무선 인터넷에서의 은익기반 서명에 의한 전자상거래*

김장환** · 이충세***

요 약

효율적이고 안전한 전자 지불시스템을 설계하는 것은 전자상거래에서 아주 중요하다. 본 논문에서는 ID를 기반으로 한 공개키 암호 시스템을 적용하여 다중 처리를 허용하는 효율적인 지불 시스템을 설계하였다. 제안한 지불 시스템은 유한체 Fq상에서의 타원곡선 암호 시스템을 사용하는 Weil-pairing 기법에 의해 생성된 인증키를 생성하는 과정을 이용한다. 따라서, 이 방법은 알려진 키 공격과 위장 공격에 대해 보다 안전하고 속도의 향상 및 안정성을 제공한다.

Blind Signature based on Mobile Commerce

Jang-Hwan Kim** · Chung-Sei Rhee***

ABSTRACT

Designing efficient and secure electronic payment is important for M-Commerce. In this paper, we propose an efficient Micro-payment protocol that allows multiple transactions using ID-based public key encryption-system. The proposed payword system requires to generate authenticated key generated by Weil-pairing which uses an elliptic curve cryptosystem over finite field Fq for transactions. Therefore, it is more secure in known key attacks as well as man-in-the middle attacks.

Key words : Blind Signature, Micro-payment, Known-key Attack, Man-in-the-middle-attacks

* This work was supported by the research grant of the Chungbuk National University in 2006.

** 성결대학교 공과대학

*** 충북대학교 컴퓨터과학과

1. Introduction

Mobile transaction is mainly used for micro-payment system. But in the future mobile communication can be also applied to micro payment system such as music files, MPEG, AVI and GIF etc. M-commerce payment protocols are Milli-cent, Payword, MicroMint, and MPTP[1]. Most Micro- payment protocol adopt strong one way hashing function such as MD5[2]. MD5 is much cheaper and faster than public key encryption operation. It is known that hashing function is 10,000 faster than RSA algorithm for message signing and 100 time faster in verification[3]. Therefore, Micro-payment system should be designed to minimize transaction time and public encryption algorithm usage. Current PayWord protocol recreates vendor's certificate for every n transactions and modify it periodically to nullify centralization problem. But it is not adequate for real time transactions. It is uncertain whether the authentication papers published by broker to user and vendor are mutually authenticated between user and vendor[4]. In this paper, we generate public/private key using ID of each entity to adjust M-commerce environment, then we use the session key by Weil-pairing from the second transaction to the last transaction. This reduces generation of authentication papers, therefore speed and centralization problems are improving. Since session keys are generated by customer, vendor and broker, works are shared among them and verification of mutual authentication between customer and vendor is possible. It is also safe from key masquerading and key attack.

2. Micro Payment System

Micro payment system is a special type of Electronic money system and developed mainly for small amount of payments. Micro payment system has an advantage of little system errors because payment size is small. MilliCent electronic Payment system was developed by DEC to handle small amount of payment which is hard to deal with credit card or other payment system. MilliCent protocol does not use encryption algorithm but it rather use message digest and minimize payment cost. But it shares the public key among transaction partner and check the effectiveness of Scrip. The publisher of scrip is responsible for the security issue.

PayWord protocol uses hash chain and customer issues electronic money directly[3].

Customer sends his(her) credit number to broker and get a certificate and creates own PayWord. The certificate (C_u) signed by broker contains broker name (B), user name (U), public key of user (PK_U), effective day (E) and other information (I_U). There are some other Micro-payment systems, such as MITLCS of Ron Rivest, MicroMint proposed by Adi Shamir and Wenbo Pay ment which is combination of PayWord and MPTP .

3. The proposed ID Key Agreement protocol

Broker takes the role of KGC in ID based system. Customer sends his(her) ID on the safe channel to request public key generation to encrypt the certified paper.

〈Table 1〉 Parameters for system setting

Parameters	Description
U, V, B	User, vendor, broker
Z	Z $\in$ {U, V, B}
Z_{ID}	z's ID
W_Z	z's public key
w_Z	z's private key
k_Z	z's session key
C_Z	z's certified paper
D_Z	z's adversary

- $H' : F^*_{qk} \rightarrow \{0, 1\}^*$: key derivation function
- $H : \{0, 1\}^* \rightarrow G$: Hash function

<Table 1> shows the parameters to generate public key/private key and session key. Broker selects a secret key $s \in \{1, \cdots, l-1\}$ and random number $p \in G$, then calculates $P_B = [s]P$. (P, P_B) which is used as a public key. Customer, vendor and broker are sharing session key. Customer sends his ID to broker. Broker creates customer's public key $(W_U = H(U_{ID})$ and private key $(w_U = [s]W_U)$. Vendor's public key/private key are created by broker in the same way. Session key (k_{UVB}) is used for transaction instead of vendor's authenticated paper for the rest of transactions. Customer, vendor and broker create short term random keys $a, b, c \in Z^*_q$, respectively. Session key generation protocol is given below.

- $U \rightarrow V : [a]P, [a]\ W_B\ ; U \rightarrow B : [a]P, [a]W_V$
- $V \rightarrow U : [b]P, [b]\ W_B\ ; V \rightarrow B : [b]P, [b]W_U$
- $B \rightarrow U : [c]P, [c]\ W_V\ ; B \rightarrow V : [c]P, [c]W_U$

Customer, vendor and broker calculate session key as given below.

$$k_U = \hat{e}([a](W_V + W_B), P_B) \cdot \hat{e}(W_U, ([b]P + [c]P)) \cdot \hat{e}([b](W_B, P_B) \cdot \hat{e}([c](W_V, P_B)$$

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

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

Therefore, common session key is used as a value of key derivation function.

$$k_{UVB} = k_U = k_v = k_B$$

$$= \hat{e}([a](W_V + W_B) + [b](W_U + W)_B + [c](\ W_U + W_V,\ [s]P)$$

Session key created by long-term secret keys is determined by three objects W_U, W_V, W_B, secret key of KGC and private keys a, b, c.

3.1 First Transaction Authentication

- Procedure to get the certificate paper is defined as follows.

Step 1 : User sends a message encrypted by broker's public key through the secure communication channel established earlier. Message contains root of hash chain ω_0, length of hash chain n, User's id U_{ID} and broker's id B_{ID}.

$$U \rightarrow B \;:\; \{w_0,\ n,\ U_{ID},\ B_{ID}\}_{w_s} \qquad (1)$$

step 2 : Broker decrypt the received message by private key and check whether he can use the length of hash chain in User's account. If length of hash chain are OK, broker issues certificate paper with effective period E.

$$B \rightarrow U : C_U = Sign_B\{\omega_0, n, U_{ID}, B_{ID}, E\} \tag{2}$$

Certificate paper signed by broker gives a right to create hash chain to the qualified user. User create hash chain for the following cases.

- The corresponding vendor spends all the hash chain.
- The effective period of certificate paper is expired.

Step 3 : When vender issues a transaction paper, he receives the certificate paper from the broker. Vender's certificate paper contains vender's ID, broker's ID and effective period.

$$B \rightarrow V : C_V = Sign_B\{V_{ID}, B_{ID}, E\} \tag{3}$$

- Procedure to request a commodity and payment is given as follows.

User searches internet and find the information of the commodity. The transaction between user and vendor must be done in predetermined time.

step 1 : User sends customer's ID, commodity's ID signed by vendor and user's ID to verify transaction.

$$U \rightarrow V : \Pr oduct\ request$$
$$\{V_{ID}, U_{ID}, C_U, \Pr oductID, \Pr ice, t, Sign_U(k_U)\}_{W_V} \tag{4}$$

step 2 : Vender checks the expiration day of the authenticated paper, then verifies root of hash chain and length of the hash chain.

Vendor encrypts the commodity by symmetric key and send it to the user signed value and price of commodity encrypted by user's public key.

$$V \rightarrow U : Goods\ Delivery$$
$$[goods]_K\{h[goods]_K, Sign_V(k_V), \Pr ice\}_{W_U} \tag{5}$$

step 3 : When user receives encrypted commodity, he send hash chains value and index to vendor for payment.

$$U \rightarrow V : Payment = (\omega_i, i) \tag{6}$$

step 4 : Vender calculates hash chain's length from the received message and compare it with root value. After check the payment amount, vender sends decoding key, remaining hash length and certified receipt to the user.

$$V \rightarrow U : \mathrm{Re}ceipt$$
$$\{K, n-i, C_V, m_i, Sign_V\{h(C_V, n-i)\}\}_{W_U} \tag{7}$$

step 5 : User verifies the remaining index of certified receipt then decrypt the commodity to receive it.

- Procedure to settlement is given as follows. Vendor issues a receipt and finish settlement with broker in a fixed time.

step 1 : Vendor requests a settlement to the broker with hash chain and signed session key created by vendor.

$$V \rightarrow B : Deposit\ request$$
$$\{C_U, k_V, \omega_i, i, Sign_V(k_V)\}_{W_B} \tag{8}$$

step 2 : Broker verifies length of hash chain of the user's authenticated paper. Broker check the value of hash chain, if root's value is same, deposit money into vendor's account.

$$B \rightarrow V : \mathrm{Re}\,demption \tag{9}$$

3.2 *kth* vendor Transaction Authentication

Payment to the *kth* vendor in the proposed protocol is performed as follows. From the second transaction, all the transactions are performed by k_{UVB} instead of authenticated paper. Assume the following to perform payment.

- User has the length of hash chain *n*.
- $(k-1)th$ vendor has the index *i*.
- *kth* vendor has index *j*.

step 1 : Commodity request step is similar to the transaction with first vendor.

$$U \rightarrow V_k : \mathrm{Pr}\,oduct\ request$$
$$\{V_{k_{ID}}, U_{ID}, C_U, \mathrm{Pr}\,oductID, \mathrm{Pr}\,ice, t, Sign_U(k_U)\}_{W_{V_k}} \tag{10}$$

step 2 : Vendor sends a commodity after authenticate the requested customer.

Commodity encrypted by symmetric key, vender's electronic signature and price are again encrypted by user's public key and send.

$$V_k \rightarrow U : Goods\ Delivery$$
$$[goods]_K \{h[goods], Sign_{V_K}(k_{Vk}), \mathrm{Pr}\,ice\}_{W_U} \tag{11}$$

step 3 : User decrypt the received message and verify the price of the requested commodity. Then user send the following message *payment* (ω_j, j), ω_{i+j}, j, $n-i$, $k_{V_{k-1}}$ to vendor.

At a same time, user send a signed message C_U, ω_{i+j}, j to broker to prevent forgery payment setting.

$$U \rightarrow V_k : payment = (\omega_i, i)$$
$$\{\omega_{i+j}, j, n-i, k_{V_{K-1}}, Sign_U\{h(k_{V_{K-1}}, n-i)\}, Sign_U\{h(C_U, \omega_{i+j}, j)\}\}_{W_{V_k}} \tag{12}$$

step 4 : V_k decrypt the received message from the user using private key, then apply hashing function ω_{i+j}, j times and check whether it is same as $(k-1)th$ vendor's password (ω_i, i). If it is correct, vendor sends the receipt containing commodity encryption key and vendor's key.

$$V_k \rightarrow U : \mathrm{Re}\,ceipt$$
$$\{K, n-i-j, \omega_{i+j}, k_{V_k}, Sign_{V_k}\{h(k_{V_k}, n-i-j)\}\}_{W_U} \tag{13}$$

step 5 : Vendor sends ω_i, ω_{i+j}, j and signed message $sign_u\{h(C_U, \omega_{i+j}, j)\}$ to broker to perform the transaction.

$$V_k \rightarrow B : Depositrequest$$
$$\{Sign_{V_k}(k_{V_k}, n-i-j), Sign_U\{h(C_U, \omega_{i+j}, j)\}, C_U, \omega_i, \omega_{i+j}, j\}_{W_B} \tag{14}$$

step 6 : Broker verifies C_U's certification and send a requested money to vendor's account.

Broker can verifies only from ω_i to ω_{i+j}.

Broker verifies whether the last payment is smaller than maximum until expiration time.

$$B \rightarrow V_k : \mathrm{Re}\,demption \tag{15}$$

4. Conclusion

In this paper, we proposed an efficient Micropayment protocol that allows multiple transactions using ID based public key cryptosystem. The proposed protocol has been developed using ID based public key and has an advantage against lost of session key, misuse and security. In the M-payment, payments are made on mobile terminals which is considered future generation payments tool. Smart card such as electronic money, ID card medical card and SIM card are impossible to copy, it gives a high quality of safety. Elliptic curve algorithm also gives a security and speed advantage compared to previous developed algorithms. Future works are application of ID based payment for general payment case.

References

[1] Steve Glassman, and Mark Manasse et al., "The MilliCent Protocol for Inexpensive Electronic Commerce", WWW journal, Vol. 1, No. 1, p. 89, 1995.

[2] R. Rivest, "The MD5 Message-Digest Algorihm", Internet RFC 1321, 1992.

[3] R. Rivest and A. Shamir, "PayWord and MicroMint : Two Simple Micropayment Schemes", CryptoBytes, pp. 7-11, 1996.

[4] M. H. Lee and K. G. Kim, "A Micro-payment System for Multiple-Shopping", SCIS 2002, Vol. 1/2, pp. 229-234, 2002.

김 장 환

1980년 서울대학교 경제학학사
1997년 한국과학기술원
(전산학 석사)
2003년 충북대학교(전산학박사)
1984년~1988년 쌍용정보통신 연구원
1988년~1993년 Qnix Data System 연구원
1993년~1998년 SK Telecom 중앙연구원 연구원
1998년~2005년 대덕대 교수
2005년~현재 성결대 공대 교수
관심분야 : Information Security, Mobile & Wireless Communication, Performance Analysis of Networks, Database System, Mobile Multimedia, Mobility Managements, Mobile Embedded System, Ubiquitous Computing, 알고리즘 및 계산이론, 결함허용, 정보통신 경제 예측

이 충 세

1979년 Univ. of South Carolina
컴퓨터과학과(석사)
1990년 Univ. of South Carolina
컴퓨터(과학과박사)
Univ. of North Dakota
전산학과 조교수
1991년~현재 충북대학교 컴퓨터과학과 교수
관심분야 : 결함허용, 알고리즘, 전문가시스템, 정보보안