2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

# 단일 해쉬 체인으로 다중 지불을 지원하는 개선된 PayWord 프로토콜

박애영, 임형석
전남대학교 전산학과
e-mail : u0020366@chonnam.chonnam.ac.kr

# An Improved PayWord Protocol Supporting Multiple Payment with Single Hash Chain

Ae-Young Park, Hyeong-Seok Lim
Dept. of Computer Science, Chonnam National Univ.

**요 약**

공개키 연산을 이용하는 고액 지불 시스템(Macro Payment System)은 높은 수수료로 인해 경제성이 맞지 않아 소액 지불(Micro Payment)에는 적합하지 않다. 해쉬 연산을 이용한 PayWord 프로토콜은 저렴한 메커니즘 비용과 신속한 트랜잭션 처리, 거래과정에서 브로커의 오프라인 참여로 소액 대금 결재에 적합하다. 그러나 특정 상점에만 사용 가능한 화폐가치를 포함하여, 사용자가 거래하는 상점이 많아지면 관리·저장해야 하는 해쉬 체인의 수가 늘어나는 단점이 있다.

본 논문에서는 전자화폐에 해당하는 해쉬 체인을 하나만 생성하여 여러 상점들에 안전한 지불을 수행하는 개선된 소액 지불 프로토콜을 제안한다. 제안한 방법은 지불과정에 MAC(Message Authentication Code)을 이용한 해쉬 값을 추가하여, 상점들의 공모 및 악의적인 수정을 방지한다. 따라서 사용자는 하나의 해쉬 체인만을 생성함으로써 기존의 PayWord보다 계산부담이 줄고, 여러 상점들과의 일시적인 거래관계에서도 효율적인 지불을 수행한다.

## 1. 서 론

인터넷을 상업적으로 이용하려는 움직임의 하나인 전자상거래(Electronic Commerce)는 시간과 공간의 제약을 받지 않고 상점 및 소비자들에게 혁신적인 거래관계를 제공하여 고도의 성장을 거듭하고 있다. 최근에는 값비싼 고가의 물품 이외에도 신문기사나 미디어 파일 등의 정보상품에 대해서도 매매가 이루어지고 있다. 이러한 저가의 상품에 대해 기존의 고액 지불 시스템(Macro Payment System)을 그대로 이용할 경우 높은 수수료로 인해 경제성이 맞지 않아 특별히 소액 지불 시스템(Micro Payment System)을 이용하게 되는데, 이는 한번에 부과되는 금액이 매우 적은 전자상거래 트랜잭션을 의미한다. 이 용어는 한번의 트랜잭션이 일어날 때마다 수 센트 정도를 부과하거나, 또는 저가의 구매대금을 모았다가 하루 또는 일정기간마다 그 합산요금을 신용카드에 부과하는 등의 방법을 가리킨다.

소액 지불 시스템은 거래되는 비용이 매우 적기 때문에 메커니즘 비용이 저렴해야 하며, 신속한 트랜잭션 처리가 요구된다. 다만 고액 지불 시스템에 비해 보안의 강도는 다소 떨어질 수 있다. 기존의 고액 지불 시스템에서는 안전한 지불을 위해 널리 공개키 연산을 사용하고 있다. 공개키 연산은 높은 보안 성능을 보장하는 대신 계산량이 많아 속도가 느리며 시스템의 부하도 크다. 따라서 최소한의 보안을 유지하고 처리비용을 줄여 소액 거래를 가능하게 하자는 소액 지불 시스템에서는 공개키 연산을 줄이고 주로 해쉬 연산을 이용하고 있다. 해쉬 연산은 공개키 연산에 비해 빠르게 계산될 수 있고, 시스템 자원도 그리 오래 차지하지 않기 때문이다. 이러한 해쉬 함수의 장점을 이용하여 설계된 소액 지불 프로토콜에는 iKP, PayWord, MicroMint, MPTP, NetCard 등이 있다[1,2,3,5]. 그 중 PayWord는 메커니즘 비용이 저렴하고, 신속한 트랜잭션 처리를 수행하며, 지불과정에서 브로커의 오프라인 참여로 소액 대금 결제에 적합한 시스템으로 알려져 있다[5].

소액 지불 시스템과 관련된 최근 동향으로는 브로커로부터 구입한 전자화폐의 사용에 있어 여러 상점에 지불을 허용할지의 여부와 거래과정에서 브로커의 참여정도를 꼽을 수 있다. PayWord는 지불과정에서 브로커가 오프라

※ 본 논문은 한국과학재단의 특정기초연구(98-0102-11-01-3) 연구비 지원에 의한 것임.

인으로 참여하고 있지만 특정 상점에게만 사용할 수 있는 화폐가치를 포함한다는 단점이 있다. 따라서 사용자는 새로운 상점과 거래할 때마다 새로운 전자화폐를 생성해야만 한다. 실제로 소액 지불 시스템의 상거래 대부분이 상점과 사용자간에 지속적인 거래를 행하지 않고 일시적인 관계에 그친다는 점을 고려하면 이는 소액 지불 프로토콜로서 효율성이 저하되는 요인이 된다.

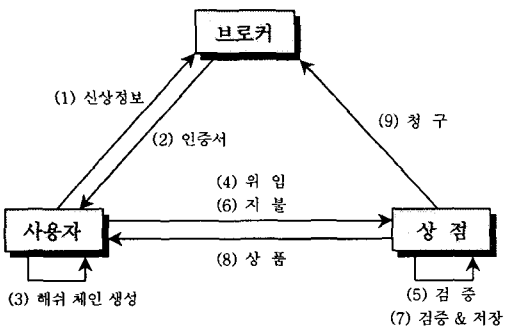
본 논문에서는 사용자가 생성한 하나의 해쉬 체인만으로 여러 상점들에 안전한 지불을 수행하는 개선된 PayWord 프로토콜을 제안한다. 제안한 방법은 지불과정에 키를 포함한 해쉬 값을 추가하여 여러 상점들에 안전한 지불을 수행한다. 즉 MAC(Message Authentication Code)을 이용하여 단일 해쉬 체인의 사용으로 발생할 수 있는 상점들의 공모를 방지하고, 상점의 악의적인 수정을 막을 수 있다[6]. 또한 메시지의 무결성과 사용자 인증을 제공하여 보다 안전한 트랜잭션 처리가 가능하다. 사용자는 하나의 해쉬 체인만을 생성하므로 기존의 PayWord보다 계산부담이 줄어 여러 상점들과의 일시적인 거래관계에서도 효율적인 지불을 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문의 기반이 되는 PayWord 프로토콜에 대해 살펴보고, 3장에서는 이중 잠금 해쉬 체인 구조를 갖는 프로토콜에 대해 설명한다. 4장에서는 사용자가 하나의 해쉬 체인만을 이용하여 여러 상점들에 안전한 지불을 수행하는 개선된 소액 지불 프로토콜을 제시하고 5장에서 결론을 맺는다.

## 2. 관련 연구

### 2.1 PayWord

PayWord는 연쇄 해쉬 함수를 이용한 소액 지불 프로토콜로서 1996년 *Ronald L. Rivest*와 *Adi Shamir*에 의해 제안되었다[5]. 전체적인 구조는 그림 1과 같다.




[그림 1] 기존의 PayWord 프로토콜

이는 브로커, 상점, 그리고 사용자로 구성되어 신용카드에 기반하고 있다. 계산량을 줄이기 위해 해쉬 연산을 이용하되, "payword"라 불리우는 해쉬 값들은 각각 1센트의 가치를 지닌다고 가정하고, 일련의 체인형태로 표현되어 상점과의 거래과정에서 지불에 이용된다. 또한 통신부하를 줄이기 위해 오프라인으로 결재를 하며, 각 상점마다 특정 해쉬 체인을 생성하므로 주기적인 지불에 효율적으로 동작한다. 반면 양도성과 익명성은 지원하지 않아 고액 지불 시스템에 비해 보안의 강도는 다소 떨어진다.

먼저 사용자는 안전한 채널을 통해 브로커에게 신상정보를 전송후 인증서를 요청한다. 브로커는 사용자의 전자화폐를 판매자가 신뢰하도록 인증서를 발급하여 추후 판매자로부터 전자화폐를 회수하여 실제화폐로 교환해주게 된다. 인증서를 통해 전자화폐를 생성할 수 있는 권리를 인정받은 사용자는 거래하고자 하는 상점을 위한 해쉬 체인을 생성한다. 사용자는 해쉬 값이 인증서를 통해 정당하게 생성됐음을 증명하는 메시지인 위임을 전송 후, 상점으로부터 검증이 완료되면 지불을 수행한다. 사용자로부터 상점에게로의 $i$번째 지불은 $(w_i, i)$ 쌍으로 구성된다. $w_i$는 구매 금액에 해당하는 해쉬 값이고, $i$는 그의 인덱스이다. 상점은 위임에 포함된 루트 값을 이용하여 지불 받은 해쉬 값의 유효성을 검증할 수 있다. 일정 마감시점이 되면 상점은 각 사용자들로부터 지불 받은 해쉬 값들을 브로커에게 전송하여 실제화폐로의 교환을 청구함으로써, PayWord 프로토콜의 모든 트랜잭션이 마감된다.

PayWord는 전체적인 프로토콜이 간략하고, 거래과정에서 브로커가 오프라인으로 참여하며, 해쉬 연산의 이용으로 사용자와 상점간의 신속한 트랜잭션 처리가 이루어진다. 그러나 사용자가 생성한 해쉬 체인은 여러 상점에 사용되지 못하고 각 상점마다 특정 해쉬 체인을 생성해야 하는 단점이 있다. 이는 사용자와 상점간의 지속적인 거래관계에 있어 유리하게 작용하지만, 소액 지불 거래가 대부분 일시적이라는 것을 고려할 경우 효율성이 저하되는 요인이 된다.

### 2.2 이중 잠금 해쉬 체인 (double-locked hash chain)

이중 잠금 해쉬 체인은 앞서 언급한 단일 해쉬 체인의 단점을 개선하고자 1997년 Nguyen이 새롭게 제시한 방법이다[4]. 이 방법은 전자화폐에 분할성을 부여한 두 개의 해쉬 체인을 사용하고 있다. 하나의 해쉬 체인은 일반적인 해쉬 함수를 사용하여 이루어지며 다른 하나는 해쉬 체인 데이터의 암호화 및 무결성 확보를 위해 사용된다.

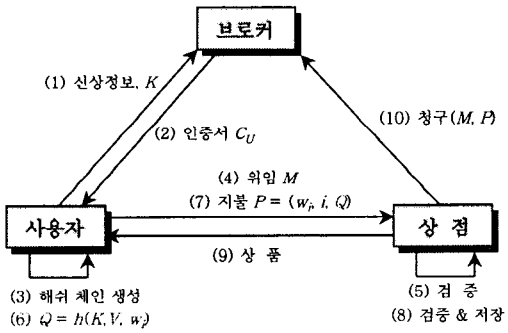
PayWord처럼 사용자가 랜덤하게 선택한 초기 값 $w_n$을 역순으로 해쉬 해가며 하나의 해쉬 체인을 생성하고, 또 다른 초기 값 $w'_n$을 역순으로 해쉬 해가며 또 하나의 해쉬 체인을 생성하게 된다. $n$ 길이를 가진 두 개의 해쉬 체인은 동전을 표현하기 위해 함께 사용되며, $w_0$와 $w'_0$는 두 해쉬 체인의 루트로서 검증 값으로 쓰이게 된다. 하나의 동전은 첫 번째 해쉬 체인의 앞쪽 해쉬 값과, 두 번째 해쉬 체인의 뒤쪽 해쉬 값으로 이루어진 쌍으로 표현

된다. 첫 번째 동전은 ($w_0$, $w'_n$), 두 번째 동전은 ($w_1$, $w'_{n-1}$), 이런 식으로 각 동전은 양쪽 끝에서부터 사용되어 표현된다.

그러나 이중 잠금 해쉬 체인 프로토콜은 지불과정에서 같은 상점이 전·후 해쉬 값의 동전을 지불 받게 되면 중간 해쉬 값들을 알아낼 수 있는 단점이 있다. 또한 소액 지불 시스템에는 적합하지 않은 공개키 연산이 빈번하게 사용되어 메커니즘 비용이 높으며, 캐쉬(cash) 기반의 선불 기법으로서 동전의 부족 및 잔여 처리에서 브로커의 계산상 오버헤드가 높다.

### 3. 단일 해쉬 체인만을 이용하는 개선된 프로토콜

본 논문에서는 PayWord 프로토콜을 기반으로, 사용자가 생성한 하나의 해쉬 체인만을 이용하여 여러 상점들에 안전한 지불을 수행하는 개선된 소액 지불 프로토콜을 제안한다. 전체적인 구조는 그림 2와 같다.




[그림 2] 개선된 PayWord 프로토콜

최근 소액 지불 시스템과 관련하여 브로커로부터 구입한 전자화폐의 사용에 있어 여러 상점에 지불을 허용할지의 여부에 대해 이슈가 되고 있는데, 본 논문의 기반이 되는 PayWord 프로토콜은 이 조건을 만족하지 못하고 있다. 따라서 사용자가 생성한 하나의 전자화폐를 여러 상점에 지불하되, 제안한 방법은 지불과정에 키를 포함한 해쉬 값을 추가한다. 즉, MAC을 이용함으로써 키를 알지 못하는 상점의 수정 및 다른 상점들의 공모를 방지한다[6].

제안한 방법은 기존의 PayWord 프로토콜과 동일하게 일정기간동안 모아둔 구매대금을 신용카드에 부과하는 방식으로 이루어진다. 프로토콜의 참여자는 브로커, 상점, 그리고 사용자로 구성된다. 브로커(Broker)는 은행 또는 신용카드 회사로서 사용자에게 전자화폐, 즉 해쉬 체인을 생성할 수 있는 권한을 부여하고, 상점들로부터 그 전자화폐들을 회수하여 실제 화폐로 교환해 주는 역할을 한다.

**(1) 인증서 발급**

프로토콜은 사용자가 브로커에게 계좌를 개설하고, 인증서를 요구하는 것으로 시작된다. 우선 사용자는 브로커에게 안전한 채널을 통해 자신의 신상정보를 전송한다.

$$Credit\ Card\ number,\ PK_U,\ A_U,\ K$$

전송되는 정보는 신용카드 번호(*Credit Card number*)와 사용자의 공개키($PK_U$), 사용자의 주소($A_U$), 해쉬 키($K$)이다. 해쉬 키 $K$는 사용자와 브로커만이 공유하는 키로서, 추후 지불에 추가되는 $Q$의 MAC 연산에 포함된다.

브로커는 사용자로부터 전송 받은 신상정보를 통해 정당한 사용자에 한하여 인증서를 발행한다.

$$C_U = \{B,\ U,\ A_U,\ PK_U,\ E,\ I_U\}_{SK_B}$$

인증서에는 브로커의 식별자($B$), 사용자의 식별자($U$), 그리고 사용자로부터 전송 받은 사용자의 공개키($PK_U$)와 주소($A_U$)가 포함된다. 그리고 인증서의 유효기간($E$)과 인증서의 일련 번호 같은 기타 부가정보($I_U$)가 포함된다. 이들 정보는 브로커의 비밀키($SK_B$)로 서명된다. 인증서는 유효기간이 지나면 재 발행 가능하다. 인증서는 사용자에게 전자화폐에 해당하는 해쉬 체인을 생성할 수 있도록 권리를 부여하고, 추후 상점이 사용자들로부터 지불받아 브로커에게 청구한 해쉬 값들이 정당하다는 것을 보증해주는 서류로 쓰이게 된다.

**(2) 구 매**

인증서 $C_U$를 발급 받은 사용자는 거래하고자 하는 상점에 접속하여 위임(commitment)과 해쉬 체인(hash chain)을 계산하게 된다. 위임은 사용자가 상점과 하루의 첫 거래를 시작하며 전송하는 메시지로서, 지불에 사용하는 해쉬 값들이 인증서에 기반한 정당한 값이라는 것을 보증해 준다. 위임에는 해쉬 체인의 첫 번째 값인 루트($w_0$)를 비롯하여, 상점의 식별자($V$), 브로커로부터 발급받은 인증서($C_U$), 현재 날짜($D$), 그리고 부가정보($I_M$)가 포함되어 사용자의 비밀키($SK_U$)로 서명된다.

$$M = \{V,\ C_U,\ w_0,\ D,\ I_M\}_{SK_U}$$

위임 $M$을 전송 받은 상점은 사용자의 서명과, 위임에 포함된 인증서의 브로커 서명을 검증한다. 또한 현재 날짜는 인증서의 유효기간을 체크할 수 있다.

해쉬 체인은 기존의 PayWord 프로토콜과 마찬가지로 사용자가 랜덤하게 선택한 초기 값 $w_n$을 역순으로 해쉬해가며 생성한다. 이는 해쉬된 결과 값으로 해쉬 이전의 메시지를 알아내기 어렵다는 강한 일방향 해쉬 함수의 성질을 이용한 것이다.

$$w_i = h(w_{i+1}) \quad i = n-1,\ n-2,\ \ldots,\ 0$$

이렇게 생성된 $w_1$, $w_2$, ..., $w_n$의 해쉬 값들은 1센트의 가치를 지닌 동전이라고 가정하고, 1번부터 순서대로 사용된다. 마지막에 생성된 $w_0$는 가치를 지닌 동전이 아니고 단지 "root"로서 $w_1$에서 $w_n$까지의 해쉬 값들에 대한 검증 값으로 사용된다.

사용자는 지불에 앞서 해당 상점에 지불되는 해쉬 값을 다른 상점들로부터 숨기기 위한 특정 값을 계산한다.

$$Q = h(w_i, V, K)$$

$Q$는 지불에 해당하는 해쉬 값($w_i$)에 사용자의 식별값($V$), 그리고 사용자와 브로커만이 공유하는 해쉬 키 $K$를 포함하여 해쉬한 값이다. 즉 MAC을 이용한 값으로서, 키를 알지 못하는 상점은 $Q$의 수정이 불가능하고, 각 상점에 전송되는 $Q$는 모두 다른 값들로서 상점들간의 공모를 방지할 수 있다. 즉 $Q$는 지불에 해당하는 해쉬 값의 무결성과 사용자 인증을 제공함으로써, 사용자가 생성한 하나의 해쉬 체인이 여러 상점들에 안전하게 지불될 수 있도록 한다.

$$P = (w_i, i, Q)$$

지불은 구매 금액에 해당하는 해쉬 값 $w_i$와 그 인덱스 $i$, 그리고 $Q$로 구성된다. 이때 사용자는 해쉬 값들을 건너 뛰어 유연한 지불을 수행할 수 있다. 예를 들어 $w_2$를 지불한 후 $w_7$을 전송하면 5센트를 지불한 셈이 된다.

같은 날 해당 상점에서의 두 번째 거래부터는 위임을 보내지 않고 지불만을 전송한다. 지불은 암호화되지 않고 전송되어, 해쉬 값을 지불 받은 상점은 역순으로 인덱스만큼의 해쉬를 적용하여 루트 값이 계산되는지 검증한다. 상점은 $i$보다 작은 인덱스의 해쉬 값이 전송되면 이중사용으로 간주하고, $Q$는 상점이 알지 못하는 키가 포함된 해쉬 값이므로 위조가 불가능하다. 또한 각 상점들이 지불 받는 $Q$는 모두 다른 값들로서, 상점들의 공모도 방지할 수 있다. 검증이 성공적으로 끝나면 상점은 사용자에게 상품을 전달 후 위임과 그에 대응되는 지불을 저장한다. 저장은 지불 받은 모든 동전의 해쉬 값을 저장하지 않고, 마지막에 지불 받은 가장 큰 인덱스의 해쉬 값만을 저장한다. 이때 상점은 구매정보를 저장하지 않는 것으로, 사용자의 사생활을 보호한다.

**(3) 회 수**

일정 마감시점이 되면, 상점은 각 사용자들로부터 지불 받은 해쉬 값을 브로커에게 전송하여 실제 화폐로의 교환을 요구한다. 브로커는 청구 메시지를 전송 받아 위임($M$)상의 사용자 서명과 인증서($C_U$)상의 자신의 서명을 검증 후, 사용자와 공유하는 키로서 청구된 금액($w_i$)과 상점의 식별자($V$)를 해쉬하여 상점이 보내온 $Q$와 비교한다. 두 해쉬 값이 같으면 브로커는 상점이 보내온 청구 금액이 변형되지 않았다는 무결성과, 사용자가 보낸 것이 확실하다는 사용자 인증도 수행할 수 있다. 브로커는 검증이 완료되면 상점의 계좌에 청구 금액을 입금시키고, 추후 사용자의 계좌에서 차감 하게 된다. 브로커의 이러한 모든 작업들은 오프라인으로 수행되어 트랜잭션의 부하를 줄인다.

제안한 방법은 구매 과정에서 사용자의 지불메시지에 MAC을 이용한 해쉬 값 $Q$를 추가함으로써, 단일 해쉬 체인의 사용으로 발생 가능한 여러 상점들의 공모를 방지한다. $Q$는 사용자와 브로커만이 공유하는 키로서만 계산될 수 있어, 키를 모르는 임의의 제 3자나 상점은 $Q$의 생성 및 악의적인 수정이 불가능하다. 또한 $Q$는 지불에 해당하는 해쉬 값에 대해 무결성과 사용자 인증 기능을 제공하고 있다. 따라서 사용자는 하나의 해쉬 체인만을 이용하여 여러 상점들에 안전한 지불을 제공할 수 있는 것이다. 제안한 방법은 기존 PayWord 프로토콜의 효율성을 높이고, 사용자의 계산부담을 줄임으로써 보다 빠르고 안전한 트랜잭션 처리가 가능하다.

## 4. 결 론

본 논문에서는 PayWord 프로토콜을 기반으로 사용자가 하나의 해쉬 체인만을 이용하여 여러 상점들에 안전한 지불을 수행하는 개선된 소액 지불 프로토콜을 제안하였다. 기존의 PayWord에서는 특정 상점에만 사용 가능한 화폐가치를 포함하여 거래하는 상점이 많을 경우 사용자가 생성 및 관리하는 해쉬 체인의 수가 늘어나게 된다. 즉, 각 해쉬 체인의 길이와 마지막 해쉬값, 그리고 해쉬 체인의 지불 위치 등 관리 정보가 많아지는 단점이 있다.

제안한 방법은 사용자가 지불 메시지에 MAC을 이용한 해쉬 값을 추가하여, 단일 해쉬 체인의 사용으로 발생할 수 있는 상점의 악의적인 수정 및 다른 상점들의 공모를 방지하고 있다. 따라서 사용자는 기존의 PayWord보다 계산부담이 줄고, 여러 상점들과의 일시적인 거래관계에서도 효율적인 지불이 가능하다.

## 5. 참고 문헌


[1] R. Anderson, C. Manifavas and C. Sutherland, "NetCard -A practical Electronic Cash System," *Proc. Security Protocol Workshop, LNCS. 1189*, pp.49-57, 1997.

[2] R. Hauser, M. Steiner, and M. Waidner. "Micro-payments based on iKP," *14th Worldwide Congress on Computer and Communications Security Protection*, pp.67-82, 1996.

[3] P. M. Hallam-Baker, "Micro Payment Transfer Protocol (MPTP)," *W3C Working Draft WD-mptp-951122* (22-Nov-95), http://www.w3.org/TR/WD-mptp.

[4] K. Q. Nguyen, Y. Mu, and V. Varadharajan, "Micro -Digital Money for Electronic Commerce," *Proceedins of Annual Computer Security Applications Conference*, pp.2-8, 1997.

[5] R. L. Rivest and A. Shamir, "PayWord and MicroMint : Two simple micropayment schemes," *Proceedings of RSA '96 conference*, pp.69-88, 1996.

[6] G. Tsudik, "Message Authentication with One-Way Hash Functions," *ACM Computer Communications Review*, pp.29-38, 1992.