였다. 이는 이산대수와 Strong RSA 가정에 근거하여 Chaum의 기본적인 Blind Signature를 향상시킨 것이다. 또한 Brands의 신용장은 digicash, ecafe esprit project, zero-knowledge systems[www.zeroknowledge.com]과 credentica에서 상업적으로 사용되었다[3].

그 후 익명 신용장(anonymous credential)의 새로운 특성인 multi-show unlinkability를 제공하는 Group Signature가 나왔다. Group Signature는 Camenisch et al.의 credential과 관계가 있다. Blind Signature가 전자화폐와 one-show credentials을 주로 고려한 것인 반면에, Group Signature는 프라이버시를 더욱 잘 보호할 수 있는 프로토콜 구성의 가능성을 보여주는 프리미티브라 할 수 있다.

Group Signature를 사용하면, 한 그룹의 멤버들은 자신의 비밀키로 메시지에 서명을 할 수 있다. 그 결과 얻은 서명은 그룹 공통의 공개키를 알고 있는 사람은 누구나 확인할 수 있다. 그러나 그 서명은 서명한 사람이 어떤 그룹의 멤버라는 사실만을 알고 있을 뿐 그 사람이 누구인지에 대한 정보는 절대 드러내지 않는다. 일반적으로 Group Signature에서는 그룹 매니저(group manager)를 고려하는데, 그

● 용 어 해 설 ●

Strong RSA 가정: 랜덤하게 선택된 RSA 모듈러 n과 랜덤 값으로 이루어진 $z \in Z_n^*$가 주어졌을 때, $z = y^r \bmod n$을 만족하는 $r > 1$과 $y \in Z_n^*$를 찾기 힘들다는 것을 기본 전제로 하는 가정

Multi-show unlinkability: multi-show는 one-show와 대비되는 용어로써, 하나의 신용장을 여러 번 재사용 가능함을 의미하고, multi-show unlinkability란 하나의 신용장을 여러 번 사용하더라도 동일한 사용자임을 알 수 없는 특성을 의미한다.

룹 매니저는 서명한 사람의 정확한 신분을 드러낼 수 있고, 그룹에 멤버를 추가하거나 제거할 수 있는 권한이 있다. 이는 주로 그룹 멤버십 인증서(group membership certificate)를 발행하거나 폐기함으로써 이루어진다. Group Signature에 의해 제공되는 익명성(anonymity), 비연결성(unlinkability), 익명성 폐기(anonymity revocation) 특성은 전자투표, 전자입찰, 익명지불, 익명 신용장처럼 프라이버시에 민감한 응용에 적합하다.

Ateniese, Camenish, Joye, and Tsudik이 실생활에 적용 가능한 수준의 Group Signature를 제안하였고[4], 익명성 폐기 기능까지 추가된 더욱 실질적인 multi-show unlinkable 익명 신용장 시스템이 [1]에서 제안되었다. 두 가지 Group Signature 구조 모두 지식 증명(proofs of knowledge)에 기반하고 있다. 지식 증명은 알려진 순서대로 이산대수 문제를 푸는 것에 기반한 것과 RSA 문제에 기반한 것이 있는데, 특히 RSA 문제에 기반한 것은 오늘날의 Group Signature의 근간이 되었다. 또한 믿을 수 있는 플랫폼 모듈을 인증하는 프로토콜인 DAA[5]도 동일한 기술에 기반하고 있다. DAA는 multi-show unlinkable credential에 관한 최초의 상업적 응용으로 볼 수 있다. 그러나, DAA의 경우 신용장이 사람과 연결되는 것이 아니라, 컴퓨터 플랫폼과 연결된다는 단점이 있다.

Ⅲ. 익명성을 제공하는 전자서명 방법

1. Blind Signature

David Chaum이 처음 소개한 디지털 서명의 한 형태로써, 서명하는 사람이 메시지의 내용을 모른 채(blinded) 서명 값을 생성하는 경우, 이를 Blind Signature라고 한다. Blind Signature는 전형적인 프라이버시 보호 프로토콜로써, 서명자와 메시지 작성자(message author)가 서로 다르다. Blind Signature를 이용한 대표적인 예로 전자 투표 시스템과 디지털 캐시 구조가 있다. Blind Signature를 쉽게 설명하면, 실생활에서 봉투 안에 메시지를 동봉하여 봉인한 후, 서명 에이전트가 서명하는 행위에 비교할 수 있다. 그래서 서명한 사람(signer)은 메시지의 내용을 볼 수 없고, 제 3자가 차후에 서명을 검증할 수 있다.

Blind Signature 구조는 RSA와 DSA 같은 일반적인 공개키 서명 구조들을 이용하여 구현될 수 있다. 메시지는 서명하기 전에 내용을 숨겨야(blind) 하는데, 일반적으로 랜덤 “blinding factor”와 메시지를 다양한 방법으로 결합하여 blind된 메시지를 얻는다. Blind된 메시지는 서명자(signer)에게 전달되고, 서명자는 일반적인 서명 알고리듬을 사용하여 서명하면 된다. Blinding factor에 영향을 받게 되는 결과 메시지는 서명자의 공개키를 이용하여 차후에 확인될 수 있다.

Blind Signature는 두 개의 party(자신의 메시지에 대한 서명을 획득하고자 하는 사용자 Alice와 자신의 비밀키를 가지고 서명을 하는 서명자 Bob)를 포함하는 암호 프로토콜이다. 프로토콜의 마지막에서, Alice는 메시지에 대해 어느 것도 알지 못하는 Bob에게서 메시지 m에 대한 서명을 얻는다.

가. Blind Signature 사용 예

Blind Signature 구조는 메시지 전송자(sender)의 프라이버시가 중요한 경우에 많이 사용되는데, 그 예로 다양한 디지털 캐시 구조와 전자투표 프로토콜이 있다. 예를 들어, 전자투표 시스템의 무결성은 각 무기명 투표용지를 합산(counting)하기 전에 투표 권한이 있음을 인증 받을 필요가 있다. 이를 통해 전자투표를 총괄하는 측(authority)에서는 투표자의 credential들을 점검하여 투표할 권한이 있는지, 한 번 이상 투표를 한 것은 아닌지를 체크할 수 있다. 동시에, 투표를 총괄하는 측에서는 투표자의 선택을 알 수 없다는 것이 중요하다. Unlinkable Blind Signature는 다음과 같은 기능을 보장하여야 한다.

- authority는 자신이 서명한 어떠한 투표용지의 내용도 볼 수 없고,
- 자신이 서명한 blinded 투표용지를 authority가 counting을 위해서 받았을 때 unblinded 투표용지와 연결 지을 수 없다.

나. Blind RSA Signatures

가장 단순한 Blind Signature 구조 중 하나는 RSA 서명에 기초한 것이다. 전통적인 RSA 서명은 메시지 m을 d승하여 모듈러 n 연산을 하는 것이다. Blind 버전은 랜덤 값 r을 사용하는데, r은 n에 대해서 relatively prime(즉, gcd(r, n) = 1)이다. 그리고 r을 e승한 후 모듈러 n 연산을 한 결과 값 r^e mod n을 "blinding factor"로써 사용한다. 메시지 소유자는 메시지와 blinding factor의 결과를 연산한다. 즉, 식 (1)을 참고하자.

$$m' = m \cdot r^e \pmod{n} \quad (1)$$

그리고 결과 값 m'을 서명자에게 전송한다. r은 랜덤 값이기 때문에 r을 r^e mod n에 매핑하는 것은 r^e mod n 또한 랜덤이 되는 치환이다. 이는 m'이 m에 대한 어떠한 정보도 유출하지 않는다는 것을 암시한다. 그러면 서명자는 blinded signature s'을 (2)와 같이 계산한다.

$$s' \equiv (m')^d \pmod{n} \quad (2)$$

s'은 메시지 소유자(message authority)에게 다시 보내지고, 메시지 소유자는 s를 드러내기 위해서 blinding factor를 제거할 수 있다. 메시지 m에 대한 유효한 RSA 서명은 (3)과 같다.

$$s \equiv s' \cdot r^{-1} \pmod{n} \quad (3)$$

이는 RSA 키가 $r^{ed} \equiv r \pmod{n}$ 방정식을 만족하고, 그 결과 (4)와 같다.

$$\begin{aligned} s &\equiv s' \cdot r^{-1} \equiv (m')^d \cdot r^{-1} \equiv m^d \cdot r^{ed} \cdot r^{-1} \\ &\equiv m^d \cdot r \cdot r^{-1} \equiv m^d \pmod{n} \end{aligned} \quad (4)$$

따라서, s는 확실히 m의 서명이 된다.

다. Dangers of Blind Signing

RSA는 또 다른 메시지를 blind 서명함으로써 어떤 메시지를 복호화하게 하는 속임수에 빠질 가능성이 있는 RSA blinding attack의 영향을 받는다. 서명 과정은 Bob이 비밀키로 암호화하는 것과 동일하므로, attacker는 Bob의 공개키로 메시지 m을 암호화하여 Bob이 서명하게 될 메시지의 blinded 버전인 m'을 제공할 수 있다. Attacker는 서명된 버전을 unblind 할 때, 평문을 얻을 수 있게 된다.

$$\begin{aligned} M'' &= m' \cdot r^e \pmod{n} \\ &= (m^e \pmod{n} \cdot r^e) \pmod{n} \\ &= (mr)^e \pmod{n} \end{aligned} \quad (5)$$

이때, m'은 메시지 m의 암호화된 버전이다. 이 메시지가 서명될 때, 평문 m은 쉽게 추출된다.

$$\begin{aligned} s' &= m''^d \pmod{n} \\ &= ((mr)^e \pmod{n})^d \pmod{n} \\ &= (mr)^{ed} \pmod{n} \\ &= m \cdot r^{-1} \pmod{n} \end{aligned} \quad (6)$$

대부분의 서명 알고리듬들은 완전한 메시지 m"에 대해서 서명을 하지 않고, 대신 문서의 해시에만 서명을 하기 때문에, 이러한 공격 방법이 직접적으로 이용되는 경우는 거의 없다.

2. Group Signature

Group Signature는 그룹 멤버 중 한 사람이 익명으로 어떤 메시지에 서명하는 것을 허용하는 서명방법이다. 기본 개념은 1991년 David Chaum과 Eugene van Heyst에 의해 처음 소개되었다. 예를 들어, 큰 회사의 직원이 Group Signature 구조를 이용하여 문서에 서명을 하였을 때, 그 서명의 유효성을 검증하는 verifier는 해당 회사 직원 중 한 명이 서명했다는 사실만을 알 수 있고, 직원 중 누가 서명을 했는지는 정확히 알 수 없는 서명 방법이다. 또 다른 응용 예로, 제한된 지역에 접근할 수 있는 키 카드를 이용하는 응용의 경우, 이 지역에서 직원 개개인의

〈표 1〉 Group Signature의 특성

Soundness and completeness (correctness)	- 그룹 멤버들에 의한 유효한 서명은 항상 제대로 검증되어야 하고 - 유효하지 않은 서명은 항상 서명 검증에 실패하여야 한다.
Unforgeable	- 그룹의 멤버들만이 유효한 서명을 생성할 수 있어야 한다.
Anonymity	- 메시지와 그 메시지에 대한 서명이 주어졌을 때, 서명자 개인의 신분은 revocation 매니저의 비밀키가 없으면 노출되지 않아야 한다.
Unlinkability	- 두 메시지와 각 메시지에 대한 서명이 주어졌을 때, 그 서명들이 동일한 서명자가 서명한 것인지 여부를 알 수 없어야 한다.
Exculpability	- 모든 다른 그룹 멤버들과 매니저가 결탁하더라도, 참여하지 않은 그룹 멤버에 대한 서명을 위조할 수 없어야 한다.

움직임을 추적할 수는 없지만, 그 그룹에 속한 직원들만이 그 지역에 접근할 수 있도록 할 수 있다.

Group Signature 구조에서 가장 중요한 요소는 그룹 매니저이다. 그룹 매니저는 그 그룹에 새로운 멤버를 추가할 수 있고, 논쟁이 발생한 경우 서명한 사람을 공개할 수 있는 권한을 갖는다. 시스템에 따라서 그룹에 멤버를 추가할 수 있는 권한을 가진 매니저(membership manager)와 서명의 익명성을 폐기하는 권한을 가진 매니저(revocation manager)를 분리하기도 한다. 다양한 Group Signature 구조가 제안되었지만, 대부분의 Group Signature 구조는 <표 1>과 같은 기본적인 요구사항을 따른다.

Group Signature는 주로 다음의 5가지 과정으로 구성된다. 즉, key generation, join, sign, verify, open.

- Key generation: 몇 개의 시큐리티 파라미터들을 이용하여 그룹 공개키와 그룹 비밀키를 생성하는 과정
- Join: 그룹 매니저와 사용자 사이의 프로토콜로써, 그룹의 멤버가 되고자 하는 사용자가 그룹 매니저로부터 멤버십 인증서와 멤버십 비밀키를 받는 과정
- Sign: 그룹 멤버가 그룹 전체를 대신하여 메시지에 서명하는 과정
- Verify: 그룹 공개키로 서명을 검증하는 과정
- Open: 논란이 발생했을 경우, 그룹 매니저(혹은 revocation manager)가 그룹 비밀키와 서명을 이용하여 서명한 사람의 신분을 밝히는 과정

Group Signature 구조는 다음 두 가지가 보장된다면 안전하다고 할 수 있다[6].

- Anonymity: revocation 매니저만이 서명자의 신분을 밝힐 수 있다.
- Traceability: 그룹 매니저는 모든 유효한 서명에 대해서 서명자의 신분을 알 수 있다.

3. Ring Signature

키를 가진 그룹 멤버들 중 어떤 사람에 의해서도 서명할 수 있고, 따라서 Ring Signature를 이용하여 서명된 메시지는 특정 그룹 멤버들 중 누군가에 의해서 보증된다. Ring Signature는 그룹 내의 어떤 멤버의 키를 이용하여 서명되었는지를 알기가 어렵다는 특징이 있다. Ring Signature는 Group Signature와 비슷하지만 다음 특성들에서 차이가 있다.

- 익명성을 폐기할 수 없다.
- 그룹 매니저가 없다.
- 어떤 그룹의 사용자든 추가적인 셋업 과정 없이 다른 그룹의 멤버가 될 수 있다.

Ring Signature는 2001년 Ron Rivest, Adi Shamir, and Yael Tauman에 의해 처음 소개되었는데[7], Ring Signature라는 용어는 서명 알고리듬의 구조가 "ring"의 구조와 유사하다는 점에서 나온 것이다. 즉, 모든 그룹 멤버들이 동일한 위치에 있고, 중심이 되는 멤버가 따로 존재하지 않는다.

그룹 구성원 각각이 공개키/비밀키 쌍(PK_1, SK_1), (PK_2, SK_2), …, (PK_n, SK_n)을 가지고 있다고 가정하자. Ring Signature σ는 그룹 구성원 모두의 공개키와 서명자의 비밀키, 그리고 서명할 메시지를 이용하여 계산될 수 있다. 그리고, 그룹의 모든 멤버들은 서명 값 σ, 메시지 m, 그리고 포함된 공개키 쌍 PK_1, …, PK_n이 주어졌을 때, 서명의 유효성을 확인할 수

있다. Ring Signature가 적절히 계산되었다면 서명 값이 제대로 확인되어야 한다. 반면에, 그 그룹 멤버들의 비밀키들을 알지 못한다면 누가 서명을 생성하였는지를 알 수 없다. Ring Signature 구조는 ring-sign과 ring-verify의 두 가지 과정으로 구성되어 있다.

- Ring-sign(m, PK_1, PK_2, …, PK_n, i, SK_i): n명의 그룹 멤버들의 공개키와 i번째 그룹 멤버의 비밀키 SK_i를 가지고 메시지 m에 대한 서명 값 σ를 생성하는 과정
- Ring-verify(m, σ): 메시지 m과 모든 그룹 멤버들의 공개키가 담긴 서명 σ를 이용하여 서명을 검증하는 과정

Ring Signature는 서명자가 그룹에 속한 사람들의 공개키만 알면 서명할 수 있으므로 그룹 멤버를 추가하거나 삭제하는 과정이 필요 없지만, 서명 값에 그룹에 속한 멤버들의 공개키가 포함되어야 하므로 멤버의 수가 많아지면 서명 값도 이에 비례하여 길어진다는 단점이 있다.

Ring Signature의 응용으로, 백악관 직원들 중 어느 누구로부터 메시지에 서명한 직원이 누구인지는 드러내지 않은 채, 익명 서명을 제공받기 위해서 사용될 수 있다. Ring Signature의 익명성은 폐기될 수 없고, Ring Signature를 위한 그룹은 급조될 수 없기 때문에 이러한 응용이 가능하다.

4. Traceable Signature

Traceable Signature는 2004년 Kiayias[8] 등이 제안한 익명성을 제공하는 전자서명 방법이다. Traceable Signature는 Group Signature가 그룹 멤버들의 프라이버시를 보호할 수 있는 방법으로 많이 논의되고 있지만, 그룹 매니저 혹은 revocation 매니저가 필요한 경우에 한해서 서명한 사람의 신분을 밝히는 것만으로는 멤버의 프라이버시 보호에 충분하지 않다는 전제 하에, 서명자가 원하는 경우 스스로 특정 서명에 대해서 자신이 서명한 것임을 밝힐 수 있도록 해야 한다는 생각을 바탕으로 생성된 서명 방법이다[8].

〈표 2〉 Traceability의 종류

User racing	- 특정 사용자가 했던 서명들을 모두 밝혀 내는 것 - 에이전트를 두어 모든 서명에 대해서 서명이 생성될 때마다 체크하여 데이터베이스에 저장해 두는 것
Signature opening	- 특정 서명을 생성한 사람을 밝히는 것 - Group Signature에서 사용하는 개념과 동일
Signature claiming	- 서명을 생성한 사람이 특정 서명에 대해서 자신이 서명을 했음을 주장하는 것

Traceable Signature에서는 <표 2>와 같은 세 가지 종류의 traceability를 고려한다.

Traceable Signature는 Setup, Join, Sign, Verify, Open, Reveal, Trace, Claim, Claim_verify의 아홉 가지 단계로 구성된다.

- Setup: 그룹 매니저가 그룹 멤버들의 키 생성에 사용할 그룹 공개키와 그룹 비밀키를 생성하는 과정
- Join: 멤버십 인증서(membership certificate)를 발행하여 새로운 멤버를 받아들이는 과정으로, 그룹 매니저는 이 과정에 생성되는 모든 메시지들을 저장해 둔다.
- Identify: 멤버십 인증서를 받은 사용자가 제 3자에게 자신이 멤버십 인증서를 소유하고 있음을 proof of knowledge 방법으로 증명하는 과정
- Sign and Verify: Identify 과정을 수행하는 도중 메시지에 서명하고, 서명 값을 확인하는 과정
- Open: 어떤 서명이 주어졌을 때, 그 서명을 만든 사람의 신분을 드러내는 과정으로, 그룹 매니저가 믿을 만한 기관에 사용자의 정보를 넘겨준다.
- Reveal: 그룹 매니저가 특정 사용자의 행적을 추적할 수 있는 자료들을 생성하는 과정
- Trace: 에이전트에게 어떤 서명이 주어졌을 때, 그 서명이 특정 사용자에 의해 서명되었는지 여부를 그 에이전트가 체크하는 과정, 즉 특정 사용자에 의해 생성된 서명들을 확인하는 과정
- Claim: 사용자가 다른 기관 혹은 사용자에게 특정 서명이 자신이 한 서명임을 주장하는 과정

• Claim_verify: 어떤 사용자가 자신의 서명이라고 주장하는 서명이 실제 그 사용자가 생성한 것인지를 확인하는 과정

이러한 Traceable Signature 구조는 옥션 같은 인터넷 경매 시스템에서 사용할 수 있다. 경매에 참여하고자 하는 사람은 그룹 매니저에게 멤버십 인증서를 발급받고, 경매에 참여하고, 경매에 낙찰되었을 때, 낙찰된 것이 자신의 서명이 담긴 것임을 주장할 수 있다.

Ⅳ. 그룹 서명의 연구 동향

앞서 기술하였듯이 Group Signature는 1991년 David Chaum에 의해 제안된 익명성 기반의 전자서명 방법이다. Group Signature는 주로 RSA 혹은 Strong RSA 가정 기반의 서명 방법이 제안되었으나, 2004년 D. Boneh[9] 이후로 SDH 가정 기반의 서명 방법도 나오고 있다. Group Signature를 포함한 대부분의 익명 인증관련 전자서명 방법들이 이론적인 연구에 치우쳐 있어서 실제 구현되어 사용되는 사례가 거의 없었으나, 최근 들어 실용적인 전자서명 방법들이 나오는 추세이다. Group Signature의 경우, 전자 서명의 길이가 적절한 수준으로 짧아졌고(RSA 서명 길이와 비슷하거나 몇 배 정도의 길이), 그룹 멤버의 수에 비례하여 길어지던 서명 길이가 그룹 멤버 수와 관계없이 일정한 길이를 갖는 서명 방법이 나오고 있다. 또한 그룹 멤버를 폐기(revoke) 할 수 있는 방법에 관한 연구도 진행되고 있다. 본 장에서는 이러한 최근의 Group Signature에 대한 연구 동향을 소개하고자 한다.

1. Short Group Signatures[9]

Group Signature는 서명자의 프라이버시를 보호하기 위한 것이고, 서명자의 프라이버시를 보호하는 것은 중요하다. 그러나 이전의 Group Signature 구조들은 서명의 길이가 너무 길어서 실제 구현하여 사용하기에 힘든 점이 있었으나, 이 논문에서는 짧아진 길이의 Group Signature를 생성하는 방법을 제안함으로써 서명자의 프라이버시 보호에 한 발 더 다가설 수 있게 되었다.

이 논문에서는 Bilinear 매핑에서 Strong Diffie-Hellman 가정을 기반으로 Short Group Signature를 생성하는 방법을 제안하였는데, 서명과 서명의 확인 과정이 이전의 연구보다 더 빨라졌고, 서명의 경우 20배 더 짧아졌다. 즉, 총 서명 길이는 1533비트이고, 이는 1024비트 RSA와 비슷한 정도의 안전성을 갖는다. 또한 revocation 메커니즘을 제시하여 그룹 멤버 중 일부만을 그룹에서 제외하는 것이 가능해졌다.

이 논문에서 제안한 Group Signature 구조는 correctness, full-anonymity, full-traceability, exculpability의 시큐리티 요소를 제공한다. Correctness란 정직하게 생성된 서명을 확인하고 정확하게 추적할 수 있는 기능을 의미하고, full-anonymity란 서명 값이 공개된다 하더라도 서명 값을 바탕으로 서명한 사람을 알아낼 수 없는 기능을 의미하며, full-traceability란 모든 서명은 여러 사용자와 그룹 매니저간의 결탁으로 서명이 생성되더라도 위조에 가담한 사람을 모두 추적할 수 있는 기능을 뜻한다. 또한 exculpability란 그룹 내의 어떠한 멤버와 그룹 매니저라도 다른 사람인 것처럼 가장하여 서명을 생성할 수 없는 기능을 뜻한다.

이 논문에서는 revocation 프로토콜 또한 제안하고 있는데, 그룹 내에서 폐기된 멤버가 있으면 revocation list RL을 참조하여 그룹 내의 다른 멤버들 모두 새로운 그룹 공개키를 연산하여야 하고, 또한 자신의 비밀키도 갱신하여야 한다는 단점이 있다. 따라서 그룹 내에서 revocation 과정이 자주 일어난다면 이 프로토콜을 사용하기 어렵다.

2. Signature Schemes and Anonymous Credentials from Bilinear Maps[10]

이 논문에서는 Strong RSA 가정을 이용한 Group Signature 구조를 제안하였는데, Lysyanskaya의

논문 “Pseudonym Systems”[11]의 기본 아이디어를 따른다. 즉 [11]에서 사용한 LRSW 가정(논문 저자 이름의 이니셜을 따서 LRSW assumption 이라 한다.)을 기본 가정으로 하고, 이를 발전시켜 새로운 credential 시스템을 제안하고, 제안한 credential 시스템을 제한하여 Group Signature에 적용하였다.

네 가지 종류의 서명 구조(signature scheme)들을 제안하고 있는데, 가장 단순한 서명 구조에서 시작하여 이를 발전시키거나 제한하여 새로운 서명 구조들을 제안한다. 새로운 그룹 멤버를 join하고, 그룹의 멤버들이 서명하고, 특수한 상황에서 서명한 사람의 신분을 노출하는 open 방법에 관하여 제시하고 있다. 그러나 특정 멤버를 revoke하는 구체적인 방법에 관하여는 언급하지 않고 있다. 즉, 특수한 상황에서 멤버의 신분을 노출함으로써 신분이 노출된 멤버의 익명성을 빼앗을 수는 있지만, 그 멤버가 Group Signature에 참여할 수 없도록 revoke 하지는 못한다.

또한, 이 논문에서 제안한 Group Signature 방법을 이용해 생성된 서명의 길이가 D. Boneh가 제안한 Group Signature[9] 방법을 이용해서 생성된 서명의 길이에 비해서 4배 이상 길다는 단점이 있다.

3. Group Signatures with Verifier-Local Revocation[12]

이 논문은 Group Signature에서 비밀키가 드러나게 된 사용자의 서명을 폐기하는 효율적인 방법을 제안한다. 즉, Group Signature에서 그룹에 소속된 사용자를 다른 그룹 멤버들에게 영향을 주지 않고, 그룹 멤버에서 제명하는 방법을 제안한다.

다른 그룹 멤버들에게 영향을 주지 않고, 한 사용자를 그룹에서 삭제하는 방법으로는 다음 세 가지가 있을 수 있다.

(1) 가장 단순한 방법으로는 새로운 서명 키를 발행하여 사용자 i를 제외한 다른 그룹 멤버들에게만 배포하는 방법이 있다. 이 방법은 서명자마다 개개의 비밀 메시지(secret message)(예를 들면, TCG chip)가 있어야 하고, 모든 서명 확인자(verifier)들에게 메시지를 공개적으로 브로드캐스트 할 필요가 있다.

(2) 좀 더 나은 revocation 방법은 하나의 짧은 브로드캐스트 메시지(short public broadcast message)를 모든 서명자와 서명 확인자에게 전송하는 것이 있다. 이 방법은 2002년 Camenisch and Lysyanskaya의 논문[13]에서 사용되었다.

(3) Brickell[14]은 revocation message를 서명 확인자에게만 보냄으로써 end user machine과 통신할 필요가 없는 좀 더 단순한 revocation 메커니즘을 제안하였다. 비슷한 메커니즘을 Ateniese et al.[15]과 Kiayias et al.[16]도 이용하였다.

이 논문에서는 Brickell[14]이 제안한 방법을 VLR Group Signature라 부르고, VLR Group Signatures의 개념을 더욱 구체화하고 있다.

이 논문의 안전성은 Strong Diffie-Hellman 가정에 근거하고 있다. 이 논문에서 제안하는 Group Signature의 길이는 1192비트로써 1024비트의 RSA 서명과 비슷한 안전성을 갖는다.

사용자를 revoke 할 때에는 revocation list RL에 revoke 할 사용자를 추가하는 방법을 사용한다. 즉, RL = $\{A_1, \cdots, A_b\}$ 형태로 사용자의 비밀키 일부를 공개하여 서명 확인자가 revoke된 사용자를 판별할 수 있도록 한다.

사이트 S가 revoke된 사용자인지 여부를 판단하는 과정은 다음과 같다.

(1) 파라미터 u, v를 다음과 같은 방법으로 생성한다.
$(u, v) = H_0(gpk, S, r)$ $1 \le r \le k$, k=128

(2) 사이트 S는 revocation list RL = $\{A_1, \cdots, A_b\}$와 한 사용자가 제출한 서명 $\sigma = (r, T_1, T_2, c, S_\alpha, S_x, S_\delta)$를 가지고 있다.

(3) RL에 속해 있는 모든 Ai에 대해서 $e(T_1, v) \cdot e(A_i, u) = e(T_2, u)$인 A_i를 찾게 되면, 해당 서

명을 제출한 사용자가 revoke 되었음을 알 수 있다.

이때, revoke된 사용자인지를 빠른 시간에 판별하기 위한 방법으로 이 논문에서는 $e(T_2, u)/e(T_1, v)$ 연산을 미리 수행하여 데이터베이스에 저장해 둔 후, 필요한 때에 데이터베이스에서 찾아보는 방법을 권장하고 있다.

이 논문에서 제안하는 방법의 경우, 사용자가 사이트 S에서 동일한 랜덤 값 r을 이용하여 서명 값을 생성할 경우 사이트 S는 두 서명에 대해 동일한 사용자가 서명하였음을 알 수 있다는 단점이 있다. 그러나, 서로 다른 사이트라면 동일한 사용자가 생성한 서명을 서로 연결 지을 수 없고(unlinkable), 또한 동일한 사이트라도 사용자가 다른 랜덤 값 r을 이용하여 서명을 생성할 경우 동일 사용자가 생성한 서명을 서로 연결 지을 수 없다.

Ⅴ. 결론

인터넷이 우리 생활에 가져다 주는 편리함과 즐거움 이면에 인터넷을 사용함으로써 우리가 원하지 않는 방법으로 많은 개인정보들이 노출되고 있다. 정당한 범위 내에서, 즉 다른 사람에게 피해를 주지 않는 범위 내에서 개인의 신분을 드러내지 않은 채 인터넷을 이용할 수 있다면, 이는 획기적인 프라이버시 보호방안이 될 수 있으리라 본다. 이러한 시도의 일환으로 익명 인증에 관한 연구가 진행되고 있고, 실생활에 적용할 수 있을 만큼 충분히 실용적인 디지털 서명 방법들이 제안되고 있다. 또한 일부 디지털 서명 방법들은 상용제품으로 사용되고 있다. 따라서 본 고에서는 익명 디지털 신용장 개념에 대한 설명과 역사에 관하여 기술하고, 익명 인증을 제공하는 디지털 서명 방법들 중 중요한 네 가지 개념에 관하여 기술하였다. 또한 Group Signature에 대한 최근 연구동향을 기술함으로써 익명 인증 시스템에 대한 현 주소를 알리고자 하였다.

● 용 어 해 설 ●

K-Strong Diffie-Hellman 가정: $G_1 \times G_2 \rightarrow G_T$인 bilinear mapping이고, $g_1 \in G_1$, g_2, g_2^r, g_2^{r2}, … $g_2^{rk} \in G_2$가 주어졌을 때, $(g_1^{1/r+x}, x)$를 연산하기 힘들다는 것을 기본 전제로 하는 가정

Proof of Knowledge: prover가 verifier와의 통신을 통해서 자신이 알고 있는 정보를 말하지 않고, 자신이 그 정보를 알고 있음을 증명하는 암호학의 한 방법

약 어 정 리

DAA	Direct Anonymous Attestation
RL	Revocation List
SDH	Strong Diffie-Hellman
TCG	Trusted Computing Group
VLR	Verifier-Local Revocation

참 고 문 헌

[1] Jan Camenisch and Anna Lysyanskayas, “An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation,” EUROCRYPT 2001, LNCS 2045, 2001.

[2] David Chaum, “Security Without Identification: Transaction Systems to Make Big Brother Obsolete,” *Communications of the ACM*, Vol.28, No.10, 1985.

[3] Ronald Leenes, “PRIME Whitepaper v2: Privacy Enhanced Identity Management,” June 2007.

[4] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Tsudik, “A Practical and Probably Secure Coalition-resistant Group Signature Scheme,” CRYPTO 2000, 2000.

[5] E. Brickell, J. Camenisch, and L. Chen, “Direct Anonymous Attestation,” *11th ACM Conf. on Compu. and Commun. Security*, 2004.

[6] M. Bellare, D. Micciancio, and B. Warinschi, “Foundations of Group Signatures: Definition, Simplified Requirements and a Construction Based on General Assumptions,” CRYPTO 2004, 2004.

[7] Ron Rivest, Adi Shamir, and Yael Tauman, “How to Leak a Secret: Theory and Applications of Ring Signatures,” ASIACRYPT 2001, 2001.

[8] Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung,

"Traceable Signatures," EUROCRYPT 2004, 2004.

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

[10] Jan Camenisch and Anna Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," CRYPTO 2004, LNCS 3152, 2004.

[11] A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," in selected Areas in Cryptography, 1999.

[12] Dan Boneh and Hovav Shacham, "Group Signatures with Verifier-Local Revocation," CCS 2004, pp.168-177.

[13] J. Camenisch and Anna Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," CRYPTO 2002, LNCS 2442, 2002, pp.61-76.

[14] E. Brickell, "An Efficient Protocol for Anonymously Providing Assurance of the Container of a Private Key," Submitted to the Trusted Computing Group, Apr. 2003.

[15] G. Ateniese, G. Tsudik, and D. Song, "Quasi-efficient Revocation of Group Signatures," *Proc. of Financial Cryptography 2002*, Mar. 2002.

[16] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Eurocrypt 2004, LNCS 3027, 2004, pp.571-589.