모바일 데이터 망에서의 거래를 위한 효율적인 보안 프로토콜

김장환* · 이충세**

요 약

기존의 전자 거래 프로토콜이 사용하고 있는 암호화 알고리즘은 메모리와 처리 능력이 제한된 모바일 환경에 적합하지 않다. 본 논문에서는 모바일 내장형 시스템에 적합하도록 ID기반의 암호화 알고리즘과 타원 곡선 알고리즘을 사용하여 계산량과 수행 시간을 감소시켰다. 제안 프로토콜에서는 첫 거래에만 서비스 제공자의 인증서를 사용하며, 두 번째 거래부터는 타원 곡선 알고리즘을 적용하여 생성된 세션키로 인증한 후 거래를 하기 때문에 서비스 제공자의 인증서 생성 횟수는 n회에서 1회로 감소되었다. 또한 160비트로 RSA에서의 1024비트와 같은 안전성을 제공하기 때문에 수행 시간이 단축되었다.

An Efficient Security Protocol for Transaction in Mobile Data Network

Jang-Hwan Kim* · Chung-Sei Rhee**

ABSTRACT

The existing electronic transaction protocol uses a cryptography algorithm that is not suitable for mobile environment because of limited memory and process ability. In this paper, we propose an efficient transaction protocol suitable for mobile embedded system. The proposed protocol reduces computation and process time by using ID-based cryptography algorithm and ECC (elliptic curve cryptosystem). It uses vendor authentication only in the first transaction, and from the second transaction, it requires transaction after authentication with session key created by applying ECC technique. Therefore, the creation number of authentication for the vendor can be reduced from n to one. And it reduces process time because it provides the same security with 160 bits as with 1024 bits of RSA.

Key words : Security, Mobile Embedded System, ID-based, ECC

* 성결대학교 공과대학
** 충북대학교 컴퓨터과학과

1. Introduction

The secure information communication and fast increasing of mobile communication are the key factors of rapid growth of mobile commerces based on internet [1]. Currently, new M-commerces providing mobility as well as portability are replacing E-commerce which usually were done on the PC terminals. Researches on the secure authorization and transactions are actively performed to provide a security service on the E-commerce. Current PayWord protocol recreates vendor's certificate for every n transactions and modify it periodically to nullify centralization problem [2]. 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 [3]. 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. The paper is organized as follows. Section 2 gives the previous works. Section 3 review ID based public key encryption system. Section 4 describe the proposed ID based payment protocol. Section 5 analyze the safety and effectiveness of proposed payment protocol. Conclusions are given in Section 6.

2. Preliminaries

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 [4].

PayWord protocol uses hash chain and customer issues electronic money directly [2, 5].

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 [2, 6, 7].

3. ID based public key cryptosytem and Weil Pairing

3.1 ID based public cryptosystem

The original PKC (Public Key Cryptosystem) is very expensive to build a infrastructure which controls public key authorization as well as key management.

But ID based PKC solves this kind of pro-

blems. In ID based PKC, all the keys are determined by E-mail address in advance.

This method was proposed by Shamir and it's main purpose was to simplify the authentication procedure in E-mail [8].

3.2 Weil Pairing

Let G be a subgroup of the group of points on the Elliptic curve E over the finite field F_q. Then, it satisfies the following properties.

1. Bilinear
   $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q) \cdot \hat{e}(P_2, Q)$
   $\hat{e}(P, Q_1 + Q_2) = \hat{e}(P, Q_1) \cdot \hat{e}(P, Q_2)$
   $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, $a,b \in Z^*_q$
2. Non-Degenerate
   There exists such that $P \in G$
3. Computable :
   One can compute $\hat{e}(P, Q)$ in polynomial time.

4. The proposed ID based payment protocol

The proposed protocol generates public/private key using each object's ID, it does not need public key authentication. In the proposed protocol, Session key is generated by Weil Pairing based on Elliptic Curve Cryptosystem in a finite field of F_q and Id based tripartite Authentication key agreement protocol is applied to the existing Micro-Payment Protocol and ID based cryptosystem. Our system gives better result in speed and security compared to previous works. The following shows the upgraded contents of the proposed ID based payment protocol.

- Create public key/private key using object's ID.
- Create session key using Weil Pairing based on ECC
- Increase safety by applying ID based public key algorithm

4.1 System setting

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

4.1.1 Safety of session key

Session key generated by tripartite key agreement protocol gives the following safety [8].

- Forward secrecy : Even if long term key(s) is known, previous used session key is unknown.
- Key independence : Since adversary who knows group A's key can't find group B's key, it provides key independence.
- Key freshness : adversary may reuse old key, but newly generated key provides freshness.
- Known key attacks

4.2 ID based micro payment protocol

The payment protocol for the first and kth transaction between customer and vendor is proposed.

4.2.1 First vendor and payment protocol

- 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}.

$$U \rightarrow B: \{\omega_0, n, U_{ID}, B_{ID}\}_{w_s} \quad (1)$$

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.

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

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.

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

- 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.

$$U \rightarrow V : \text{Product request}$$
$$\{V_{ID}, U_{UD}, C_U, \text{ProductID}, \text{Price}, t, Sign_U(k_U)\}_{W_V} \quad (4)$$

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.

$$V \rightarrow U : Goods\ Delivery$$
$$[goods]_K\{h[goods]_K, Sign_V(k_V), \text{Price}\}_{W_U} \quad (5)$$

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

$$U \rightarrow V : Payment = (\omega_i, i) \quad (6)$$

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.

$$V \rightarrow U : \text{Receipt}$$
$$\{K, n-i, C_V, m_i, Sign_V\{h(C_V, n-i)\}\}_{W_U} \quad (7)$$

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.

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

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.

$$B \rightarrow V : \text{Redemption} \quad (9)$$

4.2.2 Payment protocol for the vendor

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.

$$U \rightarrow V_k : \text{Product request}$$
$$\{V_{k_{ID}}, U_{ID}, C_U, \text{ProductID}, \text{Price}, t, Sign_U(k_U)\}_{W_{V_k}} \quad (10)$$

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.

$$V_k \rightarrow U : Goods\ Delivery$$
$$[goods]_K \{h[goods], Sign_{V_K}(k_{Vk}), \text{Price}\}_{W_U} \quad (11)$$

step 3 : User decrypt the received message and verify the price of the requested commodity. Then user send the following message $payment\ (\omega_j, j), \omega_{i+j}, j, n-i, k_{V_{k-1}}$ to vendor.
At a same time, user send a signed message C_U, ω_{i+j}, j to broker to prevent forgery payment setting.

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

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.

$$V_k \rightarrow U : \text{Receipt}$$
$$\{K, n-i-j, \omega_{i+j}, k_{V_k}, Sign_{V_k}\{h(k_{V_k}, n-i-j)\}\}_{W_U} \quad (13)$$

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

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

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.

$$B \rightarrow V_k : \text{Redemption} \quad (15)$$

5. Analysis of Safety and effectiveness

In this chapter, we consider execution time and safety of the proposed protocol. <Table 2> and <Table 3> is given as a comparison between existing method and the proposed method.

5.1 Analysis of safety

- Prevent forgery

Broker sends a certificate signed by his private key, only the user C_U can create the password for the usable money. Therefore, other can't forgery electronic payment. If vendor masquerade settlement information and send payment information to broker, he must know the information of equation (14). But it is not possible.

- Detection of user's double payment

User sends equation (10) to the vendor for commodity order. The request form contains user's certificate C_U, hash chain's length and value of root. After received from the user, ven-

dor perform equation (12) to give a payment of $payment = (\omega_{i+j}, i+j)$. Vendor verifies whether the previous root's value ω_i and the value of ω_{i+j} after appling hashing function j times to ω_{i+j}. If $\omega_{i+j-1} = h(\omega_{i+j})$ equals (ω_i, i) then vendor detects double payment before vendor receive double payment. If user sends same payment to kth and $(k+1)th$ vendor, broker can detects it.

- Detection of vendor's double payment

Two payments are made by user using equation (10), broker use the equation (15) to detect it from the transaction on the bank.

Consider the case vendor request double payment. If the vendor masquerade U and pay to other vendor, then masquerade U' use the equation (10)

$$\{V_{k_{ID}}, U_{ID}, C_U, \mathrm{Pr}oductID, \mathrm{Pr}ice, t, Sign_U(k_U)\}_{W_k}$$

for double payment. But bank keeps previous transaction record such as hash chain's root, therefore broker can detect it.

- Prevent overpayment

User's certificate issued by broker holds the size of hash chain and payment information. Vendor can checks the limit of hash chain and payment information.

- Prevent masquerade

Assume adversary eavesdrop the communication between U and V, B. We also assume that δ, δ', δ'' are random numbers generated by D_U, D_V and D_B respectively. The following short-term secret keys are used for protocol and U creates communication for transaction.

- $U \rightarrow V, B : [a]P$
- $V \rightarrow U, B : [b]P$
- $B \rightarrow V, U : [c]P$

Assume masquerade makes the following operations.

1. $D_{V,B}$ eavesdrops aP from U and D_U sends δP to V, B.
2. D_U eavesdrops bP from V and D_V sends $\delta' P$ to U.
3. D_U eavesdrops cP from B and D_B sends $\delta'' P$ to U.

In this protocol, since session key generation protocol use long-term secret keys for k_{UVB} calculation, it is safe to the above masquerade.

- Prevent known key attack

If adversary eavesdrop the previous session key and he is able to masquerade next session key, it is vulnerable to known key attacks. Since the proposed protocol applied long-term secret key, it is almost impossible for the adversary to calculate session for the next transaction. <Table 2> shows the comparison among the systems.

〈Table 2〉 Comparison of safety

(O : offer, X : non-offer)

requirement protocol	PayWord protocol	Proposed protocol
Prevent forgery	O	O
Detection of double payment	O	O
Prevent overpayment	O	O
Mutual agreement	O	O
Prevent masquerade	×	O
Prevent known-key-attack	×	O

5.2 Analysis of effectiveness

In this paper, ID based cryptosystem was proposed to handle wireless environment. ID based cryptosystem does not require public key certification, but PKI requires it.

Elliptic curve cryptosystem over finite field is easy to apply to portable system and 160 bits on elliptic curve is comparable to 1,024 bits on RSA. Furthermore, most operations are scalar multiplication.

<Table 3> shows the number generation of certification paper. Most protocol generates certification papers for each transaction.

Therefore it generates n C_V when it have transaction with n vendors. But ID based protocol generates certification only one time when it has a transaction with first vendor. Session key generation is also much safer and effective compared to most protocol.

〈Table 3〉 Comparison of effectiveness of algorithms

	PayWord protocol	The Proposed ID Based protocol
The number of C_V generation for transaction with n vendors	n	1
Key generation algorithm	Public-key encryption	ID-based public-key encryption
Commodity encryption/decryption algorithm	DES	DES

6. Conclusion

In the mobile 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 is impossible to copy, it gives a high quality of safety. The existing electronic transaction protocol uses a cryptography algorithm that is not suitable for mobile environment because of limited memory and process ability.

In this paper, we propose an efficient transaction protocol suitable for mobile environment that allows multiple transactions using ID based public key cryptosystem. The proposed protocol has an advantage against lost of session key, misuse and security. When adversary taps transaction details and tries to attack by forge, the proposed protocol provides security against man-in-the-middle attacks by using secret key creation protocol when calculating long-term secret key. Furthermore, it reduces computation by using ID-based cryptography algorithm and ECC. It uses vendor authentication only in the first transaction, and from the second transaction, it requires transaction after authentication with session key created by applying ECC technique. Therefore, the creation number of authentication for the vendor can be reduced from n to one. The total number of PayWord is n because user creates n hash chain value only once for N vendor. So the proposed protocol is more convenient compared to existing system. It does not need public key authentication because it uses ID-based cryptography algorithm. And it reduces process time because it provides the same security with 160 bits as with 1024 bits of RSA. Elliptic curve algorithm also gives a security and speed advantage compared to previous developed algorithms.

References

[1] K. Lyytinen, "M-commerce - Mobile Commerce : A New Frontier for E-business", Proc of the 34th Hawaii International Conference on System Sciences, p. 3509, 2001.

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

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

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

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

[6] P. Hallam-Baker, "Micro Payment Transfer Protocol(MPTP) Version 0.1", W3C Working Draft, 1995.

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

[8] D. Boneh and D. Franklin, "Identity-Based Encryption from the Weil Pairing", Proc. of Crypto '01 LNCS, Vol. 2139, pp. 213-229, 2001.

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 과학과 박사
Univ. of North Dakota 전산학과 조교수
1991년~현재 충북대학교 컴퓨터과학과 교수
관심분야 : 결함허용, 알고리즘, 전문가시스템, 정보보안