이동컴퓨팅 환경을 위한 소액지불시스템

이 만 호, 김 광 조

국제정보보호기술연구소, 한국정보통신대학원대학교

An Efficient Micropayment for Mobile Computing Environment

Manho Lee, Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

요 약

이동컴퓨팅 환경에서의 전자지불 시스템은 연산능력과 저장장치의 효율성을 고려하여 설계하여야 한다. 소액지불시스템은 효율성을 강조하여 설계된 지불시스템으로 이동컴퓨팅 환경에 적합한 프로토콜이다. 그러나 대부분의 경우 서명을 위해 공개키 연산이 필요하다. 본 논문에서는 해쉬체인을 사용하는 소액지불시스템을 기반으로 사용자의 저장 용량에 대한 공간 효율성을 제공함과 동시에 공개키 연산을 사용하지 않는 소액지불시스템을 제안한다.

I. 서론

전자화폐에 대한 연구는 1982년 Chaum이 은닉서명에 기반한 추적 불가능한 전자화폐 프로토콜을 제시한 이후 [1], 여러 가지 요구조건들을 만족시키는 다양한 기법과 시스템들이 제안되고 있다.

이동컴퓨팅 환경에서의 전자화폐 프로토콜은 유선환경과는 달리 이동컴퓨팅 기기의 자원환경의 제약으로 인해 [6], 연산 및 무선 통신 메시지의 수를 최소화하는 효율성에 초점이 맞추어지고 있다. 따라서, 공개키 연산의 최소화, 연산량의 최소화 및 저장비용의 최소화를 목적으로 제안된 소액지불(Micropayment) 시스템이 적합하다.

소액지불시스템의 장점은 공개키 연산의 최소화, 온라인 인증의 사용을 지양하여 연산의 효율성을 얻을 수 있다는 것이다. 그러나, 안전성 측면에서는 기존의 전자화폐보다는 취약하다.

소액지불시스템 중에서 공개키 연산의 서명과 해쉬체인을 응용한 대표적인 프로토콜로, [5]에서 제안된 PayWord가 있다. 이 프로토콜은 해쉬함수의 사용과 제한된 공개키 연산의 사용으로 효율성을 제공하였으나, 사용자가 각 상점에 대한 사용 인덱스를 각각 저장하여야 하고, 사용자의 공개키 연산 능력이 제공되어야 하는 문제를 갖고 있다. 이러한 문제점을 해결하기 위해서, 본 논문에서는 하나의 해쉬체인으로 모든 상점에 사용할 수 있고, 공개키 연산이 필요하지 않아 사용자 관점에서 저장 공간 및 연산이 효율적인 해쉬체인 기반의 소액지불시스템을 제안한다.

본문의 구성은 다음과 같다.

제 2장에서는 소액지불시스템에 대한 소개와, 해쉬체인을 이용한 소액지불시스템을 설명하고, 제 3장에서는 새로운 소액지불시스템을 제안하며, 마지막으로 제 4장에서 결론을 맺는다.

II. 관련연구

1. 소액지불시스템

1) 기본 모델

소액지불시스템은 기본적으로 사용자 C, 브로커 B, 상점 V로 구성되며 각 참여자는 다음과 같은 역할을 수행한다.

- 사용자 (Customer:C) : 소액지불시스템을 이용하여 상점 V와 거래 한다.

- 브로커 (Broker:B) : 전자화폐의 발행, 사용자

인증, 상점과 사용자의 계좌를 관리한다.

- 상점 (Vendor:V) : 사용자 C와의 거래를 통해 사용자에게 필요한 상품을 제공하고 그에 상응하는 전자화폐를 받아 브로커 B를 통해 자신의 계좌에 입금한다.

2) 전자화폐의 생성

소액지불시스템은 전자화폐의 생성주체와 형태에 따라 다음과 같이 분류한다. B가 전자화폐를 생성하고 C는 B로부터 전자화폐를 구입하여 사용하고 B는 사용자의 계좌로부터 미리 인출하는 방식 (Debit 형태)이 있는데, [5]의 MicroMint, [4], [7]이 이에 해당하며, 사용자가 전자화폐를 생성하고, 전자화폐의 상환이 이루어질 때 사용자의 계좌로부터 이에 상응하는 금액를 인출하는 방식 (Credit 형태)으로는 [5]의 PayWord, [3], [2] 등이 있다.

또는 사용자의 인증 및 전자화폐의 사용 방식에 따라 온라인, 오프라인 형태로 분류하기도 하며, 전자화폐 자체를 직접 생성하는 방식(Coin Based)과 B가 C와 V의 계좌를 관리하는 방식 (Account Based)으로도 분류한다.

3) 기본 요구사항

기본적인 소액지불시스템의 요구사항은 아래와 같다.

- 공개키 사용의 최소화

공개키 연산이 대칭키 연산에 비해 더 많은 연산능력을 요구하므로 전자화폐 사용의 인증을 위한 최소한의 사용 또는 사용치 않음이 요구된다.

- 오프라인 (Off-Line) 검증

거래 과정중 통신량의 부하를 줄이기 위하여 B에 의한 C 및 V에 대한 온라인 검증을 사용하지 않는다.

- 사용자의 연산 최소화

공개키 연산의 최소화와 함께 거래과정에서 사용자와 상점간의 통신횟수 및 메시지의 최소화를 고려한다.

- 사용자의 저장용량 최소화

사용자의 연산 및 거래에 필요한 최소한의 저장변수를 고려한다.

- 안전성 고려사항

소액지불시스템은 공격자의 공격 비용이 실제 전자화폐보다 비싼 경우 효용이 없음을 그 기본으로 하고 있으나, 이중사용에 대한 탐지, 위조방지 등을 고려한다.

2. 해쉬체인을 이용한 소액지불시스템

소액지불시스템 중에서 공개키 연산의 서명과 해쉬체인을 응용한 프로토콜들로, [5]의 PayWord, 가 대표적이다. 이 중에서 PayWord 프로토콜을 살펴보자.

1) PayWord 해쉬체인 및 사용자 인증서

PayWord 해쉬체인은 사용자 C가 생성한다. 이를 생성하기 위해서 C는 n번째 PayWord로 나머지 PayWord 체인을 생성하기 위한 값 w_n을 랜덤하게 생성하며, 이를 사용하여 PayWord 체인을 아래와 같이 생성한다.

$$w_{i-1} = h(w_i), \quad where\ i = 1, \ldots, n \quad \textbf{(1)}$$

여기에서 사용된 함수 h는 해쉬함수 (one-way and collosion-resistent)이다.

마지막으로 계산되는 w_0 값은 해쉬체인의 "Root" 값으로 해쉬체인을 검증하는 값으로 체인에 포함되지 않고, C가 V에게 위탁하는 값 M에 포함된다. M은 C의 비밀키 SK_C의해 서명된 값으로 w_0 상점 식별값 V, 사용자 인증서 C_C 사용만료기간 D, 기타정보 I_M로 구성된다.

$$M = \{w_0, V, C_C, D, I_M\}_{SK_C} \quad \textbf{(2)}$$

C는 V와의 거래를 위하여 사전에 B로부터 인증서 C_C를 받아야 한다. 이것은 브로커 식별값 B, 사용자 식별값 C, 사용자 계좌정보 A_C 사용자 공개키 PK_C 사용기간 E, 기타 정보 I_C를 B의 비밀키 SK_B로 서명한 값이다.

$$C_C = \{B, C, A_C, PK_C, E, I_C\}_{SK_B} \quad \textbf{(3)}$$

2) 프로토콜 처리 흐름

사용자 C와 브로커 B, 상점 V와의 각 처리 단계는 그림 1과 같다.

- C는 먼저 B로부터 수식 (3)의 인증서 C_C를 받는다.

- C는 거래 개시 전에 V에게 수식 (2)에 의해 같이 생성된 M을 위탁하면, V는 C의 공개키로 이를 복호화하여 V와 D 값을 검증하고 이를 저장한다.

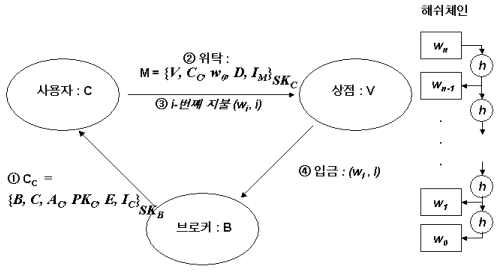

그림 1 : PayWord 지불 처리 흐름

- C는 V와 상품 거래 후 지불하고자하는 i번째 값으로 (w_i, i)값을 전송한다.

- V는 $h(w_i)$를 계산하여 검증하고, 이 값을 저장한다.

- V는 마지막 지불 값에 대한 정보 (w_i, i)와 위탁 값 M을 브로커에게 전송하여, 입금을 요구한다. B는 고객의 계좌에서 인출하여, 상점의 계좌로 입금한다.

3) 문제점

- 사용자는 각 상점에 대하여 서로 다른 해쉬체인을 사용하여야 한다.

-사용자는 각 상점에 대한 사용 인덱스를 각각 저장하여야 한다.

- 사용자는 공개키 연산 능력이 제공되어야 한다.

이러한 문제들을 해결하기 위해서, 하나의 해쉬체인으로 모든 상점에 사용할 수 있고 공개키 연산이 필요하지 않는 해쉬체인 기반의 프로토콜을 제안한다.

III. 제안방법

1. 가정

일반적으로 본 연구를 적용하기 위한 상황으로 다음을 가정한다.

- 사용자와 상점은 "Tamper-resistant" 기기를 사용한다.

- 사용자와 브로커, 브로커와 상점의 기기간의 통신은 안전하다.

이 가정들은 [7]에서 사용된 것으로 현재 이동 컴퓨팅 환경에 스마트카드가 사용되고 있으므로, 위의 가정이 유효하다.

2. 초기화 단계

소액지불시스템을 사용하기 위한 등록 단계시 브로커는 상점과 사용자가 프로토콜에서 사용할 공용키를 설정하여 안전한 통신채널을 통해 사용자와 상점의 기기에 전송한다.

- K_B : 브로커 마스터 키

- K_{BC} : 브로커와 사용자간의 공유키

- K_{BV} : 브로커와 상점간의 공유키

- $K_{CV} = h(C||K_{BV})$: 사용자와 상점간의 공유키

사용자와 상점은 브로커로부터 인증서를 받아 사용하며 아래와 같이 구성된다.

- 사용자 인증서 C_C : 브로커 식별값 B, 사용자 식별값 C, 해쉬체인 길이 n, 사용만료기간 E, 브로커와 상점간의 공유키 K_{BV}, 해쉬함수 $h()$를 사용하여 생성한다.

이 단계에서 브로커가 사용자의 계좌를 확인하여 사용자가 생성할 수 있는 해쉬체인 길이 n을 설정하여 보내준다.

$$C_C = \{B, C, E, n, h(B, C, E, n, K_{BV})\} \quad (4)$$

- 상점 인증서 C_V : 브로커 식별값 B, 사용자 식별값 V, 사용만료기간 E, 브로커와 상점간의 공유키 K_{BC}, 해쉬함수 $h()$를 사용하여 생성한다.

$$C_V = \{B, V, E, h(B, V, E, K_{BC})\} \quad (5)$$

3. 프로토콜 처리흐름

1) 단일 상점과의 거래

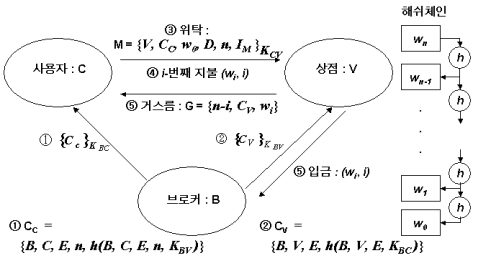

그림 2 : 단일 상점과 거래

- B는 C와 V에게 수식 (4), (5)를 사용하여 인증서를 생성하여, 사전에 서로 공유된 키로 암호

화하여 전송한다.

- C는 V에게 수식 (6)과 같이 위탁값 M을 생성하여 전송한다.

$$M=\{V, C_C, w_0, D, n, I_M\}_{K_{CV}} \quad (6)$$

- V는 M을 받아 복호화 하여 V와 D 값을 검증하고 저장한다.

- V는 i 번째 지불에 대한 거스름 G 값을 수식 (7)과 같이하여 C에게 전송한다.

$$G=\{n-i, C_V, w_i\} \quad (7)$$

- 이후, 지불 및 입금과정은 PayWord와 동일하다.

2) K-번째 상점과의 거래

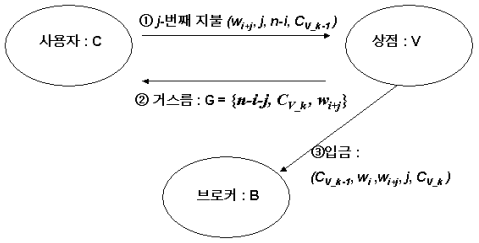

그림 3 : K-번째 상점과의 거래

- K 번째 상점에 대하여 j 만큼의 지불시 C는 해쉬체인 검증을 위한 값 w_{i+j}, $K-1$번째 V의 인증서 $C_{V,K-1}$, 그리고 전체 해쉬체인 길이에서 이전까지 사용했던 값을 뺀 값 $(n-i)$를 상점에 전송한다.

- V는 이에 대하여 거스름 G를 수식 (8)과 같이 생성하여 C에게 전송한다.

$$G=\{n-i-j, C_{V\_K}, w_{i+j}\} \quad (8)$$

- V는 입금 요구시 B에게 $K-1$번째 V의 인증서 $C_{V,K-1}$, 해쉬체인값 w_i, 자신의 해쉬체인값 w_{i+j}, 입금요구 인덱스 값 j 및 인증서 $C_{V,K}$를 전송한다.

- B는 각 해쉬체인을 검증하여, 요구된 범위에 대한 해쉬체인의 입금 여부를 검증 할 수 있다. 또한 사용자의 해쉬체인 길이를 사전에 정의하였으므로 이에 대한 초과사용여부도 확인 가능하다.

4. 프로토콜 분석

제안된 프로토콜은 사용자의 관점에서 볼 때 거래하고자 하는 각 상점에 대하여 동일한 해쉬체인을 사용할 수 있으며, 각 상점에 대하여 각각의 사용인덱스 및 해쉬체인값을 저장하지 않고, 거스름을 이용하여 다른 상점에도 같은 해쉬체인에 대한 인덱스를 계속하여 사용할 수 있다.

또한 초기화 단계에서 공용키를 분배하여, 공개키의 사용을 배제하여, 연산의 효율성을 증가하였다.

IV. 결론 및 향후 과제

본 논문에서 현재의 이동통신환경의 특성을 고려하여, 해쉬체인과 "Tamper-resistant"기기 사용을 기반으로 사용자 관점에서 저장 공간 효율성을 증가하고, 공개키의 사용을 배제하여 연산의 효율성을 증가시킨 소액지불시스템을 제안하였다.

향후, 공개키 암호화 기법을 사용하여 소액지불시스템에서 제공하지 못하는 익명성을 제공하는 방법과 전자상거래에서 요구되는 원자성을 만족하는 시스템의 연구가 필요하다.

참고문헌

[1] D. Chaum, "Blind Signatures for Untraceable Payments", *In Advances in Cryptology-Proc. of CRYPTO'82*, Plenum Press, pp.199-203, 1983.

[2] G. Horn, B. Preneel, "Authentication and Payment in Future Mobile Systems", *Computer Security ESORICS 98*, LNCS 1485, pp.277-293, 1998.

[3] M. Jakobsson, "Mini-Cash : A Minimalistic Approach to E-Commerce", *In Proc. of PKC1999*, LNCS 1560, pp.122-135, 1999.

[4] M.S. Manasse, "The Millicent Protocol for Electronic Commerce", *Proc. of the 1st USENIX Workshop on Electronic Commerce*, 1995.

[5] R. Rivest and A. Shamir, "PayWord and MicroMint : Two Simple Micropayment Schemes", *Proc. of 1996 Int. Workshop on Security Protocols*, LNCS 1189, pp.69-87, 1996.

[6] M. Satyanarayanan, "Fundamental Challenges in Mobile Computing", *Proc. of the 15th ACM Symp. on Principle of Distributed Computing*, pp.1-7, 1996.

[7] J. Stern, S. Vaudenay, "SVP : a Flexible Micropayment Scheme", *Financial Crypto 97*, LNCS 1318, pp.161-172, 1997.