명시적 수신자 은닉 서명

정익래[0], 이동훈
고려대학교 정보보호센타
jir@cist.korea.ac.kr, donghlee@korea.ac.kr

Blind Signature Scheme with Explicit Identified Receiver

Ik Rae Jeong[0], Dong Hoon Lee
CIST, Korea University

요 약

본 논문에서는 전자화폐 시스템의 인출 프로토콜의 안전성에 관해서 고찰한다. 익명성을 제공하는 인출 프로토콜에서는 사용자 인증과 더불어 은닉 서명을 동시에 사용한다. 먼저 은닉 서명을 분류하고, 이들 은닉서명 프로토콜과 사용자 인증 프로토콜의 결합 방식 중에서 인증후 은닉서명 방식(Identification-then-Blind Signature)에 대한 공격을 설명한다. 그리고 인증과 은닉서명을 동시에 하는 방식(Identification-and-Blind Signature)을 이용해서 명시적 수신자 은닉 서명(Blind Signature Scheme with Explicit Identified Receiver)을 제안하며, 그것들의 안전성에 대해서 분석한다.

1 서론

전자 화폐 시스템에는 은행들과 사용자들과 상인들이 참여한다. 사용자들과 상인들은 은행들에 계좌를 가지고 있다. 화폐의 흐름은 사용자들의 계좌에서 상인들의 계좌로 세 가지 프로토콜을 통해서 흘러간다: 인출 프로토콜에 의해서 사용자는 자신의 은행 계좌에서 코인을 발급 받으며, 지불 프로토콜에 의해서 사용자는 상인에게 코인을 지불하며, 예금 프로토콜을 통해서 상인은 은행의 자기 계좌에 코인을 예치한다. 만약 은행의 개입 없이 지불이 이루어지면 오프라인 전자 화폐 시스템이라고 한다.

실물 화폐는 익명성을 보장하며 또한 사용자들이 그들의 지불 활동을 비밀로 하는 것을 선호하기 때문에 전자 화폐 시스템에서의 익명성 역시 중요하게 생각되어진다. 하지만 익명성은 범죄자들에 의해서 돈 세탁이나 약탈 등의 완전 범죄를 가능하게 한다[8]. 따라서 국가적인 차원으로 전자 화폐 시스템이 사용 가능하게 하기 위해서는 익명성을 제어할 수 있는 신뢰 기관이 존재해서 비합법적이거나 의심스러운 거래에 대해서는 사용자의 정체성을 알 수 있는 방법이 있어야 한다.

논문 [1,3,5]에서 제안하는 익명 전자 화폐 시스템은 *은닉 서명*[4]을 통해서 사용자의 익명성을 보장한다. 만약 다중 지불이나 다중 예금이 발견되면 은행은 상인과 사용자중에서 누가 부정직한지를 가릴 수 있으며 그 정체성을 알 수 있다. 이것은 사용자의 신분을 코인에 넣어서 만약 코인이 다중 지불된다면 그 거래 기록으로부터 사용자의 신분을 복구함으로서 다중 지불자를 알 수 있다.

2 은닉 서명 분류

은닉 서명은 다음과 같이 세가지 부류로 나누어 볼 수 있다.

1. *보통 은닉 서명 (Normal Blind Signature)* : 서명자가 수신자에게 서명하되 생성되는 메시지와 서명을 알 수 없게 하는 방식이다.

2. *암시적 수신자 은닉 서명 (Blind Signature with Implicitly Identified Receiver)* : 보통 은닉 (그룹) 서명의 기능 뿐만 아니라 서명자가 수신자 비밀값의 위탁값(commitment)을 은닉 (그룹) 서명 안에 집어 넣는 은닉 (그룹) 서명 방식이다.

3. *명시적 수신자 은닉 서명 (Blind Signature with Explicitly Identified Receiver)* : 보통 은닉

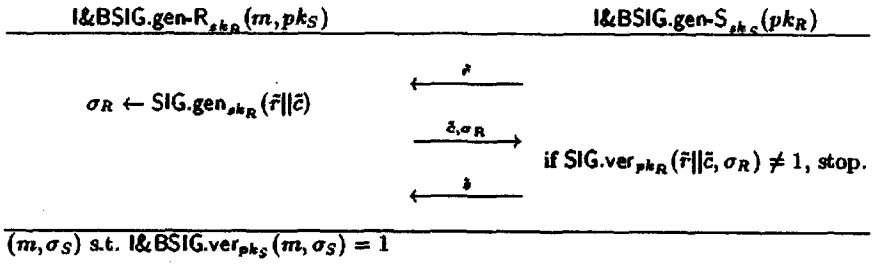

그림 1 명시적 수신자 은닉 서명으로 전환

서명의 기능 뿐만 아니라 서명자가 수신자의 신원을 확인할 수 있는 서명 방식이다.

은닉 서명은 암시적임과 동시에 명시적 수신자 은닉 서명이 될 수 있다.

예로서, 보통 은닉 서명은 논문 [2]에, 암시적 수신자 은닉 서명은 논문 [1]에, 보통 은닉 그룹 서명은 논문 [7]에, 그리고 암시적 수신자 은닉 그룹 서명은 논문 [6]에 나와 있다. 명시적 수신자 은닉 서명은 저자가 아는 한도에서는 아직 없으며 다음 절에서 제안한다.

은닉 서명 방식들이 만족해야 하는 요구사항은 다음과 같다.

1. *위조 불가능성 (Unforgeability)* : 서명자가 발급한 n개의 은닉 서명을 가지고서 n+1개 이상의 은닉 서명을 만들 수 없어야 한다.

2. *은닉성 (Blindness)* : 서명자는 사용자의 은닉 서명을 보고서 어느 시점에 자신이 발급했는지를 알 수 없어야 한다.

3 인출 프로토콜의 요구사항

익명성을 제공하는 전자 화폐 시스템의 인출 프로토콜의 요구사항은 다음과 같다.

1. *사용자 인증 (Identification)* : 사용자는 그의 신원을 은행에게 증명해야 한다.

2. *위조 불가능성 (Unforgeability)* : 사용자는 은행으로부터 발급받은 코인 이외의 다른 사용 가능한 코인을 만들 수 없어야 한다.

3. 은닉성*(Blindness)* : 은행은 사용자에게 어떤 코인을 발급하는지 알 수 없어야 한다.

4. *원자성 (Atomity)* : 인출 프로토콜 안에서 신원을 인증한 사용자하고 사용가능한 코인을 발급받는 사용자하고 같은 사람이어야 한다.

4 하이재킹(Hijacking attacks)

인출 프로토콜의 요구사항을 만족하는 전자 화폐 시스템을 설계하기 위해서 인증 프로토콜을 수행한 다음 은닉 서명 프로토콜을 수행하는 방식 - ItBS (Identification-then-Blind Signature) - 을 생각할 수 있다. 하지만 이 방식은 암시적 수신자 은닉 서명을 사용할 때는 안전해 보이는데 반하여, 보통 은닉 서명을 사용할 때는 안전하지 않다. 보통 은닉 서명을 이용한 ItBS 방식에 대해서 다음과 같은 하이재킹 공격이 가능하다.

하이재킹 공격 : 공격자는 정직한 사용자가 인출 프로토콜을 수행할 때 인증 프로토콜 부분의 수행이 끝날때까지 기다린다. 인증 프로토콜이 끝나면 정직한 사용자를 막고, 공격자가 대신 보통 은닉 서명 프로토콜을 수행해서 사용가능한 코인을 발급받는다. 이 후 공격자는 이 코인을 아무 제한없이 사용할 수 있다.

암시적 은닉 서명을 사용한 ItBS 방식에서는 하이재킹 공격을 하더라도 공격자는 정직한 사용자 위탁값에 들어있는 비밀값을 모르므로 사용가능한 코인을 얻을 수 없다.

5 새로운 결합 방식 제안

보통 은닉 서명을 사용해서 인증 프로토콜을 설계할 경우에는 ItBS 방식은 안전하지 않으므로 이 절에서는 안전한 두 결합 방식을 제안한다.

제안하는 보통 은닉 서명을 사용한 두가지 결합 방식은 다음과 같다.

1. AKEtBS (Authenticated Key Exchange then Blind Signature) : 키교환 프로토콜을 수행해서 MAC (Message Authentication Code) 키를 만든 다음 보통 은닉 서명 프로토콜의 메시지들에 MAC을 덧붙이는 방식이다.

2. 명시적 수신자 은닉 서명을 사용하는 방식 :

보통 은닉 서명을 명시적 수신자 은닉 서명으로 바꾼 다음 인출 프로토콜에서 사용한다. 보통 은닉 서명 프로토콜이 3가지 메시지로 구성될 때 이것을 사용자 서명을 이용하여 명시적 수신자 은닉 서명 프로토콜로 바꾸는 방법을 그림1에 나타낸다.

제안하는 두가지 방식중에서 두 번째 방식이 메시지 개수나 계산량에서 더욱 효율적이다.

정리 1. 사용자가 사용하는 서명 스킴이 위조 불가능성을 만족하고, 기본이 되는 은닉서명이 위조 불가능성과 은닉성을 만족한다면, 두 번째 방식으로 생성되는 명시적 수신자 은닉 서명은 사용자 인증, 위조 불가능성, 은닉성, 그리고 원자성을 만족한다.

이 정리를 증명했으나 이 논문에서는 공간 부족으로 각각에 대해서 간략하게 살펴본다.

1. 사용자 인증 : $\tilde{r}||\tilde{c}$ 에 대한 서명을 이용하여 사용자가 개인키를 알고 있는지를 테스트한다.

2. 위조 불가능성 : 사용자의 서명은 은닉서명을 위조하는데 아무런 도움이 되지 않는다. 따라서 만약 명시적 수신자 은닉 서명을 위조할 수 있으면 기본이 되는 은닉 서명을 위조할 수 있음을 보일 수 있다.

3. 은닉성 : 사용자의 서명은 은닉서명의 은닉성을 깨는데 아무런 도움이 되지 않는다. 따라서 만약 명시적 수신자 은닉 서명의 은닉성을 깨면 기본이 되는 은닉 서명의 은닉성을 깰 수 있음을 보일 수 있다.

4. 원자성 : 만약 공격자가 다른 사람의 인출 프로토콜을 사용하여 사용가능한 코인을 만들 수 있다면, 이 공격자를 사용하여 사용자가 사용하는 서명 스킴의 위조 불가능성이나, 은닉 서명의 은닉성이나 위조 불가능성을 깰 수 있음을 보일 수 있다.

6 결론

보통 은닉 서명을 사용해서 인증 프로토콜을 설계하는 방식중에서 ItBS 방식에 대한 하이재킹 공격을 보였으며, 이를 막을 수 있는 두가지 방식을 제안했다.

참고문헌

[1] S. Brands. Untraceable off-line cash in wallets with observers. Advances in Cryptology - CRYPTO '93, volume 773 of Lecture Notes in Computer Science), pages 302-318. Springer-Verlag, 1993.

[2] J. Camenisch, U. Maurer, and M. Stadler. Digital payment systems with passive anonymity-revoking trustees. Computer Security - ESORICS '96, volume 1146 of Lecture Notes in Computer Science, pages 33-43, Springer-Verlag, 1996.

[3] J. Camenisch, J. M. Piveteau, and M. Stadler. An efficient payment system protecting privacy. Computer Security - ESORICS 94, volume 875 of Lecture Notes in Computer Science, pages 207-215. Springer-Verlag, 1994.

[4] D. Chaum. Blind signature systems. In D. Chaum, editor, Advances in Cryptology - CRYPTO '83, page 153. Plenum, 1983.

[5] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. Advances in Cryptology-CRYPTO '88, volume 403 of Lecture Notes in Computer Science, pages 319-327. Springer-Verlag, 1990.

[6] Ik Rae Jeong and Dong Hoon Lee. Anonymity Control in Multi-bank E-Cash System. INDOCRYPT 2000, Lecture Notes in Computer Science 1977, Springer-Verlag, pp. 104-116, 2000.

[7] A. Lysyanskaya and Z. Ramzan. Group Blind Digital Signatures: A Scalable Solution to Electronic Cash, Proceedings of the Second International Conference on Financial Cryptography, volume 1465 of Lecture Notes in Computer Science), pages 184-197, Springer-Verlag, 1998.

[8] S. von Solms and D. Naccache. On blind signatures and perfect crimes. Computer & Security, volume 11, pages 581-583, 1992