A Simple Micro-payment Scheme *

Min-Shiang Hwang Iuon-Chang Lin Li-Hua Li

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, TAIWAN 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-3742337

October 31, 2012

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-006.

A Simple Micro-payment Scheme

Abstract

The micro-payment system is an important technique in electronic commerce. The high-value payment system is not suitable for a micro-payment system because the requirements are different. To meet sufficient security for all participants in electronic commerce, a micro-payment system makes it possible to make small payment through electronic communication networks. In this paper, we propose a simple and secure micro-payment system which can be used for purchasing information goods on the network. The new micro-payment system is developed using a tamper resistant device (i.e. smart card), an efficient Message Authentication Code (MAC) technique, and the concept of overall network security. In our proposed scheme, we achieve the authentication of the legal users, protection of the integrity of transaction messages, and prevention of duplicate spending. This new micro-payment system is a simple, efficient and economical system.

Keywords: Electronic commerce, Micro-payment, Network security, Smart card.

1 Introduction

Today, the Internet revolution is advancing rapidly, and commercial interests abound. Electronic commerce is a new business circumstance on the open network. In ideal electronic commerce, we desire that all of the steps of a transaction can be performed over the network. In an open network, information can be intercepted and tampered easily. Hence, how to build a secure and efficient environment for electronic payment is a key issue in electronic commerce development. There exist many payment systems that are based upon various cryptographic systems or models. The common purpose of these systems is the delivery information goods and payment from a payer to a payee.

A micro-payment system is a special kind of electronic payment system, which is used to buy information goods over the computer network. The important factors in such a payment system are small amounts of payment value (e.g. less than one dollar or few cents) and high frequency of transactions on the electronic commerce network. In network business transactions, a customer uses a WWW browser to buy data, software, game, music, news, or other services, and transfers these information(services) on-line through electronic communication networks. For small amount of payment, the systems do not require high transaction security since the systems have to reduce the cost of transaction. However, some security requirements are essential such as authentication of the customer and merchant, protect the integrity of transaction messages, and gain non-repudiation of transaction processes. In general, a practical system has three main properties in transaction: (1) customers get information goods in real time, (2) the prices of information goods are small, and (3) the transactions occur frequently.

Due to these properties, a good micro-payment systems must not only perform the transactions accurately but also meet the following requirements:

1. Good efficiency: the payment actions must be managed quickly and information goods delivered on line.
2. Low cost: The transaction cost must lower than the value of the payment.
3. Security: the identity of the users (customers or merchants) and the integrity of the transaction messages must be authenticated and protected.

In order to satisfy these requirements, micro-payment systems often use efficient cryptographic techniques to ensure the security of transaction. The one-way hash function is a useful technique to provide authenticity. The hash function can take an arbitrary-length input and return a fixed-length output. Furthermore, it can create one way and collision-resistance result (Damgard, 1990; Merkle, 1990-1; Merkle, 1990-1). The feature of one-way hash function is summarized as follows.

- Given an input, it is easy to compute the output through the function.
- Obtained an output, it is difficult to derive the input.
- Given an input, it is difficult to find another input, such that the two inputs have the same output.

The *Message Authentication Code (MAC)* (Davies, 1985; Schneier, 1996) is a special one-way hash function. It has the same properties as the one-way hash function, but it is augmented with a key to avoid someone forge the hash value. In addition, owner who owns the key can verify the hash value. The MAC is an efficient cryptographic technique to achieve integrity and authentication with lower operation costs. Hence, he technique is suitable for micro-payment systems.

The micro-payment systems must also provide non-repudiation proof in case of disputes. This is to avoid legal users being denied services. Furthermore, the systems must prevent the forgery of transaction message and ensure the integrity of messages. Because transaction message can be duplicated easily and bank must prevent users from double spending.

In this paper, we propose a simple micro-payment system using smart card. Smart cards are mobile device and can be trusted by its owner because smart card has computation, storage, and tamper resistant characteristics (Anderson and Kuhn, 1996; Hendry, 1997; Naccache and M'Raihi, 1996; Stirland, 1998):

1. Computation: a CPU is embedded into a smart card to process data

and execute cryptographic algorithms such as DES (NIS and NIST FIPS PUB 46-2 Technology, 1993) or RSA (Rivest, Shamir, and Adleman, 1978).

2. Storage: each smart card contains three kinds of memory: RAM, ROM and EEPROM which stores operating system designed for smart card, processed data, and permanent data (i.e. user's secret key) respectively.

3. Tamper resistance: the smart card is a tamper-proof device because the permanent data was stored in the card modified only by the issuer. Nobody can duplicate or compromise the permanent data.

From other respect, user authentication can be performed by the cardholder, i.e. card owner input Personal Identification Number (PIN) to authenticate himself (Vincent and Anthony, 1998). It is therefore concluded that smart card is suitable for electronic commerce (Dhem, Veithen, and Quisquater, 1996; Stirland, 1998). Therefore we use smart card, the MAC technique, and the information security concept to develop an efficient, low cost, and secure micro-payment system.

This paper is organized as follows. In the next section, we briefly discuss some macro-payment systems and explain why they are not suitable for micro-payment. Related works on micro-payment schemes are also discussed. In Section 3, we present the proposed simple micro-payment system. In Section 4, we present security analysis of the proposed method. In Section 5, the performance of our scheme is examined. Our scheme is compared with previous off-line based methods. Finally, the conclusions of the proposed micro-payment system is made.

2 Related Works

Many electronic payment systems have been developed. In general, electronic payment systems are classified into macro-payments and micro-payments by the amounts of payment value (O'Mahony, Peirce, and Tewari, 1997). Different payment systems handle different payment values due to security requirements placed upon each system are varied.

Macro-payment

For macro-payment systems, systems are classified into three types of models based on how the payments are implemented, that are credit card based, digital cash, and electronic check (account based). In the following, we will briefly discuss payment systems based on three models.

Credit card based payment systems, such as SET (MasterCard and Visa, 1997-1; MasterCard and Visa, 1997-2), and iKP (Bellare et al, 1995), are both on-line and post-paid payment by credit card. The SET (Secure Electronic Transaction) protocol (MasterCard and Visa, 1997-1; MasterCard and Visa, 1997-2) is proposed by MasterCard and Visa. The SET protocol is implemented into a credit card using public key cryptography (e.g. RSA system) and partly symmetric encryption (e.g. DES system) techniques. It is designed on CA-based (Certification Authority) security system. The SET protocol requires that the Acquirer Payment Gateway (APG) authenticate a credit card holder is legitimate and verify the payment instruction is correct. It achieves integrity, authentication and confidentiality through symmetrical encryption and digital signature. However, SET protocol is not suitable for micro-payment since the cost for each transaction is higher than the value of payment.

The iKP protocol (Bellare et al, 1995) was proposed by IBM Research Labs. It is also a macro-payment system based on credit card transactions over the Internet. This protocol uses public-key cryptography and applies

CA-based security. Specially, iKP can be implemented on different security levels. According to the security requirements, users can choose a suite level to implement.

Nowadays, there are many payment systems based upon cash-like payment, such as *ECash* (Wayner, 1994), and $CAFE$ (Boly et. al., 1994). ECash is the first concept of this type which was proposed by David Chaum. The protocol is applied to on-line and pre-paid payment system. It contains properties of anonymity and un-traceable which provide privacy of the customer based upon a blind signature (Chaum, 1983; Chaum, Fiat, AND, Naor, 1990; Chaum and Pedersen, 1993). The process of this concept is as follows. First, customers must install a special software called Electronic Wallet (Wayner, 1994) and deposit amounts of money in the Ecash bank. Then, customers replace the money with digital coins and store them in his electronic wallet. The digital cash does not link the relationship with customer even when the customer uses it for shopping. The merchant checks only the digit cash to see if it is minted by the Ecash bank and the bank does not determine who spent the digital cash either.

CAFE (Conditional Access for Europe) (Boly et. al., 1994) was proposed by ESPRIT which uses the blind signature technique for payments. Different from ECash which checks the double spending problem on-line, CAFE checks the double spending problem off-line by using smart card. It is a prepaid and off-line payment system. The user holds tamper resistant electronic wallet device and merchants use POS (Point-Of-Sale) terminals to check the payments from the electronic wallet. In Digital Cash payment systems, the bank must withdraw money from the customer's account, which is a pre-paid payment system. However, the pre-paid payment system requires user first deposit a sufficient amount of money into his account and, for each transaction, the bank checks the account to see if it's sufficient enough for payment.

$FSTC$ (Financial Services Technology Consortium) (Doggest, 1995) and $Netcheque$ (Neumann and Medvinsky, 1995) are famous electronic check models. In electronic check model, customer must have a legitimate account and permit funds to be transferred between accounts. FSTC used symmetrical key cryptography techniques and tamper-resistant signature cards to authenticate the legitimacy of electronic check. The Netcheque payment system based on the Kerberos' method (Schneier, 1996), was developed at the University of Southern California. It employs an account sever to transfer and authenticate electronic checks.

The foregoing payment systems cause computation and communication overhead to perform the protocol. Nevertheless they provide high level security. However, these methods are not suitable for micro-payment because the cost for each transaction may higher than the value of payment.

Micro-payment

Two types of model are classified for the micro-payment systems which are the notational model and the token model (Ferreira and Dahab, 1998). In the notational model payment systems, users transfer the payment message enabling the value of the payment and the payment orders. Some of such systems are $Millicent$ (Manassee, 1995), $MicroiKP$ (Hauser, Steiner, and Waidner, 1996), $NetBill$ (Sirbu and Tygar, 1995-1; Sirbu and Tygar, 1995-2), and SVP (Stern and Vaudenay, 1997). In the token model payment systems, transaction mainly exchanges tokens. The token represents coins or bank notes. The $PayWord$ and $MicroMint$ (Rivest and Shamir, 1997) are such type payment systems.

Millicent (Manassee, 1995) was proposed in Digital Equipment Corporation. In this protocol, the payment message is called *Scrip*. To verify the Scrip, it is efficient using symmetric encryption. However, the Scrip is vendor specific. First, customers must buy the broker Scrip form broker by using macro-payment protocol. When customers want to purchase something at certain vendor site, customers must take the broker Scrip to change the specific vendor Scrip from the broker. The vendor Scrip can only be used at specific vendor site.

In 1996, IBM aimed at micro-payments and proposed a new Micro-iKP protocol (Hauser, Steiner, and Waidner, 1996). It is an on-line micro-payment with credit card. This protocol is suitable for frequent transactions. Customers use "coupon" generated by a simple one way hash function in the transaction. Customers pay the "coupon" to the merchant, then, the merchant sends an authentication request to acquire bank approval. The bank then checks the authenticity of the "coupon" on-line. Obviously, in this scheme, the communication cost is increasing.

NetBill (Sirbu and Tygar, 1995-1; Sirbu and Tygar, 1995-2) is a low transaction costs micro-payment technique proposed in Carnegie Mellon University. It is a post-paid and account based model. The NetBill transaction process consists of three mail phases: price request phase, goods delivery phase, and payment phase. The system provides for the anonymity of the customer and uses a NetBill server which stores the accounts of customers and merchants. When information goods transferred form a merchant's server to the customer, NetBill debits the customer's account and credits the merchant's account according to the payment values.

SVP (Small Value Payment) (Stern and Vaudenay, 1997) is designed by J. Stern and S. Vaudenay. It uses a message authentication code function and a special device, such as smart card, to verify the validity of payment message. Each merchant has a smart card which issued by the broker. The smart card stored the broker's secret key to verify the identity of customer. However, this protocol needs many communications between customer and merchant. The smart card must generate a random number which sends to the customer, and waits a response from the customer in each transaction. This is not suitable for frequent transaction. Because other transactions must wait the processing transaction is completed.

The PayWord and MicroMint are the token based payment systems which designed by Ron Rivest and Adi Shamir. PayWord uses chains of hash value and each hash value called *payword*. Each payword can be represented as a specific value and each payword has the same value in the same chain. Customers obtain a certificate issued by the broker. The certificate allows the legal customers to generate paywords. To verify the payword, vendor only uses hash function and a signed *commitment* to honor payments of that chain. MicroMint uses k-way hash function collisions to mint coins. MicroMint coins have lower security but provides higher speed. Customer generates coins efficiently and vendor verifies these coins off-line.

The introduced micro-payment systems are efficient for repeated small payments. In order to achieve good efficiency and low transaction costs, a practical micro-payment system without any additional communication and expensive public key cryptography. Sometimes, they requires to establish a trusted party (e.g. broker or intermediary) to speed up the transaction process to satisfy the requirements of micro-payment.

3 The Proposed Scheme

The new payment scheme to be described in this section is limited for information goods or services on the Internet. Our scheme based on the concept of SVP method (Stern and Vaudenay, 1997). Unlike other proposed pre-paid micro-payment systems, merchant uses a tamper resistant device (e.g. smart

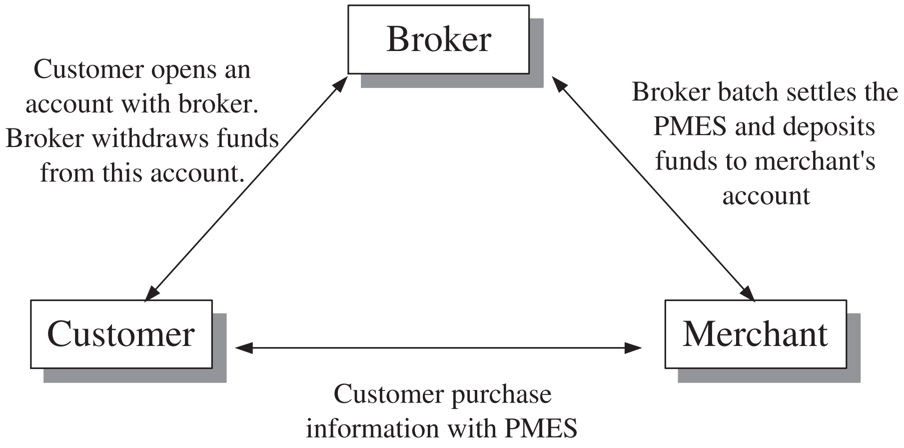

Figure 1: The new micro-payment protocol architecture

card) which is issued by a bank for authenticating payment messages sent by customers and verifying the legality of on-line payment messages. This system makes transactions to be completed on-line possible. Virtually, the bank is not involved in the payment process. Thus, the payment process will be more efficient and the cost per payment reduced.

The proposed micro-payment scheme consists of three entities: customer, merchant (or service providers) and broker (e.g. bank). The architecture of the micro-payment process is illustrated in Figure 1.

The broker is a trusted party, which function like a bank and a Certifying Authority (CA). It issues all kinds of identity numbers and securely archives these identity numbers. Furthermore, each customer's secret key K_C is created using the broker's secret key K_B. The merchant holds a smart card, which is issued by the broker and enables the merchant to use the smart card in the merchant's electronic point-of-sale device. The device ables to check the payment message sent by the customer using the broker's secret key hidden in the smart card. The integrated circuit chip of the smart card allows the protection of the information stored in secret area in the card from duplication or leak (Jones, Watson, and O'Neill, 1998). The merchant also establishes a database system, which stores each authentic payment message for checking double spending. Before proceeding to our scheme protocol, following notations should be introduced first.

- $MAC(k, M)$: Message Authentication Code function is a key-dependent one way hash function. The inputs of this function are a message M and a key k, and the output is a message digest.
- ID_C/ID_M: Each customer / merchant's identity.
- K_B/K_C: The broker / customer's secret key, where $K_C = MAC(K_B, ID_C)$.
- $AMOUNT$: The amount of money of each payment.
- SUM: The sum of money of all payments in the merchant. This information is stored in the smart card and is update with each purchase. Only the broker can clear this information.
- PO: The purchase order information, e.g. e-mail address and the ordered information goods.
- SER: An automatically increasing time serial number, which is like a time-stamp. The combination can be as ($year\|$ $month\|$ $date\|$ $times$), and it is generated by the customer.
- $PMES$: The payment message that contains, at a minimum, $\{ID_C$, $AMOUNT$, PO, SER, $H\}$. H expresses the $MAC(K_C$, $ID_C\|ID_M$ $\|AMOUNT$ $\|PO$ $\|SER)$ where the symbol $\|$ denotes the concatenation.

The detail process of micro-payment scheme is described as follows.

1. *Initiation:* A customer must open an account with the broker and register his personal information. Then, the broker delivers the customer's secret key K_C in secure manner, and issues an identity ID_C for the customer. Every merchant must also register and open an account with

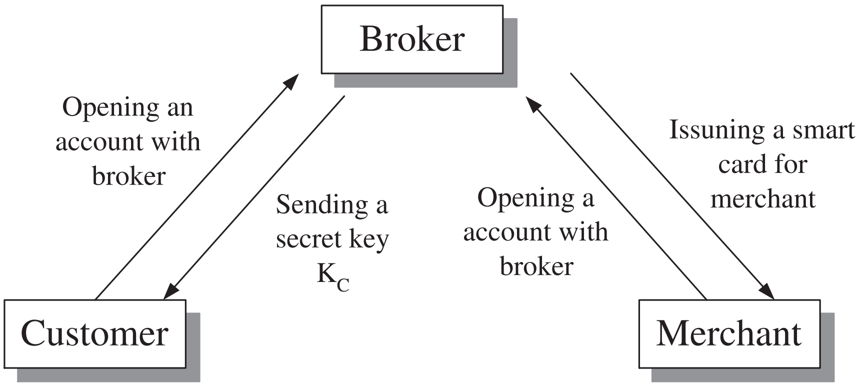

Figure 2: The initially phase of the new micro-payment protocol

the broker. Each merchant obtains an identity ID_M and a smart card issued by the broker. The smart card is a tamper-proof device, i.e. the secret information stored in the card cannot be tampered (Dhem, Veithen, and Quisquater, 1996; Stirland, 1998). The parameter of broker's secret key K_B and the merchant's identity ID_M are stored in a register of the CPU embedded in the card. The K_B and ID_M are used for internal computation and they can not be read or tampered. No one can hack the smart card to obtain the broker's secret key. Furthermore, the parameters of SUM, and the merchant's identity ID_M are also stored in the $EEPROM$ of the card which can not be tampered or cleared by any user except the broker. The MAC algorithm is hid in the ROM of the card. Figure 2 shows the initiation phase of this protocol.

2. *Payments:* When a customer purchase, he sends a $PMES$, i.e. $\{ID_C$, $AMOUNT$, PO, SER, $H\}$, to the merchant.

3. *Authentication:* After received $PMES$, the merchant checks if the payment is different from the customer's last payment which recorded in merchant's database. Then, the merchant forwards the payment message $PMES$ to his point-of-sale device. This device is a terminal that can read smart card. The smart card will authenticate the payment message and acknowledge the customer the outcome of his transaction

real time. The authentication processes of smart card are describes as follows.

First, the device generates a SER' to checks the SER of the processed transaction. If the time interval between SER and SER' is smaller than ΔSER, the smart card accepts the payment request. Otherwise, the smart card rejects the payment request. The ΔSER denotes the expected legal time interval for transaction delay between the terminal and the customer. Once pass the SER checking, the smart card authenticate the payment message $PMES$ to ensure it is not altered if the following equation is hold,

$$\begin{aligned}
& MAC(MAC(K_B, ID_C), ID_C \| ID_M \| AMOUNT \| PO \| SER) \\
= \; & MAC(K_C, ID_C \| ID_M \| AMOUNT \| PO \| SER) \\
= \; & H. \qquad (1)
\end{aligned}$$

where the broker's secret key was stored in the merchant's smart card and obtains the information, ID_c, ID_M, $AMOUNT$, PO and SER from the message $PMES$. If the authentication is hold, the smart card adds the $AMOUNT$ into SUM and stores the SUM in the smart card. At the end, the smart card sends an acceptance message to the merchant. During the authentication process, the smart card does not reveal any secret information.

If the PMES is responded valid, then the merchant transfers the information goods to the customer. In addition, the merchant records the $PMES$ into database system. If the authentication is responded incorrect, then the merchant ignores this transaction and sends a rejection message to the customer.

The payment and the authentication processes are shown in Figure 3.

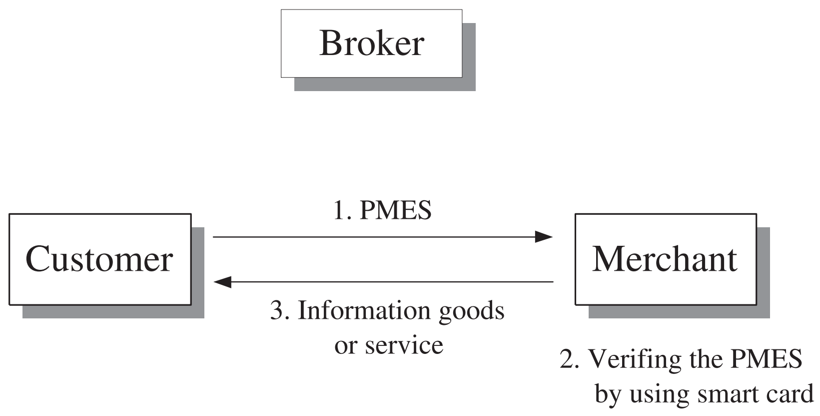

Figure 3: The payment and authentication phases

4. *Batch settlement for merchant:* This phase is handled off-line and does not perform frequently since the accumulated SUM for all transactions in the merchant, is stored in the smart card. The merchant takes the smart card to be batch settled. The merchant also transfers each payment message to the broker through an authentication channel. The broker then checks the all payments are different and authenticate each PMES using the Equation 1. After authentication, the broker totals each payment to see if it equals to the SUM. If the verification is hold, the broker deposits the money of SUM in the merchant's account and the payments messages are stored in the broker's database system. If the verification fails, the broker ignores this transaction and sends a rejection message to the merchant. After settling the account, the SUM should be cleared by the broker and all PMESs stored in merchant's database can be cleared. The batch settlement process is similar to SVP scheme (Stern and Vaudenay, 1997). This technique can prevent the database from unlimited growing because the database will be cleared regularly by the broker.

5. *Settling for customer:* Each customer may purchase in different merchant, but all PMESs of specific customer are stored in broker's database system. The broker's database can total the payments for each customer.

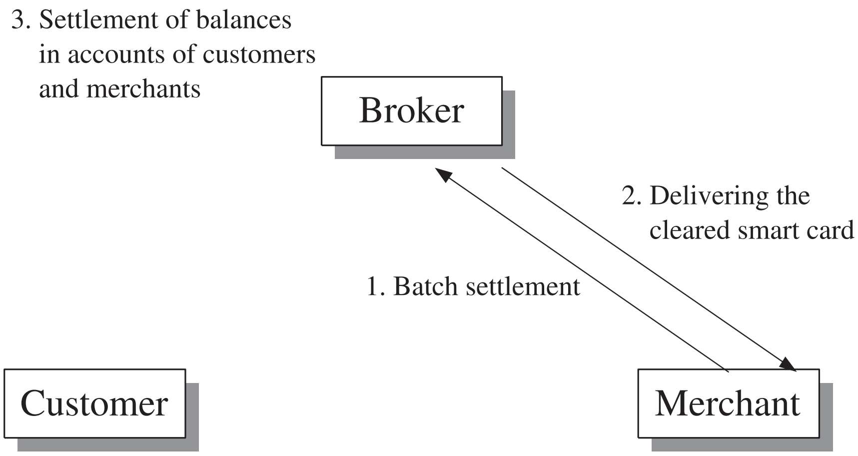

Figure 4: The settlement of merchant and customer

Broker withdraws money from the customer's account once a period of time. Furthermore, if the customer requires transaction report, broker can send a detailed list of every transaction to the customer. Figure 4 shown the settlement phase of this protocol.

During the payment process, the merchant can directly verify the payment message, without transferring the message to the broker. Furthermore, the broker pays the sum of all transaction values and charges each customer the total of his individual payment values possibly with various merchants. Thus, the transaction can be completed efficiently and the customer can get information goods quickly.

An essential property of micro-payment system is its small amount of product value. The Message Authentication Code cryptographic technique is suitable for use in micro-payment system with low operating costs per payment because the speed of compute the message digest is quicker than encrypting message. This results efficient authentication but less confidential. However, micro-payment systems do not require high security, due to the small value payment.

4 Security Analysis

In this section we will demonstrate the security of the proposed micro-payment scheme.

Unforgability

Each smart card has embedded IC chip that stores the broker's secret key K_B and SUM. The properties of the smart card are tamper resisted and data protected, which cannot be read except by the issuer.

It is assumed here that no one can obtain the broker's secret key which is stored in the smart card. Thus, the customer's secret key $K_C = MAC(K_B, ID_C)$ is impossible to be decoded through computing without the broker's secret key. On the other hand, the $PMES$ can be acquired through an open network, but forger can not obtain the secret key. Because the $MAC()$ is a one way hash function which makes it difficult to find the customer's secret key.

During the payment process, it is impossible for a forger (include the merchant) attempting to forge a secret key K'_C on behalf of a legal customer. Because the forger will find it hard to get a valid H', $MAC(K'_C$, $ID_C\|$ $ID_M\|$ $AMOUNT\|$ $SER)$ and let $H' = MAC(MAC(K_B, ID_C)$, $ID_C\|$ $ID_M\|$ $AMOUNT\|$ $SER)$.

In addition to the above, let us assume that there is a person who steals the payment message, and alters the ID_C to another customer's ID. Then, he takes the $PMES'$: $\{ID'_C$, ID_M, $AMOUNT$, SER, $H\}$ to pay for the purchases. The merchant's device will determine that the payment message is invalid by checking the Equation 1.

Therefore, this scheme is secure against forgery. Nobody can forge a legal customer to generate a valid payment message without the legal customer's secret key.

Authentication and Integrity

This scheme uses a message authentication code for authenticating the payment message. We assume that the broker is a trusted party in issuing each customer's identity and secret key. The secret key $K_C = MAC(K_B, ID_C)$ is generated with the broker's secret key K_B. Without the broker's secret key, nobody can derive the valid secret key of customer. Therefore, except the trust broker we can believe that the secret key K_C is only known by the corresponding customer.

The broker can authenticate that who issues the payment message. In previous section, we showed that no one can forge a valid payment message on behalf of a legal customer. Therefore, the broker is convinced that the message is issued by a certain customer if the authentication is correct in Equation 1. It is, hence, the certain customer can not deny what he has issued about the purchasing. .

The broker also can verify the integrity of the payment message. If an attack attempts to alter $AMOUNT$ to charge more money or alter ID_M to reuse the payment in other merchant, it will not be succeed. Because the broker can use the identity ID_M stored in smart card and secret key K_B for authenticating payment messages and this process will prevent the merchant from tampering with the payment value.

Non-repetition

Due to the characteristics of electronic commerce, a payment message can be easily duplicated. There are two cases discussed in this section. We will show this scheme can prevent the customer or merchant from committing double spending or multi-charging. Furthermore, the merchant also establishes a database system to store each authentic payment message.

Let us consider two cases, one is the adventurer taking a prepaid payment message in the same merchant and the other case is the merchant duplicate the payment message for multi-charge. In the first case, assume that an adventurer steals a prepaid payment message through the open network. And the adventurer consumes in the same merchant under the expected legal time interval. However, the merchant can find the last payment record of this customer is the same as the current payment message. The merchant rejects the payment request. If the merchant can not find out this problem, this would mean the payment message has passed the expected legal time interval and, hence, will be rejected too.

In the second case, assume that the merchant duplicates a certain customer's payment message for multi-charge. However, in the Step 3 of Section 3 the broker will reject the same payments in the merchant. Thus anyone attempting to double spending or multi-charge will be thwarted.

5 Discussions

In this section, we discuss the performance of our scheme and compare our scheme with PayWord, Millicent, and SVP.

Our proposed micro-payment scheme is a post-paid and credit based system. The pre-paid system is beneficial for merchant. However, it is somehow not fair for customer. On the contrary, the post-paid system is beneficial for customer, but the merchant and the bank must take their risks. Weather to choose pre-paid or post-paid we must consider the environment of commerce and society. In general, the post-paid system can attract more customers to use.

Several micro-payment methods are briefly introduced in Section 2. The PayWord, MicroMint, SVP, NetBill, and ikp are post-paid micro-payment sys-

Methods		Our scheme	PayWord	Millicent	SVP
Public key signature	C	0	1	0	0
	M	0	2	0	0
	B	0	1	0	0
Symmetric key encryption	C	1	0	4	1
	M	2	0	2	2
	B	1	0	2	1
Hash function	C	1	n	0	1
	M	2	n	2	2
	B	1	n	2	1
Network connection	B-C	0	0	1	0
	C-M	1	1	1	2
	M-B	0	0	0	0

Table 1: The summary of the computation and communication cost for off-line based micro-payment systems.

tems and only the MIllicent is the pre-paid micro-payment system.

In order to reduce the overhead of communication, transactions with the central authority, such as broker or bank should be reduced or eliminated. The payment message can be authenticated by the merchant. This means message does not forward to the bank. This is also called an off-line based micro-payment system. Most micro-payment systems uses off-line process, such as PayWord, Millicent, SVP, and the proposed scheme, trading the security off efficiency.

Our proposed micro-payment scheme uses MAC hash function to generate and verify the payment message. The ISO standard of MAC algorithm is described in (ISO/IEC 9797, 1989). It is the simplest way to perform the MAC function. The algorithm uses DES or FEAL encryption function to encrypt the hash value. Furthermore, the cost of MAC computation is a hash computation and a symmetric key encryption.

We compare our scheme with other off-line based micro-payment schemes in the literature. The performance of computation and communication of each transaction is summarized in Table 1. In this table, C represents the customer, M represents the merchant, and B represents the broker. The four micro-payment schemes are off-line based and batch settlement micro-payment

Operation	Number per second
Public key signature (1024 bits RSA)	2
Symmetric key encryption (DES)	2,000
One way hash function (MD5/SHA)	20,000
Network connection (TCP/Internet)	1,000

Table 2: The comparisons of the computation and network connection speed.

system. The settlement phase of these schemes are off-line and not frequency. Therefore, we does not determine the cost of this phase. Furthermore, in the four micro-payment schemes, merchants must maintain a small database to prevent double spending and store each payment message. After settlement phase, the database can be cleaned. This property prevents the database unlimited growth.

Table 2 shows comparisons of public key signature, symmetric key encryption, hash function, and network connection, that can be performed number per second on a typical workstation. The data references (O'Mahony, Peirce, and Tewari, 1997; Schneier, 1996). The hash function and symmetric key encryption cryptography are more fast. They are suitable for micro-payments. According to the summary of these micro-payment schemes. PayWord uses a public key signature to generate and verify a certificate, this is not efficient. Millicent uses more symmetric key encryption and customer must redeem the vendor scrip firstly. Our proposed scheme is similar to SVP. We all use MAC to authenticate the payment message and use a special device, e.g. smart card. However, our scheme uses less parameters and network connection. Therefore, our proposed scheme is efficient to suite micro-payments.

6 Conclusions

This paper proposed a simple micro-payment scheme that is a efficient and low cost method. This simple micro-payment scheme was developed based upon the using of smart card and the message authentication code. This scheme was designed to provide good efficiency and low transaction cost. It is especially suitable for micro-payments for information goods on the Internet. This system allows payments to be authenticated and information goods to be purchased in real time. Furthermore, this scheme is a post-paid and off-line based micro-payment system.

Acknowledgements

The author wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-324-006.

References

Anderson, R.J., Kuhn, M.G., 1996. Tamper resistance - a cautionary note. Proc. of The 2nd Usenix Workshop on Electronic Commerce, Oakland, California, U.S.A., pp. 1-11.

Bellare M. et al., 1995. iKP-A family of Secure Electronic Payment Protocols. IBM. (http://www.zurich.ibm.com/Technology/Security/extern/ ecommerce/)

Boly, J.P., et al., 1994. The ESPRIT project CAFE-high security digital payment system. Computer Security - ESOLICS'94, vol. 875, Nov.

Chaum, D., 1983. Blind signatures for untraceable payment. Advances in Cryptology-Crypto 82, pp. 199-203.

Chaum, D., Fiat, A., Naor, M., 1990. Untraceable electronic cash. Advances in Cryptology-Crypto 88, pp. 319-327.

Chaum, D., Pedersen, T.P., 1993. Wallet database with observers. Advances in Cryptology-Crypto 92, pp. 89-105.

Doggest, J., 1995. Electronic check project. Financial Services Technology Consortium (FSTC). (http://macke.wiwi.hu-berlin/IMI/micropayments.html)

Damgard, I.B., 1990. A design principle for hash functions. Advances in Cryptology-Crypto 89, pp. 416-427.

Davies, D.W., 1985. A message authentication algorithm suitable for a mainframe computer. Advances in Cryptology-Crypto 84, pp. 393-400.

Dhem, J.F., Veithen, D., Quisquater, J.J., 1996. SCALPS: smart card for limited payment systems. IEEE Micro, vol. 163, pp. 42-51.

Ferreira, L.C., Dahab, R., 1998. A scheme for analyzing elecronic payment system. Computer Security Applications Conference 14th, pp. 137-146.

Glassman, S., et al., 1995. The Millicent protocol for inexpensive electronic commence. Digital Equipment Crop..

Hauser, R., Steiner, M., Waidner, M., 1996. Micro-payments based on iKP. IBM. (http://www.zurich.ibm.com/publications/1996/HSW96.ps.gz/)

Hendry, M., 1997. Smart card security and applications. Artech House.

ISO/IEC 9797, 1989. Data cryptographic techniques-Data integrity mechanism using a cryptographic check functionemploying a block cipher algorithm. Internal Organization for Standardization.

Jones, H.W.E., Watson, A.C., O'Neill, T.J., 1998. Vehicle security using smartcards. Security Journal, vol. 10, no. 2, pp. 79-87.

Merkle, R.C., 1990-1. One way hash function and DES. Advances in CryptologyCrypto 89, pp. 428-446.

Merkle, R.C., 1990-2. A fast software one-way hash function, Journal of Cryptology, vol. 3, no. 1, pp. 43-58.

Manassee, M., 1995. Millicent (electronic micro-commerce). Digital Equipment Corp..

MasterCard and Visa, 1997-1. Secure Electronic Transaction (SET) specification book 1: business decryption.

MasterCard and Visa, 1997-2. Secure Electronic Transaction (SET) specification book 2: programmer's guide.

Naccache, D., M'Raihi, D., 1996. Cryptographic smart cards. IEEE Micro, pp. 14-24.

NIS and NIST FIPS PUB 46-2 Technology, 1993. Data encryption standard. U.S. Department of Commerce.

Neumann, C., Medvinsky, G., 1995. Requirements for network payment-the NetCheque perspective. IEEE Compcon.

O'Mahony, D., Peirce, M., Tewari, H., 1997. Electronic Payment Systems. Artech House.

Rivest, R., Shamir, A., 1997. PayWord and MicroMint: Two simple micro payment schemes. MIT Laboratory for Computer Science.

Rivest, R., Shamir, A., Adleman, L.M., 1978. A method for obtaining digital signature and public-key cryptosystems. Communication of the ACM, vol. 21, pp. 120-126.

Schneier, B., 1996. Applied cryptography (second edition). John Wiley and Sons.

Sirbu, M., Tygar, J.D., 1995-1. NetBill: An internet commerce system optimized for network delivered services. IEEE Personal Communications, vol. 2, no. 4.

Sirbu, M., Tygar, J.D., 1995-2. NetBill: An electronic commerce system optimized for network delivered information and services. Proceedings of IE-

EE Compcon'95.

Stern, J., Vaudenay, S., 1997. SVP: A flexible micropayment scheme. LNCS, Proc. Financial Cryptography Workshop.

Stirland, M., 1998. Smartcards in secure electronic commerce. Information Security Technical Report, vol. 3, no. 2, pp. 41-54.

Vincent, C., Anthony, W., 1998. Access contral determination of smart cards using a quantification of security level. Security Journal, vol. 10, pp. 89-95.

Wayner, P., 1994. Digital cash. Byte, vol. 19, No. 10, pp. 126.