Proceedings of International Conference
on Cryptology and Information Security

# Some On-line Shopping Systems

Hideki Nagano and Hideki Imai

Institute of Industrial Science
The University of Tokyo
7-22-1, Roppongi, Minato, Tokyo, 106 Japan
E-mail: nagano@imailab.iis.u-tokyo.ac.jp

## Abstract

*In this paper, we introduce an on-line shopping system based on credit and debit merged scheme using anonymous channel, and evaluate its security such as privacy, dishonesty and conspiracy. We also propose another on-line shopping system considering a privacy by-pass scheme which reveals dishonest user's name and illegal transactions without revealing user's secret key.*

## 1 Introduction

Recently, an electronic shopping using communication network has attracted a great deal of public attention accompanied with the development of communication and cryptographic technology. Considering the present-time rapid development of communication network, lower cost and faster response on network transactions can be achieved in the near future in case of on-line electronic commerce systems.

We consider the on-line electronic commerce systems here because on-line systems have soundness, that is, if any entities do dishonest acts, then it reveals instantly before the wrong payment has been executed. Many protocols have been proposed enabling users to execute payments with credit card for on-line electronic shopping([7],[4],[6]). These protocols, however, still have some problems as follows:

- Consistency of both privacy and security.
- Accumulation of memory of historical information.
- Measures against money crimes.
- Convenience.

For example, the system organizations, such as the bank or the credit company, can know user's personal information easily.

In this paper, we introduce two on-line shopping systems which overcome the problems mentioned above. First we propose an on-line shopping system based on credit and debit merged scheme which need no memory of historical information. We utilize the anonymous channel and credit company's account to protect user's personal information during dealings. Second we propose an on-line shopping system introducing a privacy by-pass scheme to measure against money crimes such as money laundering. We utilize chinese remainder theorem and key escrow scheme[2] to reveal dishonest user's name and illegal transactions which does not depend on user's secret key.

## 2 On-line Electronic Commerce System Based on Credit and Debit Merged Scheme

In this section we propose one on-line electronic commerce system utilizing credit company's account and anonymous channel, which has the property of both credit and debit system[9].

### 2.1 Elements

Let us introduce four entities which we use in our on-line electronic shopping system.

User(U) : who wants to purchase something.

Shop(S) : which wants to sell commodities over the communication network.

Credit company(C) : in which a user registers before transaction.

Bank(B) : which transfers money between user and shop's account (actually managed by a bank server(Bs)).

### 2.2 Requirements

An on-line shopping system is very useful because anyone can buy something from the distant shop easily. On the other hand, there are many requirements to achieve secure transaction. Here we summarize principal requests in the on-line shopping system.

- An attacker cannot alter or peep the messages dishonestly on the communication channel.
- User's privacy have to be protected; this means no other entities can get user's whole payment information. A user would also be the weakest position of all, so each transaction should be checked by the user in order to prevent forgery.
- No permission of conspiracy among any entities. Even if any entity does the dishonest act, this reveals within the protocol session and no other entity is damaged.

- The exchange of the commodity and its expense should be done smoothly at almost the same time.

In what follows, we explain anonymous channel, the position of credit company, and the transaction simultaneity, which are necessary for our scheme.

### Anonymous Channel

On a communication network with relay stations, shopping schemes using anonymous channel(figure1) are proposed([6],[3]) that enables to keep a secret which channel a sender choose to communicate with a receiver from observers tapping on the communication channel, relay stations except the final relay station, and even from the receiver (Figure1). In anonymous channel we assume that each relay station is operated independently and communicates correctly.

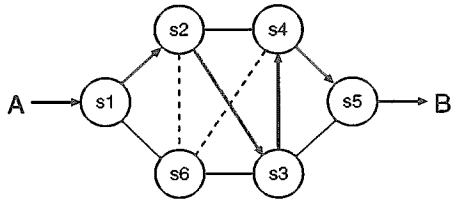


Figure 1: Anonymous channel

### The Position of Credit Company

In general credit based on-line shopping systems, a shop must contract with a credit company and register its name[5], but this makes it difficult to keep user's privacy a secret because of existence of the contact point between the bank and the credit company. Here we consider the case in which the credit company is only an auxiliary system to supply credit company's account to users, which can prevent user's payment information from leaking out.

On the other hand, non-limited lending of credit company's account will have a risk on the credit company if the user cannot or does not pay his expense. It is desirable to set a time or sum limit for using its account according to user's payment capacity or trust information. When the time or sum limit is reached, then the user follows the renewal procedure to the credit company.

### Simultaneity of delivery and transfer

It is desirable to deliver the commodity and transfer its expense at the same time between a user and a shop. However, it is very difficult to achieve the synchronous commerce when a user purchases the commodity far away from a shop like an on-line shopping system. Prepaid or postpaid systems have been adopted in the current system, which have the problems in unpayment or undelivery. Here we consider the scheme which takes some time for transfer in order to avoid the problems mentioned above. To put it concretely, the bank transfer trade money from user's account to shop's account after a certain interval, and until then trade money is stocked into the bank's temporary account. If the user have not received the commodity after the certain interval, he can stop the transaction and trade money is transferred back to user's account.

## 2.3 Protocol

We assume the following:

- Transaction money is a certain or upper limit amount to be profitable.
- The sets of each entity's address and public key are open.
- Transactions between a user and a bank are communicated over anonymous channel.
- A bank executes the protocol correctly and never conspires with any other entities.

The proposed shopping protocol is as follows:

Step 1 : A user makes an application to a credit company for his account beforehand. If it is accepted, then the credit company sends its account encrypted with bank's public key to the user.

Step 2 : When the user wants to buy a commodity from a shop, he sends the commodity's code with user's digital signature and his bank's name to the shop.

Step 3 : After confirming the code and user's digital signature, the shop makes its digital signature on the transaction code and sends it to the user to inform him that the application has been accepted.

Step 4 : After confirming the shop's digital signature, the user sends to the bank the price of transaction money, his account, his shop's name and a pair of session key and header used for anonymous channel so that the bank can send back the receipt to the user.

Step 5 : The bank verifies the validity of the account. If it is right, the bank transfer transaction money from user's account to bank's temporary account, and the bank sends the receipt to the user. The bank also sends to the shop the transaction code, along with the bank's digital signature for reconfirmation.

Step 6 : The shop confirms the transaction code and the bank's digital signature. If it is right, then the shop sends the commodity to the user. At the same time, the shop sends back shop's account to the bank.

Step 7 : The bank transfers transaction money from bank's temporary account to shop's account after a fixed interval when there comes no objection. Finally, the bank sends the receipt of this transaction to the shop and the credit company.

This protocol is formulated below using symbolic expressions (Figure2).

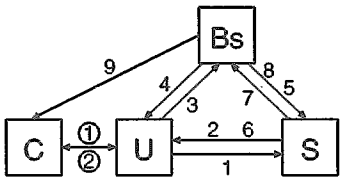


Figure 2: Proposed on-line shopping protocol

Registration protocol

1. U → C : $E_{P_C}(U \parallel D_U(A_U \parallel R_U) \parallel T)$
2. C → U : $E_{P_U}(C \parallel D_C(D_U(A_U \parallel R_U) \parallel T \parallel V) \parallel ACT_C \parallel B)$

Payment protocol

1. U → S : $E_{P_S}(U \parallel D_U(G \parallel Z \parallel L \parallel T) \parallel B)$
2. S → U : $E_{P_U}(S \parallel D_S(M) \parallel B)$
3. U → B : $E_{P_B}(K \parallel H \parallel h(D_S(M)) \parallel Z \parallel ACT_C \parallel S)$
4. B → U : $E_K(B \parallel D_B(h(D_S(M))) \parallel Z \parallel ACT_C \parallel C \parallel O)$
5. B → S : $E_{P_S}(B \parallel h(D_S(M)) \parallel D_B(S \parallel T) \parallel Z)$
6. S → U : $E_{P_U}(S \parallel h(D_S(M)) \parallel Z \parallel Q \parallel T)$
7. S → B : $E_{P_B}(S \parallel h(D_S(M)) \parallel Z \parallel ACT_S)$
8. B → S : $E_{P_S}(B \parallel D_B(h(D_S(M))) \parallel Z \parallel ACT_S)$
9. B → C : $E_{P_C}(B \parallel D_B(h(D_S(M))) \parallel Z \parallel ACT_C)$

where

$M = D_U(G \parallel Z \parallel L \parallel T) \parallel R_S$ : Transaction Identity

$ACT_S = D_S(A_S \parallel R_S) \parallel T$ : Shop's Account

$ACT_C = E_{P_B}(C \parallel D_C(A_C \parallel R_C) \parallel E_{P_C}(D_U(A_U \parallel R_U) \parallel T \parallel V))$ : Credit Company's Account

## 2.4 Security

### Privacy

By using anonymous channel, an observer tapping on the communication network cannot specify the message sender from the encrypted message. The bank also cannot discover the user's name from the received message in spite of recognizing two account numbers under transaction. This is because the user's account, used to transfer between the user and the shop, is credit company's account, and user's address for reply is encrypted with a public key of every relay station. Likewise, the credit company can know only sum of transaction money in user's payment information. All information which each entity can get after the transaction is given in Table2.

Table 1: Notation1

| | |
|---|---|
| $A_X$ | Account number of $X$ |
| $B$ | Bank's name |
| $C$ | Credit company's name |
| $D_X$ | Digital signature of $X$ |
| $E_X$ | Encryption with the key $X$ |
| $G$ | Transaction code |
| $H$ | Header for anonymous channel |
| $h$ | One-way hash function |
| $K$ | Session key |
| $L$ | User's real address |
| $M$ | Transaction identity |
| $O$ | Time margin for delivery |
| $P_X$ | Public key of $X$ |
| $Q$ | Commodity |
| $R_X$ | Random number generated by $X$ |
| $S$ | Shop's name |
| $T$ | Time stamp |
| $U$ | User's name |
| $V$ | Maximum available money |
| $Z$ | Transaction money |

### Dishonesty

By using public key cryptography, an observer tapping on the communication network cannot forge any messages. One of the shop's dishonest act is not to send the applied commodity to the user in Step 6. In this case, however, the user can ask for the bank to stop the transaction before transfer has been finished between user and shop's account. After the transaction is interrupted, the user makes a reconfirmation to the shop to learn if the commodity has really been sent out. One of the user's dishonest act is to ask for bank to stop the transaction by reason of the commodity's undelivery, although he had received the commodity from the shop. There are several ways to solve this problem; for example, shop presents some proofs of the commodity's delivery to bank. But these solution still has problems in the proof process. One of the credit company's dishonest act is to give user a wrong account in registration, but it can also be detected by including information about the account used for practical transaction in the receipt from the bank(Step 5). If any entity deliberately or accidentally executes other incorrect transactions in each step, it is detected by either the user or the bank instantly without failure.

### Conspiracy

The most serious problem of the credit based scheme so far is a leakage of user's secret information by conspiring the shop and the credit company. The proposed scheme solves this problem because there is no contact point between the shop and the credit company. Even in the case that the user and the credit company conspire, the bank verifies whether the received message from the user is right, so other entities including the shop have no damage.

Table 2: Information which each entity can get

| Information | Bank | Credit company | Shop |
|---|---|---|---|
| User ID | × | ○ | ○ |
| Credit Company ID | ○ | – | × |
| Shop ID | ○ | × | – |
| Bank ID | – | ○ | ○ |
| Trade money | ○ | ○ | ○ |
| Trade information | × | × | ○ |

# 3 On-line Electronic Commerce System Introducing a Privacy By-pass Scheme

In this section we consider to apply a privacy by-pass scheme to our on-line electronic shopping system. We use key escrow([2],[8]) for a privacy by-pass scheme which can prevent money crimes, such as money laundering.

## 3.1 Preliminaries

First let us introduce Chinese Remainder Theorem briefly.

Let $p_1, p_2, \ldots, p_k$ be integers $(k \geq 2)$ and every two of which be pairwise relatively prime. We also define the next equation about $P$.

$$\begin{aligned} P &= \prod_{i=1}^{k} p_i \\ &= p_1 P_1 = p_2 P_2 = \ldots = p_k P_k \end{aligned} \quad (1)$$

Then there is at least one integer $b_i (1 \leq b_i \leq k)$ which satisfies the following equation.

$$X \equiv b_1 \bmod p_1 \equiv b_2 \bmod p_2 \equiv \ldots \equiv b_k \bmod p_k \quad (2)$$

The integer solution of the above equation is given by

$$X \equiv (\sum_{i=1}^{k} b_i P_i' P_i) \bmod P \quad (3)$$

where $P_i' = (P_i)^{-1} \bmod p_i$.

## 3.2 Elements

We define three entities which we use in a privacy by-pass scheme.

- User : who produces his personal secret and public keys for communication.
- Trustee : which shares partial information about user's secret key.
- Center : which registers user's name and his public key, and approves its utilization.

If the center executes any dishonest acts, the key escrow system itself cannot work normally. We assume that the center is perfectly trustworthy in this paper.

## 3.3 Requirements

Key escrow system itself has following properties.

- User's privacy can be kept a secret unless at least a fixed number of trustees conspire.
- The center can decodes User's secret key if at least a fixed number of trustees conspire by law enforcement.

However, there are still many problems in its security and reliability in the current key escrow systems. Here we explain principal requirements in our key escrow system.

### Protection of Lawful information

In the presently proposed escrow cash systems based on Diffie-Hellman scheme, once user's secret key has been decoded by law enforcement, all of other payment histories including information unrelated to the crime have been also disclosed. It is desirable, however, to reveal only illegal transactions by introducing key escrow so that other lawful transactions can be still kept a secret. We consider to introduce *session* secret and public keys. Session secret key is based on public key cryptography and not exactly user's secret key which could be produce in every or any transaction. By using this key for encryption of each transaction information with user's digital signature, the center can reveal dishonest user's name and illegal transactions without disclosing user's other lawful payment transactions by law enforcement.

### Dishonesty of Trustees

The current key escrow systems deeply depend its security and reliability on trustees. By the way, when we consider the case that trustees cannot be wholly trustworthy, dishonest acts executed by trustees will become a big problem. And we think it is also very difficult to keep many entirely trustful trustees from a point of view of cost and security. So we had better to release the reliance and dependence on trustees.

As trustees' dishonesty, we consider following cases.

1. One trustee executes dishonest process by itself.
2. One trustee conspires with a user to convince that the center received the proper public key.
3. At least two trustees conspire to decode user's secret key.

We cannot prevent the personal information leakage in the third case. So we assume that each trustee cannot know the existence of others.

### Completeness

In the usual key escrow systems, we consider to establish other organizations which can trustworthy such as a center and trustees. On the other hand, if we can achieve the system which has the completeness in the on-line shopping protocol, it is significant in the respect of cost and completion of commerce. In this

paper, completeness means that we can construct key escrow components with the entities appeared in the electronic commerce system. When we make this into practice, we must be very careful because each entity in the protocol has a large common interest with the secret information they had received.

### 3.4 Protocol

On the basis of these requirements, first we explain key escrow scheme which allows trustees' dishonesty to some extent in Diffie-Hellman scheme using chinese remainder theorem. Next we explain how to apply this key escrow scheme to proposed on-line shopping system.

#### Key Escrow Methods

Assume that there is $n$ trustees and $(N_i, e_i)$ is $i$-th trustee's public key(Figure3).

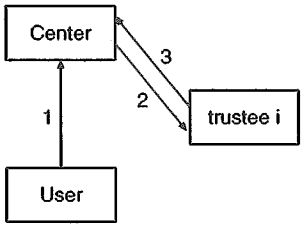


Figure 3: Proposed privacy by-pass protocol

Step1 : A user produces a secret key $X$ and determines each $b_1, b_2, \ldots, b_n$ to meet the equation (2). Then he calculates his public key by the next equation.

$$Y = g^B \bmod P \tag{4}$$

where $g$ is a generator and $B = \sum_i b_i$. Next he also calculates each piece of his public key $w_{i,j}$ correspond to $b_i$ by the next equation.

$$w_{i,j} = g^{b_j} \bmod p_i \tag{5}$$

where $j$ is any number which satisfies $(1 \leq j \leq n, j \neq i)$. Then the user sends the pair $(Y, U_i, w_{i,j}, p_i)$ to the center, where $U_i = b_i^{e_i} \bmod N_i$.

Step2 : The center verifies the next equation.

$$Y = \sum_{i,j}^{n} (w_{i,j} \bmod P_i) \bmod \prod_{k \neq i} p_k, \tag{6}$$

If it is right, then he sends the pair $(U_i, w_{i,j}, p_i)$ to each trustee $T_i$.

Step3 : The trustee $T_i$ verifies $w_{i,j}$ by using the equation (5). If it is right, then he sends it to the center and stores the pair $(b_i, U_i)$. After receiving the notification of verification from all the trustees, the center approves and registers $Y$ as user's public key.

Step4 : When the center wants to decode user's secret key $X$ by law enforcement, he randomly chooses $R_i = r_i \bmod N_i$ and calculates the next equation.

$$Z_i = U_i \cdot u_i \tag{7}$$

where $u_i = R_i^{e_i} \bmod N_i$. Then the center sends $Z_i$ to each trustee $T_i$ and request to send back $z_i$ calculated by next equation.

$$z_i = b_i \cdot R_i \tag{8}$$

Finally, the center calculates $b_i$ by using the equation (7), (8), and decodes the secret key $X$ with the equation (3).

#### Key Escrow Trusting Bank

In the on-line shopping system, we can suppose a bank to be a center, and a shop and a credit company to be trustees. Then we can apply the key escrow system mentioned above to our protocol because we assume the bank to be trustworthy and the shop and the credit company can't conspire. Escrow cash procedure is as follows;

Step 1 : A user produces a pair of secret and public key called session secret and public key. He divides the session secret key into two secret pieces and computes each public piece.

Step 2 : The user sends each pair of a secret piece, a public piece and session public key to the bank.

Step 3 : The bank verifies the pair and sends secret piece of session secret key to the shop and the credit company respectively They verifies the pair in the same way and inform the bank of its validity.

Here we propose an on-line shopping protocol introducing privacy by-pass scheme. This protocol is almost the same as the previous mentioned protocol, so we only formulate below using symbolic expressions.

Registration protocol

1. U $\rightarrow$ C: $E_{P_C}(U \parallel D_U(A_U \parallel R_U) \parallel (F_{UC} \parallel W_C \parallel Y_U) \parallel T)$
2. C $\rightarrow$ U : $E_{P_U}(C \parallel D_C(D_U(A_U \parallel R_U) \parallel (F_{UC} \parallel W_C \parallel Y_U) \parallel T \parallel V) \parallel ACT_C \parallel B)$

Payment protocol

1. U $\rightarrow$ S : $E_{P_S}(U \parallel D_U(G \parallel Z \parallel L \parallel T) \parallel (F_{US} \parallel W_S \parallel Y_U) \parallel B)$
2. S $\rightarrow$ U : $E_{P_U}(S \parallel D_S(M) \parallel (F_{US} \parallel W_S \parallel Y_U) \parallel B)$
3. U $\rightarrow$ B : $E_{P_B}(H \parallel E_{Y_U}(D_S(M)) \parallel Z \parallel ACT_C \parallel S)$
4. B $\rightarrow$ U : $E_{Y_U}(B \parallel D_B(E_{Y_U}(D_S(M))) \parallel Z \parallel ACT_C \parallel C \parallel O)$
5. B $\rightarrow$ S : $E_{P_S}(B \parallel E_{Y_U}(D_S(M)) \parallel D_B(S \parallel T) \parallel Z)$

6. S → U : $E_{P_U}(S \parallel E_{Y_U}(D_S(M)) \parallel Z \parallel Q \parallel T)$
7. S → B : $E_{P_B}(S \parallel E_{Y_U}(D_S(M)) \parallel Z \parallel ACT_S)$
8. B → S : $E_{P_S}(B \parallel D_B(E_{Y_U}(D_S(M))) \parallel Z \parallel ACT_S)$
9. B → C : $E_{P_C}(B \parallel D_B(E_{Y_U}(D_S(M))) \parallel Z \parallel ACT_C)$

where

$M = D_U(G \parallel Z \parallel L \parallel T) \parallel R_S$ : Transaction Identity

$ACT_S = D_S((A_S \parallel R_S) \parallel (W_S \parallel Y_U)) \parallel T$ : Shop's Account

$ACT_C = E_{P_B}(C \parallel D_C((A_C \parallel R_C) \parallel (W_C \parallel Y_U)) \parallel E_{P_C}(D_U(A_U \parallel R_U) \parallel T \parallel V))$ : Credit Company's Account

Table 3: Notation2

| | |
|---|---|
| $F_X$ | Session secret key of $X$ |
| $W_X$ | One share of session public key which $X$ has |
| $Y_X$ | Session public key of $X$ |

### 3.5 Security

Security about on-line shopping system such as privacy, dishonesty and conspiracy is the same as the previous mentioned protocol. So we describe only about security of our key escrow system here.

In the proposed protocol, the transaction ID is represented by transaction information signed with user's digital signature encrypted with session public key. So once user's session secret key is decoded, user's name and transaction information of each transaction can be disclosed by law enforcement. On the other hand, a shop and a credit company cannot conspire, so transaction information cannot be revealed without law enforcement. In any case, user's lawful information can be kept a secret because user's session secret key is not user's private key. But if a user, a shop and a credit company conspire, they can make wrong session secret and public key which can deceive bank to be convinced to get the proper pairs. This is a problem that remains to be solved.

## 4 Conclusions and Further Works

In this paper, we consider electronic commerce systems and introduce an on-line shopping system based on credit and debit merged scheme, which satisfies user's privacy and transaction security at the same time by using anonymous channel. We also explain another on-line shopping system introducing privacy by-pass scheme, which can be achieved to detect illegal transactions securely without revealing dishonest user's secret key and his lawful information.

However, there are still several open problems. The adjustment between the delivery of the commodity and the transfer of its expense is one of the big problem in any on-line shopping systems. Another problem is bank's load and responsibility increase when we introduce more complicated systems, which result in an increase of communication cost and a loss of communication simultaneity. Furthermore we need to consider more secure and established privacy by-pass scheme in the electronic commerce system.

## References

[1] [DH76] Diffie, W. and Hellman, M.E., "New Directions in Cryptography", IEEE Trans. Inf. Theory, IT-22,6 (1976).

[2] [FPC93] S.Micali, "Fair Public-Key Cryptosystems", Advances in Cryptology - Crypto'92 Proceedings (1993).

[3] [PB93] B.Pifzmann, "Breaking an Efficient Anonymous Channel", to appear in the Proceedings of Eurocrypt'93 (1993).

[4] [LP94] Steven.H. Low, Sanjoy Paul, "Anonymous Credit Cards", to appear in the Proceedings of 2nd ACM Conference on Computer Communications Security (1994).

[5] [CCC] Credit Card Club, "Credit Card FAQ", http://mktz.com/creditfaq/faqindex.html.

[6] [SCIS96] T.Yamamoto, R.Sakai, M.Kasahara, "Shopping schemes on anonymous channel", SCIS96-15D(1996).

[7] [DC96] P.Wayner, "Digital Cash - Commerce on the Network -",(1996).

[8] [IT95-51] E.Fujisaki, T.Okamoto, "An escrow cash system", IT95-51(1996-03).

[9] [HN96] H.Nagano, H.Imai, "A practical On-line Shopping System", to appear in the Proceedings of ISITA'96 (1996).