수신자 지정 서명을 이용한 안전한 전자지불시스템에 관한 연구

강서일, 이임영
순천향대학교 정보기술공학부

A study on Secure Electronic Payment System Using Nominate Signature

Se-Il Kang, Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang University

요 약

전자화폐는 전자상거래의 발달로 인해 이용이 높아지고 있다. 전자화폐는 실질 화폐의 가치를 가지고 있으므로, 여러 가지의 보안 사항 및 요구 사항이 필요하다. 그 중에서 익명성의 제공은 사용자의 프라이버시를 제공할 수 있는 방안이다. 보안 기술로는 은닉 서명 방식을 이용하는데 서명자가 메시지의 내용을 알 수 없는 상태에서 서명을 하는 것으로 사용자만이 값을 알고 있다. 그러나 서명 받을 메시지의 정당성을 확인하는 연산을 수행하여야 한다. 본 논문에서 제안하는 것은 수신자 지정 서명방식을 이용하여, 전자화폐를 발급받고 이를 이용한다. 수신자 지정 서명은 서명자가 선택하는 검증자만이 확인 가능하므로, 전자화폐를 다른 제 3자가 이용할 수 없게 된다. 그러나 익명성을 제공할 수 없으므로, 변형이 필요하다. 제안 방식은 사용자의 지정을 통해 정당한 사용자만이 검증 할 수 있으며, 익명성의 제공을 위해 사용자가 선택한 임의 값을 삭제한다.

1. 서론

전자화폐는 실질화폐처럼 이용하기 위해서는 여러 가지 특징을 가져야 한다. 그 중에서도 사용자의 프라이버시를 제공하는 방안으로 익명성이 있다. 익명성은 사용자가 활용하는 전자화폐와 사용자를 연결할 수 없는 것으로, 사용자가 물건을 구매하고, 지불한 전자화폐를 가지고 사용자를 알 수 없는 경우를 말한다.

이러한 방안으로 이용되는 암호 기술은 은닉 서명이다. 은닉 서명은 사용자가 서명을 받을 메시지에 임의 값을 곱하여 서명받기 위해 전송하고, 서명을 받은 후에는 서명의 메시지 값에서 임의 값을 삭제함으로 인해 서명자는 메시지의 내용을 모르는 상태에서 서명을 제공한다. 이로 인해 서명자는 사용자로부터 메시지의 정당성을 확인 할 수 있는 방안이 제공되어야 한다. 메시지의 내용은 모르나 메시지가 사용자로부터 제공되었다는 정당성은 제공되어야 한다. 이러한 메시지의 정당성을 확인하는 방안으로 영지식 증명이나, 사용자와 은행이 서로 연산을 통해서 값을 생성하고 은행에서 은닉 서명을 제공 받아 이용한다[1, 4, 6]. 본 논문은 2장에서 전자화폐의 보안 요구사항에 논의하며, 3장에서 익명성을 제공하는 지불시스템과 관련 연구를, 4장에서 제안 방식을 설명한다. 5장에서는 제안 방식을 분석하고, 6장에서 향후 연구 방향 및 결론에 대해 논의 한다.

2. 전자화폐 보안 요구 사항

익명성은 전자화폐에서 사용자의 프라이버시를 제공하기 위해 진행되어 왔다. 전자화폐에서 익명성을 제공하기 위해서는 전자화폐를 활용하는 데이터가 사용자와 연결성이 없어야 한다. 사용자는 은행으로부터 전자화폐를 발행 받는 경우 전자화폐에 대한 이중 사용 및 사용자의 부정이 발생될 경우를 대비하는 방안이 필요로 한다. 이와 같은 보안 서비스와 동시에 익명성을 제공하여야 하는데 완전한 익명성이 제공되는 경우 사용자의 부정 이용, 돈 세탁의 취약성이 발생하였을 경우 사용자를 알 수 없는 취약성이 발생한다.

사용자는 전자화폐를 이용하는 경우 다음과 같이 전자화폐의 보안 요구 사항이 필요하다.[1, 2, 6]

- 전자화폐의 정당성 : 은닉 서명을 제공받는 메시지의 내용을 확인 할 수 없으나 메시지의 정당성을 확인 할 수 있어야 한다.

- 이중 사용에 대한 검출 방안 : 전자화폐를 이중 사용하는 경우 검출 할 수 있는 방안이 필요하다.
- 전자화폐의 수정 변경 및 위조 : 전자화폐의 내용이 변경되거나 위조, 수정되는 경우의 서명으로 인해 검출 될 수 있어야 한다.
- 오프라인성 : 전자화폐는 상점과 사용자사이에 제 3자의 개입 없이도 정당성을 확인 할 수 있어야 한다.

이외에도 전자화폐는 다른 요구 사항이 필요할 수 있다. 하지만 본 논문에서는 이상의 보안 요구사항만을 고려하였다.

3. 익명성을 제공한 지불시스템 및 관련 연구

3.1 해쉬체인을 이용한 새로운 오프라인 전자화폐

해쉬체인을 이용한 새로운 오프라인 전자화폐는 해쉬체인을 이용하여 전자화폐를 생성한다[5]. 익명성의 제공은 은닉 서명을 이용하여, 제공 받는다. 메시지의 정당성을 확인하기 위해 영지식을 이용한다. 전자화폐의 발급 프로토콜의 흐름은 다음 그림 1과 같다.

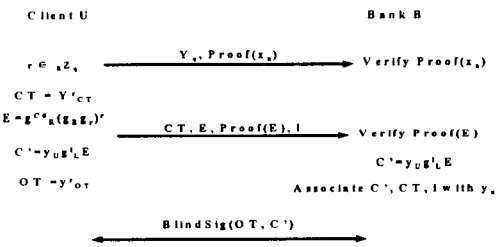

그림 1 해쉬체인을 이용한 새로운 오프라인 전자화폐

전자화폐는 해쉬체인을 이용하여 생성되며, 익명성을 제공받기 위해 제한적 은닉 서명 기술을 이용한다. 제한적 은닉서명은 서명자가 제공하는 정보와 서명 받는 사용자가 서로의 정보를 교환하여 생성하며, 이와 같은 경우 각각의 값을 연산하는 지수승 연산이 필요하다. 또한 값을 가지고 있다는 증명을 하기 위해 영지식 증명을 이용하고 있다. 영지식 증명은 각각의 값에 대해 상대방에게 알리지 않고, 정당한 값을 가지고 있음을 확인 시켜주는 방식이다.

3.2 해쉬를 이용한 익명성 제공 기술

해쉬를 이용한 방법은 해쉬값을 제공하고, 전자화폐를 이용하는 것은 해쉬되기 이전의 값을 이용한다. 해쉬의 값을 생성할 수 있다는 것을 증명할 수 있으므로 전자화폐로 활용될 수 있다. 은행에 제공되는 것은 해쉬값으로 은행은 사용자가 전송한 해쉬값과 계좌 총액에 서명을 제공한다. 전자화폐를 이용하는데 있어서는 해쉬되기 이전의 값을 이용하는 것이다. 그러므로 사용자의 전자화폐를 발급당사자인 은행은 알 수 없게 된다. 이와 같은 방식을 이용한 전자지불시스템은 An Efficient Anonymous Scheme for Secure Micropayments로써 전체적인 흐름은 그림 2과 같다.[2]

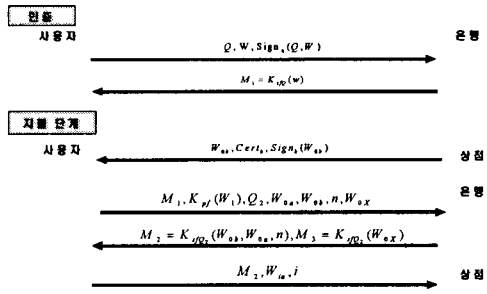

그림 2 An Efficient Anonymous Scheme for Secure Micropayments

사용자는 초기에 만든 해쉬값과 다음의 해쉬값을 등록한다. 그런데 여기에서 취약성이 발생하는데 해쉬값의 등록시 해쉬값을 다시 확인 하는 과정이 없는 관계로 인해 제 3자가 임의 값을 등록하여 이용할 수 있다. 제 3자는 임의 해쉬값을 만들어 사용하기 위해서는 임의 해쉬값과 총액만을 알고 있으면 가능하다. 첫 번째 전자 화폐는 제 3자가 이용할 수 없으나 그 이후의 전자화폐는 제 3자가 사용할 수 있는 취약성을 가지고 있다. 다른 취약성으로는 사용자와 상점, 모두 참여하여야 하며, 오프라인을 제공하지 못한다. 이유는 은행으로부터 상점의 값을 이용한 해쉬값을 제공하여야한다. 이로 인해 상점에 제약되어 전자화폐를 이용한다.

4. 제안 방식

제안 방식의 수신자 지정 서명을 방식을 이용한다. 수신자 지정 서명의 검증자 지정을 이용하여 검증자로 지정된 사용자만이 정당한 전자화폐를 생성하고, 은행이 서명을 제공하면, 사용자는 은행의 서명을 확인하고 이용한다. 상점은 사용자가 제공하는 데이터의 값을 은행의 공개키로 서명의 값을 확인 한다. 그러나 수신자 지정 서명 방식을 그대로 이용한다면, 사용자에 대한 익명성을 제공할 수 없으며, 검증자의 공개키를 이용하므로 인해 검증자의 신원이 확실하게 밝혀진다. 그러므로 검증자에게 익명성을 제공하며, 전자화폐로 이용하기 위해 다음과 같이 수신자 지정 서명에 이용되는 계수에 변형을 준다.

- 수신자의 지정 : 수신자는 검증자를 지정하기 위해 수신자 지정 서명에서 검증자의 공개키를 이용한다. 그러므로 서명을 검증하는 과정에서는 검증자의 개인키를 필요로 하며, 개인키를 알고 있는 검증자만이 검증을 할 수 있는 것이다. 문제가 발생한 경우 검증자는 자신의 개인키를 제 3자에게 영지식 증명으로 가지고 있다는 것을 보여 주며, 제 3자가 수신자의 서명의 값을 검증하도록 한다. 본 논문에서의 제안 방식은 수신자의 지정으로 이용하는 것을 g^{TW}를 이용한다. 즉, g^{TW}의 값을 사용자가 제공하면, 공개키를 이용하는 부분에서 공개키 대신 이용하여 검증자를 지정하는 부분으로 이용한다.
- 수신자와 검증자의 확인 값 : 수신자와 검증자는 세션키 k를 생성한다. 이는 은행에서 L값을 생성하여 전송하는 서명을 필요로 하지 않으며, 은행과 사용자가 서로의 공통의 값을 연산하여, 서명을 검증하는데 이용된다. 수신자 지정 서명에 있어 e값을 모든 값이 변경되었는지 검증하지만. 여기서의 e의 역할은 값의 변경도 확인하고, 수신자와 검증자가 서로 교환한 값의 변경도 확인할 수 있으며, 제 3자의 부정 개입을 막을 수 있다.
- 전자화폐의 익명성 : g^{TW}를 이용하므로 인해 사용자의 익명성을 제공할 수 있다. g^{TW}의 값을 전송하므로 상점에 이용하는 g^{W}값을 은행은 알 수 없다. 만약 은행이 gW의 값을 알고자 한다면 T값을 알고 T^{-1}을 이용해야하는데 이는 사용자만이 알고 있는 값이다.

4.1 제안 전자지불시스템 계수

제안 시스템의 계수는 다음과 같이 표현한다.

- * : 각가의 객체 (U : 사용자(User), B : 은행(Bank), M : 상점(Merchant))
- R, r : 은행이 선택한 임의 값
- T : 사용자가 선택한 임의 값
- W : 사용자가 전자화폐로 이용하기 위해 선택한 임의 값
- a : ($a = g^{TW} \bmod p$)로 사용자가 생성한 값
- L : ($L = g^{(R-r)} \bmod p$)로 은행이 생성한 값
- h(*) : *를 해쉬한 값
- p : 임의의 소수
- q : q|q-1를 만족하는 소수
- g : q를 위수로 하는 원소
- Y* : *의 공개키 ($Y^{*}=g^{X^{*}} \bmod p$)
- X* : *의 개인키
- Sing* : *의 서명값

4.2 제안 방식의 프로토콜

전자화폐의 적용한 제안 방식은 발급, 지불, 이체 프로토콜로 각각의 프로토콜은 다음과 같다.

가. 발급 프로토콜

전자화폐를 발급 받기 위해서 사용자와 은행은 다음과 같은 연산 및 정보를 전송한다.

1단계 : 전자화폐를 발급 받기 위해서 사용자는 은행에 다음과 같은 정보를 전송한다.

U->B : $a = g^{TW} modp$,Sing$_U$(a)

2단계 : 은행은 사용자에게 다음과 같은 정보를 전송한다.

B->U : $L = g^{(R-r)} modp$

3단계 : 은행은 다음과 같은 연산을 통해 서명을 제공한다.

$$k = g^{TW(R-r)} modp$$
$$e = h(k)$$
$$d = g^{TWR} modp$$
$$S = r - X_B e$$

4단계 : 은행은 사용자에게 다음과 같은 정보를 전송하고 사용자는 서명을 검증한다.

B->U : d, S 전송

서명의 검증 단계 연산

$$k' = g^{TW(R-r)} modp$$
$$e' = h(k)$$
$$d = (g^S Y_B^{e'} L)^{TW} modp$$

$d = (g^S Y_B^{e'} L)^{TW} modp$를 검증을 하면 다음과 같이 연산된다.

$(g^{r - X_B e} \cdot g^{X_B e} \cdot g^{R-r})^{TW} modp = g^{RTW} modp = d$

d의 검증 결과로 올바른 서명을 제공 받은 것을 알 수 있다. 전체적인 흐름은 다음 그림 3와 같다.

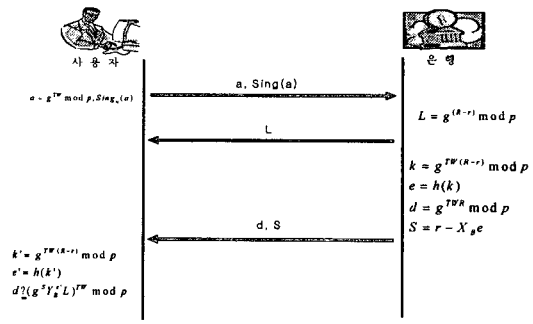

그림 3 제안 방식의 발급프로토콜

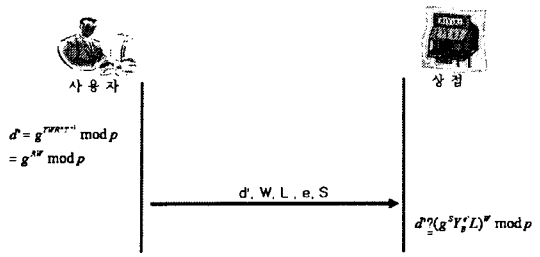

그림 4 제안 방식 지불 프로토콜

나. 지불 프로토콜

검증을 통해 서명을 받은 메시지를 다음과 같은 연산을 통해서 익명성을 제공한다.

1단계 : 사용자는 익명성을 제공하기 위해 다음과 같이 연산한다.

$$d' = d^{T^{-1}} = g^{RTWT^{-1}} modp = g^{RW} modp$$

2단계 : 사용자는 상점에게 물건의 지불로 다음과 같은 정보를 전송한다.

U->M : d',W, L, e, S

3단계 : 상점은 다음의 연산을 통해 전자화폐를 검증한다.

$$d' = (g^{S} Y_{B}^{e} L)^{W} modp = (g^{r-X_B e} \cdot g^{X_B e} \cdot g^{R-r})^{W} modp$$
$$= g^{RW} modp$$

다. 이체 프로토콜

상점은 사용자에게 받은 정보 중 다음과 같은 내용을 전송하여, 이체를 받는다.

M->B : d', W, e

5. 제안방식 고찰

제안방식을 2장에서 언급한 요구사항으로 분석한다.

- 전자화폐의 정당성 : 은닉서명은 메시지지의 내용을 알 수 없는 관계로 인해 메시지의 정당성이 필요하지만, 수신자 지정 서명은 메시지 a의 내용을 알고 있는 상태이다. 이후 은행의 b의 값을 이용하여 k를 생성함으로 사용자나 은행외의 제 3자는 생성할 수 없는 값이다.
- 전자화폐 수정 및 변조 : 메시지의 수정 및 변조를 하는 경우 e의 값이 변하게 된다. e의 값이외의 다른 값을 활용하기 위해서는 은행의 b값을 수정하여야 하며, 은행에서 제공하는 d를 검증할 수 없게 된다. 그러므로 다른 메시지를 생성하여, 사용할 수 없다.
- 오프라인성 : 은행이 직접 참여하지 않더라도 은행의 공개키를 가지고 전자화폐의 정당성을 확인 가능하다.
- 이중 사용 방지 : 은행은 상점으로부터 제공받은 e의 값이 이중으로 등록되는 경우 이중 사용으로 검출할 수 있으며, 이와 같은 경우 상점에 L의 정보를 요구한다. L은 은행이 사용자 마다 생성해서 제공하는 값으로 은행이 사용자를 알 수 있으며, 사용자의 증명은 L과 e를 통해 사용자가 제공한 g^{TW}를 확인 할 수 있으며, 이 값은 발급에서 e를 생성하는데 사용된 것을 알 수 있다.

6. 결론 및 향후 방향

본 논문에서는 전자화폐의 발급에 있어 수신자 지정 서명을 이용하였다. 수신자 지정 서명의 특성에 따라 발급된 전자화폐는 사용자만이 확인 가능하며, 제3자의 확인 방식에서 전자화폐의 서명을 확인하는 방안을 제공하였다. 이와 같은 방식으로 수신자가 제공하는 메시지에 대한 다른 방식을 추가하여 검증하는 부분을 제공하지 않아도 된다. 즉 은닉서명을 제공함으로 인한 메시지의 정당성 검사를 줄이기 위한 방안으로 수신자 지정 서명의 특징을 이용하는 것이다. 그러나 검증을 제공하고 위해서, 많은 값을 사용자가 상점에 전송하며, 일반적인 연산이 사용자한테서만 이루어진다. 이와 같은 경우 사용자의 이용 단말기의 높은 연산 능력을 요구하게 된다. 앞으로의 방안은 좀더 안전하게 서비스를 제공하면, 효율성이 높은 방안에 대한 지속적인 연구가 계속되어야 한다.

[참고문헌]

[1] Stefan Brands, "Untraceable Off-line Cash in Wallets with Observers", CRYPTO'93, LNCS 733, pp. 302-318, 1994

[2] Magdalena Payeras-Capella외 2명, "An Efficient Anonymous Scheme for Secure Micropayments", ICWE 2003, LNCS 2722, pp. 80~83, 2003

[3] Magdalena Payeras-Capella외 2명, "A fully Anonymous Electronic Payment Scheme for B2B", ICWE 2003, LNCS 2722, pp. 76~79, 2003

[4] Markus Stadler외 2명, "Fair Blind signatures", EUROCRYPT'95, LNCS 921, pp 209~219, 1995

[5] 김상진 외 1명, "해쉬체인을 이용한 새로운 오프라인 전자화폐 시스템", 정보과학회논문지, 정보통신 제 30 권 제 3호, pp. 207~221, 2003

[6] 장석철, "분할성 및 익명성 제어를 갖는 네트워크형 전자화폐 시스템에 관한 연구", 석사학위논문, 순천향대학교 정보기술공학부, 2001

[7] 이임영, "전자 상거래 보안 입문", 생능출판사, 2001