사생활 정보가 노출되지 않는 해쉬체인 기반 소액지불시스템

정 윤 수[†] · 백 승 호[††] · 황 윤 철[†††] · 이 상 호[††††]

요 약

해쉬체인은 계산속도가 빠른 해쉬함수를 이용하여 체인을 구성하는 구조이다. 이 구조를 이용하여 one-time 패스워드, 서버지원 서명(signature) 그리고 소액지불과 같은 다양한 암호학 응용에 사용되고 있다. 그러나 선불방식에 사용하고 있는 대부분의 해쉬 체인기반 시스템들은 익명성을 지원하지만 익명성으로 인하여 지불비용이 증가하는 문제점을 가지고 있다. 따라서, 이 논문에서는 고객의 사생활 보호에 중점을 두면서 루트값이 인출되는 과정에서 한번만 은닉서명을 하여 사용자의 익명성을 보장하고, 시스템에 사용하는 공개키 대신 비밀키를 사용하여 인증서의 역할을 수행하지 않도록 효율성을 향상시킨 새로운 해쉬체인 기반 소액지불시스템을 제안한다.

키워드 : 소액지불시스템, 사생활 보호, 해쉬체인, 비밀키, 은닉서명

Hash-Chain based Micropayment without Disclosing Privacy Information

Yoon-Su Jeong[†] · Seung-Ho Baek[††] · Yoon-Cheol Hwang[†††] · Sang-Ho Lee[††††]

ABSTRACT

A hash chain is a structure organized by hash function with high speed in computation. Systems using the hash chain are using extensively in various cryptography applications such as one-time passwords, server-supported signatures and micropayments. However, the most hash chain based on the system using pre-paid method provides anonymity but has the problem to increase payment cost. In this paper, we propose a new hash chain based on the micropayment system to keep user anonymity safe through blind signature in the withdrawal process of the root value without disclosing privacy information, and to improve efficiency by using secret key instead of public key in the system without the role of certificate.

Key Words : Micropayment, Privacy, Hash-chain, Secret Key, Blind Signature

1. 서 론

최근 초고속 정보통신망 구축에 따른 인터넷의 보급확산으로 가장 큰 이슈화가 되고 있는 것이 소액지불시스템(micropayment system)이다. 소액지불시스템은 뉴스, 신문, 잡지, 음악, 증권정보와 같은 저가의 디지털 상품을 거래할 때 적합한 지불시스템이다[1-8].

최근 소액지불이 주목을 받은 이유는 인터넷 환경이라는 특수성에서 기인한다. 인터넷을 통하여 MP3 파일의 다운로드가 폭발적으로 증가하고 있고 최근 음반, 영상 업체들이 자사 콘텐츠의 지적보호를 위해 이의 유료화에 적극 나서고 있기 때문이다.

많은 소액지불시스템이 지불 과정에서 화폐의 유효성을 확인하는 비용을 줄이기 위해 해쉬체인을 사용하여 화폐를 구성한다[4-8]. 또한 트랙잭션의 처리 비용이 커지는 것을 피하기 위해 설계단계부터 익명을 고려하지 않거나[1-3, 6], 실명으로 하는 신용기반(credit-based)의 후불 시스템으로 구성하기도 한다[4, 5]. 익명 거래가 가능한 [7, 8]은 해쉬체인을 이용한 범용화폐로 연산비용이 작지 않아 소액지불에는 부담스럽다. 그러나 거래의 규모가 아무리 작다 하더라도 대다수의 고객은 자신의 거래가 알려지기를 꺼려한다. 이것은 거래의 건전성(fressness)과도 무관하지 않다. 사이버 거래가 일반화되면 될수록 사생활 보호에 대한 고객의 관심과 요구는 더 높아질 것은 쉽게 예측할 수 있다.

따라서, 이 논문에서는 고객의 사생활 보호[18]에 중점을 두면서 은행으로부터 지불 권한을 위임받은 고객이 동일한 상인과 잦은 거래를 하는 경우에 판매자와 익명의 거래를 효율적으로 하기 위한 해쉬체인 기반 전용화폐를 제안한다. 제안기법은 루트값이 인출되는 과정에서 한번만 은닉서명을 하여 사용자의 익명성을 보장하고, 시스템에 사용되는 공개키 대신 비밀키를 사용하여 인증서의 역할을 수행하지 않도록 효율성을 향상시키고 있다. 또한 기존의 분할 가능한 화

† 준 회 원 : 충북대학교 이공대학 전자계산학과 박사과정
†† 준 회 원 : 충북대학교 전기전자컴퓨터공학부 전자계산학과 석사과정
††† 준 회 원 : 충북대학교 전기전자컴퓨터공학부 전자계산학과 박사수료
†††† 종신회원 : 충북대학교 전기전자컴퓨터공학부&컴퓨터정보통신연구소 교수

논문접수 : 2004년 8월 19일, 심사완료 : 2005년 3월 31일

폐가 익명성을 유지하면서 환불기능을 제공할 수 있도록 하기 위해 객체간의 세션키와 상인 유효기간 E_M, 상인의 위치정보 L_M등을 이용하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 기존 소액지불 시스템들의 지불방식에 대해 기술한다. 3장에서는 사생활 정보가 노출되지 않은 해쉬체인(hash chain) 기반 소액지불 시스템에 대해 설명하고, 4장에서는 제안된 기법을 성능분석한다. 마지막으로 5장에서는 결론에 대해 기술한다.

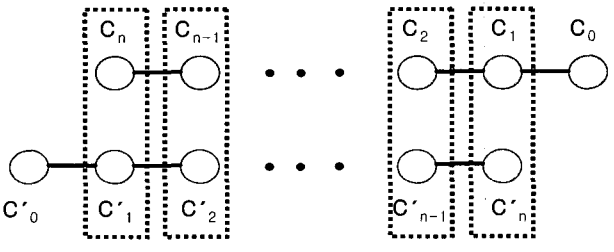
2. 관련 연구

2.1 해쉬체인에 기반한 전자화폐 시스템

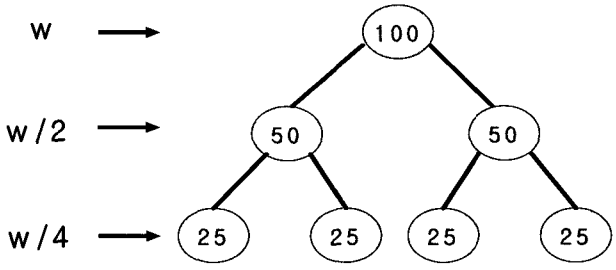
전자화폐는 화폐의 정당성을 인증하기 위하여 공개키 전자서명 방식을 이용하여 동전마다 은행이 서명을 한다. 그러나 공개키 전자서명 방식은 계산상 매우 복잡하기 때문에 생성된 동전마다 공개키 전자서명을 붙이기에는 비효율적이다.

1996년도 Rivest와 adi Shamir는 해쉬함수를 이용하여 동전을 체인형식으로 구성하고 체인의 루트값 하나에만 서명을 받음으로써 생성된 동전마다 서명을 받지 않도록 하여 효율성을 향상시킨 Payword 전자화폐를 제안하였다[4]. Payword 전자화폐에서 고객은 동전을 인출할 때 임의의 수 w_n을 선택하고 $w_i = h(w_{i+1})(i=n-1,n-2,...,0)$의 식을 적용하여 역방향으로 동전 w_1, w_2,...,w_n을 생성하고 해쉬체인의 루트값 w_0에만 은행의 서명을 받는다. 고객은 서명된 w_0를 상인에게 보내고 w_1부터 지불금액만큼 동전을 지불한다. 상인은 w_0의 서명을 확인하고, 지불된 동전의 인덱스만큼 해쉬함수를 적용하여 루트값이 w_0가 되는지 확인함으로써 동전이 정당한지 검증한다.

이중해쉬체인 전자화폐는 Payword에서 제안한 동전 구성 방법에 의해 두개의 해쉬체인을 생성하고 두 개의 해쉬체인의 원소 한 쌍을 하나의 동전을 구성하는데 이용한다[5, 6, 11]. 즉, (그림 1)과 같이 해쉬체인을 두개 생성한 후 각 체인의 요소들을 서로 역순으로 번호가 같은 것끼리 쌍을 이루어 동전을 구성한다. 이 방식은 동전을 구성하는 한 체인의 종자값(seed)을 알아냈다 하더라도 다른 체인의 종자값도 알아야만 위조가 가능하다는 특징을 이용하여 동전의 위조에 대한 안전성을 향상시켰다. 해쉬함수를 기반으로 하는 전자화폐 시스템의 안전성은 해쉬함수가 역방향으로 계산하기 어렵다는 해쉬함수의 일방향성에 근거한다.



(그림 1) 이중해쉬체인 동전



(그림 2) 이진 트리를 이용한 분할 가능 전자화폐

2.2 분할 가능한 전자화폐 시스템

분할 가능한 전자화폐 시스템이란 동전의 분할성을 만족하는 전자화폐이다. 분할성은 고객이 전자화폐를 발급 받는 경우 고객이 보유하고 있는 전자화폐의 총액을 초과하지 않는 범위 내에서 고객이 전자화폐를 나누어 사용할 수 있는 성질이다.

1991년 T. Okamoto 등은 이진트리 구조를 이용하여 분할 가능한 효율적인 전자화폐 프로토콜을 제안하였다[12, 13]. 이진 트리 구조에서 트리의 각 노드는 동전의 액면가를 나타내며 트리의 자식 노드의 금액의 합이 부모 노드의 금액이 되는 방식으로 각 노드별로 금액을 준다. (그림 2)에서 루트노드가 w원의 액면금액을 가지면 그 다음 레벨의 노드들은 $w/2$원의 액면금액을 갖는다.

대부분의 분할 사용 가능한 전자화폐 프로토콜에서는 이진 트리를 이용한 접근 방식을 이용하여 화폐의 분할 사용 기능을 구현하고 있다. 그러나 이 방식은 계산량이 트리의 깊이(depth)에 따라 변하고 복잡한 수학식을 사용하며, 법(mod) 연산 방식을 사용함으로써 계산량이 많아지는 단점이 있다.

3. 제안된 해쉬체인기반 소액지불시스템

이 논문에서는 고객의 사생활 정보가 노출되지 않는 전자화폐의 동전을 구성할 때 Payword와 같이 해쉬함수를 이용한다. 전자화폐는 고객, 은행 그리고 상인 등 세 개의 구성원으로 이루어지며 동작 프로토콜은 고객과 상인이 은행에게 계정을 개설하는 등록 프로토콜, 고객과 은행사이의 인출 프로토콜, 고객과 상인간의 지불 프로토콜 그리고 상인과 은행간의 예치 프로토콜로 구성된다.

3.1 가정

이 논문에서의 제안기법의 구성요소(고객, 상인, 은행)들이 원활하게 동작하기 위한 가정은 아래와 같다[18].

① 고객과 상인은 은행을 신뢰한다.
② 고객(Customer)과 상인(Merchent)은 거래를 하기 전 은행(Bank)으로부터 계정을 받는다.
③ 고객은 은행에 등록되어 있는 상인 계정으로 지불 금액을 전달하였을 경우에 서비스를 제공받는다.

④ 은행은 고객과 상인의 중계역할 업무, 계정 관리, 전자화폐 거래의 타당성 검증 등의 역할을 한다.

⑤ 개인 신상정보는 고객과 은행사이의 거래에서만 공유된다. 이것은 RFC 2905의 개인정보 요구에 정의되어 있다[19]. 상인은 업무를 처리하는데 개인 신상정보가 필요없다.

⑥ 구매 정보(Order Information:OI)는 고객과 상인 사이에서만 공유한다. 은행은 구매정보의 내용을 알 필요가 없다.

⑦ 상인의 실제 ID는 은행에게 노출되지 않아야 한다. 상인이 거래하는 업무는 은행에게 불필요하다. 은행은 단지 지불과 같은 고객의 권한을 검증하는데만 필요하다. 상인의 정보없이 고객의 구매 습관을 추적하기 위한 은행의 능력은 제한되어야 한다.

3.2 용어정의

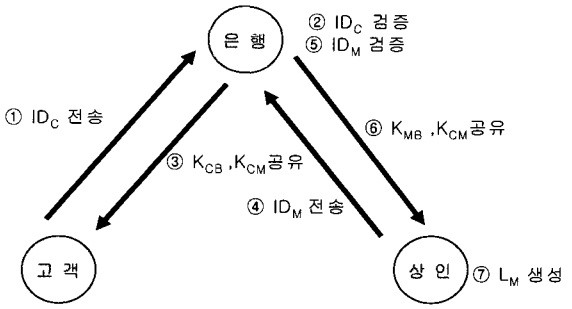
이 절에서는 앞으로 사용하게 될 기호들을 정의한다.

- C : 고객
- B : 은행
- M : 상인
- C_M : 거래 코드
- ID_C : 거래에서 사용되는 고객의 익명 ID
- ID_{M_k} : 상인 M_k의 ID
- ID_B : 은행의 ID
- L_M : 상인의 위치정보
- E_M : 상인의 유효기간
- K_{CB} : 고객과 은행간에 공유된 비밀키
- K_{CM} : 고객과 상인간에 공유된 비밀키
- K'_{CM} : 은행에서 생성한 고객과 상인간의 공유된 one-time 세션 키
- K_{M_kB} : 상인 M_k와 은행사이의 공유된 비밀키
- $\{M\}_{K_{ij}}$: M은 비밀키 K_{ij}에 의해 암호화
- $H(\cdot)$: MD5와 SHA-1과 같은 암호 해쉬 함수
- $H^r(W_N)$: 함수 H가 W_N을 r번 적용한 결과는 $H^r(W_N)$이고 이 결과를 표시하면 다음과 같다.

$$H^r(W_N)=H(H(\cdots\ (H(W_N))\ \cdots)) \quad (\text{r times})$$

3.3 프로토콜

이 논문에서의 해쉬체인은 체인의 루트를 통해 식별되므로 익명성을 제공하기 위해서는 루트값이 인출되는 과정에서 한번 은닉되어야 한다. 또한 선불방식이므로 고객이 체인의 길이에 대해 부정을 할 수 없어야 한다. 길이에 대한 부정을 방지하는 방법으로는 Solages와 Traore가 제안한 제한적 은닉서명과 추적 기능을 적용한다[16].



(그림 3) 등록 프로토콜

3.3.1 등록 프로토콜(Registration protocol)

고객은 자신의 사생활 정보와는 상관없는 임의의 신원정보 ID_C를 생성한 후, 생성한 정보를 검증받기 위해 ID_C를 은행에게 전달한다. ID_C를 전달받은 은행은 고객의 신원정보를 통해 ID_C를 검증한다. 검증이 끝나면 은행은 고객의 계정을 만들고, 고객의 고객 식별자 정보를 데이터베이스에 기록해 놓는다. 이런 과정이 모두 끝나면 고객과 은행은 비밀키 K_{CB}를 공유한다[17]. 상인도 고객과 유사한 방법으로 은행에게 계정을 개설하고 은행과 정보를 공유하기 위해 비밀키 K_{MB}를 공유한다. 공유 작업이 모두 끝난 후에 은행은 고객과 상인사이에 사용하게 될 비밀키 K_{CM}을 생성하여 고객과 상인에게 전달한다. 또한, 상인은 고객의 익명성 및 사생활 정보를 노출시키지 않으면서 서로 다른 상인과 거래를 할 수 있도록 상인의 위치정보 L_M을 생성한다. 마지막으로 은행은 상인의 위치정보 L_M을 $M(ID_M)$의 실제 인식 정보와 묶는다.

3.3.2 인출 프로토콜(Withdrawal protocol)

고객은 상인으로부터 서비스를 요청하기 전에, 상인을 방문하여 거래 코드, 상품 대금, 상인 위치정보등의 구매정보를 이용하여 다중의 상인에게 지불할 수 있는 해쉬체인 값을 만든다.

상인은 거래코드 C_M, 상인위치정보 L_M, 그리고 고객이 지불의 root 값으로 사용할 해쉬 체인값을 생성한다. 상인은 해쉬 체인값을 생성하기 전에 해쉬 체인의 키 값으로 T_U를 생성한다. T_U는 고객의 신원정보 ID_C와 상인이 생성한 난수 r_M, 고객과 상인사이에 공유된 비밀키 K_{CM}으로 구성된다. T_U는 상인이외에는 생성할 수 없으며 상인이 생성하는 해쉬 체인이 어느 고객에게 발급되는 것인지를 분명히 하기 위해 사용된다. 그리고 상인은 고객이 수행하는 해쉬 체인 연산과 유사한 방법으로 새로운 해쉬 체인값 HC를 생성한다. 즉 상인은 해쉬체인 길이 N에 대하여 임의의 S_N을 선택하고, i=N-1,...,0에 대하여 해쉬 체인값을 생성한다.

$$T_u=\{ID_C,\ r_M,\ K_{CM}\}$$
$$HC = \{\ s_i |\ s_i = h(\ s_{i+1},\ T_u),\ i=N-1,...,0\} \quad (1)$$

상인이 생성한 정보 중 거래코드 C_M, 임의의 수 r_M은 상인이 랜덤하게 선택한 수로서 이중사용 방지 및 고객의 다중 상품 관리를 해주는 역할을 한다. 고객은 C_M, r_M정보 이외에 S_N과 T_U를 n번 해쉬함수에 적용한 상품 대금 HC와 함께 구매정보를 구성한다. 상인이 거래코드 C_M 및 상인의 위치정보 L_M을 고객에게 전달하게 되면 은행은 상인이 고객에게 전달한 거래코드 및 위치정보 L_M을 알 수 없어 고객의 구매정보를 추적할 수 없게 된다. 상인은 이와같이 생성된 (2)의 정보를 고객에게 전송한다.

$$\{ID_C,\ ID_M,\ HC,\ T_U,\ \mathrm{N},\ C_M,\ L_M\}_{K_{CM}} \qquad (2)$$

이 방법은 해쉬함수와 비밀키를 사용하기 때문에 공개키를 사용하는 방법보다 비용측면에서 소액지불시스템에 더 적합하다. 그리고, 고객은 (3)과 같은 방법으로 은행에게 인출요구를 전달한다. 인출요구 중 $\{C_M, L_M\}_{K_{CM}}$은 T_U에서 생성한 고객과 상인의 세션키로 암호화하였기 때문에 은행은 거래코드를 알 수 없으며 거래코드를 통한 구매자의 구매정보를 추적할 수 없게 된다. 이 방법은 eCash의 blind 서명기법보다 소액지불시스템에 적합하다.

$$(ID_C, ID_B, \{C_M, L_M\}_{K_{CM}}, T_U, S_N, h(T_U, S_k))_{K_{CB}} \qquad (3)$$

은행은 고객의 ID_C 테이블을 유지하면서 고객과 공유하고 있는 비밀키 K_{CB}를 이용하여 인출 요구를 인증한다. 은행은 고객이 보내온 상품대금과 은행에 남아있는 대금을 비교하여 지불가능한지를 판단한다. 그리고 은행은 고객이 보낸 상품금액을 통해 해쉬 체인 길이 N을 결정하고, 해쉬체인의 루트인 W_N을 선택하여 (4)의 식을 만족하는 해쉬체인 W_0, W_1, ..., W_N을 생성한다.

$$W_i = H(W_{i+1}),\quad \mathrm{i} = \mathrm{N}\text{-}1,\ \mathrm{N}\text{-}2,\ \ldots,\ 0. \qquad (4)$$

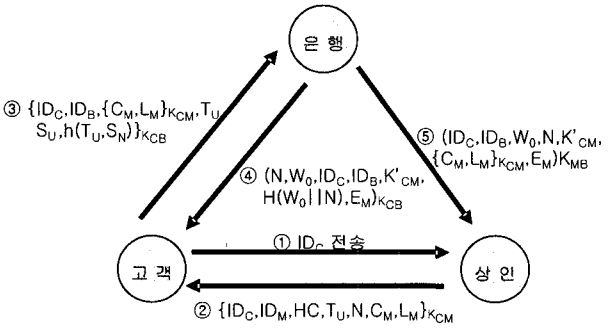
W_0는 해쉬체인의 종자값(SEED)이라고 불리우는 마지막 해쉬값이다. 체인의 W_i 는 소액지불을 위해 고정된 값을 미리 결정한다. 그리고, 은행은 고객과 상인간의 공유된 one-time 세션 키 K'_{CM}을 생성한다. 그 때 고객은 은행으로부터 (5)와 같은 인출응답 정보를 전달받는다.

$$(N,\ W_N,\ W_0,\ K'_{CM},\ H(W_0 \| N),\ E_M)_{K_{CB}} \qquad (5)$$

$H(W_0 \| N)$은 해쉬체인의 명확성을 보이면서 해쉬체인의 상태정보를 저장하기 위해 사용되고 있다. 은행은 고객의 계좌에 남아있는 금액과 상품대금에 대한 모든 정보를 가지고 상품에 대한 지불여부를 판단할 수 있다. 은행은 상인에게 권한을 주기 위해 (6)과 같은 정보를 전달한다.

$$(N,\ W_0,\ ID_C,\ ID_B,\ K'_{CM},\ E_M,\ \{C_M, L_M\}_{K_{CM}})_{K_{MB}} \qquad (6)$$

상인은 은행에게 정보의 타당성을 체크받은 후 권한 정보를 저장한다.



(그림 4) 인출 프로토콜

3.3.3 지불 프로토콜(Payment protocol)

고객은 $W_i = H(W_{i+1})$(i=N-1, N-2, ...,0)과 같은 등식으로 은행으로부터 수신된 W_N을 N번 해쉬한다. 인출비용의 명확성을 체크하기 위해 W_0와 일치하는지 마지막 해쉬값을 비교한다. 만일 모든 검증이 통과되면 고객은 (7)의 지불내용을 상인에게 제출한다.

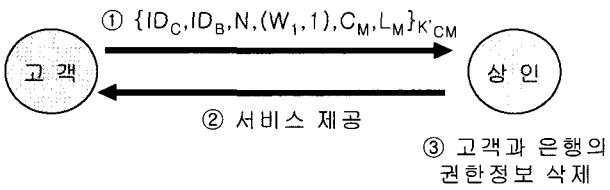
$$\{N, ID_C, ID_B, (W_1, 1), C_M, L_M\}_{K'_{CM}} \qquad (7)$$

(W_i, i)는 체인의 해쉬값과 인덱스로 구성된 지불쌍으로 표현한다. 상인은 구매정보를 위해 처음 해쉬값을 재구성하여 지불의 무결성을 체크할 수 있다. 상인은 ID_C와 일치하는 은행 권한 메시지가 지불명령을 전달한 고객에 의해 제공되고 있는지를 데이터베이스를 통해 검색한다. 상인은 상인의 데이터베이스에 저장된 E_M을 체크하여 해쉬체인을 명확하게 검증하기 위해 고객으로부터 수신된 W_1을 해쉬하여 해쉬값을 계산한다.

$$H(W_1) = W_0 \qquad (8)$$

W_0는 상인의 데이터베이스에 저장된 해쉬 체인의 루트이다. 만일 모든 검증이 성공적으로 검증되었다면, 상인은 은행과 고객에게 제공된 N 값을 이용하여 아이템이나 서비스를 고객에게 전달한다.

첫 지불쌍 (W_1, 1)이 상인에게 수신되면 고객은 다중 지불을 위해 (W_i, i)를 상인에게 전달하고, 상인은 마지막 해쉬 값 W_N까지 계속적으로 아이템이나 서비스를 전달한다. 고객과 상인 사이의 모든 세션이 끝나면 상인은 해쉬체인 W_0 값, 구매 관련정보, E_M, 고객의 ID_C, 은행의 ID_B등 고객 및 은행 권한 정보를 제거한다.



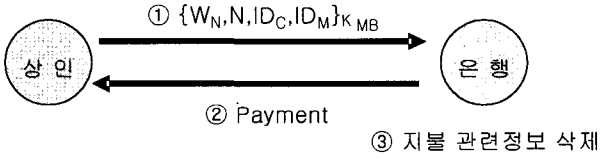
(그림 5) 지불 프로토콜

3.3.4 예치 프로토콜(Deposit protocol)

지불을 수신하기 위해 상인은 거래가 끝난 후에 은행과 함께 고객으로부터 수신된 해쉬체인을 되찾아야 한다. 상인은 고객의 지불 구조로부터 유추된 (9)의 예치 요구를 은행에게 전달한다.

$$(W_N, N, ID_C, ID_M)_{K_{MB}} \tag{9}$$

예치 요구를 전달받은 은행은 해쉬체인을 통해 은행의 데이터베이스에 저장된 E_M파라미터를 검증하거나 예치 요구에 관련된 각 항목의 명확성을 검증한다. 만일 검증이 성공하면 은행은 상인의 계좌에 돈을 전달하고 지불과 관련된 정보를 삭제한다.



(그림 7) 예치 프로토콜

4. 성능 분석

4.1 분할성(Divisibility)

고객이 구매정보와 관련된 정보를 은행에게 전달하는 방법은 크게 두 가지가 있다. 첫째는 고객이 상인과 거래하고자 할때이고, 두 번째는 고객이 은행으로부터 필요한 전자화폐를 모두 얻기 위해 인출을 원할때이다. 은행은 고객에 의해 전달받은 총액을 나타내는 N과 W_N을 선택한다. N 동전을 얻기 위한 동전 체인은 P 하위체인으로 나누어 질 수 있다(P≤N). 만일 동전 체인이 $\{W_i\}$(i=0,1,...,N)으로 주어진다면 다음과 같은 하위체인이 만들어진다.

$$C_1,\ \mathrm{N},\ W_N,\ W_i,\ \mathrm{i}=0,1,\ldots,C_1$$
$$C_2,\ \mathrm{N},\ W_N,\ W_i,\ \mathrm{i}=C_1+1,\ C_1+2,\ldots,C_1+C_2$$
$$\cdots\cdots$$
$$C_P,\ \mathrm{N},W_N,\ W_i,\ \mathrm{i}=C_1+\ldots+C_{P-1}+1$$
$$C_1+\ldots+C_{P-1}+2,\ldots,C_1+\ldots+C_{p-1}+C_P$$

하위체인이 만들어지면 은행은 C_1, C_2,...,C_P는 $C_1+C_2+\ldots+C_P$=N을 만족하는 각 상인의 서비스의 값을 표현한다. 그리고, 은행은 $W_0, W_{C_1}, W_{C_1+C_2},\ldots, W_{C_1+C_2+\cdots+C_P}$을 저장하고 고객과 상인에게서 각 하위체인의 타당성이 만족하는 동안 저장된 W값을 상인에게 전달한다. 각 상인은 고객의 구매정보와 일치하는 하위체인의 종자값만 획득할 수 있다. 예를 들어 상인 M_K는 하위체인 C_K: $W_{C_1+\cdots+C_{k-1}}$의 종자값을 수신받는다. 지불이 발생하면 고객은 상인에게 다음과 같은 M_K의 지불 구조를 보낸다.

$$\{C_K, ID_C, ID_B, L_M,\ W_{C_1+\cdots+C_{k-1}+1}, OI_K\}_{K_{CM_K}} \tag{10}$$

M_K는 $H(W_{C_1+\cdots+C_{k-1}+1})=W_{C_1+\cdots+C_{k-1}}$이 맞는지 검증한다. M_K는 고객에게 전자 아이템이나 서비스의 단위를 보낸다. 세션이 끝난후에 M_K는 은행에게 다음의 지불요구를 보낸다.

$$(W_{C_1+\cdots+C_{k-1}}, W_{C_1+\cdots+C_k}, C_k, ID_C, ID_M)_{K_{MB}} \tag{11}$$

4.2 공평성(Fairness)

제안기법은 다른 구성 요소간에 은행이 신뢰성을 갖을 수 있는 선불방식이다. 제안 기법에서 고객은 요청된 아이템이나 서비스가 수신되기 전에 은행에게 돈을 지불해야 한다. 이렇게 하면 상인과 은행사이에 발생되는 불이익을 예방할 수 있다. 은행은 고객이 이중지불의 위험성을 줄이기 위해 거래에 사용된 해쉬 체인의 타당성을 생성하는 책임을 진다. 반면 상인은 고객의 구매요구가 받아들이기 전에 은행에게 은행의 권한 메시지를 요구하고 은행은 데이터베이스를 통해 지불 명령의 타당성을 체크한다. 지불이 되면 상인은 고객의 이중 지불을 막기위해 고객과 관련된 정보를 삭제한다. 동일한 이유로 은행은 상인이 두 번 지불요청하는 것을 예방하기 위해서 지불에 관련된 정보를 제거한다. 지불 프로토콜 실행에서 고객의 지불과 상인의 서비스는 거래가 취소되도 추가적인 이익이 발생하지 않도록 단계적으로 수행된다. 은행은 체크의 타당성 이후에 상인으로부터 수신된 해쉬체인의 일부를 회수한다. 제안 시스템은 고객과 상인 사이가 공평하다.

4.3 보안성(Security)

이 논문에서는 지불 프로토콜이 실행되면 공격자가 위조할 수 없도록 하기위해 해쉬 체인을 사용한다. 그 이유는 $h(\cdot)$가 강한 암호학인 ONE-WAY 함수를 사용하고 있고, 고객과 은행사이에 세션키를 사용하기 때문이다. 상인은 항상 비밀키에 의해 암호화된다. 상인이 비밀키에 의해 암호화 되는 그 시점에 은행은 입금 과정이 끝난 후 데이터베이스로부터 입금 요구의 타당성을 검증하는 정보를 제거한다. 상인은 은행에 의해 요청된 타당성 조사가 통과되지 않고는 다른 어떤것도 되찾지 못한다. 제안시스템은 고객의 이중소

비와 초과소비(overspend)로부터 고객을 예방한다.

공격자가 임의의 어떤 고객으로 화폐를 인출하기 위해서는 먼저 그 고객의 신원을 증명할 수 있어야 한다. 이 증명을 하기 위해서는 고객의 공개 신원정보를 통해 고객의 실제 신원정보를 알아야 하지만 제안기법에서는 알 수 없다. 또한 고객은 신원을 증명할 때 시간 정보를 포함하므로 공격자는 기존 증명을 다시 사용할 수 없다.

4.4 효율성(Efficiency)

제안된 소액지불시스템은 해쉬함수를 기반으로 한 선불구조방식이다. 상인은 고객의 지불 요구의 복호화를 통해 타당성을 검증한다. 따라서 단지 두개의 비밀 대칭키 K_{CB}와 K_{CM}만이 고객, 은행, 상인사이에 필요하다. 즉, 세션키 이외의 어떤 인증서도 요구하지 않는다. 거래가 이루어지는 동안 해쉬 동작(해쉬 체인 생성과 검증)의 수는 Payword 기법과 동일하다.

초기 Payword 기법에서 고객은 은행에 의해 생성된 인증서와 루트 값 W_0의 디지털 서명, 기타 다른 정보 및 지불을 수신받기 위한 상인의 ID등을 생성한다. 이것은 Payword가 후불시스템이기 때문이고, 디지털 서명은 후에 고객이 지불하기 위한 약속으로써 사용되었다. 그러나 공개키 기반의 이러한 디지털 서명 요구는 항상 단점이 되고 있다. 이런 문제를 해결하기 위해 제안기법에서는 공개키 대신 세션키를 사용하여 연산비용을 향상시키고 있다.

특히, 제안한 논문에서는 동전을 해쉬체인으로 구성하여 인증서의 역할을 비밀키로 대처하였기 때문에 생성된 동전 각각에 공개키 서명을 수행하는 방식보다 빠르게 수행될 수 있다. 또한 기존의 익명성을 보장하는 전자화폐 시스템과 비교하여 계산상 효율적이다.

4.5 익명성(Anonymity)

초소액 지불 시스템의 익명성은 연동되는 일반적인 지불 시스템의 익명성과 밀접한 관계를 갖는다. 만일 연동되는 시스템이 익명성을 지원할 경우, 일반적으로 초소액 지불 시스템은 동일한 익명성을 갖는다. 그러나 그렇지 않을 경우, 별도의 방법이 요구된다.

제안 시스템의 경우, 고객의 익명성은 거래를 하는동안 예방할 수 있는 소액지불시스템의 중요한 부분이다. 제안기법에서 사용되는 해쉬체인은 은행에 의해 매도되고 상인에 의해 매수된다. 거래에 사용되는 고객의 익명 ID_C는 고객의 실제 정보와 관련이 없다. 상인은 고객이 거래하는 것을 결정하지 못하지만 은행은 상인의 위치정보가 포함된 고객의 구매정보를 이용한다.

de Solages 와 Traore의 제한적 은닉서명 정리 2에 의해 은행은 서명과정에서 얻은 정보로부터 서명한 메시지나 결과 서명에 대한 어떤 정보도 얻을 수 없다[16]. 뿐만 아니라 서명에 포함되는 C_M, L_M을 인출 과정에서 보지 못하므로 어느 판매자용 화폐를 인출했는지 알 수 없다.

4.6 기존 분할 가능한 화폐와 비교

기존 해쉬체인 기반 지불시스템과 제안시스템의 비교는 <표 1>과 같다. <표 1>에서 제안 시스템과 Nguyen등의 시

〈표 1〉 기존 해쉬체인 기반 지불시스템과의 비교

	선불 : ○ 후불 : □	범용 : ○ 판마재 전용 : □	익명성	효율성	안전성	인출비용	지불비용
Payword	□	□	×	공개키, 인증서사용	-고객의 프라이버시 노출 -이중사용 방지	×	-체인루트에 대한 서약(서명) 확인 -나머지 : 해쉬연산
iKP 기반 소액지불시스템	□	□	×	공개키, 인증서사용	-온라인과 오프라인의 중간형태의 지불방식 사용	×	-체인루트에 대한 서약(서명) 확인 -신용한도 확인 -나머지 : 해쉬연산
Mao의 시스템	○	○ 상인이 거스름	△ 가명 사용	공개키, 인증서사용	-이중사용 방지 -위조방지	한번 은닉서명	-여러 상인에게 지불할수록 그 다음 상인이 확인하여야 하는 정보가 많음
Nyugen의 이중잠금 해쉬체인	○	○ 이중잠금 해쉬체인	×	공개키, 인증서사용	-위조방지 -이중사용 방지	한번 일반서명	-체인루트에 대한 서약(서명) 확인 -나머지 : 해쉬연산 -영수증 발급
Nyugen의 시스템	○	○ 각 동전에 서명	○ 각 동전에 은닉서명	공개키, 인증서사용	-위조방지 -이중사용 방지	n번 은닉서명	-첫 동전: 서명과 시도와 응답 -나머지 : 서명
제안된 시스템	○	○ 지불대금에 서명	○ 루트에 은닉서명	비밀키, 인증서 필요없음	-이중사용 방지 -초과소비 방지 -위조방지	한번 은닉서명	-체인루트에 대한 서약(서명) 확인 -나머지 : 해쉬연산
일반 오프라인 동전방식	○	○ 각 동전에 서명	○ 완전한 연결불가능성	공개키, 인증서사용	-위조방지	n번 은닉서명	-각 동전마다 서명과 시도와 응답

스템은 길이가 n인 해쉬체인을 인출한다고 가정하며, 일반 동전방식의 화폐는 n개의 동전을 인출한다고 가정하고 비교한다[9, 10].

해쉬체인을 기반으로 화폐를 구성하고 있는 기존 기법들은 공개키를 사용하여 거래를 수행하지만 제안기법에서는 공개키대신 세션키를 사용하고 있기 때문에 기존 기법들보다 효율적이면서 인증서를 사용하지 않기 때문에 연산비용이 적게 든다. 그리고 제안기법에 사용되고 있는 해쉬체인은 체인의 루트를 통해 식별되므로 익명성을 제공하기 위해서 Nguyen등의 시스템이나 일반 오프라인 동전에서는 n번 은닉서명을 하지만 제안기법에서는 루트값이 인출되는 과정에서 한번만 은닉되기 때문에 효율적이다.

또한, 대부분의 분할 가능한 화폐[12-15]는 이진트리 구조를 이용하고 있다. 이 이진트리 구조는 인출하기 전에 미리 만든 구조가 아니며 지불할 때 필요한 노드만 만들어 사용한다. 반면 제안 시스템에서는 어떤 임의의 대금을 지불하기 위해 그만큼의 노드를 전달할 필요가 없으며, 그 만큼의 시도와 응답을 할 필요도 없다. 항상 최종 값 하나만 전달되며, 시도와 응답을 한번 수행하거나 서명을 하나 생성한다.

5. 결 론

앞으로의 전자상거래에서는 네트워크를 통해 직접 전송이 가능한 비교적 소액의 상품들이 많이 등장할 것이다. 이러한 소액 상품의 지불을 위해 해쉬함수와 같은 비용이 적게 드는 암호화 기법을 사용하는 Millicent, Payword, Micro Mint와 같은 지불 시스템들이 있다. 하지만 이러한 지불 시스템들은 고객의 익명성 보장이 되지 않는 문제점이 있다.

이 논문에서는 고객의 익명성이 보장되면서 고객의 프라이버시가 노출되지 않는 소액지불 시스템을 제안하였다. 해쉬 체인의 사용때문에 복잡해지는 이중사용 문제는 익명의 화폐가 범죄에 악용되는 것을 막기 위한 추적 기능을 이용하여 해결함으로써 인출과 지불 비용을 최소화 하였다.

또한, 시스템에 사용하는 공개키 대신 비밀키를 사용하여 인증서의 역할을 수행하지 않도록 효율성을 향상시켰고, 상품코드 C_M과 상인의 위치정보 L_M 등을 이용하여 익명성을 유지하면서 환불 기능을 제공하고 있다. 향후 연구에서는 제안된 방식보다 효율적이면서 안전한 기법 연구가 필요하다.

참 고 문 헌

[1] M. S. Manasse, "The Millicent Protocols for Electronic Commerce," Proc. of the 1st USENIX Workshop on Electronic Commerce, pp.117-123, Jul., 1995.

[2] A. Herzberg and H. Yochai, "Mini-pay: Charging per Click on the Web," Proc. of the 6th Int. World Wide Web Conf., Apr., 1997.

[3] C. Jutla and M. Yung, "PayTree: Amortized-Signature for Flexible MicroPayments," Proc. of the 2nd USENIX Workshop on Electronic Commerce, pp. 213-221, Nov. 1996.

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

[5] Y. Mu, V. Varadharajan, and L. Y. X. Lin "New Micropayment Schemes Based on PayWords," In Proceedings of 2nd Australasian Conference on Information Security and Privacy(ACISP '97), Lecture Notes in Computer Science 1270, pp.283-293, Springer-verlag, 1997.

[6] K. Q. Nguyen, Y. Mu, and V. Varadharajan, "Micro-Digital Money for Electronic Commerce," Proc. of the 13th IEEE ACSAC, pp.2-8, Dec., 1997.

[7] W. Mao, "Lightweight Micro-Cash for the Internet," Proc. of the ESORICS'96, LNCS 1146, pp.15-32, Sep., 1996

[8] K. Q. Nguyen, Y. Mu, and V. Varadharajan, "Secure and Efficient Digital Coins," Proc. of the 13th IEEE ACSAC, pp. 9-15, Dec., 1997.

[9] S. brands, "Untraceable Off-line Cash in Wallets with Observers," Crypto'93, LNCS 773, pp.302-318, Aug., 1993.

[10] A. De Solages and J. Traore, "An Efficient Fair Off-Line Electronic Cash System with Extensions to Checks and Wallets with Observers," Proc. of the 2nd Int. Conf. on Financial Cryptography, :NCS 1465, pp.275-295, Feb., 1998.

[11] Q. N. Khanh, Y. Mu and V. Varadharajan, "Digital Coins based on Hash Chain," In proceeding of the ACM SIGMOD conference on Management of Data, pp.169-180, Philadelphia, 1999.

[12] T. Okamoto, "An Efficient Divisivle Electronic Cash Scheme," In Proceedings of Crypto'95, Lecture Notes in Computer Science, pp.438-451, Springer-Verlag, Berlin, Germany, 1995.

[13] T. Okamoto and K. Ohta, "Universal Electronic Cash," In proceedings of Crypto'91, Lecture Notes in Computer Science 576, pp.324-337, Springer-Verlag, Berlin, Germany, 1992.

[14] Chan, A., Frankel, Y., and Tsiounis, Y., "Easy Come - Easy Go Divisible Cash," Advances in Cryptology, Eurocrypt 1998, LNCS 1403, pp.561-575, Springer, 1998.

[15] Nakanishi, T. and Sugiyama, Y., "Unlinkable Divisible Electronic Cash," Proc. of the 3rd Int. Workshop on Information Security, ISW 2000, LNCS 1975, pp.121-134, Springer, 2000.

[16] de Solages, A. and Traore, J., "An Efficient Fair Off-line Electronic Cash System with Extensions to Checks and Wallets with Observers," Proc. of the 2nd Int. Conf. on Financial Cryptography, FC 1998, LNCS 1465, pp.275-295, Springer, 1998.

[17] Schnorr, C.P., "Efficient Signature Generation by Smart Cards" J. of Cryptology, Vol.4, No.3, pp.161-174, 1991.
[18] Jing-Jang Hwang, Tzu-Chang Yeh, Jung-Bin Lie, "Securing on-line credit card payments without disclosing privacy information," computer Standards & Interfaces 25, pp.119-129, 2003.
[19] Network Working Group, "AAA Authorization Appllication Examples," RFC 2905, http://www.faqs.org/rfcs/rfc2905.html.

정 윤 수

e-mail : bukmunro@netsec.cbnu.ac.kr
1998년 청주대학교(이학사)
2000년 충북대학교 대학원 전자계산학과 (이학석사)
2003년~현재 충북대학교 이공대학 전자계산학과 박사과정
관심분야 : 암호이론, 정보보호, Network Security, 이동통신보안, 전자상거래보안

백 승 호

e-mail : manitto@netsec.cbnu.ac.kr
2003년~현재 충북대학교 전기전자컴퓨터 공학부 전자계산학과 석사과정
관심분야 : 침입탐지, 정보보호, Network Security

황 윤 철

e-mail : dolpin98@netsec.cbnu.ac.kr
1994년 한남대학교 전자계산공학과
1996년 한남대학교 전자계산공학과 (공학석사)
1999년~현재 충북대학교 전기전자컴퓨터 공학부 전자계산학과 박사수료
관심분야 : 인터넷, 정보보호, Network Security

이 상 호

e-mail : shlee@chungbuk.ac.kr
1976년 숭실대학교 전자계산학과
1981년 숭실대학교 전자계산학과(MS)
1989년 숭실대학교 전자계산학과(PHD)
1976년~1979년 한국전력 전자계산소
1981년~현재 충북대학교 전기전자컴퓨터 공학부 & 컴퓨터정보통신연구소 교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture