전자면허를 이용한 전자현금시스템의 문제점 분석

김지연*, 이동렬**, 원동호*

* 성균관대학교 정보공학과
** 중부대학교 전자계산학과

Analysis of Electronic Cash System using Electronic License

Jeeyeon Kim*, Dongryul Lee** and Dongho Won*
* Dept. of Information Engineering, Sung Kyun Kwan University
** Dept. of Computer Science, Joong Bu University
E-mail : jykim@dosan.skku.ac.kr

요 약

T. Okamoto와 K. Ohta는 전자현금의 발급과정을 간략히 하기 위해 전자면허의 개념을 도입하였다. 전자면허란, 은행에서 현금을 발급받을 수 있는 일종의 자격증이다. 전자면허 발급 프로토콜은 전자현금 발행 프로토콜 이전에 오직 한 번만 수행되고 이후에는 이 전자면허를 이용하여 전자현금의 발행 프로토콜을 단순화시킬 수 있는 장점을 지닌다.

본 논문에서는 전자면허를 사용하는 기존의 전자현금시스템이 사용자의 프라이버시를 침해하는 문제점이 있음을 지적한다.

1. 서 론

현재 전 세계의 거의 모든 컴퓨터가 인터넷이라는 거대한 네트워크에 연결이 되어 있다고 해도 과언이 아니다. 이러한 인터넷을 이용한 전자상거래는 가장 유망한 새로운 사업으로 떠오르고 있다. 전자상거래에서 가장 중요한 문제는 지불 방법에 관한 것이다. 현재에는 신용카드를 많이 이용하나, 신용카드의 모든 거래내역은 은행 또는 카드회사에서 알 수 있으므로 사용자의 프라이버시를 보장하지 못한다는 문제점이 있다. 사용자의 프라이버시도 보장하면서 네트워크에 적합한 형태의 새로운 무언가가 필요한데 그것이 바로 전자현금이다.

즉, 전자현금이란, 물리적 화폐의 특성을 모두 갖춘 디지틀화된 정보이다.

전자현금의 가장 최소한의 요구조건은 불추적성과 중복사용의 방지이다. 불추적성이란, 사용자의 거래가 어디에서 이루어졌는 지 알려져서는 안되고 거래가 두 번이상 일어났을 경우, 그 거래가 같은 사람에 의한 것이라는 것도 알려져서도 안된다. 이것은 은행에 대해서는 물론이고 은행과 상점 또는 다른 사용자와의 공모를 해도 보장되어야 한다. 그리고 전자현금은 디지틀화된 정보이기 때문에 복사가 용이하다. 그러므로 같은 전자현금의 중복사용의 방지는 필수적이다. 만약, 전자현금시스템이 매 거래시마다 은행이 개입하는 온라인 시스템일 경우에는 중복사용을 미리 막을 수 있으나 은행이 개입이 필요없는 오프라인일 경우에는 막을 방도가 없다. 그래서 한 번 사

용할 때에는 사용자의 프라이버시가 보장되지만, 중복사용할 경우에는 사용자의 개인식별정보가 드러나는 방법을 사용한다.

Chaum은 최초로 불추적성과 중복사용 방지를 만족하는 전자현금시스템을 제안하였다.[1] 그러나, 이 시스템은 매 거래가 발생할 때마다 은행이 개입해야하는 단점이 있다.

이러한 단점을 극복한 것인 Chaum, Fiat, Naor의 전자현금시스템(이하, CFN 시스템)이다.[2] 그러나 CFN 시스템은 중복사용을 방지하기 위해 전자현금의 발급 프로토콜에서 cut-and-choose 방식을 사용하므로 매우 비효율적이다.

Okamoto와 Ohta는 전자현금의 발급 프로토콜을 간략히 하기위해 전자면허의 개념을 도입하여 보다 효율적인 전자현금시스템(이하, OO 시스템)을 제안하였다.[3] 그리고 이 시스템에서 Okamoto와 Ohta는 전자현금에 대한 요구조건으로 양도성과 분할성을 추가하였다.

그러나, OO 시스템은 전자현금의 가장 중요한 요건인 불추적성을 만족하지 못한다.

본 논문에서는, 2장에서 OO 시스템을 살표보고, 3장에서 전자면허를 이용한 시스템들[3][4][5][6]이 왜 불추적성을 만족하지 못하는 지를 알아본다.

2. OO의 전자현금시스템

OO 시스템이전의 전자현금시스템은 전자현금을 발행받을 때 은닉서명기법과 cut-and-choose 방법을 이용한다. 전자현금을 발행받을 때마다 cut-and-choose 방법을 사용하므로 매우 비효율적이다. 이러한 단점을 극복하기 위해 Okamoto와 Ohta는 전자면허의 개념을 도입하였다.

전자면허란, 은행에서 발행하는 현금을 사용할 수 있는 일종의 자격증으로 전자현금의 발행과정 이전에 발급받아야 한다. 전자면허 발급과정은 사용자가 현금을 정당하게 사용하면, 계좌 개설시에 오직 한 번만 수행되며 이후에는 전자면허 발급없이 바로 전자현금을 발급받을 수 있다.

OO 시스템의 전자면허 발급 과정에서는 은닉서명기법과 cut-and-choose방법을 사용하여 전자면허를 발행한다. 이 전자면허는 이후에 사용자의 계좌에서 인출되는 전자현금의 한 부분이 된다. 전자현금 프로토콜에서는 전자면허를 이용하므로 cut-and-choose 방식을 사용하지 않는다. 그러므로 CFN 시스템보다 훨씬 효율적으로 전자현금을 발행받을 수 있는 것이다.

본 절에서는 OO 시스템을 간략히 살펴보겠다.

[기호 정의]

P : 사용자

A : 은행

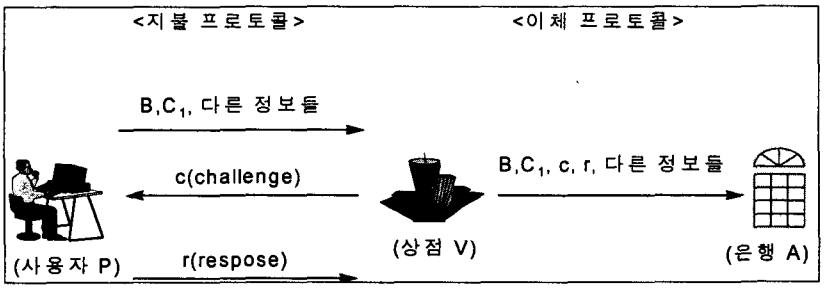
V : 상점

B : 전자면허, $B = Sig_A[g(\text{사용자의계좌번호}||\text{다른 정보들})]$
(단, g : 일방향 해쉬함수)

C_i : 전자현금, $C_i = Sig_A[g(B||b_i)]$ $(i = 1, \ldots, n)$(단, b_i는 난수)

전자면허 발급프로토콜과 전자현금 발급프로토콜을 수행하고 난 후 사용자 P는 전자면허 B와 전자현금 C_i를 가지게 된다. 사용자는 지불 프로토콜을 통해 상점 V에게 (B, C_i, 다른 정보들)

을 보내게 된다. 상점은 B와 C_i의 정당성을 확인한 후 정당하면, 전자현금을 받아들인다. 시간이 흐른 후, 상점은 전자현금을 자신의 계좌로 이체하기 위해 은행에게 이 정보를 전송한다. 은행은 전송된 정보들의 정당성과 전자현금이 이전에 사용되지 않았음을 확인한 후, 상점의 계좌로 해당하는 현금을 이체하고 자신의 데이터 베이스에 저장한다. 이 과정은 [그림 1]과 같다. c와 r은 사용자가 전자현금을 중복사용했을 때 사용자의 개인식별정보를 드러나도록 하는데에 이용된다.



[그림 1] OO 시스템의 지불 프로토콜과 이체 프로토콜

3. 기존 전자면허의 문제점

전자현금시스템에서 가장 중요한 관심사 중의 하나는 사용자의 프라이버시를 보호하기 위한 불추적성이다. Ferguson은 자신의 논문[7]에서 프라이버시에 대해 다음과 같은 정의를 내렸다.

① 허위 프라이버시(Fake Privacy)

약한 개념의 불추적성으로 은행과 모든 상점은 공모를 하더라도 프로토콜 사본을 보고 사용자가 어디에 돈을 사용했는지에 관한 정보를 알 수 없어야 한다.

② 프라이버시(Privacy)

강한 개념의 불추적성으로 은행은 두 개의 거래가 발생했을 경우, 모든 상점이 공모를 하더라도 그 거래가 동일한 사람에 의한 것인지를 판별할 수 없어야 한다.

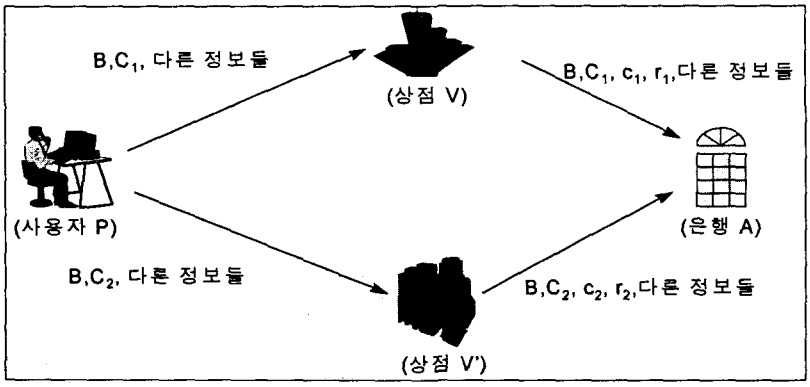
만약, 프라이버시 조건을 보장하지 못한다면, 허위 프라이버시 조건은 보장하지 못한다. 예를 들어, 실제상황에서는 개인이 단골로 가는 상점이 있다면, 그 상점에서는 개인이 누구인지를 안다. 만약, 두 개의 거래가 같은 사람에 의한 것임을 알고 그 중 한 거래의 사용자가 누구인지가 드러난다면, 그 이후의 그 사용자의 모든 거래는 어디에서 이루어지는 지가 밝혀진다. 즉, 프라이버시 조건이 보다 더 강력한 요구조건이라 볼 수 있다.

Ferguson은 Chaum의 시스템과 CFN 시스템은 위의 두 조건을 모두 만족하나, 분할성을 갖는 OO 시스템은 분할되어진 현금 조각마다 동일한 전체 현금 정보를 포함하므로 프라이버시의 조건을 만족하지 못함을 지적하였다.

또한, Stadler 등은 EUROCRYPTO '96에서 불추적성 때문에 전자현금이 돈세탁이나 탈세 등의 범죄에 이용될 수 있음을 지적하고 이를 막기 위해 특수한 상황(법정 요구 등)에서는 신뢰센터

(예를 들어 정부)가 전자현금을 추적할 수 있도록 하는 정당한 은닉서명기법(fair blind signatures)을 제안하였다.[8] 그리고 그 기법을 구현하기 위해 cut-and-choose방식, oblivious transfer기법 그리고 신뢰센터에 자신의 비밀 정보를 등록하는 방법을 이용하였다. 그들은 논문에서 제안한 방법 중 등록을 이용한 정당한 은닉서명기법은 한 사람이 각각 다른 메시지에 대해 서명을 받았을 경우, 그 두 서명이 같은 사람에 의한 것이라는 것을 알 수 있는 문제가 발생한다고 밝히고 있다.

본 절에서는 OO 시스템을 비롯한 전자면허를 사용하는 전자현금시스템에서도 앞에서 살펴본 것과 같은 문제점이 발생함을 보이도록 한다. 다시, 2절에서의 OO 시스템을 살펴보도록 하자. OO 시스템에서 사용자 P가 [그림2]와 같이 두 개의 거래를 수행했을 경우를 생각해 보자.



[그림 2] OO 시스템에서 두 개의 거래가 발생한 경우

은행 A는 상점 V와 V'로부터 전송받은 정보에 포함된 같은 전자면허(B)를 보고, 그 거래가 사용자 P에 의한 것인지는 알 수 없으나, 동일한 사람에 의한 것임을 확인할 수 있다. 즉, Ferguson의 프라이버시 조건을 만족하지 못한다.

또한, 기존의 전자면허를 이용한 모든 시스템[3][4][5][6]은 OO 시스템과 같은 원리이므로 같은 문제점이 나타난다.

4. 결 론

Okamoto등이 제안한 시스템은 전자면허를 이용하여 전자현금 프로토콜 과정을 단순화시킨 장점이 있다. 그러나 사용자의 모든 지불 사본에 동일한 정보(전자면허)가 포함되므로 두 거래가 발생했을 경우 은행은 그 두 거래가 누구에 의한 것임은 알 수 없으나, 동일한 사람에 의한 것임을 확인할 수 있다. 즉, 전자현금의 가장 중요한 특성인 불추적성을 만족하지 못하는 문제점이 있다.

향후에는 전자면허를 이용하면서도 불추적성을 만족하는 효율적인 전자현금시스템을 제안하도록 하겠다.

참 고 문 헌

[1] D. Chaum, "Blind Signatures for untraceable payments", Proc. of Crypto '82, pp. 199-203, 1982

[2] D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash", Proc. of Crypto '88, pp. 319-327, 1988

[3] T. Okamoto and K. Ohta, "Universal Electronic Cash", Proc. of Crypto '91, pp. 324-337, 1991

[4] T. Okamoto, and K. Ohta, "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash", Proc. of Crypto '89, pp. 481-496, 1989

[5] J. C. Pailles, "New Protocol For Electronic Money", Proc. of AUSCRYPT'92, pp.7.1-7.6, 1992

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

[7] N. Ferguson, "Single Term Off-Line Coins", Porc. of EUROCRYPTO '93, pp. 318-328, 1993

[8] M. Stadler, J. M. Piveteau, and J. Camenisch, "Fair Blind Signatures", Proc. of EUROCRYPTO '95, pp. 209-219, 1995