ElGamal방식을 이용한 새로운 소액전자지불시스템에 관한 연구

강서일°, 이임영
순천향대학교 정보기술공학부

A Study on New Anonymity of Micropayment System using ElGamal Scheme

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

요 약

현재의 인터넷의 발달로 인해 전자 상거래의 E-비즈니스 서비스를 이용하고 있는 사용자가 증가하고 있다. E-비즈니스 서비스에는 이용료나 상품의 가격을 지불하게 된다. 현재의 기존 화폐로 지불할 경우 E-비즈니스 서비스에 적용하는데 많은 취약성을 가지고 있다. 이로 인해 전자 화폐가 제안되고 연구하게 되었다. 전자 화폐는 화폐를 전자적으로 구현하여 사용하는 것으로써 현재 많은 전자 화폐가 연구되고 있다. 본 논문에서는 익명성을 제공하는 방법으로는 은닉서명을 이용한 기존의 논문들을 분석하고 ElGamal 방식을 사용하여 익명성을 제공해주는 소액전자지불시스템을 제안한다.

1. 서론

인터넷의 발달로 인해 현재 우리의 생활에서 전자 상거래가 활발해 졌다. 전자 상거래의 발달은 새로운 소비문화 형태를 가지고 오게 되었다. 자신의 회사나 집, 개인 PC가 있는 어느 곳이든지 재화를 살 수 있는 기회를 제공 받고 있어 아무리 늦은 밤이라도 상품을 구입할 수 있다. 이러한 소비는 기존의 화폐를 이용하여 지불하기에는 어려운 점이 많아 전자 화폐라는 새로운 지불 수단을 요구하게 되었다. 전자 화폐는 전자적으로 화폐의 가치를 가지고 있는 정보로써 기존 화폐를 이용할 때 생기는 취약성을 보안할 수 있다. 또한 전자 상거래의 E-비즈니스서비스를 이용할 때 사용자의 편리성을 제공한다.

본 논문에서는 익명성과 이중 사용 방지, 임의의 동전 생성을 방지 할 수 있는 방식을 제안한다. 제 2장에서는 전자 화폐의 보안 요구 사항을 알아보고, 3장에서는 기존의 관련 논문에 대해 분석한다. 4장에서는 제안 프로토콜을 설명한다. 5장에서는 제안 방식이 보안 요구사항을 어떻게 만족하는 지를 알아보고 6장에서 결론으로 끝을 맺는다.

2. 전자 화폐의 보안 요구사항

기존의 화폐를 전자 화폐로 구성할 때 다음과 같은 보안 요구사항이 발생한다. 다음은 보안 요구사항에 대해서 알아 본다.

안전성 : 전자 화폐의 복사, 위조 등으로 인한

부정 이용을 방지해야 한다.

익명성 : 전자 화폐의 지불 과정에서 물품 구입 내용과 사용자 식별정보가 어느 누구에 의해서도 연계될 수 없어야 한다.

오프라인성 : 전자화폐의 유효성 확인은 은행의 개입 없이 즉시 이루어져야 한다. 즉 화폐 자체가 정당성을 가지고 있어야 한다.

양도성 : 전자 화폐를 받은 사람은 제 3자에게 다시 사용할 수 있어야 한다.

분할성 : 인정한 가치를 가지는 전자화폐는 그 가치만큼 자유롭게 분할 사용 가능해야 한다.

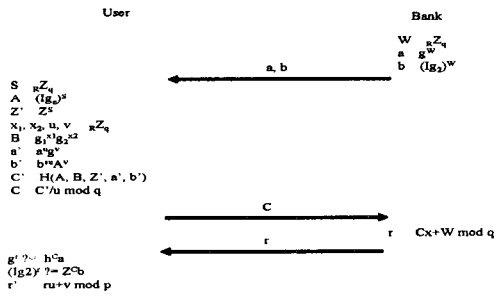
이중 사용 방지 : 전자화폐는 복사 및 위조가 가능하며, 불법 사용자는 즉시 판별 가능해야 한다.

전자 화폐는 위와 같은 보안 요구사항 요구된다.

3. 관련연구

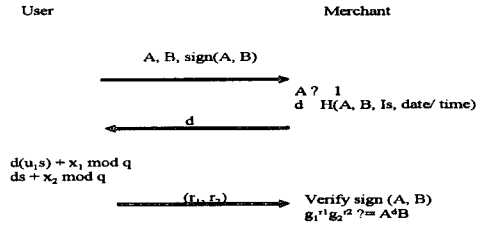
3.1 Untraceable Off-line Cash in Wallets With Observers

Stefan Brands가 제안한 방식으로 cut & choose 방식의 비효율적인 발행 단계를 보다 개선한 Challenge Response방식을 이용한 전자 화폐이다[1]. 이 방식에서 은행과 사용자는 미리 공통의 식별자를 나누어가지고 있다. 그림 1은 인출 프로토콜의 흐름도 이다.



[그림 1] Brands 방식의 인출 프로토콜

인출 프로토콜은 사용자와 은행간의 통신이다. 여기서는 은닉 서명을 이용하여 C의 값을 은행이 알아도 C'값은 은행으로부터 은닉되어 있다. Ig_2는 은행과 사용자가 공통으로 가지고 있는 식별자이다. 사용자와 상점간의 통신에서도 사용되어 임의의 동전을 생성할 수 없게 한다. 다음 그림 2은 사용자와 상점간의 지불 프로토콜을 간략히 도식화 한 그림이다.

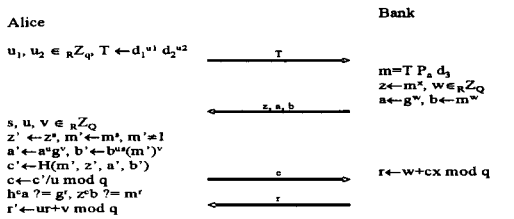


[그림 2] Brands방식의 지불 프로토콜

상점은 두 개 r의 값을 받아 검증을 한다. 이중의 사용할 경우 은행에서는 r의 값을 검증하여 사용자의 U_1의 값을 알아 낼 수 있다. U_1은 은행과 사용자가 이용한 Ig_2의 구성 값으로 사용자를 검증할 수 있다.

3.2 A New Approach for Anonymity Control In Electronic Cash Systems

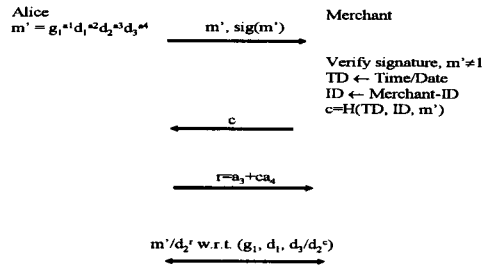
Tomas Sander와 Amnon Ta-Shma가 제안한 방식으로 Brands의 방식의 메시지 구성을 차별화 하였다[2]. 사전에 분배한 식별자 P_A와 사용자에게 받은 T의 값을 이용하여 전자 화폐를 생성한다. 다음의 그림 3은 인출 프로토콜이다.



[그림3] Tomas Sander, Amnon Ta-Shma 방식의 인출 프로토콜

여기서 사용되는 T의 값에 의해 임의의 동전 생성이 불가능 하게 된다. S라는 인수를 사용하여 메시지의 은닉성을 준다. 지불 프로토콜을 보면 이중 사용했을 경우 은닉 인수 S를 검출할 수 있다.

S를 검출하면 메시지 m을 은행에서 알 수 있다. 그림 4는 지불 프로토콜을 도식화한 것이다.



[그림 4] Tomas Sander, Amnon Ta-Shma 방식의 지불 프로토콜

4. ElGamal방식을 이용한 익명성을 제공하는 제안 방식

본 논문의 제안 방식은 ElGaml방식의 서명을 이용하여 전자화폐를 발행한다. 본 논문의 전체 과정은 다음과 같이 인출과 지불과정으로 나누어서 프로토콜이 구성된다.

4.1 시스템 계수

본 논문의 ElGamal방식을 이용한 익명성을 제공하는 제안방식을 설명하기 위한 시스템 계수의 구성은 다음과 같다.

User : 사용자 (U)

Bank : 은행 (B)

Merchant : 상점 (M)

Y_B : 은행의 공개키 ($Y_B = g^x \bmod p$)

K : 사용자와 은행이 공유하고 있는 사용자의 식별자 ($K = g^U$)

r : 사용자가 선택한 랜덤 수

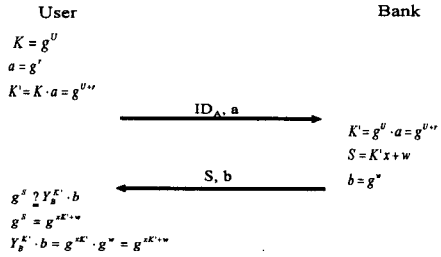
w : 은행이 선택한 랜덤 수

T : 상점의 식별자 인수

4.2 제안된 ElGamal방식을 이용한 프로토콜

① 인출 프로토콜

사용자와 은행 사이의 전자 화폐를 발급 받기 위해 다음과 같은 과정을 수행한다. 그림5은 프로토콜을 도식화한 것이다.



[그림5] 제안방식의 인출 프로토콜

사용자는 은행과 인출 프로토콜이 시작하기 전에 다음의 값을 비밀리에 공유하고 있다고 가정한다.

$$K = g^U$$

㉮ 사용자는 랜덤 수 r을 선택하여 다음을 계산하고 ID_A, a를 보낸다.

$$a = g^r$$
$$K' = K \cdot a = g^{U+r}$$

$$User \rightarrow Bank$$
$$ID_A, a$$

㉯ 은행은 사용자에게 받은 a를 이용하여 다음을 계산하여 K'를 생성하고 서명을 하여 S, b를 사용자에게 전송한다.

$$K' = g^U \cdot a = g^{U+r}$$
$$S = K'x + w$$
$$b = g^w$$
$$Bank \rightarrow User$$
$$S, b$$

㉰ 사용자는 은행에게 받은 S, b를 이용하여 사용자가 생성한 K'를 은행이 동일하게 생성 했는지 검증한다.

$$g^S \stackrel{?}{=} Y_B^{K'} \cdot b$$
$$g^S = g^{xK'+w}$$
$$Y_B^{K'} \cdot b = g^{xK'} \cdot g^w = g^{xK'+w}$$

② 지불 프로토콜

지불 프로토콜 과정은 은행으로부터 받은 S, b와 사용자가 생성한 K'를 이용하여 지불하는 과정이다. 그림6는 지불 프로토콜을 도식화 하였다.

㉮ 사용자는 상점으로부터 상점의 식별자 T를 전송하다.

$$T = g^{M}$$
$$Merchant \rightarrow User$$
$$T$$

㉮ 사용자는 받은 T를 다음과 같이 은행에서 받은 서명 S를 이용하여 다음과 같이 계산하여 K_1을 생성하여 상점에 K_1, K', b를 전송한다.

$$K_1 = g^{SM}, K', b$$
$$User \rightarrow Merchant$$
$$K_1, K', b$$

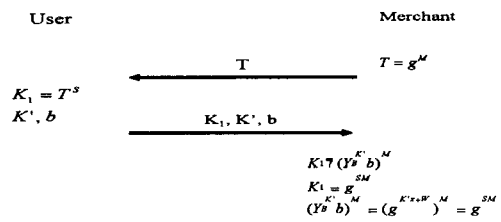
㉯ 상점은 받은 K_1, K', b와 은행의 공개키를 이용하여 K_1의 정당성을 검증한다.

$$K_1 \stackrel{?}{=} (Y_B^{K'} b)^{M}$$
$$K_1 = g^{SM}$$
$$(Y_B^{K'} b)^{M} = (g^{K'x+W})^{M} = g^{SM}$$

㉰ 상점은 K_2를 생성하여 sig(K_2)를 은행에 전송한다.

$$K^2 = g^{SM/M} = g^{S}$$
$$Merchant \rightarrow Bank$$
$$K_2, sig(K_2)$$

㉱ 은행은 K_2의 값이 저장되어 있는지 확인을 하고 저장이 되어 있지 않으면 사용되지 않은 화폐로 상점에 이체 과정을 수행한다.



[그림6] 제안 방식의 지불 프로토콜

5. 보안 요구 사항 고찰

본 논문에서 제안된 방식은 다음의 보안적 요구 사항에 대해 특징을 확인 할 수 있다.

익명성 : 은행은 K_2의 값을 알아도 은행이 생성한 S의 모든 값을 계산해서 검출하기 전까지는 사용자를 식별할 수 없다.

임의 생성 : 사용자는 임의의 동전을 생성 하려고 한다면 은행은 서명한 값인 S와 다른 값이 검출됨으로 임의의 동전을 생성할 수 없다.

이중 사용 부정 : 이중 사용할 경우 K2의 값이 이미 은행에 저장되어 있어 이중 사용을 알 수 있고 상점에서 은행에 K'를 제공하면 은행은 이중 사용한 사용자를 검출 할 수 있다.

6. 결론

본 논문에서는 전자 화폐의 익명성을 제공하는 방식에 대해서 기존의 논문을 연구하고 ElGaml방식을 이용하여 제안하였다. 제안된 방식은 인출, 지불에서 통신 회수를 2회로 함으로써 기존의 방식 보다 효율성을 높게 하였다. 향후 본 연구는 은행과 상점의 결탁으로 인한 사용자의 익명성 제거에 대한 방지가 필요하고 양도성과 분할성에 대한 추가적인 연구가 진행되어야 할 것으로 사료된다.

[참고문헌]

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

[2] Tomas Sander and amnon Ta-Shma, "Flow Control : A New Approach for Anonymity Control in Electronic Cash systems" FC'99, LNCS 1648, pp. 46-61, 1999.

[3] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, "Fair Blind Signatures", Advances in Cryptology-EUROCRYPT'95 LNCS 921, pp. 209-219, 1995

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

[5] 용승림, 이은경, 하상호, "해쉬 체인에 기반한 분할 가능 전자 화폐 시스템의 설계", 정보과학회 2002년 춘계학술대회, VOL.29, NO0.1, pp.802-804,

[6] 최형섭, 정명구, 김상진, 오희구, "해쉬 체인을 이용한 익명의 판매자 전용화폐", 정보과학회 2002년 춘계학술대회 VOL.29, NO.01, pp.835-837

[7] 이임영, "전자 상거래 보안 입문", 생능출판사, 2001년