Linkable 은닉 서명방식

김승주*, 박성준**, 원동호*

* 성균관대학교 정보공학과

** 한국정보보호센터

Linkable Blind Signatures

Seungjoo Kim*, Sungjun Park** and Dongho Won*

* Department of Information Engineering, Sung Kyun Kwan University

** KISA (Korea Information Security Agency)

E-mail : sjkim@dosan.skku.ac.kr

요 약

D. Chaum은 묵지가 내장된 봉투를 사용하는 실제적인 상황을 수식으로 표현한 은닉 서명방식을 제안하였다. 이 방식은 메시지를 숨기는 서명 방식으로 제공자의 신원과 메시지를 연결시킬 수 없는 익명성을 유지할 수 있다. 또한 M. Stadler 등은 전자화폐에서의 돈 세탁 문제를 해결하는 공정한 은닉 서명방식을 제안하였다.

본 논문에서는 비밀키의 일부를 공개함으로써 은닉 서명을 제공자의 신원과 연결시킬 수 있는 "linkable 은닉 서명방식"을 제안한다. 또한, M. Stadler 등의 공정한 은닉 서명방식이 linkable 은닉 서명방식의 한 종류임을 살펴보고, 공정한 은닉 서명방식의 문제점과 해결방안을 제시한다.

1. 서 론

현재 우리는 컴퓨터와 통신이 비약적으로 발전한 정보화 사회에 살고 있다. 정보화 사회에서는 모든 정보가 전자화 되며 그 전자화된 정보가 정치, 경제의 중요한 가치로 인정을 받는다. 이러한 정보화 사회에서는 통신망을 이용한 전자 거래 결재가 필수적이다. 그렇지만 기존의 현금의 형태는 전자 거래에 이용하기에는 적절치 못하다. 그래서 새로운 화폐가 요구되는데 그것이 전자화폐이다.

전자화폐의 가장 핵심적인 기술인 추적 불가능성(untraceability), 프라이버시(privacy) 제공 기술 등을 제공하기 위하여 일반적으로 D. Chaum의 은닉 서명방식(blind signatures)을 이용한다. Crypto'82에서 D. Chaum이 제안한 은닉 서명 방식은 제공자(provider)의 신원과 메시지를 연결시킬 수 없는(unlinkability) 익명성을 유지할 수 있는 서명방식이다. 또한 M. Stadler외 2인은 Eurocrypt'95에서 전자화폐에서의 추적불가능성이 돈 세탁 등의 범죄에 악용될 수 있는 문제점을 지적하고, 이러한 문제를 해결하고자 하는 공정한 은닉 서명방식(fair blind signatures)을 제안하였다.

본 논문에서는, 새로운 개념인, 비밀키의 일부를 공개함으로써, 대응하는 하나의 은닉 서명만 선택적으로 혹은 전체 은닉 서명을 모두 제공자의 신원과 연결시킬 수 있는 "linkable 은닉 서명

방식(linkable blind signatures)"을 제안하고 3 가지 종류의 linkable 은닉 서명방식 - (1) 제공자에 의한 linkable 은닉 서명방식, (2) 제3자에 의한 linkable 은닉 서명방식, (3) 제공자 또는 제3자에 의한 linkable 은닉 서명방식 - 을 소개한다. 또한 M. Stadler 등의 공정한 은닉 서명방식이 제3자에 의한 linkable 은닉 서명방식임을 살펴보고, 문제점을 제시하며 이의 해결방안을 제시한다.

2. 기존의 은닉 서명방식

D. Chaum은 개인의 프라이버시를 유지하면서 전자화폐를 사용할 수 있는 방안으로 묵지가 내장된 봉투를 사용하는 상황을 암호를 이용하여 구현한 은닉 서명방식을 제안하였다. 은닉 서명방식의 개념적인 내용은 다음과 같다.

[정의 2.1] 은닉 서명방식 (blind signatures)[1] … 은닉 서명은 기본적으로 임의의 디지틀 서명을 만들 수 있는 서명자(signers)와 서명 받을 메시지를 제공하는 제공자(providers)로 구성되어 있는 서명방식으로, 제공자의 신원과 (메시지, 서명) 쌍을 연결시킬 수 없는 "unlinkability" 특성을 유지할 수 있는 서명 방식을 말한다.

D. Chaum은 이러한 은닉 서명방식을 이용하여 최초의 이론적인 전자화폐 방식인 추적불가능한 전자화폐를 제안하였다. 또한, M. Stadler, J. M. Piveteau, J. Camenisch 등은 전자화폐에서의 추적불가능성이 돈 세탁이나 탈세 등의 범죄에 악용될 수 있음을 지적하고, 이러한 문제를 해결하고자 문제가 되는 경우에 신뢰 기관이 비밀 정보를 공개함으로써, 제공자의 신원과 (메시지, 서명) 쌍을 연결시킬 수 있는 공정한 은닉 서명방식을 제안하였다. 공정한 은닉 서명방식의 정의는 다음과 같다.

[정의 2.2] 공정한 은닉 서명방식 (fair blind signatures)[2] … 공정한 은닉 서명방식은 신뢰 기관(trusted entity)이 필요시에 자신의 비밀 정보의 일부를 공개함으로써, 서명자가 제공자의 신원과 (메시지, 서명) 쌍을 연결시킬 수 있는 은닉 서명방식을 말한다.

M. Stadler 등은 cut-and-choose 방식, oblivious transfer 방식, registration 방식을 이용한 공정한 은닉 서명방식을 제안하였다.

3. Linkable 은닉 서명방식

linkable 은닉 서명방식(linkable blind signatures)은 제공자의 신원과 메시지를 연결시킬 수 없는 익명성을 유지하도록 하되, 문제가 되는 경우 대응되는 비밀 정보를 공개함으로써, 제공자의 신원과 메시지를 연결시킬 수 있도록 하는 서명방식을 말한다.

[정의 3.1] linkable 은닉 서명방식 (linkable blind signatures) … linkable 은닉 서명방식은 제공자의 신원과 (메시지, 서명) 쌍을 연결시킬 수 없는 익명성을 유지하도록 하되, 필요시에 비밀키의 일부를 공개함으로써, 대응하는 하나의 (메시지, 서명) 쌍만 선택적으로 혹은 전체 (메시지, 서명) 쌍을 모두 제공자의 신원과 연결(linkability)시킬 수 있는 서명방식을 말한다. 비밀키의 소유에 따라 linkable 은닉 서명방식에는 다음의 3가지가 있을 수 있다.

(1) 제공자에 의한 linkable 은닉 서명방식 (linkable blind signatures by provider)
(2) 제3자에 의한 linkable 은닉 서명방식 (linkable blind signatures by third party)
(3) 제공자 또는 제3자에 의한 linkable 은닉 서명방식 (linkable blind signatures by provider or third party)

[정의 3.2] 제공자에 의한 linkable 은닉 서명방식 (linkable blind signatures by provider) … 제공자에 의한 linkable 은닉 서명방식은 필요시에 제공자가 자신의 비밀키의 일부를 공개함으로써, 대응하는 하나의 (메시지, 서명) 쌍만 선택적으로 혹은 전체 (메시지, 서명) 쌍을 모두 자신의 신원과 연결시킬 수 있는 서명방식을 말한다.

전자화폐의 특성 중에서 특히 "프라이버시(privacy)"는 어디에 전자화폐를 사용하였거나 어디서 전자화폐를 가져왔는 가에 대한 개인의 비밀정보를 다른 사람이 알 수 없게 하는 것이다. 그러나 자신의 전자화폐가 분실되었거나 강탈을 당한 경우에 이러한 프라이버시는 전자화폐 시스템의 안전성을 떨어뜨리는 요인이 될 수 있다. 이러한 경우에 위의 제공자에 의한 linkable 은닉 서명방식이 유용하게 사용될 수 있다. 즉, 자신의 전자화폐가 분실되었거나 전자화폐 강탈을 당한 경우에 사용자가 자신의 비밀키를 공개함으로써 수표의 분실 신고와 같은 기능을 할 수 있다.

[정의 3.3] 제3자에 의한 linkable 은닉 서명방식 (linkable blind signatures by third party) … 제3자에 의한 linkable 은닉 서명방식은 필요시에 신뢰받는 제3자가 자신의 비밀키의 일부를 공개함으로써, 대응하는 하나의 (메시지, 서명) 쌍만 선택적으로 혹은 전체 (메시지, 서명) 쌍을 모두 제공자의 신원과 연결시킬 수 있는 서명방식을 말한다.

Eurocrypt'95에서 소개된 M. Stadler 등의 공정한 은닉 서명방식은 "제3자에 의한 linkable 은닉 서명방식"을 만족하는 예이다. 하지만 M. Stadler 등의 방식은 제공자가 "자신의 전자화폐가 분실 혹은 강탈되었다"고 주장하는 경우에, 진위를 판별할 수 없다는 문제점이 있다. 그러므로 공정한 전자화폐 시스템을 구성하기 위해서는 다음의 "제공자 또는 제3자에 의한 linkable 은닉 서명방식"을 이용하여야 한다. 즉, 필요에 따라 신뢰기관이 전자화폐의 제공자를 추적하는 경우에, 이 전자화폐의 분실 또는 강탈 여부를 판단할 수 있어야 한다.

[정의 3.4] 제공자 또는 제3자에 의한 linkable 은닉 서명방식 (linkable blind signatures by provider or third party) … 제공자 또는 제3자에 의한 linkable 은닉 서명방식은 필요시에 제공자나 제3자가 비밀키의 일부를 공개함으로써, 대응하는 하나의 (메시지, 서명) 쌍만 선택적으로 혹은 전체 (메시지, 서명) 쌍을 모두 제공자의 신원과 연결시킬 수 있는 서명방식을 말한다.

4. 프로토콜

공개키 암호인 RSA 암호와 blob(· , ·)을 이용하여 구현한 linkable 은닉 서명방식은 다음과 같다. 여기서, 서명자의 RSA 공개키 암호의 공개키를 (n, e)라 하고 비밀키를 d라고 하자.

프로토콜 (protocol)

(1) 제공자는 먼저 난수 $r \in Z_n$를 선택하여 $t = blob(m, f_{k_{seed}}(m)) \cdot r^e \pmod n$을 계산한 후 서명자에 보낸다. 이 때, m은 식별정보를 포함할 수 있다.

제3자에 의한 linkable 은닉 서명방식, 제공자 또는 제3자에 의한 linkable 은닉 서명방식의 경우에는 k_{seed}의 정당성을 확인한다.

(2) 서명자는 비밀키 d를 이용하여 $t^d = (blob(m, f_{k_{seed}}(m)) \cdot r^e)^d \pmod n$을 계산한 후 제공자에게 돌려준다.

(3) 제공자는 자신만이 알고 있는 난수(blind factor) r를 이용하여 $t^d/r = (blob(m, f_{k_{seed}}(m)))^d \pmod n$을 계산하면 $(blob(m, f_{k_{seed}}(m)), (blob(m, f_{k_{seed}}(m)))^d)$가 서명자로부터 받은 linkable 은닉 서명이 된다.

여기서, k_{seed}의 소유주에 따라 제공자에 의한 linkable 은닉 서명방식, 제3자에 의한 linkable 은닉 서명방식, 제공자 또는 제3자에 의한 linkable 은닉 서명방식을 구성할 수 있다.

전체 은닉 서명을 모두 변환 (linkage of all signatures)

(1) 제공자(제3자)는 f의 비밀키 k_{seed}를 공개한다.

(2) 이를 받은 자는 누구나 m을 확인하여 임의의 $(blob(m, f_{k_{seed}}(m)), (blob(m, f_{k_{seed}}(m)))^d)$ 쌍을 제공자의 신원과 연결시킬 수 있다.

특정한 은닉 서명만 선택적으로 변환 (selective linkage)

(1) 제공자(제3자)는 자신이 선택한 $blob(m, f_{k_{seed}}(m))$에 대응하는 $f_{k_{seed}}(m)$을 공개한다.

(2) 이를 받은 자는 제공자(제3자)가 선택한 (메시지, 서명) 쌍만을 제공자의 신원과 연결시킬 수 있다.

5. 결 론

본 논문에서는 은닉 서명방식의 "unlinkability" 특성을 필요에 따라 통제할 수 있는 linkable 은닉 서명방식을 정의하였으며, 3 가지 종류의 linkable 은닉 서명방식 즉, 제공자에 의한 linkable 은닉 서명방식, 제3자에 의한 linkable 은닉 서명방식, 제공자 또는 제3자에 의한 linkable 은닉 서명방식을 제안하였다. 또한 기존의 공정한 은닉 서명방식이 제3자에 의한 linkable 은닉 서명방식의 특성을 가짐으로써 생기는 문제점을 지적하고, 이의 해결방안을 제시하였다.

향후에는 linkable 은닉 서명방식의 정의와 요구 조건을 좀 더 구체화하고, 이 조건을 만족하는 효율적인 linkable 은닉 서명방식 프로토콜을 제안하며, 또한 이를 이용한 공정한 전자화폐 시스템을 제안하고자 한다.

참 고 문 헌

[1] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology - Crypto'82, 1983, pp. 199-203.

[2] M. Stadler, J-M. Piveteau and J. Camenisch, "Fair Blind Signatures," Advances in Cryptology - Eurocrypt'95, 1995, pp. 209-219.

[3] S. Micali, "Fair Public-key Cryptosystens," Advances in Cryptology - Crypto'92, 1992, pp. 113-138.

[4] J. Kilian and T. Leighton, "Fair Cryptosystems, Revisited," Advances in Cryptology - Crypto'95, 1995. pp. 208-221.

[5] 박춘식, 이대기, "전자화폐가 세계를 바꾼다," 통신정보보호학회지, 1996. 6., pp. 53-70.

[6] 김지연, 김승주, 원동호, "블랙리스트 기능을 갖는 양도가능한 전자현금시스템," 한국통신학회 학술발표회 논문집, 1996. 7., pp. 609-612.