# ID 기반 키동의 프로토콜을 이용한 PayWord 시스템

준회원 이 현 주*, 정회원 이 충 세**

# PayWord System using ID-based tripartite Key Agreement Protocol

Hyun-Ju Lee* *Associate Member*, Chung-Sei Rhee** *Regular Members*

요 약

모바일 환경에서 전자 지불 메카니즘이 구축되기 위해서는 안전성과 효율성을 갖춘 지불 시스템의 개발이 필요하다. 기존의 PayWord 프로토콜은 판매자와 거래를 할 때마다 판매자의 인증서를 생성해야 하기 때문에 연산량이 빈번해진다. 본 논문에서는 유한체 $F_q$에서 타원곡선(Elliptic Curve Cryptosystem)을 이용한 ID 기반 3자간의 키 동의 프로토콜에 의해 생성된 세션키로써 개체간의 인증이 이루어지기 때문에 알고리즘 연산이 감소된다. 특히, ID 기반 공개키 암호 시스템을 적용하여 속도의 향상 및 위장 공격(Man-in-the-middle attacks)과 Forward secrecy에 안전하다.

Key Words : ID-based key agreement protocol, PayWord, Man-in-the-middle attacks, Forward secrecy

ABSTRACT

Development of an efficient and secure payment system is prerequisite for the construction of electronic payment mechanism in mobile environment. Since current PayWord protocol system generates vendor's certificate for each transaction, it requires lot of operation for transaction. In this paper, we use a session key generated by ID-based tripartite Key agreement protocol which use an Elliptic Curve Cryptosystem over finite field $F_q$ for transactions. Therefore, our protocol reduces algorithm operations. In particular, proposed protocol using ID-based public key cryptosystem has the advantages over the existing systems in speed and it is more secure in Man-in-the-middle attacks and Forward secrecy.

## I. 서 론

급속한 정보통신망의 발전에 힘입어 등장한 전자상거래는 시간적, 공간적 제약이 없는 새로운 시장으로 부각되고 있으며 세계 각국은 이러한 시장을 선점하기 위해 다양한 사이버 서비스를 제공하고 있다[1]. 신속성, 편의성 및 광역성으로 인하여 매우 빠른 속도로 발전하고 있는 전자상거래의 주요 요건들 중의 하나는 안전성과 효율성을 갖춘 전자 지불 시스템을 개발하는 것이다. 거래에 사용된 지불 정보들을 사용자가 복사해 두었다가 다른 거래에 복사된 지불 정보를 다시 사용하는 이중사용을 방지해야 하고, 제3자에 의해 위조나 변조된 지불 정보의 사용을 막을 수 있어야 한다. 그리고 거래가 인터넷을 통해 이루어지기 때문에 거래 주체간의 신뢰 구축을 위한 상호 인증이 우선되어야 하며, 지불 시스템 사용자의 사생활 침해를 막기 위해서 사용자에 대한 익명성이 보장되도록 설계되어야 한다. 전자저널, 게임, MP3 같은 음악화일, MPEG과

*충북대학교 컴퓨터과학과 알고리즘 연구실(pinklee104@korea.com)
**충북대학교 전기전자 및 컴퓨터공학부(csrhee@cbucc.chungbuk.ac.kr)
논문번호 : #030416-0923, 접수일자: 2003년 9월23일

AVI같은 동영상화일 및 GIF나 JPEG그림화일 등과 같은 소액 정보 상품에 대한 전자 지불을 효과적으로 수행하기 위한 전자 지불 프로토콜에는 PayWord, MilliCent, MicroMint, MPTP등이 있다[2,3,4]. 대부분의 소액 지불 프로토콜에서는 MD5와 같이 암호학적으로 강한 일방향 해쉬 함수를 반복해서 수행하는 해쉬 체인 기법을 사용한다[5].

기존 MilliCent 프로토콜은 Scrip의 보안에 대한 내용을 Scrip의 발행인만이 알고 있기 때문에 사용자가 브로커로부터 받은 Scrip에 대한 유효성 여부를 판단할 수 없다는 문제점을 가지고 있다[3]. 또한, PayWord프로토콜은 사용자가 거래하고자 하는 판매자마다 다른 해쉬 체인을 사용해야 하므로 사용자의 측면에서 판매자의 수만큼 공개키 연산을 수행해야 한다. 그러므로 좁은 대역폭을 가지고 메모리 용량과 계산 능력도 부족한 무선 환경에 적용하기에는 여러 가지 어려움이 따른다.

본 논문에서는 ID 기반 ECC(Elliptic Curve Cryptosystem)알고리즘에 의해 생성된 세션키를 사용하여 각 개체의 역할을 분산시킴으로써 효율성 및 안전성을 제공한다. 본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안한 ID기반 키동의 프로토콜에 사용된 bilinear map에 대해 설명하고, 3장에서는 기존의 PayWord프로토콜을 설명한다. 4장에서는 새로운 ID기반 지불 프로토콜을 기술하고, 5장에서는 제안 방식을 고찰하고 기존 방식과 비교 분석을 수행한다. 마지막으로 6장에서 결론을 제시한다.

## Ⅱ. ID 기반 공개키 암호 시스템

ID 기반 PKC(Public Key Cryptosystem)에서 모든 사람의 공개키는 사전에 이메일 주소와 같은 정보에 의해 결정된다. Shamir에 의해 제안된 이 개념은 원래 e-mail 시스템에서 인증 관리를 단순화하기 위한 것이었다.[6] Alice가 Bob에게 bob@hotmail.com으로 메일을 보낼 때 공개키 스트링 bob@hotmail.com을 사용하여 메시지를 암호화한다. Alice는 Bob의 공개키 인증서를 획득할 필요가 없다. Weil pairing은 타원곡선 이산대수 문제의 공격에 사용되어왔으며 3자 키 공유 시스템의 구성도 가능하다[7]. Weil pairing은 초특이 타원곡선 상에서 정의되는 쌍선형사상(bilinear map)이다. $G$가 유한체 $F_q$상에서 초특이 타원곡선 위의 점으로 이루어진 군(group)이라 하자. $G$의 위수(order)를 $l$로 표기하고, $l/q^k-1$을 만족하는 가장 작은 정수 $k$를 정의하자. 쌍선형 사상 $\hat{e}$는 다음과 같이 정의된다.

$$\hat{e}: G\times G \rightarrow F_{q^k}^*$$

이 때, 쌍선형 사상은 다음과 같은 성질을 만족한다.

- $\hat{e}(P_1+P_2, Q) = \hat{e}(P_1, Q)\cdot \hat{e}(P_2, Q)$
- $\hat{e}(P, Q_1+Q_2) = \hat{e}(P, Q_1)\cdot \hat{e}(P, Q_2)$
- $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, $a, b\in Z_q^*$

## Ⅲ. PayWord

PayWord 프로토콜은 해쉬 체인을 이용하여 전자화폐인 payword를 사용자가 직접 발행하는 것이 특징이다[2]. 고객은 브로커에게 신용카드 번호를 전송하여 인증서를 발급 받아 payword를 생성한다. 브로커가 서명한 인증서 $C_U$에는 브로커의 이름 $B$, 사용자의 이름 $U$, IP주소 $A_U$, 고객의 공개키 $PK_U$, 유효기간 $E$, 그리고 다른 기타 정보 $I_U$를 포함한다.

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

마지막 payword인 $w_n$을 임의로 정하고, $w_n$을 제외한 나머지 payword들은 $w_i = h(w_{i+1})$, $(i=n-1, n-2, \ldots, 0)$을 계산함으로써 체인을 생성한다. 사용자의 $i$번째 지불은 $(w_i, i)$로 구성되며 상인은 $w_{i-1}$을 사용한 해쉬 연산으로 유효성을 확인할 수 있다. 하루의 마지막에 상인은 각 사용자에게 받은 마지막 지불인 $P_l=(w_l, l)$과 이에 대응하는 위임 메시지를 함께 브로커에게 보낸다. 브로커는 $l$번의 해쉬 함수를 반복 수행하여 $w_l$을 확인한 후, 사용자의 계좌에서 $l$만큼의 금액을 청구하여 상인의 계좌로 지급한다. payword는 각 상인에 대한 고유한 payword를 사용하기 때문에 상인이 독립적으로 payword의 이중 사용, 위조, 변조를 검사할 수 있다는 장점이 있다. 그러나 PayWord 시스템은 몇 가지 결점을 가지고 있다[5].

- 사용자는 거래하고자 하는 상인마다 다른 해쉬 체인을 사용해야 한다. 그러므로 사용자의 측면에서, 상인의 수만큼 공개키 연산을 수행해야 한다.
- 사용자는 거래에 사용되었던 마지막 인덱스 값을 모두 저장해야 한다.

## Ⅳ. 새로운 ID기반 지불 프로토콜

본 논문에서는 ID기반 인증 모델을 적용하여 공개키 인증서가 필요 없으며, 타원곡선 암호 방식의 사용으로 연산 속도를 향상시킨다.

### 4.1 ID 기반 키 동의 프로토콜

브로커는 ID 기반 시스템에서 KGC 역할을 한다고 가정한다. 사용자는 브로커에게 자신의 인증서 암호화에 필요한 공개키 생성 요청을 위해 안전한 채널로 자신의 ID를 전송한다.

- $H': F_q^* \rightarrow \{0,1\}^*$: 키 유도 함수(key derivation function)
- $H: \{0,1\}^* \rightarrow G$ : 해쉬함수(hash function

표 1. 시스템 설정에 필요한 파라메터

| 데이터 요소 | 설 명 |
|---|---|
| $C, V, B$ | 사용자, 판매자, 브로커 |
| $Z$ | $Z \in C, V, B$ |
| $Z_{ID}$ | $Z$의 ID |
| $W_Z$ | $Z$의 공개키 |
| $w_Z$ | $Z$의 개인키 |
| $k_Z$ | $Z$의 세션키 |
| $C_Z$ | $Z$의 인증서 |

브로커는 비밀키 $s \in \{1, \ldots, l-1\}$와 난수 $p \in G$을 선택한 후, $P_B = [s]P$를 계산한다. 그리고 $(P, P_B)$는 공개한다. 사용자, 판매자, 그리고 브로커는 세션키를 공유하길 원한다고 정의한다. 사용자는 브로커에게 자신의 아이디를 보낸다. 브로커는 사용자의 공개키 $W_C = H(C_{ID})$를 생성하고 개인키 $w_C = [s]W_C$ 를 생성한다. 판매자의 공개키/개인키도 같은 방법으로 브로커에 의해 생성된다. 두 번째 거래부터 판매자의 인증서 대신 세션키 $k_{CVB}$ 를 사용하여 거래가 이루어진다. 사용자, 판매자, 브로커는 각각 개인키 역할을 하는 난수 $a, b, c \in Z_q^*$ 를 생성한다. 세션키 생성 프로토콜은 다음과 같다.

- $C \rightarrow V, B$: $[a]P_B$
- $V \rightarrow C, B$: $[b]P_B$
- $B \rightarrow C, V$: $[c]P_B$

사용자, 판매자, 그리고 브로커는 세션키를 계산한다.

$$k_C = \hat{e}(w_C, P) \cdot \hat{e}(W_V, [b]P_B) \cdot \hat{e}(W_B, [c]P_B) = \hat{e}([a]W_C + [b]W_V + [c]W_B, [s]P)$$

$$k_V = \hat{e}(W_C, [a]P_B) \cdot \hat{e}([b]w_V, P) \cdot \hat{e}(W_B, [c]P_B) = \hat{e}([a]W_C + [b]W_V + [c]W_B, [s]P)$$

$$k_B = \hat{e}(W_C, [a]P_B) \cdot \hat{e}(W_V, [b]P)) \cdot \hat{e}([c]w_B, P_B) = \hat{e}([a]W_C + [b]W_V + [c]W_B, [s]P)$$

따라서, 공통 세션키는 키유도함수(key derivation function) $H'$의 값이 된다.

$$k_{CVB} = \hat{e}([a]W_C + [b]W_V + [c]W_B, [s]P)$$

### 4.2 ID 기반 소액 지불 프로토콜

사용자가 $k$번째 판매자와 거래 하는 경우의 지불 프로토콜을 제안한다. 사용자는 인증서 획득을 위해 브로커와 미리 설정된 안전한 통신 채널을 통해 해쉬 체인의 root값 $w_0$, 해쉬 체인의 길이 $n$, 사용자의 아이디 $C_{ID}$, 브로커의 아이디 $B_{ID}$를 포함한 메시지를 브로커의 공개키로 암호화하여 전송한다.

$$C \rightarrow B: \; w_0, n, C_{ID}, B_{ID}{}_{W_B}$$

브로커는 받은 메시지를 개인키로 복호화한 후 해쉬 체인의 길이가 사용자의 계정에서 사용 가능한지를 체크한다. 해쉬 체인의 길이가 초과되지 않으면 브로커는 사용자에게 인증서를 발급한다.

$$B \rightarrow C: C_C = Sign_B w_0, n, C_{ID}, B_{ID}, E$$

또한, 판매자는 사용자에게 첫 거래시 영수증을 발급할 때 사용될 인증서를 브로커에게 받는다.

$$B \rightarrow V: C_V = Sign_B V_{ID}, B_{ID}, E$$

#### 4.2.1 $k$번째 판매자와의 지불 프로토콜

두 번째 거래부터는 판매자의 인증서 대신 $k_{CVB}$를 사용하여 인증한 후 거래가 이루어진다. 다음을 가정한다.

- 사용자는 해쉬 체인 길이 $n$을 갖는다.
- $(k-1)th$ 판매자는 인덱스 $i$를 갖는다.
- $k$번째 판매자는 인덱스 $j$를 갖는다.

1) 사용자는 판매자의 웹 사이트로부터 상품 구매 요청을 위해 아래와 같은 메시지를 전송한다.

$$C \rightarrow V_k: Product\ request$$
$$V_{k_{ID}}, C_{ID}, C_C, ProductID, Price, t, Sign_C(k_C)_{W_{V_k}}$$

2) 요청을 받은 판매자는 인증 후 상품을 보낸다. 대칭키 $K$로 암호화한 상품, 정당한 판매자의 신원을 위해 $k_{V_k}$에 자신의 전자 서명, 그리고 사용자에게 지불을 받기 위해 $Price$를 모두 암호화 하여 전송한다.

$$V_k \rightarrow C: Goods\ \nabla ivery\ [goods]_K$$
$$h[goods]_K,\ Sign_{V_k}(k_{V_k}),\ Price$$

3) 사용자는 판매자에게 payword 마지막 인덱스 $payment = (w_j, j)$를 해쉬 함수를 수행하여 지불 금액을 확인할 수 있도록 $w_{i+j}, j, n-i$ 와 $k_{V_{k-1}}$, 그리고 $(k-1)$번째 판매자와 거래 후 남은 해쉬 함수의 길이 $n-i$ 과 $k_{V_{k-1}}$에 서명한 메시지를 보낸다.

$$C \rightarrow V_k: payment = (w_j, j)$$
$$w_{i+j}, j, n-i, k_{V_{k-1}}, Sign_C h(k_{V_{k-1}}, n-i)_{W_{V_k}}$$

4) $V_k$는 자신의 개인키로 복호화한 후 $w_{i+j}$에 해쉬 함수를 $j$번 수행하여 $(k-1)$번째 판매자의 마지막 payword값 $(w_i, i)$와 같은지를 확인한다. 값이 일치하면 $V_k$는 사용자에게 다음 거래에 사용가능한 해쉬 체인의 길이 $n-i-j$, 마지막 payword값 $w_{i+j}$ ,상품 복호화키 $K$와 $k_{V_k}$의 메시지를 갖는 영수증을 보낸다.

$$V_k \rightarrow C: Receipt$$
$$K, n-i-j, w_{i+j}, k_{V_k}, Sign_{V_k} h(k_{V_k}, n-i-j)_{W_C}$$

5) 상품에 상응하는 값을 결제 받기 위해 브로커에게 $w_i, w_{i+j}, j, n-i-j$ 를 보낸다.

$$V_k \rightarrow B: Deposit\ Request$$
$$Sign_{V_k}(k_{V_k}, n-i-j), C_C, w_i, w_{i+j}, j_{W_B}$$

6) 사용할 수 있는 해쉬 체인의 길이 한도를 체크하여 판매자의 계좌로 결제 금액을 이체시킨다.

$$B \rightarrow V_k: Redemption$$

## V. 제안 방식 고찰 및 비교 분석

소액 지불 시스템에서는 화폐 단위가 낮은 반면 거래가 빈번하기 때문에 모바일 환경에서 지불 데이터를 전송할 때 알고리즘 연산량과 안전성에 대해 고려해야 한다.

### 5.1 안전성 분석

• 위조 방지

브로커는 사용자에게 payword를 생성할 수 있는 정당한 권한을 주기 위해 인증서에 자신의 서명한 메시지를 전송한다. 따라서, 인증서를 소유하고 있는 사용자만이 화폐 가치를 지닌 payword를 생성할 수 있다.

• 이중 지불 탐지

사용자는 거래를 시작하기 전에 브로커에게 root

값, 해쉬 체인 길이 등의 메시지를 포함한 인증서를 발급받는다. 판매자와 거래 후 결제 과정에서 판매자는 브로커에게 고객의 인증서, root값, *payment*를 포함한 메시지가 전달되기 때문에 payword를 이중으로 사용하면 브로커가 이를 탐지한다.

• 위장 공격 방지

세션키가 유출되어도 다른 개체가 공통의 세션키를 소유하고 있으므로 제3자가 위조된 세션키로 공격할 수 없다. 따라서 제안한 프로토콜은 위장 공격에 안전하다.

• Forward Secrecy

long term 비밀키의 분실 및 노출로 인하여 이전에 생성된 세션키가 공개된다면 forward secrecy에 취약하다. 제안한 프로토콜은 short term 키를 사용하여 세션키를 생성하기 때문에 forward secrecy에 안전하다.

표 2. 기존방식과 제안방식 비교 분석표

| 요구사항 \ 프로토콜 | PayWord 프로토콜 | 제안한 프로토콜 |
|---|---|---|
| 위조방지 | O | O |
| 이중지불탐지 | O | O |
| 위장공격방지 | X | O |
| Forward Secrecy | X | O |
| 공개키인증서 | 필 요 | 필요없음 |
| 키생성 알고리즘 | 공개키 암호 | ID 기반 공개키 암호 |
| 상품의 암/복호화 키 | DES | DES |
| $n$명의 판매자와 거래시 $C_i$의 사용 횟수 | $(n*2)-1$ | 1 |

O: 제공, X: 제공하지 않음

### 5.2 효율성 분석

기존 PayWord 프로토콜에서는 첫 거래에서 판매자의 인증서가 사용되고 두 번째 거래부터는 전 단계에서 사용된 판매자의 인증서와 거래하고자 하는 판매자의 인증서가 모두 사용되므로 $n$명의 판매자와 거래시 $C_i$의 사용 횟수는 $(n*2)-1$이고 제안한 프로토콜에서는 첫 거래에만 판매자의 인증서가 1회 사용된다. 또한 세션키의 생성은 ID 기반 공개키 암호 알고리즘을 적용했기 때문에 기존 프로토콜에서 공개키 암호 알고리즘을 적용했을 때보다 매우 안전성이 뛰어나고 효율적이다.

## VI. 결 론

본 논문에서는 기존에 제시되었던 PayWord 프로토콜의 문제점을 분석하여 새로운 프로토콜을 제시하였다. 제안한 프로토콜은 ID 기반 3자간의 키 동의 프로토콜을 적용하여 세션키의 분실이나 오용 등에 의해 발생하는 문제점을 해결할 수 있기 때문에 기존에 제안된 프로토콜에 비해 안전성이 매우 뛰어나다. 향후 스마트카드를 이용한 결제 과정에서 통신 횟수, 연산 속도와 계산량을 감소시켜 무선 PKI 환경에 적용한다면 위장 공격에 대한 안전성을 더욱 높일 수 있을 것이다.

## 참 고 문 헌


[1] Lyytinen, K., "M-commerce-mobile commerce: a new frontier for E-business," System Sciences, *Proceedings of the 34th Annual Hawaii International Conference*, pp. 3509-3509, 2001.

[2] R.L.Rivest, "PayWord and MicroMint: Two simple micropayment schemes", *CryptoBytes*, pp.7-11,1996.

[3] Steve Glassman, "The MilliCent Protocol for Inexpensive Electronic Commerce", *World Wide Web Journal*, 1(1), p.89, December 1995.

[4] Phillip M. Hallam-Baker, "Micre Payment Transfer Protocol(MPTP) Version 0.1", *W3C Working Draft*, 1995.

[5] R.Rivest, "The MD5 Message-Digest Algorithm," Internet RFC 1321, April 1992.

[6] Divya Nalla, and K.C. Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings, *Cryptology ePring* Archive, Report 2003/004, available at http://eprint.iacr.org/2003/004. 2002.

[7] N.P.Smart, "An Identity based authenticated Key Agreement Protocol based on the Weil pairing", Cryptology ePrint Archive, Report 2001/111,2001. http://eprint.iacr.org/.

이 현 주 (Hyun-Ju Lee) 준회원

1990년 2월 : 청주대학교 수학교육과 졸업(이학사)
1992년 2월 : 청주대학교 수학과 졸업(이학석사)
2000년 8월 : 청주대학교 수학과 졸업 (이학박사)
2003년 2월 : 충북대학교 대학원 컴퓨터과학과 박사과정 수료

<관심분야> 정보보안, 스마트카드, 전자지불

이 충 세(Chung-Sei Rhee) 정회원

1989년 : University of South Carolina, 전산학 박사
University of North Dakota 전산학과 조교수
1991년~현재 : 충북대학교 전기전자 및 컴퓨터공학부 교수

<관심분야> 결함허용, 알고리즘 및 전문가 시스템, 정보보안